

Grandstream Networks, Inc.

GDS3725/GDS3726/GDS3727

GDS Manager 2 Guide



GDS Manager 2 Guide

Introduction

GDS Manager 2 is a comprehensive software platform designed to centrally manage and monitor GDS372x facility access systems deployed within the same local network through a unified and user-friendly interface.

It provides an overview of connected devices and alarm events. It enables access control management for device configuration, firmware upgrades, and synchronization of user, group, schedule, and holiday information. It supports user management for managing users associated with connected devices. It supports group management for managing User Groups and Device Groups. It provides access schedule management for configuring schedules and holidays. It offers live video monitoring of connected devices. It provides alarm event monitoring for viewing and managing alarm events triggered by connected devices. It maintains operation logs for tracking management activities performed within the application.

GDS Manager 2 does not support configuration of door opening, alarm, or call settings. These options can only be configured through the device's local web UI or through GDMS SecureAccess Cloud or App.

Product Overview and Key Features

The GDS Manager 2 provides a wide range of features and tools designed to simplify facility access system management and administration. The key features of the GDS Manager 2 include:

- Batch firmware upgrade support without requiring direct interaction with each individual device.
- Device discovery and centralized management through manual addition or local network scanning.
- Centralized monitoring and visibility of connected devices, application activity, alarm events, and operation logs.
- User and group management with configurable access permissions.
- User management through manual entry, import, and Quick enrollment using a USB RFID Card Reader.
- Flexible user-to-device association for individual users or groups.
- Schedule-based access control for defining authorized door access timing.
- Provides live video preview and alarm linkage functionality.

Installation and Access

The GDS Manager 2 is available for download and installation on Windows operating systems. It requires a 64-bit version of Windows 10 or later.

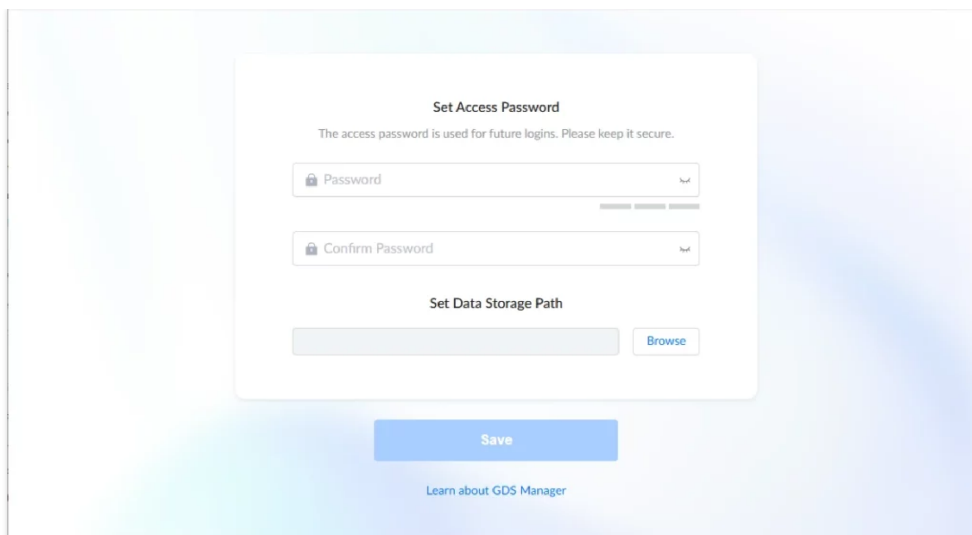
Download and install the GDS Manager 2 package by pressing the link below:

[Download GDSManager2 Software v1.1.16](#)

Access the GDS Manager 2

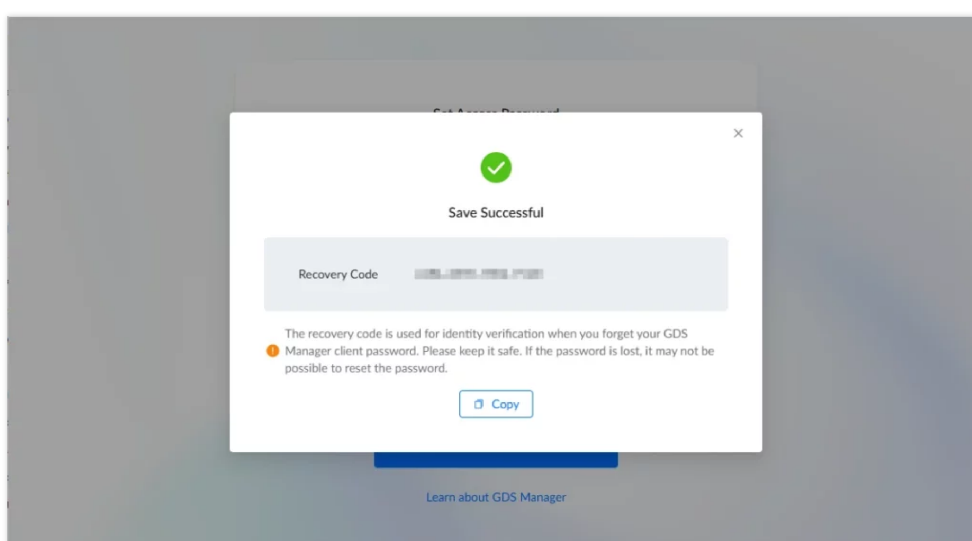
After downloading and installing the application, follow the instructions below to complete the initial setup and log in to GDS Manager 2:

- Launch the application and set an **Access Password**, then re-enter it to confirm.
- Specify the storage path for the application data, then click **Save**.



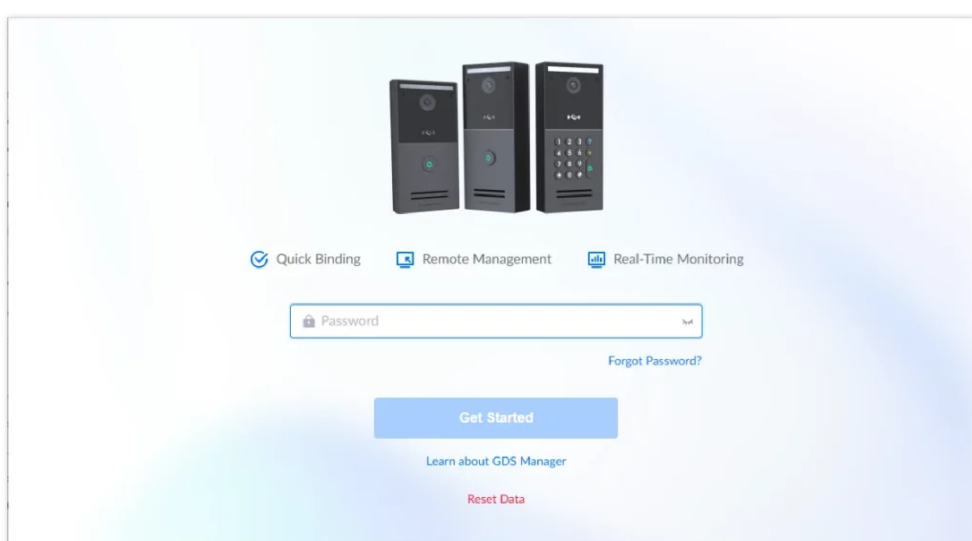
GDS Manager 2 → Set Access Password

- Copy the generated **Recovery Code** and store it securely.



GDS Manager 2 → Copy Recovery Password

- On the login interface, enter the configured **Access Password** to log in to the application.



GDS Manager 2 → Login

Reset Password

If the configured **Access Password** is forgotten, the previously generated **Recovery Code** can be used to reset it by following the steps below:

- On the login interface, click **Forgot Password?**.
- On the Password Reset interface, enter the **Recovery Code**, then set and confirm the new password, and click **Save**.
- On the login interface, enter the new password to regain access to the application.

GDS Manager 2 → Reset Access Password

Important

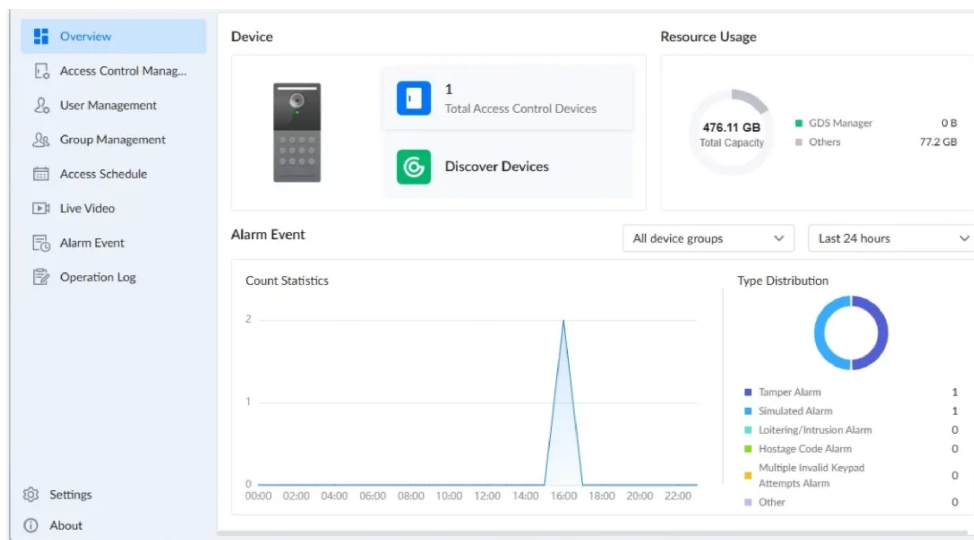
- By default, entering an incorrect access password more than **5 times within 5 minutes** will result in a **15-minute logout**.
- Access can be restored using the Recovery Code if the access password is lost; however, if the code is also lost, access to the application and its data will be permanently lost.
- The Access Password and Recovery Code must be stored securely. A new Recovery Code is generated whenever the access password is changed.

Application Interface Overview

The application interface is structured into eight main functional tabs, in addition to the Settings and About sections. This layout provides users with an overview of the system and a centralized workspace to efficiently manage devices, users, access control, scheduling, live monitoring, alarms, and system operation records. Detailed information about each section is provided below.

Overview

The **Overview** interface provides a centralized dashboard that gives users a quick summary of system status, device activity, storage usage, and alarm event statistics. It presents key information through interactive panels and charts, enabling efficient real-time monitoring of access control devices and system resources, as shown below:



GDS Manager 2 → Overview

Device

Displays a quantitative overview of devices and provides quick access to Device Discovery and Access Control Management for simplified monitoring and management.

- **Total Access Control Devices:** Displays the total number of configured access control devices and redirects to Access Control Management.
- **Discover Devices:** Opens the Discover Devices window in Access Control Management.

Resource Usage

Displays the total capacity of the storage path specified by the client application and the current percentage utilized by GDS Manager 2. This section presents data in chart form, intuitively illustrating the storage consumed by recorded events, snapshots, and other access control data.

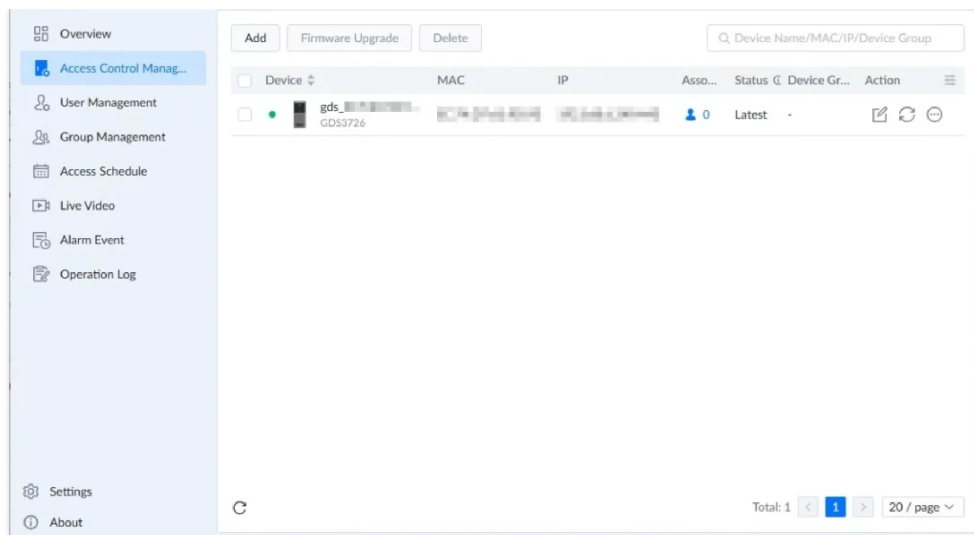
Alarm Event

Displays alarm event statistics for a selected device, device group, or all device groups within a selected time range, including the last 24 hours, last 7 days, or last 30 days.

- **Count Statistics:** Displays a timeline view of recorded alarm events.
- **Type Distribution:** Displays the distribution of alarm event types in a chart format, visualizing the proportion of each alarm type.

Access Control Management

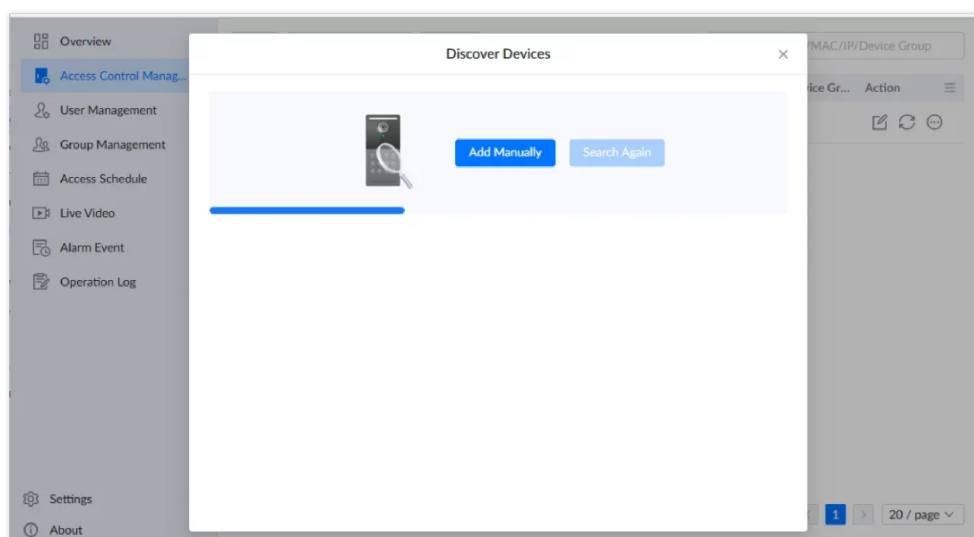
The **Access Control Management** interface provides centralized management and monitoring of connected access control devices. It enables users to add, delete, search, refresh, and manage devices, perform bulk firmware upgrades, and monitor device status and related information through the interface shown below:



GDS Manager 2 → Access Control Management

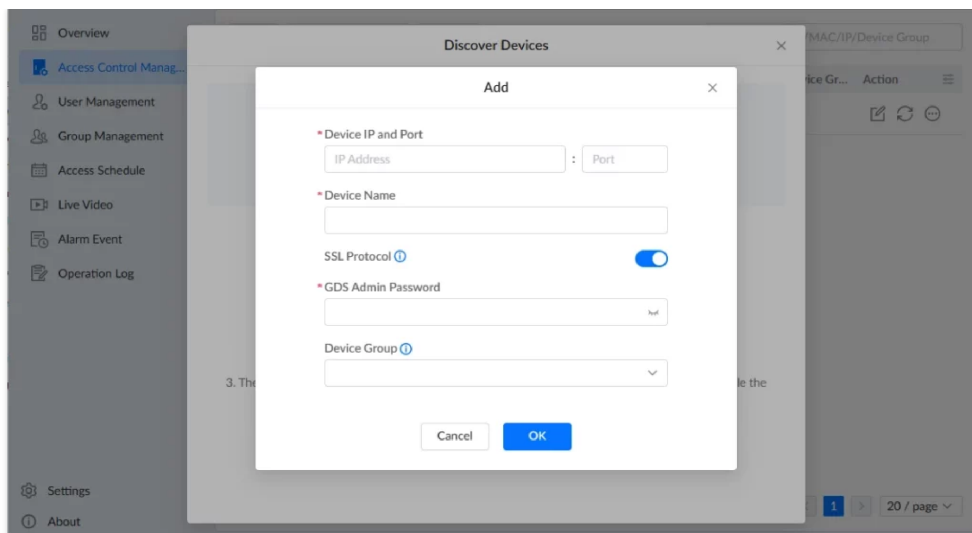
Add a Device

Devices can be added by pressing **Add**, which opens the **Discover Devices** window, where discovered devices can be added automatically or manually by pressing **Add Manually**.



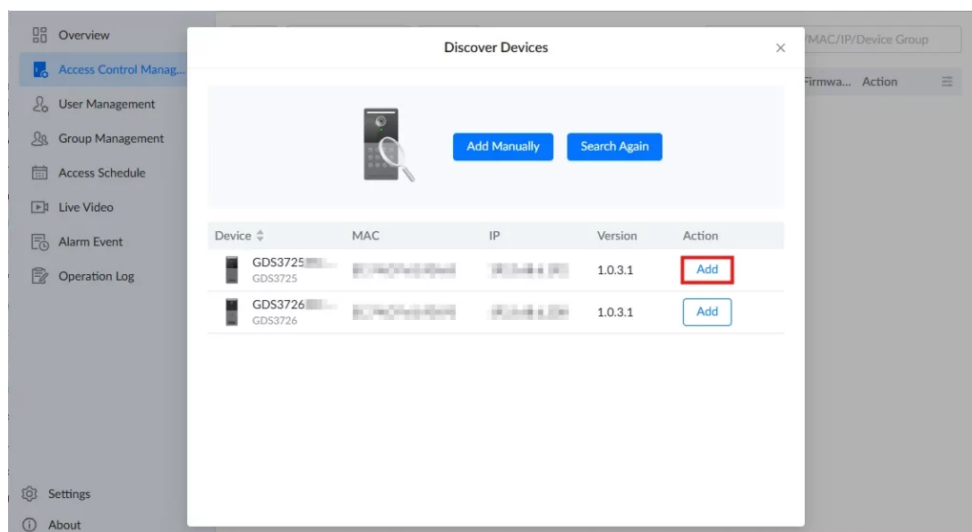
GDS Manager 2 → Access Control Management → Discover Devices

- Devices can be added manually by following the steps below:
 - Select **Add Manually** in Discover Devices
 - Specify the device's IP Address and Port Number.
 - Enter the device's Name.
 - Enable or disable the SSL protocol. When enabled, connections between the application and the devices are encrypted and transmitted through HTTPS.
 - Enter the device's Admin Password.
 - Assign the device to a Device Group.
 - Press **OK**.

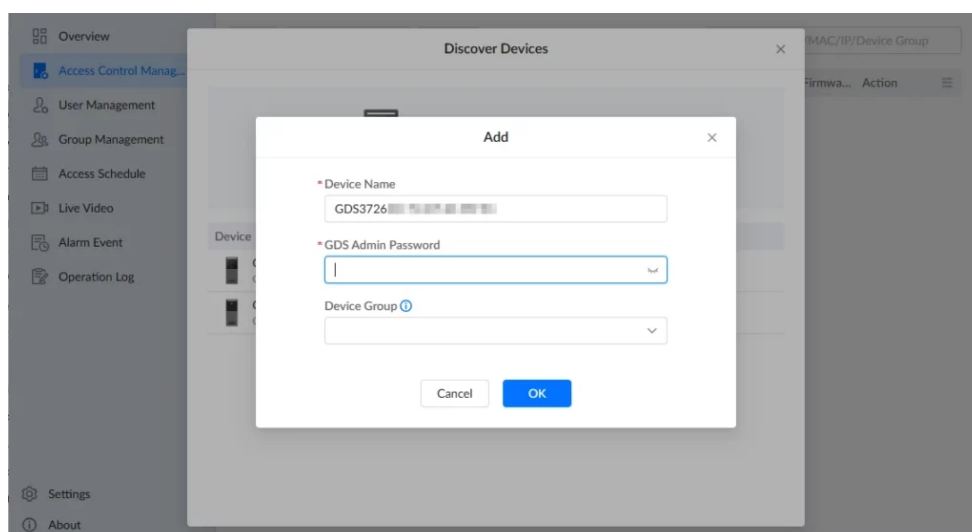


GDS Manager 2 → Access Control Management → Add Device Manually

- Alternatively, devices can be added using the Search tool by following the steps below:
 - Select **Add** on the target device.
 - Enter the device's Admin Password.
 - Assign the device to a Device Group, if applicable.
 - Press **OK**.



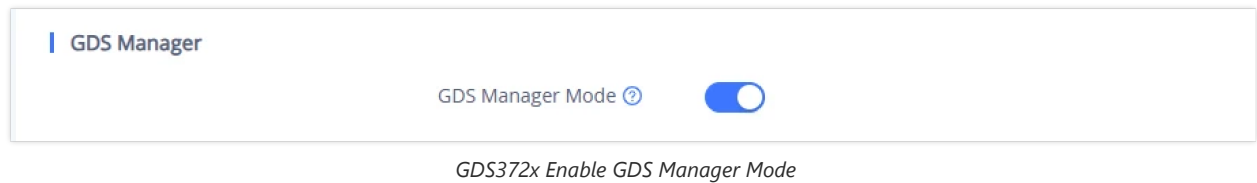
GDS Manager 2 → Access Control Management → Discovered Devices



GDS Manager 2 → Access Control Management → Add Discovered Device

Note

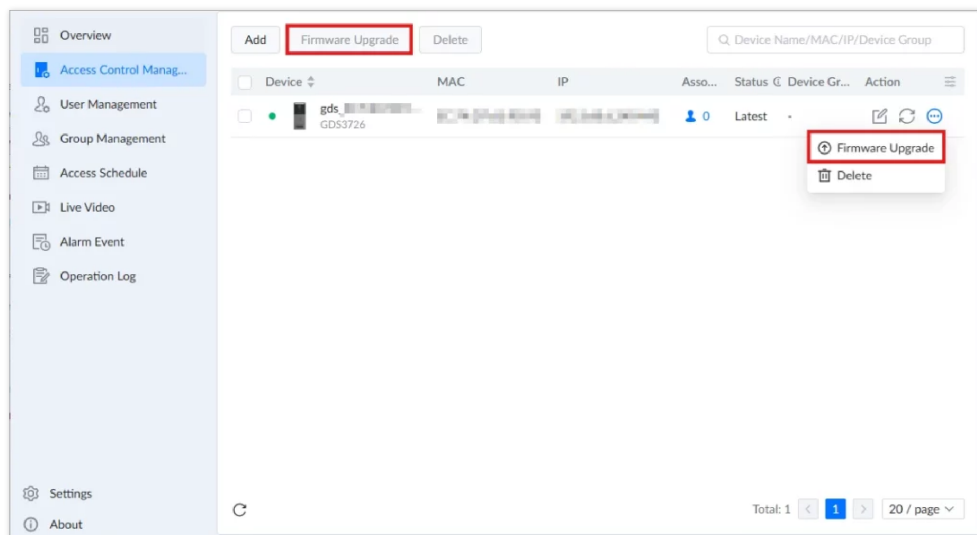
- Before adding a device to GDS Manager 2, ensure that **GDS Manager Mode** is enabled on the device. For example, on the GDS372x series, navigate to **Access Control Settings** → **Basic Settings** → **Access Control Settings** → **GDS Manager** and enable the toggle.
- If GDS Manager Mode is not enabled, the device will not be detected during device discovery in the GDS Manager 2 application.



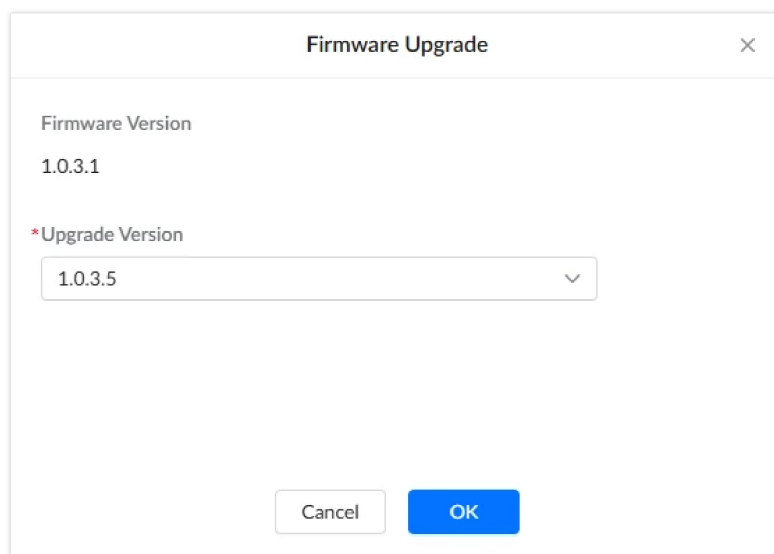
Upgrade a Device

Users can upgrade device firmware for selected devices or all devices in bulk by selecting the target devices and clicking **Firmware Upgrade**. Upgrades can also be initiated for an individual device by clicking the device's three-dot menu and selecting **Firmware Upgrade**. The upgrade window displays the current firmware version and provides a drop-down list of firmware files that have been uploaded to the application for selection.

For more information about uploading firmware files, refer to the [Firmware Upload](#) section.



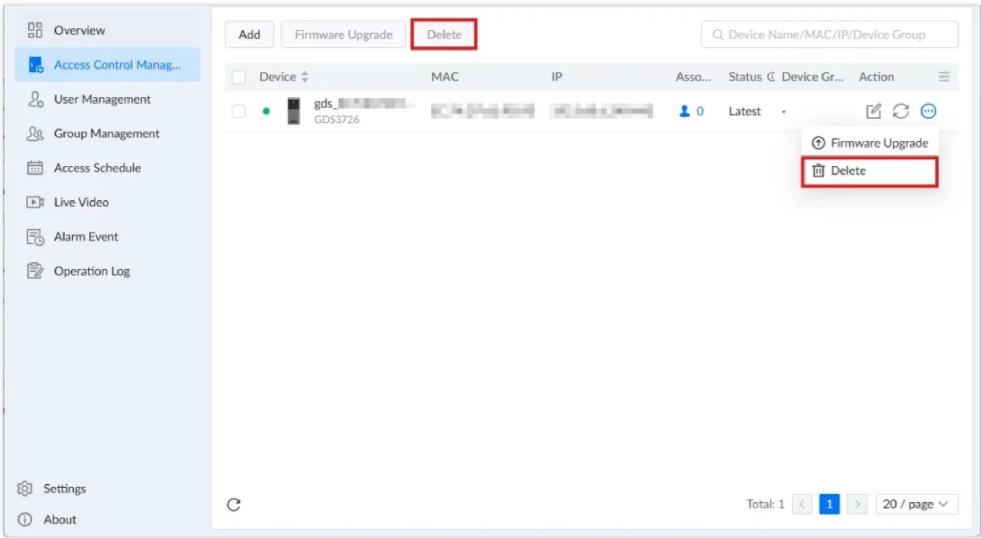
GDS Manager 2 → Access Control Management → Firmware Upgrade



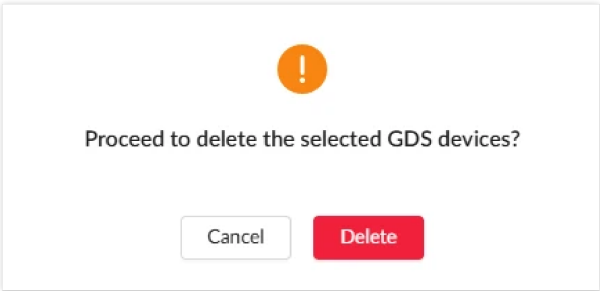
GDS Manager 2 → Access Control Management → Firmware Version

Delete a Device

Users can delete selected devices or all devices in bulk by selecting the target devices, clicking **Delete**, and confirming the deletion. Individual devices can also be deleted by clicking the device’s three-dot menu and selecting **Delete**.

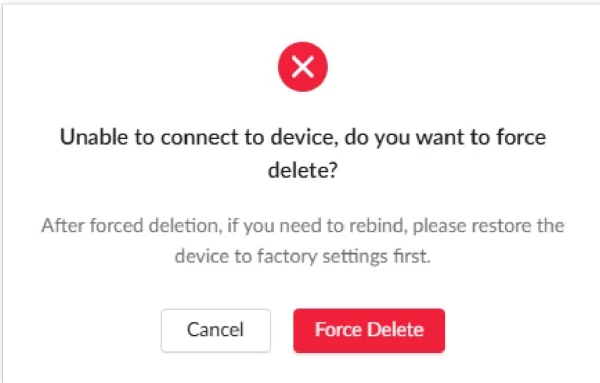


GDS Manager 2 → Access Control Management → Delete Device



GDS Manager 2 → Access Control Management → Confirm Deletion

Offline devices must be **Force Deleted**. After force deletion, the device must be reset to factory settings before it can be re-added to GDS Manager 2.



GDS Manager 2 → Access Control Management → Force Delete Device

Devices

Device	Displays the name of the device.
MAC	Displays the MAC address of the device.
IP	Displays the IP address and port number of the device.
Associate User	Displays the user associated with the device.

Status	Displays the current status of the device.
Device Group	Displays the Device Group assigned to the device.
Firmware Version	Displays the current firmware version of the device.
Action	Provides management actions for the selected device. The available actions include: ● Edit: Modify the device IP address, port number, device name, SSL setting, Admin Password, and assigned Device Group. ● Sync Information: Provides two synchronization methods between the GDS Manager 2 and connected GDS devices: Push user/schedule information to GDS devices: Pushes user information, schedules and holidays information, or both from the GDS Manager 2 to the selected GDS devices. Retrieve the latest user/schedule information from GDS devices: Pulls user information, schedules and holidays information, or both from the selected GDS devices to the GDS Manager 2. ● More: Access additional actions, including Firmware Upgrade and Delete for the selected device.

Access Control Management Controls

The interface provides tools that assist users in managing and navigating device data:

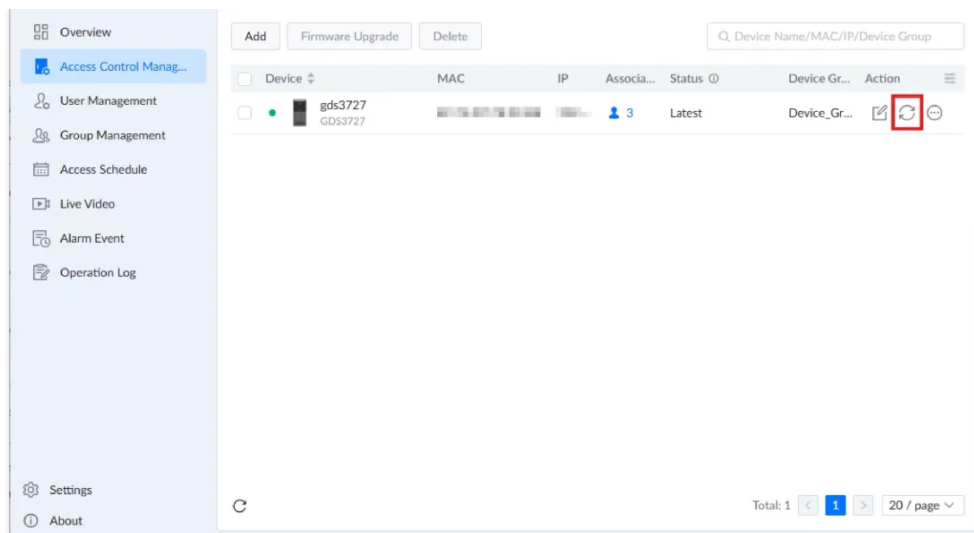
- **Search Bar:** Allows users to search for specific devices within the device list by Name, MAC, IP or Device Group.
- **Refresh Icon:** Updates the device list and device information.

Synchronizing and Pushing Configuration to Devices

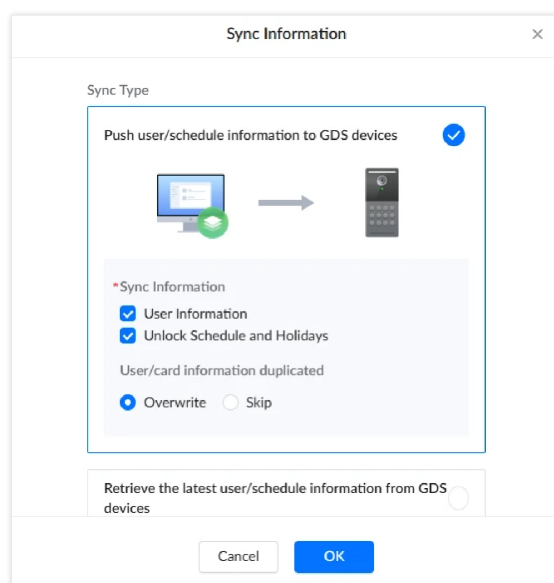
GDS Manager 2 supports synchronizing user information, schedules, and holidays between the application and managed GDS devices. Users can either push information from GDS Manager 2 to selected devices or retrieve the latest information from devices and import it into GDS Manager 2.

To synchronize configuration:

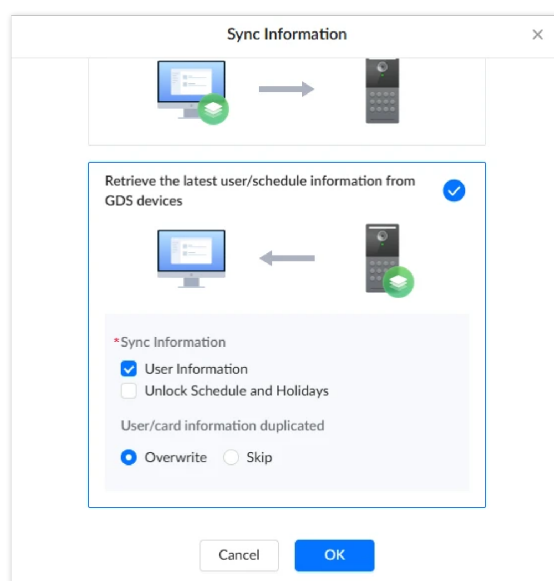
- Click the **Sync** icon on the target device.
- Select one of the following actions:
 - **Push User/Schedule Information to GDS Devices:** Pushes configurations from GDS Manager 2 to the selected GDS devices.
 - **Retrieve the Latest User/Schedule Information from GDS Devices:** Pulls configurations from the selected GDS devices and imports them into GDS Manager 2.
- Select the information to synchronize by choosing one or both of the following options:
 - User Information
 - Unlock Schedules and Holidays
- Choose whether duplicated user or card information should be **overwritten** or **skipped**.
- Click **OK** to start the synchronization process.



GDS Manager 2 → Sync Information



GDS Manager 2 → Sync Information → Push Information to GDS Devices



GDS Manager 2 → Sync Information → Retrieve Information from GDS Devices

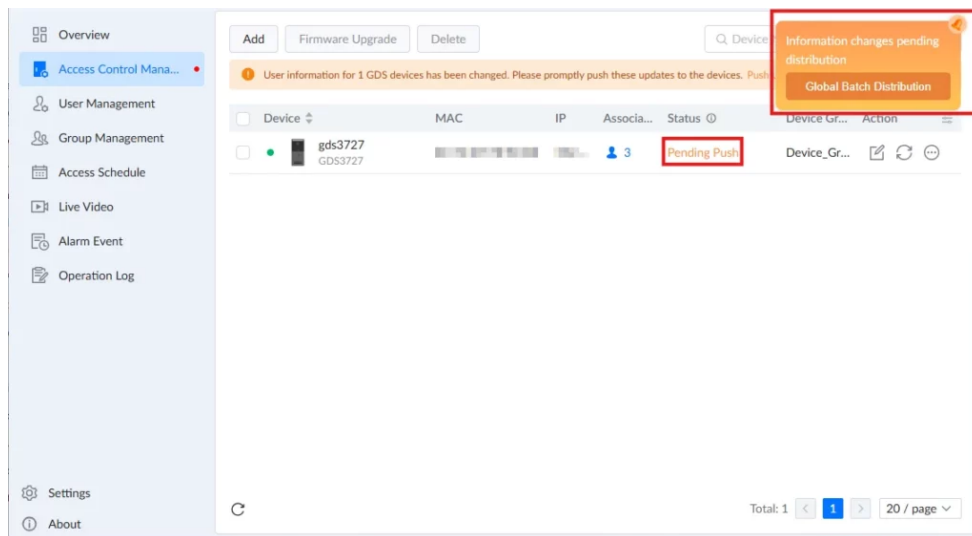
Note

Synchronizing schedules and holiday information from a GDS device to the GDS Manager 2 will update the corresponding configuration on all other synchronized devices. Use this option with caution.

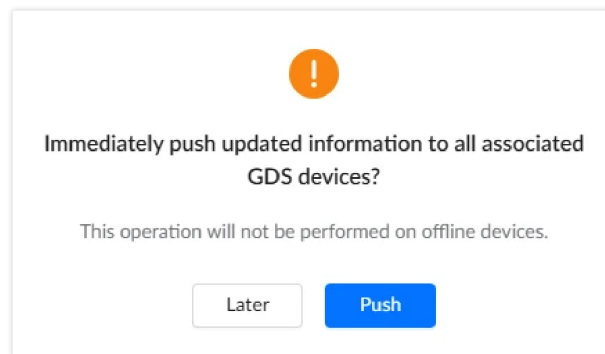
After configuration changes are made in GDS Manager 2, a notification is displayed, and the device status changes to **Pending Push**. This status indicates that the changes have not yet been synchronized to the device.

To push the configuration to the devices:

- Click the **Push** notification.
- Click **Push** to apply the pending configuration changes to the devices.
- Once the process is complete, the device status will be updated from **Pending Push** to **Latest**.



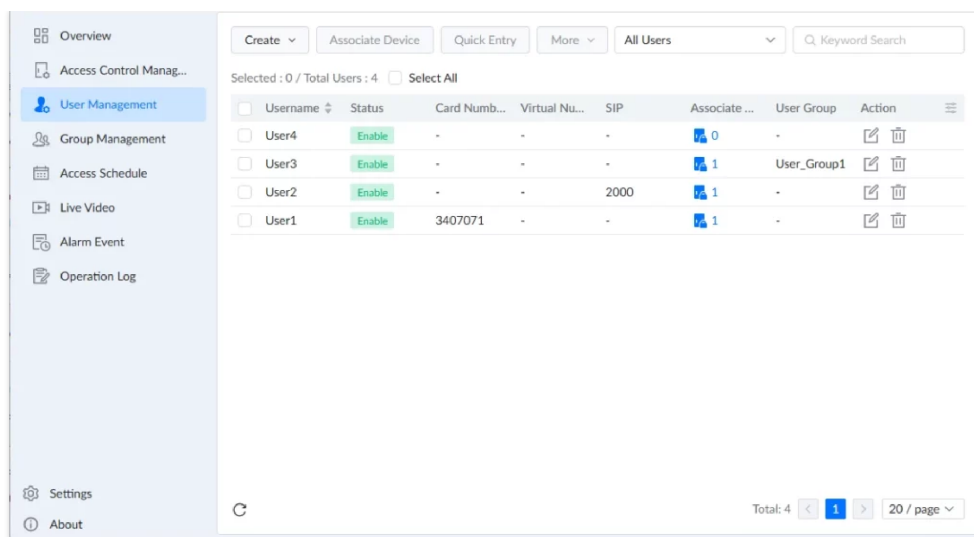
GDS Manager 2 → Push Configuration



GDS Manager 2 → Confirm Push

User Management

The **User Management** interface provides centralized administration of user profiles and access credentials within the system. It enables users to create, import, configure device group access permissions, and manage device associations. Users can also be maintained through batch operations, quick enrollment, filtering options, and additional functions such as batch configuration, export, and deletion, ensuring efficient user management across connected devices and device groups, as shown below:



GDS Manager 2 → User Management

Create a User

Users can be created by pressing **Create**, either manually using **Create User** or **Batch Import** via a CSV file.

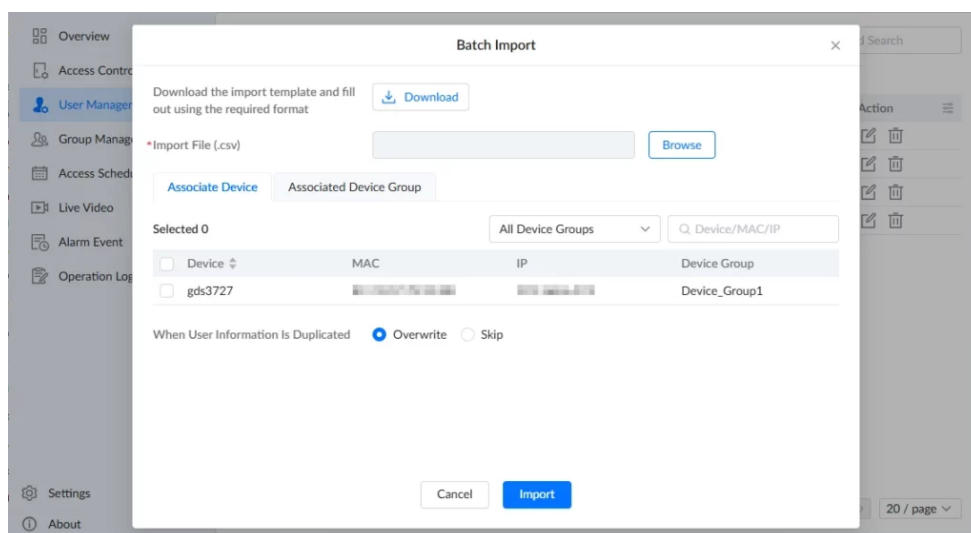
- Users can be created manually by pressing **Create**, then selecting **Create User**, and filling in the required fields documented in the table below. The information can be verified in the Overview section before clicking **Create** to complete the process.

GDS Manager 2 → User Management → Create User

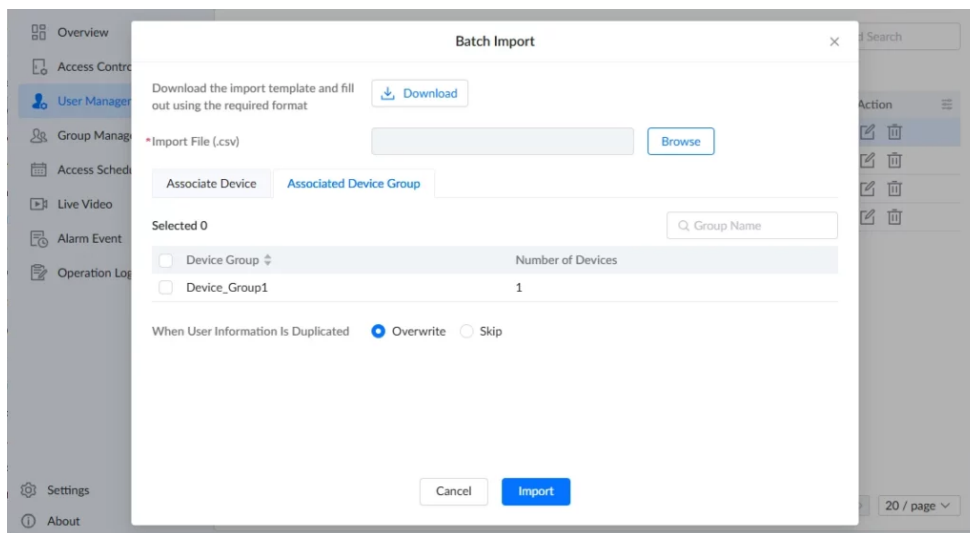
Basic Information	
Username	Define the login/identity of the user (required field).
Full Name	Enter the full name of the user.
Gender	Select the user's gender, the available options are: • General • Female • Male
ID Number	Enter an identifier such as employee number or badge ID.
User Group	Assign the user to a user group for centralized management.
Virtual Number	Define an internal extension used for intercom and internal calling.

SIP	Enter a SIP extension number used for VoIP calling.
Phone Number	Enter the user's phone number.
Card Information	
Card Type	• IC Card • ID Card • Unknown
Card Number	Enter the unique identifier of the access card. It can be obtained via a USB card reader. Note: • If "Enable Compatible with Unencrypted IC Card" is not enabled in the device web UI, non-encrypted IC cards added via the USB card reader will not function. • Card numbers for non-DesFire and non-S50 cards cannot be retrieved via the card reader.
Card Notes	Add additional notes related to the card.
Validity Start Time	Set the card validity start date.
Validity End Time	Set the card validity end date.
Associate Device	
Associate Device	Select one or more devices associated with the user. Filter devices by device group or search by name, MAC address, or IP.
Associated Device Group	Assign the user to a device group.
Access Schedule	Select an access schedule from custom schedules created in the application (up to 50 schedules), or set it to All Day for unrestricted access.
Device Call Number	Specify an account as the device call number or set it to Automatic.

- Users can be imported by pressing **Create**, then selecting **Batch Import**, and uploading the CSV file as documented in the table below. The process is completed by clicking **Import**.



GDS Manager 2 → User Management → Batch Import → Associate Device



GDS Manager 2 → User Management → Batch Import → Associated Device Group

Download	Download the import template and fill it out using the required format.
Import File	Upload the CSV file after filling in the information.
Associate Device	Assign the batch of users to a device.
Associated Device Group	Assign the batch of users to a device group.
When User Information is Duplicated	When user information is duplicated, the following options are available: • Overwrite: Replaces existing user data with the imported data. • Skip: Keeps the existing user data and ignores the imported duplicate.

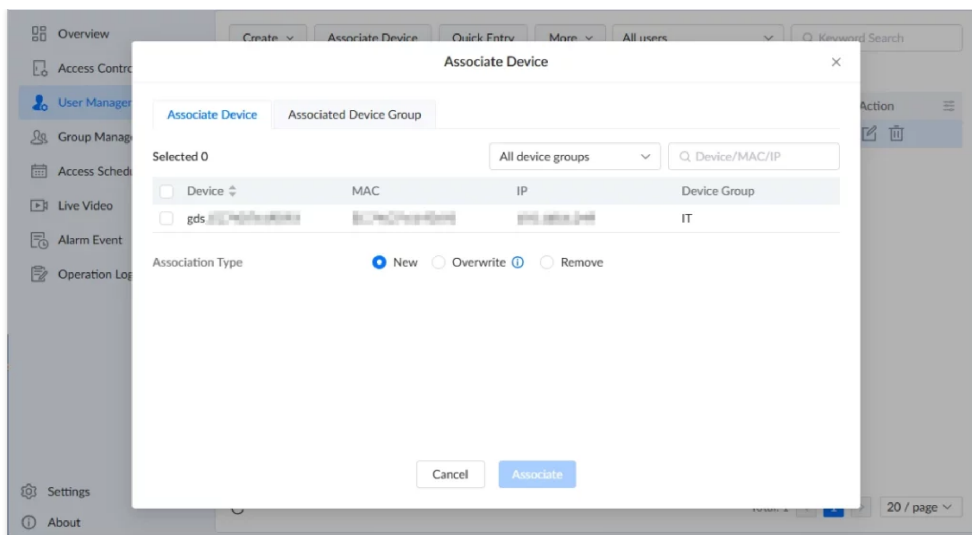
Note

Adding a user to a device group automatically grants access to all devices within that group. However, associating a user with an individual device only grants access to that specific device, even if it belongs to a device group.

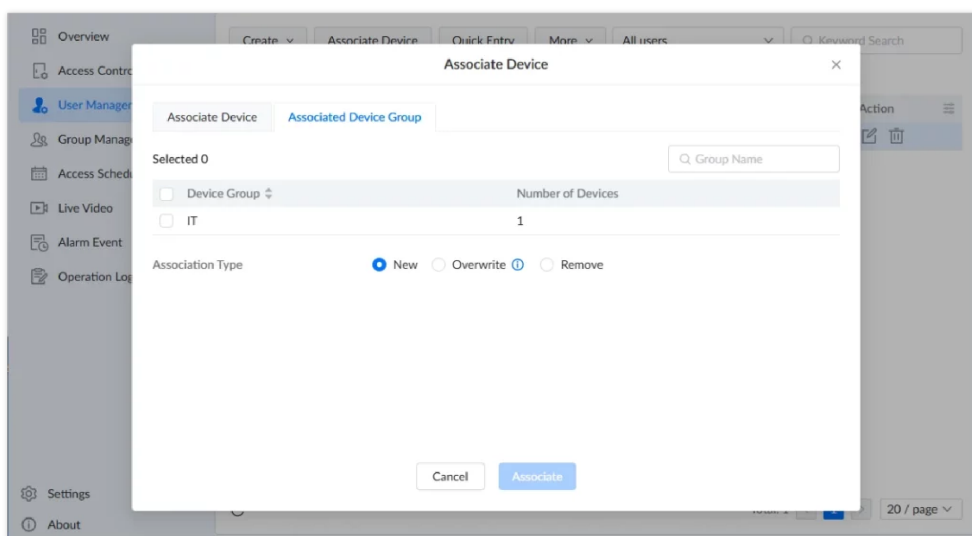
Associate Device

Previously added users can be associated or disassociated from devices and device groups by following the steps below:

- Select the user(s) from the list.
- Press **Associate Device**.
- In the Associate Device window, select the desired device(s) or device group(s).
- Select the association type:
 - **New:** Adds new associations without removing existing ones.
 - **Overwrite:** Removes all existing associations and applies the new selection.
 - **Remove:** Removes the association between the selected device or device group and the user(s).
- Press **Associate**.



GDS Manager 2 → User Management → Associate Device → Associate Device



GDS Manager 2 → User Management → Associate Device → Associated Device Group

Notes

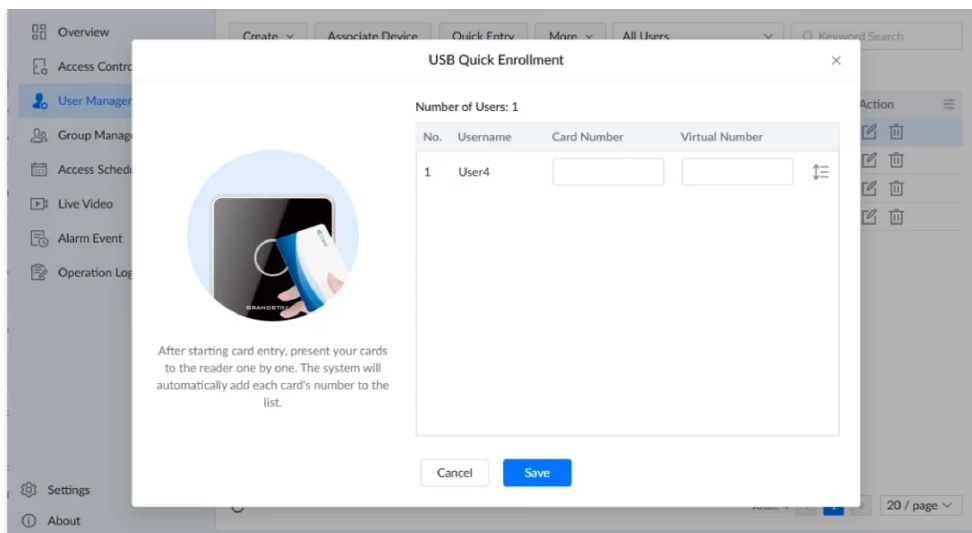
- Users associated with a device via a **User Group** will be displayed in the **Associated Devices** list with an icon indicating that the user belongs to a user group.
- Disassociating a user from a **Device Group** under **Group Management** removes all devices within that group from the user's **Associated Devices** interface.
- Removing a device from a **Device Group** under **Group Management** automatically removes it from the **Associated Devices** interface for all users associated with that device.
- Removing a device that was associated through a device group from the **Associated Devices** interface disassociates the user from the entire device group. Other devices within the same group remain displayed in the **Associated Devices** list.

Quick Entry

Users can use the Quick Entry tool to simplify card assignment using the Grandstream RFID card reader. After connecting the card reader to the computer, enrollment is performed by swiping the card. The scanned cards are automatically added to the system.

USB Quick Entry supports the following features (can be executed in parallel):

- **Bind existing user cards:** Select existing GDS Manager users. Drag and drop users to reorder them if needed, then swipe cards to bind them to the selected users.
- **Quick add new users:** Swipe cards to automatically create new users and edit their names during the enrollment process.



GDS Manager 2 → User Management → USB Quick Enrollment

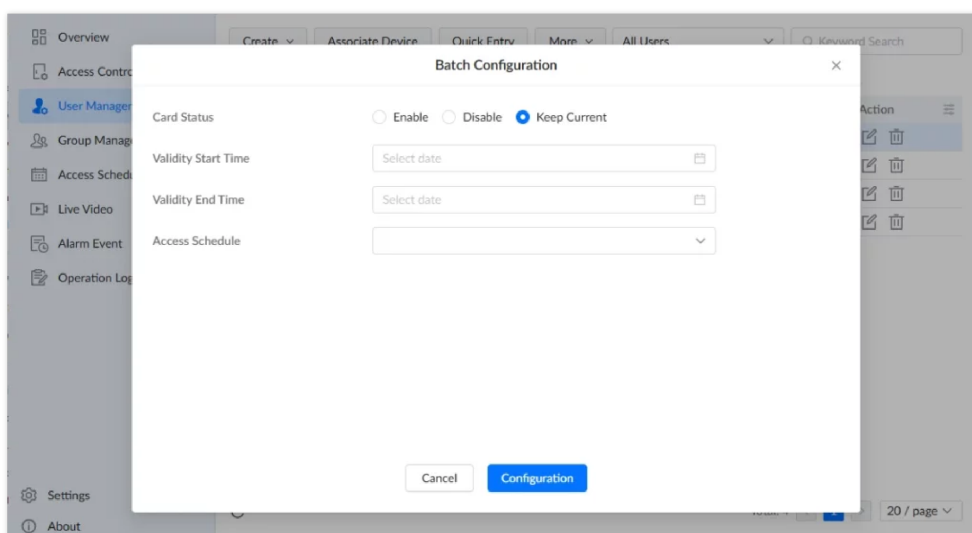
Note

The Grandstream USB RFID Card Reader supports only **125 kHz** RFID cards compatible with the EM4100 or TK4100 format.

More

The More menu provides additional tools for managing users, including batch configuration, data export, and deletion operations, as shown below.

- **Batch Configuration:** Applies bulk changes to multiple users, including:
 - Card Status: Enables, disables, or keeps the current card status.
 - Validity Start/End Time: Sets or modifies the card validity period.
 - Access Schedule: Assigns an access schedule to users for controlled access permissions.



GDS Manager 2 → User Management → More → Batch Configuration

- **Export:** Exports user data for backup, reporting, or external use.
- **Delete:** Deletes selected users from the system.

Users

Username	Displays the username used for login and identification.
Status	Displays the current status of the user account.

Full Name	Displays the full name of the user.
Card Number	Displays the unique identifier of the access card assigned to the user.
Virtual Number	Displays the abbreviated internal extension used for intercom and internal calling.
SIP	Displays the SIP extension number used for VoIP communication.
Associate Device	Displays the total number of devices linked to the user and allows editing via the icon.
User Group	Displays the user group assigned to the user for centralized management.
Validity Start Time	Displays the start date of the card validity period.
Validity End Time	Displays the end date of the card validity period.
Action	Allows editing of user details, including basic information, card information, and associated devices.

User Management Controls

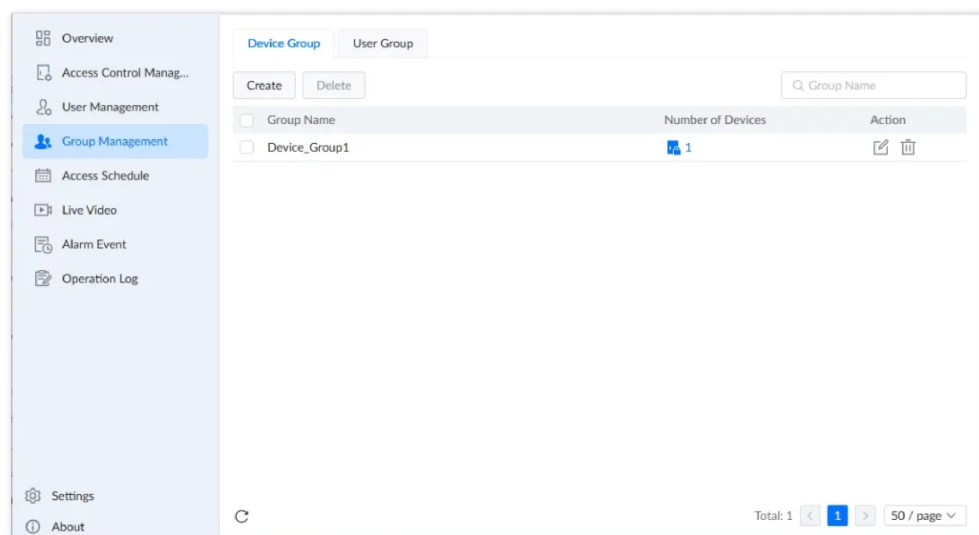
The interface provides tools that assist users in managing and navigating the user data:

- **Filter by Users:** Filters the list based on user association status, including all users, associated users, or users not associated with devices.
- **Search Bar:** Allows searching for users by username, name, card number, virtual number, SIP account, etc.

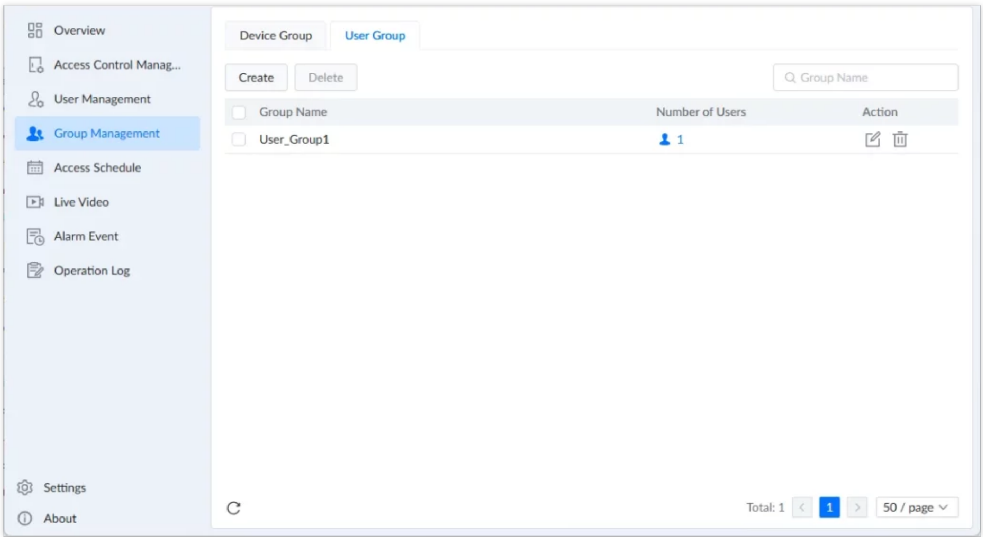
Group Management

The **Group Management** interface provides centralized management of device groups and user groups, allowing users to organize devices and users for simplified administration and access management as shown below:

- **Create Device Group:** Creates a new device group by specifying the **Group Name** and selecting the devices to be added.
- **Delete Device Group:** Deletes the selected device group from the system.



- **Create User Group:** Creates a new user group by specifying the **Group Name** and selecting the users to be added.
- **Delete User Group:** Deletes the selected user group from the system.



GDS Manager 2 → Group Management → User Group

Groups

Device Group	
Group Name	Displays the name of the device group.
Number of Devices	Displays the total number of devices assigned to the group and allows editing by adding or deleting devices from the group.
Action	● Edit: Allows users to edit the device group name. ● Delete: Deletes the device group.
User Group	
Group Name	Displays the name of the user group.
Number of Users	Displays the total number of users assigned to the group and allows editing by adding or deleting users from the group.
Action	● Edit: Allows users to edit the user group name. ● Delete: Deletes the user group.

Group Management Controls

The interface provides tools that assist users in managing and navigating data:

- **Search Bar:** Allows users to search for device groups or user groups by name.

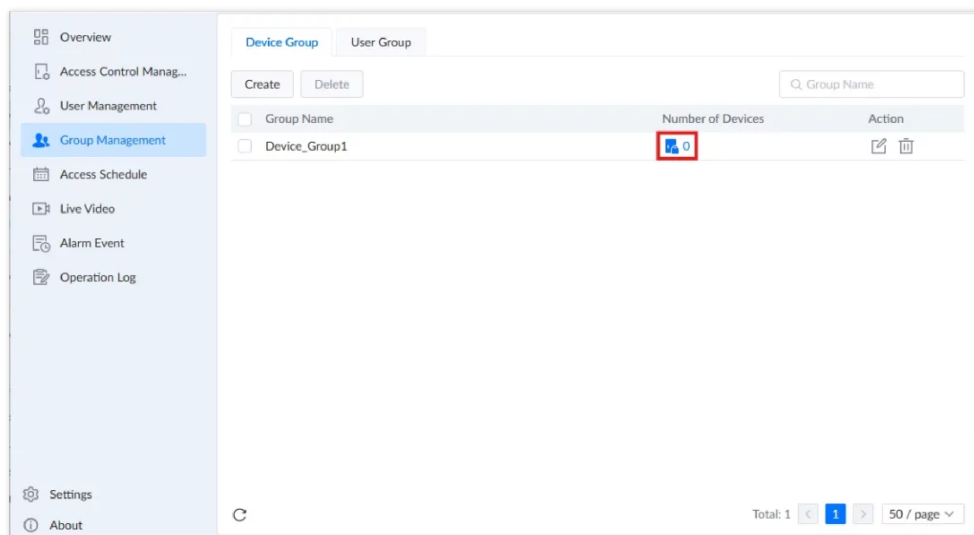
Device Group and User Group Management

Device Groups and User Groups can be managed by adding or removing devices and users, enabling efficient control of group membership and permissions.

Add Devices to a Device Group

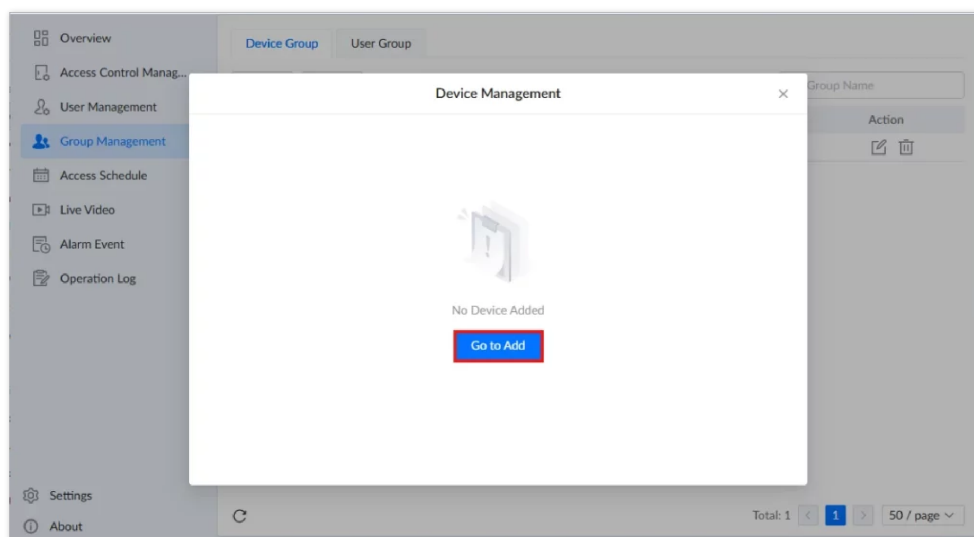
To add devices to a Device Group, follow the steps below:

- Press the **Devices** icon on the target Device Group.



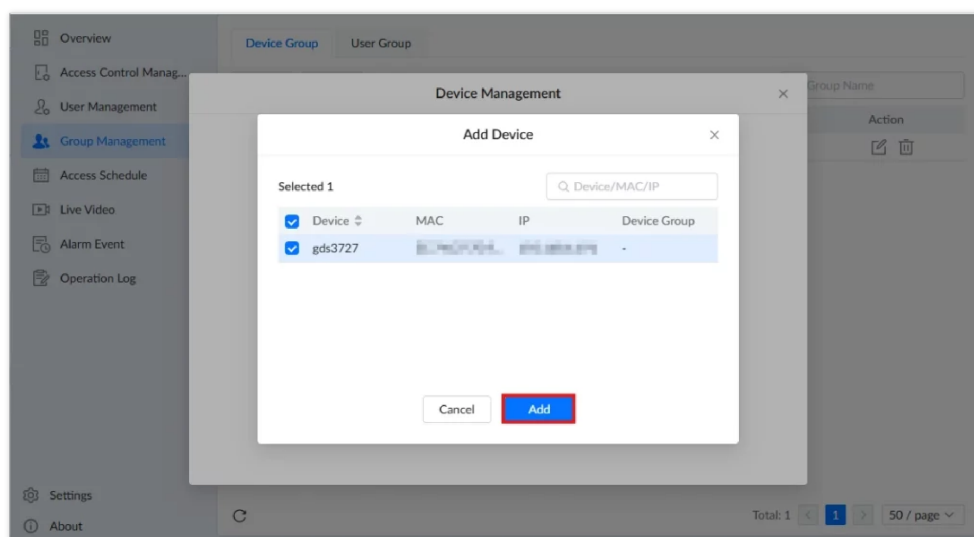
GDS Manager 2 → Group Management → Add Devices

- In Device Management, click **Go to Add** or **Add**.



GDS Manager 2 → Group Management → Add Devices

- Select the devices, then click **Add**.

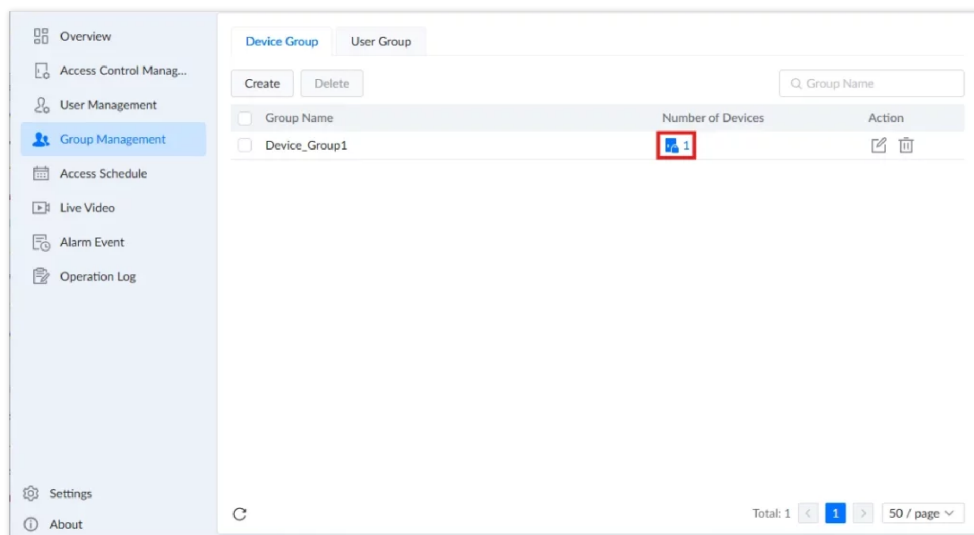


GDS Manager 2 → Group Management → Add Devices

Delete Devices from a Device Group

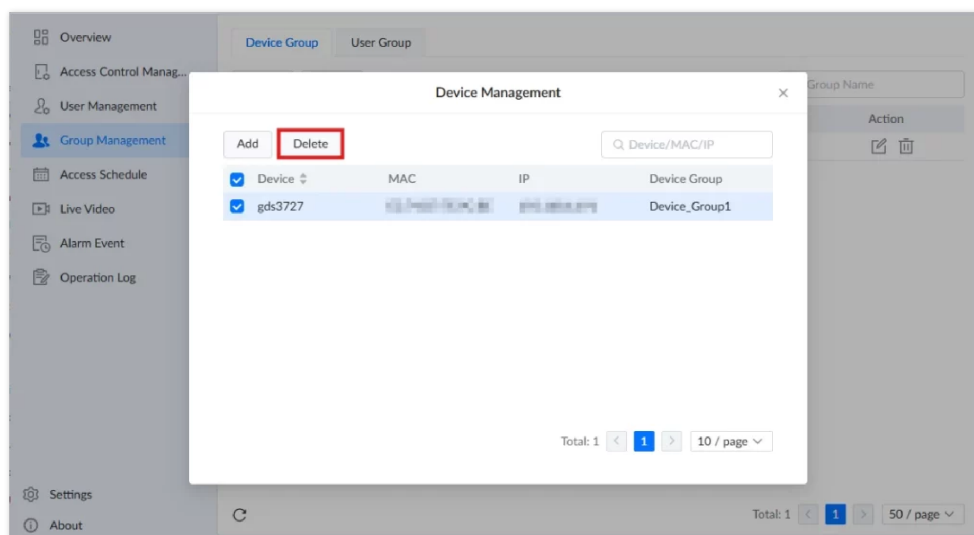
To remove devices from a Device Group, follow the steps below:

- Press the **Devices** icon on the target Device Group.



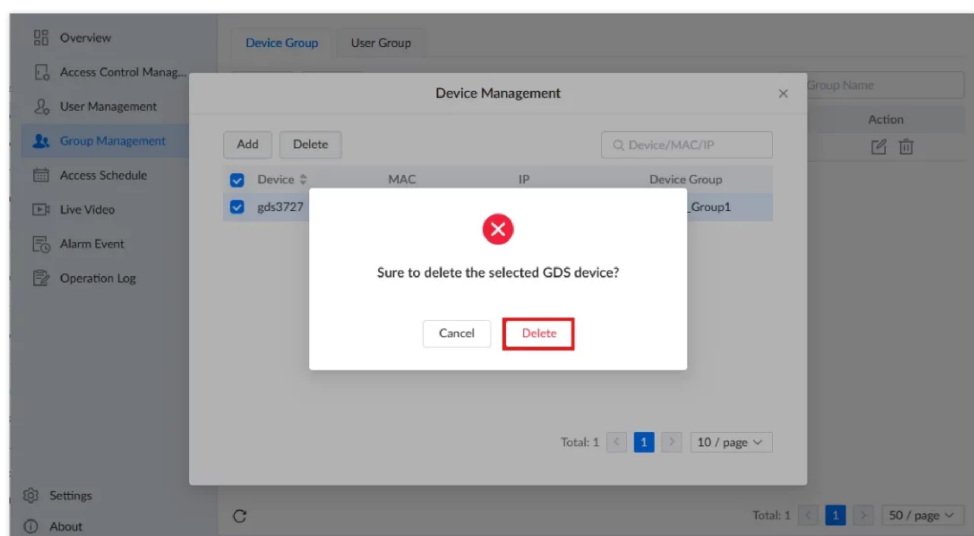
GDS Manager 2 → Group Management → Delete Devices

- In Device Management, select the devices, then click **Delete**.



GDS Manager 2 → Group Management → Delete Devices

- Confirm the deletion.

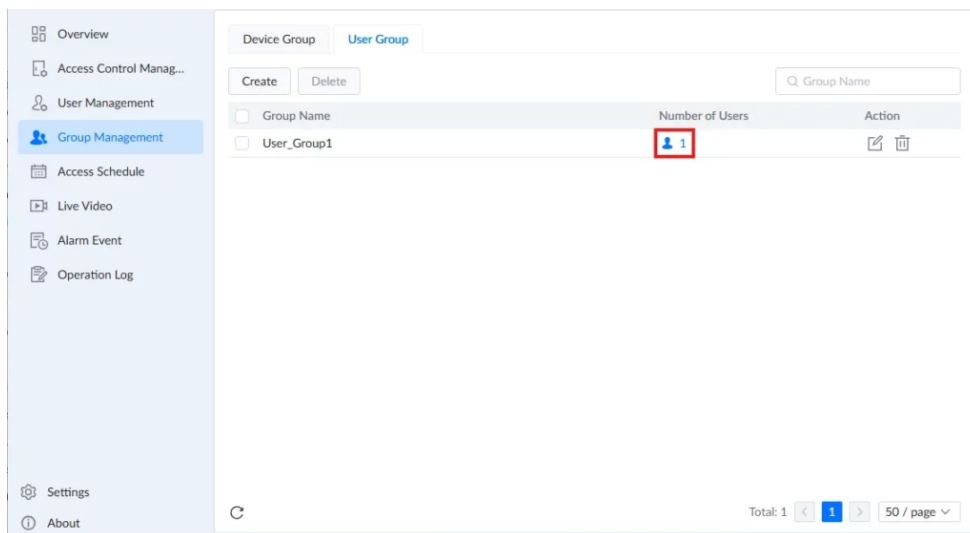


GDS Manager 2 → Group Management → Delete Devices

Add Users to a User Group

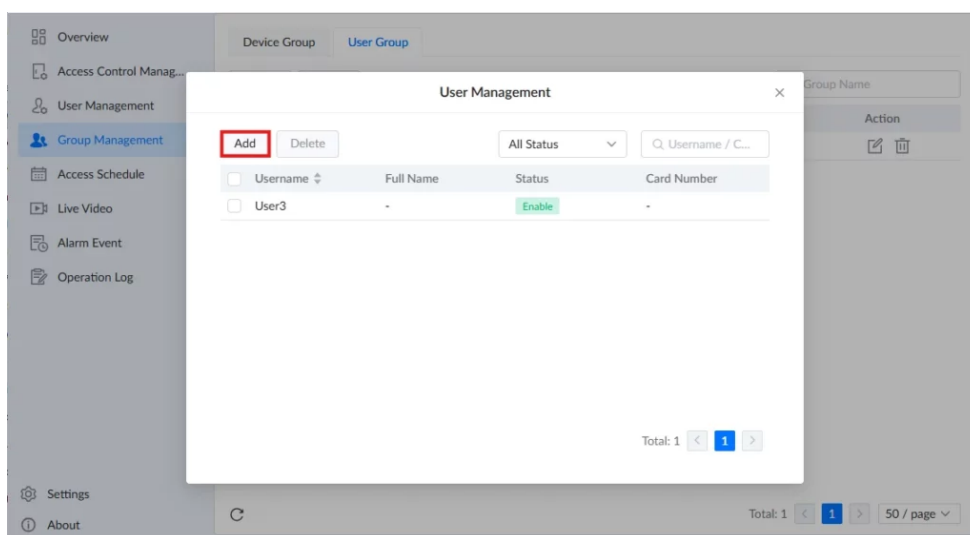
To add users to a User Group, follow the steps below:

- Press the Users icon on the target User Group.



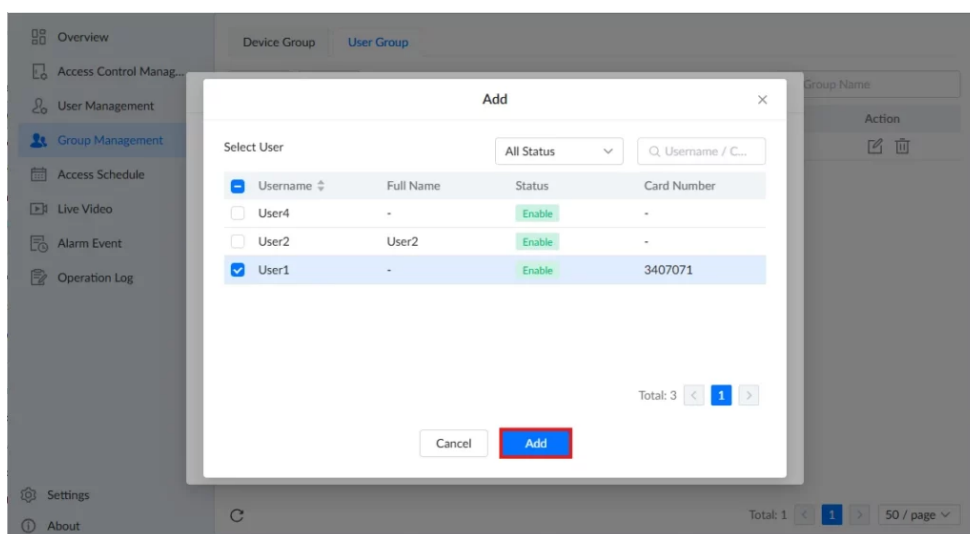
GDS Manager 2 → Group Management → Add Users

- In **User Management**, click **Go to Add** or **Add**.



GDS Manager 2 → Group Management → Add Users

- Select the users, then click **Add**.

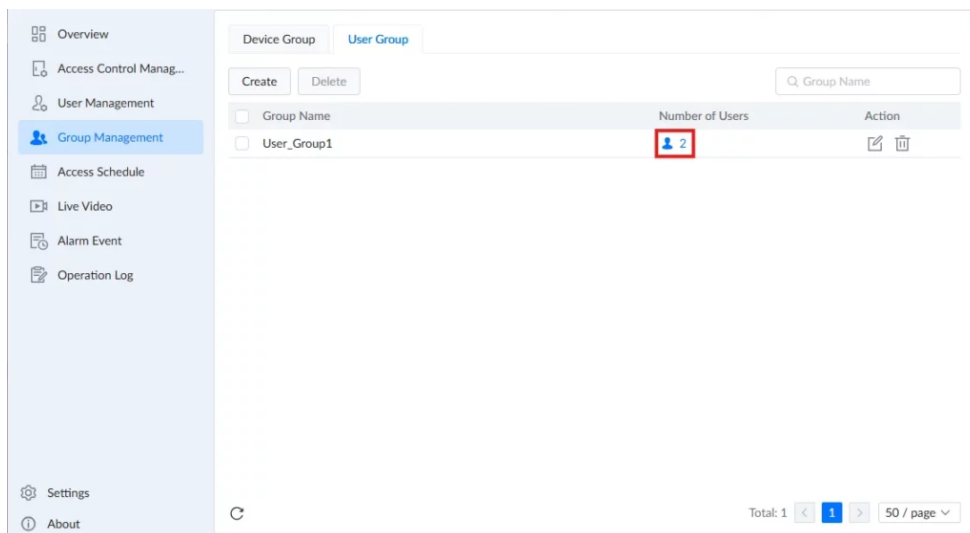


GDS Manager 2 → Group Management → Add Users

Delete Users from a User Group

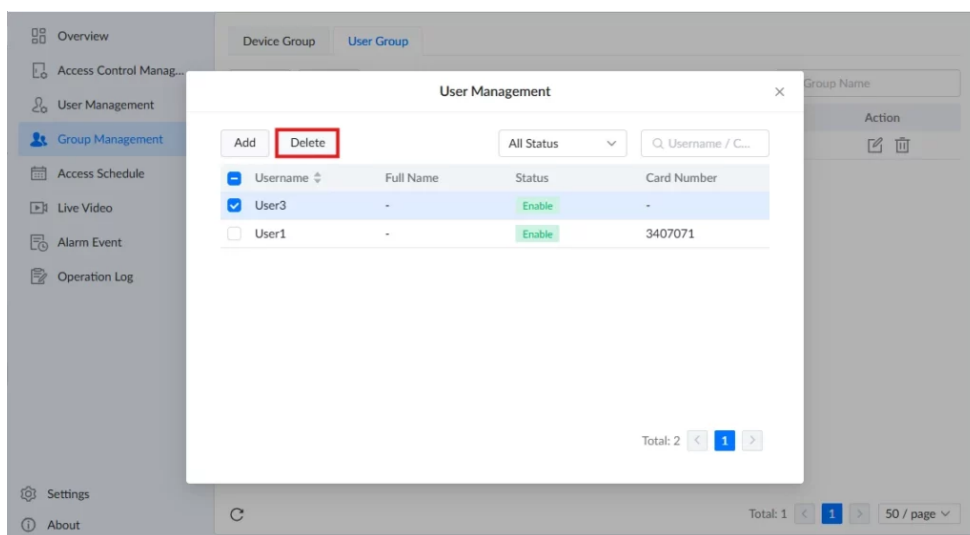
To remove users from a User Group, follow the steps below:

- Press the Users icon on the target User Group.



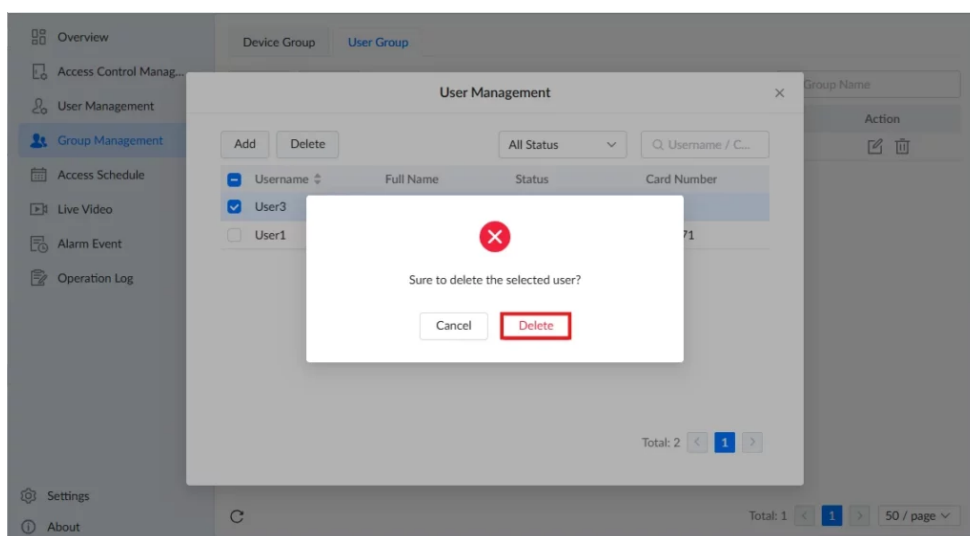
GDS Manager 2 → Group Management → Delete Users

- In **User Management**, select the users, then click **Delete**.



GDS Manager 2 → Group Management → Delete Users

- Confirm the deletion.



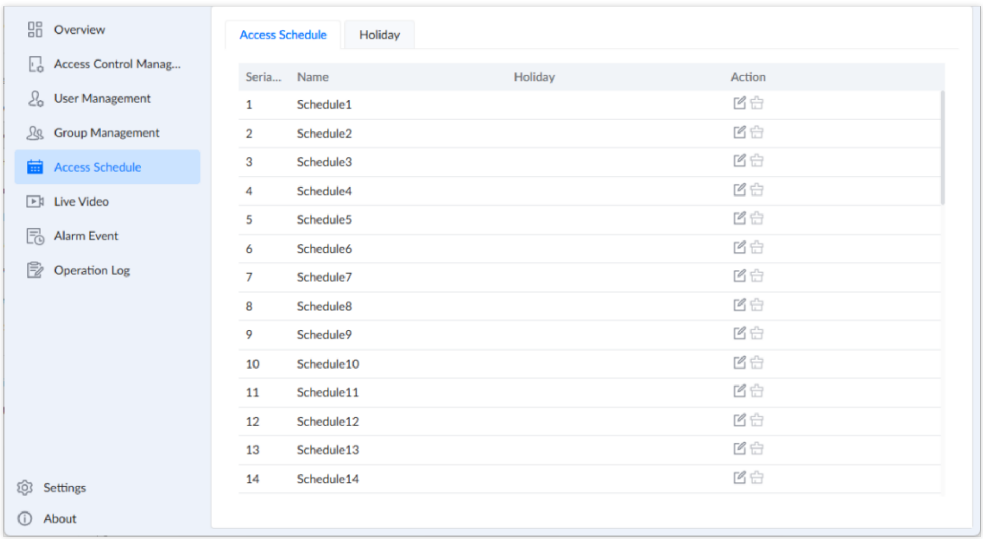
GDS Manager 2 → Group Management → Delete Users

Important

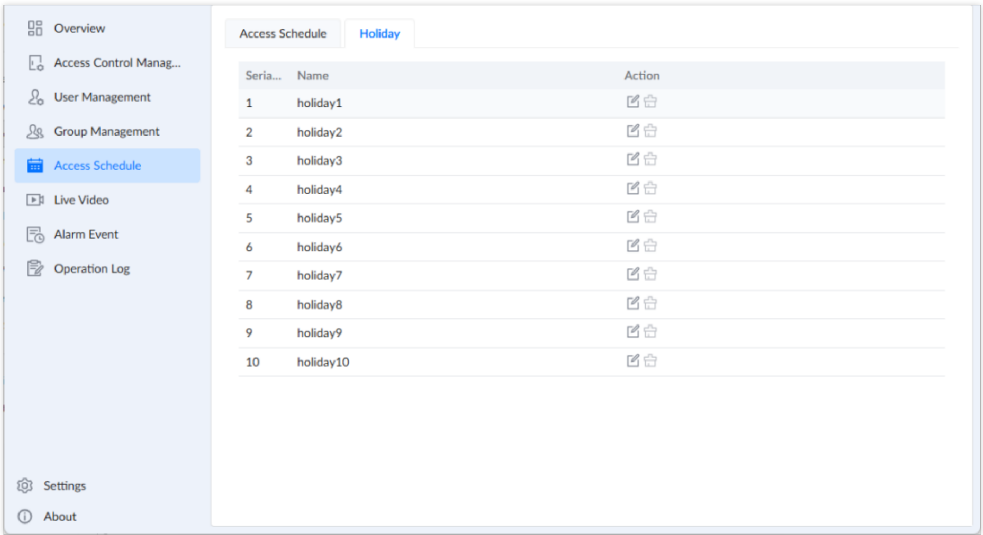
Ensure that changes made in Group Management are pushed to the devices.

Access Schedule

The **Access Schedule** interface provides centralized management of access time profiles and holiday definitions, allowing client users to configure the time periods during which system users can access the access control devices, as shown below:



GDS Manager 2 → Access Schedule → Access Schedule



GDS Manager 2 → Access Schedule → Holiday

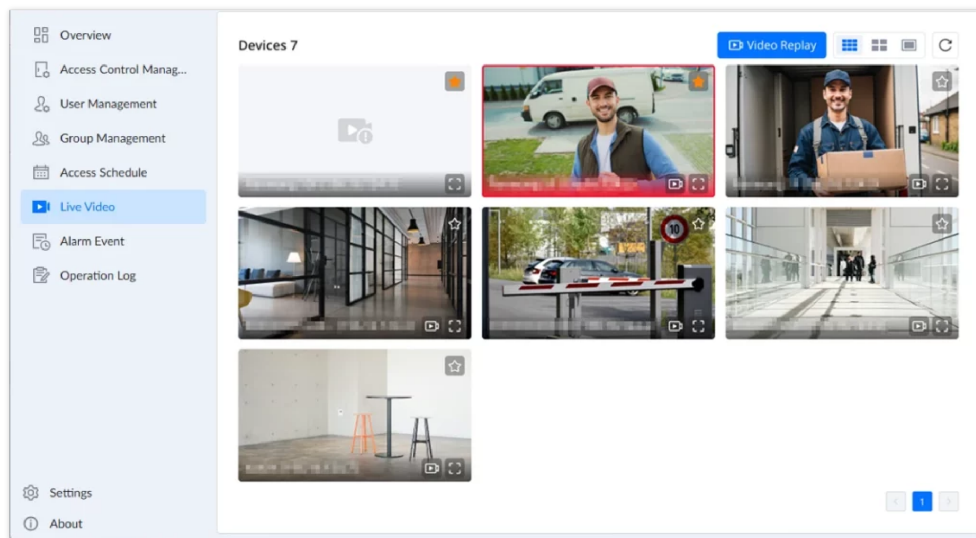
Access Schedules & Holidays

Access Schedule	
Serial Number	Displays the serial number of the access schedule. The application supports up to 50 access schedules.
Name	Displays the name of the access schedule.
Holiday	Displays the holiday assigned to the access schedule.
Action	● Edit: Allows users to edit the schedule name, assigned holiday, and customize the weekly schedule. ● Clear: Removes the access schedule.
Holiday	

Serial Number	Displays the serial number of the holiday entry. The application supports up to 10 holiday entries.
Name	Displays the name of the holiday.
Action	• Edit: Allows users to edit the holiday name and duration, or import holidays by selecting the region/country and year from a list of available holidays. • Clear: Deletes the holiday entry.

Live Video

The **Live Video** interface provides real-time video streaming from connected GDS devices, enabling users to monitor live activity directly from the system, as shown below:



GDS Manager 2 → Live Video

Live Video Controls

The interface provides tools that assist users in managing and navigating live video feeds:

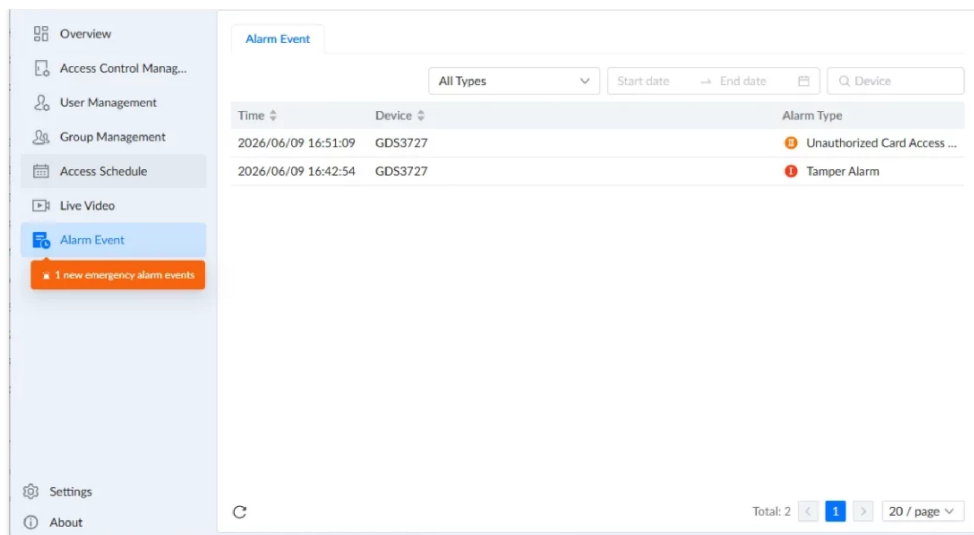
- **Layout:** Allows users to change the layout of the video feed display, adjusting how multiple streams are arranged within the interface.
- **Refresh Icon:** Reloads the live video feed and updates the current stream status.

Notes

- When an alarm is triggered on a device, an alarm notification appears in the left sidebar under the **Live Video** option to alert the user.
- In the **Live Video** interface, the device that triggered the alarm is highlighted, with red, orange, and yellow representing different alarm levels.
- Live feeds can be added to favorites by clicking the star icon in the top-right corner of each video tile.

Alarm Event

The **Alarm Event** interface provides a detailed overview of alarm activity across connected devices, allowing users to monitor and filter security-related events within a selected time range, as shown below:



GDS Manager 2 → Alarm Event

Alarm Events

Time	Displays the date and time when the alarm event occurred.
Device	Displays the name of the device associated with the alarm event.
Alarm Type	Displays the type of alarm event. Available alarm types include: • All • Intrusion/Loitering Alarm • Hostage Alarm • Tamper Alarm • Unauthorized Access Alarm • SD Card Alarm • Multiple Remote Unlock Password Error Alarm • Safe Room Alarm • Door Open Timeout Alarm • High Temperature Alarm • Multiple Invalid Keypad Attempts Alarm • Access Alarm Beyond Schedule • Digital Input Alarms • Simulated Alarm

Alarm Event Controls

The interface provides tools that assist users in managing and navigating the alarm data:

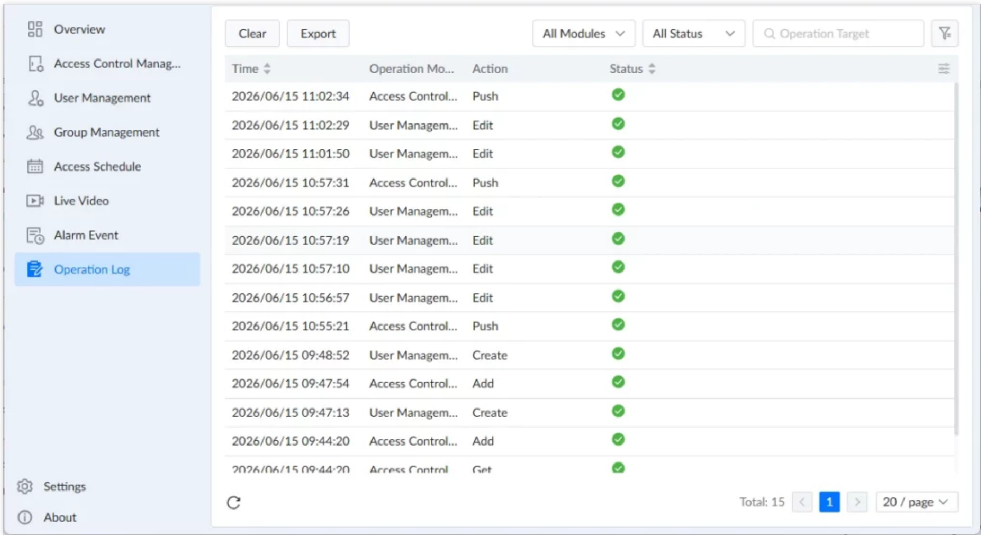
- **Alarm Type Filter:** Filters alarm events based on the selected alarm type.
- **Start & End Dates:** Filters alarm events within a defined time range by selecting the start and end date.
- **Search by Device:** Allows searching alarm events by device name.

Operation Log

The **Operation Log** interface provides a centralized record of system activities, displaying all actions performed within the application for monitoring, auditing, and troubleshooting purposes. It allows users to filter logs by module, status, and target, as well as clear or export log data, as shown below:

- **Clear:** Deletes all operation logs from the system.

- **Export:** Exports operation logs for external use, reporting, or troubleshooting.



GDS Manager 2 → Operation Log

Operation Logs

Time	Displays the date and time when the operation was performed.
Operation Module	Displays the application module related to the operation, such as User Management, Access Control Management, or Holiday.
Action	Displays the type of operation performed, including configuration synchronization, upgrades, creation, deletion, modification, and other management actions.
Target	Displays the target associated with the operation, such as a user, device, or device group.
Status	Displays the operation status. Successful operations are shown in green , while failed operations are shown in red . Additional failure information can be viewed by hovering over the status icon.

Operation Log Controls

The interface provides tools that assist users in managing and navigating the operation log:

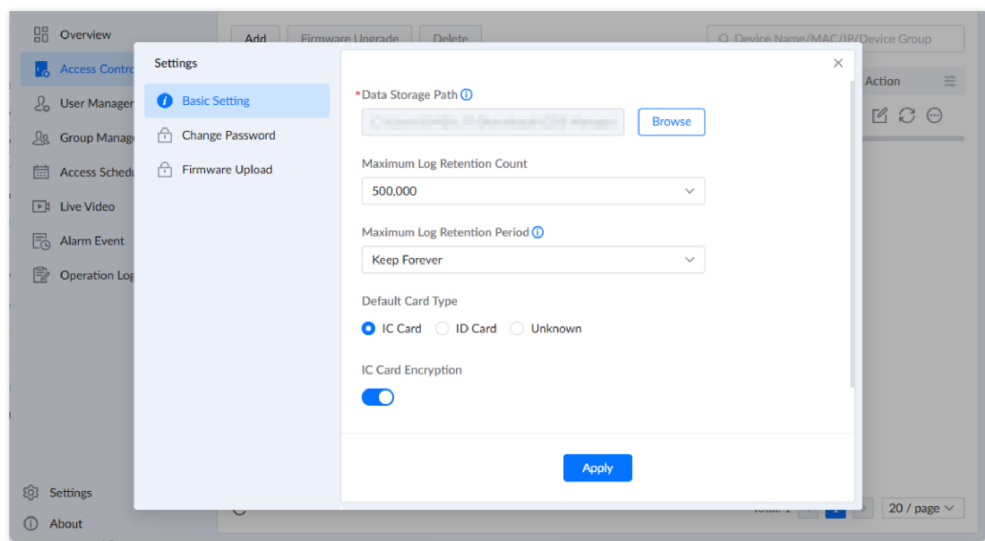
- **Filter by Module:** Filters log entries based on the application module where the operation was performed.
- **Filter by Status:** Filters log entries based on operation status: success, failure, or all.
- **Search by Target:** Allows searching log entries by the name of the target, such as a user, device, or device group.

Settings

The **Settings** interface provides centralized configuration of system parameters, enabling users to manage system preferences, security settings, and firmware resources. It allows control over data storage, retention rules, device and card configuration, language options, and password management, as shown below:

Basic Settings

Configure the basic settings of the application, including the storage location of application data, retention parameters, card specifications, and application language, as documented in the table below:

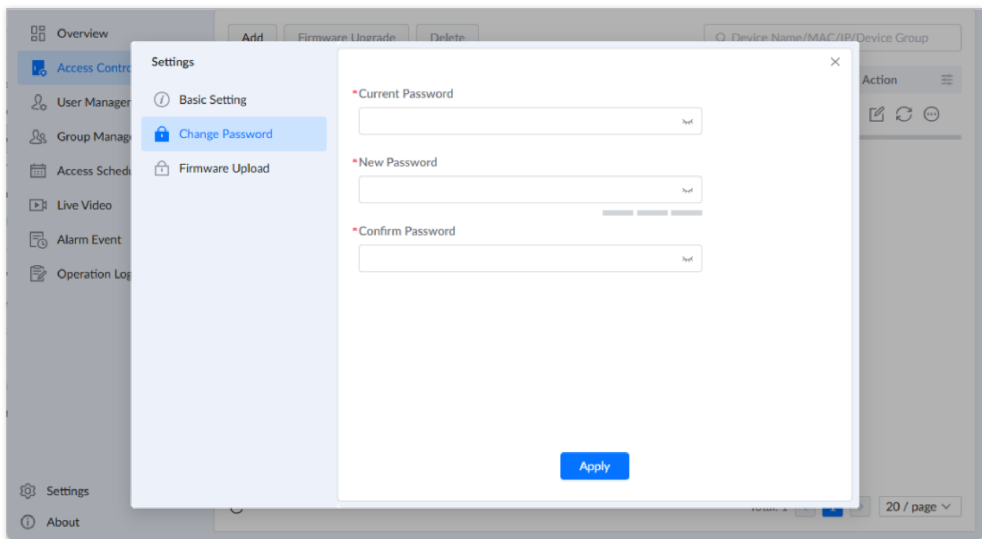


GDS Manager 2 → Settings → Basic Setting

Data Storage Path	Defines the storage location of the application data. The path configured during installation can be modified by pressing Browse and selecting a different directory. Note: After the storage path is changed, historical data stored in the original path is not migrated to the new location and can no longer be accessed through GDS Manager. All subsequent data will be stored in the new path.
Maximum Log Retention Count	Defines the maximum number of logs retained by the application. The default value is 500000.
Maximum Log Retention Period	Defines how long logs are retained before automatic deletion. The default setting is “Keep Forever”.
Default Card Type	Defines the default card type used when creating users. Available options are: ● IC Card ● ID Card ● Unknown The default setting is “IC Card”.
IC Card Encryption	Enables or disables IC card encryption. Enabled by default.
Language	Defines the application display language. Available options are: ● Automatic (default) ● English ● Simplified Chinese ● Traditional Chinese ● French ● Spanish ● Portuguese ● German ● Italian ● Arabic

Change Password

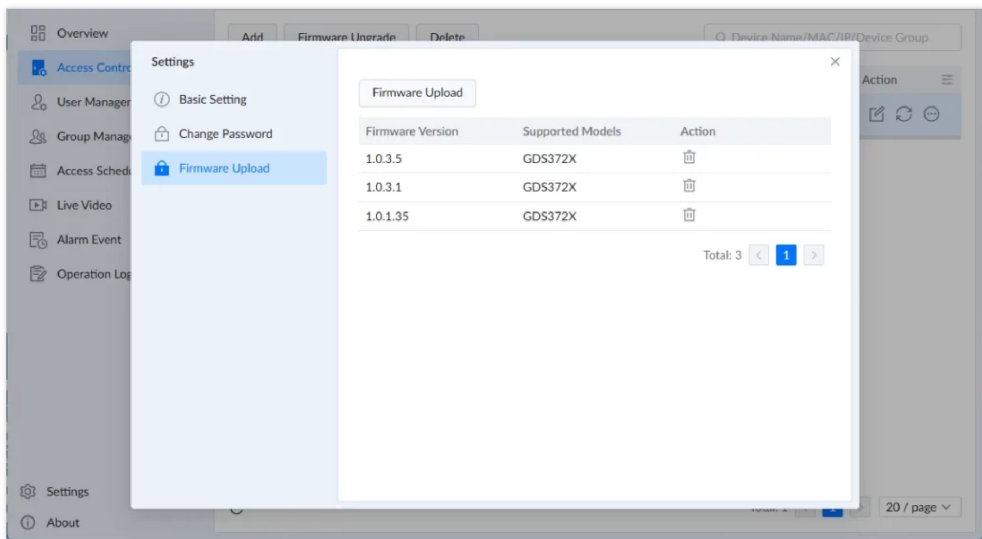
Change the application password by entering the current password, specifying the new password, and re-entering the new password for confirmation.



GDS Manager 2 → Settings → Change Password

Firmware Upload

Firmware files are used in the **Access Control Management** interface to upgrade GDS devices. To upload a firmware file, click **Firmware Upload**, browse the local directory, and select the desired .bin file.



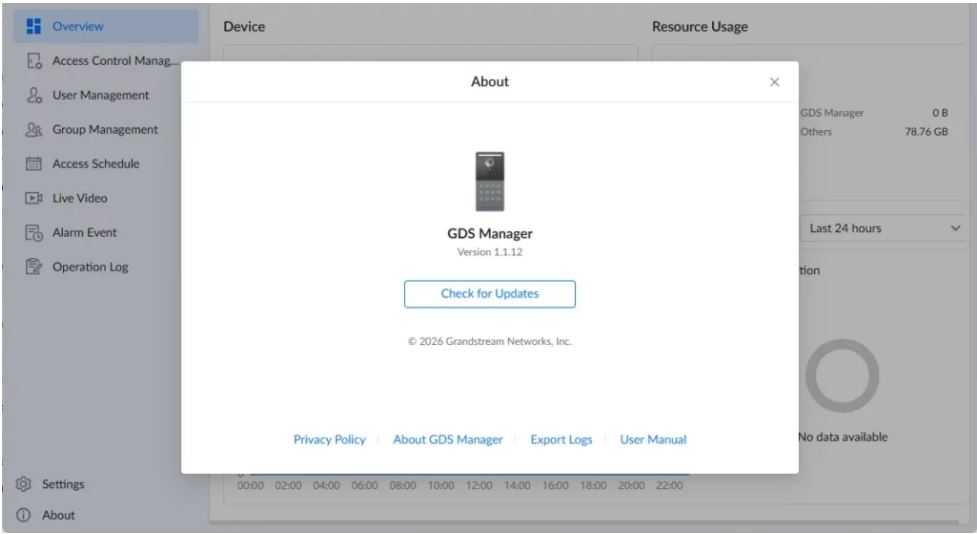
GDS Manager 2 → Settings → Firmware Upload

Firmware Version	Displays the firmware version of the uploaded firmware file.
Supported Models	Displays the GDS device models supported by the firmware file. Firmware files are model-specific.
Action	Delete: Deletes the selected firmware file from the application.

About

The **About** interface displays the application version and general information about GDS Manager 2. It also provides additional options, including:

- **Privacy Policy:** Opens the Grandstream Privacy Statement.
- **About GDS Manager:** Redirects to Grandstream’s Cloud Services website.
- **Export Logs:** Exports system logs in .ZIP format for troubleshooting and maintenance purposes.
- **User Manual:** Redirects to the GDS Manager 2’s user manual on the Grandstream documentation center for usage guidance.



GDS Manager 2 → About

Supported Devices

Model	Firmware Version
GDS3725 / GDS3726 / GDS3727	1.0.3.9 or higher

Changelog

Software Version 1.1.16

- This is the initial version.