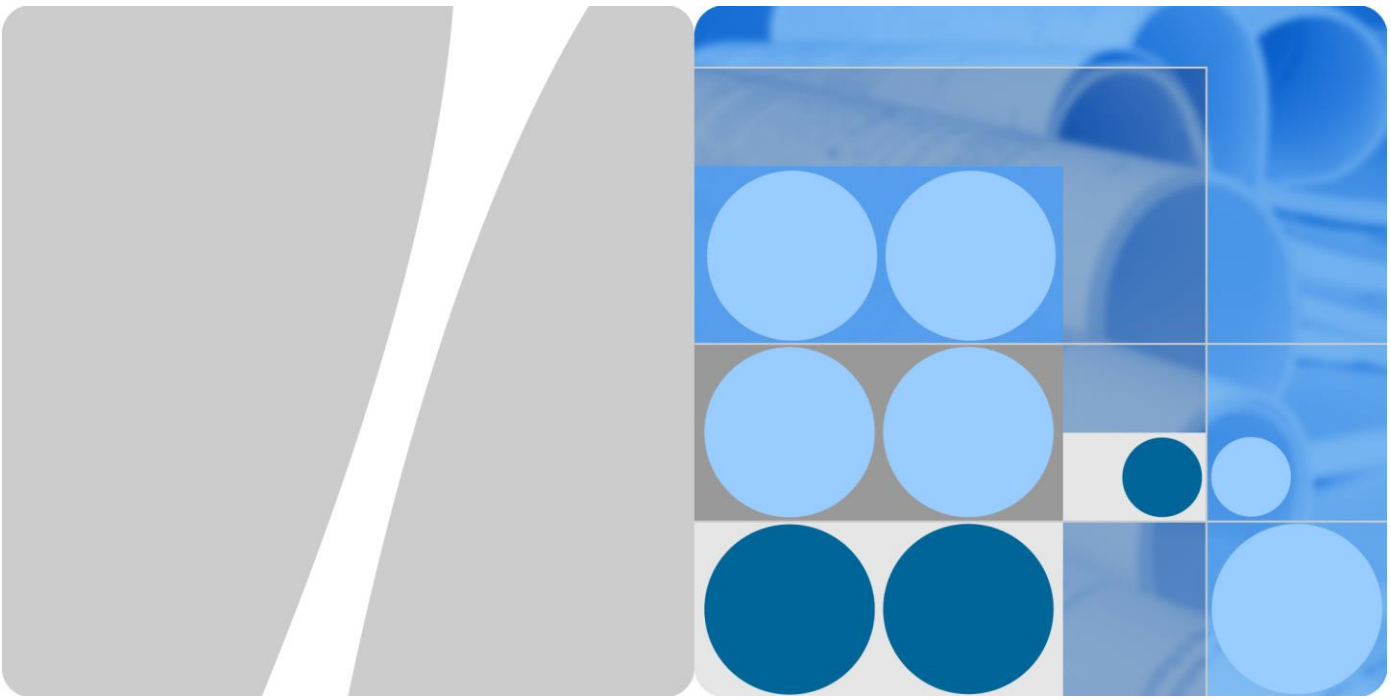


eAN3810A V100R001C00 Deployment Guide

Issue 01

Date 2017-04-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

1 eAN3810A Deployment Guide

About This Chapter

Overview

This document describes how to use the CME and U2000 to configure data for eAN3810A and to commission and verify configured eAN3810A based on design requirements. This document applies to the initial stage of cellular network deployment.

Product Version

NOTE

Unless otherwise stated, "eNodeB", "Pico", "eAN", and "AirNode" in this document refer to the 3810 series AirNode.

The 3810 series AirNode is a base station that provides communications services in Huawei OneAir solution. The following table lists the product name and product version related to the 3810 series AirNode.

Product Name	Product Version
eAN3810A	V100R001C00

Intended Audience

This document is intended for:

- Network planning engineers
- Network operators
- System engineers

Organization

With site deployment, data is planned, delivered, and activated on a per eAN3810A, MicroSD card commissioning and MML can be used.

1.1 Site Deployment Overview

With site deployment, data is planned, delivered, and activated on a per eAN3810A, MicroSD card commissioning and MML can be used.

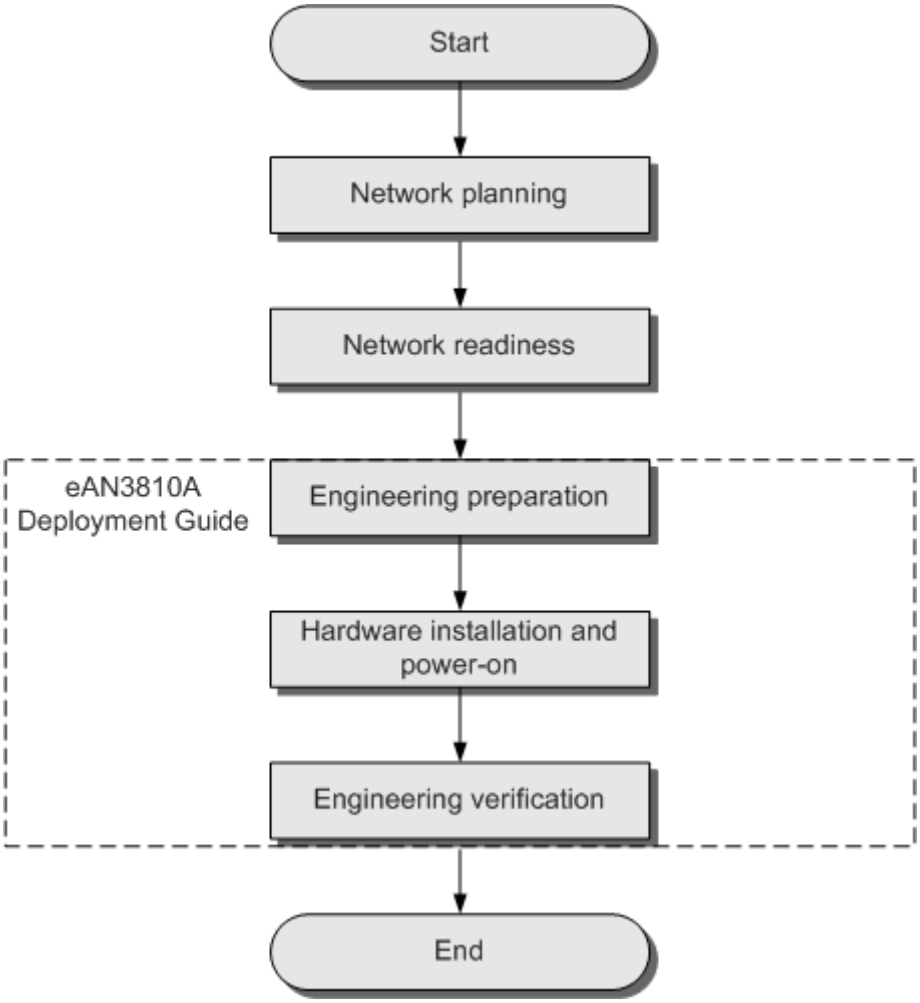
Application Scenarios and Deployment Principles

Site deployment applies to outdoor coverage scenarios where operator-provided private transport networks are used.

Scope

Figure 1-1 shows the procedures for site deployment in this document.

Figure 1-1 Site deployment in this document



1. Network planning: Plan deployment solutions based on network conditions. These include: Networking solution, Transmission solution and Parameter planning.
2. Network readiness: This is a prerequisite to Pico deployment. Specifically, network readiness indicates that the core network, RNC, U2000, SeGW, CA server, and clock server have been deployed and configured, and the transport network is working properly.
3. Engineering preparation: Use the U2000 to prepare configuration data, software packages, and commissioning licenses based on the network plan. At the site, get ready service dialing tools.
4. Hardware installation and power-on: At the site, install and power on the Pico and perform checks.
5. Engineering verification: Create, query deployment results, and verify services.

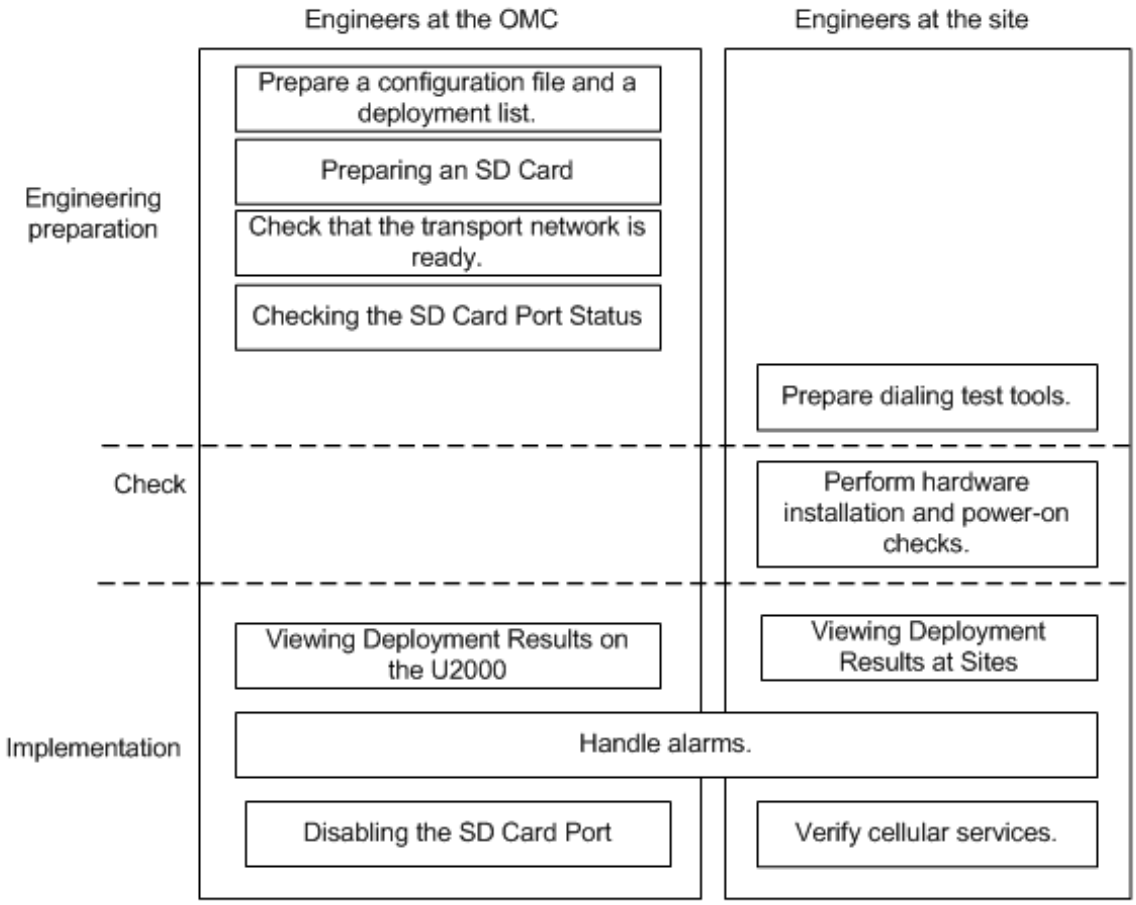
1.2 MicroSD Card Site Deployment

1.2.1 Micro SD Card Deployment Process

This section describes the eAN3810A site deployment process.

Site deployment requires cooperation of engineers at sites and the OMC, who must master the deployment process shown in Figure 1 in advance of the deployment.

Figure 1-2 Site deployment process



1.2.2 Deployment Preparation

This section describes the data and files to be prepared for eAN3810A deployment.

Preparing Common Base Station Deployment Data Files on the CME

This section describes how to prepare, verify, and export common base station deployment data files on the CME.

Data Configuration Process

This section describes the data configuration process. Before configuring data, you are advised to learn the initial base station configuration process on the CME.

Figure 1-3 shows the data configuration process.

Figure 1-3 Data configuration process

Configuration methods are described as follows.

Base Station Creation Method	Scenario	Remarks
Wizard-based single base station creation	No base station has been deployed on the live network or only a small number of base stations need to be deployed.	You can create base stations using the base station creation wizard on the CME.
Batch base station creation using the tool for customizing a summary data file	A large number of base stations need to be deployed, and their planned data differs greatly from data of existing base	You can obtain ranges of MOs and parameters in the summary data file by specifying MOCs in the

Base Station Creation Method	Scenario	Remarks
	stations.	MOC list.
Batch base station creation using the MOC Export function to generate a summary data file	A large number of base stations need to be deployed, and their planned data is similar to data of existing base stations.	You can obtain ranges of MOs and parameters in the summary data file by customizing MOs and parameters using the tool for customizing a summary data file.

Data Preparation

Before starting configuration, prepare data for each eAN3810A based on the network plan. The data to be prepared includes basic data, device data, transport data, and radio data.

Select data preparation tables by scenario and prepare the data in the tables. Table 1-1 describes scenario-specific data preparation tables .

Table 1-1 Scenario-specific data preparation tables

Scenario	Data Preparation Table (on the eAN3810A Side)
Non-secure transmission networking	Click Data Preparation in Non-secure Transmission Networking to download the table. Data to be prepared on the eAN3810A side for enabling cellular services includes device data, common transport data, LTE radio data.

Creating a Work Area

The CME provides one current data area and allows users to create multiple planned data areas. The current data area is used for synchronizing and saving configuration data on the live network, and you can only view data in the current data area. A planned data area is used for configuring data. Therefore, you need to create a planned data area before configuring data.

Context

CME functions can be started in the following modes. Table 1-2describes the modes. The navigation paths for starting CME functions are different in CME client mode and U2000 client mode. For example, to enable the function of customizing a summary data file on the CME, choose **Advanced** > **Customize Summary Data File (CME client mode)** or **CME** > **Advanced** > **Customize Summary Data File (U2000 client mode)** on the menu bar.

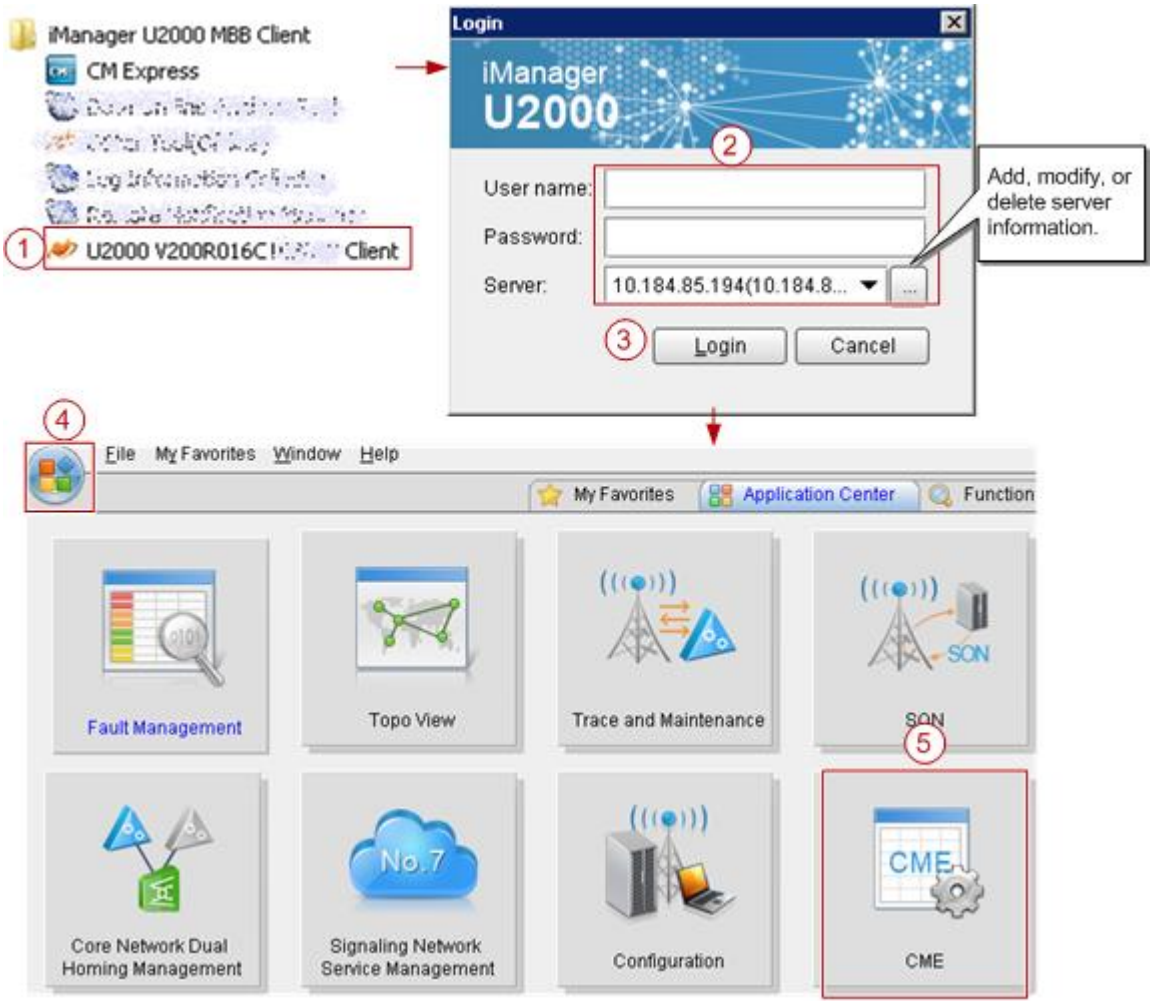
Table 1-2 Startup modes

Startup Mode	Description
CME client mode	This mode applies when the CME functions are used. In this mode, only the CME functions are started, and the U2000 functions are not started, such as fault management, topology management, and performance management. In this mode, the CME functions can be started using either of the following methods: • Start CME functions on the U2000 client in application mode. • Start the CME client directly.
U2000 client mode	This mode applies when both the CME and U2000 functions are used. In this mode, both the CME functions and U2000 functions (such as fault management, topology management, and performance management) are started. For detailed operations, see Start CME functions on the U2000 client in traditional mode.

Procedure

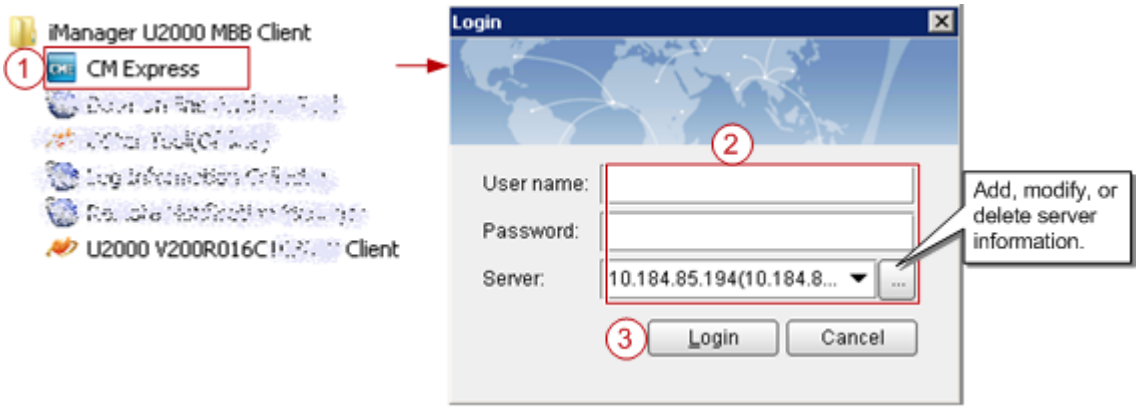
1. Start the CME.
   - Start CME functions on the U2000 client in application mode.

     On the Windows desktop, choose **Start** > **All Programs** > **iManager U2000 MBB Client**.



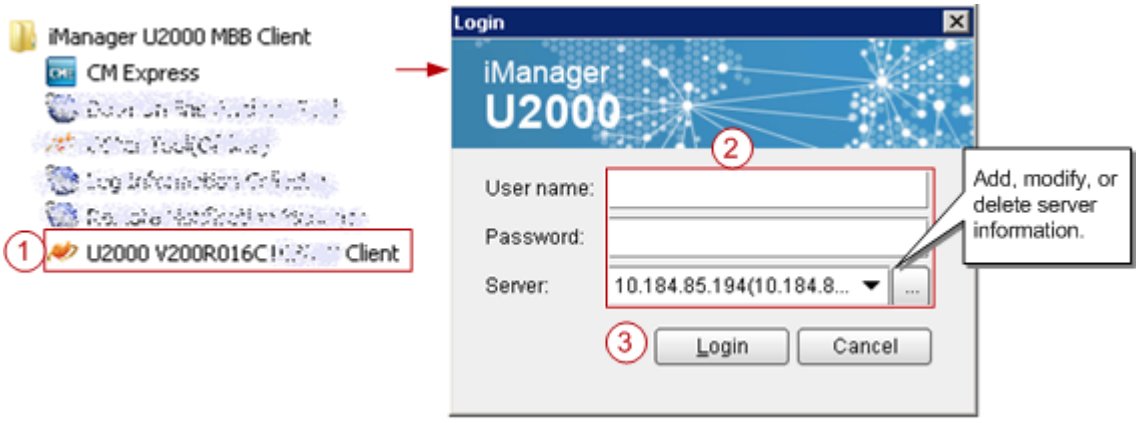
– Start the CME client directly.

  On the Windows desktop, choose **Start** > **All Programs** > **iManager U2000 MBB Client**.



– Start CME functions on the U2000 client in traditional mode.

  On the Windows desktop, choose **Start** > **All Programs** > **iManager U2000 MBB Client**.



After logging in to the U2000 client, choose **CME** on the menu bar of the U2000 main window and then choose a submenu item to start the related CME function.

2. Create a planned data area.
   a. On the menu bar, choose **Area Management** > **Planned Area** > **Create Planned Area** (CME client mode) or **CME** > **Planned Area** > **Create Planned Area** (U2000 client mode). A dialog box is displayed for you to create a planned data area.
   b. Set related information.
      i. Enter the name of the planned data area.
      ii. Select a user group.
   c. Click **OK**. The CME starts to create the planned data area.

      After successfully creating the planned data area, the CME automatically opens it.

NOTE

- If a multimode base station capable of working in LTE mode is to be created, add the controller associated to the base station to the planned area when you create a planned area.
- For details about how to create a planned data area, press **F1** to obtain the online help.

Configuring Data on GUIs

This section describes how to initially configure a single base station on GUIs using a default or user-defined template.

?.1.Creating Base Stations

This section describes how to create base stations. To create base stations, you need to start the wizard provided by the CME for creating base stations, set basic base station data, and select a required template. After the base stations are created, configure global data and maintenance modes for the base stations in the general configuration window of the CME.

Procedure

1. On the menu bar of the planned data area, choose **CME** > **OneAir Application** > **Create Base Station** (U2000 client mode) or **OneAir Application** > **Create Base Station** (CME client mode). A dialog box is displayed for you to create base stations.
2. Set site information.
   a. Select **eAN3810A** from the **Product type** drop-down list.

b. Set basic base station information, including the base station name, ID, version. The CME provides two types of base station templates:
   - Base Station template
   - Radio template

3. Click **Next** and set basic information and radio template for each RAT.

   The eNodeB ID can be set to any valid value. After the configuration takes effect, the base station name is automatically changed to ESN, and the eNodeB ID is automatically changed to the value allocated on the U2000.

4. After the configuration is complete, click **Next**. The CME starts to create a base station.
5. Click **Finish** to exit the wizard.

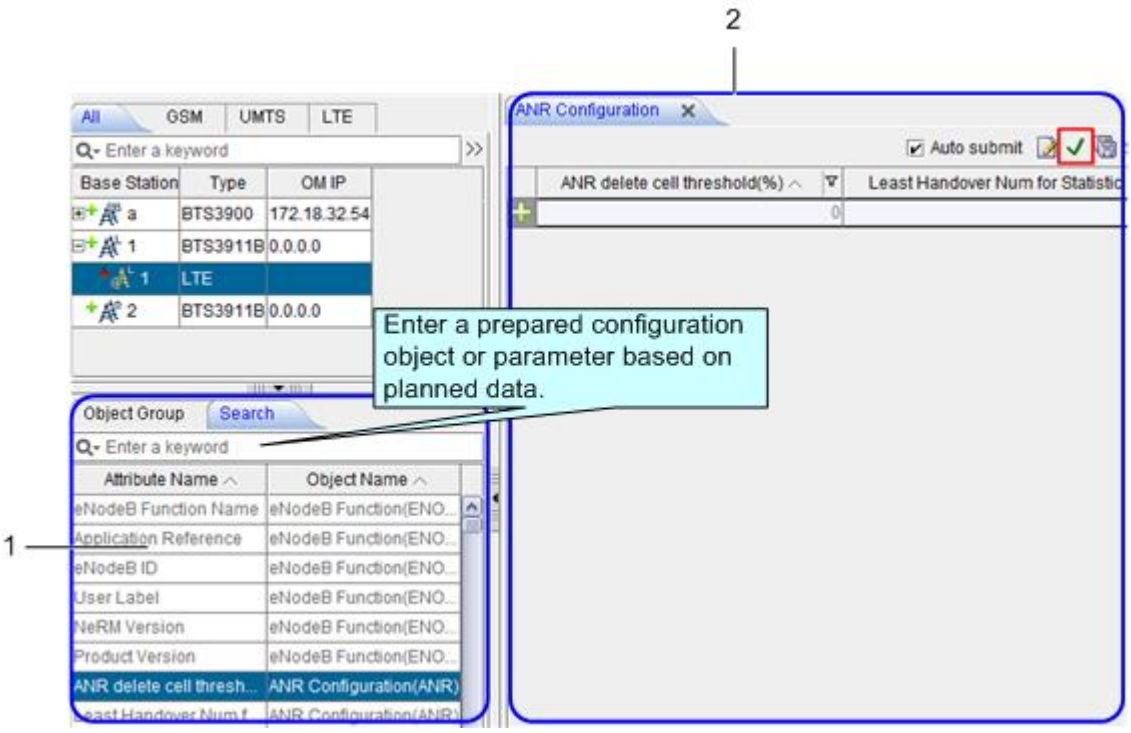
?.2.Configuring eAN3810A Data

This section describes how to configure device data, transport data, and radio data for the eAN3810A by using the CME.

Procedure

1. Click the required tab (Controller/Base Station/Cell) in the left pane of the planned data area. On the displayed tab page, select an item. The navigation tree of involved configuration objects is displayed in the lower part of the left pane. See Figure 1-4.

Figure 1-4 Configuration window



2. In area 1, select or search the MO to be configured based on the planned data and double-click the MO. On the displayed page as shown in area 2, set parameters as required, and click  to save the parameter configuration.

NOTE

- To add a record, click + in area 2 and set parameters as required.
- After selecting a base station root node, you can search for the common configuration objects in area 1. After selecting a RAT node, you can search for configuration objects specific to the RAT in area 1. Therefore, you must select a node correctly. Otherwise, target configuration objects may fail to be found in area 1.

Verifying Data

This section describes how to verify the validity and integrity of base station configuration data before you export the data. Validity verification is to check whether base station configuration data meets NE configuration rules. If the data does not meet the rules, it is not sent to NEs. Integrity verification is to check whether base station configuration data is complete. If the data is incomplete, services cannot be provided. For example, a base station without cell data cannot provide radio services.

Prerequisites

You have configured base station data.

Procedure

1. In the left pane of the planned data area, right-click a base station whose data you want to verify and choose **Check Data**from the shortcut menu. The CME starts to verify the data validity and integrity of the base station.
2. View the verification results and modify incorrect data until the validity and integrity of the data are successfully verified.

Exporting the Deployment Lists and Configuration Files of Base Stations

This section describes how to export the deployment lists and configuration files of base stations. After base stations are initially configured on the CME, you need to export the deployment lists and configuration files of the base stations, and then use the automatic deployment function on the U2000 client or use a USB flash drive locally to load the data to the base stations for the data to take effect.

Specifications and Restrictions

- Deployment list: The naming convention is **Auto_Deployment_List_ID of the planned data area_time stamp.xml**. If multiple NEs are selected at a time, the NE data is exported to one deployment list.
- Data configuration script: The script is in XML format. Each site has one configuration script.

Procedure

1. On the menu bar, choose **Advanced Export Auto Deployment Data** (CME client mode) or **CME Advanced Export Auto Deployment Data** (U2000 client mode). A dialog box is displayed for you to export auto-deployment data.
2. Select Site **creation expansion** and click **Next**.
3. Select the base stations whose auto-deployment data you want to export, and click **Next**.
4. Select a save path for the exported file and a method for processing data, and click **Next**.

5. View data in the base station deployment list, and click **Next**. The CME starts to verify data correctness and exports the data.

NOTE

- You are advised to set the connection type to **Common**.
- The ESN is optional. If it is no set, you need to manually associate the ESN with the related base station during the subsequent deployment commissioning.
- You can only set the first-level subnet in the subnet information. To specify a subnet of another level, you can adjust the subnet information in the U2000 topology after the base station commissioning. If the user-specified subnet information does not exist on the U2000, the U2000 automatically generates the subnet during the import of automatic deployment data in the subsequent commissioning.

6. If the export is successful in U2000 client mode, set the following options:
   - Select **Do not open the Auto Deployment window**to close the wizard.
   - Select **Open the Auto Deployment window**. The CME automatically switches to the auto-deployment window and creates a commissioning task.
   - Select **Open the Auto Deployment window and start Auto Deployment task**. The CME automatically switches to the auto-deployment window and starts a commissioning task.
7. Click **Finish**.

NOTE

The save paths for the exported data configuration scripts and deployment lists are as follows:

- Data configuration scripts: **export directory\CfgData\base station name**
- Deployment lists: **export directory\ADList**

You can use the script executor to check and edit the exported data configuration scripts.

Preparing an SD Card

This section describes how to prepare an SD card before loading the software package and data configuration file onto a eAN3810A.

Prerequisites

- The data copy rights have been obtained for the computer used to make the SD card.
- Prerequisites

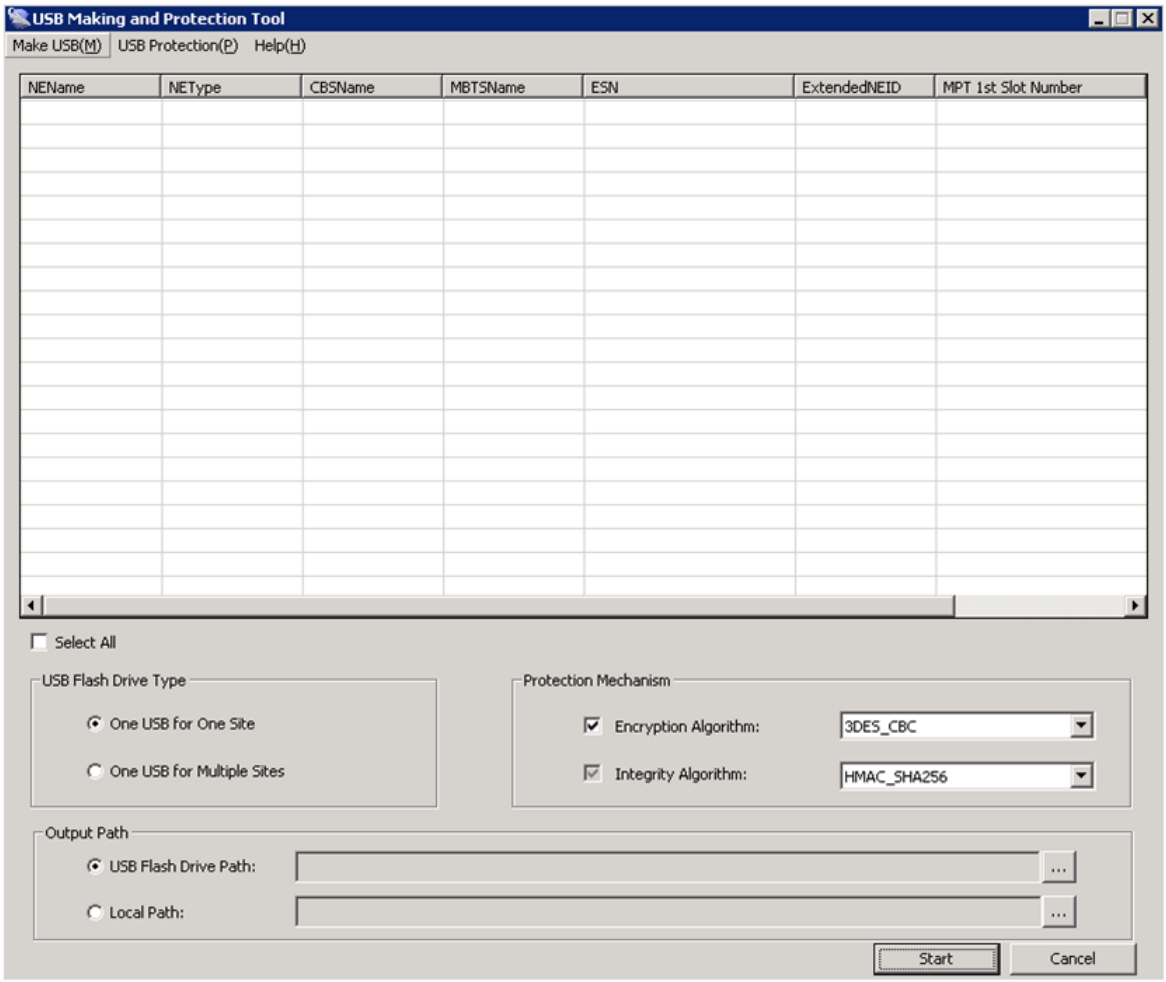
Item	Description
SD card	The SD card must be the one delivered with Huawei eAN3810A.
USB making and protection tool	The tool is saved in **U2000 installation directory\client\client\USBProtector** on the computer where the U2000 is installed.

For details about the save path of each type of file in the SD card, seeDirectory Structure on a MicroSD Card. the tool will automatically generate \ MBTS path, do not manually add the path.

Procedure

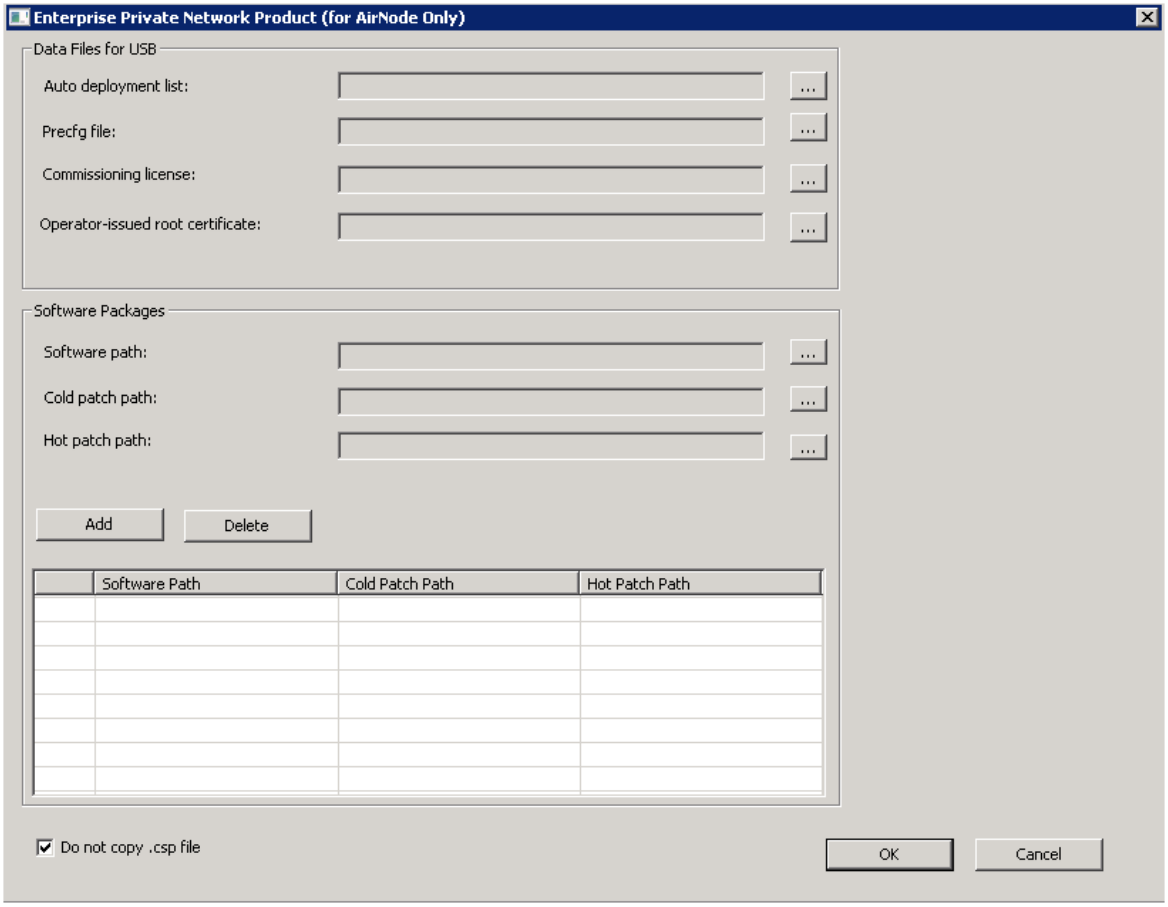
1. Choose **Start** > **Programs** > **iManager U2000 MBB Client** > **USB Making and Protection Tool** to start the tool.

   Figure 1-5 USB making and protection tool



2. Choose **Make USB(M)** > **Enterprise Private Network Product (for AirNode Only)**. The **Enterprise Private Network Product (for AirNode Only)** dialog box is displayed, as shown in Figure 1-6.

Figure 1-6 Enterprise Private Network Product (for AirNode Only)



a. Click ... to the right of **Auto deployment list** to specify the directory where the *Auto_Deployment_List_[Date].xml* file exported from the CME is stored.

b. Click ... to the right of **Precfg file** to specify the directory where the preconfiguration file *Precfg.ini* is stored.

c. Click ... to the right of **Software path** to specify the directory where the software package is stored.

   Click **Add** to add the software package path.

d. Deselect the **Do not copy .csp file** option according to the site deployment scenario.

3. Set the local save paths for the software package and data files based on the type of SD card directory. Then, click **OK**. And then according to the number of open station number (One USB for One Site or One USB for Multiple Sites) and the output directory, click**Start**.

NOTE

When making different types of directories on an SD card, specify items listed in the Information to Set column only and do not set items that are not listed in this column.

Option	Information to Set
Directory for upgrading	• **Software path**: mandatory, save path of the files

Option	Information to Set
the software and updating configuration files	decompressed from a specified version software package • Cold patch path: optional, save path of the files decompressed from a specified cold patch package • **Hot patch path**: optional, save path of the files decompressed from a specified hot patch package Based on different version combinations of NEs to be deployed in the deployment list, specify **Software path**, **Cold patch path**, or **Hot patch path**. Then, click **Add** to add the path to the software version list. Based on the target version information in the deployment list, the USB making and protection tool copies different versions to the corresponding directories of the NEs to be deployed. If an unnecessary software version is added, you can click Delete to remove this software version. **NOTE** The software version of the original and target versions must be eAN3810A V100R001C00SPC200 and later.
	Auto deployment list: mandatory. Select the deployment list exported from the CME. The exported deployment list is saved in **export path/ADList/** by default. Engineers must select the only .xml file in this directory.
	Do not copy .csp file: It is good practice to deselect this option. In this case, all files and integrity protection information except the .csp files are saved in the directories and you can send them through emails. Then, copy the SD card directories to the SD card containing the intact software package. Use this SD card to upgrade the software and update configuration files.
Directory for updating configuration files only	**Auto deployment list**: mandatory. Select the deployment list exported from the CME. The exported deployment list is saved in export path/ADList/ by default. Engineers must select the only .xml file in this directory.
	NE Type and Service Mode: mandatory. Select LTE based on the working mode of the NE.
	Do not copy .csp file: selected by default.

4. The USB making and protection tool automatically parses and displays the information of the target NE on the USB Making and Protection Tool window. Select the NE that requires an SD card. After all NE information is correctly specified, select a deployment mode in the USB Flash Drive Type area.

Option	Description
One USB for One Site	Save the information about each NE to an independent SD card.

Option	Description
One USB for Multiple Sites	• Save the information about all NEs to an SD card. • This mode requires that each NE be configured with a unique ESN.

5. In the **Protection Mechanism** area, select algorithms as required from the **Encryption Algorithm** and **Integrity Algorithm** drop-down lists.
   - **Encryption Algorithm** is optional. It is selected by default and can be cleared. **Encryption Algorithm** can be set to **DES3_CBC**, **AES192_CBC**, or **AES256_CBC**. The default value **DES3_CBC** is recommended.
   - **Integrity Algorithm** is mandatory. It is selected forcibly and cannot be cleared. **Integrity Algorithm** can be set to **HMAC_SHA1** or **HMAC_SHA256**. The default value **HMAC_SHA1** is recommended.
6. In the **Output Path** area, specify a save path.

Option	Description
USB Flash Drive Path	Save all the information to an SD card. All the directories of one SD card are prepared at a time. • One USB for One Site: In this mode, select only one NE and save this NE's information to the SD card. • One USB for Multiple Sites: In this mode, save the information about all NEs to an SD card. The software package is shared by all NEs and the data configuration files are distinguished by directories named after ESN.
Local Path	Save all the information to the specified directory on a local computer. • One USB for One Site: In this mode, a folder is created in a specified directory for this NE and named after NE name. In addition, NE information is saved in this folder. • One USB for Multiple Sites: In this mode, save the information about all NEs to a specified directory. The software package is shared by all NEs and the data configuration files are distinguished by directories named after ESN.

NOTE

The existing data configuration files may be damaged when being copied, encrypted, or integrity protected. To prevent any damages, ensure that USB Flash Drive Path and Local Path do not contain any files or directories.

7. Click **Start**.

   During the procedure, the USB making and protection tool automatically performs the following operations:

   - Applies integrity protection and encryption protection to files in the SD card directories according to manual settings.
   - Copies the configuration files to the SD card directories of corresponding NEs according to the save path of configuration files in the deployment list.
   - Copies all files under the directory specified by Software path to the SD card directories of corresponding NEs according to the directory structure of the SD card.

8. Click OK in the dialog box displayed after the SD card is prepared.
9. **Optional:**If Output Path is set to Local Path, copy the files to the SD card. If Local Path is set to Computer/DataCenter(D:)/SD in step 6:

   - One USB for One Site: Choose Computer > DataCenter(D:) > SD. If the NE to be deployed is site 1, copy the MBTS folder from the Site1 folder to the SD card. See Figure 1-7.
   - One USB for Multiple Sites: Choose Computer > DataCenter(D:) > SD. Copy the MBTS folder from the SD folder to the SD card. See Figure 1-8.

NOTICE

- After a file is copied from a computer to an SD card, the file may change due to faults on hardware or the Windows OS, but this seldom occurs. If the problem occurs, you can copy the file from another computer, to another SD card, or restart the OS and copy the file again.
- To remove an SD card from the computer after the files are copied to the SD card, eject or safely remove the SD card from the Windows OS. If the SD card is forcibly ejected, the files in the SD card may be damaged. As a result, software and data configuration files cannot be loaded by using the SD card.
- When transferring files for an SD card, do not copy the .xml files from a remote desktop to a local computer. Otherwise, deployment will fail. You are advised to compress the required files into a .rar or .zip file for file transfer.

Figure 1-7 File copy procedure in One USB for One Site mode

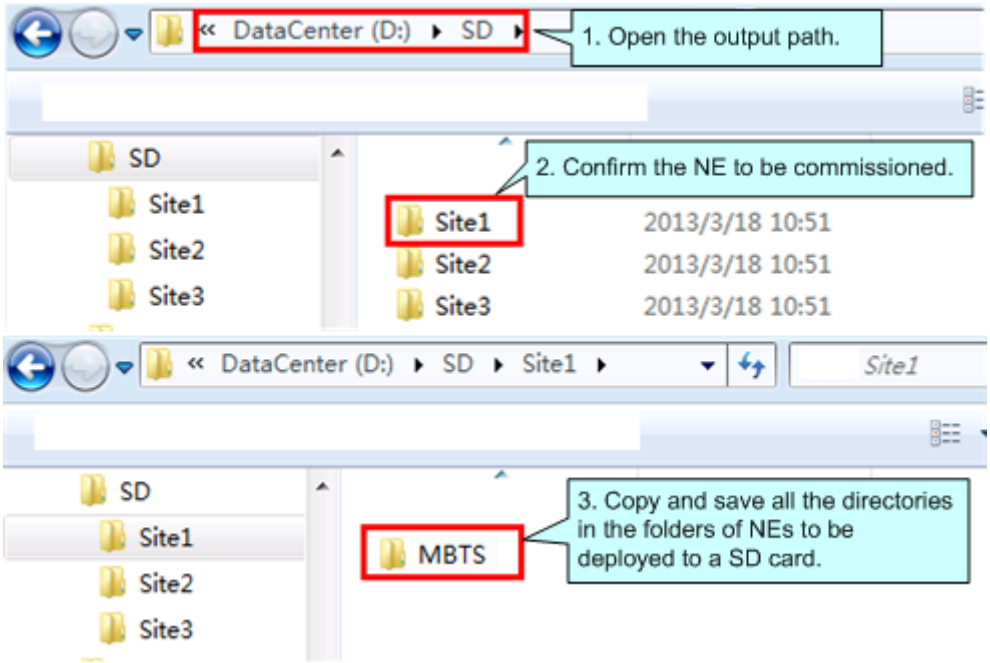
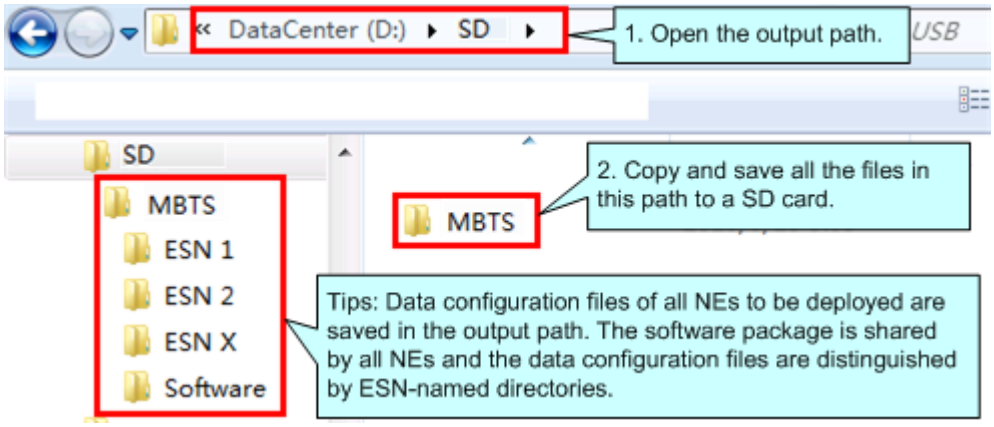


Figure 1-8 File copy procedure in One USB for Multiple Sites mode



10. **Optional:** If you need to preset the operator's root certificate in the SD card, you can manually copy the root certificate file provided by the carrier to the SD card: \ MBTS directory.

Checking a Transport Network

This section describes how to check a transport network. The transport network affects the Automatic OMCH Establishment feature. Therefore, before commissioning an eAN3810A,O&M engineers must check whether the OMCH networking and the network equipment meet the configuration requirements of the corresponding scenario.

Check Methods

O&M engineers can check whether the transport network meets the configuration requirements of the Automatic OMCH Establishment feature by using either of the following methods:

Method 1: Confirm with the department in charge of the transport network whether the transport network meets the requirements.

Method 2:

- Check the network connectivity. If nodes in the transport network can be pinged, ping the port corresponding to each node to check whether the transmission channel at each node is ready.
- Check whether the network equipment at each node is configured as required to ensure that an eAN3810A can automatically establish the OMCH.

Checking the SD Card Port Status

This section describes how to check the SD card port status with MML commands.

Prerequisites

- The transmission network is ready.
- The eAN3710A is connected to the U2000 or Web LMT.

Procedure

Step 1 Run the **LST MICROSDCARDPORT:;** command to verify that the **Port Switch** parameter is **On**.

Step 2 Log in to the U2000 or Web LMT. Run the **SET MICROSDCARDPORT** command with the **Port Switch** parameter set to **On**.

NOTE
The default value of **Port Switch** parameter is **On** upon factory delivery.

----End

Preparing Dialing Test Tools

Dialing tests are performed by using test terminals to check whether deployed eAN3810A can provide services properly. Prepare test terminals and ensure that the test subscriber identity module (SIM) cards have registered with the Core Network.

1.2.3 Hardware Installation and Power-on Check

This section describes how to perform hardware installation and power-on checks at the site after eAN3810A hardware is installed. If a MicroSD card is used for local deployment, engineers at the site need to insert the MicroSD card to the eAN3810A to load software and the configuration file.

Prerequisites

- The SD card has been prepared.
- The eAN3810A is working correctly.

Context

The port for housing a MicroSD card is enabled by default on the eAN3810A. Insert a MicroSD card into the powered on eAN3810A and then restart the eAN3810A to read data from the MicroSD card. Alternatively, insert the MicroSD card into the powered off eAN3810A and then power on the eAN3810A.

Table 1-3 Precautions for using an SD card

Deployment Mode	Precautions
Site deployment	The eAN3810A automatically detects the MicroSD card and installs the driver for the card after a MicroSD card is inserted into the eAN3810A. Then, the eAN3810A automatically reads the files in the fixed directories on the MicroSD card and checks the file names and formats. The eAN3810A compares the software version and configuration data on the MicroSD card with those on the eAN3810A. If consistent, it does not load the software or configuration file on the MicroSD card. If inconsistent, it loads the software and configuration file on the MicroSD card. Note the following points about loading: • If the MicroSD card only stores software, the

Deployment Mode	Precautions
	eAN3810A loads only the software. • If the MicroSD card only stores configuration files, the eAN3810A loads only the target configuration file. • The eAN3810A does not load the software or configuration file on the MicroSD card and its RUN indicator indicates a loading failure (steady on) in any of the following conditions: – The MicroSD card is not intended for it. – The expected directories or files are not present. – The directories or file formats are not correct. – Data in the MicroSD card is not encrypted or integrity protected.

Procedure

- U2000-based commissioning
  a. Ensure that the eAN3810A hardware has been installed and has passed the installation check. For details about how to perform the hardware installation check, see section "Checking Hardware Installation" in *eAN3810A Installation Guide*.
  b. Perform the power-on check. For details about how to perform the power-on check, see section "Power-On Check on the eAN3810A" in *eAN3810A Installation Guide*.
- SD card+U2000-based commissioning
  a. Ensure that the eAN3810A hardware has been installed and has passed the installation check. For details about how to perform the hardware installation check, see section "Checking Hardware Installation" in *eAN3810A Installation Guide*.
  b. Determine whether to restart the eAN3810A after a MicroSD card is inserted based on the power-on status of the eAN3810A.

If...	Then...
The eAN3810A has been powered on.	Insert the MicroSD card into the related port on the eAN3810A. Remove and reinsert the Ethernet cable for power supply, and then go to 3.
The eAN3810A has not been powered on.	Insert the MicroSD card into the related port on the eAN3810A. Connect the eAN3810A to a PSE over an Ethernet cable. Power on the eAN3810A, and then go to c.

  c. Perform the power-on check. For details about how to perform the power-on check, see section "Power-On Check on the eAN3810A" in *eAN3810A Hardware Installation Guide*.

     Check the RUN indicator for hardware faults on the MicroSD card. The RUN indicator blinks orange (on for 0.125s and off for 0.125s), if the eAN3810A fails to

read files on the MicroSD card or fails to be deployed. The MicroSD card may be faulty and cannot be detected, if the RUN indicator status does not change.

d. In configuration-free deployment scenarios, wait until the eAN3810A automatically downloads the preconfiguration file and reads the preconfigured information. In site deployment scenarios, wait until the eAN3810A completes the following procedure: automatically loads and activates the software and data configuration files, and restarts itself to make them take effect.

Table 1-4 Mapping between the RUN indicator status and loading status

Loading Status	RUN Indicator Status
The loading succeeds	Slowly blinking (on for 1s and off for 1s) for more than 1 minute
Loading...	Blinking orange and white alternately (on for 0.125s and off for 0.125s)
The loading fails.	Blinking orange (on for 0.125s and off for 0.125s)

NOTE

- In MicroSD card deployment scenarios, the eAN3810A automatically activates the downloaded software and configuration file and then restarts for them to take effect. The activation and restart take about 30 minutes, during which the indicator status is negligible.
- During loading, do not remove the MicroSD card.

e. Remove the MicroSD card only after you have confirmed that the loading succeeds.

Follow-up Procedure

If the software version is incorrect after the loading process is completed, perform the following operations:

1. Insert a MicroSD card storing the correct software version to the eAN3810A.
2. Remove the MicroSD card after the eAN3810A loads the software package and successfully completes the upgrade.

1.2.4 Engineering Verification

This section describes how to complete the eAN3810A commissioning task, view deployment results, and verify services.

Viewing Deployment Results at Sites

This section describes how to view deployment results at sites based on indicator status.

Check the status of indicators on a newly deployed eAN3810A.

The following table shows the indicator status if an eAN3810A is deployed successfully and working properly. See Table 1-5

Table 1-5 Indicator status of a functional eAN3810A

Indicator	Status
RUN	Steady white
ETH	Slow blinking white (on for 1s and off for 1s)
LINK	Steady white

If the indicator status of an eAN3810A differs from that in the preceding table, contact Huawei technical support engineers.

Viewing Deployment Results on the U2000

This section describes how to view deployment results after an eAN3810A is powered on.

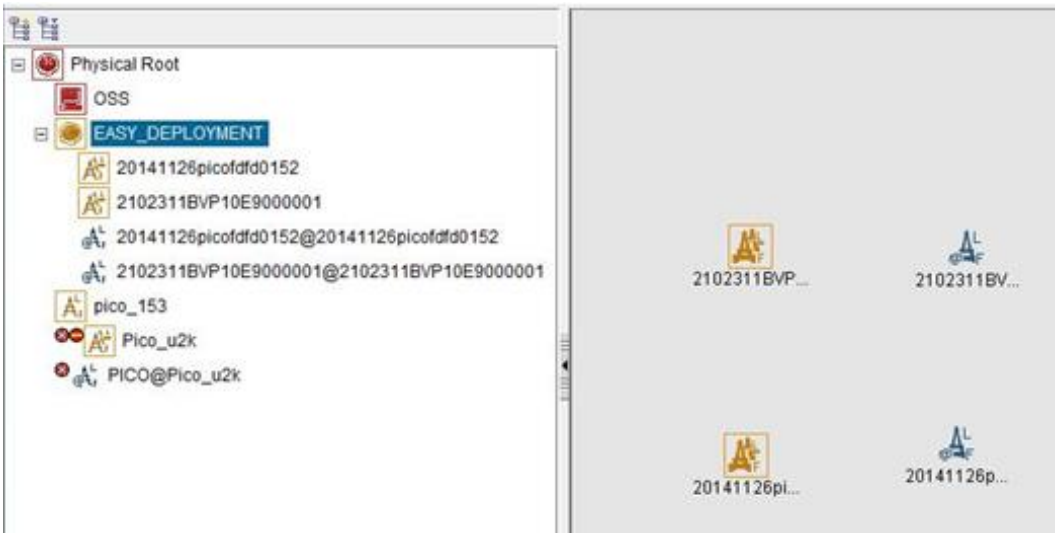
Context

After site deployment is completed, you need to log in to the Web LMT or connect the eAN3810A to the U2000 within 30 minutes. Otherwise, the eAN3810A will be rolled back to the source version upon timer expiry.

Procedure

1. Wait 3 to 4 minutes after an eAN3810A is powered on. Then, on the U2000, choose Topology > Main Topology (traditional style), or double-click Topo View in Application Center and then choose Topology > Main Topology (application style). On the displayed Main Topology window, check whether the eAN3810A topology is created. See the following Figure 1-9.

Figure 1-9 Main topology view



- If the eAN3810A is displayed as  in the main topology, the deployment task is successful. No further action is required.
- If no icon or another icon is displayed for the eAN3810A, the deployment task fails. Proceed to the next step.

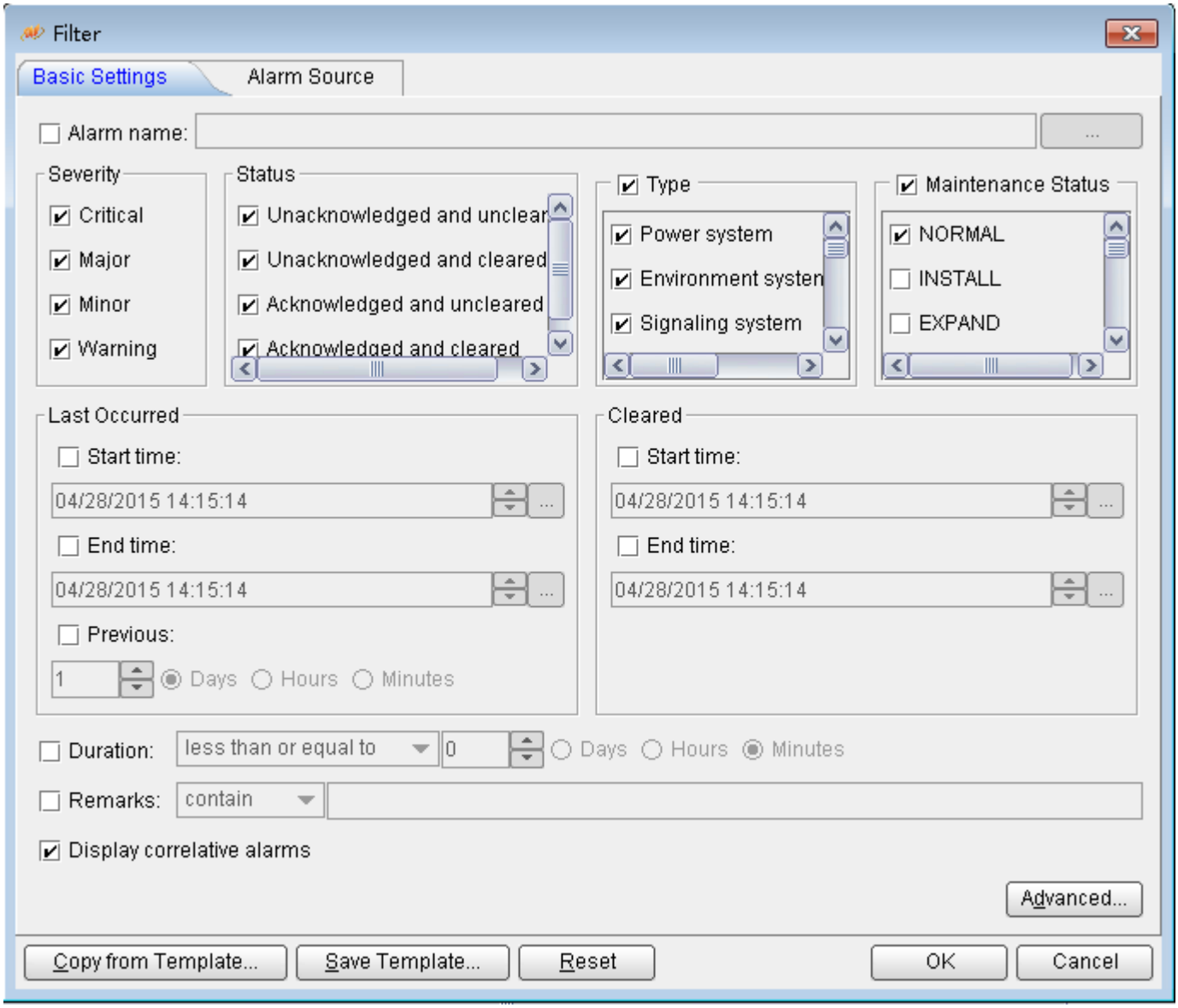
Handling Alarms

This section describes how to handle alarms generated by a newly deployed eAN3810A. All active alarms must be cleared during the commissioning.

Procedure

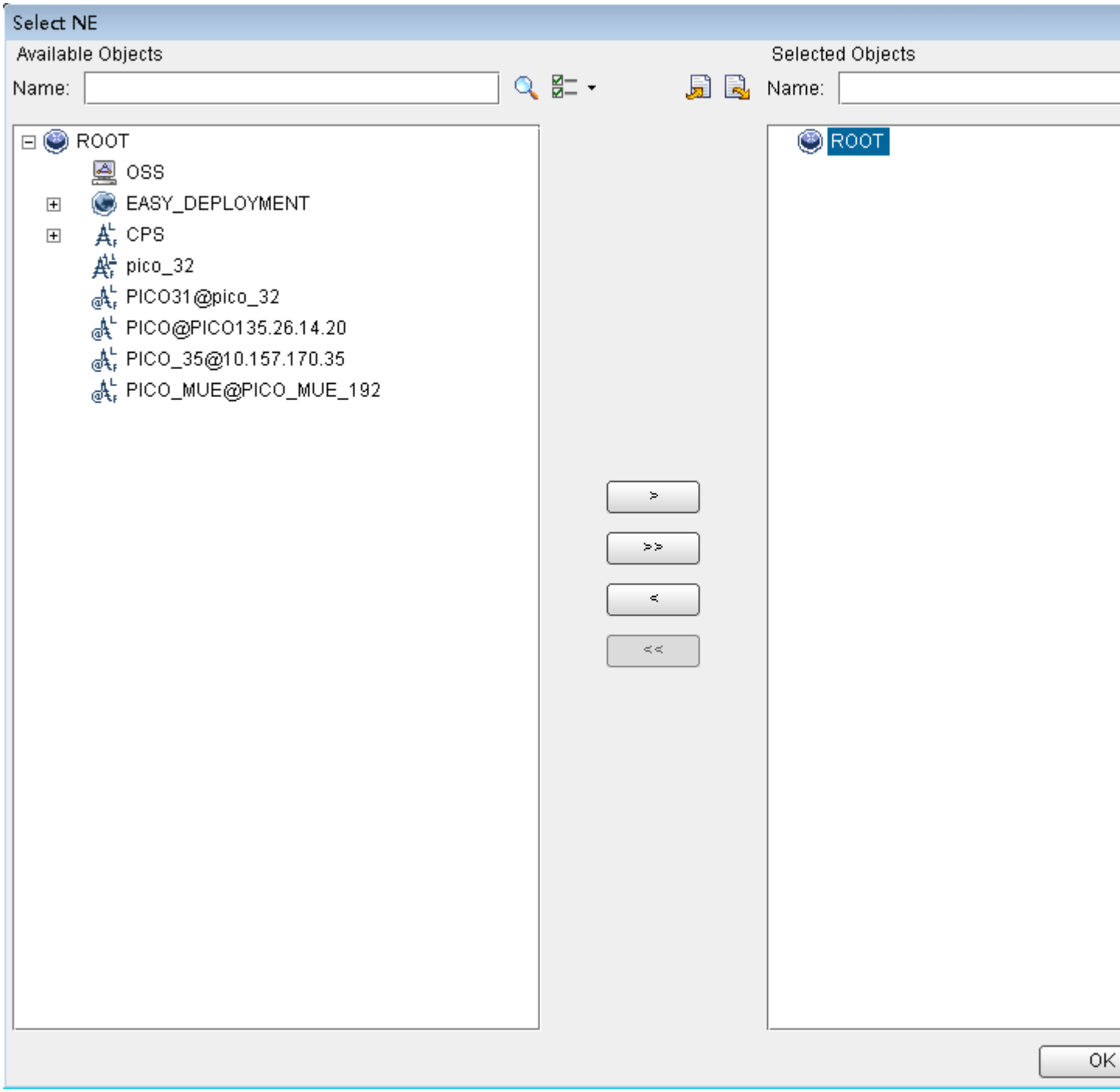
1. On the U2000, choose **Monitor** > **Browse Current Alarms** (traditional style), or double-click **Fault Management in Application Center** and then choose **Browse Alarms** > **Browse Current Alarms** (application style). On the displayed **Browse Current Alarm** window, click **Filter**. The **Filter** dialog box is displayed.

Figure 1-10 Filter dialog box



2. Click the Alarm Source tab and click the Custom option button. Then, click Add and choose NE from the shortcut menu. The NE dialog box is displayed.

Figure 1-11 NE dialog box



3. In the **Available Objects** area on the left, select NEs in the navigation tree.

   Click > to add the selected NEs to the **Selected Objects** area on the right. Then, click **OK**.

4. In the **Filter** dialog box, click **OK**. All alarms reported by the selected NEs are displayed on the **Browse Current Alarm** window.

5. Check the alarms one by one to determine whether they are related to the new eAN3810A deployment. If related, handle the alarms. For details about how to handle the alarms, see the alarm reference.

Disabling the SD Card Port

Prerequisites

- The transmission network is ready.
- The eAN3710A is connected to the U2000 or Web LMT.

Procedure

Step 1 Run the **SET MICROSDCARDPORT** command with the **Port Switch** parameter set to **Off**.

----End

Verifying Services

This section describes how to verify that UEs can attach to the eAN3810A and perform ping services.

Prerequisites

Cells are activated.

UEs have been defined on the core network.

Procedure

1. Check whether UEs can successfully attach to the eAN3810A and perform ping services.

1.2.5 FAQ

This section describes the graphical user interfaces (GUIs) involved in deployment and troubleshooting methods for common problems.

How Do I Set the U2000 Client Display Style?

The U2000 client has two display styles: application style and traditional style. You can set the display style as required.

Context

Switching between styles changes the overall usability of the U2000 client and the way the U2000 client is launched. The U2000 client supports two display styles:

- Application style
- Traditional style

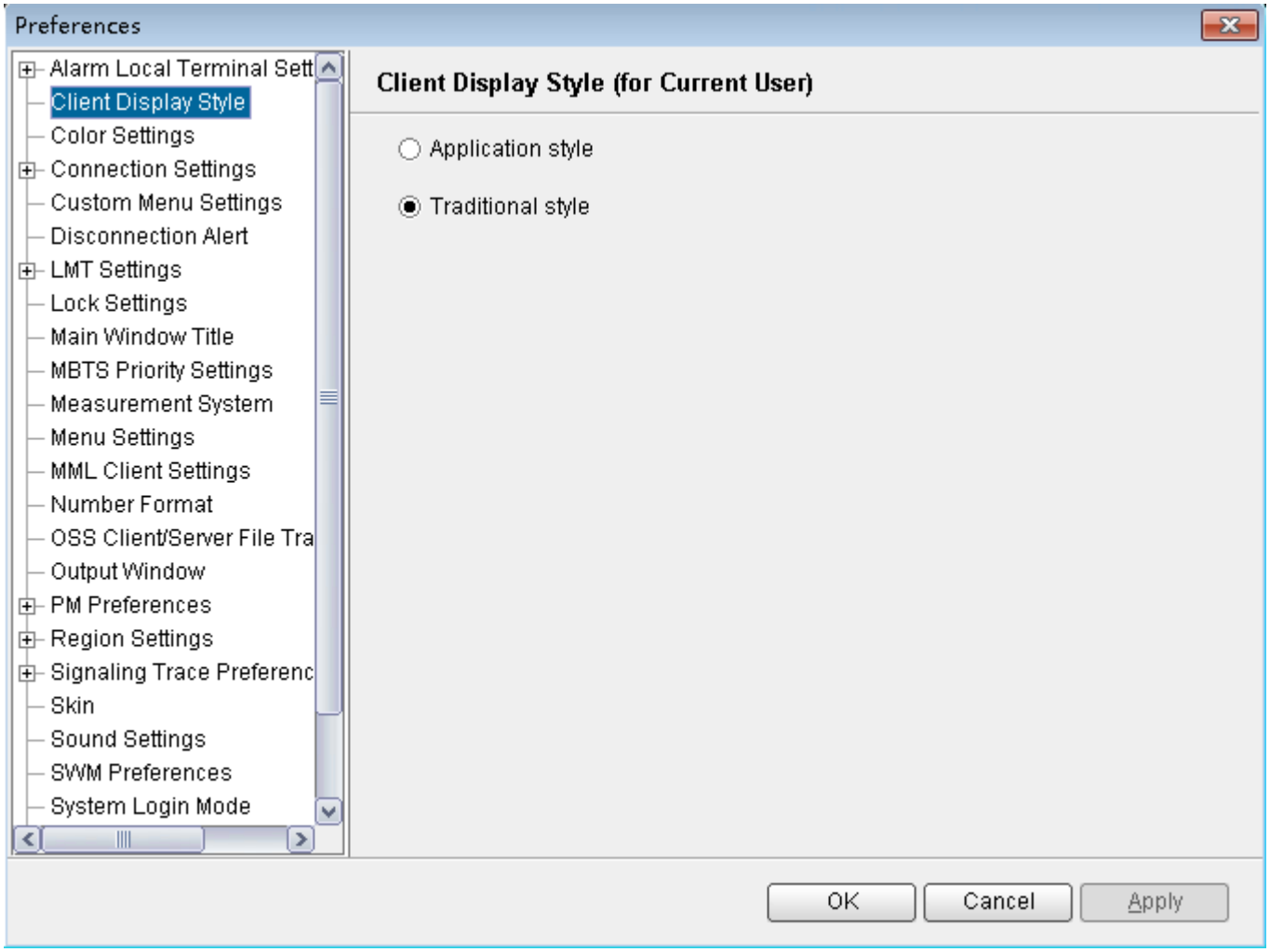
Table 1-6describes the differences between the two styles.

Table 1-6 Differences between the traditional style and application style

Traditional Style	Application Style
The client is launched with all the supported functions and applications.	The client is launched only with the applications required by a user.
Menu items cannot be searched for.	You can search for menu items.
The Favorites feature is not supported.	You can add functions and menu items that are frequently used to the Favorites tab.
Traditional welcome page features are supported.	The welcome page features are not supported.

Procedure

1. On the U2000, choose **System Preferences**(traditional style) or **File Preferences**(application style) from the main menu.
2. In the **Preferences** dialog box, click **Client Display Style** Client Display Style.



3. Select the **Application style** or **Traditional style** option button.
4. Click **OK**.

Follow-up Procedure

Restart the U2000 client for the settings to take effect.

How Do I Prepare a Precfg.ini File?

This section describes how to prepare a Precfg.ini file. This file specifies the software to be loaded during local deployment by a MicroSD card.

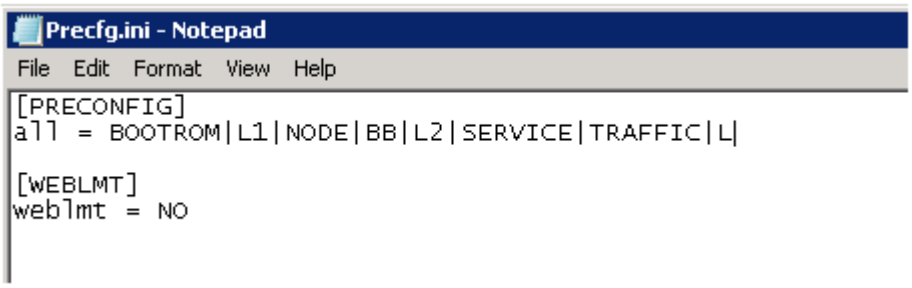
Context

The Precfg.ini file is contained in the software package and can be used only after the target RAT is added.

Procedure

1. Open the **Precfg.ini** file using the Notepad in the Windows OS.
2. Add the target RAT at the end of the **ALL** record in the **Precfg.ini** file.
   - Add |L if the target RAT is LTE.

   Retain the other settings in the file.



3. Save the file and retain the name **Precfg.ini**.

Directory Structure on a MicroSD Card

his section provides the save paths and names for files in a MicroSD card and describes file usage.

Table 1-7 Directory structure on a MicroSD card

Deployment Mode	File	Usage	How to Obtain	Save Path in the MicroSD Card
Local deployment by a MicroSD card	Configuration file	• It specifies the deployment mode and target version.	The MicroSD card making and protection tool	MBTS\DeployCfg.xml

Deployment Mode	File	Usage	How to Obtain	Save Path in the MicroSD Card
		• It provides save paths and check codes for: – Software packages – Configuration files – Certificates – Commissioning licenses	generates the file based on the data in the deployment list.	
	Version software package	Software upgrade	Obtain the software package from http://support.huawei.com/enterprise/.	• MBTS\Software\ • MBTS\Software*software version* **NOTE** When a MicroSD card stores software of different versions, the save paths are named by software version.
	Cold patch package	It is used to apply a cold patch.	Obtain the software package from http://support.huawei.com/enterprise/	• MBTS\ColdPatch\ • MBTS\ColdPatch*cold patch version* **NOTE** When a MicroSD card stores cold patches of different versions, the save paths are named by cold patch version.
	Hot patch package	It is used to apply a hot patch.	Obtain the software package from http://support.huawei.com/enterprise/	• MBTS\HotPatch\ • MBTS\HotPatch*hot patch version* **NOTE** When a MicroSD card stores hot patches of different versions, the save paths are named by

Deployment Mode	File	Usage	How to Obtain	Save Path in the MicroSD Card
				hot patch version.
	Precfg.ini	It specifies the software to be loaded.	It is manually prepared.	MBTS\Precfg.ini **NOTE** For details about how to prepare the **Precfg.ini** file.
	Configuration file	Configuration data update	It is generated by the CME and exported with the deployment list.	The USB making and protection tool copies the file to a MicroSD card directory based on the parameter settings in the tool. • One SD card for a single site: MBTS\CFGDATA.XML • One SD card for multiple sites: SD card:\MBTS\ESN\SlotNo.\CFGDATA.XML

Integrity and Encryption Protection on Files in MicroSD Cards

This section describes how to use the USB making and protection tool to apply integrity and encryption protection to files in MicroSD cards. This prevents malicious modification, unauthorized possession, and information disclosure.

Applying Integrity and Encryption Protection to Files in a Single MicroSD Card

This section describes how to apply integrity and encryption protection to files in a single MicroSD card.

Prerequisites

- The USB making and protection tool is ready. The tool is saved in ***U2000 installation directory*** **\client\client\USBProtector** on the computer where the U2000 client is installed.
- You have scanned the MicroSD card for viruses by using antivirus tools before applying protection. This can prevent files on the computer from infections.
- Files to be protected are ready.

Context

- Integrity protection

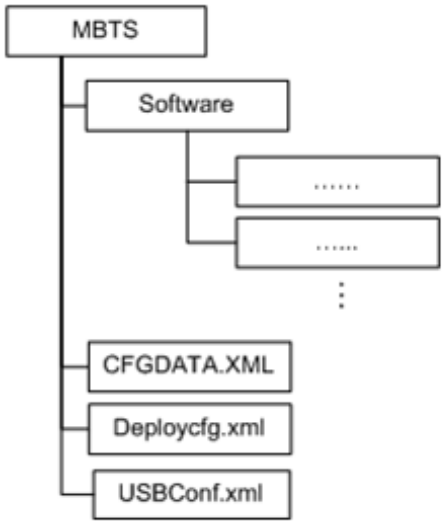
  - The digital signatures in the software and patch packages are used to verify integrity. Do not use the USB making and protection tool to apply integrity protection to these files. Otherwise, deployments or upgrades using a MicroSD card will fail.
  - Integrity protection must be applied to all other files.
- Encryption protection
  - **Do not** apply encryption protection to any files in the SD card if the target version of a base station upgrade does not support SD card-based encryption. Otherwise, deployments or upgrades using an SD card will fail.
  - If the target version of a base station upgrade supports SD card-based encryption,
  - **Do not** apply encryption to the version, BootROM, and patch software packages. Otherwise, deployments or upgrades using an SD card will fail.
  - You **must** apply encryption to the **CFGDATA.XML** file for eAN3810A.
- After you use the USB making and protection tool to apply integrity and encryption protection to files, the **USBConf.xml** file is generated and the file name cannot be changed. When loading files in the MicroSD card, the Pico checks file integrity and decrypts the files based on the data in the **USBConf.xml** file.

Procedure

1. Prepare the directory for files to be protected.

   The directory structure is fixed. It cannot be modified, or deployments or upgrades using a MicroSD card will fail. The following figure shows an example with the CA server deployed in the secure domain.

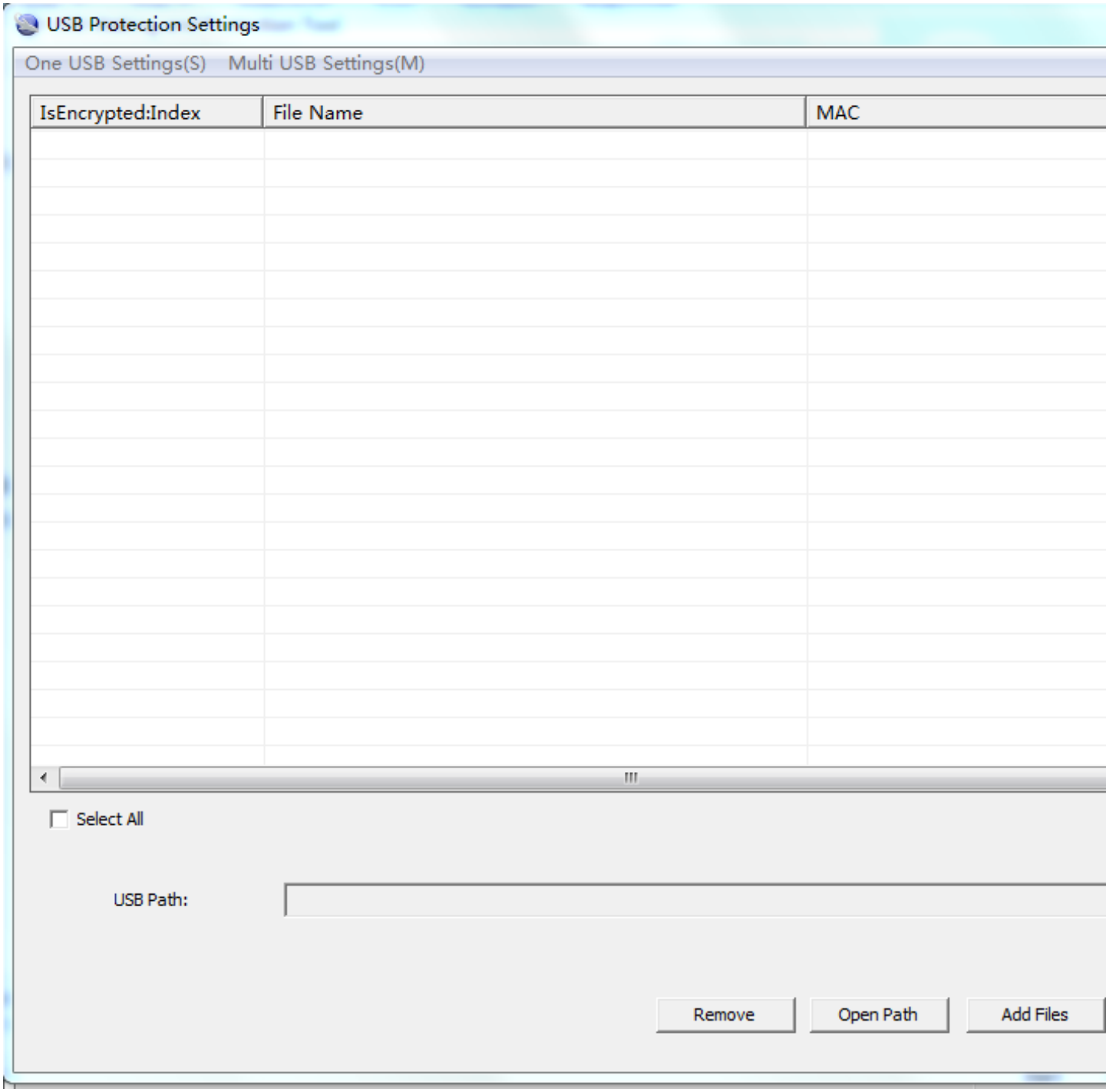
   Figure 1-12 Directory structure for files to be protected (single MicroSD card)



   NOTE
   The USB making and protection tool applies integrity and encryption protection to files but it cannot decrypt files. Back up the files to be protected before applying integrity and encryption protection.

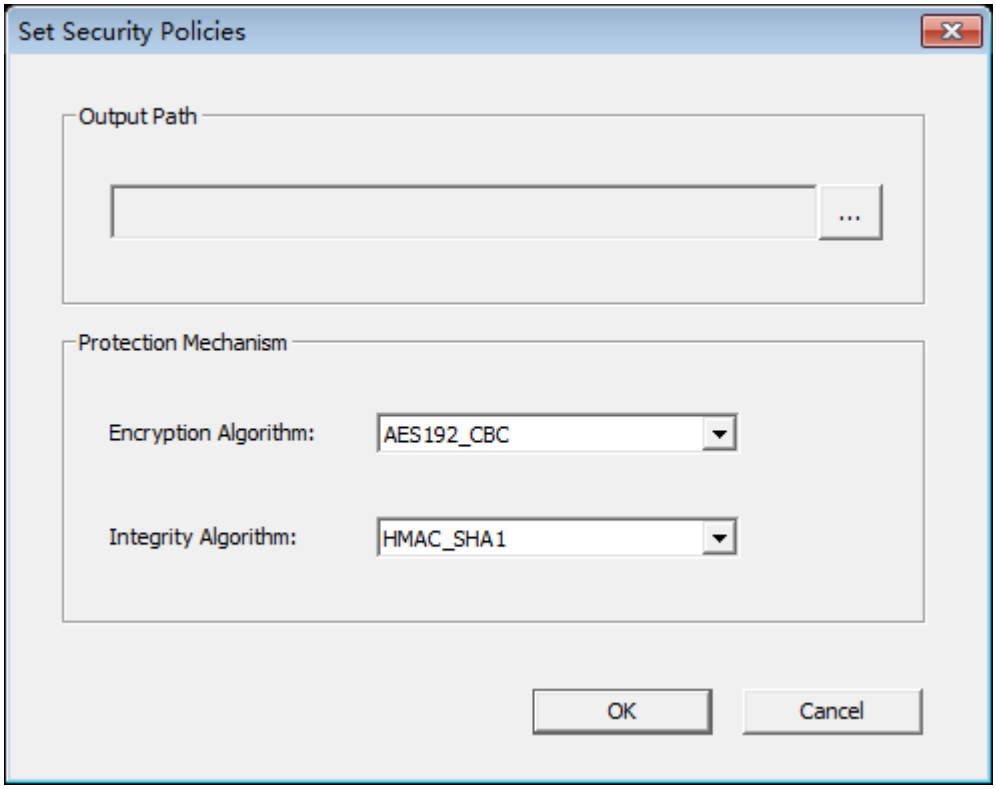
2. Choose **Start** > **Programs** > **iManager U2000 MBB Client** > **USB Making and Protection Tool** to start the tool.
3. Choose **USB Protection** > **USB Protection Settings**. The **USB Protection Settings** dialog box is displayed. See Figure 1-13

Figure 1-13 USB Protection Settings



4. Choose **One USB Settings** > **Set Security Policies**. The **Set Security Policies** dialog box is displayed.See Figure 1-14

Figure 1-14 Set Security Policies



a. In the **Output Path** area, click ... to specify a save path for the **USBConf.xml** file and then click **OK**.

b. In the **Protection Mechanism** area, select algorithms as required from the **Encryption Algorithm** and **Integrity Algorithm** drop-down lists.

   Encryption Algorithm can be set to:

   - DES3_CBC
   - AES192_CBC
   - AES256_CBC

   Integrity Algorithm can be set to:

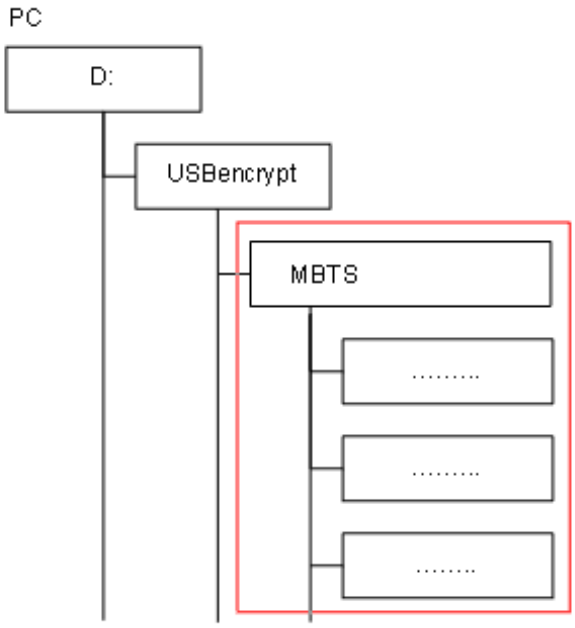
   - HMAC_SHA1
   - HMAC_SHA256

   You can choose any encryption and integrity algorithms but the defaults are recommended.

c. Click **OK**.

5. Choose **One USB Settings Set USB Path**to specify the root path on the local computer for the folder storing files to be protected and click **OK** . The path information will be displayed in the USB Path area after the setting succeeds.In the example shown in the following figure, the path must be set to **D:\USBencrypt\NodeB**, **D:\USBencrypt\eNodeB**, or **D:\USBencrypt\MBTS**.

Figure 1-15 Directory structure example



6. Add files to be protected, and select the **IsEncrypted:Index** check box. The system applies only integrity protection to added files by default. If encryption must be applied to, select the **IsEncrypted:Index** check box.

Option	Description
Adding a single file	Click **Add Files** to select the file to be protected specified in 5.
Adding multiple files	Click **Open Path** and select the path specified in 5. The tool automatically adds all the files in the indicated directory. **NOTE** The tool automatically adds the .csp file in the folder but will not apply integrity protection to it.

NOTICE

describes the files for which integrity and encryption protection must be applied. You must follow these rules; otherwise, deployments or upgrades using a MicroSD card will fail.

- Integrity protection and encryption must not be applied to software and patch packages.
- Integrity protection must be applied to the **Precfg.ini** file. However, encryption must not be applied to the file.
- Integrity protection must be applied to other files. Encryption can be applied to them based on customers' security requirements.

7. Click **Execute Protect**

- The system applies the selected encryption protection to files, and applies integrity protection to all files in the file list area based on the specified integrity algorithm.
- Sizes of files remain the same after encryption is completed because the system uses a symmetrical encryption algorithm.

8. Click **OK**, when a dialog box is displayed indicating the completion of integrity and encryption protection.

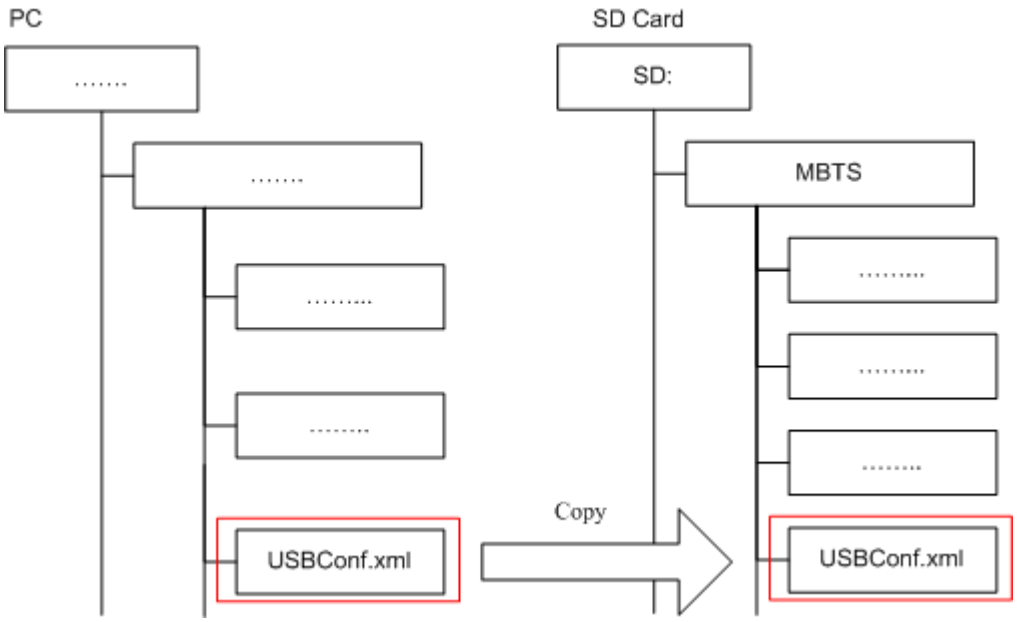
   Integrity protection codes of files are displayed in the MAC address list. The **USBConf.xml** file generated by the tool is saved in the path specified in 4.1.

NOTE

Ensure that the path for configuration files in the **USBConf.xml** file is consistent with the save path in the MicroSD card.

9. Delete existing files on the MicroSD card. Copy the folder containing the files that have been protected by using the tool from the computer to the MicroSD card. All the files in the folder must be copied. SeeFigure 1-16

Figure 1-16 Copying the **USBConf.xml** file



NOTICE

Do not change the directory structure in the folder when files are being copied. Otherwise, deployments or upgrades using a MicroSD card will fail.

NOTE

f software needs to be upgraded but no software package is contained in the MicroSD card, manually copy the software package to the fixed directory. For details about the save path for the software package in the MicroSD card.

10. (Optional) If the **USBConf.xml** file has not been saved in the **NodeB eNodeB** , or **MBTS** folder when you perform step 4.1 you **must** copy the **USBConf.xml** file to the fixed path in the MicroSD card, in accordance with the following table. Otherwise, the files in the MicroSD card cannot be downloaded.

Option	Description
eAN3810A	MicroSD card:\MBTS\USBConf.xml

Applying Integrity and Encryption Protection to Files in Multiple SD Cards

This section describes how to apply integrity and encryption protection to files in multiple SD cards.

Prerequisites

- You have obtained the USB making and protection tool (tool for preparing and protecting an SD card) on the PC where the U2000 is installed. The save path of this tool on the PC is U2000 installation directory\client\client\USBProtector.
- You have scanned viruses for the SD cards by using the anti-virus tool before applying protection to files. This can prevent files on the PC from infections.
- Files in the SD cards are ready for integrity and encryption protection.

Context

- Integrity protection
  - The digital signatures in the version, and patch software packages are verified for integrity verification. Do not use the USB making and protection tool to apply integrity protection to them. Otherwise, deployments or upgrades using an SD card will fail.
  - You must apply integrity protection to all files except for the version and patch software packages.
- Encryption protection
  - Do not apply encryption to the version and patch software packages and the Precfg.ini file. Otherwise, deployments or upgrades using an SD card will fail.
  - You must apply encryption to the VERCFG.XML file.
- After you use the USB making and protection tool to apply integrity and encryption protection to files in the SD card, the USBConf.xml file is generated and the file name cannot be changed. When loading files in the SD card, the base station performs integrity check and decryption by using data in the USBConf.xml file.

Procedure

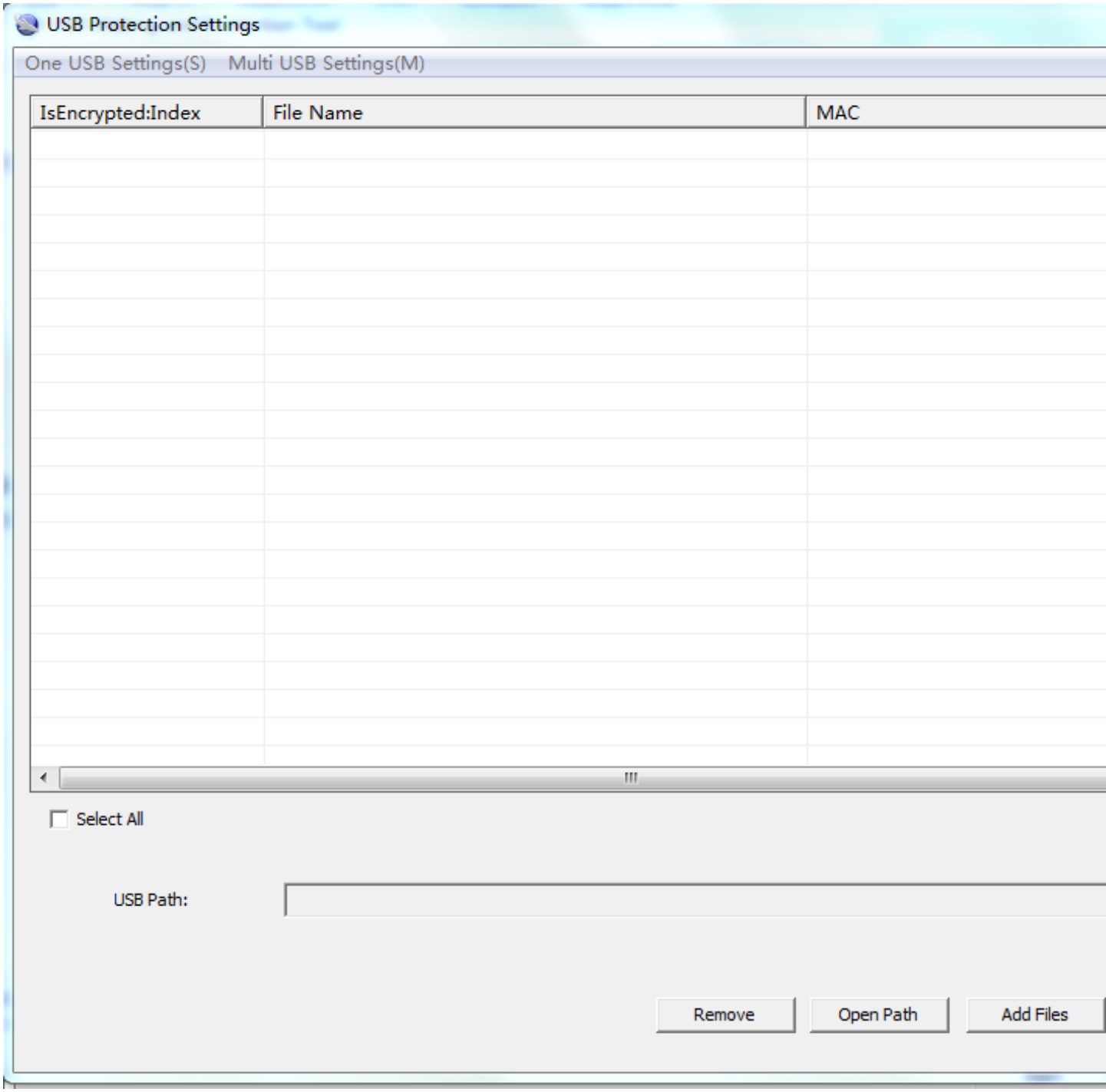
1. Prepare the directory for files to be protected.

NOTE

The USB making and protection tool directly applies integrity and encryption protection to files but it cannot decrypt files. Back up the files before applying integrity and encryption protection to those files.

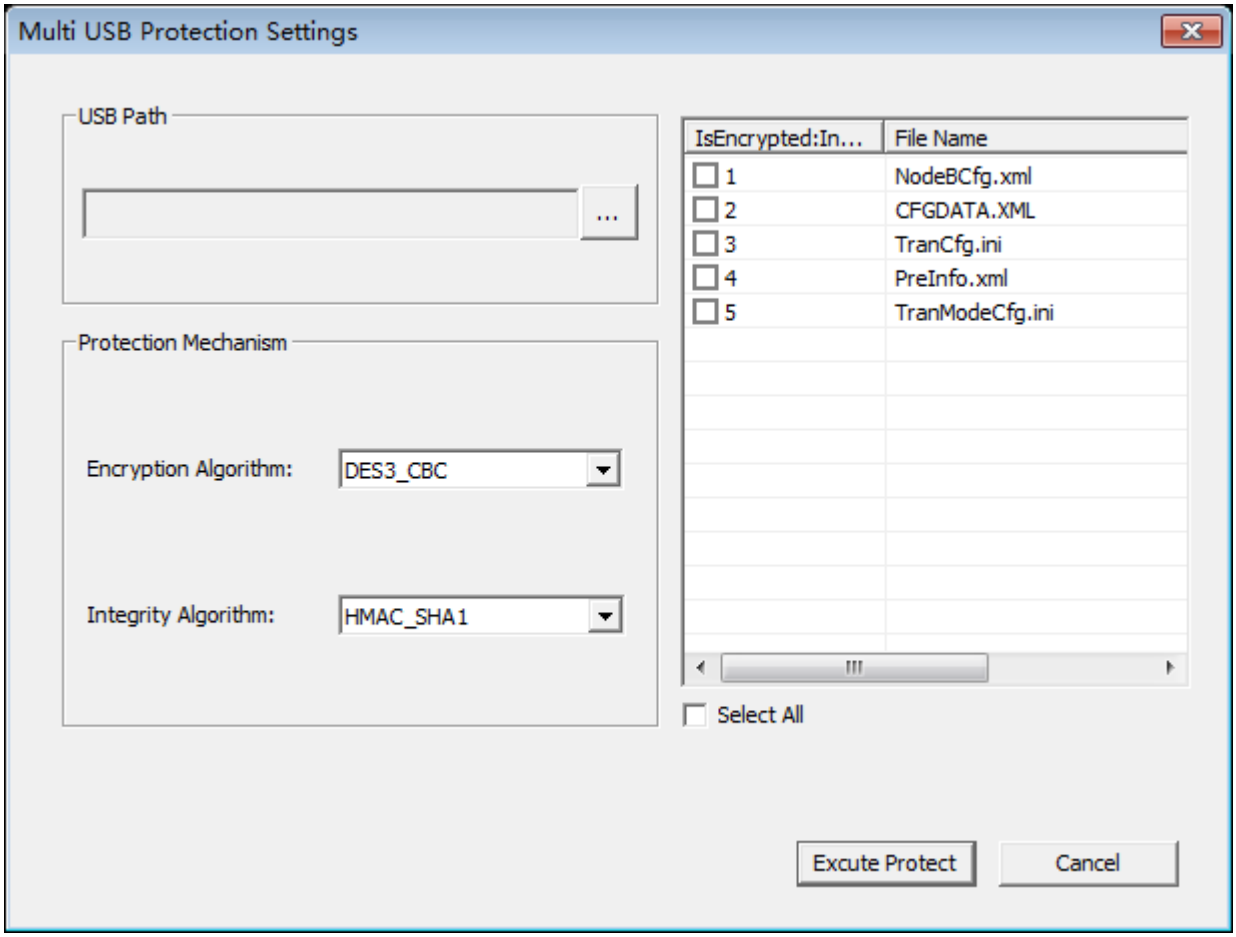
2. Choose **StartProgramsiManager U2000 MBB ClientUSB Making and Protection Tool** to start the tool.
3. Choose **USB ProtectionUSB Protection Settings**. The USB Protection Settings dialog box is displayed. See the followingFigure 1-17.

Figure 1-17 USB Protection Settings dialog box



4. Choose **Multi USB Settings** > **Set USB Path and Security Policies**. The **Multi USB Protection Settings** dialog box is displayed. See the following Figure 1-18.

Figure 1-18 Multi USB Protection Settings dialog box



5. In the **USB Path** area, click ... and specify the root path on the local PC for the folders storing files to be protected.
6. In the **Protection Mechanism** area, select algorithms as required from the **Encryption Algorithm** and **Integrity Algorithm** drop-down lists.

NOTICE

Encryption Algorithm can be set to DES3_CBC, AES192_CBC, or AES256_CBC. Integrity Algorithm can be set to HMAC_SHA1 or HMAC_SHA256. You can choose any encryption and integrity algorithms but the default ones are recommended.

7. Select the **IsEncrypted:Index** check box: In the file list area, if **IsEncrypted:Index** is selected for a file, the system applies encryption protection to this file. Otherwise, the system applies only integrity protection to the file.

NOTICE

The files for which integrity and encryption protection must be applied are described in Context. You must follow the rules; otherwise, deployments or upgrades using an SD card will fail.

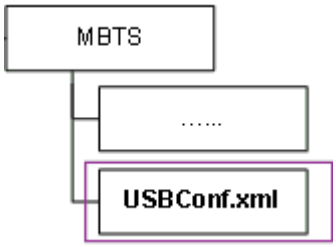
- Encryption cannot be applied to version and patch software packages and the Precfg.ini file.
- Whether to apply encryption to other files depends on customers' security requirements and whether the target version of a base station to be upgraded supports SD card-based encryption.

8. Click **Execute Protect**.
   - The system applies encryption protection to files based on the specified encryption algorithm and applies integrity protection to all files in the current file list area based on the specified integrity algorithm.
   - Sizes of files remain the same before and after encryption because the system uses a symmetrical encryption algorithm.
9. Click **OK** when a dialog box is displayed indicating that the integrity and encryption protection is completed.

NOTE

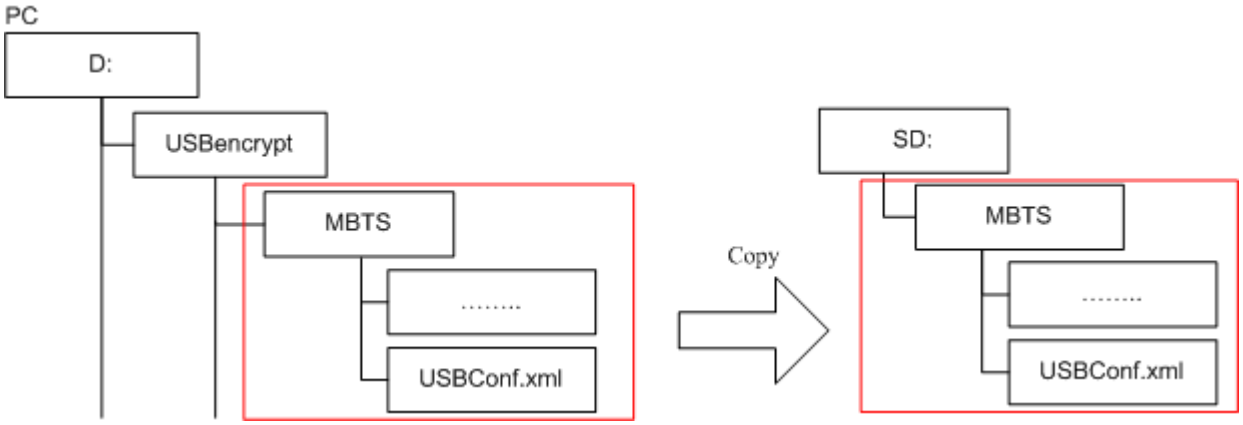
- Do not delete or move the USBConf.xml file which has been automatically saved to a fixed path. Otherwise, the base station cannot download files from the SD cards.
- Ensure that the path of data configuration files in the USBConf.xml file is consistent with the save path in the SD cards.

Figure 1-19 Save path for the USBConf.xml file



10. Delete source files on the SD cards. Copy the folder on the PC containing the files that have been protected by using the tool to the SD cards. Note that all the files in this folder must be copied.

Figure 1-20 Copying files from the PC to the SD cards



NOTICE

Do not change the directory structure in the folder when files are being copied. Otherwise, deployments or upgrades using an SD card will fail.

NOTE

If the base station software needs to be upgraded but no software package is contained in the SD cards, manually copy the software package to the fixed directory.

Saving Alarms/Events

This section describes how to save alarms and events to acquire system operating status in real time.

Prerequisites

You have logged in to the local maintenance terminal (LMT) by using an account with the required operation rights.

Procedure

Step 1 On the menu bar of the LMT, click the **Browse Alarm/Event** or **Query Alarm/Event Log** tab on the **Alarm/Event** tab page.

Step 2 Right-click an alarm/event record to be saved and choose **Save Selected** to save the record. Choose **Save All** to save all the alarm/event records.

Step 3 You can also save all the records by clicking the **Save All** button on the lower part of the **Alarm/Event** tab page.

NOTE

You can click one record and drag the mouse to select multiple alarms/events.

----End

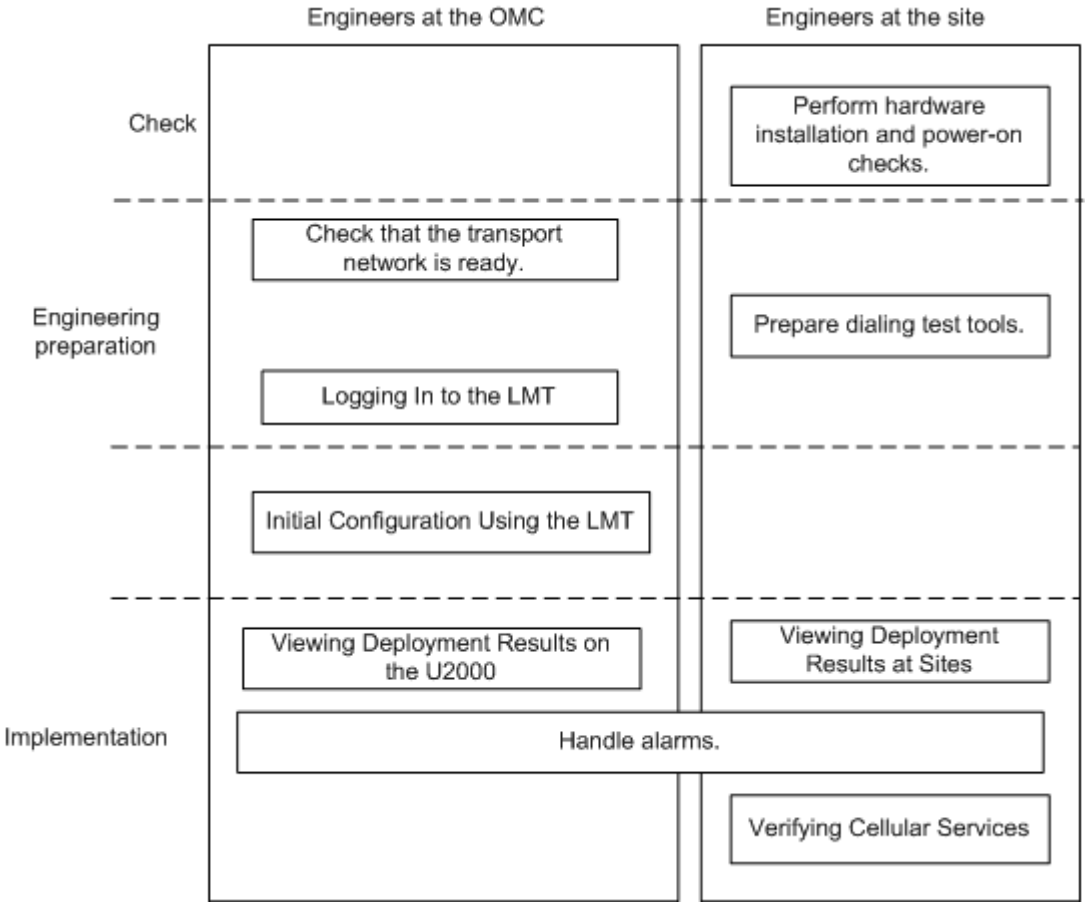
1.3 MML Site Deployment

1.3.1 MML Site Deployment Process

This section describes the eAN3810A site deployment process.

Site deployment requires cooperation of engineers at sites and the OMC, who must master the deployment process shown in Figure 1 in advance of the deployment.

Figure 1-21 Site deployment process



1.3.2 Hardware Installation and Power-on Check

This section describes how to perform hardware installation and power-on checks at the site after eAN3810A hardware is installed. If a MicroSD card is used for local deployment, engineers at the site need to insert the MicroSD card to the eAN3810A to load software and the configuration file.

Prerequisites

- The SD card has been prepared.
- The eAN3810A is working correctly.

Context

The port for housing a MicroSD card is enabled by default on the eAN3810A. Insert a MicroSD card into the powered on eAN3810A and then restart the eAN3810A to read data from the MicroSD card. Alternatively, insert the MicroSD card into the powered off eAN3810A and then power on the eAN3810A.

Table 1-8 Precautions for using an SD card

Deployment Mode	Precautions
Site deployment	The eAN3810A automatically detects the MicroSD card and installs the driver for the card after a MicroSD card is inserted into the eAN3810A. Then, the eAN3810A automatically reads the files in the fixed directories on the MicroSD card and checks the file names and formats. The eAN3810A compares the software version and configuration data on the MicroSD card with those on the eAN3810A. If consistent, it does not load the software or configuration file on the MicroSD card. If inconsistent, it loads the software and configuration file on the MicroSD card. Note the following points about loading: • If the MicroSD card only stores software, the eAN3810A loads only the software. • If the MicroSD card only stores configuration files, the eAN3810A loads only the target configuration file. • The eAN3810A does not load the software or configuration file on the MicroSD card and its RUN indicator indicates a loading failure (steady on) in any of the following conditions: – The MicroSD card is not intended for it. – The expected directories or files are not present. – The directories or file formats are not correct. – Data in the MicroSD card is not encrypted or integrity protected.

Procedure

- U2000-based commissioning
  a. Ensure that the eAN3810A hardware has been installed and has passed the installation check. For details about how to perform the hardware installation check, see section "Checking Hardware Installation" in *eAN3810A Installation Guide*.
  b. Perform the power-on check. For details about how to perform the power-on check, see section "Power-On Check on the eAN3810A" in *eAN3810A Installation Guide*.
- SD card+U2000-based commissioning
  a. Ensure that the eAN3810A hardware has been installed and has passed the installation check. For details about how to perform the hardware installation check, see section "Checking Hardware Installation" in *eAN3810A Installation Guide*.

b. Determine whether to restart the eAN3810A after a MicroSD card is inserted based on the power-on status of the eAN3810A.

If...	Then...
The eAN3810A has been powered on.	Insert the MicroSD card into the related port on the eAN3810A. Remove and reinsert the Ethernet cable for power supply, and then go to 3.
The eAN3810A has not been powered on.	Insert the MicroSD card into the related port on the eAN3810A. Connect the eAN3810A to a PSE over an Ethernet cable. Power on the eAN3810A, and then go to c.

c. Perform the power-on check. For details about how to perform the power-on check, see section "Power-On Check on the eAN3810A" in *eAN3810A Hardware Installation Guide*.

   Check the RUN indicator for hardware faults on the MicroSD card. The RUN indicator blinks orange (on for 0.125s and off for 0.125s), if the eAN3810A fails to read files on the MicroSD card or fails to be deployed. The MicroSD card may be faulty and cannot be detected, if the RUN indicator status does not change.

d. In configuration-free deployment scenarios, wait until the eAN3810A automatically downloads the preconfiguration file and reads the preconfigured information. In site deployment scenarios, wait until the eAN3810A completes the following procedure: automatically loads and activates the software and data configuration files, and restarts itself to make them take effect.

Table 1-9 Mapping between the RUN indicator status and loading status

Loading Status	RUN Indicator Status
The loading succeeds	Slowly blinking (on for 1s and off for 1s) for more than 1 minute
Loading...	Blinking orange and white alternately (on for 0.125s and off for 0.125s)
The loading fails.	Blinking orange (on for 0.125s and off for 0.125s)

NOTE

- In MicroSD card deployment scenarios, the eAN3810A automatically activates the downloaded software and configuration file and then restarts for them to take effect. The activation and restart take about 30 minutes, during which the indicator status is negligible.
- During loading, do not remove the MicroSD card.

e. Remove the MicroSD card only after you have confirmed that the loading succeeds.

Follow-up Procedure

If the software version is incorrect after the loading process is completed, perform the following operations:

1. Insert a MicroSD card storing the correct software version to the eAN3810A.
2. Remove the MicroSD card after the eAN3810A loads the software package and successfully completes the upgrade.

Checking Hardware Installation

eAN3810A hardware installation checking includes hardware and cable installation checking.

Table 1-10 lists the hardware installation checking items.

Table 1-10 Hardware installation checking list

No.	Item
1	The installation position of each device strictly complies with the engineering design and meets clearance requirements. Sufficient space is reserved for equipment maintenance.
2	The eAN3810A is securely installed.
3	The cover plate is securely installed on the eAN3810A cabling cavity.
4	Waterproof blocks are securely installed in vacant cable troughs of the eAN3810A cabling cavity, and the cover plate of the cabling cavity is securely installed. In addition, vacant RF ports are covered with dustproof caps and the caps are tightened.
5	Labels are correct, legible, and complete at both ends of each cable, feeder, and jumper.

Table 1-11 lists the check items of the signal cable connection.

Table 1-11 Checklist for the signal cable connection

No.	Item
1	The connectors of the signal cables must securely connected.
2	The connectors of the signal cables are intact.
3	The signal cables are intact.
4	The cable ties are evenly spaced. The signal cables are bound neatly with cable ties to proper tightness, and arranged at even intervals in the same direction.
5	The extra length of the cable ties is cut and removed. The cut surfaces of the indoor cables are smooth and have no sharp edges.
6	The cable layout facilitates maintenance and expansion.
7	Correct and clear labels are attached to both ends of the signal cables.

Table 1-12 lists the checking items for other cable connections.

Table 1-12 Checklist for other cable connections

No.	Item
1	The connectors of the other cables must securely connected.
2	Labels on the cables are legible and bound based on the engineering requirements. The cables must be bound tightly and neatly. The sheaths of the cables must not be damaged.
3	Positions for routing the cables must meet requirements of the engineering design.
4	There are no connectors or joints on each PGND cable. None of PGND cables can be short-circuited or reversely connected. In addition, these cables are not damaged or broken.
5	PGND cables are separately bound from other cables.
6	The protection grounding of the eAN3810A and the surge protection grounding of the building share one group of ground conductors.

Power-On Check on the eAN3810A

This section describes the procedure for performing a power-on check on the eAN3810A.

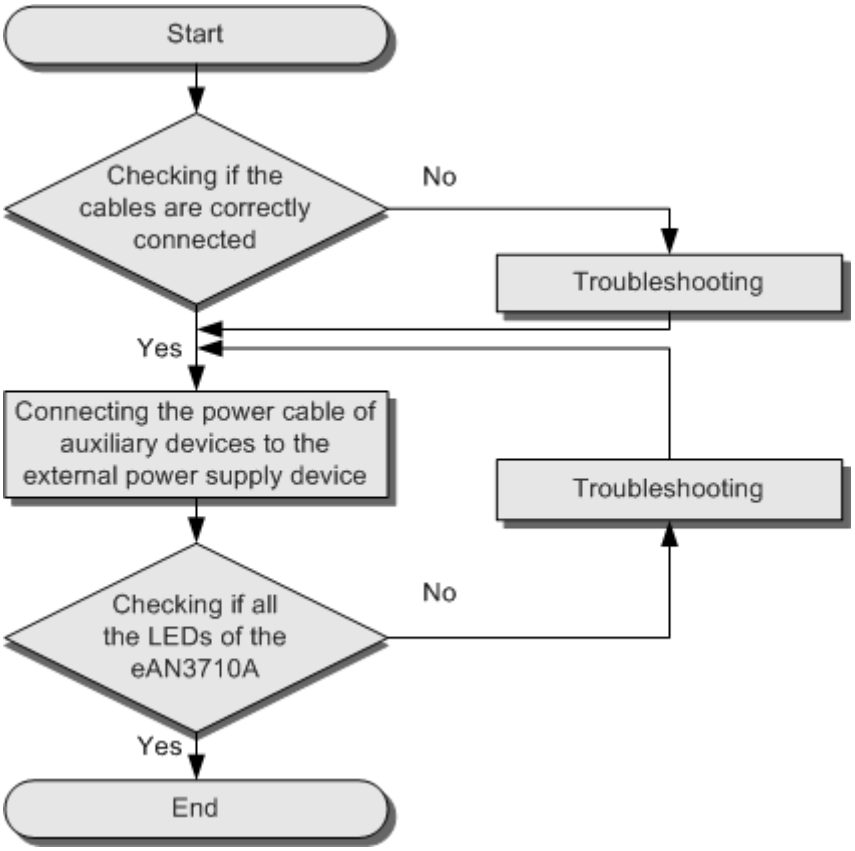
eAN3810A Power-On Check Procedure

NOTICE

After you unpack a eAN3810A, you must power on it within 24 hours. If you power off the eAN3810A for maintenance, you must restore power to it within 24 hours.

Figure 1-22 shows the eAN3810A power-on check procedure.

Figure 1-22 Power-on check procedure



Checking the Indicator Status

Table 1-13 Checking the indicator status

If...		then...
RUN	Steady white	The eAN3810A is running correctly.
ETH	Blinking white	
WIFI	Off	
LINK	Off	

NOTE

- During the eAN3810A startup, there is no need to observe the indicator status.
- During a start, the eAN3810A reads and writes the flash and therefore the indicators blinking quickly may blink irregularly for 1-2 seconds, which does not affect services.

1.3.3 Deployment Preparation

This section describes the data and files to be prepared for eAN3810A deployment.

Checking a Transport Network

This section describes how to check a transport network. The transport network affects the Automatic OMCH Establishment feature. Therefore, before commissioning an eAN3810A,O&M engineers must check whether the OMCH networking and the network equipment meet the configuration requirements of the corresponding scenario.

Check Methods

O&M engineers can check whether the transport network meets the configuration requirements of the Automatic OMCH Establishment feature by using either of the following methods:

Method 1: Confirm with the department in charge of the transport network whether the transport network meets the requirements.

Method 2:

- Check the network connectivity. If nodes in the transport network can be pinged, ping the port corresponding to each node to check whether the transmission channel at each node is ready.
- Check whether the network equipment at each node is configured as required to ensure that an eAN3810A can automatically establish the OMCH.

Preparing Dialing Test Tools

Dialing tests are performed by using test terminals to check whether deployed eAN3810A can provide services properly. Prepare test terminals and ensure that the test subscriber identity module (SIM) cards have registered with the Core Network.

1.3.4 Initial Configuration Using the LMT

This section describes the procedure for initial configuration of the eAN3810A using the LMT.

Prerequisites

- You have installed the hardware and connected the cables.
- You have logged in to the eAN3810A LMT. For detailed operations, see pico/xmlhelp/en-us/lmt/lmt_11.xml.

Context

Table 1-14 lists the data that needs to be planned and collected before the initial configuration.

Table 1-14 Parameter preparation

Category	Related Command	Parameter Name	Value Sample	Description
eNodeB IP	**ADD IPINTERFACE**	IP Address	193.168.100.59	Used for connection to the S1 interface.
		IP Address	172.253.254.59	Used for

Category	Related Command	Parameter Name	Value Sample	Description
				connection to the U2000.
S1-C Interface IP	**ADD SCTPPEER**	Peer IPv4 Address	200.100.109.100	Indicates the first SCTP peer IPv4 address for signaling channel setup. This IP address serves as the first peer IPv4 address for automatic SCTP link setup.
S1-U Interface IP	**ADD USERPLANEPEER**	Peer IPv4 Address	200.100.109.109	Indicates the user-plane IPv4 address of the peer end.
U2000 IP	**MOD IPOAM**	Peer IPv4 Address	10.145.35.15	Indicates the first SCTP peer IPv4 address for signaling channel setup. This IP address serves as the first peer IPv4 address for automatic SCTP link setup.
PLMN	**ADD CNOPERATOR**	Mobile country code	460	Indicates the mobile country code (MCC) of the operator.
		Mobile network code	90	Indicates the mobile network code (MNC) of the operator.
Cell Parameters	**ADD CELL**	Frequency band	60	Indicates the frequency band in which the cell operates.
		Uplink bandwidth	CELL_BW_N100(20M)	
		Downlink bandwidth	CELL_BW_N100(20M)	
		Cell FDD TDD	CELL_TDD	Indicates the duplex mode of

Category	Related Command	Parameter Name	Value Sample	Description
		indication		the cell. **CELL_FDD** indicates the FDD mode, and **CELL_TDD** indicates the TDD mode.
		SubframeAssignment	SA0	
		SpecialSubframePatterns	SSP7	

Procedure

Step 1 Add NE applications.

1. Run the **ADD APP** command to add an NE application.

   Set the **Application Type** parameter to **LTE(LTE)**.

Step 2 Add IP addresses and routes (used for connection to the S1 interface and the U2000).

1. Run the **ADD IPINTERFACE** command to add a device IP address used for connection to the S1 interface.
   - Set the **Interface Reference Type** parameter to **ETHERNET(Ethernet)**.
   - Set the **IP Address** parameter to the eNodeB IP address used for connection to the S1 interface.
2. Run the **ADD IPINTERFACE** command to add a device IP address used for connection to the U2000.
   - Set the **Interface Reference Type** parameter to **ETHERNET(Ethernet)**.
   - Set the **IP Address** parameter to the eNodeB IP address used for connection to the U2000.
3. Run the **ADD ROUTE** command to add a static IP route.

Step 3 Add local and peer information of the data-plane and control-plane of the S1 interface.

1. Run the **ADD LOGICALPORT** command to add a transmission logical port.

   Before running the **ADD LOGICALPORT** command, run the **LST LOGICALPORT** command to query whether an **ADD LOGICALPORT** record already exists. If so, skip the previous substep.
2. Run the **ADD TRANSPORTDEVICE** command to add a transport device.
3. Run the **ADD SCTPHOST** command to add an SCTP host.
4. Run the **ADD USERPLANEHOST** command to add a user-plane host.
5. Run the **ADD SCTPPEER** command to add an SCTP peer.

   Set the **Peer IPv4 Address** parameter to S1-C interface IP.
6. Run the **ADD USERPLANEPEER** command to add a user-plane peer.

Set the **Peer IPv4 Address** parameter to **200.100.109.109**.

Step 4 Add mapping relations required by the S1 interface.

1. Run the **ADD LOGICALPORT2TRPDEV** command to add a logical port to a transport device.
2. Run the **ADD SCTPHOST2TRPDEV** command to add an SCTP host to a transport device.
3. Run the **ADD SCTPPEER2TRPDEV** command to add an SCTP peer to a transport device.
4. Run the **ADD UPHOST2TRPDEV** command to add a user-plane host to a transport device.
5. Run the **ADD UPPEER2TRPDEV** command to add a user-plane peer to a transport device.

Step 5 Add configurations of operators and tracing areas (TAs).

1. Run the **ADD CNOPERATOR** command to add an operator.
   - Set the **Mobile country code** parameter to **460**.
   - Set the **Mobile network code** parameter to **90**.
2. Run the **ADD CNOPERATORTA** command to add TA configuration information.

Step 6 Add an S1 object.

1. Run the **ADD S1** command to add an S1 object.

Step 7 Add sectors and cell antennas.

1. Run the **ADD SECTOREQM** command to add a set of sector equipment.
2. Run the **ADD TXSECTORANTENNA** command to add a transmit sector antenna.
3. Run the **ADD RXSECTORANTENNA** command to add a receive sector antenna.

NOTE

Adding an antenna depends on the type of the added cell. Note that the **Sector Equipment No.** must be consistent with the previous configurations.

Step 8 Add cell and set sectors and operators for the cells.

1. Run the **ADD CELL** command to add a cell.
   - Set the **Frequency band** parameter to **60**.
   - Set the **Uplink bandwidth** parameter to **CELL_BW_N100(20M)**.
   - Set the **Downlink bandwidth** parameter to **CELL_BW_N100(20M)**.
   - Set the **Cell FDD TDD indication** parameter to **CELL_TDD**.
   - Set the **UL-DL subframe configurations** parameter to **SA0**.
   - Set the **Special subframe configurations** parameter to **SSP7**.
2. Run the **ADD EUCELLSECTOREQM** command to add a set of sector equipment for a cell.
3. Run the **ADD CELLOP** command to add a cell operator.

Step 9 Change the eNodeB ID according to the plan and restart the eNodeB.

1. Run the **MOD ENODEBFUNCTION** command to modify an eNodeB function.
2. Run the **RST BTSNODE** command to restart the eNodeB.

Step 10 Activate cells.

1. Run the **ACT CELL** command to activate a cell.

Step 11 Connect to the U2000.

1. Run the **MOD IPOAM** command to modify the configuration of an IP maintenance channel.

   Set the **Peer IPv4 Address** parameter to **10.145.35.15**.

----End

Script

```
//Adding NE applications. If there is an LTE application, do not run the following command.
ADD APP:applicationNo=2,applicationType=LTE;

//Adding IP addresses and routes (used for connection to the S1 interface and the U2000)
ADD
IPINTERFACE:IPINTERFACENO=1,INTERFACEREFTYPE=ETHERNET,INTERFACEREF=0,IPADDRESS="19
3.168.100.59",IPMASK="255.255.255.0";
ADD
IPINTERFACE:IPINTERFACENO=2,INTERFACEREFTYPE=ETHERNET,INTERFACEREF=0,IPADDRESS="17
2.253.254.59",IPMASK="255.255.255.0";
ADD
ROUTE:ROUTENO=0,DESTIPADDR="200.100.109.0",DESTIPMASK="255.255.255.0",NEXTHOPIP="1
93.168.100.100";
ADD
ROUTE:ROUTENO=1,DESTIPADDR="10.145.35.0",DESTIPMASK="255.255.255.0",NEXTHOPIP="172
.253.254.254";

//Adding local and peer information of the data-plane and control-plane of the S1
interface
ADD LOGICALPORT: LOGICALPORTNO=0,INTERFACENO=0;
ADD TRANSPORTDEVICE:TRANSPORTDEVICENO=0;
ADD SCTPHOST:SCTPHOSTNO=0,IPINTERFACEREF=1,LOCALPORT=1024;
ADD USERPLANEHOST:USERPLANEHOSTNO=0,IPINTERFACEREF=1;
ADD SCTPPEER:SCTPPEERNO=0,PEERIPV4ADDR="200.100.109.100",PEERPORT=36412;
ADD USERPLANEPEER:USERPLANEPEERNO=0,PEERIPV4ADDR="200.100.109.109",REMOTEID="1";

//Adding mapping relations required by the S1 interface
ADD LOGICALPORT2TRPDEV:TRANSPORTDEVICENO=0,REFNO=0;
ADD SCTPHOST2TRPDEV:TRANSPORTDEVICENO=0,REFNO=0;
ADD SCTPPEER2TRPDEV:TRANSPORTDEVICENO=0,REFNO=0;
ADD UPHOST2TRPDEV:TRANSPORTDEVICENO=0,REFNO=0;
ADD UPPEER2TRPDEV:TRANSPORTDEVICENO=0,REFNO=0;

//Adding operators and TAs
ADD
CNOPERATOR:CNOPERATORID=0,CNOPERATORNAME="CMCC",CNOPERATORTYPE=CNOPERATOR_PRIMARY,
MCC="460",MNC="90";
ADD CNOPERATORTA:TRACKINGAREAID=0,CNOPERATORID=0,TAC=1;

//Adding an S1 object
ADD
S1:S1ID=0,CNOPERATORID=0,TRANSPORTDEVICECFGFLAG=CP_UP_CFG,CPTRANSPORTDEVICENO=0,UP
```

```
TRANSPORTDEVICENO=0;

//Adding sectors and cell antennas
ADD SECTOREQM:sectorEqmNo=0;
ADD TXSECTORANTENNA:TXSECTORANTENNANO=0,SECTOREQMNO=0,TXBRANCHREF=0;
ADD RXSECTORANTENNA:RXSECTORANTENNANO=0,SECTOREQMNO=0,RXBRANCHREF=0;
ADD TXSECTORANTENNA:TXSECTORANTENNANO=1,SECTOREQMNO=0,TXBRANCHREF=1;
ADD RXSECTORANTENNA:RXSECTORANTENNANO=1,SECTOREQMNO=0,RXBRANCHREF=1;

//Adding cells and set sectors and operators for the cells
ADD
CELL:LOCALCELLID=0,CELLNAME="Cell0",FREQBAND=60,ULEARFCNCFGIND=NOT_CFG,DLEARFCN=61
336,ULBANDWIDTH=CELL_BW_N100,DLBANDWIDTH=CELL_BW_N100,CELLID=0,PHYCELLID=115,FDDTD
DIND=CELL_TDD,ROOTSEQUENCEIDX=0,EMERGENCYAREAIDCFGIND=NOT_CFG,UEPOWERMAXCFGIND=NOT
_CFG,SubframeAssignment=SA0,SpecialSubframePatterns=SSP7;
ADD EUCELLSECTOREQM:LOCALCELLID=0,SECTOREQMID=0;
ADD CELLOP:LOCALCELLID=0,TRACKINGAREAID=0,MMECFGNUM=CELL_MME_CFG_NUM_0;

//Changing the ENODEBID according to the plan and restarting the eNodeB
MOD ENODEBFUNCTION:ENODEBID=586189;
RST BTSNODE:;

//Activating cells
ACT CELL:LOCALCELLID=0;

//Connecting to the U2000
MOD IPOAM:IPOAMNO=0,IPINTERFACEREF=2,
PEERIPV4ADDR="10.145.35.15",PEERIPV4MASK="255.255.255.0";
```

1.3.5 Engineering Verification

This section describes how to complete the eAN3810A commissioning task, view deployment results, and verify services.

Viewing Deployment Results at Sites

This section describes how to view deployment results at sites based on indicator status.

Check the status of indicators on a newly deployed eAN3810A.

The following table shows the indicator status if an eAN3810A is deployed successfully and working properly. See Table 1-15

Table 1-15 Indicator status of a functional eAN3810A

Indicator	Status
RUN	Steady white
ETH	Slow blinking white (on for 1s and off for 1s)
LINK	Steady white

If the indicator status of an eAN3810A differs from that in the preceding table, contact Huawei technical support engineers.

Viewing Deployment Results on the U2000

This section describes how to view deployment results after an eAN3810A is powered on.

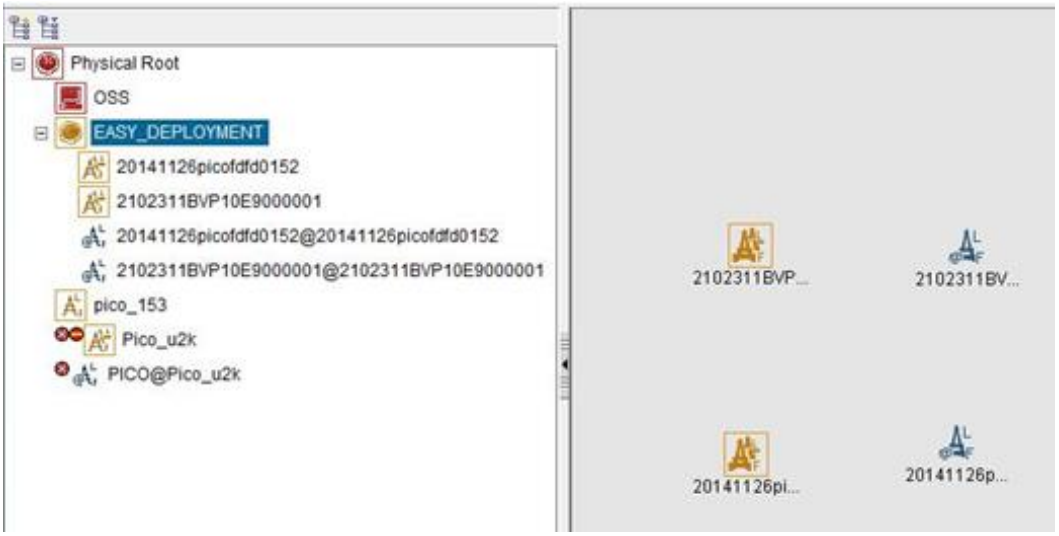
Context

After site deployment is completed, you need to log in to the Web LMT or connect the eAN3810A to the U2000 within 30 minutes. Otherwise, the eAN3810A will be rolled back to the source version upon timer expiry.

Procedure

1. Wait 3 to 4 minutes after an eAN3810A is powered on. Then, on the U2000, choose Topology > Main Topology (traditional style), or double-click Topo View in Application Center and then choose Topology > Main Topology (application style). On the displayed Main Topology window, check whether the eAN3810A topology is created. See the following Figure 1-23.

   Figure 1-23 Main topology view

   - If the eAN3810A is displayed as  in the main topology, the deployment task is successful. No further action is required.
   - If no icon or another icon is displayed for the eAN3810A, the deployment task fails. Proceed to the next step.

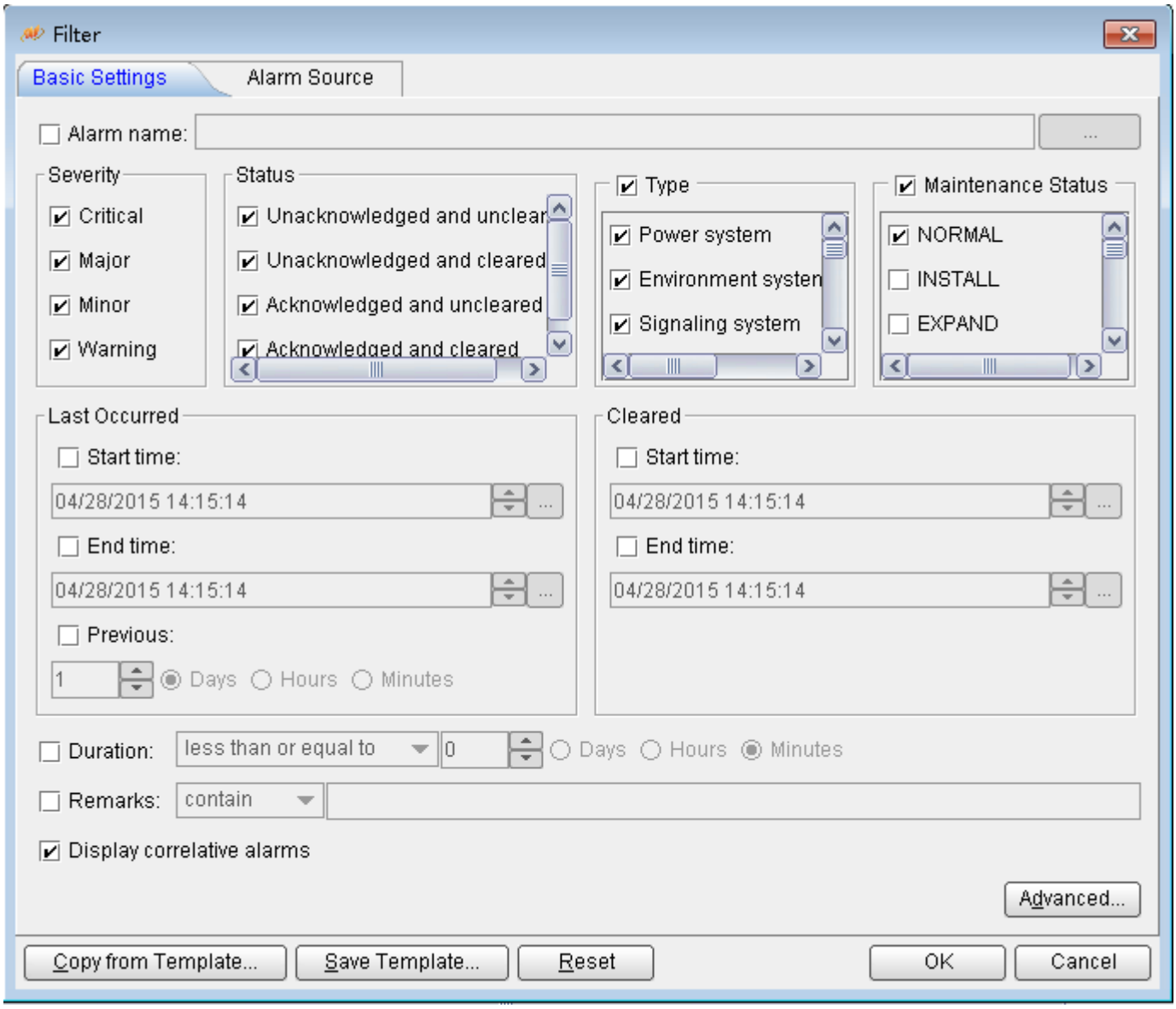
Handling Alarms

This section describes how to handle alarms generated by a newly deployed eAN3810A. All active alarms must be cleared during the commissioning.

Procedure

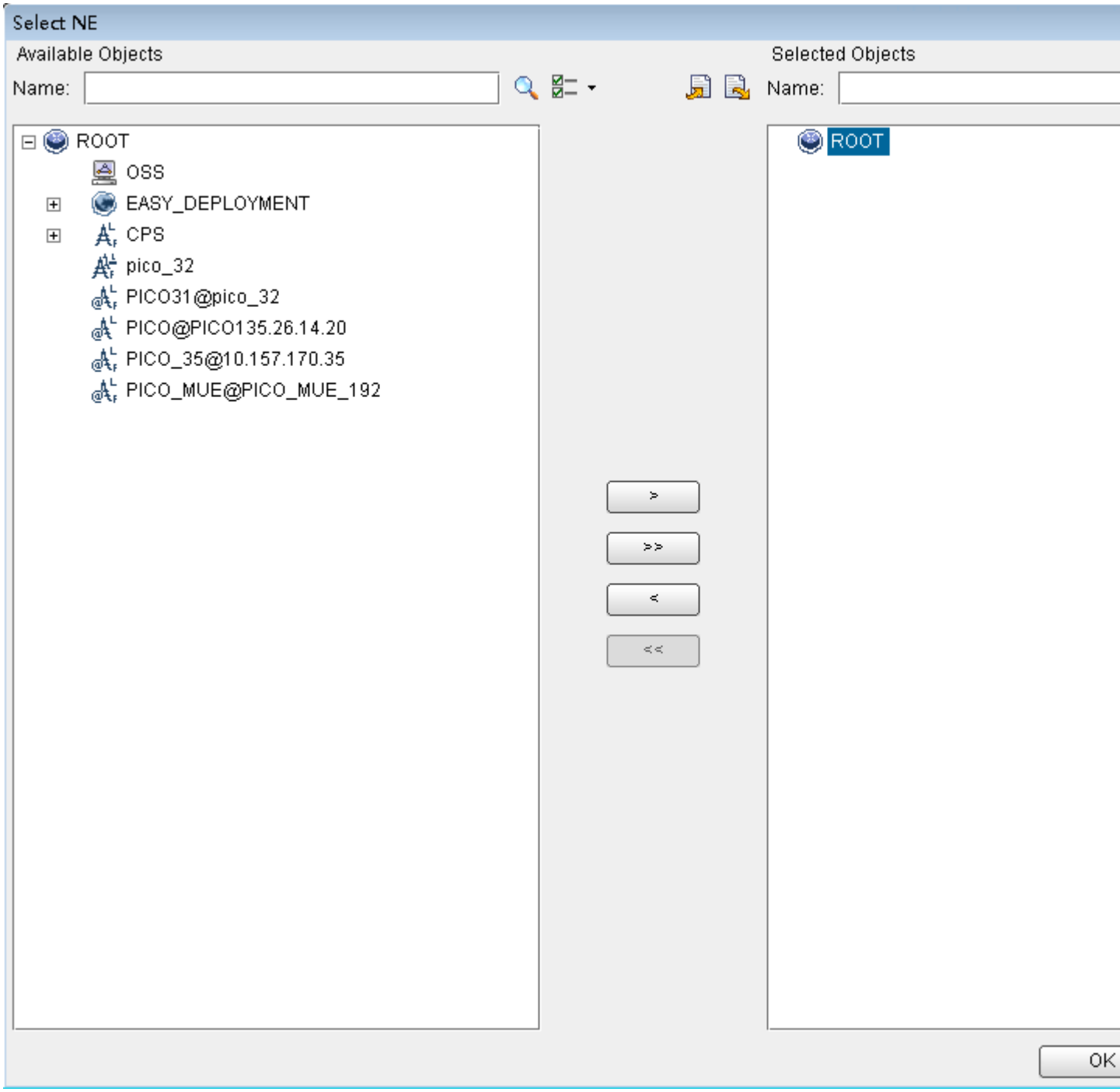
1. On the U2000, choose **Monitor** > **Browse Current Alarms** (traditional style), or double-click **Fault Management in Application Center** and then choose **Browse Alarms** > **Browse Current Alarms** (application style). On the displayed **Browse Current Alarm** window, click **Filter**. The **Filter** dialog box is displayed.

   Figure 1-24 Filter dialog box



2. Click the Alarm Source tab and click the Custom option button. Then, click Add and choose NE from the shortcut menu. The NE dialog box is displayed.

Figure 1-25 NE dialog box



3. In the **Available Objects** area on the left, select NEs in the navigation tree.

   Click > to add the selected NEs to the **Selected Objects** area on the right. Then, click **OK**.

4. In the **Filter** dialog box, click **OK**. All alarms reported by the selected NEs are displayed on the **Browse Current Alarm** window.

5. Check the alarms one by one to determine whether they are related to the new eAN3810A deployment. If related, handle the alarms. For details about how to handle the alarms, see the alarm reference.

Verifying Services

This section describes how to verify that UEs can attach to the eAN3810A and perform ping services.

Prerequisites

Cells are activated.

UEs have been defined on the core network.

Procedure

1. Check whether UEs can successfully attach to the eAN3810A and perform ping services.