DME IQ Client
23.0.x

User Guide

Issue	01
Date	2023-10-19

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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: https://e.huawei.com

About This Document

Purpose

This document mainly introduces the overall architecture, functions and features, and installation and configuration methods of the DME IQ Client (originally named eService Client).

Having this document in hand, you can quickly learn about the DME IQ Client and install and configure the DME IQ Client.

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
📖 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Issue	Date	Description
01	2023-10-19	This issue is the first official release.

Contents

1 About the DME IQ Client

As a large number of IT products such as Huawei storage devices, servers, and cloud computing products are put into use, users have increasingly high requirements on the troubleshooting efficiency.

Background

In traditional service support mode, technical support personnel provide local services manually. Faults may not be detected in a timely manner and information may not be delivered correctly.

Therefore, Huawei launches a professional service tool named DME IQ Client that provides alarm reporting and other remote service functions. When a device becomes faulty, the DME IQ Client provides the alarm reporting function and sends device fault information, logs, inspection reports to the DME IQ cloud system in a timely manner, reducing the troubleshooting time.

Security

- Data collection security
  - Information can be collected only with customers' authorization. Only the O&M information can be obtained from the customer. The information items to be collected are listed in the ***Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data***.
  - All non-query operations performed on the DME IQ Client are recorded, integrity check is performed, and data transmission records can be traced.
  - Sensitive data and important configurations are encrypted using the AES256 algorithm to prevent information leakage.

  NOTE

  The DME IQ Client collects personal data based on user service functions. If you want to disable the personal data collection function of the DME IQ Client, uninstall the DME IQ Client. To delete personal data stored on the cloud system, send an email to **dmeiq@huawei.com** and specify the name of the site where the data needs to be deleted. Huawei technical support will delete the data within 30 working days.

- Data transmission security
  - Bidirectional authentication

The DME IQ Client uses certificates to authenticate the DME IQ cloud system, and the DME IQ cloud system uses Uniportal accounts to authenticate the DME IQ Client.

  - Unidirectional access

    The DME IQ Client can access the DME IQ cloud system but the DME IQ cloud system cannot access the DME IQ Client.

  - Secure transmission

    When the Internet channel is used, the DME IQ Client connects to the DME IQ cloud system through HTTPS and transmits data through the HTTPS encryption channel to ensure connection security.

    When the email channel is used, the DME IQ Client adopts the data envelope technology to encrypt the email content before transmission.

  - The DME IQ Client has been certified by the China National Computer Quality Supervising Test Center after all security items (100%) are tested, and obtained the *Security Qualification Report*.

- Data storage security
  - DME IQ cloud system

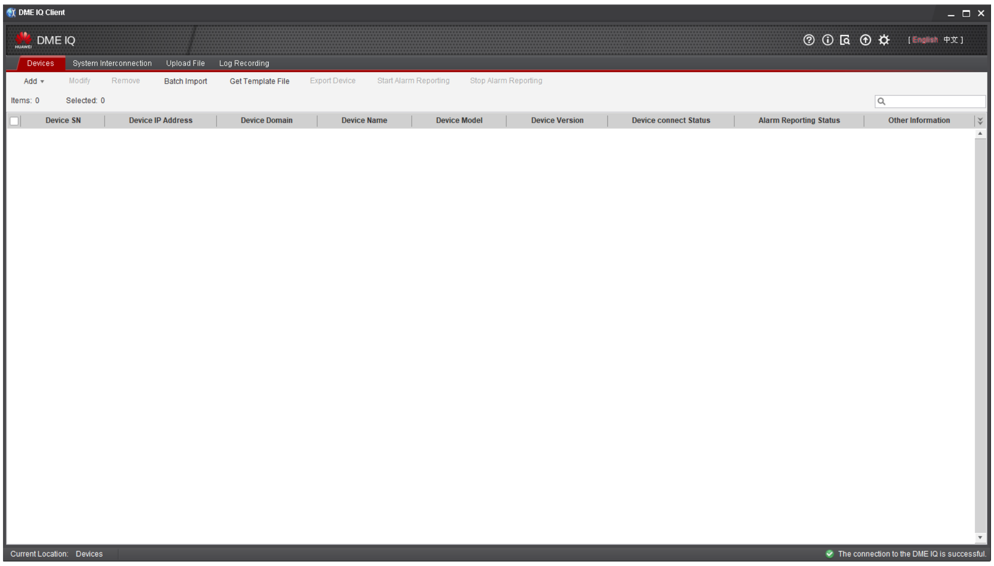
    The information security condition complies with the ISO/IEC 27001:2013 standard, and obtains the *ISO 27001 Information Security Management System Certification*.

GUI

The DME IQ Client provides a clear and intuitive graphical user interface (GUI) for easy configuration and management.

Figure 1-1 shows the DME IQ Client GUI.

Figure 1-1 DME IQ Client GUI



Items: 0 Selected: 0

□	Device SN	Device IP Address	Device Domain	Device Name	Device Model	Device Version	Device connect Status	Alarm Reporting Status	Other Information

Current Location: Devices

The connection to the DME IQ is successful.

For details about the functions of each area on the GUI, see **Table 1-1**.

Table 1-1 Functions of each area on the DME IQ Client GUI

No.	Area	Description
1	Menu bar	● Devices Allows you to add, modify, and remove devices, and manage alarms reported by online devices. Devices can be added in batches. ● System Interconnection Allows you to interconnect various systems with the DME IQ Client. ● Upload File Allows you to upload log files and inspection reports, helping locate and solve problems. ● Log Recording Allows you to manage operation logs, run logs, and message records of devices to know device status in real time.
2	Setting and help area	● Allows you to manage device information by set basic information, Call Home, log dumping, and advanced properties. The device information will be sent to maintenance personnel for fault locating, facilitating real-time troubleshooting. ● Allows you to view help documents and version information and select a desired language. For more information, visit https://www.huawei.com. ● Allows you to check the DME IQ Client functions, detect the new version, and upgrade it.
3	Status bar	Displays the location of the current operation.
4	Information display area	Displays all function module information of the DME IQ Client.

2 Typical Deployment Solutions

2.1 Solution Description

The DME IQ Client connects to devices, processes alarms generated by the devices, and sends the alarms to the DME IQ cloud system through emails or the Internet.

When deploying the DME IQ Client, select a deployment solution based on **Figure 2-1** and **Table 2-1**.

Figure 2-1 DME IQ Client deployment solutions

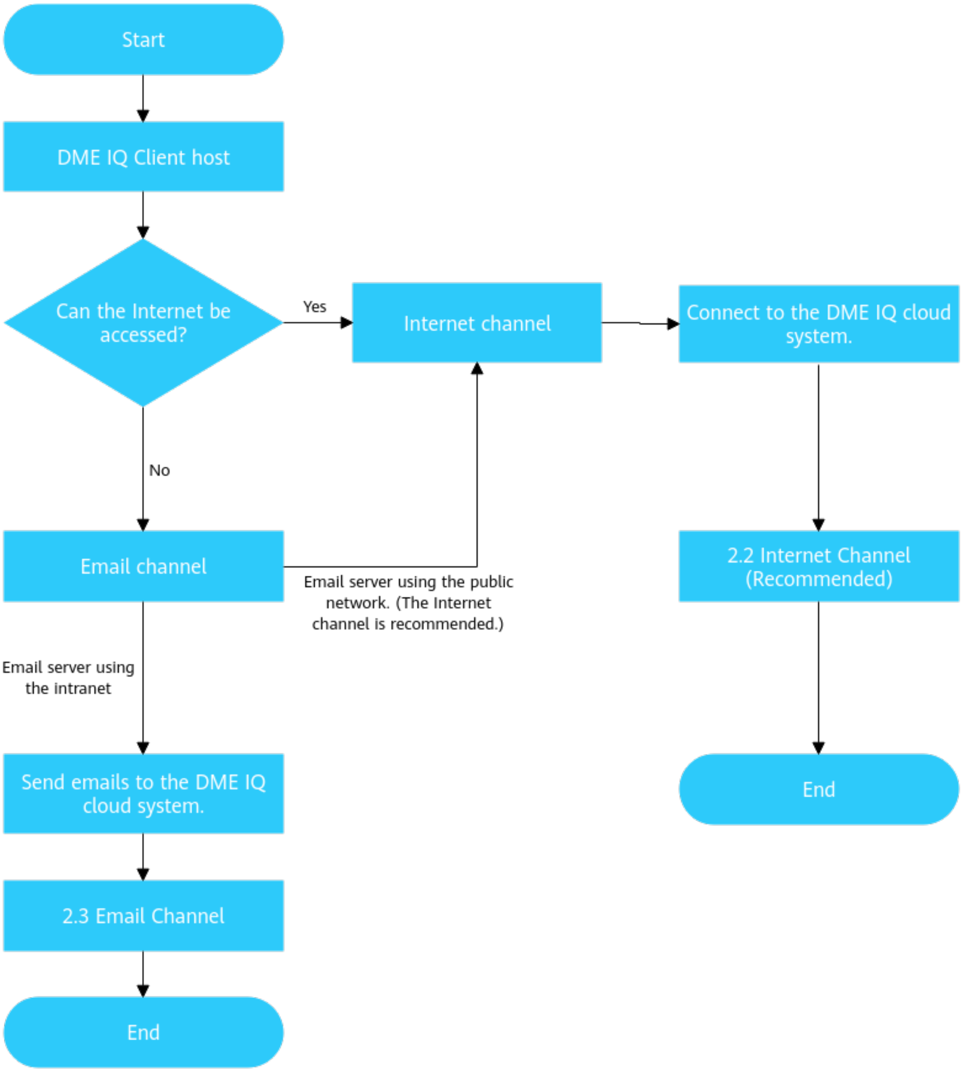

Start
DME IQ Client host
Can the Internet be accessed?
Yes
Internet channel
Connect to the DME IQ cloud system.
No
Email channel
Email server using the public network. (The Internet channel is recommended.)
2.2 Internet Channel (Recommended)
Email server using the intranet
Send emails to the DME IQ cloud system.
End
2.3 Email Channel
End

Table 2-1 DME IQ Client deployment solution description

DME IQ Client Host Network	Deployment Solution	Technical Requirements
The Internet can be accessed.	Internet channel	1. Enable the outbound rules for the firewall to connect to the DME IQ cloud system. 2. Connect to the IP address of the DME IQ cloud system. 3. For details, see **2.2 Internet Channel (Recommended)**.

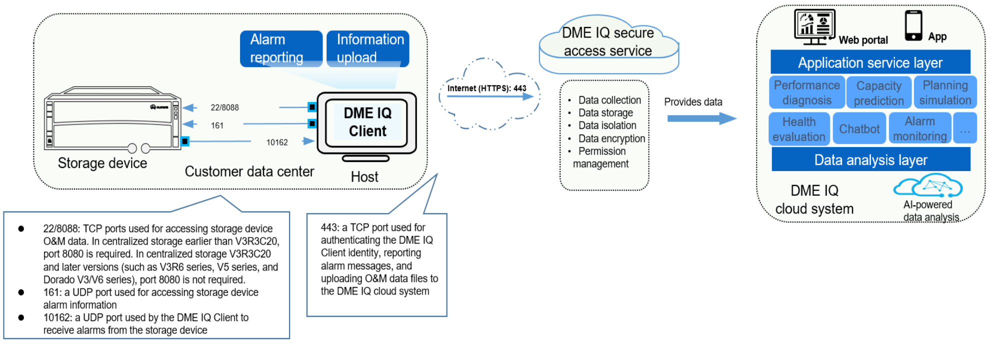
DME IQ Client Host Network	Deployment Solution	Technical Requirements
The network is an intranet and cannot access the Internet.	Email channel	1. If an email server using the intranet is used, the email channel is used to send emails to the DME IQ cloud system. 2. If an email server using the public network can be used, the DME IQ Client host can connect to the Internet. In this case, you are advised to switch to the Internet channel. 3. For details, see **2.3 Email Channel**.

2.2 Internet Channel (Recommended)

The Internet channel supports services such as alarm monitoring, remote inspection, remote log collection, archiving, and automatic upload of historical performance data.

Networking Description

Figure 2-2 Networking diagram when the Internet channel is used



- 22/8088: TCP ports used for accessing storage device O&M data. In centralized storage earlier than V3R3C20, port 8080 is required. In centralized storage V3R3C20 and later versions (such as V3R6 series, V5 series, and Dorado V3/V6 series), port 8080 is not required.
- 161: a UDP port used for accessing storage device alarm information
- 10162: a UDP port used by the DME IQ Client to receive alarms from the storage device

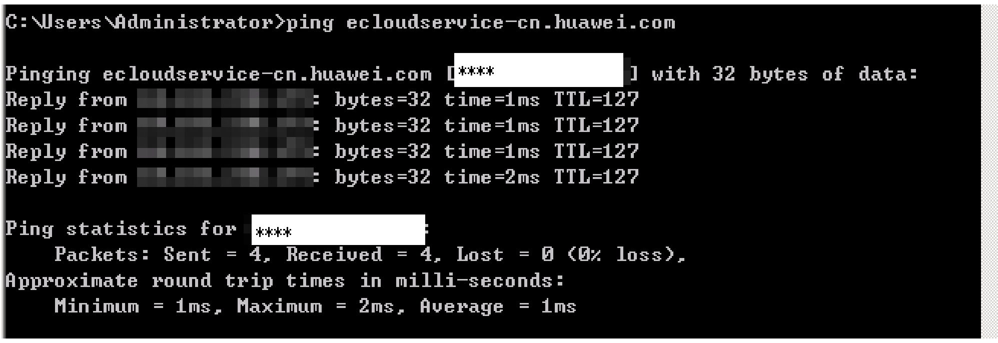
443: a TCP port used for authenticating the DME IQ Client identity, reporting alarm messages, and uploading O&M data files to the DME IQ cloud system

NOTE

- **Figure 2-2** lists the ports that need to be enabled on storage devices and the port functions.
- If the DME IQ cloud system is connected through the Internet, the firewall on the customer network must be enabled to access port 443 of the secure access service. You can run the cmd command to ping the corresponding domain name to obtain the corresponding public network IP address.

  For example, run the following command to ping the domain name of the enterprise technical support center in the Chinese mainland.

  ```
  ping ecloudservice-cn.huawei.com
  ```



```
C:\Users\Administrator>ping ecloudservice-cn.huawei.com

Pinging ecloudservice-cn.huawei.com [****] with 32 bytes of data:
Reply from [redacted]: bytes=32 time=1ms TTL=127
Reply from [redacted]: bytes=32 time=1ms TTL=127
Reply from [redacted]: bytes=32 time=1ms TTL=127
Reply from [redacted]: bytes=32 time=2ms TTL=127

Ping statistics for ****:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Table 2-2 lists the ports to be enabled on the DME IQ cloud system, devices, and interconnected systems and the port functions.

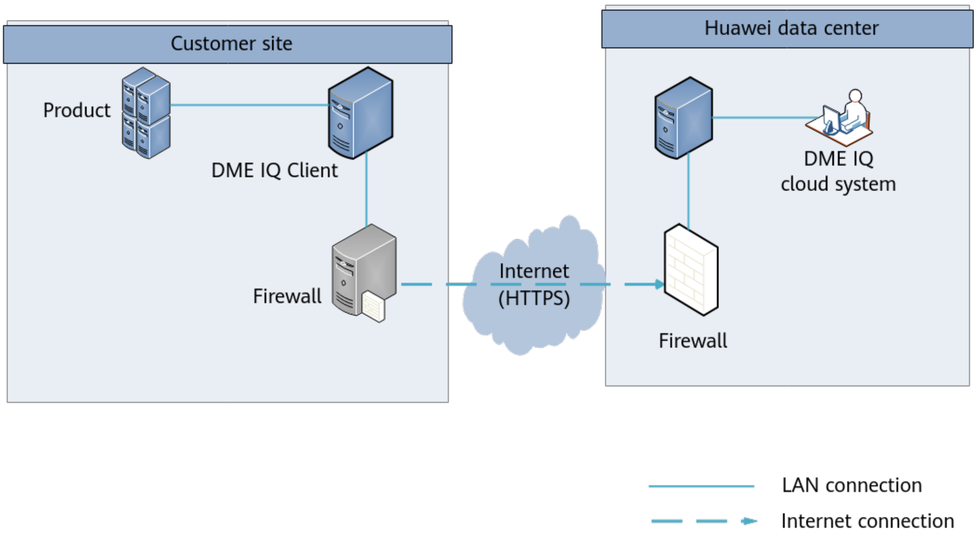
Table 2-2 Networking description

Type	Port	Protocol	Rule	Description
Secure access service	443	TCP	Outbound	● In the Chinese mainland: – Technical support center for enterprises: https://ecloudservice-cn.huawei.com – Technical support center for carriers: https://icloudservice-cn.huawei.com ● Outside the Chinese mainland: – Technical support center for enterprises: Romania: https://itr-eservicero-ent.huawei.com Russia: https://enterpriseru.eservice.huawei.com – Technical support center for carriers: Romania: https://itr-eservicero-carrier.huawei.com Mexico: https://itr-eservicemx-carrier.huawei.com Russia: https://carrierru.eservice.huawei.com
Storage device	22/8088/25081	TCP	Outbound	Port for accessing storage device O&M data **NOTE** In centralized storage earlier than V3R3C20, port 8080 is required. In centralized storage V3R3C20 and later versions (such as V3R6 series, V5 series, and Dorado V3/V6 series), the port is not required.
	161	UDP	Outbound	Port for accessing storage device alarm information

Type	Port	Protocol	Rule	Description
	10162	UDP	Inbound	Port used by the host to receive alarm information from the storage device
Server	22/443	TCP	Outbound	Port for accessing server O&M data
	623	UDP	Outbound	Port for accessing server O&M data
	161	UDP	Outbound	Port for accessing server alarm information
	10162	UDP	Inbound	Port used by the host to receive alarm information from the server
Network device	22	TCP	Outbound	Port for accessing network device alarm information
FusionCare	8805	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionCare
ManageOne (6.3/6.5.0/8.0)	26335	TCP	Outbound	Port for interconnecting the DME IQ Client with ManageOne
ManageOne (6.5.1)	443	TCP	Outbound	Port for interconnecting the DME IQ Client with ManageOne
FusionDirector	443	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionDirector
vCenter	443	TCP	Outbound	Port for interconnecting the DME IQ Client with vCenter
FusionCube Vision Pro	30443	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionCube Vision Pro
FusionCube Vision	443	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionCube Vision

2.2.1 Common Scenario

Figure 2-3 Common deployment solution



In this scenario, the DME IQ Client host must be able to directly access the DME IQ cloud system.

2.2.2 Access Using a Proxy Server

Figure 2-4 Access process using a proxy server

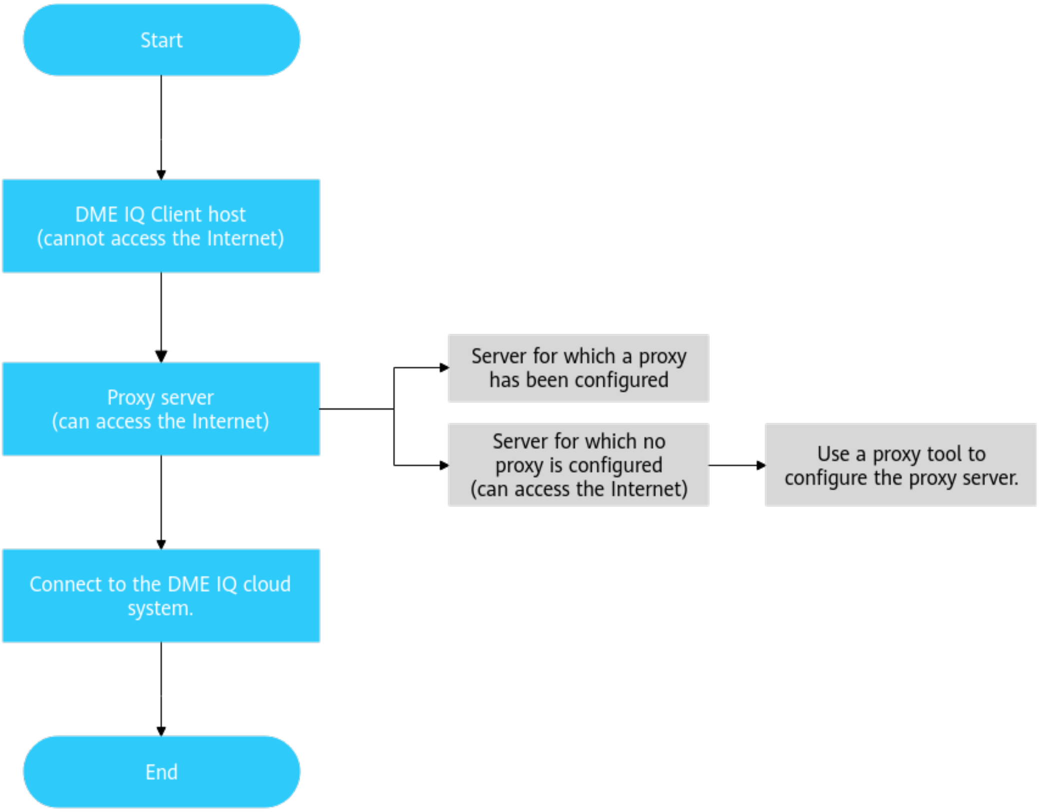
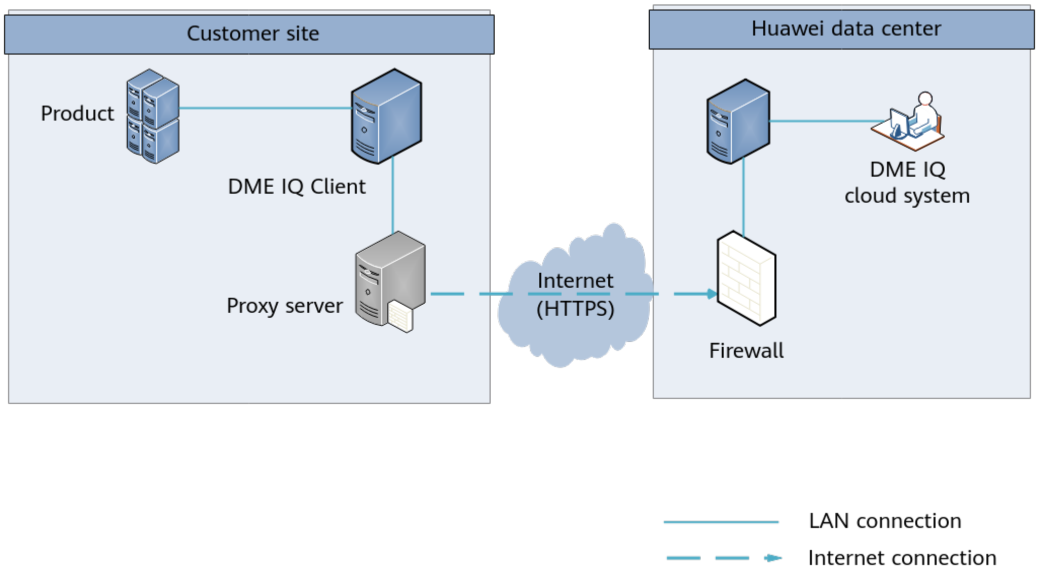
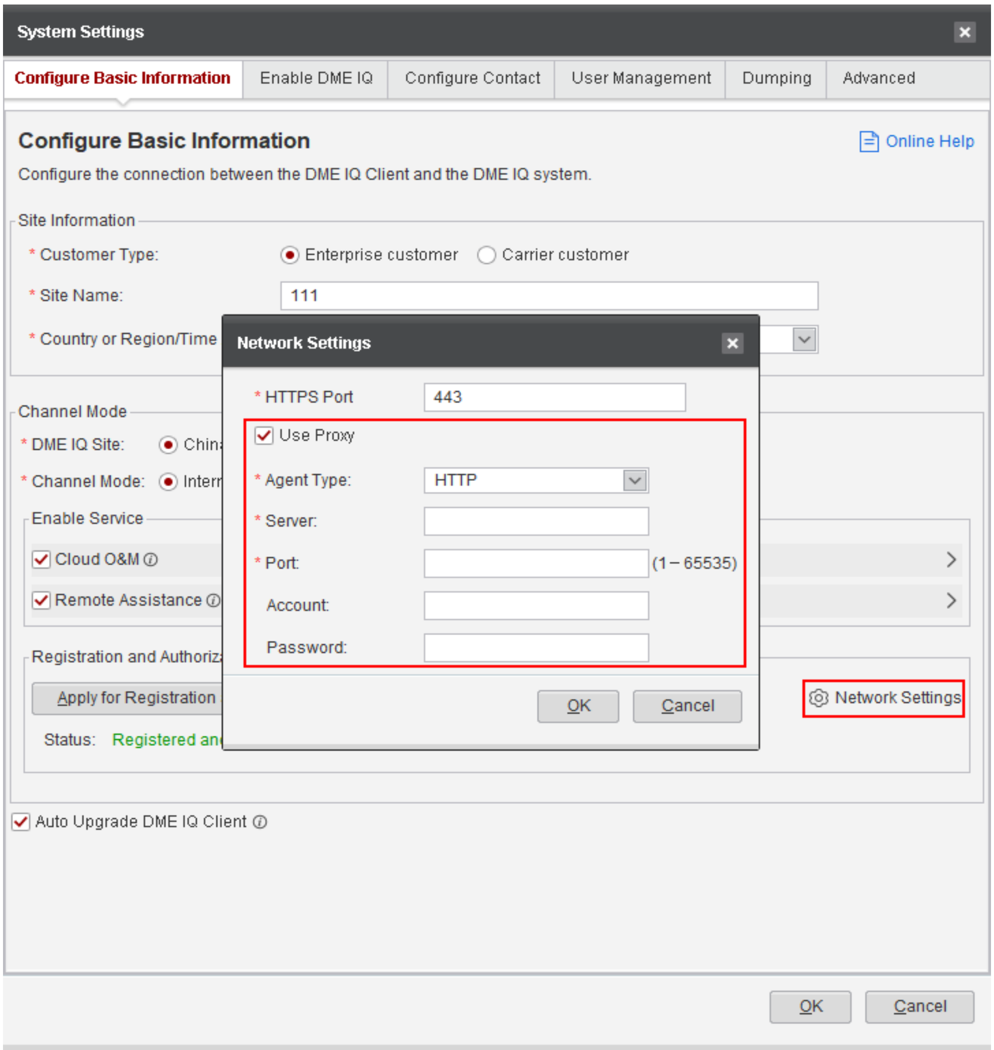


Figure 2-5 Deployment solution of using a proxy server for access



In this scenario, the DME IQ Client host cannot access the Internet. You need to configure a proxy server on the DME IQ Client and use the proxy server to access the DME IQ cloud system.



System Settings

Configure Basic Information | Enable DME IQ | Configure Contact | User Management | Dumping | Advanced

Configure Basic Information

Configure the connection between the DME IQ Client and the DME IQ system.

Site Information

* Customer Type: ● Enterprise customer ○ Carrier customer

* Site Name: 111

* Country or Region/Time

Channel Mode

* DME IQ Site: ● Chin

* Channel Mode: ● Interr

Enable Service

☑ Cloud O&M

☑ Remote Assistance

Registration and Authoriz

Status: Registered an

☑ Auto Upgrade DME IQ Client

Network Settings

* HTTPS Port: 443

☑ Use Proxy

* Agent Type: HTTP

* Server:

* Port: (1 – 65535)

Account:

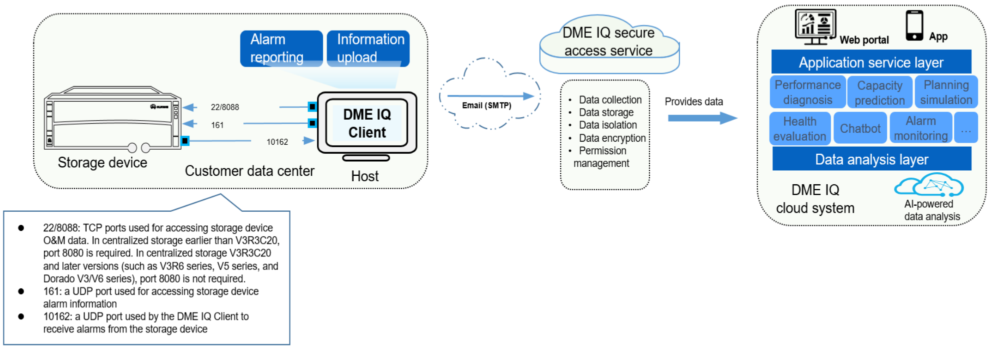
Password:

- If a proxy server has been configured in the customer network, use the proxy server when deploying the DME IQ Client.
- If no proxy server is configured in the customer network, prepare a server that can access the Internet and install a proxy tool on the server to configure the server as a proxy server.

2.3 Email Channel

The email channel supports alarm monitoring, log collection, and performance collection.

Figure 2-6 Networking diagram when the email channel is used



- 22/8088: TCP ports used for accessing storage device O&M data. In centralized storage earlier than V3R3C20, port 8080 is required. In centralized storage V3R3C20 and later versions (such as V3R6 series, V5 series, and Dorado V3/V6 series), port 8080 is not required.
- 161: a UDP port used for accessing storage device alarm information
- 10162: a UDP port used by the DME IQ Client to receive alarms from the storage device

NOTE

Figure 2-6 lists the ports that need to be enabled on storage devices and the port functions.

Table 2-3 lists the ports that need to be enabled for the interconnection between devices or interconnected systems and the DME IQ Client and the port functions.

Table 2-3 Networking description

Type	Port	Protocol	Rule	Description
Storage device	22/8088/25081	TCP	Outbound	Port for accessing storage device O&M data **NOTE** In centralized storage earlier than V3R3C20, port 8080 is required. In centralized storage V3R3C20 and later versions (such as V3R6 series, V5 series, and Dorado V3/V6 series), the port is not required.
	161	UDP	Outbound	Port for accessing storage device alarm information
	10162	UDP	Inbound	Port used by the host to receive alarm information from the storage device
Server	22/443	TCP	Outbound	Port for accessing server O&M data
	623	UDP	Outbound	Port for accessing server O&M data
	161	UDP	Outbound	Port for accessing server alarm information
	10162	UDP	Inbound	Port used by the host to receive alarm information from the server

Type	Port	Protocol	Rule	Description
Network device	22	TCP	Outbound	Port for accessing network device alarm information
FusionCare	8805	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionCare
ManageOne (6.3/6.5.0/8.0)	26335	TCP	Outbound	Port for interconnecting the DME IQ Client with ManageOne
ManageOne (6.5.1)	443	TCP	Outbound	Port for interconnecting the DME IQ Client with ManageOne
FusionDirector	443	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionDirector
vCenter	443	TCP	Outbound	Port for interconnecting the DME IQ Client with vCenter
FusionCube Vision Pro	30443	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionCube Vision Pro
FusionCube Vision	443	TCP	Outbound	Port for interconnecting the DME IQ Client with FusionCube Vision

3 Installation and Deployment

This chapter describes the pre-installation preparations, installation methods, and post-installation configurations of the DME IQ Client.

3.1 Preparing for Installation and Configuration

Before installing the DME IQ Client, you need to prepare planned data, required hardware and software resources, as well as related security policies. Sufficient preparations facilitate quick installation and configuration.

3.1.1 Signing the Authorization Letter with the Customer

Before deploying the DME IQ Client, ensure that the DME IQ Client complies with local laws and formal authorization in written form has been obtained.

When the transmission channel is Internet, you can use the DME IQ Client to perform online authorization and generate an electronic authorization letter. Alternatively, you can sign a paper authorization letter and upload it to the DME IQ cloud system. For details, see "Apply for Registration and Authorization" in **3.3 Initial Configuration**. When the transmission channel is email, sign the authorization letter offline and send it to the DME IQ cloud system.

How to obtain the *Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data*:

- Enterprises: ***Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data***
- Carriers: ***Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data***

Copyright © Huawei Technologies Co., Ltd.

3.1.2 Confirming the Customer Requirements and Transmission Channel

Before installing and configuring the DME IQ Client, confirm with the customer about the requirements and determine the transmission channel to be used based on the customer's environment. This section introduces the functions supported by different transmission channels and environment requirements.

Table 3-1 Functions supported by different transmission channels and environment requirements

Transmission Channel	Supported Function	Environment Requirement
Email channel	● Alarm reporting ● Automatic upload of diagnosis information ● Real-time performance analysis	The server where the DME IQ Client is located can connect to an email server that has the permission to send emails to the DME IQ cloud system. **NOTE** If the customer cannot access the DME IQ cloud system and only the alarm reporting function is required, the email channel is recommended.
Internet channel	● Alarm reporting ● Automatic upload of diagnosis information ● Real-time performance analysis ● Fault locating ● Remote inspection ● Remote upgrade ● Historical performance analysis	The server where the DME IQ Client is located can access the DME IQ cloud system directly or using a proxy server. The network bandwidth must be greater than or equal to 2 Mbit/s. It is recommended that the network bandwidth be greater than or equal to 10 Mbit/s.

3.1.3 Preparing Hardware and Software Resources

This section describes how to check and prepare hardware and software resources before the installation.

- For details about how to install hardware of storage devices, see installation guides of the corresponding devices.
- For details about other hardware and software resources required for installing the DME IQ Client and the corresponding specifications requirements, see **Table 3-2**.

Table 3-2 Software and hardware resources and specifications requirements for deploying the DME IQ Client

Category	Environment	Type	Recommended Configuration and Requirement	Remarks
DME IQ Client software package	-	DME IQ Client software	-	How to obtain: ● Enterprise network: 1. Log in to Huawei technical support website for enterprises (**https://support.huawei.com/enterprise/en/index.html**). 2. In the search box, enter **DME IQ** and click the suggested path to go to the documentation page. 3. Click **Software Download** to download the software package of the required version. ● Carrier network: 1. Log in to Huawei technical support website for carriers (**https://support.huawei.com/**

Category	Environment	Type	Recommended Configuration and Requirement	Remarks
				carrierindex/en/hwe/index.html). 2. In the search box, enter **DME IQ** and click the suggested path to go to the documentation page. 3. Click **Software** to download the software package of the required version.
Host	Windows server (physical machine or VM)	CPU and memory	● CPU: 4-core 1.6 GHz or above ● Memory: 4 GB or above	If the number of devices exceeds 300, it is recommended that the CPU be 8-core 1.6 GHz or above and the memory be 8 GB or above.
		Disk	Free space: 20 GB or above	Size of the partition where the installation directory is located

Category	Environment	Type	Recommended Configuration and Requirement	Remarks
		Supported operating system	● Windows 7 64-bit ● Windows 10 64-bit ● Windows Server 2008 64-bit ● Windows Server 2012 64-bit ● Windows Server 2016 64-bit ● Windows Server 2019 64-bit	-
HTTPS channel	Communication network	Network	The Windows server must be connected to both the device and the DME IQ cloud system.	Storage management IP address, server BMC IP address, and cloud computing management plane
		Communication port	● SNMP: UDP 161, 10162 ● HTTPS: TCP 443 ● SSH: TCP 22 ● REST: 8088	● From DME IQ Client to device: UDP 161, TCP 22 and 8088 ● From device to DME IQ Client: UDP 10162 ● From DME IQ Client to Huawei data center: TCP 443 **NOTE** In direct connection mode, the HTTPS port number is TCP 7448, 8448, and 9448.

Category	Environment	Type	Recommended Configuration and Requirement	Remarks
		Proxy server (optional)	Address of the proxy server provided by the customer	If the proxy server requires authentication, provide the account and password.
		Firewall	Enable the firewall by referring to the communication port.	-
Email channel	Email server	Email server	You can use the email server to send emails to the DME IQ cloud system. The following basic information about the email server needs to be obtained from the customer: domain name (or IP address) of the SMTP server, sending port, and security protocol type.	The customer's own email server is recommended. If an extranet email address can be used, the HTTPS channel is recommended.
		Email account	The customer needs to provide an email account and password for logging in to the email server.	Once an alarm is generated on a device, the alarm information is automatically sent to the DME IQ cloud system using this account.

Category	Environment	Type	Recommended Configuration and Requirement	Remarks
		Communication port	SMTP: TCP 25 SNMP: UDP 161, 10162 SSH: TCP 22 REST: 8088	● From DME IQ Client to device: UDP 161, TCP 22 and 8088 ● From device to DME IQ Client: UDP 10162 ● From DME IQ Client to email server: TCP 25
Contact information	O&M contact	O&M contact information	The customer needs to provide the names, phone numbers, and email addresses of the O&M contacts. At least one and a maximum of five contacts are supported.	Used by the DME IQ cloud system to contact O&M engineers.

NOTE

- The host can be a personal computer (PC), server, service processor (SVP), or VM. If a firewall exists between the DME IQ Client host and the storage device, ask the customer to enable the UDP port 10162 of the DME IQ Client host and port 161 of the device controller. They are used by the DME IQ Client to query and receive alarms.
- In centralized storage earlier than V3R3C20, port 8080 is required. In centralized storage V3R3C20 and later versions (such as V3R6 series, V5 series, and Dorado V3/V6 series), the port is not required.
- To enhance the Windows security, you are advised to perform system security hardening operations before installing the DME IQ Client. For details, see the *Security Configuration Guide* of the desired product and version.

3.1.4 Preparing Configuration Information

Before installing and configuring the DME IQ Client, you need to collect and plan the login password, server or storage device information, SNMP parameters, mailbox parameters, and system connection information to ensure smooth installation and configuration of the DME IQ Client.

Login Password

Upon the first login, the administrator must set the password to log in to the DME IQ Client.

NOTICE

To guarantee system security, you must set a password upon the first login. The rules of setting the password are as follows:

- The password must contain 8 to 32 characters including uppercase letters, lowercase letters, and special characters. The password cannot be set to a weak password, such as **Huawei@123** or **Admin@123**.
- A new password must be different from any of the five recently used passwords.
- The password validity period is six months. Change the password periodically.

Device Information

Before initial configuration, you need to obtain information about the management IP addresses of storage devices, servers, and network devices from the device administrator.

NOTE

If a device has multiple management IP addresses, you need to enter only one management IP address when adding the device.

SNMP Parameters

SNMP parameters are used to enable the device alarm reporting function. To enable the device alarm reporting function, configure SNMP parameters on the DME IQ Client.

You need to create an SNMP account for the device first.

- For details about how to create an SNMP account for a storage device, see **C.1 Configuring SNMP Parameters (for Storage Devices)**.
- For details about how to create an SNMP account for a server, see **C.2 Configuring SNMP Parameters (for Servers)**.

NOTE

- SNMP parameters can be configured in v2c or v3 version. v3 is recommended. If v2c is used, security risks exist.
- For OceanStor V300R003 and later versions, SNMP v3 parameters are configured.
- To check whether a device supports v3, visit the Huawei technical support website to obtain the corresponding product documentation.
  - For enterprises: Log in to Huawei technical support website for enterprises (**https://support.huawei.com/enterprise/en/index.html**).
  - For carriers: Log in to Huawei technical support website for carriers (**https://support.huawei.com/carrierindex/en/hwe/index.html**).

Proxy Parameters

If the Internet channel is used, HTTP or SOCKS proxy parameters need to be configured. **Table 3-3** lists common proxy parameters and example values.

Table 3-3 Common proxy parameters

Parameter	Description	Example Value
Proxy server address	IP address or domain name of the proxy server that provides access from the external network.	proxy.test.com
Port	Port of the proxy server.	8081
Account	User name for logging in to the proxy server.	proxyuser
Password	Password for logging in to the proxy server.	password

System Interconnection Parameters

- To perform log collection and remote inspection for cloud computing devices, you need to interconnect with FusionCare.

  Table 3-4 lists the parameters required for interconnecting with FusionCare and example values. Contact FusionCare administrators to obtain the actual parameter information.

  Table 3-4 Parameters required for interconnecting with FusionCare

Parameter	Description	Example Value
IP Address/Website	IP address or website of FusionCare.	192.168.0.1
Port	Port of FusionCare.	8805
Account	Account for interconnecting with FusionCare.	systemman
Password	Password for interconnecting with FusionCare.	Rest@Care123
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCare.	-

- To configure the alarm reporting function for FusionDirector, you need to interconnect the FusionDirector system with the DME IQ Client. Currently, only FusionDirector 1.5.0 or later can be interconnected with the DME IQ Client.

  Table 3-5 lists the parameters required for interconnecting with FusionDirector and example values. Contact FusionDirector administrators to obtain the actual parameter information.

Table 3-5 Parameters required for interconnecting with FusionDirector

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionDirector alarms.	Yes
IP Address/Website	IP address of FusionDirector.	192.168.0.1
Port	Port of FusionDirector.	443
Account	Account for interconnecting with FusionDirector.	rootRedfish
Password	Password for interconnecting with FusionDirector.	Machine@123
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionDirector.	-

- To configure the alarm reporting function for Huawei ManageOne, you need to interconnect ManageOne with the DME IQ Client. Currently, only ManageOne 6.3/6.5.0, 6.5.1, 8.0, or later can be interconnected with the DME IQ Client.

  Table 3-6 lists the parameters required for interconnecting with ManageOne and example values.

Table 3-6 Parameters required for interconnecting with ManageOne

Parameter	Description	Example Value
System Version	ManageOne version.	8.0
Enable Alarm Reporting	Whether to report ManageOne alarms.	Yes
IP Address/Website	IP address of the ManageOne OC Maintenance Portal.	192.168.0.1
Port	Port of the ManageOne OC Maintenance Portal.	26335
Account	Account for interconnecting with the ManageOne OC Maintenance Portal.	thirdparty

Parameter	Description	Example Value
Password	Password for interconnecting with the ManageOne OC Maintenance Portal.	Sy@1#3!5-OC6
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify ManageOne.	-

- To collect performance and diagnosis information about vCenter, you need to interconnect vCenter with the DME IQ Client. Currently, vCenter 6.0 and later versions can be interconnected with the DME IQ Client.

  Table 3-7 lists the parameters required for interconnecting with vCenter and example values.

Table 3-7 Parameters required for interconnecting with vCenter

Parameter	Description	Example Value
IP Address/Website	IP address or website of vCenter.	192.168.0.1
Port	Port of vCenter.	443
Account	Account for interconnecting with vCenter. The value is in the format of *vCenter read-only user name***@vsphere.local**.	user1@vsphere.local
Password	Password for interconnecting with vCenter.	Huawei@123
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify vCenter.	-

- To configure the alarm reporting and remote log collection functions for FusionCube Vision Pro, you need to interconnect it with the DME IQ Client. Currently, FusionCube Vision Pro 8.0 or later can be interconnected with the DME IQ Client.

  Table 3-8 lists the parameters required for interconnecting with FusionCube Vision Pro and example values.

Table 3-8 Parameters required for interconnecting with FusionCube Vision Pro

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionCube Vision Pro alarms.	Yes
IP Address/Website	IP address of FusionCube Vision Pro.	192.168.0.1
Port	Port of FusionCube Vision Pro.	30443
Account	Account for interconnecting with FusionCube Vision Pro.	openapi
Password	Password for interconnecting with FusionCube Vision Pro.	Huawei@4321
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCube Vision Pro.	-

- To configure the alarm reporting and remote log collection functions for FusionCube Vision, you need to interconnect it with the DME IQ Client. Currently, FusionCube Vision 8.0.RC1 or later can be interconnected with the DME IQ Client.

  Table 3-9 lists the parameters required for interconnecting with FusionCube Vision and example values.

Table 3-9 Parameters required for interconnecting with FusionCube Vision

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionCube Vision alarms.	Yes
IP Address/Website	IP address of FusionCube Vision.	192.168.0.1
Port	Port of FusionCube Vision.	443
Account	Account for interconnecting with FusionCube Vision.	openapi
Password	Password for interconnecting with FusionCube Vision.	Huawei@4321

Parameter	Description	Example Value
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCube Vision.	-

- To configure functions such as alarm reporting for FusionCompute, you need to interconnect it with the DME IQ Client. Currently, FusionCompute 8.0 or later can be interconnected.

  Table 3-10 lists the parameters required for interconnecting with FusionCompute and example values.

Table 3-10 Parameters required for interconnecting with FusionCompute

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionCompute alarms.	Yes
IP Address/Website	FusionCompute IP address.	192.168.0.1
Port	Port of FusionCompute.	7443
Account	Account for interconnecting with FusionCompute.	gesysman
Password	Password of the user for interconnecting with FusionCompute.	GeEnginE@123
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCompute.	-

NOTE

- For 8.3 and later versions, the default interface interconnection user does not exist and you need to log in to FusionCompute as user **admin** to add the user for interconnection. To do so, log in to FusionCompute, choose **System** > **Rights Management** > **User Management**, and click **Add User** to create an interface interconnection user.
- Only versions 8.0 to 8.2 support performance data and diagnosis information collection. To use the performance data and diagnosis information collection function, interconnect FusionCompute with the DME IQ Client and then add the corresponding storage device. In addition, ensure that the performance monitoring function of FusionCompute is enabled. To check whether the function is enabled, log in to FusionCompute and choose **Monitoring** > **Performance** > **Monitoring Settings**, and check whether all indicators of hosts, datastores, clusters, and VMs are selected in the **Select KPIs to monitor** area. If the performance monitoring function is not enabled, select all indicators and click **Save** to enable the function.

3.1.5 Checking Security Preparations

Before installing the DME IQ Client, check security requirements of network and device permissions according to this section.

For details about security requirements of the DME IQ Client, see **Table 3-11**.

Table 3-11 DME IQ Client security requirements

Category	Scenario	Description
Network	Connection between a host and a device	The host and the device can access each other and the following operations are allowed: ● The DME IQ Client registers a trap IP address on the device through SNMP. ● The device reports alarms to the DME IQ Client through SNMP.
	Using the email channel	The host can connect to the email server. The email server must have the permission to send emails to the DME IQ cloud system. You are advised to use email servers that support secure connections (TLS/SSL).
	Using the Internet channel	The host can access the DME IQ cloud system directly or using a proxy. The DME IQ Client performs inspection or log collection by accessing the device management port through SSH.
Device permission	Alarm reporting	Minimum permission requirements: SNMP read and write permissions (used to report device alarm information)
File permission	Accessing and running the DME IQ Client	Before installing and configuring the DME IQ Client, you need to add a new user to the **Administrators** group or log in to the system as **Administrator** to install, run, and maintain the DME IQ Client. For details, see **3.2.2 Installing the DME IQ Client**. **NOTE** After the DME IQ Client is installed, you need to set the directory permission to allow only newly created users to access the program installation directory. For details, see the *Security Configuration Guide*.

3.2 Installing and Configuring the DME IQ Client

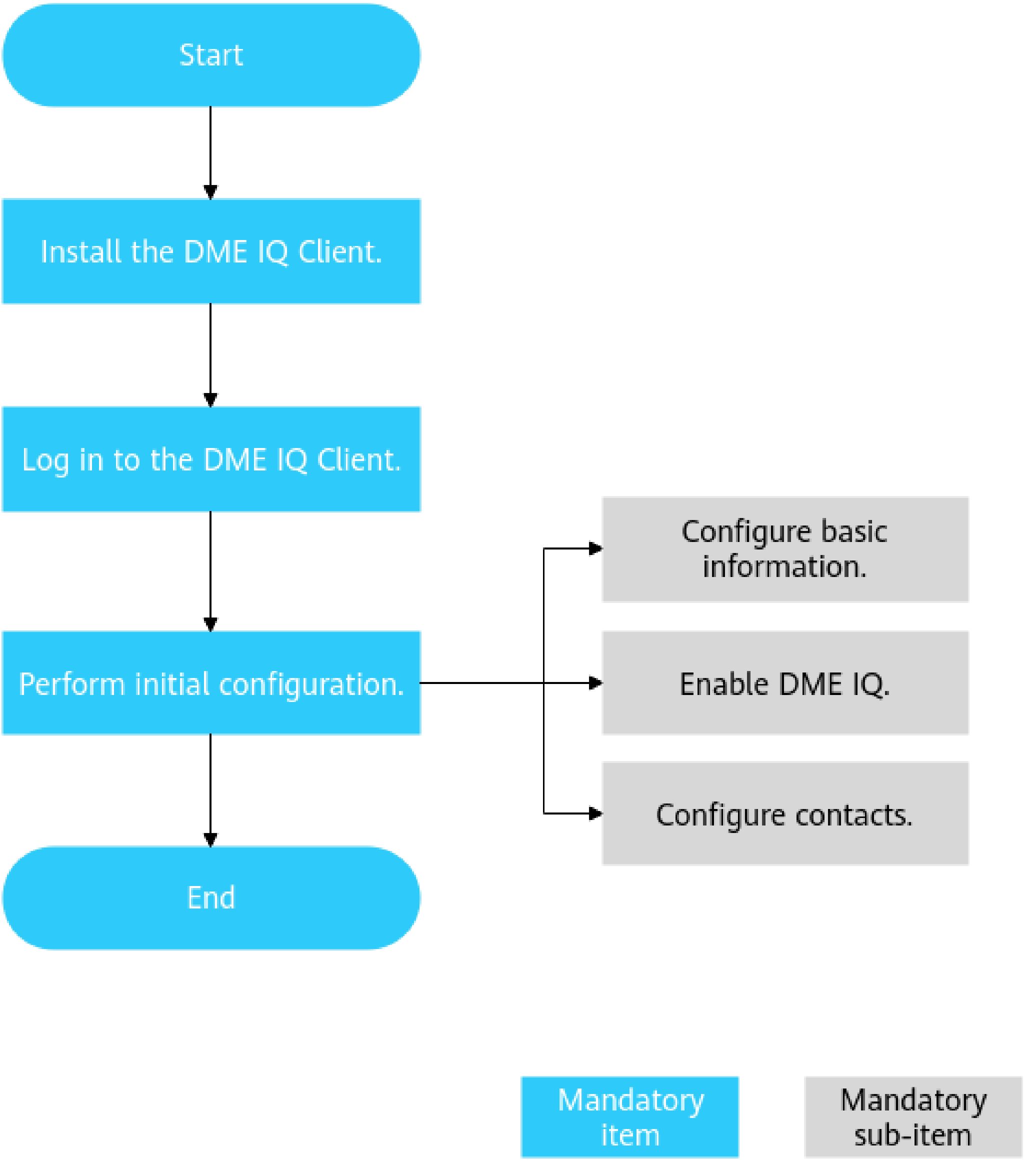
To ensure the normal use of the DME IQ Client, correctly install and configure it. This section describes how to install and configure the DME IQ Client, including the installation and configuration process, as well as installing and logging in to the DME IQ Client.

3.2.1 Installation and Configuration Process

Before installing the DME IQ Client, look through the overall installation and configuration procedure, which can help you install and configure the DME IQ Client.

Figure 3-1 shows the installation and configuration process.

Figure 3-1 Installation and configuration process


Start
Install the DME IQ Client.
Log in to the DME IQ Client.
Perform initial configuration.
End
Configure basic information.
Enable DME IQ.
Configure contacts.
Mandatory item
Mandatory sub-item

3.2.2 Installing the DME IQ Client

The DME IQ Client can be deployed on a physical machine, VM, or SVP in an equipment room. This section describes the procedure for installing the DME IQ Client.

Prerequisites

Software and hardware resources and corresponding specifications requirements described in **Table 3-2** have been met.

Preparations described in **3.1 Preparing for Installation and Configuration** have been completed.

NOTE

- If you want to use the DME IQ Client to monitor OceanStor 18000, you can install the DME IQ Client on the SVP.
- If you install the DME IQ Client on the SVP of OceanStor 18000 V100R001, the Cloud Service software built in the SVP will be overwritten and then the storage alarms of the original Cloud Service cannot be forwarded to the specified email address. Therefore, before installing the DME IQ Client, you need to confirm it with the customer. Otherwise, install the DME IQ Client on another server.
- If you need to install the DME IQ Client on the SVP server of OceanStor 18000 V100R001C00SPC300 or earlier, check whether the **C:\cloudservice_config** directory and the **D:\Huawei\CloudService\clientinformation.dat** file exist before installation. If they exist, delete them before the installation.

Procedure

Step 1 Log in to the Windows system as an administrator or administrator group to install the DME IQ Client.

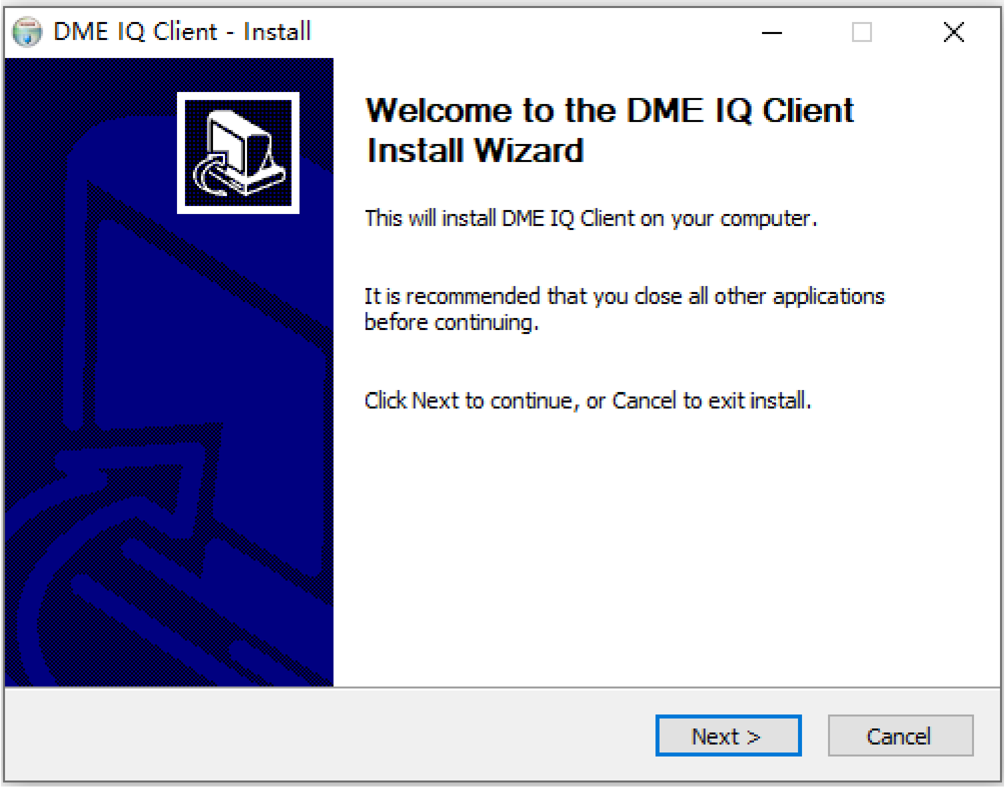
Step 2 (Optional) Before installing the DME IQ Client, create a user as an administrator or administrator group account to log in to Windows. The operation may vary with your operating system. The following uses Windows 7 as an example.

1. Choose **Start** > **Control Panel** > **User Accounts** > **Manage User Accounts** > **Add or remove user accounts** > **Create a new account**.
2. Enter a name for the account. Click **Properties** and then select **Administrator**.
3. Click **Manage User Accounts**. The newly created administrator user is displayed.
4. Choose **Start** > **Log off** > **Switch User** and use the newly created account to log in to Windows.

NOTE

- For Windows Server 2008 SP2, if you install the DME IQ Client as a super administrator, the permission of the DME IQ Client installation directory will change when a common administrator accesses the directory. This common user will have the permission to read the DME IQ Client installation directory. Therefore, you are advised to reconfigure the directory permission.
- It is recommended that you minimize the permissions of the administrator group so that the accounts in the administrator group are necessary and trustworthy.

Step 3 Double-click the software package, and follow the installation wizard to install the DME IQ Client.



Welcome to the DME IQ Client Install Wizard

This will install DME IQ Client on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit install.

NOTE

- The installation directory cannot contain Chinese characters or consecutive spaces.
- If the DME IQ Client is installed on the SVP, the system will automatically uninstall the legacy DME IQ Client software built in the SVP.
- On the SVP, the client needs to be installed in a directory on the D drive (except **D:\Huawei**). If the client is not installed on the SVP, you can use the default path.

Step 4 Wait until the DME IQ Client installation is complete, select whether you want to start the DME IQ Client immediately, and then click **Finish**.

----End

Follow-up Procedure

Set the access permission on the DME IQ Client directory to allow only newly created users to access the program installation directory. For details, see the *Security Configuration Guide*.

3.2.3 Logging In to the DME IQ Client

This section describes how to log in to the DME IQ Client for the first time and when you forget the password, and how to change the login password.

3.2.3.1 Logging In

This section describes how to log in to the DME IQ Client and how to set the administrator password upon the first login.

Prerequisites

The DME IQ Client has been properly installed.

Procedure

Step 1 Start the DME IQ Client.

You can start the DME IQ Client using either of the following methods:

- After the DME IQ Client is installed, start it immediately and click **Finish**.
- On the desktop, double-click icon to start the DME IQ Client.

Step 2 **Optional:** Set the login password of the administrator upon the first login.

1. In the dialog box displayed upon the first login indicating "This is your first login. Please set the login password.", click OK.

   The **Set Password And Secure Mailbox** dialog box is displayed.
2. Set **Password**, **Confirm Password**, and **Secure Mailbox**.
3. Click and read the **Privacy Policy** and **Security Precautions**, and select **I have read and agree to the Privacy Policy and Security Precautions**.
4. Click **OK**.

   A message is displayed, indicating that the password and secure mailbox are set successfully.

NOTE

- The new password must contain 8 to 32 characters including uppercase letters, lowercase letters, and special characters. The password cannot be set to a weak password, such as **Huawei@123** or **Admin@123**.
- The password validity period is six months. Change the password periodically. Keep the password secure and do not disclose it to others.
- Set a secure mailbox to receive the verification code for resetting the password.

Step 3 Log in to the DME IQ Client.

On the login page, select a language, enter the user name and password, and click **Log In**.

NOTE

- The default user name is **admin**. You can change it to another user name.
- The account is locked after incorrect passwords are entered for five consecutive times. It will be automatically unlocked three minutes later.

----End

Follow-up Procedure

- For system security, the DME IQ Client will log out automatically if a user who has logged in does not perform any operations for 10 minutes. A window that asks the user to log in again is displayed. You can enter the password to log in again.
- When the host where the DME IQ Client resides is in sleep mode, the DME IQ Client process will be suspended and cannot run properly. Therefore, you are advised to forbid the host from going to sleep after the screen is locked.

3.2.3.2 Logging In When Forgetting the Password

This section describes how to log in to the DME IQ Client when you forget the login password.

Prerequisites

A secure mailbox has been configured.

Procedure

Step 1 Start the DME IQ Client.

Step 2 In the login dialog box that is displayed, enter the user name and click **Forgot Password?**

Step 3 In the **Retrieve Password** dialog box, click **Get Verification Code**. A message is displayed indicating that a verification code is successfully sent.

NOTE

The system sends the verification code to the configured secure mailbox.

Step 4 Enter the verification code and click **OK**.

Step 5 In the **Change Password** dialog box that is displayed, set **New Password** and **Confirm Password** and click **OK**.

NOTE

- The new password must contain 8 to 32 characters including uppercase letters, lowercase letters, and special characters. The password cannot be set to a weak password, such as **Huawei@123** or **Admin@123**.
- The new password must be different from any of the five recently used passwords.
- The password validity period is six months. Change the password periodically.

Step 6 Enter the new password to log in again.

----End

3.2.3.3 Changing the Password

This section describes how to change the password for logging in to the DME IQ Client.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⚙.

The **System Settings** page is displayed.

Step 3 Click the **Advanced** tab.

The page for advanced settings is displayed.

Step 4 Click **Change Login Password**.

The **Reset Password** dialog box is displayed. Specify **Old Password**, **New Password**, and **Confirm Password** to change the password of the current login user.

NOTE

- The new password must contain 8 to 32 characters including uppercase letters, lowercase letters, and special characters. The password cannot be set to a weak password, such as **Huawei@123** or **Admin@123**.
- The new password must be different from any of the five recently used passwords.
- The password validity period is six months. Change the password periodically.

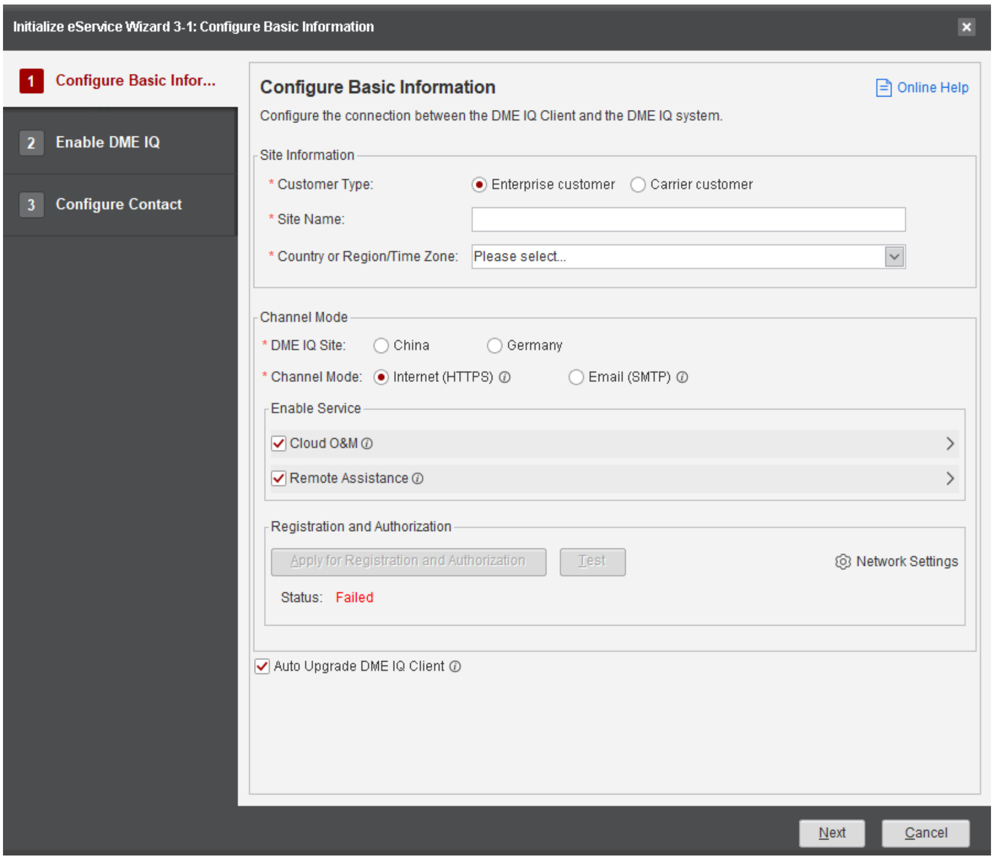
----End

3.3 Initial Configuration

When you log in to the DME IQ Client for the first time, you need to perform initial configuration.

Procedure

Step 1 After the first login is successful, the initialization window pops up. The **Configure Basic Information** page is displayed by default.



Initialize eService Wizard 3-1: Configure Basic Information

1 Configure Basic Infor...
2 Enable DME IQ
3 Configure Contact

Configure Basic Information

Configure the connection between the DME IQ Client and the DME IQ system.

Site Information
- * Customer Type: ● Enterprise customer ○ Carrier customer
- * Site Name:
- * Country or Region/Time Zone: Please select...

Channel Mode
- * DME IQ Site: ○ China ○ Germany
- * Channel Mode: ● Internet (HTTPS) ○ Email (SMTP)

Enable Service
- ☑ Cloud O&M
- ☑ Remote Assistance

Registration and Authorization

Status: Failed

☑ Auto Upgrade DME IQ Client

Step 2 Configure basic information.

Set the information based on site conditions. Items with red asterisks are mandatory.

1. Select a customer type, including **Enterprise customer** and **Carrier customer**.
2. Set **Site Name** and **Country or Region/Time Zone**.
3. Configure the DME IQ site.

   After you select a country or region/time zone, the system will automatically match the DME IQ site. You can also select another DME IQ site.
4. Select the channel mode, including **Internet (HTTPS)** and **Email (SMTP)**.
   - **Internet (HTTPS)**: recommended.

     i. **Optional:** Enable services.

     You can select **Cloud O&M** and **Remote Assistance**.

     ○ Cloud O&M includes basic information, alarm reporting, diagnosis, and real-time performance analysis. Basic site and device information can be automatically uploaded to the DME IQ cloud system.

     ○ Remote assistance includes fault locating, inspection, upgrade, and historical performance analysis. You can obtain routine O&M information from the DME IQ cloud system, execute tasks, and upload information or files generated by tasks.

     ii. Set account registration and authorization.

1) Click **Apply for Registration and Authorization**.

   The **Apply for Registration and Authorization** dialog box is displayed.

2) Select an authorization mode, including **Online** and **Paper**.

   Online authorization:

   Select an application method, including **Phone**, **Email**, and **Uniportal account**. After selecting **Phone**, you need to enter the phone number and the verification code. After selecting **Email**, you need to enter the email address and the verification code. After selecting **Uniportal account**, you need to enter the Uniportal account and password.

   Set **Customer Company Name** and **Customer Email** to generate and receive an electronic authorization letter respectively.

   Click **Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data** to read it, and select **I have read and agree to the Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data and agree to connect to the DME IQ cloud system.**

   NOTE

   If the device O&M service is provided by a supplier, you can also configure **O&M Service Supplier** and **O&M Service Supplier Email** to generate and receive an electronic authorization letter respectively.

   Paper authorization:

   Select an application method, including **Phone**, **Email**, and **Uniportal account**. After selecting **Phone**, you need to enter the phone number and the verification code. After selecting **Email**, you need to enter the email address and the verification code. After selecting **Uniportal account**, you need to enter the Uniportal account and password.

   To upload an authorization letter, click **Browse** and upload the *Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data* signed by the customer.

   NOTE

   Supported authorization letter file types include: zip, rar, 7z, jpeg, jpg, png, doc, docx, and pdf.

3) Click **OK** and confirm the registration and authorization as prompted.

4) After the registration is passed, the system automatically performs the test. If the test is passed, **Status** will change to **Registered and authorized** and the system will send the generated electronic authorization letter to the customer's email address.

   If the connection test fails, **Status** will change to **Failed**. . You can click **Test** to connect again.

iii. **Optional:** Set the network.

1) Configure the communication port.

   The port is used by the DME IQ Client to connect to the DME IQ cloud system. The default port is **443**.

2) Select **Use Proxy**.

3) Set **Agent Type**, **Server**, **Port**, **Account**, and **Password**.

   NOTE

   The port number is an integer ranging from 1 to 65535.

iv. **Optional:** Configure **Auto Upgrade DME IQ Client**.

If this option is selected, the DME IQ Client will automatically detect and install updates.

– **Email (SMTP)**:

NOTE

The configured email server must be connected to the host where the DME IQ Client is located over the network. You can run the **ping** command to check the network connection between the host and the email server.

i. **Optional:** Enable services.

The email channel supports only **Automatic O&M**, including basic information, alarm reporting, diagnosis, and real-time performance analysis.

ii. Configure the email server.

Table 3-12 describes related parameters.

Table 3-12 Email server parameters

Parameter	Description	Value
Outgoing Server (SMTP)	IP address of the customer's SMTP server. The SMTP server is an email sending server that complies with the SMTP protocol. You can send alarm emails to the inbox of the DME IQ cloud system through the SMTP server.	[Example] SMTP.customer.com
Server Port	Port number of the email server. The value ranges from 1 to 65535.	[Example] 25

Parameter	Description	Value
Secure Connection Mode	Whether to use the secure connection mode to send emails. The value can be **TLS1.2**, **TLS1.1/TLS1.0**, **SSL**, or **Disable**. **NOTE** **TLS1.2** is recommended. Otherwise, security risks may exist.	[Example] If you want to use the secure connection mode, select **TLS1.2**, **TLS1.1/TLS1.0**, or **SSL**. Otherwise, select **Disable**.

iii. **Optional:** Click **Advanced**. The **Advanced** dialog box is displayed.

1) Select **Use Proxy** and enter the address and port number of the server.

2) Select **Mailbox certificate requires authentication** and click **Browse**. In the dialog box that is displayed, select a file that you need and click **Open**.

NOTE

You are advised to perform mailbox certificate authentication.

3) In the **Change Public Key** area, click **Browse**.

Select a public key file that you need and click **Open**.

Click **Apply**.

NOTE

Enter the login password again to import the new public key file. After the file is imported, the system sends an email to the administrator.

You can contact technical support engineers to obtain the latest public key.

4) Click **OK**.

iv. Set the sender email.

Table 3-13 describes related parameters.

Table 3-13 Sender email parameters

Parameter	Description	Value
Sender Email	Sender email address.	[Example] zhangsan@huawei.com

Parameter	Description	Value
Account	SMTP account of the sender. When the sender sends alarm emails over the SMTP server, the sender is required by the SMTP server to enter the SMTP account and password for authentication.	[Example] user01
Password	SMTP account password of the sender. When the sender sends alarm emails over the SMTP server, the sender is required by the SMTP server to enter the SMTP account and password for authentication.	[Example] aJ1p23dySQ
Max. Attachment Size	Maximum size of the attachment that can be sent by the email.	Value range: 1 MB to 20 MB

v. Click **Test**. The **Test** dialog box is displayed.

1) In **Receiver Email**, enter the email address for receiving test results.

NOTE

Receiver Email can be the email address of the sender or the receiver.

2) Click **Test**. A dialog box is displayed indicating the test result.

3) Click **OK**.

Step 3 Click **Next** and enter your Uniportal account to enable DME IQ.

If you do not have a Uniportal account, click **Click here to register**, register an account, and then enter the account.

You can also click **Experience Demo** in the upper right corner to access and experience the DME IQ Demo.

Step 4 Click **Next** and set the contact information.

1. Configure O&M contacts.
   - Adding an O&M contact

     i. Click **Add**. The **Add O&M Contact** dialog box is displayed.

     ii. Set the first name, last name, phone number, and email address of the contact.

     iii. Click **OK**.

> 🕮 NOTE
>
> The contact information configured here can be used by the DME IQ cloud system to contact you when the DME IQ Client detects a device fault.

- Modifying an O&M contact
  1. In the contact list, select the contact you want to modify.
  2. Click **Modify**.

     The **Modify O&M Contact** dialog box is displayed.
  3. Modify the contact No., phone number, and email address.
  4. Click **OK**.
- Deleting an O&M contact
  1. In the contact list, select the contact you want to delete.
  2. Click **Delete**.

     A dialog box is displayed, asking you whether to delete the contact.
  3. Click **OK**.

     > 🕮 NOTE
     >
     > The DME IQ Client requires that at least one contact be retained so that maintenance engineers can contact you. Do not delete all contacts.

2. **Optional:** Configure the O&M service supplier.

   If the customer type is set to **Enterprise customer** and the device O&M service is provided by a supplier, you need to set the O&M service supplier information.

   a. Click **Set**. The **Set Supplier Information** window is displayed.

   b. Select an access mode.

   - Supplier information

     Enter the supplier's partner company name, technical support email, technical support phone, and engineer Uniportal account.
   - Access key

     Enter the access key obtained from the partner portal of the DME IQ cloud system.

   c. Click **OK**.

   > 🕮 NOTE
   >
   > To delete the supplier information, click **Delete** and confirm the operation as prompted.

Step 5 Click **Finish**.

The system will display different messages depending on the progress of the initial configuration. Perform operations as prompted.

You have finished initializing the DME IQ Client. The device management page is displayed.

NOTE

After the DME IQ Client is initialized, it is enabled to automatically start when the system starts. Therefore, firewall or antivirus software messages may be displayed. Allow this operation when such messages are displayed.

----End

3.4 Adding a Device

After the initial configuration is complete, you need to add devices to be maintained and managed on the device management page.

For details about how to add a device, see **4.1.1 Adding a Device**.

3.5 Actions After Installation and Deployment

To ensure that the DME IQ Client can work properly, you need to check the system service, contact the TAC for site authentication, and verify the alarm reporting function after the installation and configuration.

3.5.1 Checking the System Service

This section describes how to check and manually register the system service. You can follow the instructions in this section to check whether the system service of the DME IQ Client has been registered successfully.

Context

When the DME IQ Client is initialized, **Background Services** will be automatically installed. After the services are successfully installed, the system will automatically run the services in the background even if you restart your computer or exit the DME IQ Client.

Procedure

Step 1 Click ⚙.

The **System Settings** page is displayed.

Step 2 On the **Advanced** tab page, check whether the status of **Background Services** is **Enabled**.

- If yes, the registration is successful. No further operation is required.
- If no, go to **Step 3**.

Step 3 Click **Enable** to enable **Background Services**.

NOTE

If you fail to enable it, exit the DME IQ Client, log in to the Windows operating system as user **Administrator**, go to the installation directory of the DME IQ Client, right-click **dmeiq.exe**, and choose **Run as administrator** from the shortcut menu to start the software. Then, choose **System Settings** > **Advanced** and enable **Background Services**.

----End

3.5.2 Contacting the TAC for Site Authentication

After the DME IQ Client is installed and initialized, TAC authentication is required for accessing the DME IQ cloud system.

You can select online or paper authorization during initial configuration. The TAC will authenticate the site in about one week.

3.5.3 Verifying the Alarm Reporting Function

After confirming that the site has been authenticated, verify that the alarms of each device can be correctly reported to the DME IQ cloud system.

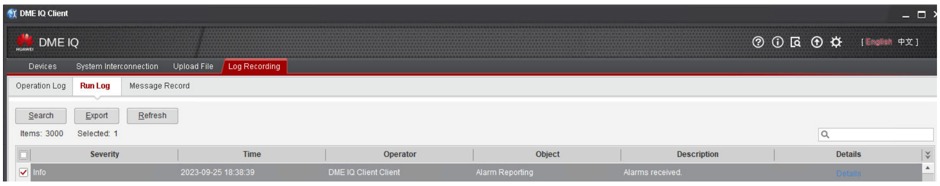
Procedure

Step 1 Send a test alarm on each added device.

NOTE

- For storage devices, send test alarms on DeviceManager.
- For servers, send test alarms on the device management page.
- For cloud computing products, send test alarms on the product management page.
- For network devices, send test alarms on the device management page.

Step 2 Choose **Log Recording** > **Run Log** on the DME IQ Client and check whether there are log records for the test alarms.



Items: 3000 Selected: 1

☐	Severity	Time	Operator	Object	Description	Details
☑	Info	2023-09-25 18:38:39	DME IQ Client Client	Alarm Reporting	Alarms received.	Details

Step 3 Contact the TAC to confirm that the DME IQ cloud system has received the test alarms.

----End

3.5.4 Verifying the Remote Inspection and Log Collection Functions

The DME IQ Client has integrated service plug-ins such as inspection, log collection, and performance data collection. You need to contact the TAC to check whether the service plug-ins are normal.

Procedure

Step 1 Contact the TAC to create remote inspection and log collection tasks.

Step 2 Choose **Log Recording** > **Run Log** on the DME IQ Client and confirm that there are log records for the tasks and the tasks are being executed.

Step 3 After the inspection reports and logs generated by the tasks are displayed on the **Upload File** tab page, confirm with the TAC that the back-end system has received the inspection reports and logs.

----End

3.6 Other Deployment Modes

3.6.1 (Optional) Dual-Host Deployment

3.6.1.1 Description

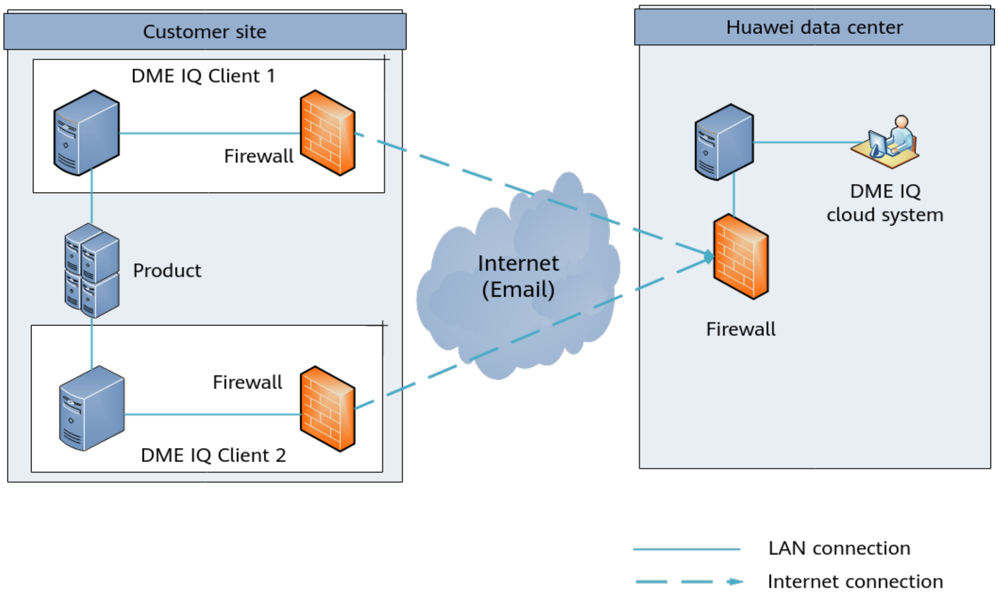
- One DME IQ Client host can meet requirements of a common user.
- If the DME IQ Client host is faulty, the DME IQ Client will be disconnected from the cloud system and cannot monitor alarms. If you want to ensure the reliability of real-time alarm monitoring, use the dual-host deployment solution.
- In the dual-host deployment solution, the DME IQ Client is deployed on two hosts on the user network. When one host is faulty, the other host is running properly.

3.6.1.2 Deployment

When the dual-host deployment solution is used, the following requirements must be met:

- The DME IQ Client must be deployed on two hosts to ensure that the two hosts are in different network environments and can back up each other.
- If the DME IQ Client is deployed on two hosts, select all functions when the active DME IQ Client is deployed, and select only the alarm reporting function when the standby DME IQ Client is deployed. Otherwise, service exceptions will occur. You need to log in to the DME IQ Client and choose **System Settings** > **Configure Basic Information** to view or configure the functions.

Figure 3-2 Dual-host deployment networking



4 System Management

This chapter describes how to use DME IQ Client functions, such as device management, system interconnection, file upload, and log recording. In addition, you can view or manage current system settings.

4.1 Device Management

You can add, modify, remove, and import device information, as well as enable and disable alarm reporting, facilitating your management and maintenance of devices.

4.1.1 Adding a Device

This section describes how to add a device you want to manage and maintain.

Prerequisites

The management IP address and the SNMP parameters of the device that you want to add have been obtained from the system administrator. For details about the SNMP parameters, see **SNMP Parameters** and **C Configuring SNMP Parameters**.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

Step 3 Click **Add**.

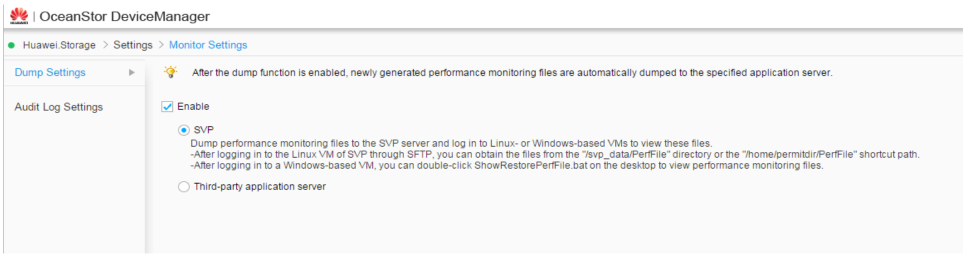
Storage Device, **Server Device**, and **Network Device** are displayed in the drop-down list. Click the type of the device to be added. The dialog box for adding a device is displayed.

Step 4 Add a management IP address.

Click + in the **Management IP Address** area. The **Add Management IP Address** dialog box is displayed. Enter the management IP address of the device and click **OK**.

NOTE

- If you want to query IPv6 addresses in an SVP environment, consult device administrators. You can also choose **Start** > **Run** and run the **cmd** command. In the dialog box that is displayed, run the **ipconfig** command. In the CLI, **IPv6 Address** is the device management IP address.
- If the IP address to be added is the management IP address in the SVP environment of a high-end storage device, you need to log in to DeviceManager and choose **Settings** > **Monitor Settings** > **Dump Settings**. When the following page is displayed, select **Enable**, select **SVP**, and then click **Save** to configure the performance monitoring file dump.



| OceanStor DeviceManager
Huawei.Storage > Settings > Monitor Settings
Dump Settings ▸
Audit Log Settings

After the dump function is enabled, newly generated performance monitoring files are automatically dumped to the specified application server.

☑ Enable

● SVP
Dump performance monitoring files to the SVP server and log in to Linux- or Windows-based VMs to view these files.
-After logging in to the Linux VM of SVP through SFTP, you can obtain the files from the "/svp_data/PerfFile" directory or the "/home/permitdir/PerfFile" shortcut path.
-After logging in to a Windows-based VM, you can double-click ShowRestorePerfFile.bat on the desktop to view performance monitoring files.

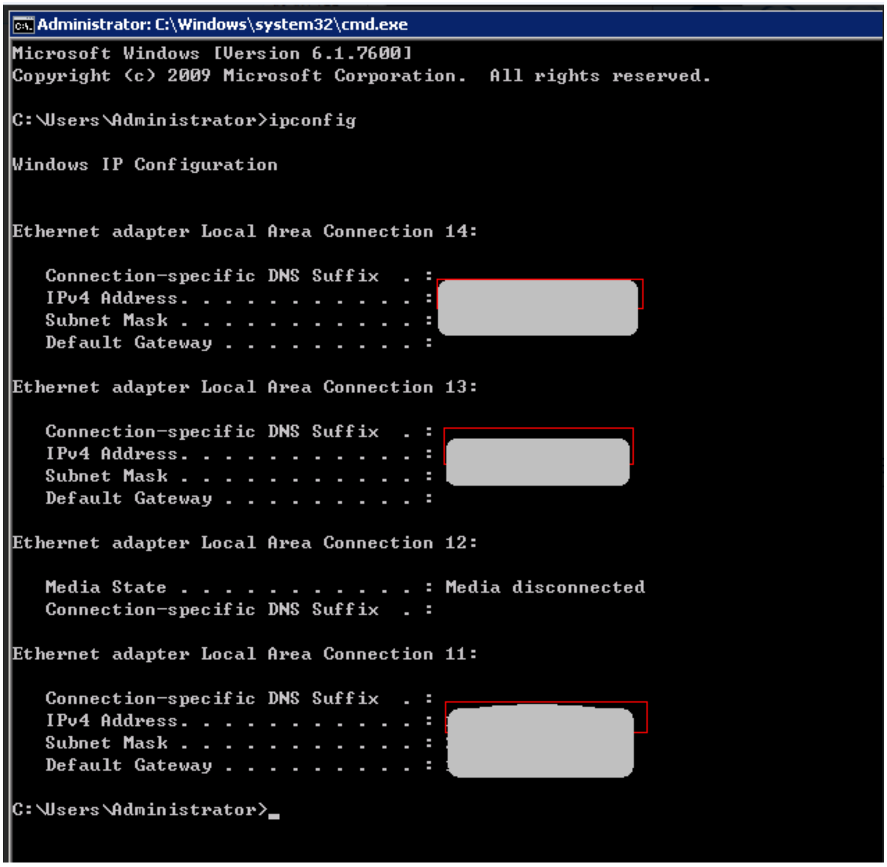
○ Third-party application server

WARNING

If you are adding a device in the SVP environment on 18000 V3, the management network port IP address of the SVP must be added.

If you are adding a device in the SVP environment on 18000 V100R001, add all IP addresses of the device. Otherwise, the alarms reported by the device may fail to be received. The following explains how to query IP addresses:

Choose **Start** > **Run** and enter **cmd** to open the **cmd** window. In the dialog box that is displayed, enter **ipconfig**. **IPv4 Address** in the dialog box is the device management IP address. See the following figure.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 14:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection 13:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection 11:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

C:\Users\Administrator>_
```

Step 5 Set the device account and password.

NOTE

Storage devices can be added in standard or simplified access mode. Servers and network devices are added in standard access mode by default.

- Standard access

  a. In the **Authentication Type** drop-down list, select **Password authentication** or **Public key authentication**.

     - **Password authentication**

       1) Specify **Username**, **Password**, and **Port**.

       2) Set **SSH Security Algorithm** to **Yes** or **No**.

       3) You also need to specify **HTTPS Port** and **HTTPS Certificate Verification** when adding a storage or server device.

4) When adding a storage device, if **Password authentication** is selected, you need to set **Auto Password Update**.

NOTE

- **Auto Password Update** enables the password of the account to be automatically updated. The new password is encrypted using AES256 and saved. This prevents the DME IQ Client from being incapable of accessing the device when the device password expires.
- Accounts for which the password is automatically updated can be used only by the DME IQ Client to manage storage systems.
- The password cannot be automatically updated for the super administrator, user **admin** and user **omuser**, and read-only users. You are advised to create a common administrator account named **dmeIq_xx** on DeviceManager of the storage device. When creating the account, you must select **CLI**, **RESTful**, and **SFTP** for **Login Method**. If you need to log in to DeviceManager to create an SNMP user, select **DeviceManager** too.
- Distributed storage does not support automatic password update.

- **Public key authentication**

1) Specify **Username**, **Key**, **Key Password**, and **Port**.
2) Set **SSH Security Algorithm** to **Yes** or **No**.
3) You also need to specify **HTTPS Port** and **HTTPS Certificate Verification** when adding a storage or server device.

NOTICE

- To add a data protection storage device, manually change the value of **HTTPS Port** to **25081**. OceanCyber devices can be added only using the user name and password of the super administrator.
- For a FusionStorage Block device, the default authentication user name and password are **cmdadmin** and **IaaS@PORTAL-CLOUD9!**, respectively. To add the device, manually change the value of **HTTPS Port** to **28443**.

b. **Optional:** If the device to be added is a storage or server device and you need to use only the alarm reporting function, select **Only the alarm reporting function is used and therefore, no device account is configured.**

NOTE

- When you add a storage device, the session timeout duration of the device will be checked. If the session timeout duration is less than 8 minutes, you may frequently log in to and log out of the storage device during performance collection. In this case, you are advised to set the session timeout duration to more than 8 minutes on DeviceManager.
- If the device to be added is a scale-out storage device and is about to be upgraded from OceanStor Pacific series 8.1.0 to a later version, you need to configure the FSM node information required for the upgrade. The procedure is as follows:
  1. Choose **System Settings** > **Configure Basic Information**, select **Upgrade** under **Remote Assistance**, and click **OK**.
  2. Select the device to be upgraded and click **Modify**. The **Modify Storage Device** page is displayed. Then, click **Configure** and configure the information on the FSM node information page.

     When you configure the FSM node, the common user must be the **fsadmin** user in the system.

c. Set device SNMP parameters.

To add storage and server devices, you need to set SNMP parameters. To add network devices, you only need to set the IP address and device account and password.

NOTE

The versions configured for the DME IQ Client and the device must be the same.

- If v2c is used, the read and write communities and port must be the same as those configured for the device.
- If v3 is used, the user name, context name, port, encryption protocol and password, and authentication protocol and password must be the same as those configured for the device.
- If two or more 18000 V3R3C20SPC100 storage devices or earlier versions need to be added, SNMP v2c must be used.

For details about SNMP parameters, see **Table 4-1** and **Table 4-2**.

Table 4-1 Description of parameters in the v2c template

Parameter	Description	Value
Port	Port number used for the communication between devices.	The value is an integer ranging from 1 to 65535. Default value: **161** **NOTE** To add a FusionStorage Block device, change the port to **20161**.
Read Community	Name of the community that has the read permission.	[Example] storage_public

Parameter	Description	Value
Write Community	Name of the community that has the write permission.	[Example] storage_private **NOTE** OceanCyber devices do not support the write community. When adding the devices, you do not need to set this parameter.
NOTE You can run commands to change the read and write communities. For details about the commands, see the *Command Reference* of the device.		

Table 4-2 Description of parameters in the v3 template

Parameter	Description	Value
Port	Port number used for the communication between devices. This parameter is mandatory.	The value is an integer ranging from 1 to 65535. Default value: **161** **NOTE** To add a FusionStorage Block device, change the port to **20161**.
Timeout	Timeout interval for device SNMP (unit: seconds).	The value is an integer ranging from 1 to 60.

Parameter	Description	Value
Username	User name used for accessing the device. This parameter is mandatory.	[Description] 1. Storage device ○ For devices earlier than V300R003C00, the user name must be **Kaimse**. Otherwise, the alarm reporting function is unavailable. ○ For devices of V300R003C00 and later versions, there is no default user name. You need to manually add a user name. 2. Server device For RH, KunLun, and E9000 servers, the default user name is **root**.

Parameter	Description	Value
Context Name	Name of the context engine.	[Description] ■ The value must be the same as the context name on the device or left blank. ■ This parameter is mandatory for 18000 V100R001C10 or earlier and the default value is **Array**. ■ For V3 series V300R006C00 and later versions, this parameter value can be modified on DeviceManager. You are advised to retain the default value **Array**. If you want to modify the value, enter a name that contains only uppercase and lowercase letters. Otherwise, devices cannot be added to the DME IQ Client. [Example] Array

Parameter	Description	Value
Authentication Protocol	Protocol used for verifying messages. This parameter is mandatory. If this parameter is set to **NONE**, **Authentication Password**, **Encryption Protocol**, and **Encryption Password** cannot be modified.	The value can be **MD5**, **SHA**, **SHA224**, **SHA256**, **SHA384**, or **SHA512**, or left blank. If a protocol is selected, you must set the authentication password. **NOTE** ■ **SHA256** is selected by default. ■ **MD5** is an insecure protocol, and **SHA** indicates the SHA1 protocol.

Parameter	Description	Value
Authentication Password	If the authentication protocol is used to verify messages, you need to set the authentication password.	[Description] 1. Storage device ○ For devices earlier than V300R003C00, the default password is **ism@Storage**. ○ For devices of V300R003C00 and later versions, there is no default password. You need to manually add a password. 2. Server device ○ For RH, KunLun, and E9000 servers, the default password is **Huawei12#$**. ○ The authentication password must be the same as the login password of the device management software. Otherwise, the alarm reporting function may be abnormal.

Parameter	Description	Value
Encryption Protocol	Encryption protocol used to encapsulate data.	The value can be **DES**, **AES**, **3DES**, **AES192**, or **AES256**, or left blank. If a protocol is selected, you must set the encryption password. ▪ Data Encryption Standard (DES) is an internationally universal encryption algorithm. The key length is 56 bits. ▪ Advanced Encryption Standard (AES) supports three types of key lengths: 128, 192, and 256 bits. Different key lengths provide security protection of different levels. **NOTE** ○ **AES** is selected by default, and **AES** indicates the AES128 protocol. ○ **DES** is an insecure protocol.

Parameter	Description	Value
Encryption Password	If an encryption algorithm is used to encapsulate data, you must set an encryption password.	[Description] 1. Storage device ○ For devices earlier than V300R003C00, the default password is **ism@Storage**. ○ For devices of V300R003C00 and later versions, there is no default password. You need to manually add a password. 2. Server device ○ For RH, KunLun, and E9000 servers, the default password is **Huawei12#$**. ○ The encryption password must be the same as the login password of the device management software. Otherwise, the alarm reporting function may be abnormal.
NOTE You can run commands to query the user name, authentication protocol, encryption protocol, and context name, and to modify the user name, authentication protocol and password, and encryption protocol and password. For details about the commands, see the *Command Reference* of the device.		

d. Click **Finish**.

The system displays a message indicating the result of adding the device and asking you whether to enable alarm reporting.

e. Click **OK**.

About 10 minutes after storage and server devices are added, you can view the device information on the DME IQ cloud system.

- Simplified access

  The DME IQ Client uses the super administrator (**admin**) of a storage device to create an SSH account with the CLI, RESTful, and SFTP login permissions on DeviceManager and uses the account to create a USM user. The created SSH account and the USM user start with **dmeIq** and are used to connect the DME IQ Client to the storage device.

  a. Select a storage device model from the drop-down list.

  NOTE

  Currently, only OceanStor 6.1.5, OceanStor Dorado 6.1.5, and OceanProtect 1.2.0 can be added in simplified access mode.

  b. Enter the user name and password of the super administrator of the storage device.

  c. Click **OK**.

  About 10 minutes after devices are added, you can view the device information on the DME IQ cloud system.

----End

NOTE

If a storage device is added to the DME IQ Client, you do not need to configure DME IQ (Call Home for V500R007C30, Dorado V3, and their earlier versions; or eService for V500R007C50 or later, and OceanStor & OceanStor Dorado 6.1.5 or earlier) on DeviceManager to avoid repeated access to the DME IQ cloud system.

4.1.2 Modifying a Device

This section describes how to modify the account password and SNMP parameters of a device.

Prerequisites

- A device has been added to the device list.
- The alarm reporting function is not enabled for the device to be modified.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

Step 3 In the device list, select the device to be modified and click **Modify**.

The page for modifying a device is displayed.

Step 4 Modify the account password and SNMP parameters of the device.

- You can modify the **Authentication Type**, **Username**, **Password**, and **Port** parameters of the device.
- For details about the SNMP parameters, see **Step 5.c**.

NOTE

If the device to be modified is a network device, you do not need to modify SNMP parameters.

- If the device to be modified is a storage device, you can set whether to automatically update the password. For details, see **whether to automatically update the password**.

Step 5 Click **OK**. The account password and SNMP parameters of the device are modified.

A dialog box is displayed, indicating the modification result.

----End

4.1.3 Removing a Device

This section describes how to remove a device. After a device is removed, it cannot be managed by the DME IQ Client any longer.

Prerequisites

- A device has been added to the device list.
- The alarm reporting function is not enabled for the device to be deleted.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

The device list page is displayed.

Step 3 In the device list, select the device to be removed and click **Remove**.

The **Information** dialog box is displayed.

NOTE

If the alarm reporting function has been enabled for the device to be removed, a dialog box is displayed, prompting you to stop alarm reporting before removing the device. For details about how to stop alarm reporting, see **4.1.8 Stopping Alarm Reporting**.

Step 4 Click **OK**.

The device is removed.

----End

4.1.4 Adding Devices in Batches

After you import a device information file, the system automatically adds devices to the device list in batches.

Prerequisites

The import template has been obtained and device information has been filled in the template.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

The device list page is displayed.

Step 3 Click **Batch Import**.

The **Batch Import** dialog box is displayed.

Step 4 Select the file to be imported.

NOTE

You can obtain the file to be imported by using the following method:

Choose **Devices** > **Get Template File** and obtain **Import_DeviceList_Template.xls**. Then fill in device information in the file.

Step 5 Click **Open**.

You have finished adding devices in batches.

----End

4.1.5 Obtaining an Import Template

This section describes how to obtain a template for importing a device information file. Then you can fill in detailed device information in the template.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

The device list page is displayed.

Step 3 Click **Get Template File**.

The **Save Template File** dialog box is displayed.

Step 4 Select a save path for the template.

Step 5 Click **Save**.

You have finished obtaining the import template.

----End

Follow-up Procedure

You can fill in device configuration information in the template to add devices in batches. For details, see **4.1.4 Adding Devices in Batches**.

4.1.6 Exporting Devices

This section describes how to export a device information file.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

The device list page is displayed.

Step 3 Click **Export Device**.

The **Save Export Device File** dialog box is displayed.

Step 4 Select a save path for the file.

Step 5 Click **Save**.

You have finished exporting devices.

----End

4.1.7 Starting Alarm Reporting

This section describes how to start alarm reporting. After alarm reporting is started, the system will send alarm information (excluding event information) to the DME IQ cloud system. Service personnel of the DME IQ cloud system will take measures to handle the alarms.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

The device list page is displayed.

Step 3 Select the device for which you want to start alarm reporting.

Step 4 Click **Start Alarm Reporting**.

📖 NOTE

- If the alarm information about an E9000 server to be added is being monitored by other management tools, ensure that the port number used by these tools for receiving alarms is 10162. Otherwise, the DME IQ Client cannot receive alarms.

----End

Follow-up Procedure

- If alarm reporting fails to be started, troubleshoot the fault by referring to **G.1 What Can I Do If the Alarm Reporting Function Fails to Be Enabled for a Device?**
- When the DME IQ Client is running, if the alarm reporting status becomes **Failed to receive the device alarms** or **Failed to connect the device**, troubleshoot the fault by referring to **G.2 What Can I Do If the Alarm Reporting Status Is Abnormal When the DME IQ Client Is Running?**

4.1.8 Stopping Alarm Reporting

This section describes how to stop alarm reporting. After alarm reporting is stopped, no more alarm emails are sent.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Devices** tab.

The device list page is displayed.

Step 3 Select the device for which you want to stop alarm reporting.

Step 4 Click **Stop Alarm Reporting**.

A dialog box is displayed asking you to confirm your operation.

Step 5 Click **OK**.

You have finished stopping alarm reporting.

----End

4.2 System Interconnection

This chapter describes how to interconnect the DME IQ Client with various systems.

4.2.1 Interconnecting with a System

Prerequisites

- The DME IQ Client has been deployed and connected to the DME IQ cloud system.
- The interconnected system is running properly and has been connected to the devices to be managed.

Configuration Information

- To perform log collection and remote inspection for cloud computing devices, you need to interconnect with FusionCare.

  Table 4-3 lists the parameters required for interconnecting with FusionCare and example values. Contact FusionCare administrators to obtain the actual parameter information.

Table 4-3 Parameters required for interconnecting with FusionCare

Parameter	Description	Example Value
IP Address/Website	IP address or website of FusionCare.	192.168.0.1

Parameter	Description	Example Value
Port	Port of FusionCare.	8805
Account	Account for interconnecting with FusionCare.	systemman
Password	Password for interconnecting with FusionCare.	Rest@Care123
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCare.	-

- To configure the alarm reporting function for FusionDirector, you need to interconnect the FusionDirector system with the DME IQ Client. Currently, only FusionDirector 1.5.0 or later can be interconnected with the DME IQ Client.

  Table 4-4 lists the parameters required for interconnecting with FusionDirector and example values. Contact FusionDirector administrators to obtain the actual parameter information.

  Table 4-4 Parameters required for interconnecting with FusionDirector

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionDirector alarms.	Yes
IP Address/Website	IP address of FusionDirector.	192.168.0.1
Port	Port of FusionDirector.	443
Account	Account for interconnecting with FusionDirector.	rootRedfish
Password	Password for interconnecting with FusionDirector.	Machine@123
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionDirector.	-

- To configure the alarm reporting function for Huawei ManageOne, you need to interconnect ManageOne with the DME IQ Client. Currently, only ManageOne 6.3/6.5.0, 6.5.1, 8.0, or later can be interconnected with the DME IQ Client.

  Table 4-5 lists the parameters required for interconnecting with ManageOne and example values.

Table 4-5 Parameters required for interconnecting with ManageOne

Parameter	Description	Example Value
System Version	ManageOne version.	8.0
Enable Alarm Reporting	Whether to report ManageOne alarms.	Yes
IP Address/Website	IP address of the ManageOne OC Maintenance Portal.	192.168.0.1
Port	Port of the ManageOne OC Maintenance Portal.	26335
Account	Account for interconnecting with the ManageOne OC Maintenance Portal.	thirdparty
Password	Password for interconnecting with the ManageOne OC Maintenance Portal.	Sy@1#3!5-OC6
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify ManageOne.	-

- To collect performance and diagnosis information about vCenter, you need to interconnect vCenter with the DME IQ Client. Currently, vCenter 6.0 and later versions can be interconnected with the DME IQ Client.

  Table 4-6 lists the parameters required for interconnecting with vCenter and example values.

Table 4-6 Parameters required for interconnecting with vCenter

Parameter	Description	Example Value
IP Address/Website	IP address or website of vCenter.	192.168.0.1
Port	Port of vCenter.	443
Account	Account for interconnecting with vCenter. The value is in the format of *vCenter read-only user name***@vsphere.local**.	user1@vsphere.local
Password	Password for interconnecting with vCenter.	Huawei@123

Parameter	Description	Example Value
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify vCenter.	-

- To configure the alarm reporting and remote log collection functions for FusionCube Vision Pro, you need to interconnect it with the DME IQ Client. Currently, FusionCube Vision Pro 8.0 or later can be interconnected with the DME IQ Client.

  Table 4-7 lists the parameters required for interconnecting with FusionCube Vision Pro and example values.

Table 4-7 Parameters required for interconnecting with FusionCube Vision Pro

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionCube Vision Pro alarms.	Yes
IP Address/Website	IP address of FusionCube Vision Pro.	192.168.0.1
Port	Port of FusionCube Vision Pro.	30443
Account	Account for interconnecting with FusionCube Vision Pro.	openapi
Password	Password for interconnecting with FusionCube Vision Pro.	Huawei@4321
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCube Vision Pro.	-

- To configure the alarm reporting and remote log collection functions for FusionCube Vision, you need to interconnect it with the DME IQ Client. Currently, FusionCube Vision 8.0.RC1 or later can be interconnected with the DME IQ Client.

  Table 4-8 lists the parameters required for interconnecting with FusionCube Vision and example values.

Table 4-8 Parameters required for interconnecting with FusionCube Vision

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionCube Vision alarms.	Yes
IP Address/Website	IP address of FusionCube Vision.	192.168.0.1
Port	Port of FusionCube Vision.	443
Account	Account for interconnecting with FusionCube Vision.	openapi
Password	Password for interconnecting with FusionCube Vision.	Huawei@4321
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCube Vision.	-

- To configure functions such as alarm reporting for FusionCompute, you need to interconnect it with the DME IQ Client. Currently, FusionCompute 8.0 or later can be interconnected.

  Table 4-9 lists the parameters required for interconnecting with FusionCompute and example values.

Table 4-9 Parameters required for interconnecting with FusionCompute

Parameter	Description	Example Value
Enable Alarm Reporting	Whether to report FusionCompute alarms.	Yes
IP Address/Website	FusionCompute IP address.	192.168.0.1
Port	Port of FusionCompute.	7443
Account	Account for interconnecting with FusionCompute.	gesysman
Password	Password of the user for interconnecting with FusionCompute.	GeEnginE@123
HTTPS Certificate Verification	Whether to use the HTTPS certificate to verify FusionCompute.	-

NOTE

- For 8.3 and later versions, the default interface interconnection user does not exist and you need to log in to FusionCompute as user **admin** to add the user for interconnection. To do so, log in to FusionCompute, choose **System** > **Rights Management** > **User Management**, and click **Add User** to create an interface interconnection user.
- Only versions 8.0 to 8.2 support performance data and diagnosis information collection. To use the performance data and diagnosis information collection function, interconnect FusionCompute with the DME IQ Client and then add the corresponding storage device. In addition, ensure that the performance monitoring function of FusionCompute is enabled. To check whether the function is enabled, log in to FusionCompute and choose **Monitoring** > **Performance** > **Monitoring Settings**, and check whether all indicators of hosts, datastores, clusters, and VMs are selected in the **Select KPIs to monitor** area. If the performance monitoring function is not enabled, select all indicators and click **Save** to enable the function.

Procedure

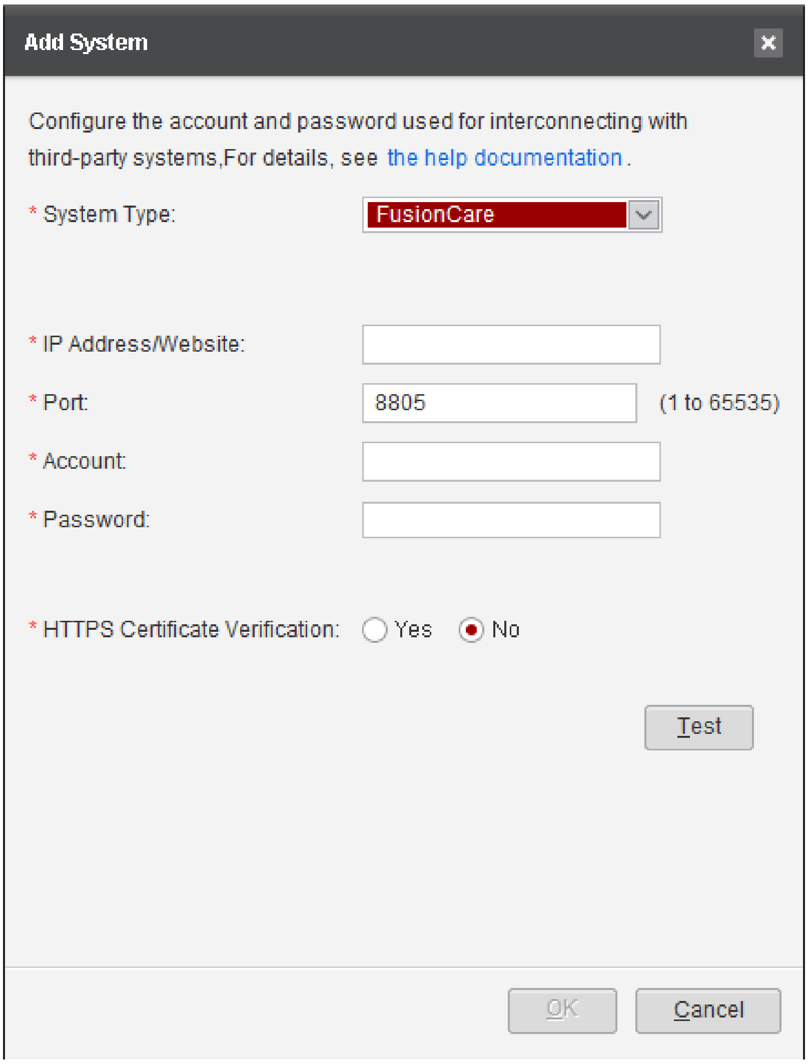
Step 1 Log in to the DME IQ Client.

Step 2 Click the **System Interconnection** tab.

The **System Interconnection** tab page is displayed.

Step 3 Click **Add**.

The **Add System** dialog box is displayed.



Add System

Configure the account and password used for interconnecting with third-party systems,For details, see the help documentation .

* System Type: FusionCare

* IP Address/Website:

* Port: 8805 (1 to 65535)

* Account:

* Password:

* HTTPS Certificate Verification: ○ Yes ● No

Step 4 Select a system type and enter the IP address/website, port, account, and password.

NOTE

- Currently, systems that can be interconnected with the DME IQ Client include FusionCare, FusionDirector, ManageOne, vCenter, FusionCube Vision Pro, FusionCube Vision, and FusionCompute.
- Set **Allow O&M** if the ManageOne version is 6.5.1 or 8.0.
- To interconnect with ManageOne 6.5.1, you need to enter the website, port, tenant name, account, password, O&M account, and O&M password.
- To interconnect with FusionCube Center Vision, set **System Type** to **FusionCube Vision Pro**, and set the values of other parameters to be the same as those for interconnecting with FusionCube Vision Pro.

Step 5 Select **Yes** or **No** for **HTTPS Certificate Verification**.

NOTICE

If the HTTPS certificate of the system to be interconnected is not verified, the identity of the system cannot be verified and the system may be forged. As a result, false information such as logs and inspection reports may be obtained from the forged system, which poses security risks.

Step 6 Click **Test** to check whether the system is interconnected successfully.

Step 7 After the test is passed, click **OK**.

----End

4.2.2 Modifying an Interconnected System

Step 1 Log in to the DME IQ Client.

Step 2 Click the **System Interconnection** tab.

The **System Interconnection** tab page is displayed.

Step 3 Select the interconnected system to be modified and click **Modify**.

The **Modify System** dialog box is displayed.

Step 4 You can modify **Port**, **Account**, and **Password** of the system.

Step 5 Click **Test** to check whether the system is interconnected successfully.

Step 6 After the test is passed, click **OK**.

----End

4.2.3 Deleting an Interconnected System

Step 1 Log in to the DME IQ Client.

Step 2 Click the **System Interconnection** tab.

The **System Interconnection** tab page is displayed.

Step 3 Select the interconnected system to be deleted and click **Delete**.

In the displayed dialog box, click **OK**.

----End

4.3 File Uploading

The file uploading function allows you to view files automatically uploaded to the DME IQ cloud system for fault locating and analysis of devices.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Upload File** tab. The page for uploading files is displayed.

Step 3 View details about the files that have been automatically uploaded.

The file types include logs, performance collection reports, and inspection reports.

NOTE

If a file fails to be uploaded, you can view the details in the **Details** column and click **Continue** in the **Operation** column to upload the file again.

----End

4.4 Log Recording

The log recording management function allows you to view and export operation logs, run logs, and message logs. This helps you learn about the operation records and running status of the devices under maintenance.

4.4.1 Managing Operation Logs

This section describes how to search for operation logs by criteria and export some or all operation logs to learn about user operations on the DME IQ Client.

4.4.1.1 Searching for Operation Logs

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Log Recording** tab.

The **Operation Log** tab page is displayed by default.

Step 3 Click **Search**.

The **Search for Operation Log** dialog box is displayed.

Set the search criteria, including **Module**, **Severity**, **Start Time**, **End Time**, and **Result**.

NOTE

In the **Search for Operation Log** dialog box, you can click **Reset** to quickly clear all search criteria.

Step 4 Click **OK**.

The search result is displayed in the operation log list.

NOTE

- You can search for operation logs generated in the latest year.
- **Optional:** You can click **Refresh** to search for the latest operation logs.

Step 5 Click **Details** to view details of operation logs about abnormal operations.

----End

4.4.1.2 Exporting Operation Logs

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click the **Log Recording** tab.

The **Operation Log** tab page is displayed by default.

Step 3 Select the operation logs to be exported and click **Export**.

The **Export Operation Logs** dialog box is displayed.

Step 4 Select a save path for exported logs and enter a name for the exported file.

The default name is **operalog**.

NOTE

If no operation log is selected, all searched operation logs are exported.

Step 5 Click **Save**.

A dialog box is displayed indicating the export result.

----End

4.4.2 Managing Run Logs

This section describes how to search for run logs by criteria and export some or all run logs to learn about the running status of the DME IQ Client.

4.4.2.1 Searching for Run Logs

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Choose **Log Recording** > **Run Log**.

The run log page is displayed.

Step 3 Click **Search**.

The **Search for Run Log** dialog box is displayed.

Step 4 Set the search criteria, including **Module**, **Severity**, **Start Time**, and **End Time**.

NOTE

In the **Search for Run Log** dialog box, you can click **Reset** to quickly clear all search criteria.

Step 5 Click **OK**.

The search result is displayed in the run log list.

NOTE

- You can search for the latest 3000 run logs.
- **Optional:** You can click **Refresh** to search for the latest operation logs.

Step 6 Click **Details** to view details of run logs about abnormal operations.

----End

4.4.2.2 Exporting Run Logs

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Choose **Log Recording** > **Run Log**.

The run log page is displayed.

Step 3 Select the run logs to be exported.

Step 4 Click **Export**.

The **Export Run Logs** dialog box is displayed.

Step 5 Select a save path for exported logs and enter a name for the exported file.

The default name is **runlog**.

NOTE

If no run log is selected, all searched run logs are exported.

Step 6 Click **Save**.

A dialog box is displayed indicating the export result.

----End

4.4.3 Managing Message Records

This section describes how to search for message records by criteria and export some or all message records to learn about the status of the channel configuration information about the DME IQ Client.

4.4.3.1 Searching for Message Records

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Choose **Log Recording** > **Message Record**.

The message record page is displayed.

Step 3 Click **Search**.

The **Search for Message Record** dialog box is displayed.

Step 4 Set the search criteria, including **Module**, **Severity**, **Start Time**, and **End Time**.

NOTE

In the **Search for Message Record** dialog box, you can click **Reset** to quickly clear all search criteria.

Step 5 Click **OK**.

The search result is displayed in the message record list.

NOTE

- You can search for the latest 3000 message records.
- You can click **Refresh** to search for the latest message records.

Step 6 In the message record list, click **Details** to view details of message records.

----End

4.4.3.2 Exporting Message Records

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Choose **Log Recording** > **Message Record**.

The message record page is displayed.

Step 3 Select the message records to be exported.

Step 4 Click **Export**.

The **Export Messages Records** dialog box is displayed.

Step 5 Select a save path for exported records and enter a name for the exported file.

The default name is **messagelog**.

NOTE

If no message record is selected, all searched message records are exported.

Step 6 Click **Save**.

A dialog box is displayed indicating the export result.

----End

4.5 System Settings

System settings include: configuring basic information, enabling DME IQ, setting the Call Home service, setting log dumping, and setting advanced properties. This chapter describes how to modify basic system information to facilitate management and operations.

4.5.1 Configuring Basic Information

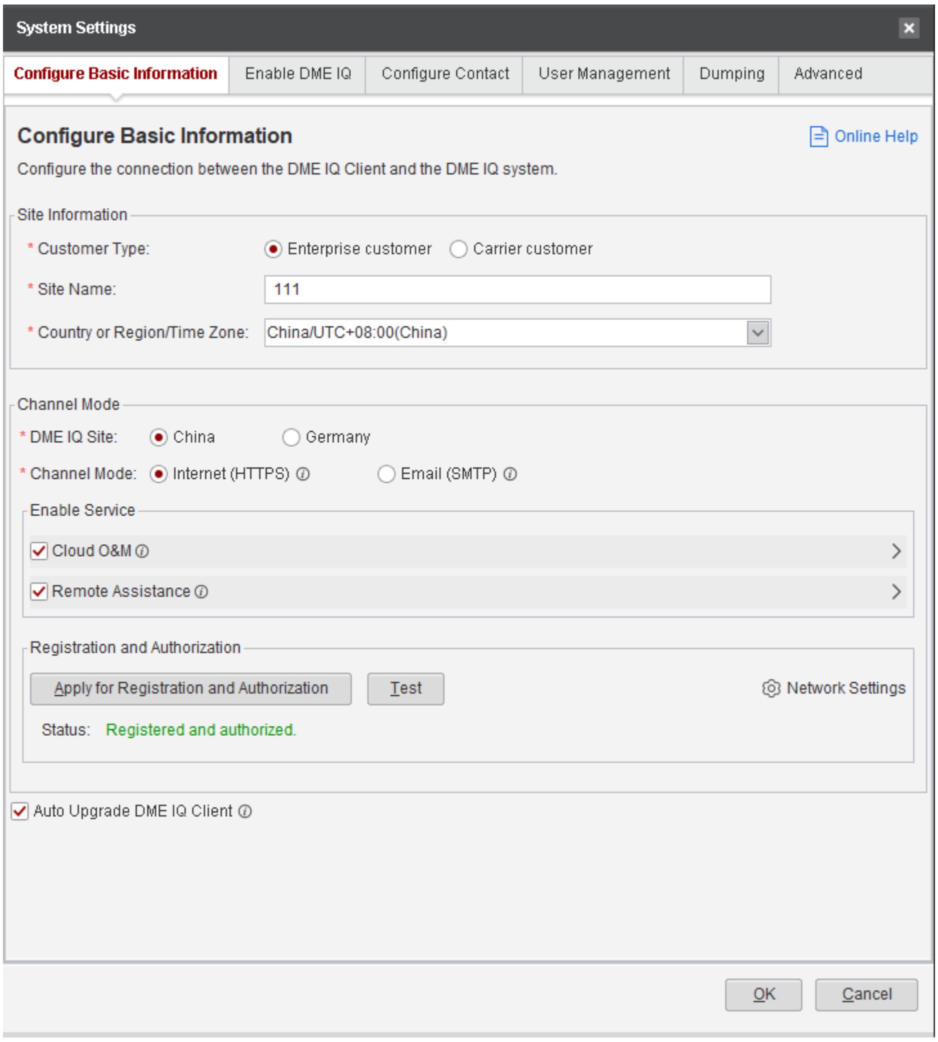
This section describes how to set the site information and channel mode. After the setting is complete, the system can send alarm information to the DME IQ cloud system by email or over the Internet.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⚙. The **System Settings** dialog box is displayed.

The **Configure Basic Information** tab page is displayed by default.



System Settings

Configure Basic Information

Configure the connection between the DME IQ Client and the DME IQ system.

Site Information

* Customer Type: ● Enterprise customer ○ Carrier customer

* Site Name: 111

* Country or Region/Time Zone: China/UTC+08:00(China)

Channel Mode

* DME IQ Site: ● China ○ Germany

* Channel Mode: ● Internet (HTTPS) ⓘ ○ Email (SMTP) ⓘ

Enable Service

☑ Cloud O&M ⓘ

☑ Remote Assistance ⓘ

Registration and Authorization

Status: Registered and authorized.

☑ Auto Upgrade DME IQ Client ⓘ

Step 3 Select a customer type, including **Enterprise customer** and **Carrier customer**.

Step 4 Set **Site Name** and **Country or Region/Time Zone**.

Step 5 Configure the DME IQ site.

After you select a country or region/time zone, the system will automatically match the DME IQ site. You can also select another DME IQ site.

Step 6 Select the channel mode, including **Internet (HTTPS)** and **Email (SMTP)**.

- **Internet (HTTPS)**: recommended.

  a. **Optional:** Enable services.

     You can select **Cloud O&M** and **Remote Assistance**.

     ▪ Cloud O&M includes basic information, alarm reporting, diagnosis, and real-time performance analysis. Basic site and device information can be automatically uploaded to the DME IQ cloud system.

     ▪ Remote assistance includes fault locating, inspection, upgrade, and historical performance analysis. You can obtain routine O&M information from the DME IQ cloud system, execute tasks, and upload information or files generated by tasks.

  b. Set account registration and authorization.

     i. Click **Apply for Registration and Authorization**.

        The **Apply for Registration and Authorization** dialog box is displayed.

     ii. Select an authorization mode, including **Online** and **Paper**.

        Online authorization:

        Select an application method, including **Phone**, **Email**, and **Uniportal account**. After selecting **Phone**, you need to enter the phone number and the verification code. After selecting **Email**, you need to enter the email address and the verification code. After selecting **Uniportal account**, you need to enter the Uniportal account and password.

        Set **Customer Company Name** and **Customer Email** to generate and receive an electronic authorization letter respectively.

        Click **Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data** to read it, and select **I have read and agree to the Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data and agree to connect to the DME IQ cloud system.**

        NOTE

        If the device O&M service is provided by a supplier, you can also configure **O&M Service Supplier** and **O&M Service Supplier Email** to generate and receive an electronic authorization letter respectively.

        Paper authorization:

        Select an application method, including **Phone**, **Email**, and **Uniportal account**. After selecting **Phone**, you need to enter the phone number and the verification code. After selecting **Email**, you need to enter the email address and the verification code. After selecting **Uniportal account**, you need to enter the Uniportal account and password.

        To upload an authorization letter, click **Browse** and upload the *Authorization Letter for Enabling DME IQ and Processing [Customer]'s Network Data* signed by the customer.

        NOTE

        Supported authorization letter file types include: zip, rar, 7z, jpeg, jpg, png, doc, docx, and pdf.

iii. Click **OK** and confirm the registration and authorization as prompted.

iv. After the registration is passed, the system automatically performs the test. If the test is passed, **Status** will change to **Registered and authorized** and the system will send the generated electronic authorization letter to the customer's email address.

If the connection test fails, **Status** will change to **Failed**. . You can click **Test** to connect again.

c. **Optional:** Set the network.

i. Configure the communication port.

The port is used by the DME IQ Client to connect to the DME IQ cloud system. The default port is **443**.

ii. Select **Use Proxy**.

iii. Set **Agent Type**, **Server**, **Port**, **Account**, and **Password**.

NOTE

The port number is an integer ranging from 1 to 65535.

d. **Optional:** Configure **Auto Upgrade DME IQ Client**.

If this option is selected, the DME IQ Client will automatically detect and install updates.

- **Email (SMTP)**:

NOTE

The configured email server must be connected to the host where the DME IQ Client is located over the network. You can run the **ping** command to check the network connection between the host and the email server.

a. **Optional:** Enable services.

The email channel supports only **Automatic O&M**, including basic information, alarm reporting, diagnosis, and real-time performance analysis.

b. Configure the email server.

Table 4-10 describes related parameters.

Table 4-10 Email server parameters

Parameter	Description	Value
Outgoing Server (SMTP)	IP address of the customer's SMTP server. The SMTP server is an email sending server that complies with the SMTP protocol. You can send alarm emails to the inbox of the DME IQ cloud system through the SMTP server.	[Example] SMTP.customer.com

Parameter	Description	Value
Server Port	Port number of the email server. The value ranges from 1 to 65535.	[Example] 25
Secure Connection Mode	Whether to use the secure connection mode to send emails. The value can be **TLS1.2**, **TLS1.1/TLS1.0**, **SSL**, or **Disable**. NOTE **TLS1.2** is recommended. Otherwise, security risks may exist.	[Example] If you want to use the secure connection mode, select **TLS1.2**, **TLS1.1/TLS1.0**, or **SSL**. Otherwise, select **Disable**.

c. **Optional:** Click **Advanced**. The **Advanced** dialog box is displayed.

i. Select **Use Proxy** and enter the address and port number of the server.

ii. Select **Mailbox certificate requires authentication** and click **Browse**. In the dialog box that is displayed, select a file that you need and click **Open**.

NOTE

You are advised to perform mailbox certificate authentication.

iii. In the **Change Public Key** area, click **Browse**.

Select a public key file that you need and click **Open**.

Click **Apply**.

NOTE

Enter the login password again to import the new public key file. After the file is imported, the system sends an email to the administrator.

You can contact technical support engineers to obtain the latest public key.

iv. Click **OK**.

d. Set the sender email.

Table 4-11 describes related parameters.

Table 4-11 Sender email parameters

Parameter	Description	Value
Sender Email	Sender email address.	[Example] zhangsan@huawei.com

Parameter	Description	Value
Account	SMTP account of the sender. When the sender sends alarm emails over the SMTP server, the sender is required by the SMTP server to enter the SMTP account and password for authentication.	[Example] user01
Password	SMTP account password of the sender. When the sender sends alarm emails over the SMTP server, the sender is required by the SMTP server to enter the SMTP account and password for authentication.	[Example] aJ1p23dySQ
Max. Attachment Size	Maximum size of the attachment that can be sent by the email.	Value range: 1 MB to 20 MB

e. Click **Test**. The **Test** dialog box is displayed.

i. In **Receiver Email**, enter the email address for receiving test results.

📖 NOTE

Receiver Email can be the email address of the sender or the receiver.

ii. Click **Test**. A dialog box is displayed indicating the test result.

iii. Click **OK**.

Step 7 Click **OK**.

----End

4.5.2 Enabling DME IQ

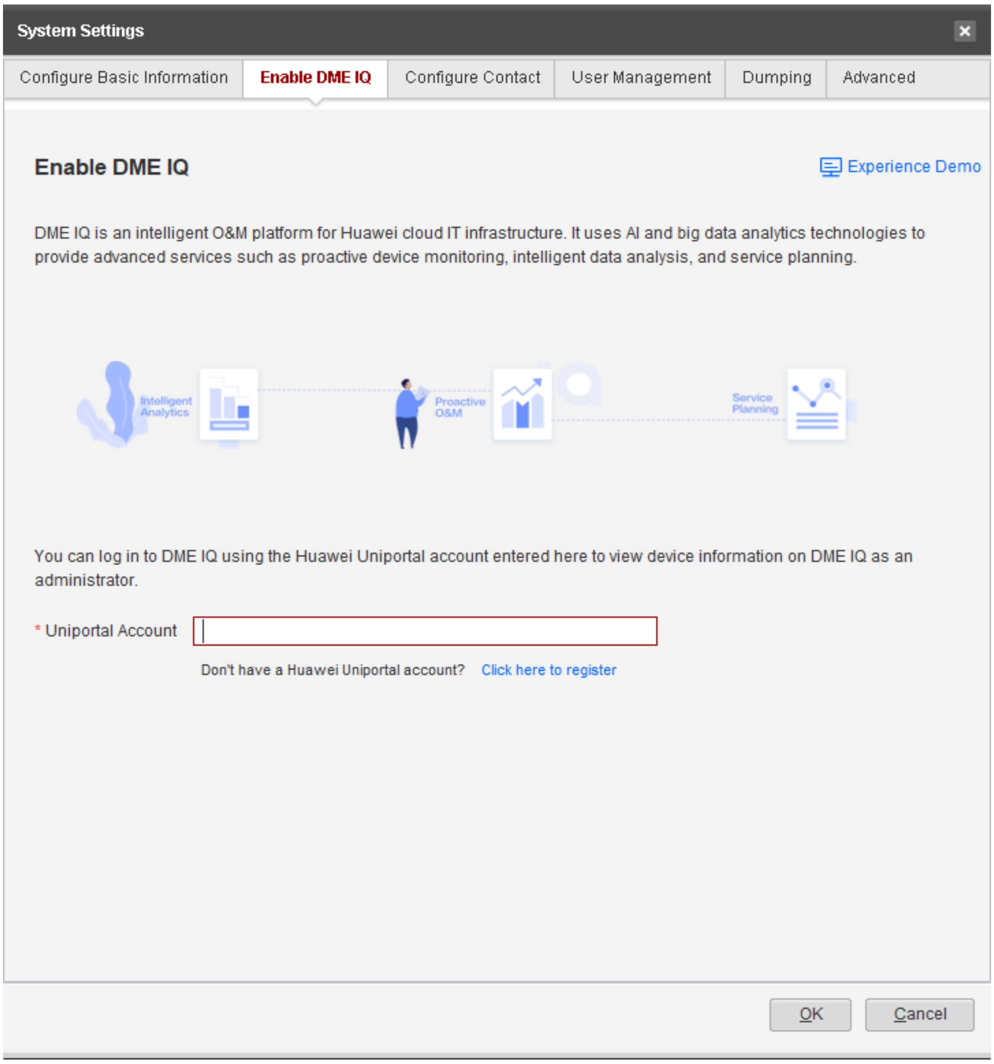
This section describes how to enable DME IQ. After enabling DME IQ, you can use the Uniportal account to log in to DME IQ and view device information on DME IQ as an administrator.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⚙. The **System Settings** dialog box is displayed.

Step 3 Click the **Enable DME IQ** tab.



Enable DME IQ

DME IQ is an intelligent O&M platform for Huawei cloud IT infrastructure. It uses AI and big data analytics technologies to provide advanced services such as proactive device monitoring, intelligent data analysis, and service planning.

You can log in to DME IQ using the Huawei Uniportal account entered here to view device information on DME IQ as an administrator.

* Uniportal Account

Don't have a Huawei Uniportal account? Click here to register

Step 4 **Optional:** Enter the Uniportal account used for logging in to DME IQ.

If you do not have a Uniportal account, click **Click here to register**, register an account, and then enter the account.

You can also click **Experience Demo** in the upper right corner to access and experience the DME IQ Demo.

Step 5 Click **OK**.

----End

4.5.3 Configuring Contact Information

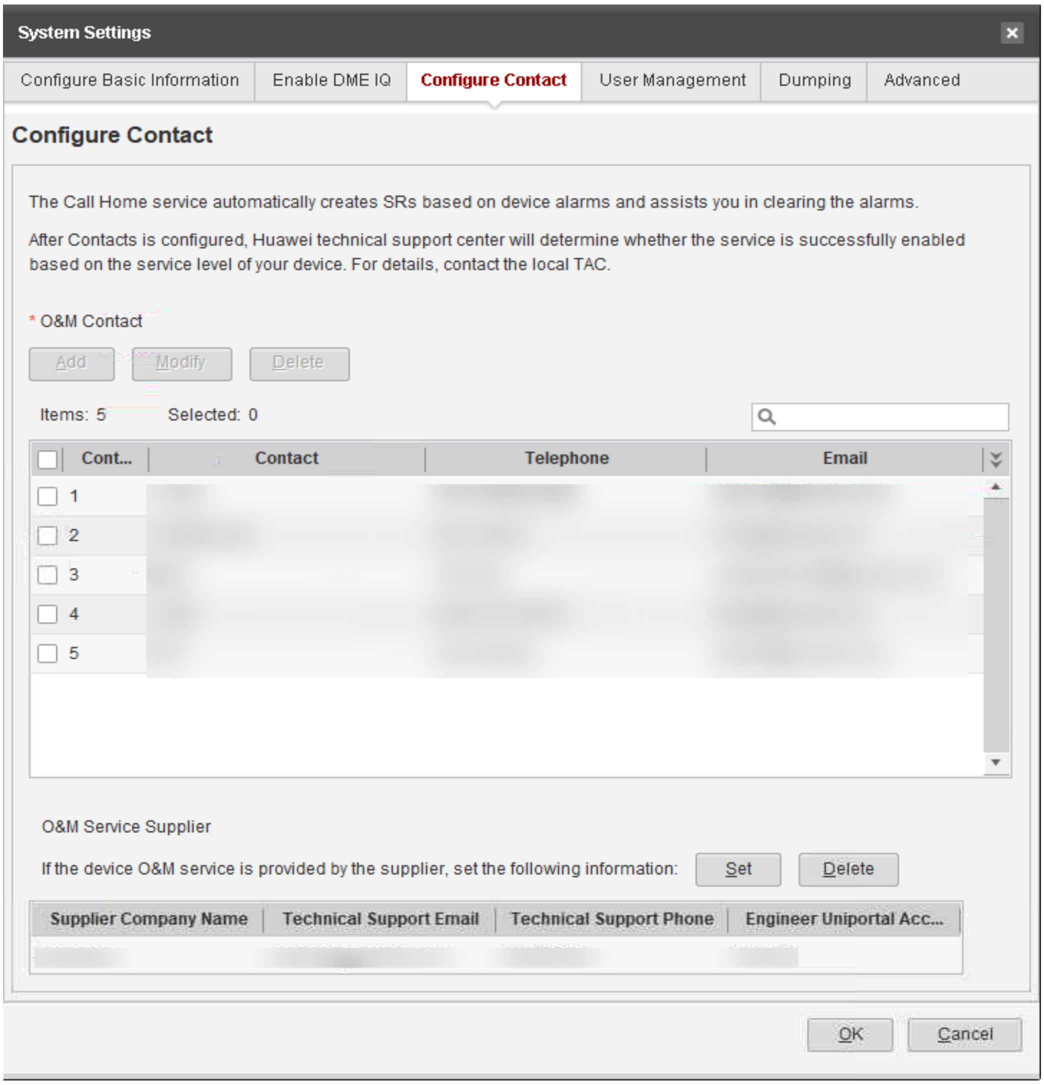
The Call Home service automatically creates service requests (SRs) based on device alarms and helps you clear alarms. To use this function, you need to configure O&M contact information.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⚙. The **System Settings** dialog box is displayed.

Step 3 Click the **Configure Contact** tab.



Configure Contact

The Call Home service automatically creates SRs based on device alarms and assists you in clearing the alarms.

After Contacts is configured, Huawei technical support center will determine whether the service is successfully enabled based on the service level of your device. For details, contact the local TAC.

* O&M Contact

Items: 5 Selected: 0

	Cont...	Contact	Telephone	Email
□	1	[redacted]	[redacted]	[redacted]
□	2	[redacted]	[redacted]	[redacted]
□	3	[redacted]	[redacted]	[redacted]
□	4	[redacted]	[redacted]	[redacted]
□	5	[redacted]	[redacted]	[redacted]

O&M Service Supplier

If the device O&M service is provided by the supplier, set the following information:

Supplier Company Name	Technical Support Email	Technical Support Phone	Engineer Uniportal Acc...
[redacted]	[redacted]	[redacted]	[redacted]

Step 4 Configure O&M contacts.

- Adding an O&M contact
  a. Click **Add**. The **Add O&M Contact** dialog box is displayed.
  b. Set the first name, last name, phone number, and email address of the contact.
  c. Click **OK**.

  NOTE

  The contact information configured here can be used by the DME IQ cloud system to contact you when the DME IQ Client detects a device fault.

- Modifying an O&M contact
  a. In the contact list, select the contact you want to modify.
  b. Click **Modify**.
  The **Modify O&M Contact** dialog box is displayed.

   c. Modify the contact No., phone number, and email address.
   d. Click **OK**.

- Deleting an O&M contact
   a. In the contact list, select the contact you want to delete.
   b. Click **Delete**.
      A dialog box is displayed, asking you whether to delete the contact.
   c. Click **OK**.

      NOTE

      The DME IQ Client requires that at least one contact be retained so that maintenance engineers can contact you. Do not delete all contacts.

Step 5 **Optional:** Configure the O&M service supplier.

If the customer type is set to **Enterprise customer** and the device O&M service is provided by a supplier, you need to set the O&M service supplier information.

1. Click **Set**. The **Set Supplier Information** window is displayed.
2. Select an access mode.
   - Supplier information
     Enter the supplier's partner company name, technical support email, technical support phone, and engineer Uniportal account.
   - Access key
     Enter the access key obtained from the partner portal of the DME IQ cloud system.
3. Click **OK**.

NOTE

To delete the supplier information, click **Delete** and confirm the operation as prompted.

Step 6 Click **OK**.

----End

4.5.4 Setting Log Dumping

This section describes how to set the dump directory of operation and run logs and the size of the dump directory.

Context

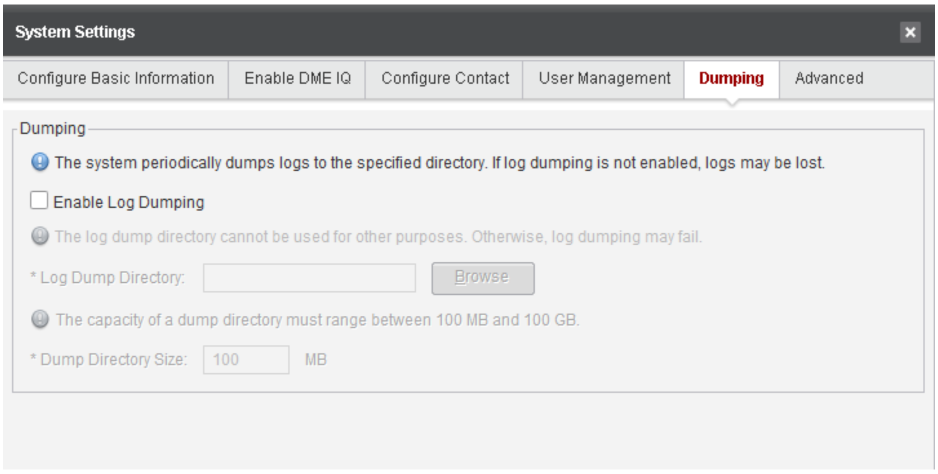
If you do not enable log dumping, historical logs will be cleared when the upper limit is reached. In this case, you cannot audit historical logs.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⚙. The **System Settings** dialog box is displayed.

Step 3 Click the **Dumping** tab.



Dumping

The system periodically dumps logs to the specified directory. If log dumping is not enabled, logs may be lost.

□ Enable Log Dumping

The log dump directory cannot be used for other purposes. Otherwise, log dumping may fail.

* Log Dump Directory:

The capacity of a dump directory must range between 100 MB and 100 GB.

* Dump Directory Size: 100 MB

Step 4 Select **Enable Log Dumping**.

Step 5 Click **Browse**.

Select the directory to which logs are saved and enter a name for the dumped file. The system will periodically dump operation and run logs to the directory.

NOTE

- The directory for saving logs cannot contain subdirectories. Otherwise, a dialog box is displayed, asking you to change the directory and try again.
- If log dumping is not configured, the system will dump operation and run logs to *DME IQ Client installation directory***/tmp/log/***xxx*. After log dumping is configured, logs in the directory will be dumped to the specified directory in the next dumping period.

Step 6 Set **Dump Directory Size** to restrict the total size of dumped logs.

NOTE

- The value of **Dump Directory Size** ranges from 100 MB to 100 GB.
- After log dumping is enabled, you are advised to manually dump logs for backup periodically and control the read/write permissions of the dumped logs.

----End

4.5.5 Setting Advanced Properties

Through the advanced settings, you can set the DME IQ Client login password and secure mailbox, enable/disable **Background Services**, handle timeout, export logs, and manage certificates.

Context

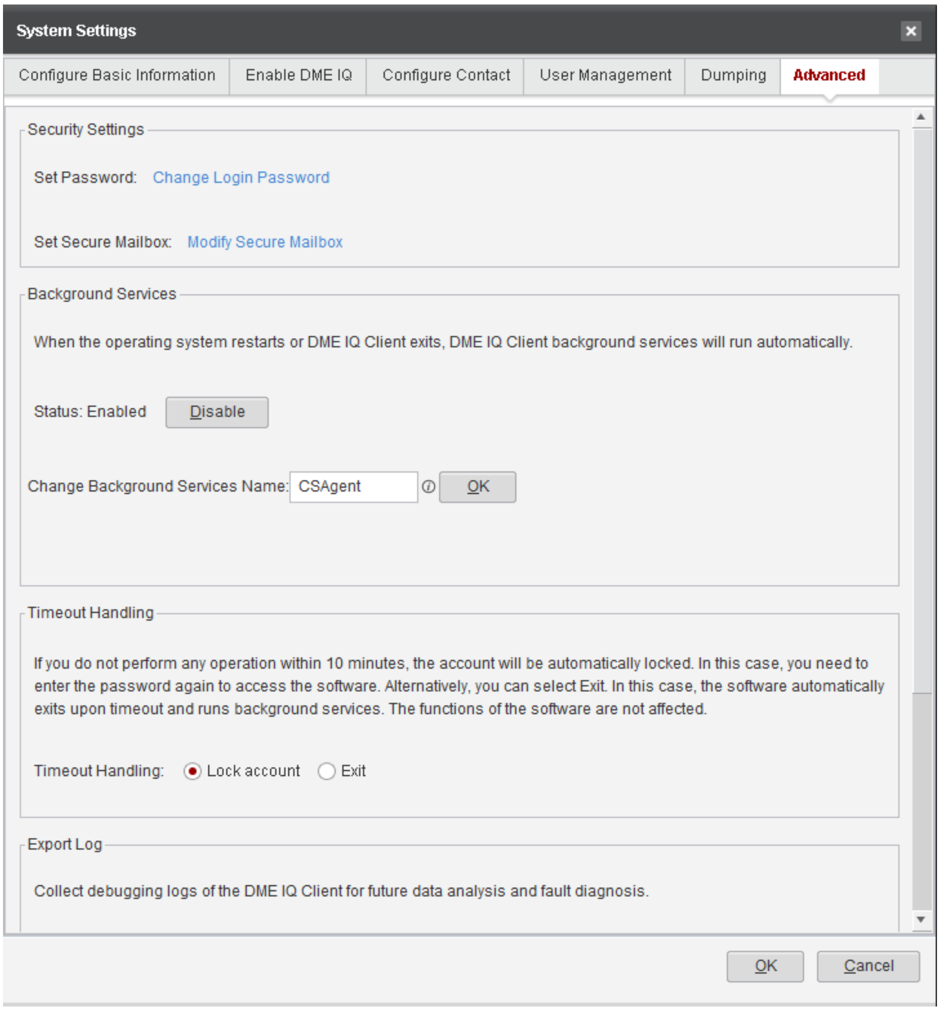
- The password validity period is six months. You need to change a password before it expires.
- The status of **Background Services** is **Enabled** by default.

Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⚙. The **System Settings** dialog box is displayed.

Step 3 Click the **Advanced** tab.



Security Settings

Set Password: Change Login Password

Set Secure Mailbox: Modify Secure Mailbox

Background Services

When the operating system restarts or DME IQ Client exits, DME IQ Client background services will run automatically.

Status: Enabled

Change Background Services Name: CSAgent

Timeout Handling

If you do not perform any operation within 10 minutes, the account will be automatically locked. In this case, you need to enter the password again to access the software. Alternatively, you can select Exit. In this case, the software automatically exits upon timeout and runs background services. The functions of the software are not affected.

Timeout Handling: ● Lock account ○ Exit

Export Log

Collect debugging logs of the DME IQ Client for future data analysis and fault diagnosis.

Step 4 Perform security settings.

You can change the password and secure mailbox of the current login user.

1. Click **Change Login Password**.

   The **Reset Password** dialog box is displayed. Specify **Old Password**, **New Password**, and **Confirm Password** to change the login password.

   NOTE

   - The new password must contain 8 to 32 characters including uppercase letters, lowercase letters, and special characters. The password cannot be set to a weak password, such as **Huawei@123** or **Admin@123**.
   - The new password must be different from any of the five recently used passwords.
   - The password validity period is six months. Change the password periodically.

2. Click **Modify Secure Mailbox**.

The **Modify Secure Mailbox** dialog box is displayed. Specify **Login Password** and **New Secure Mailbox**, and then click **OK**.

Step 5 Configure **Background Services**.

1. Enable/Disable **Background Services**.
   - Enable **Background Services**.

     When the status of **Background Services** is **Disabled**, you can enable it. You are advised to enable **Background Services**.

     i. In the **Background Services** area, click **Enable**.

     NOTE

     ○ If you fail to enable it, exit the DME IQ Client, go to its installation directory, right-click **dmeIq.exe**, and choose **Run as administrator** from the shortcut menu to start the software. Then, choose **System Settings** > **Advanced** and enable **Background Services**.

     ○ If you still fail to enable it after running the DME IQ Client as an administrator, exit the DME IQ Client, log in to the Windows operating system as user **Administrator**, go to its installation directory, right-click **dmeIq.exe**, and choose **Run as administrator** from the shortcut menu to start the software. Then, choose **System Settings** > **Advanced** and enable **Background Services**.

     ii. Click **OK**.
   - Disable **Background Services**.

     When the status of **Background Services** is **Enabled**, you can disable it.

     i. Click **Disable**.

     The **Warning** dialog box is displayed.

     ii. Confirm your operation as prompted.

     iii. After it is successfully disabled, click **OK**.
2. Change the background services name.

   By default, the DME IQ Client uses **CSAgent** as the background services name. If the name is in use, you are advised to change it to ensure the normal running of the background services.

   Enter a new name, click **OK**, and confirm your operation as prompted.

Step 6 Set timeout handling.

In the **Timeout Handling** area, select **Lock account** or **Exit**.

- If **Lock account** is selected and no operation is performed for more than 10 minutes, the software automatically locks the account. In this case, you need to enter the password again to access the software.
- If **Exit** is selected, the software automatically exits and runs background services after the timeout.

Step 7 Export logs.

You can collect debugging logs of the DME IQ Client for subsequent data analysis and fault locating.

1. In the **Export Log** area, click **Export**.

2. In the displayed **Export Log** dialog box, set the log file name and save path.

Step 8 Manage certificates.

1. Click **Import Certificate**.

   In the **Import Certificate** dialog box that is displayed, select the certificate to be imported and click **Open** to import the certificate.

   NOTE

   - Import an HTTPS server root certificate for verifying a device or system to prevent the device or system from being forged.
   - When importing vCenter root certificates, you need to place all the vCenter root certificates to be added to a .pem file named **vcenterCaCerts.pem**.

2. Click **Import CRL**.

   In the **Import CRL** dialog box that is displayed, select the CRL to be imported and click **Open** to import the CRL.

   NOTE

   Import a CRL for checking whether the HTTPS server certificate of a device or system has been revoked to prevent the device or system from being forged.

3. **Optional:** Configure the number of remaining days before password expiration to display a reminder and the certificate verification period.

   - Number of remaining days before password expiration to display a reminder

     Open the **configuration\certificateCfg.properties** file in the local installation directory of the DME IQ Client and configure the **client.import.cert.prompt.expiring.advance.days** parameter.

     The value ranges from 7 to 180 (days). If the value is not within the valid range or is incorrectly configured, the default value 90 is used.

   - Certificate verification period

     Open the **configuration\certificateCfg.properties** file in the local installation directory of the DME IQ Client and configure the **client.import.cert.check.interval.days** parameter.

     The value ranges from 1 to 14 (days). If the value is not within the valid range or is incorrectly configured, the default value 7 is used.

   NOTE

   The number of remaining days before password expiration to display a reminder must be greater than the certificate verification period. Otherwise, the default values are used for both parameters.

Step 9 **Optional:** Update symmetric encryption keys.

- Immediate update
  a. Open the **cfg\manual.properties** file in the local installation directory of the DME IQ Client and change the value of **immediate.update.key.flag** to **0**.
  b. Run the DME IQ Client software again.
- Automatic update

a. Open the **config\mm\appConfig.properties** file in the local installation directory of the DME IQ Client and change the value of **auto_update_mk_enabled** to **true**.

b. Configure **crypt_key_lifetime_days** to specify the automatic update period. The value is an integer ranging from 1 to 180. If the parameter value *N* is specified, the key update period is (180 – *N*) days.

   If this parameter is not specified, the update period is 180 days by default.

c. Run the DME IQ Client software again.

----End

5 Related Operations

This chapter describes how to close, uninstall, and upgrade the DME IQ Client, as well as the file clearing function.

5.1 Upgrading the DME IQ Client

According to the configured communication mode, the DME IQ Client supports automatic upgrade and manual upgrade. Manual upgrade modes include online upgrade and offline upgrade.

5.1.1 Automatic Upgrade

You can set the automatic upgrade to automatically upgrade the DME IQ Client.

Prerequisites

The communication mode is set to **Internet (HTTPS)**.

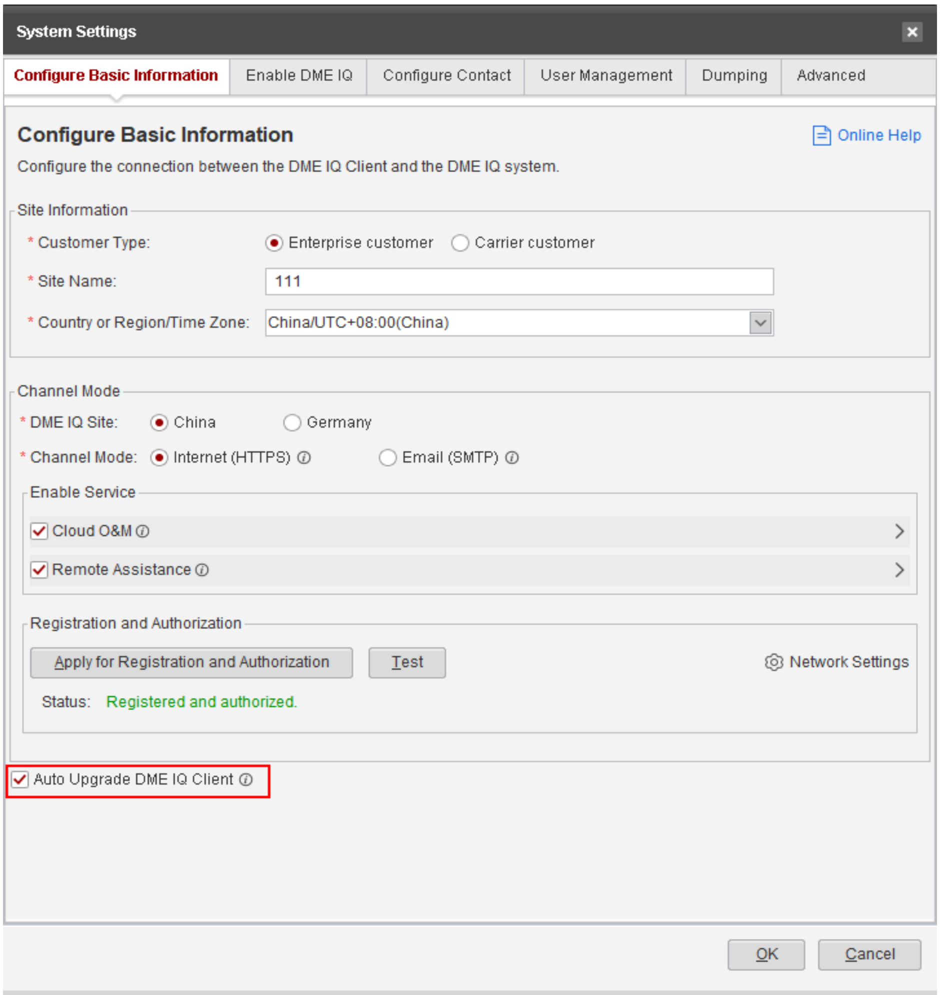
Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⚙. The **System Settings** page is displayed.

Step 3 Click the **Configure Basic Information** tab.

Step 4 Select **Auto Upgrade DME IQ Client**.



Configure Basic Information

Configure the connection between the DME IQ Client and the DME IQ system.

Site Information

* Customer Type: ● Enterprise customer ○ Carrier customer

* Site Name: 111

* Country or Region/Time Zone: China/UTC+08:00(China)

Channel Mode

* DME IQ Site: ● China ○ Germany

* Channel Mode: ● Internet (HTTPS) ○ Email (SMTP)

Enable Service

☑ Cloud O&M

☑ Remote Assistance

Registration and Authorization

Status: Registered and authorized.

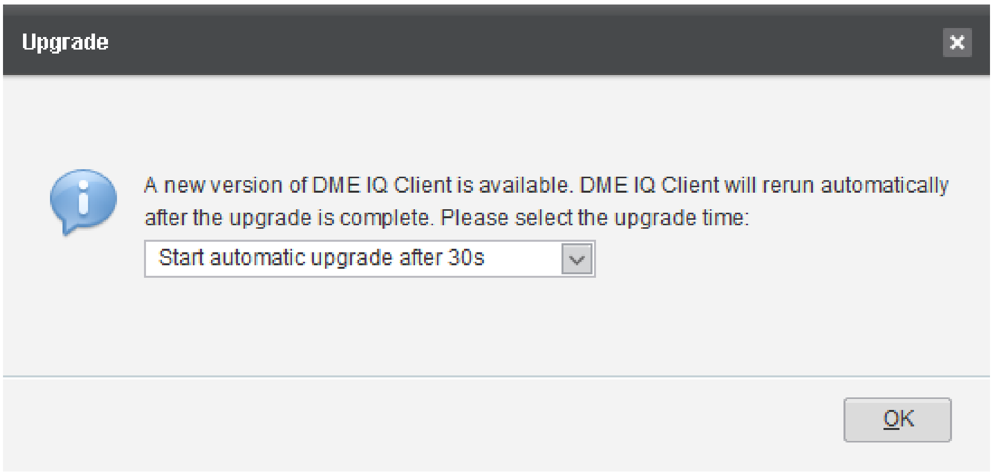
☑ Auto Upgrade DME IQ Client

Step 5 After this option is selected, the latest software (or components) of the DME IQ Client will be automatically downloaded from the DME IQ cloud system and installed.

----End

Follow-up Procedure

1. When a new DME IQ Client version is available, the **Upgrade** dialog box will be displayed.



A new version of DME IQ Client is available. DME IQ Client will rerun automatically after the upgrade is complete. Please select the upgrade time:

Start automatic upgrade after 30s

2. Select the upgrade time according to actual situations.

   The options are as follows:

   - Start automatic upgrade after 30s
   - Delay the upgrade for 5 minutes
   - Delay the upgrade for 1 hour
   - Delay the upgrade for 4 hours

3. Click **OK** to enable automatic upgrade.

5.1.2 Manual Upgrade

Manual upgrade modes include online upgrade and offline upgrade.

5.1.2.1 Online Upgrade

This section describes how to upgrade the DME IQ Client online.

Context

When the communication mode is set to **Internet (HTTPS)**, online upgrade can be used.

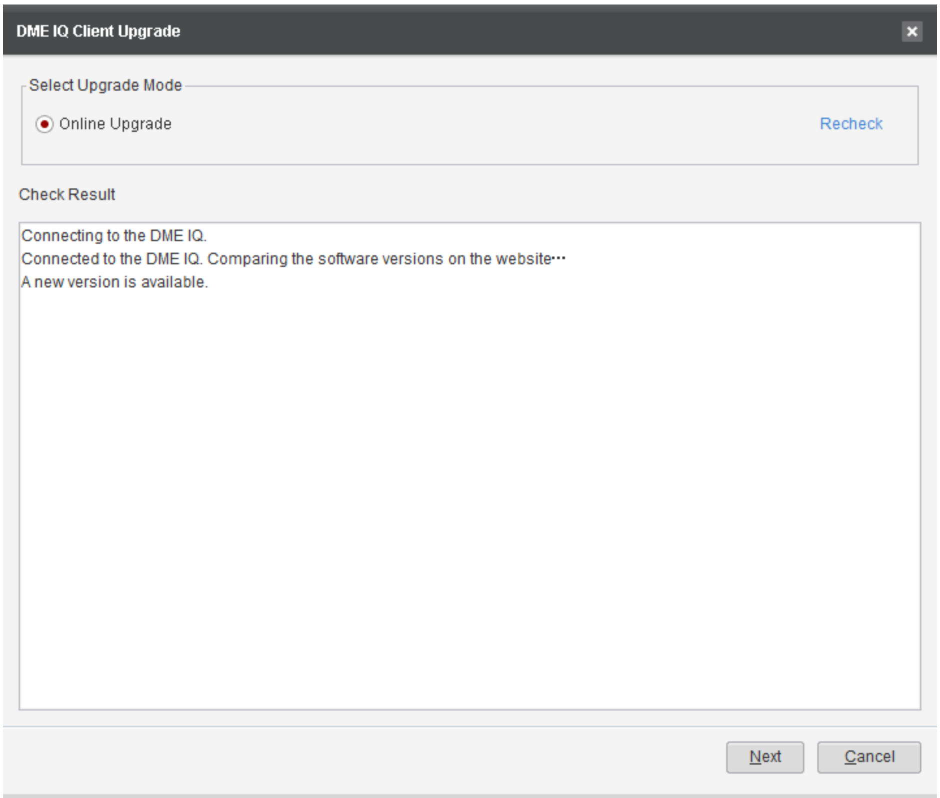
Procedure

Step 1 Log in to the DME IQ Client.

Step 2 Click ⓘ.

The DME IQ Client upgrade page is displayed.

Copyright © Huawei Technologies Co., Ltd.



Connecting to the DME IQ.
Connected to the DME IQ. Comparing the software versions on the website···
A new version is available.

Step 3 Select **Online Upgrade**.

The system will automatically check whether a new software version is available on the cloud system website.

Step 4 If a new version is available, click **Next**. The page for upgrading the DME IQ Client is displayed.

The system automatically obtains the current version number and release date of the DME IQ Client, as well as the version number, release date, and new features of the latest version on the server.

Step 5 Click **Upgrade**.

The system automatically downloads the upgrade package. After the download is complete, click **OK**. The system automatically completes the upgrade.

----End

5.1.2.2 Offline Upgrade

If the communication mode is set to **Internet (HTTPS)** or **Email (SMTP)**, you can upgrade the DME IQ Client offline.

For details about the offline upgrade procedure, see the *Upgrade Guide*.

5.2 Closing the DME IQ Client

This section describes how to minimize or exit the DME IQ Client.

Procedure

- Minimize the DME IQ Client.
  a. In the main window of the DME IQ Client, click × in the upper right corner.

     The **Information** dialog box is displayed.

  b. Click **OK**.

     The DME IQ Client is minimized to the system tray.

     NOTE

     You can right-click the icon in the system tray and choose **Show Window** from the shortcut menu that is displayed to go to the DME IQ Client main window.

- Exit the DME IQ Client.

  Right-click the icon in the system tray and choose **Exit** from the shortcut menu that is displayed to exit the DME IQ Client.

  NOTE

  After you exit the DME IQ Client, if **Background Services** are enabled, the DME IQ Client will run in the background. To exit the DME IQ Client completely, choose **System Settings** > **Advanced** and disable **Background Services**.

5.3 Uninstalling the DME IQ Client

This section describes how to uninstall the DME IQ Client when it is no longer used or needs to be reinstalled.

Prerequisites

Before uninstalling the DME IQ Client, right-click the icon in the system tray and choose **Exit** from the shortcut menu to stop the DME IQ Client.

Procedure

Step 1 Go to the installation directory of the DME IQ Client.

Step 2 Double-click **uninst.exe**.

Confirm your operation as prompted.

Step 3 On the displayed page indicating the uninstallation success, click **Finish**.

The DME IQ Client is uninstalled.

NOTE

- If users withdraw their consent to the DME IQ Client processing their personal data, uninstall the DME IQ Client and delete local data. Then, contact the DME IQ cloud system to withdraw the authorization letter of DME IQ.
- If the DME IQ Client needs to be upgraded to a new version and the configured data needs to be reserved, you are advised not to uninstall the DME IQ Client of the current version.

----End

5.4 Clearing Files

The DME IQ Client automatically clears inspection reports, performance files, and log files.

The DME IQ Client checks the disk space every day and clears the files using specified policies based on the time sequence of file generation, as shown in **Table 5-1** and **Table 5-2**.

Table 5-1 Clearing policy for inspection reports and log files specific to file generation time

X (Days) After File Generation	Policy
X > 90	Automatic file clearing
3 < X ≤ 90	See **Table 5-3**.
X ≤ 3	No file clearing

Table 5-2 Clearing policy for performance files specific to file generation time

X (Days) After File Generation	Policy
X > 30	Automatic file clearing
3 < X ≤ 30	See **Table 5-3**.
X ≤ 3	No file clearing

Inspection reports, performance files, and log files are generated by plug-ins of their respective domains. The DME IQ Client clears files based on plug-in types. The available space of the disk where the DME IQ Client is installed may affect the running of the DME IQ Client. Therefore, when the disk space is greater than or equal to 5 GB, the disk space that can be occupied by plug-ins is different, as shown in **Table 5-3**.

Table 5-3 Clearing policy based on the file size

Plug-in Type	Maximum Space That Can Be Occupied (Available Space of Disk Where DME IQ Client Is Installed > 5 GB)	Maximum Space That Can Be Occupied (Available Space of Disk Where DME IQ Client Is Installed ≤ 5 GB)
Plug-in for collecting storage performance	200 MB	100 MB
Plug-in for collecting storage inspection reports and logs	2 GB	500 MB
Plug-in for collecting cloud computing inspection reports and logs	1 GB	300 MB
Plug-in for collecting server inspection reports and logs	1 GB	300 MB

A Related Services and Processes

This section describes the services and processes related to the DME IQ Client when it is running.

NOTICE

Do not shut down the services and processes listed in **Table A-1**. Otherwise, the running of the DME IQ Client may be affected.

If the automatic startup function of the DME IQ Client is enabled, you can view the DME IQ Client services and processes listed in **Table A-1** by starting the task manager when the DME IQ Client is running.

Table A-1 Services and processes

Category	Name	Description
Service	CSAgent	Background services of the DME IQ Client, corresponding to the **prunsrv.exe** process. To change the background services name, choose **System Settings** > **Advanced**.

Category	Name	Description
	cswatchdog	Watchdog service, corresponding to the **watchdog.exe** process. It is used to monitor the running status of the DME IQ Client process **dmeiq.exe** in real time so that the DME IQ Client can report device alarms to the DME IQ cloud system in real time. After a user exits the DME IQ Client foreground process **dmeiq.exe**, the watchdog service will automatically start the CSAgent service and run the DME IQ Client background process **prunsrv.exe**. If the watchdog service detects that the CSAgent service does not exist, it will register and then start the CSAgent service, and run the **prunsrv.exe** process.
Process	dmeiq.exe	Foreground process of the DME IQ Client.
	prunsrv.exe	Process corresponding to the DME IQ Client background services CSAgent.
	watchdog.exe	DME IQ Client watchdog process, used to monitor the DME IQ Client running status and automatically start the DME IQ Client background services when the foreground service is stopped.

B Technical Specifications

This section describes the deployment environment requirements, specifications, and supported device and interconnected system models and versions of the DME IQ Client.

B.1 Specifications

Table B-1 lists the specifications of the DME IQ Client.

Table B-1 Specifications

Category	Item	Description	Remarks
General specifications	Managed device	● A maximum of 256 storage devices are supported. ● A maximum of 256 network devices are supported. ● A maximum of 5000 servers are supported. ● A maximum of 10 vCenter devices (a maximum of 1000 VMs in total) are supported. ● A maximum of one FusionCare system is supported. ● A maximum of 20 FusionCube Vision Pro/FusionCube Vision systems are supported. ● A maximum of one FusionDirector system is supported. ● A maximum of one ManageOne system is supported. ● A maximum of 2 FusionCompute systems (a maximum of 500 VMs in total) are supported.	The maximum number of devices is for reference only and subject to the service load and device status.
	O&M contact	A maximum of five contacts can be added, and at least one contact is a security administrator.	The email address of the security administrator is used to retrieve the password.

Category	Item	Description	Remarks
	Operation log	The logs can be saved for one year at most.	If the dumping function is enabled, logs are automatically dumped after the preset upper limit is reached.
	Run log	A maximum of 3000 logs can be saved at most.	If the dumping function is enabled, logs are automatically dumped after the preset upper limit is reached.
	Message log	A maximum of 3000 logs can be saved at most.	If the dumping function is enabled, logs are automatically dumped after the preset upper limit is reached.
	Size of uploaded files that can be retained	A maximum of 1 GB latest uploaded files can be retained.	If the disk space is less than 2 GB, the size of data that can be retained is less than 1 GB.
	Password validity period	6 months	-
Alarm reporting (email channel)	Supported protocol	SNMPv2c/v3 is supported.	SNMPv3 is recommended.
	Severity of alarms that need to be reported	Critical, major, minor, and warning alarms and related recovery alarms	Events are not reported.
	Alarm reporting method	Email	Alarm emails include the device serial number (SN) and alarm information.

Category	Item	Description	Remarks
	Recipient email address	● In the Chinese mainland: – Technical support center for enterprises: cloudservice@huawei.com – Technical support center for carriers: cs.alarm.cn@huawei.com ● Outside the Chinese mainland: – Technical support center for enterprises: Romania: rocloudservice@huawei.com Russia: esruentmail@huawei.com – Technical support center for carriers: Romania: romaniacs@huawei.com Mexico: mexicocs@huawei.com Russia: russiacs@huawei.com	-
	Reporting frequency	● The first received device alarm will be delayed by up to 30 seconds. ● The interval between two alarm reporting emails must be at least 5 minutes.	-

Category	Item	Description	Remarks
	Periodic handshake with the DME IQ cloud system	By default, handshake emails are sent every two hours.	-
Alarm reporting (Internet channel)	Supported protocol	SNMPv2c/v3 is supported.	SNMPv3 is recommended.
	Severity of alarms that need to be reported	Critical, major, minor, and warning alarms and related recovery alarms	Events are not reported.
	Alarm reporting method	HTTPS request	HTTPS requests include the device serial number (SN) and alarm information.

Category	Item	Description	Remarks
	Recipient email address	● In the Chinese mainland: – Technical support center for enterprises: https://ecloudservice-cn.huawei.com – Technical support center for carriers: https://icloudservice-cn.huawei.com ● Outside the Chinese mainland: – Technical support center for enterprises: Romania: https://itr-eservicero-ent.huawei.com Russia: https://enterpriseru.eservice.huawei.com – Technical support center for carriers: Romania: https://itr-eservicero-carrier.huawei.com Mexico: https://itr-eservicemx-carrier.huawei.com Russia: https://carrierru.eservice.huawei.com	-
	Reporting frequency	Sent with handshake requests	-

Category	Item	Description	Remarks
	Periodic handshake with the DME IQ cloud system	Every 30 seconds	-

Category	Item	Description	Remarks
File uploading (email channel)	File size	Less than or equal to 10 MB	● In the Chinese mainland: – Technical support center for enterprises: cloudservice@huawei.com cloudservice-file@huawei.com eservicecn-ent-file1@huawei.com eservicecn-ent-file2@huawei.com – Technical support center for carriers: cs.alarm.cn@huawei.com cs.alarm.cn-file@huawei.com eservicecn-carrier-file1@huawei.com eservicecn-carrier-file2@huawei.com ● Outside the Chinese mainland: – Technical support center for enterprises: Romania: rocloudservice@huawei.com rocloudservice-file@huawei.com eservicero-ent-file1@huawei.com eservicero-ent-file2@huawei.com Russia: esruentmail@huawei.com esruentfile1@huawei.com esruentfile2@huawei.com

Category	Item	Description	Remarks
			esruentfile3@huawei.com – Technical support center for carriers: Romania: romaniacs@huawei.com romaniacs-file@huawei.com eservicero-carrier-file1@huawei.com eservicero-carrier-file2@huawei.com Russia: russiacs@huawei.com russiacs-file@huawei.com eservice-ru-carrier-file1@huawei.com eservice-ru-carrier-file2@huawei.com Mexico: mexicocs@huawei.com mexicocs-file@huawei.com eservicemx-carrier-file1@huawei.com eservicemx-carrier-file2@huawei.com
File uploading (Internet channel)	File size	Less than or equal to 1 GB	Files include alarm, performance, configuration, and disk information files.

B.2 Supported Storage Devices

Table B-2 lists the storage device models and versions supported by the DME IQ Client.

Table B-2 Supported storage devices

Storage Device Model	Version	Supported Services
OceanStor S2200T	V100R005C00 V100R005C01 V100R005C02 V100R005C30	Alarm reporting, remote inspection, and remote log collection
OceanStor S2600T	V100R002C01 V100R005C00 V100R005C01 V100R005C02 V100R005C30 V200R001 V200R002C00 V200R002C30 V200R003C00	Alarm reporting, remote inspection, and remote log collection
OceanStor S5500T/ S5600T/ S5800T/S6800T	V100R002C00 V100R005C00 V100R005C01 V100R005C02 V100R005C30 V200R001 V200R002C00 V200R002C10 V200R002C20 V200R002C30 V200R003C00	Alarm reporting, remote inspection, and remote log collection
OceanStor 18500/18800/18800F	V100R001C00 V100R001C10 V100R001C20 V100R001C30	Alarm reporting, remote inspection, and remote log collection

Storage Device Model	Version	Supported Services
OceanStor 18500 V3/18800 V3	V300R003C00 V300R003C10 V300R003C20 V300R006C00 V300R006C10 V300R006C20 V300R006C30 V300R006C50 V300R006C60	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2100 V3	V300R006C20 V300R006C30 V300R006C50 V300R006C60	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2200 V3	V300R005C00 V300R006C00 V300R006C10 V300R006C20 V300R006C30 V300R006C50 V300R006C60	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2600 V3	V300R005C00 V300R006C00 V300R006C10 V300R006C20 V300R006C30 V300R006C50 V300R006C60 V300R006C61	Alarm reporting, remote inspection, remote log collection, and historical performance data collection

Storage Device Model	Version	Supported Services
OceanStor 2800 V3	V300R001C00 V300R003C00 V300R003C20 V300R006C00 V300R006C10 V300R006C20 V300R006C30 V300R006C50 V300R006C60	Alarm reporting, remote inspection, remote log collection, and historical performance data collection (V300R002C00 and later versions)
OceanStor 2200 V3 Enhanced/2600 V3 Enhanced/2600F V3 Enhanced	V300R006C20 V300R006C50	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 6900 V3	V300R001C10 V300R001C20	Alarm reporting, remote inspection, and remote log collection
OceanStor 5300 V3/5500 V3	V300R001C10 V300R001C20 V300R002C00 V300R002C10 V300R003C00 V300R003C10 V300R003C20 V300R006C00 V300R006C10 V300R006C20 V300R006C30 V300R006C50 V300R006C60	Alarm reporting, remote inspection, remote log collection, and historical performance data collection (V300R002C00 and later versions)

Storage Device Model	Version	Supported Services
OceanStor 5600 V3/5800 V3/6800 V3	V300R001C00 V300R001C10 V300R001C20 V300R002C00 V300R002C10 V300R003C00 V300R003C10 V300R003C20 V300R006C00 V300R006C10 V300R006C20 V300R006C30 V300R006C50 V300R006C60	Alarm reporting, remote inspection, remote log collection, and historical performance data collection (V300R002C00 and later versions)
OceanStor 2600F V3/5500F V3/5600F V3/5800F V3/6800F V3/18500F V3/18800F V3	V300R006C00 V300R006C10 V300R006C20 V300R006C30 V300R006C50 V300R006C60	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2800 V5/5300 V5/5500 V5/5600 V5/5800 V5/6800 V5/18500 V5/18800 V5/5300F V5/5500F V5/5600F V5/5800F V5/6800F V5/18500F V5/18800F V5	V500R007C00 V500R007C10 V500R007C20 V500R007C30 V500R007C50 V500R007C60 V500R007C61	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 5110 V5/5110F V5/5210 V5/5210F V5	V500R007C30 V500R007C60 V500R007C61	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 5300 V5 Enhanced	V500R007C10 V500R007C30	Alarm reporting, remote inspection, remote log collection, and historical performance data collection

Storage Device Model	Version	Supported Services
OceanStor 2810 V5/5310 V5/5510 V5/5610 V5/5810 V5/6810 V5/18510 V5/18810 V5/5310F V5/5510F V5/5610F V5/5810F V5/6810F V5/18510F V5/18810F V5/5500K V5	V500R007C60 Kunpeng V500R007C70 Kunpeng	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 5100K V5/5200K V5	V500R007C61	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 5300K V5	V500R007C70 Kunpeng	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2600 V5/5110 V5 Enhanced/5210 V5 Enhanced/5210F V5 Enhanced	V500R007C71 Kunpeng	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2810 V5/5210 V5 Enhanced/5310 V5	V500R007C72 Kunpeng	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2210 V5/2810 V5/5110 V5 Enhanced/5210 V5 Enhanced/5310 V5/5510 V5/5810 V5/6810 V5/18510F V5	V500R007C73 Kunpeng	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 2220/5120 V5/5220 V5	V500R007C73 Kunpeng	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor 5310/5510/5610/6810/18510/18810	6.1.3 6.1.5 6.1.6	Alarm reporting, remote inspection, remote upgrade, remote log collection, and historical performance data collection

Storage Device Model	Version	Supported Services
OceanStor 2220/2620/2200/2600	6.1.6	Alarm reporting, remote inspection, and remote log collection
OceanStor Dorado2100 G2	V100R001C00	Alarm reporting, remote inspection, and remote log collection
OceanStor Dorado18000 V3	V300R001C30 V300R002C00 V300R002C10 V300R002C20	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor Dorado6000 V3	V300R001C00 V300R001C01 V300R001C20 V300R001C21 V300R001C30 V300R002C00 V300R002C10 V300R002C20	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor Dorado5000 V3	V300R001C01 V300R001C20 V300R001C21 V300R001C30 V300R002C00 V300R002C10 V300R002C20	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor Dorado3000 V3	V300R002C10 V300R002C20	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanStor Dorado NAS	V300R002C10 V300R002C20	Alarm reporting, remote inspection, remote log collection, and historical performance data collection

Storage Device Model	Version	Supported Services
OceanStor Dorado 3000 V6/Dorado 5000 V6/Dorado 6000 V6/ Dorado 8000 V6/ Dorado 18000 V6	6.0.0 6.0.1 6.1.0 6.1.2 6.1.3 6.1.5 6.1.6	Alarm reporting, remote inspection, remote upgrade, remote log collection, and historical performance data collection
OceanStor Dorado 2000	6.1.5 6.1.6	Alarm reporting, remote inspection, remote upgrade, remote log collection, and historical performance data collection
OceanDisk 1300/1500	1.0.0 1.1.0	Alarm reporting, remote inspection, remote upgrade, remote log collection, and historical performance data collection
OceanDisk 1600/1500T/1600T	1.1.0	Alarm reporting, remote inspection, remote upgrade, remote log collection, and historical performance data collection
OceanProtect X8000/ X9000/A8000	1.0.0 1.1.0 1.2.0 1.3.0	Alarm reporting, remote inspection, remote log collection, and historical performance data collection
OceanProtect X6000	1.1.0 1.2.0 1.3.0	Alarm reporting, remote inspection, remote upgrade, remote log collection, and historical performance data collection
OceanProtect X3000	1.3.0	Alarm reporting, remote inspection, remote upgrade, remote log collection, and historical performance data collection
OceanCyber	1.0.0	Alarm reporting

Storage Device Model	Version	Supported Services
OceanStor 9000	V300R005C00 V300R006C00 V300R006C10 V300R006C20 7.0	Alarm reporting, remote inspection, and remote log collection
OceanStor 9500/ OceanStor 9000-K	7.1	Alarm reporting, remote inspection, and remote log collection
OceanStor UDS	V300R003C00	Alarm reporting, remote inspection, and remote log collection
FusionStorage Object	V100R006C10 V100R006C20	Alarm reporting, remote inspection, and remote log collection
FusionStorage OBS	7.0 8.0	Alarm reporting, remote inspection, and remote log collection
FusionStorage File	7.0	Alarm reporting, remote inspection, and remote log collection
FusionStorage Block	V100R006C30	Alarm reporting
FusionStorage	8.0	Alarm reporting, remote inspection, and remote log collection
OceanStor 100D	8.0	Alarm reporting, remote inspection, and remote log collection
OceanStor Pacific 9520/9540/9550/9920/9950	8.1	Alarm reporting, remote inspection, and remote log collection
OceanStor Pacific 9140/9146	8.1.5	Alarm reporting, remote inspection, and remote log collection
Data Turbo 6000	1.0.0	Alarm reporting, remote inspection, and remote log collection

B.3 Supported Servers

Table B-3 lists the server models and versions supported by the DME IQ Client.

Table B-3 Supported servers

Server Type	Model	Management Software Version	Supported Services
Rack server	RH1288 V3/ RH2288 V3/ RH2288H V3/ RH5885 V3/ RH5885H V3/ RH8100 V3/5288 V3 1288H V5/2288H V5/5288 V5/2488 V5/2488H V5/5885H V5/8100 V5/5288X V5	iBMC 2.30 or later	Alarm reporting, remote inspection, and remote log collection
High-density server	X6000 V3(XH321 V3)/X6800 V3(XH628 V3/ XH622 V3/XH620 V3) X6000 V5(XH321 V5)	iBMC 2.30 or later	Alarm reporting, remote inspection, and remote log collection
Blade server	E9000	MM910 2.10 or later	Alarm reporting, remote inspection, and remote log collection
KunLun server	9008/9016/9032/9032L	CMC 3.62 or later	Alarm reporting
	9008L	CMC 3.80 or later	Alarm reporting
Heterogeneous server	G530/G560/ G2500/G5500	iBMC 2.30 or later	Alarm reporting, remote inspection, and remote log collection

Server Type	Model	Management Software Version	Supported Services
TaiShan server	TaiShan 2280/ TaiShan 5280/ TaiShan X6000/ TS100-2280K TS200-1280/ TS200-2180/ TS200-2180K/ TS200-2280/ TS200-2280E/ TS200-2280K/ TS200-2480/ TS200-2480K/ TS200-5180/ TS200-5280/ TS200-5280K/ TS200-5290/ TaiShan X6000 V2 TS200-Pro-1280/ TS200-Pro-2280/ TS200-Pro-2480	iBMC 2.30 or later	Alarm reporting, remote inspection, and remote log collection
Atlas	Atlas 800 9000	iBMC 2.30 or later	Alarm reporting, remote inspection, and remote log collection
	Atlas 900 PoD A2	iBMC 2.30 or later	Alarm reporting, remote inspection, remote log collection, and diagnosis information collection

B.4 Supported Network Devices

Table B-4 lists the network device models and versions supported by the DME IQ Client.

Table B-4 Supported network devices

Network Device Model	Version	Supported Services
CloudEngine 12800	V200R002C50	Alarm reporting
CloudEngine 6800	V200R002C50	Alarm reporting
CloudEngine 6863	V200R019C00	Alarm reporting
CloudEngine 6865	V200R019C00	Alarm reporting

Network Device Model	Version	Supported Services
CloudEngine 16804	V200R019C00	Alarm reporting
S7706	V200R010C00	Alarm reporting
S5720S-28P-LI-AC	V200R011C10	Alarm reporting

B.5 Supported Interconnected Systems

Table B-5 lists the interconnected systems supported by the DME IQ Client and their versions.

Table B-5 Supported interconnected systems

System Name	Version	Supported Services
ManageOne	6.3/6.5.0	Alarm reporting
	6.5.1	Alarm reporting, remote log collection, and remote O&M
	8.0 or later	Alarm reporting, remote log collection, and remote O&M
FusionDirector	FusionDirector 1.5.0 or later	Alarm reporting
FusionCare	V100R005C00SPC535 or later	Remote inspection and remote log collection
vCenter	6.0 or later	Performance data collection and diagnosis information collection
FusionCube Vision Pro	8.0 or later	Alarm reporting and remote log collection
FusionCube Vision	8.0.RC1 or later	Alarm reporting and remote log collection
FusionCompute	8.0 or later	Alarm reporting, performance data collection, and diagnosis information collection

C Configuring SNMP Parameters

This section describes how to configure SNMP parameters for servers and storage devices.

C.1 Configuring SNMP Parameters (for Storage Devices)

Table C-1 lists the SNMP versions and parameters of storage devices.

For OceanStor V300R003 and later versions, SNMPv3 parameters are configured and have no default values. The procedure for configuring SNMP parameters is as follows.

Creating an SNMP User on DeviceManager

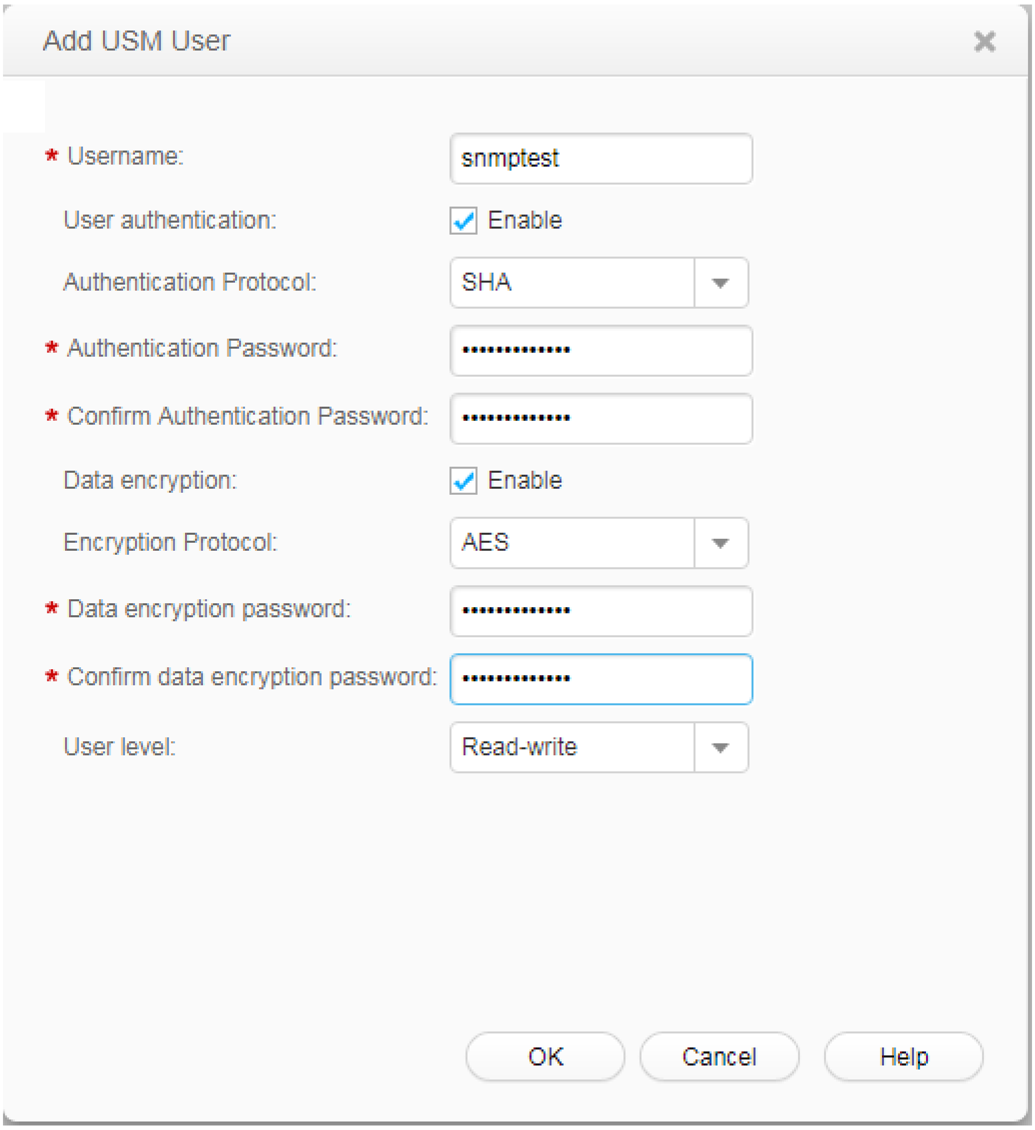
Step 1 Log in to DeviceManager and choose **Settings** > **Alarm Settings** > **USM User Management**.

NOTE

The entry to the **USM User Management** page may be different for different storage versions. For details, log in to DeviceManager and view the online help.

Step 2 Click **Add**. In the displayed dialog box as shown in **Figure C-1**, set **Authentication Protocol**, **Encryption Protocol**, **Username**, **Authentication Password**, and **Data encryption password**.

Figure C-1 Adding an SNMP user



* Username: snmptest

User authentication: ☑ Enable

Authentication Protocol: SHA

* Authentication Password: ••••••••••••••

* Confirm Authentication Password: ••••••••••••••

Data encryption: ☑ Enable

Encryption Protocol: AES

* Data encryption password: ••••••••••••••

* Confirm data encryption password: ••••••••••••••

User level: Read-write

NOTE

- In this example, an SNMP user is being created with **Username** set to **snmptest**, **Authentication Protocol** set to **SHA**, and **Encryption Protocol** set to **AES** for OceanStor Dorado V300R002C10.
- When adding an SNMP user, you must set **Authentication Password** and **Data encryption password** to different values.

Step 3 Click **OK** and then click **Save** to add an SNMP user.

----End

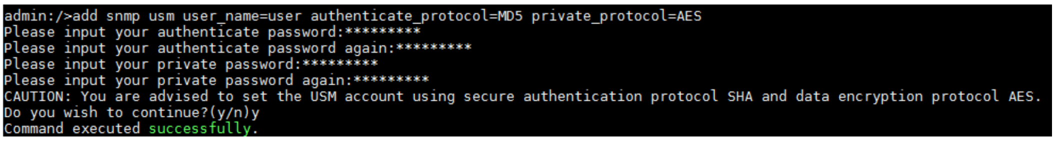
Creating an SNMP User in the CLI

Step 1 Log in to the CLI.

Step 2 Enter the **add snmp usm user_name=**_?_ **authenticate_protocol=**_?_ **private_protocol=**_?_ command.

Parameter	Description	Value
user_name=*?*	USM user name.	The value contains 4 to 32 ASCII characters, including digits, letters, underscores (_), or hyphens (-), and must start with a letter.
authenticate_protocol=*?*	Authentication protocol.	The value can be **MD5**, **SHA**, **SHA224**, **SHA256**, **SHA384**, **SHA512**, or **NONE**. **SHA** indicates the SHA1 protocol. To ensure the data security, you are advised to use **SHA512**.
private_protocol=*?*	Data encryption protocol.	The value can be **DES**, **AES**, **NONE**, **3DES**, **AES192**, or **AES256**. **AES** indicates the AES128 protocol. To ensure the data security, you are advised to use **AES256**.
user_level=*?*	USM user level.	The value can be **read_only** or **read_write**. The default value is **read_write**. USM users of the read-only level can only read device information. USM users of the read/write level can read and write device information. All USM users can report Trap messages.

In the following example of adding an SNMP user, the user name is **user**, the authentication protocol is **MD5**, and the data encryption protocol is **AES**.



```
admin:/>add snmp usm user_name=user authenticate_protocol=MD5 private_protocol=AES
Please input your authenticate password:*********
Please input your authenticate password again:*********
Please input your private password:*********
Please input your private password again:*********
CAUTION: You are advised to set the USM account using secure authentication protocol SHA and data encryption protocol AES.
Do you wish to continue?(y/n)y
Command executed successfully.
```

NOTE

- In the CLI command output, **authenticate_protocol** indicates the authentication protocol, **authenticate password** indicates the authentication password, **private_protocol** indicates the data encryption protocol, and **private password** indicates the data encryption password.
- To obtain the context name, run the **show snmp context_name** command.

----End

For OceanStor V300R003 and earlier versions, **Table C-1** lists the SNMP parameters.

Table C-1 SNMP parameters

Protocol Version	Parameter	Default Value	Remarks
v2c	Read community	storage_public	To enable the v2c protocol, run the **change snmp version v1v2c_switch=On** command.
	Write community	storage_private	
v3	User name	Kaimse	Run the **show snmp usm** command to query the value.
	Context name	Array	Run the **show snmp context_name** command to query the value.
	Authentication protocol	● OceanStor V100R001C00SPC 200 and earlier: MD5 ● OceanStor V100R001C00SPC 300 and later: SHA	Run the **show snmp usm** command to query the value.
	Authentication password	ism@Storage	● The default value is recommended. If the password has been changed, ask the device administrator for it. ● If you change the password, ensure that the new authentication password and data encryption password are different.
	Encryption protocol	● OceanStor V100R001C00SPC 200 and earlier: NONE ● OceanStor V100R001C00SPC 300 and later: AES	Run the **show snmp usm** command to query the value.

Protocol Version	Parameter	Default Value	Remarks
	Encryption password	- OceanStor V100R001C00SPC 200 and earlier: no password - OceanStor V100R001C00SPC 300 and later: **ism@Storage**	- The default value is recommended. If the password has been changed, ask the device administrator for it. - If you change the password, ensure that the new authentication password and data encryption password are different.

C.2 Configuring SNMP Parameters (for Servers)

Table C-2 lists the SNMP versions and parameters of servers.

Table C-2 SNMP parameters

Protocol Version	Parameter	Default Value	Remarks
v2c	Read community	-	SNMPv2c is disabled by default.
	Write community	-	
v3	User name	- **root** (iBMC V3 series and MM910) - **Administrator** (iBMC V5 series)	If the default values are incorrect, set the parameters according to the device user guide. **NOTE** **SHA** indicates the SHA1 protocol and **AES** indicates the AES128 protocol.
	Context name	-	
	Authentication protocol	SHA	
	Authentication password	- **Huawei12#$** (iBMC V3 series and MM910) - **Admin@9000** (iBMC V5 series)	
	Encryption protocol	AES	

Protocol Version	Parameter	Default Value	Remarks
	Encryption password	- **Huawei12#$** (iBMC V3 series and MM910) - **Admin@9000** (iBMC V5 series)	

D Mailbox Parameters

If the email channel is used, you need to set mailbox parameters. **Table D-1** lists common mailbox parameters. As long as mailbox parameters are correctly configured, the DME IQ Client can send alarms to the DME IQ cloud system.

NOTE

- The parameters in **Table D-1** may not be the latest information. For details about the SMTP server and port parameters, see the official website of the email service provider.
- If a mailbox fails to pass the test, the SMTP service of the mailbox may not be enabled by default. In this case, enable it on the page for setting the email address of the corresponding service provider.

Table D-1 Common mailbox parameters

Email Supplier	Sender Email	SMTP Server	Server Port	Secure Connection
163 Mail	@163.com	smtp.163.com	25	TLS1.2
126 Mail	@126.com	smtp.126.com	25	TLS1.2
QQ Mail	@qq.com	smtp.qq.com	25/587	TLS1.2
Sina Mail	@sina.com	smtp.sina.com	25	TLS1.2
Sohu Mail	@sohu.com	smtp.sohu.com	25	TLS1.2
Gmail	@gmail.com	smtp.gmail.com	587	TLS1.2

E Certificate and Public Key Information

Table E-1 Default certificate information

Certificate Name	Function
actalis_Root_CA.crt	When the DME IQ Client connects to the DME IQ cloud system through HTTPS, the DME IQ Client checks whether the certificate chain returned by the DME IQ cloud system is issued by the Actalis certificate authority to prevent the DME IQ cloud system from being spoofed.
DigiCert_Root_CA_G2.crt	Standby certificate. When the certificate for the DME IQ cloud system is switched to the one issued by the certificate authority of the standby certificate, you do not need to update the root certificate of the DME IQ Client.
EntrustCert_CA_G2.crt	Standby certificate. When the certificate for the DME IQ cloud system is switched to the one issued by the certificate authority of the standby certificate, you do not need to update the root certificate of the DME IQ Client.
GlobalSign_Root_CA_R3.crt	Standby certificate. When the certificate for the DME IQ cloud system is switched to the one issued by the certificate authority of the standby certificate, you do not need to update the root certificate of the DME IQ Client.

Table E-2 Default public key information

Public Key	Function
KEYS	Verifies the integrity of a product software package when it is downloaded from the DME IQ cloud system.
KEYS4096	Verifies the integrity of a product software package when it is downloaded from the DME IQ cloud system.

Public Key	Function
RsaPublic	Verifies the integrity of a product software package when it is downloaded from the DME IQ cloud system.

F Account Information of Open-Source Software

Software Name	Account Usage	Account	Password	Remarks
Quartz	Account and password in an SQL example of the Quartz open-source software. The account is not used in practice and has no service usage.	quartz2	quartz2123	-

G FAQs

This chapter describes how to troubleshoot common problems that occur during the installation and use of the DME IQ Client.

G.1 What Can I Do If the Alarm Reporting Function Fails to Be Enabled for a Device?

Question

What can I do if the alarm reporting function fails to be enabled for a device?

Answer

After the SNMP parameters of the device are configured and the alarm reporting function is enabled for the device, a message indicating that the operation fails is displayed. The six possible causes are as follows. OceanStor V3 series V300R002 products are used as examples to describe how to locate and rectify the fault.

- The read or write community of SNMPv2c is incorrect or the security parameters of SNMPv3 are incorrect.

  Check whether the SNMP parameters are correctly configured by referring to the SNMP parameters in **3.1.4 Preparing Configuration Information**.

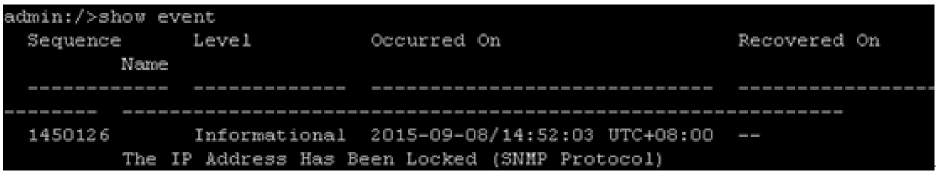
- The number of alarm dump servers reaches the upper limit.

  A maximum of four alarm dump servers can be added. You can run the **show notification trap** command to view the added servers. If four alarm dump servers have been added, check with the device administrator whether there is a Trap server that is not used. If yes, run the **delete notification trap server_id=***?* command to delete it.

- SNMPv2c of the device is not enabled (if the device uses the v2c version).

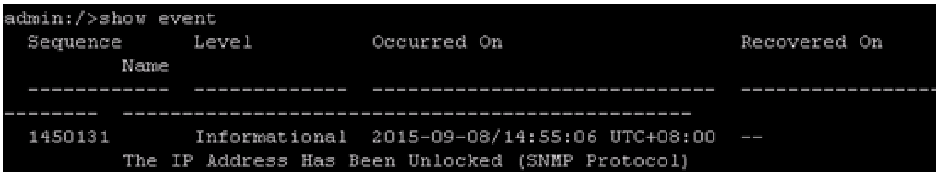
  SNMPv2c is disabled on devices by default. If you want to use SNMPv2c, run the **change snmp version v1v2c_switch=On** command to enable it.

- Incorrect SNMP parameters are used. As a result, the IP address of the server where the DME IQ Client is installed is locked. (Try again later.)
  - Run the **show event** command to check whether an IP address is locked recently.



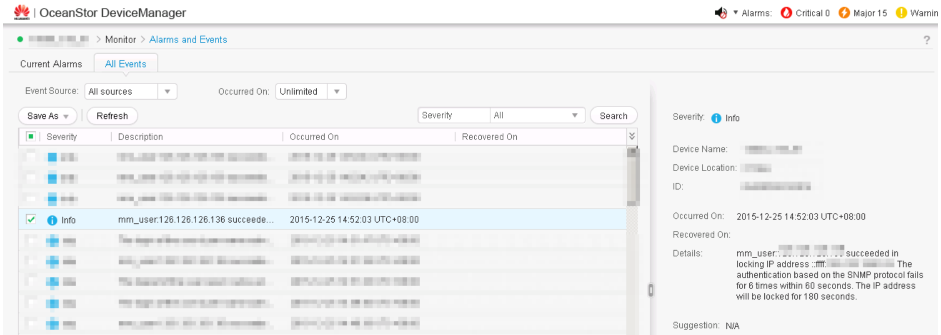
```
admin:/>show event
  Sequence       Level          Occurred On                    Recovered On
          Name
  ------------  -------------  -----------------------------  -----------------
--------  ----------------------------------------------------------------
  1450126       Informational  2015-09-08/14:52:03 UTC+08:00  --
          The IP Address Has Been Locked (SNMP Protocol)
```

– The IP address is unlocked automatically after a specific period (three minutes by default). You can run the **show event** command to view unlock events.



```
admin:/>show event
  Sequence       Level          Occurred On                    Recovered On
          Name
  ------------  -------------  -----------------------------  -----------------
--------  ------------------------------------------------
  1450131       Informational  2015-09-08/14:55:06 UTC+08:00  --
          The IP Address Has Been Unlocked (SNMP Protocol)
```

- You can enter **https://***Device IP address***:8088** in the Uniform Resource Locator (URL) address box of a browser to open OceanStor DeviceManager. On the monitoring page, you can check whether there are IP lock events recently.



☑ Info mm_user:126.126.126.136 succeede... 2015-12-25 14:52:03 UTC+08:00

Severity: Info

Device Name: [redacted]

Device Location: [redacted]

ID: [redacted]

Occurred On: 2015-12-25 14:52:03 UTC+08:00

Recovered On:

Details: mm_user:[redacted] succeeded in locking IP address ::ffff:[redacted] The authentication based on the SNMP protocol fails for 6 times within 60 seconds. The IP address will be locked for 180 seconds.

Suggestion: N/A

- The port number of the SNMP service is incorrect.

  Run the **show snmp port** command to view the SNMP port.

- The SNMP service is not correctly enabled for the device.

  If the service is not correctly enabled, contact the device administrator for troubleshooting.

G.2 What Can I Do If the Alarm Reporting Status Is Abnormal When the DME IQ Client Is Running?

Question

What can I do if the alarm reporting status is abnormal when the DME IQ Client is running?

Answer

When the DME IQ Client is running, if the alarm reporting status of a device becomes "Failed to receive the device alarms" or "Failed to connect the device", perform the following steps:

- Failed to receive device alarms

Step 1 On the **Devices** page, select the device whose alarm reporting status is abnormal and click **Stop Alarm Reporting**. When alarm reporting is stopped, click **Start Alarm Reporting**. If alarm reporting is started successfully, go to the next step. If alarm reporting fails to be started, perform the steps in **G.1 What Can I Do If the Alarm Reporting Function Fails to Be Enabled for a Device?** and go to the next step.

Step 2 Check whether the DME IQ Client can receive the test alarms sent by the device. If yes, skip this step. If no, check whether port 10162 using UDP between the local host and device is enabled. If the port is not enabled, add an inbound rule for the port on the local host running Windows. If the inbound rule is added successfully, check whether the DME IQ Client can receive the test alarms sent by the device.

----End

- Failed to connect the device

Step 1 Check whether the network connection between the local host and the device is normal. If yes, go to the next step. If no, contact the equipment room administrator of the customer. After the network connection is restored, wait for 5 to 10 minutes. If the fault persists, go to the next step.

Step 2 On the **Devices** page, select the device whose alarm reporting status is abnormal and click **Stop Alarm Reporting**. After alarm reporting is stopped, click **Modify** to open the **Modify Device** page. Enter the correct SNMP parameters and then start alarm reporting again. If the fault persists, see **G.1 What Can I Do If the Alarm Reporting Function Fails to Be Enabled for a Device?**.

----End

G.3 What Can I Do If I Forget the Administrator Login Password?

Question

What can I do if I forget the administrator login password of the DME IQ Client?

Answer

Step 1 Start the DME IQ Client.

Step 2 In the login dialog box that is displayed, click **Forgot Password?**

Step 3 In the **Retrieve Password** dialog box, click **Send Verification Code**.

NOTE

The system sends a verification code to the email address for retrieving the password.

Step 4 Enter the verification code and click **OK**.

Step 5 In the **Change Password** dialog box that is displayed, set **New Password** and **Confirm Password** and click **OK**.

NOTE

- The new password must contain 8 to 32 characters including uppercase letters, lowercase letters, and special characters. The password cannot be set to a weak password, such as **Huawei@123** or **Admin@123**.
- The new password must be different from any of the five recently used passwords.
- The password validity period is six months. Change the password periodically.

Step 6 Enter the new password to log in to the DME IQ Client.

NOTE

Keep this password safe.

----End

G.4 What Can I Do If an OceanStor 9000 Device Cannot Use SNMPv3 to Enable the Alarm Reporting Function?

Question

What can I do if an OceanStor 9000 device cannot use SNMPv3 to enable the alarm reporting function?

Answer

For OceanStor 9000 V300R006C10 and later versions, on the **Devices** tab page of the DME IQ Client, select the device and then click **Start Alarm Reporting**. For versions earlier than V300R006C10, perform the following steps:

Step 1 In the address box of the browser, enter **https://***xxx.xxx.xxx.xxx***:8088**. Then enter the user name and password to log in to DeviceManager.

NOTE

xxx.xxx.xxx.xxx indicates the IP address of the device.

Step 2 Choose **Settings** > **Alarm Settings** > **Trap IP Address Management** and click **Add** in the function pane.

The **Add Server IP Address** dialog box is displayed.

1. Enter the following information:
   - **Server IP**: Enter the IP address of the server where the DME IQ Client is deployed.
   - **Port**: Enter **10162**.
   - **Version**: Select **SNMPv3**.
   - **Type**: Select **All**.
2. Click **OK**.
3. In the lower left corner of the function pane, click **Save**.

Step 3 On the **Devices** page of the DME IQ Client, select the OceanStor 9000 device whose parameters you want to modify and click **Modify**.

The **Modify Device** dialog box is displayed. In the **Modify Device** dialog box, enter the correct SNMPv3 parameters of the OceanStor 9000 device and click **OK**.

Step 4 On the **Devices** page of the DME IQ Client, select the OceanStor 9000 device and click **Start Alarm Reporting**.

----End

G.5 What Can I Do If an E9000 Server Cannot Use SNMPv2c to Enable the Alarm Reporting Function?

Question

What can I do if an E9000 server cannot use SNMPv2c to enable the alarm reporting function?

Answer

Step 1 In the address box of the browser, enter **https://***xxx.xxx.xxx.xxx*. Then enter the user name and password to log in to the E9000 management page.

NOTE

xxx.xxx.xxx.xxx indicates the IP address of the device.

Step 2 Choose **Chassis Settings** > **Network Settings** > **MM**, and click **Edit**. Under **SNMP Trap Settings**, perform the following settings:

- Set **Trap** to **Enable**.
- Set **Trap mode** to **OID**.
- Set **Trap version** to **V2C**.
- Set **Trap port number** to **10162**.
- Choose one box from **Trap address 1** to **Trap address 5** and then enter the IP address of the server where the DME IQ Client is deployed.

Step 3 In the upper left corner of the function pane, click **Save**.

Step 4 On the **Devices** page of the DME IQ Client, select the E9000 server and click **Start Alarm Reporting**.

----End

G.6 What Can I Do If the DME IQ Client Does Not Respond When I Click the Shortcut on the Desktop After the DME IQ Client Is Installed?

Question

What can I do if the DME IQ Client does not respond when I click the shortcut on the desktop after the DME IQ Client is installed?

Answer

If the preceding problem occurs, perform the following operations:

Step 1 Click **My Computer** to go to the path where the DME IQ Client is installed. Double-click the **dmeiq** directory. A dialog box is displayed. Click **Continue**. After you log in to the installation path, double-click the shortcut on the desktop to open the DME IQ Client.

Step 2 If you still cannot log in to the DME IQ Client after performing the preceding operations, uninstall the DME IQ Client. Then log in to the system as the Windows administrator who has higher permission, and reinstall and restart the DME IQ Client.

----End

G.7 What Can I Do If the System Prompts that Port 10162 Is Occupied When the DME IQ Client Is Being Started?

Question

What can I do if the system prompts that port 10162 is occupied when the DME IQ Client is being started?

Answer

Step 1 Check whether port 10162 is occupied by **prunsrv**.

- If yes, go to **Step 2**.
- If no, go to **Step 3**.

Step 2 Exit the DME IQ Client, go to the installation directory of the DME IQ Client, right-click **dmeiq.exe**, and choose **Run as administrator** from the shortcut menu.

Step 3 Perform any of the following operations.

- Change the port occupied by the DME IQ Client. For details, see **G.9 How Do I Change the Port Occupied by the DME IQ Client?**.
- Release port 10162 occupied by other programs.
- Replace the device on which the DME IQ Client is installed.

----End

G.8 What Are Common Weak Passwords?

Question

What are common weak passwords?

Answer

The login password of the DME IQ Client cannot be set to a weak password. Common weak passwords are as follows:

Huawei123@, huawei123@, Admin123@, admin123@, Root123@, root123@, Huawei123#, huawei123#, Admin123#, admin123#, Root123#, root123#, Huawei123!, huawei123!, Admin123!, admin123!, Root123!, root123!, Huawei@123, huawei@123, Admin@123, admin@123, Root@123, root@123, 123@Huawei, 123@Root, Huawei_123, huawei_123, Admin_123, admin_123, Root_123, root_123, abcd@1234, abcd1234!, abcd_1234, Huawei!@#, huawei!@#, Admin!@#, admin!@#, Huawei!@, huawei!@, Password@123, Password_123, Password123!

G.9 How Do I Change the Port Occupied by the DME IQ Client?

Question

How do I change the port occupied by the DME IQ Client?

Answer

To change the port occupied by the DME IQ Client, perform the following operations:

Step 1 Exit the DME IQ Client in the system tray of Windows taskbar.

Step 2 Open the installation directory of the DME IQ Client, go to the **configuration** folder, and open the **defaultSnmpParam.properties** file with a text editor.

Step 3 Change the value of **snmptrap.port** to the port number that needs to be occupied.

Step 4 Start the DME IQ Client and then enable alarm reporting for all added devices.

----End

G.10 How Do I Collect the Debugging Logs of the DME IQ Client?

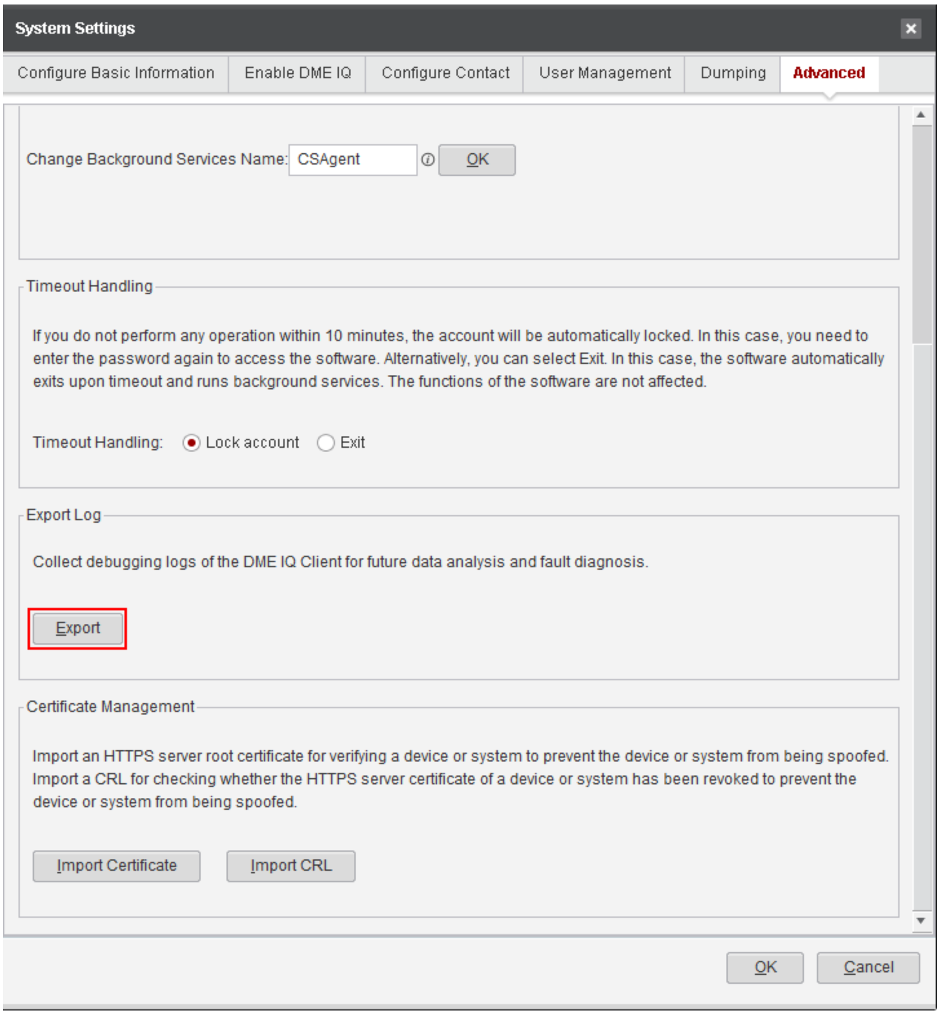
Question

How do I collect the debugging logs of the DME IQ Client?

Answer

- You have logged in to the DME IQ Client.
  a. Click ⚙.
     The **System Settings** dialog box is displayed.

b. Choose **Advanced** > **Export**.



System Settings

Change Background Services Name: CSAgent

Timeout Handling

If you do not perform any operation within 10 minutes, the account will be automatically locked. In this case, you need to enter the password again to access the software. Alternatively, you can select Exit. In this case, the software automatically exits upon timeout and runs background services. The functions of the software are not affected.

Timeout Handling: ● Lock account ○ Exit

Export Log

Collect debugging logs of the DME IQ Client for future data analysis and fault diagnosis.

Certificate Management

Import an HTTPS server root certificate for verifying a device or system to prevent the device or system from being spoofed. Import a CRL for checking whether the HTTPS server certificate of a device or system has been revoked to prevent the device or system from being spoofed.

c. Select the path where logs will be stored and click **Save**.

d. After the export is successful, click **OK**. The DME IQ Client automatically generates a package, that is, a package of debugging logs.

- The DME IQ Client cannot be logged in to or is not deployed.

  a. Open the installation path of the DME IQ Client. For example, if it is installed in the C drive, the path is **C:\dmeiq**.

  b. Find the **log** folder.

  c. Compress the **log** folder to obtain the debugging logs of the DME IQ Client.

G.11 What Can I Do If the DME IQ Client Is Disconnected from the Cloud System?

Question

The DME IQ Client periodically sends information for establishing a heartbeat connection to the cloud system. If the cloud system does not receive the information, it considers that the DME IQ Client is disconnected.

How do I restore the connection between the DME IQ Client and the cloud system?

Answer

Table G-1 lists possible causes for the disconnection of the DME IQ Client.

Table G-1 Possible causes

Possible Cause	Description	Estimated Probability
Abnormal network channel	The network where the DME IQ Client is located is abnormal, the firewall port is disabled, or the DNS service is abnormal.	65%
Abnormal deployment environment	The host where the DME IQ Client is deployed is powered off, or the disk space for installing it is insufficient.	15%
Abnormal running status	The running status of the DME IQ Client is abnormal or the background services are not enabled.	15%
Improper hibernation settings of Windows	When the host where the DME IQ Client is deployed hibernates, the DME IQ Client process is suspended and cannot run properly.	5%

To restore the connection, use the following methods:

Abnormal Network Channel

Abnormal Deployment Environment

Abnormal Running Status

Improper Hibernation Settings of Windows

Others

Abnormal Network Channel

- **Internet channel**

Step 1 Obtain the DME IQ Client version.

Open the installation directory of the DME IQ Client and view the modification date of the **dmeiq.exe** file.

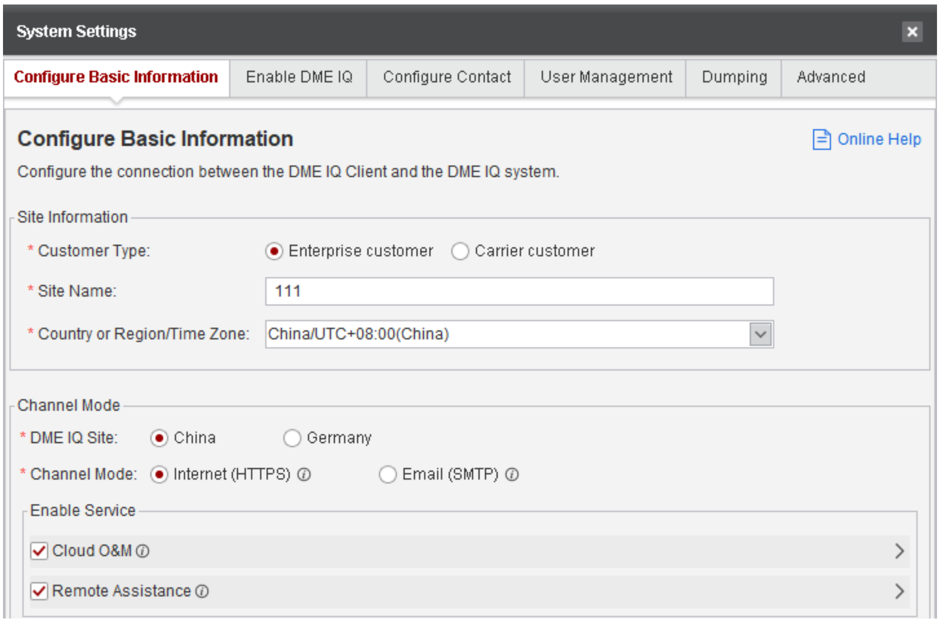
Step 2 Check the network connectivity by performing the following steps. This section uses the technical support center for enterprises in the Chinese mainland as an example.

1. On the server where the client is installed, choose **Start** > **Run** and enter **cmd** to open a command prompt. Then, run the following command:

```
telnet ecloudservice-cn.huawei.com 443
```

   – In the preceding command, **ecloudservice-cn.huawei.com** is an example domain name of the server corresponding to the technical support center for enterprises in the Chinese mainland. You can obtain the domain name in the following way.

      i. Log in to the DME IQ Client and check the DME IQ cloud system in the basic information, as shown in the following figure.



Configure Basic Information

Configure the connection between the DME IQ Client and the DME IQ system.

Site Information

* Customer Type: ● Enterprise customer ○ Carrier customer

* Site Name: 111

* Country or Region/Time Zone: China/UTC+08:00(China)

Channel Mode

* DME IQ Site: ● China ○ Germany

* Channel Mode: ● Internet (HTTPS) ○ Email (SMTP)

Enable Service

☑ Cloud O&M

☑ Remote Assistance

      ii. Obtain the website of the server corresponding to the secure access service according to the following:

         ○ In the Chinese mainland:

         Technical support center for enterprises: https://ecloudservice-cn.huawei.com

         Technical support center for carriers: https://icloudservice-cn.huawei.com

         ○ Outside the Chinese mainland:

         Technical support center for enterprises:

         Romania: https://itr-eservicero-ent.huawei.com

         Russia: https://enterpriseru.eservice.huawei.com

         Technical support center for carriers:

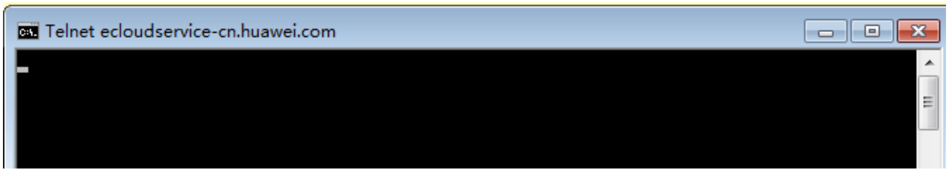
         Romania: https://itr-eservicero-carrier.huawei.com

         Mexico: https://itr-eservicemx-carrier.huawei.com

   – In the preceding command, **443** is the port number used by the host where the DME IQ Client is located to access the DME IQ cloud system.

2. Check the command output.

- If the command output is displayed as shown in the following figure, the network connection is normal.



```
Telnet ecloudservice-cn.huawei.com
```

- If a message indicating that the connection fails is displayed, go to the next step.

3. Check whether the DNS function of the VM where the DME IQ Client is installed is normal and contact the network administrator to check whether the port of the domain name is enabled on the firewall.

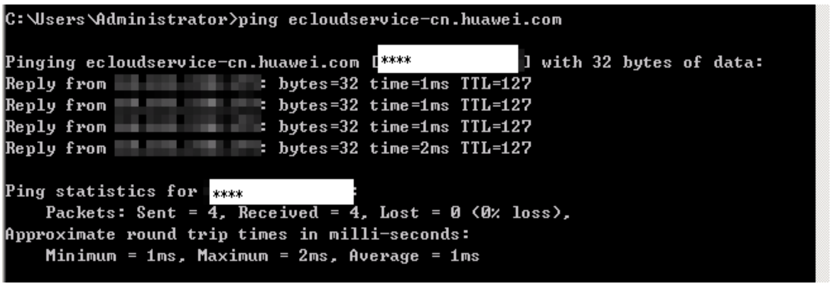
   Perform the following steps to check whether the DNS function of the VM where the DME IQ Client is installed is normal:

   a. Choose **Start** > **Run** and enter **cmd** to open a command prompt. Then, run the following command (the technical support center for enterprises in the Chinese mainland is used as an example):

   ```
   ping ecloudservice-cn.huawei.com
   ```

   b. Check the command output.

      ■ If the ping operation succeeds and the IP address of the domain name is displayed, the DNS function is normal.



```
C:\Users\Administrator>ping ecloudservice-cn.huawei.com

Pinging ecloudservice-cn.huawei.com [****          ] with 32 bytes of data:
Reply from [redacted]: bytes=32 time=1ms TTL=127
Reply from [redacted]: bytes=32 time=1ms TTL=127
Reply from [redacted]: bytes=32 time=1ms TTL=127
Reply from [redacted]: bytes=32 time=2ms TTL=127

Ping statistics for ****          :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

NOTE

**** is the IP address corresponding to the domain name. In this example, **ecloudservice-cn.huawei.com** is the domain name corresponding to the technical support center for enterprises in the Chinese mainland. Change the IP address and domain name based on the actual conditions.

      ■ If the ping operation fails, the DNS function is abnormal. In this case, contact the network administrator.

----End

- **Email channel**

Step 1 Check whether the email server is normal.

Table G-2 Check methods

Email Server Type	Description	Check Method
Intranet email server	For example, the internal email server of a company.	Contact the network administrator.
Public network email server	Public network email servers such as 163 and qq email servers	For example, 163 email: telnet smtp.163.com

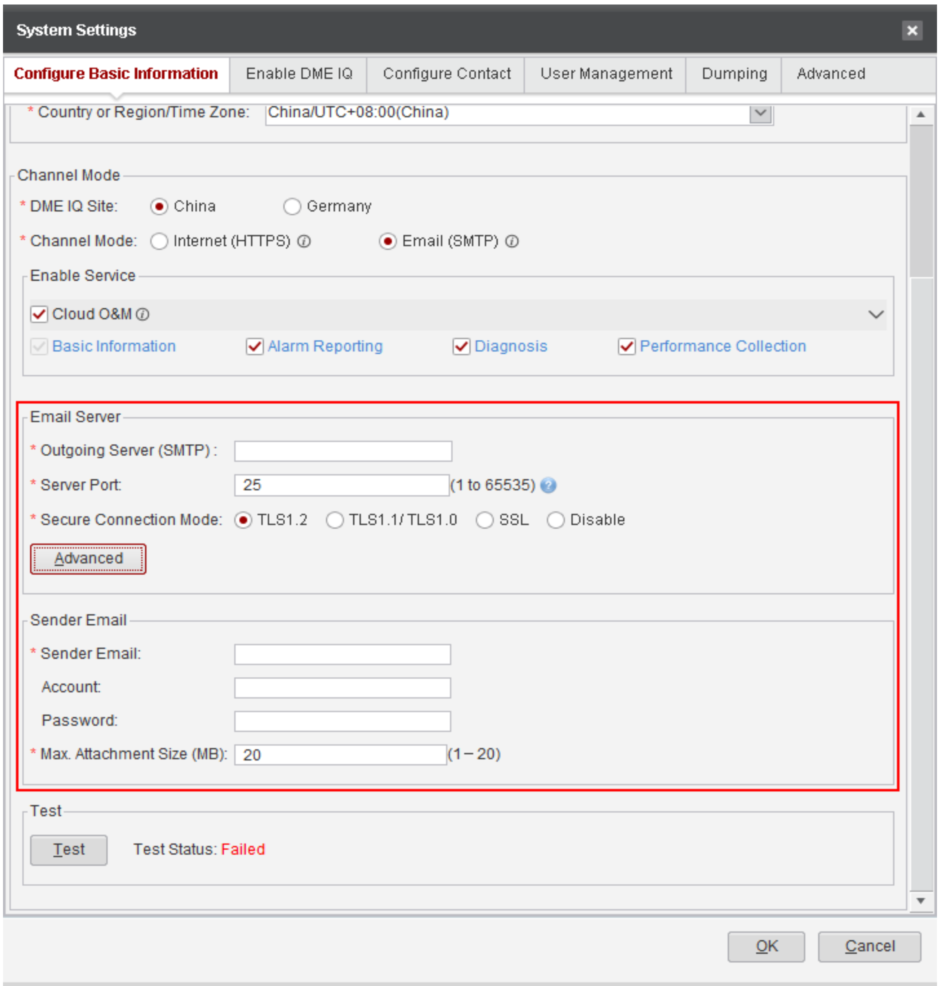
Step 2 Check whether the email account and password entered for the email channel are correct.

NOTE

- The email account and password configured for the email channel of the DME IQ Client must be the same as the actual account and password.
- If the password of the outbox has been changed recently, you need to change the outbox password on the DME IQ Client.

Step 3 Send a test email on the DME IQ Client.

1. Configure the email server and sender email.



* Country or Region/Time Zone: China/UTC+08:00(China)

Channel Mode

* DME IQ Site: ● China ○ Germany

* Channel Mode: ○ Internet (HTTPS) ● Email (SMTP)

Enable Service

☑ Cloud O&M

☑ Basic Information ☑ Alarm Reporting ☑ Diagnosis ☑ Performance Collection

Email Server

* Outgoing Server (SMTP) :

* Server Port: 25 (1 to 65535)

* Secure Connection Mode: ● TLS1.2 ○ TLS1.1/TLS1.0 ○ SSL ○ Disable

Sender Email

* Sender Email:

Account:

Password:

* Max. Attachment Size (MB): 20 (1 – 20)

Test

Test Status: Failed

2. Click **Test**. The **Test** dialog box is displayed.
3. In **Receiver Email**, enter the email address for receiving test results.

   NOTE

   – **Receiver Email** can be the email address of the sender or the receiver.

   – You are advised to use a Huawei email address (****@huawei.com) for receiving test results.

4. Click **Test**. A dialog box is displayed indicating the test result.

Step 4 Check the recipient email box. If the recipient email box receives the test email and **Test Status** on the DME IQ Client is **Passed**, the email channel is normal.

----End

Abnormal Deployment Environment

Step 1 Check whether the power supply of the host is normal, whether the host is powered on, and whether the operating system is running properly.

- If no, contact the device administrator to restore the host.
- If yes, go to the next step.

Step 2 Check whether the free disk space of the host where the DME IQ Client is installed is sufficient.

- If the free disk space is greater than 5 GB, the disk space is sufficient.
- If the free disk space is less than or equal to 5 GB, the disk space is insufficient. In this case, go to the next step.

Step 3 Clean up or expand the disk for installing the DME IQ Client.

----End

Abnormal Running Status

Step 1 Check whether the DME IQ Client process is running.

Click ▲ at the lower right corner of the Windows desktop. The hidden icons are displayed. Check whether the DME IQ Client icon is displayed.

- If the icon is displayed, the DME IQ Client process is running.
- If the icon is not displayed, restart the DME IQ Client.

Step 2 Check whether the DME IQ Client background services are running.

Exit the DME IQ Client. Start the Windows Task Manager and select **Services**. Check the running status of the cswatchdog and CSAgent services.

- If **Status** is **Running**, the DME IQ Client services are running properly.
- If **Status** is **Stopped**, go to the next step.

Step 3 Enable the background services of the DME IQ Client.

Start the DME IQ Client again as the administrator. Log in to it and click ⚙ to go to the **System Settings** page. Click **Advanced** to go to the advanced settings page and enable the background services.

If the background services are enabled, disable them and then enable them again.

Step 4 Perform **Step 2** again to check the running status of the DME IQ Client background services.

- If **Status** is **Running**, the DME IQ Client services are running properly.
- If **Status** is **Stopped**, contact the DME IQ cloud system.

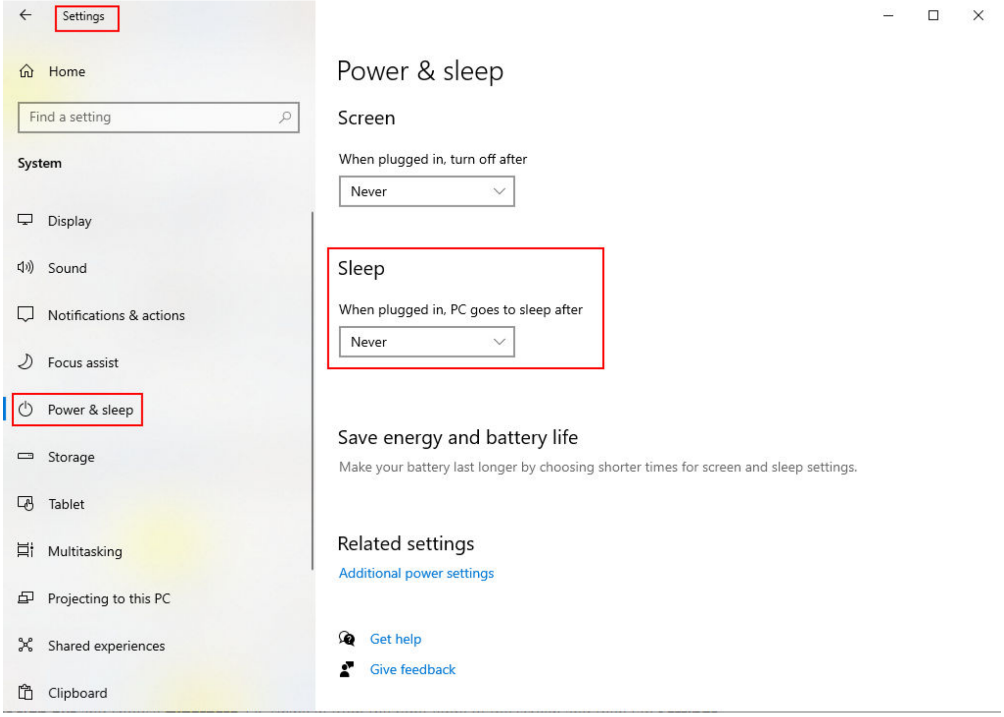
----End

Improper Hibernation Settings of Windows

Step 1 Click ⊞ and select ⚙. The **Window Settings** page is displayed.

Step 2 Choose **System** > **Power & sleep**. The **Power & sleep** page is displayed.

Step 3 Set **Sleep** to **Never**.



Power & sleep

Screen

When plugged in, turn off after

Never

Sleep

When plugged in, PC goes to sleep after

Never

Save energy and battery life

Make your battery last longer by choosing shorter times for screen and sleep settings.

Related settings

Additional power settings

NOTE

This document uses the Windows 10 operating system as an example. Set sleep according to the actual operating system.

----End

Others

Restart the DME IQ Client. If the DME IQ Client is still disconnected from the cloud system after the restart, contact the DME IQ cloud system.

G.12 What Can I Do If the DME IQ Client Is Falsely Reported As a Virus or Risky Software?

Question

What can I do if the DME IQ Client is falsely reported as a virus or risky software?

Answer

According to the feedback and analysis from Huawei and antivirus software vendors, scan reports by KAV, McAfee, and OSCE are normal. Customers can feel relieved to use the DME IQ Client.

G.13 What Can I Do If a Message Is Displayed Indicating that the Dependent Component Required for Running the Software Is Missing When I Start the DME IQ Client?

Question

What can I do if a message is displayed indicating that the dependent component required for running the software is missing when I start the DME IQ Client?

Answer

You need to visit the **software download page** to download and install Microsoft Visual C++ Redistributable for Visual Studio 2015 or later (x86 architecture).

📖 NOTE

For better compatibility, the 32-bit JRE is used for running the software. Therefore, the dependent component of the x86 architecture must be installed. You are advised to install the dependent component of the x64 architecture as well for better scalability.

G.14 What Can I Do If the DME IQ Client Fails to Collect Performance Data of the vCenter System?

Question

What can I do if the DME IQ Client fails to collect performance data of the vCenter system?

Answer

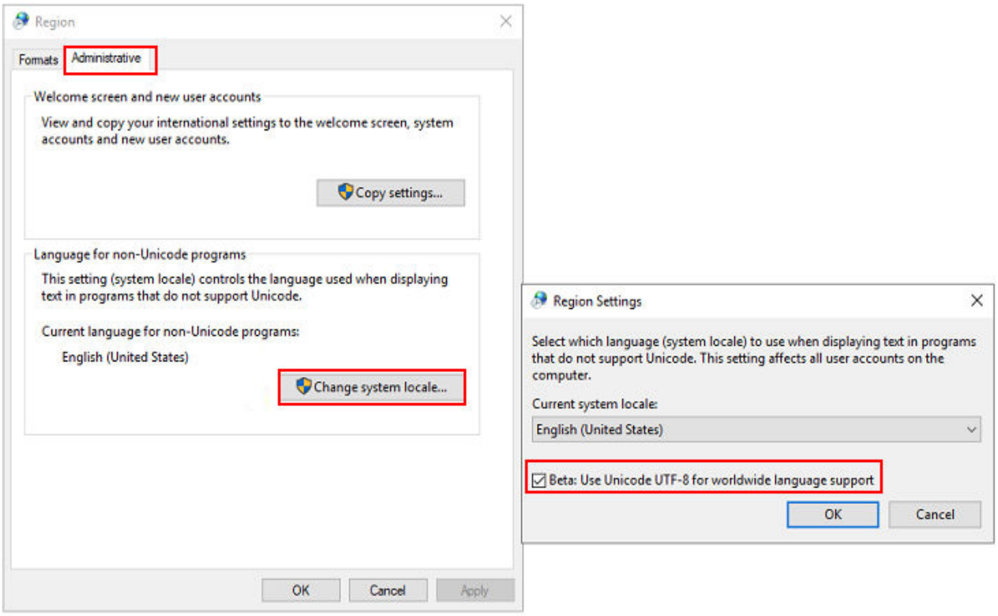
If the preceding problem occurs, perform the following operations:

Step 1 Open the system control panel and select **Region**.

Step 2 On the **Administrative** tab page, click **Change system locale**.

Step 3 On the **Region Settings** page, select **Beta: Use Unicode UTF-8 for worldwide language support** and click **OK**.

After setting the region, restart Windows for the settings to take effect.



Welcome screen and new user accounts

View and copy your international settings to the welcome screen, system accounts and new user accounts.

Language for non-Unicode programs

This setting (system locale) controls the language used when displaying text in programs that do not support Unicode.

Current language for non-Unicode programs:

English (United States)

Select which language (system locale) to use when displaying text in programs that do not support Unicode. This setting affects all user accounts on the computer.

Current system locale:

English (United States)

☑ Beta: Use Unicode UTF-8 for worldwide language support

----End

NOTE

This document uses the Windows 10 operating system as an example. Configure the region according to the actual operating system.

G.15 What Can I Do If the HTTPS Certificate Verification of an SVP Device Fails?

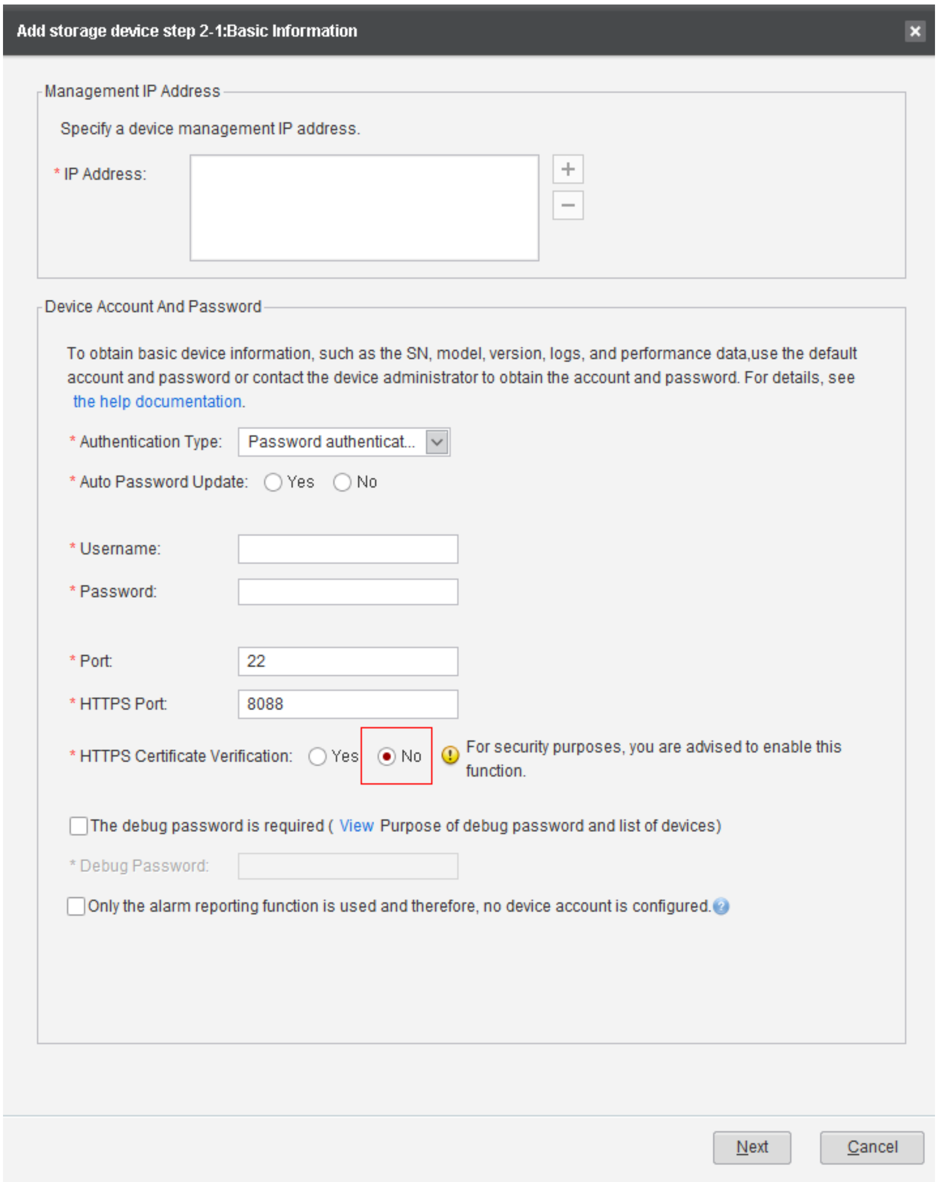
Question

When I add a storage device with an SVP to the DME IQ Client, the message "Failed to verify the HTTPS server certificate" is displayed. What can I do?

Answer

The HTTPS security suite supported by a storage device with an SVP cannot match the latest HTTPS security suite. Therefore, the certificate verification fails.

When adding a storage device with an SVP, set **HTTPS Certificate Verification** to **No**.



Add storage device step 2-1:Basic Information

Management IP Address

Specify a device management IP address.

* IP Address:

Device Account And Password

To obtain basic device information, such as the SN, model, version, logs, and performance data,use the default account and password or contact the device administrator to obtain the account and password. For details, see the help documentation.

* Authentication Type: Password authenticat...

* Auto Password Update: ○ Yes ○ No

* Username:

* Password:

* Port: 22

* HTTPS Port: 8088

* HTTPS Certificate Verification: ○ Yes ● No For security purposes, you are advised to enable this function.

□ The debug password is required (View Purpose of debug password and list of devices)

* Debug Password:

□ Only the alarm reporting function is used and therefore, no device account is configured.

G.16 What Can I Do If the Device Fingerprint Is Not Verified for an SSH Connection After the DME IQ Client Is Upgraded?

Question

What can I do if the device fingerprint is not verified for an SSH connection after the DME IQ Client is upgraded?

Answer

If you change the value of **ssh.fingerprints.verification.default.disabled** to **false** in software configuration file **defaultSshParam.properties** before the upgrade, the device fingerprint will be verified when you connect the device using SSH.

After the upgrade, the value is reset to **true**. In this case, you need to manually change the value to **false**.

NOTE

After the device software version is upgraded, the device fingerprint also changes. As a result, the DME IQ Client fails to connect to the device. To improve usability, the device fingerprint is not verified by default when the device is connected using SSH.

G.17 How Do I Configure a Verification Certificate When the DME IQ Client Collects vCenter System Performance or Log Data?

Question

How do I configure a verification certificate when the DME IQ Client collects vCenter system performance or log data?

Answer

Step 1 Change the value of **constants.KEY_IS_VERIFY_DEVICE_CERT** in **CONFIG_DATA** in **dmeiq\tools\VMwareGrabPlugin\lib\common\global_config.py** to **1**, indicating that certificate authentication is enabled.

Step 2 Place the root certificate of vCenter in the **dmeiq\tools\VMwareGrabPlugin\backend_files\device_cer** folder.

----End

H How to Obtain Help

If a problem persists in routine maintenance or troubleshooting, contact the technical support center for help.

The technical support center can be Huawei technical support center or partner technical support center.

For customers who purchase Huawei warranty services, contact Huawei technical support center. For customers who purchase partner warranty services, contact the corresponding partner technical support center.

H.1 Preparations Before Contacting the Technical Support Center

You are advised to collect necessary troubleshooting information and make preparations before contacting technical support.

Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

- Name and address of the customer
- Contact person and telephone number
- Time when the fault occurred
- Description of the fault phenomena
- Device type and software version
- Measures taken after the fault occurs and the related results
- Troubleshooting level and required solution deadline

H.2 How to Use the Document

Huawei provides guide documents shipped with the device. The guide documents can be used to handle the common problems occurring in daily maintenance or troubleshooting.

To better solve the problems, use the documents before you contact Huawei for technical support.

H.3 How to Obtain Help from Huawei Support Website

- Huawei technical support website for enterprises: **https://support.huawei.com/enterprise/en/index.html**
- Huawei technical support website for carriers: **https://support.huawei.com/carrierindex/en/hwe/index.html**