Smart Managed Switch Client

User Manual

UD33917B

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- ***HIKVISION*** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF

THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Preface

Applicable Models

This manual is applicable to smart managed switches.

Symbol Conventions

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

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

1 Product Introduction

The switches support management through the iVMS-4200 client, including network topology management, network configuration, port management, etc.

Note

All pictures in this manual are only for illustration, and the specific interfaces are subject to the actual device.

2 Device Management

You can perform device configuration and management on the iVMS-4200 client, mainly including network parameter configuration, port configuration, network topology management, etc.

Note

This chapter will briefly introduce device management via iVMS-4200 client. For other functions, please refer to *iVMS-4200 Client User Manual*.

2.1 Activate Device

For an inactive device, you are required to create a password to activate it before it can be added to the client and work properly.

Before You Start

Make sure that the device to be activated is connected to the network and is in the same network segment with the PC running the client.

Steps

Note

This function should be supported by the device.

1. Click **Maintenance and Management → Device Management → Device** .
2. Click **Online Device**.

   The searched online devices are displayed in the online device list below.
3. Check the device status (shown in the **Security Level** column), and select an inactive device.

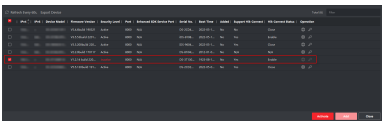

Figure 2-1 Online Device List

4. Click **Activate**.

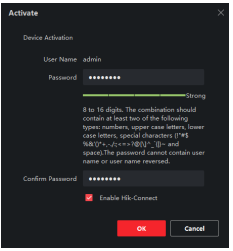

Figure 2-2 Activate Device

5. Create a password in the password field, and confirm the password.

Note

- The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of the following categories: uppercase letters, lowercase letters, digits, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system. Changing the password monthly or weekly can better protect your product.
- The password cannot contain "admin" or its reverse.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. Optional: Check **Enable Hik-Connect** if the device supports Hik-Connect service.

7. Click **OK**.

Note

After the device is activated, you can click or in the **Operation** column of the online device list to modify network parameters or reset the password of the device.

2.2 Add Device

After the device is activated, you can add it to the client in OTAP mode for remote configuration and management.

Before You Start
Obtain the IP address, user name, and password of the device to be added.

Steps
1. Click **Device Management** → **Device**.

2. Click **Add**.

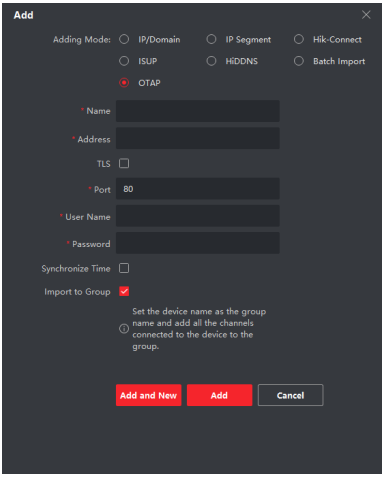

Figure 2-3 Add Device

3. Select **OTAP** as **Adding Mode**.
4. Enter the required information.

   Name

   Enter a descriptive name for the device.

   IP Address

   Enter the IP address of the device.

   Port

   Set the port number of the device. The default port number is 80.

   User Name

   Enter the user name set when the device is activated. By default, the user name is ***admin***.

   Password

   Enter the password set when the device is activated.
5. **Optional:** Check **TLS** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purposes.

   Note

   - This function should be supported by the device.
   - The client does not support security certificate authentication. Importing a trusted device certificate is not required. You only need to set **Enhanced SDK Service Port** (443 by default) to enable transmission encryption.
6. Check **Synchronize Time** to synchronize the device time with the PC running the client.
7. **Optional:** Check **Import to Group** to create a group by device name, and import all channels of the device to this group.
8. Click **Add** to finish device adding, or click **Add and New** to continue adding another device.

9. Optional: Perform the following operations.

Perform Remote Configuration	Click ⚙ in the **Operation** column for remote configuration of the corresponding device.
View Device Status	Click ▤ in the **Operation** column to view the device status.
Edit Device Information	Click ✎ in the **Operation** column to edit the device information, including the device name, IP address, pot number, user name, and password.
Refresh	Click ↻ in the **Operation** column or click Refresh to get the latest device information.
Delete Device	Select one or multiple devices, and click Delete to delete the selected device(s) from the client.
View Alarm Events	The device reports an alarm event when the device is offline, the port is disconnected, PoE is powered off, or the whole device PoE power reaches or exceeds the upper limit. You can click the corresponding button in the lower right corner of the interface to automatically hide, lock, maximize, or manually hide the alarm event list. The client supports viewing device alarm event information and batch processing alarm events.

3 Device Status

You can view the device status, port status, port statistics, and PoE port status.

Click **Device → Operation →** ▤ .

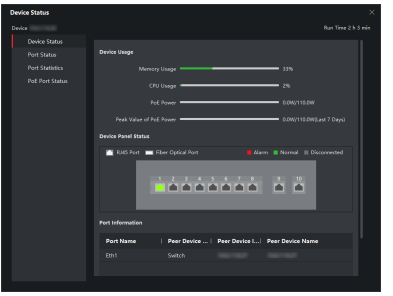

Figure 3-1 Device Status

Device Status

You can view the device usage, device panel status, and port information.

Port Status

You can view the rate, duplex mode, and flow control enabling status of each port.

Port Statistics

You can view the number of bytes sent or received, the number of packets sent or received, sending or receiving rate, and peak value of the sending or receiving rate (in the last seven days). You can also set the interval at which port statistics are automatically refreshed, manually refresh port statistics, or clear port statistics.

Note

You can drag the scroll bar to view all statistics.

PoE Port Status

For devices that support PoE, you can view the PoE enabling status and output power of each PoE RJ45 port.

4 Topology Management

You can view and configure the network topology between devices added to the client.

4.1 Related Operations

Select an added device, and click → **General Application** → **Topology** .

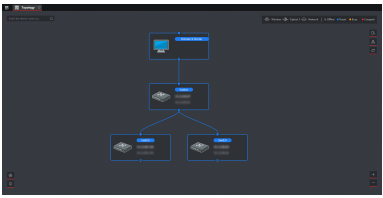

Figure 4-1 Topology Management

Interface Description

- In the upper left corner, you can enter a device name or IP address to search the desired device.
- In the upper right corner, you can obtain the meanings of different link icons and colors, select two devices to show the transmission path between them, and export or refresh the topology view.
- In the lower left corner, you can enable security protection with one click, perform topology settings, and view the tips.
- In the lower right corner, you can click the icons or scroll your mouse wheel to zoom in or out on the topology view.

Note

- Before generating the topology, make sure that all devices have been added to the client. If a device is added to the client for

the first time, click **Add Topology** to generate the device's network topology.

- If no topology is displayed when you access the topology interface for the first time, click to refresh the topology view or get topology again.

Related Operations

Operation	Description
Double-click a device to view the device details.	You can view the basic device information such as the device type, model, and IP address as well as the device usage, panel status, and port information.
Double-click a link to view the link details.	You can view the transmission rates of the link and the information about devices at both ends of the link.
Right-click a device, and select **Device Status**, **Event Handling**, **Remote Configuration**, **Edit Name**, or **Set as Root Node** from the shortcut menu.	**Device Status**: You can jump to the **Device Status** interface. For details, see ***Device Status***.
	Event Handling: You can view the information about alarm events such as the event time, event source, and event details, or clear events.
	Remote Configuration: You can jump to the web page of the device for remote configuration. For detailed operations, see *Smart Managed Switch Web User Manual*.
	Edit Name: You can customize the device name.
	Set as Root Node: You can set the device as the root node on the topology view.
Click to export the topology view.	You can select the saving path and format, and export the topology view. **Note** The default format is PDF.
Click to show the transmission path.	You can select a network camera (IPC) and the current device to show the path of signal transmission between them.

4.2 Topology Settings

Steps

1. Click in the lower left corner to edit topology settings.

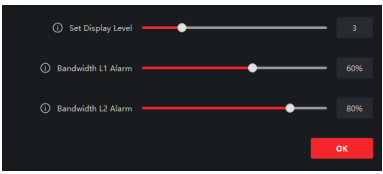

Figure 4-2 Topology Settings

Set Display Level

Set the topology display level. The value ranges from 1 to 10.

Note

You need to manually refresh the topology view for the setting to take effect.

Bandwidth L1 Alarm

Set the L1 alarm threshold of bandwidth. The value ranges from 1% to 100%.

Note

The link will turn yellow (busy) when the bandwidth exceeds this threshold.

Bandwidth L2 Alarm

Set the L2 alarm threshold of bandwidth. The value ranges from 1% to 100%.

Note

- The link will turn red (congested) when the bandwidth exceeds this threshold.
- The L2 alarm threshold should be larger than the L1 alarm threshold.

2. Click **OK**.

Note

After topology settings are changed, you can click to obatin the latest topology.