NIVIAN Control Center AC Software

User Manual

Legal Information

User Manual

About this Manual

Please use this user manual under the guidance of professionals.

Trademarks

Disclaimer

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

Chapter 1 Introduction

The software provides multiple functionalities, including person management, access control, video intercom, time & attendance, etc., for the connected devices to meet the needs of monitoring task. With the flexible distributed structure and easy-to-use operations, the client software is widely applied to the surveillance projects of medium or small scale.
This user manual describes the functions, configurations and operation steps of the client software. To ensure the properness of usage and stability of the software, refer to the contents below and read the manual carefully before installation and operation.

Chapter 2 Service Management

Nivian Control Center AC Service is mainly applicable for data storage, data management, and data calculation. With continuous running and processing, it can manage the data, such as event records and attendance records, received by the Nivian Control Center AC Software. Nivian Control Center AC Service also provides management for user permissions, devices, groups, logs, etc.

You can view the module running status and edit its ports, including HTTP port and EHome port. You need to restart the Nivian Control Center AC Service to take effect.

Check **Auto-Launch** to enable launching the Nivian Control Center AC Service automatically after the PC started up.

Note

- The Nivian Control Center AC Service will not show after running it. Enter the system tray and click to open the service window.
- After closing the service window, the client will logout and return to the login page. You need to run the service and then login again.
- The service and the client should be installed on the same PC.

Chapter 3 Device Management

You can manage devices on the client, including adding, editing, and deleting the devices. You can also perform operations such as checking device status.

3.1 Add Device

After running the client, devices including access control devices, video intercom devices, etc., should be added to the client for the remote configuration and management, such as controlling door status, attendance management, event settings, etc.

3.1.1 Activate Devices

For some devices, you are required to create the password to activate them before they can be added to the software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Optional: Click on the right of **Device Management** and select **Device**.
   The added devices are displayed in the list.
3. Click **Online Device** to show the online device area.
   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. Click **OK** to activate the device.

3.1.2 Add Online Device

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area.

Note

- You can click **Refresh per 60s** to refresh the information of the online devices.
- SADP log function can be enabled or disabled by right-clicking **Online Device**.

Add Single Online Device

You can add single online device to the client software.

Steps

1. Enter the Device Management module.
2. Optional: Click on the right of **Device Management** and select **Device**.
   The added devices are displayed in the list.
3. Click **Online Device** to show the online device area.
   The searched online devices are displayed in the list.
4. Select an online device from the **Online Device** area.

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activate Devices***.

5. Click **Add** to open the device adding window.
6. Enter the required information.

Name

Enter a descriptive name for the device.

Address

The IP address of the device is obtained automatically in this adding mode.

Port

The port number is obtained automatically.

User Name

By default, the user name is admin.

Password

Enter the device password.

Caution

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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. Optional: Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. Optional: Check **Import to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

9. Click **OK** to add the device.

Add Multiple Online Devices

You can add multiple online devices to the client software.

Steps

1. Enter the Device Management module.
2. Optional: Click on the right of **Device Management** and select **Device**.
   The added devices are displayed in the list.
3. Click **Online Device** to show the online device area.
   The searched online devices are displayed in the list.
4. Select multiple devices.

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activate Devices***.

5. Click **Add** to open the device adding window.
6. Enter the required information.

User Name

By default, the user name is admin.

Password

Enter the device password.

Caution

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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. Optional: Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the devices to the client.
8. Optional: Check **Import to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

9. Click **OK** to add the devices.

3.1.3 Add Device by IP Address or Domain Name

When you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, and other related parameters.

Steps

1. Enter Device Management module.
2. Optional: Click on the right of **Device Management** and select **Device**.
   The added devices are displayed in the list.
3. Click **Add** to open the Add window.
4. Select **IP/Domain** as the adding mode.
5. Enter the required information, including name, address, port number, user name, and password.

Name

Create a descriptive name for the device. For example, you can use a name that can show the location or feature of the device.

Address

The IP address or domain name of the device.

Port

The devices to add have the same port No. The default value is 8000.

User Name

Enter the device user name. By default, the user name is admin.

Password

Enter the device password.

Caution

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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. Optional: Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. Optional: Check **Import to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

8. Finish adding the device.
   – Click **Add** to add the device and back to the device list page.
   – Click **Add and New** to save the settings and continue to add other device.
9. Perform the following operations after adding the devices.

Remote Configuration	Click on Operation column to set remote configuration of the corresponding device.
	Note ● For some models of devices, you can open its web window. To open the original remote configuration window, press **Ctrl** and click . ● For detail operation steps for the remote configuration, see the user manual of the device.
Device Status	Click on Operation column to view device status.

3.1.4 Add Devices by IP Segment

If you want to add devices of which the IP addresses are within an IP segment, you can specify the

start IP address and end IP address, user name, password, and other parameters to add them.

Steps

1. Enter the Device Management module.
2. Optional: Click on the right of **Device Management** and select **Device**.
   The added devices are displayed in the list.
3. Click **Add** to open the Add window.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

   Start IP

   Enter a start IP address.

   End IP

   Enter an end IP address in the same network segment with the start IP.

   Port

   Enter the device port No. The default value is 8000.

   User Name

   By default, the user name is admin.

   Password

   Enter the device password.

   Caution

   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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. Optional: Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. Optional: Check **Import to Group** to create a group by the device name.

   Note

   You can import all the channels of the device to the corresponding group by default.

8. Finish adding the device.
   – Click **Add** to add the device and back to the device list page.
   – Click **Add and New** to save the settings and continue to add other device.
9. Optional: Click on Operation column to view device status.

3.1.5 Add Device by EHome Account

For areas where devices using dynamic IP addresses instead of static ones, you can add access control device connected via EHome protocol by specifying the EHome account.

Before You Start

Set the network center parameter first. For details, refer to ***Set Network Parameters***.

Steps

Note

For the devices added by EHome don't support uploading events with captured pictures to the client.

1. Enter Device Management module.
2. Optional: Click on the right of **Device Management** and select **Device**.
   The added devices are displayed in the list.
3. Click **Add** to open the Add window.
4. Select **EHome** as the adding mode.
5. Enter the required information.

   Device Account

   Enter the account name registered on EHome protocol.

   EHome Key

   Enter the EHome key if you have set it when configuring network center parameter for the device.

   Note

   This function should be supported by the device.

6. Optional: Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. Optional: Check **Import to Group** to create a group by the device name.
8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.
9. Optional: Click on Operation column to view device status.

3.1.6 Import Devices in a Batch

The devices can be added to the software in a batch by entering the device information in the pre-defined CSV file.

Steps

1. Enter the Device Management page

2. Optional: Click on the right of **Device Management** and select **Device**.
3. Click **Add** to open the adding device window.
4. Select **Batch Import** as the adding mode.
5. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
6. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Adding Mode

You can enter ***0*** or ***1*** which indicated different adding modes. ***0*** indicates that the device is added by IP address or domain name; ***1*** indicates that the device is added via EHome.

Address

Edit the address of the device. If you set ***0*** as the adding mode, you should enter the IP address or domain name of the device; if you set ***1*** as the adding mode, this filed is not required.

Port

Enter the device port No. The default value is 8000.

Device Information

If you set ***0*** as the adding mode, this field is not required. If you set ***1*** as the adding mode, enter the EHome account.

User Name

Enter the device user name. By default, the user name is admin.

Password

If you set ***0*** as the adding mode, enter the password. If you set ***1*** as the adding mode, enter the EHome key.

Caution

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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Import to Group

You can enter ***1*** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. ***0*** indicates disabling this function.

7. Click and select the template file.
8. Click **Add** to import the devices.

3.2 Edit Device's Network Information

After activating device, you can edit the network information for the online device.

Before You Start

Activate the device if the device status is inactivated.

Steps

1. Enter Device Management page.
2. Optional: Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.
   All the online devices in the same subnet will display in the list.
4. Select an activated device in **Online Device** area.
5. Click on the Operation column to open the Modify Network Parameter window.

> **Note**
>
> This function is only available on the **Online Device** area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.

6. Change the device IP address to the same subnet with your computer.
   - Edit the IP address manually.
   - Check **DHCP**.
7. Enter the password created when you activate the device.
8. Click **OK** to complete the network settings.

3.3 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password through the client.

Steps

1. Enter Device Management page.
2. Optional: Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.
   All the online devices in the same subnet will display in the list.
4. Select the device from the list and click on the Operation column.
5. Reset the device password.
   - If the page with Export button, password, and confirm password field displays, click **Export** to save the device file on your PC and then send the file to our technical support.

     > **Note**
     >
     > For the following operations for resetting the password, contact our technical support.

   - If GUID is supported, you can import the GUID files which is saved when activating the device.

Note

For the following operations for resetting the password, contact our technical support.

Caution

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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Chapter 4 Group Management

The resources added should be organized into groups for convenient management, such as access control points. You can do some further operations of the device through the group.

4.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click → **Group** to enter the group management page.
3. Create a group.
   – Click **Add Group** and enter a group name as you want.
   – Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.

4.2 Import Resources to Group

You can import the device resources to the added group in a batch.

Before You Start

Add a group for managing devices. Refer to ***Add Group***.

Steps

1. Enter the Device Management module.
2. Click → **Group** to enter the group management page.
3. Select a group from the group list and select the resource type such as **Access Control Point**.
4. Click **Import**.
5. Select the channel names from the To Be Imported area.
6. Click **Import** to import the selected resources to the group.

4.3 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For access control points, you can edit the resource name.

Before You Start

Import the resources to group. Refer to ***Import Resources to Group***.

Steps

1. Enter the Device Management module.

2. Click → **Group** to enter the group management page.
   All the added groups are displayed on the left.
3. Select a group on the group list and click a resource type.
   The resource channels imported to the group will display.
4. Click in the Operation column to open the Modify window.
5. Edit the required information.
6. Click **OK** to save the new settings.

4.4 Remove Resources from Group

You can remove the added resources from the group.

Steps

1. Enter the Device Management module.
2. Click → **Group** to enter the group management page.
   All the added groups are displayed on the left.
3. Click a group to show the resources added to this group.
4. Select the resource(s) and click **Delete** to remove the resource(s) from the group.

Chapter 5 Event Center

You can configure the event of the added resources and set the linkage actions so that when the event is triggered, the software client can notify the security personnel and record the event details for checking afterwards.
In the event management page, you can configure access control event. For details about access control event configuration, refer to ***Configure Linkage Actions for Access Control***.
In the event center, you can view the real-time events and search the historical events. For details, refer to ***View Real-Time Events*** and ***Search Historical Events***.

5.1 Enable Receiving Events from Devices

Before the client can receive the event information from the device, you need to arm the device first.

Steps

1. Click → **Tool** → **Device Arming Control** open Device Arming Control page.
   All the added devices display on this page.
2. In the Operation column, turn on the switch to enable auto-arming, or click **Arm All** to arm all the devices.

Note

One access control device can only be armed by one client.

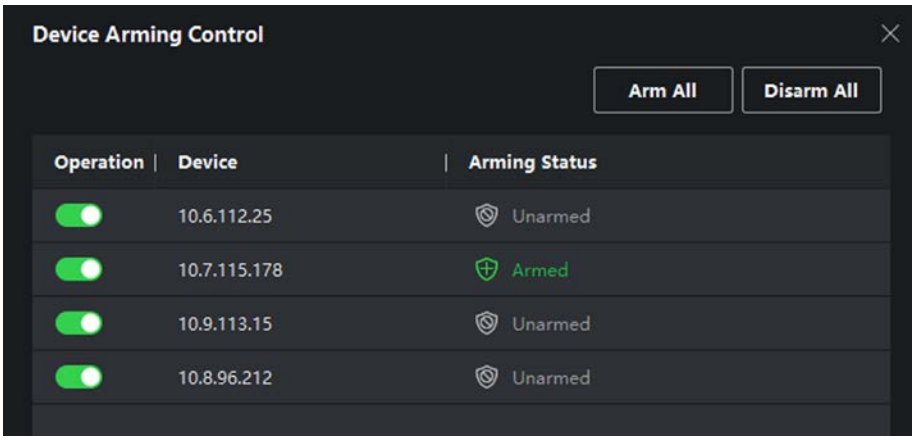

Figure 5-1 Device Arming Control

3. View the arming status of each device in the Arming Status column.

Result

The events of armed device(s) are automatically uploaded to the client when the event is triggered.

5.2 View Real-Time Events

In the Real-time Event module of the event center page, you can view the real-time event information, including event source, event time, priority, event key words, etc.

Before You Start

Enable receiving events from devices before the client can receive event information from the device, see ***Enable Receiving Events from Devices*** for details.

Steps

1. Click **Event Center** → **Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

   Event Time

   For video device, event time is the client time when it receives the event. For none-video device, event time is the time when the event is triggered.

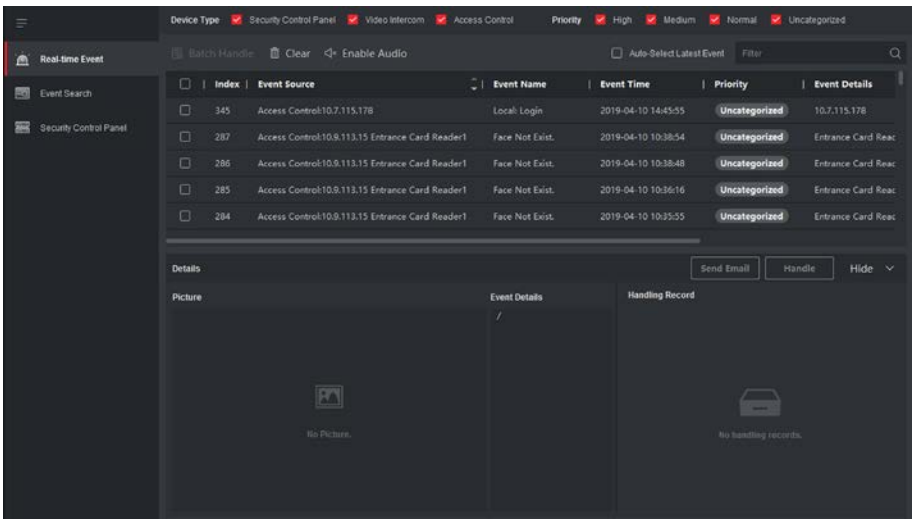

Figure 5-2 View Real-Time Events

2. Set the filter conditions or enter the event key word in the Filter text field to display the required events only.

   Device Type

   The type of device that occurred the event.

   Priority

   The priority of the event that indicates the urgent degree of the event.

3. Optional: Right click the table header of the event list to customize the event related items to be displayed in the event list.

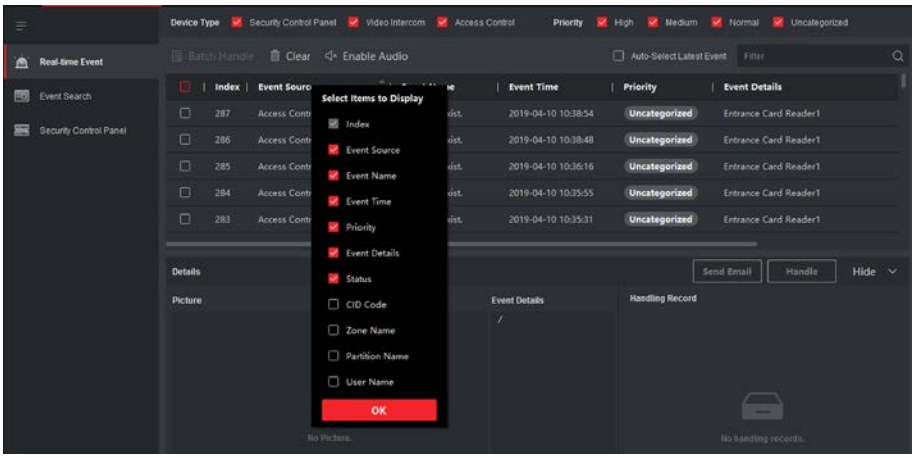

Figure 5-3 Customize Event Related Items to be Displayed

4. View the event information details.
   1) Select an event in the event list.
   2) Click **Expand** in the right-lower corner of the page.
   3) View the related picture, detail description and handing records of the event.
   4) Optional: Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.
5. Optional: Perform the following operations if necessary.

Handle Single Event	Click **Handle** to enter the processing suggestion, and then click **Commit**.

Note

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

Handle Events in a Batch	Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **Commit**.
Enable/Disable Alarm Audio	Click **Enable Audio**/**Disable Audio** to enable/disable the audio of the event.
Select the Latest Event Automatically	Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.
Clear Events	Click **Clear** to clear the all the events in the event list.

Send Email	Select an event and then click **Send Email**, and the information details of this event will be sent by email.

Note

You should configure the email parameters first, see ***Set Email Parameters*** for details.

5.3 Search Historical Events

In the Event Search module of the event center page, you can search the historical events via time, device type, and other conditions according to the specified device type, and then process the events.

Before You Start

Enable receiving events from devices before the client can receive event information from the device,see ***Enable Receiving Events from Devices*** for details.

Steps

1. Click **Event Center** → **Event Search** to enter the event search page.

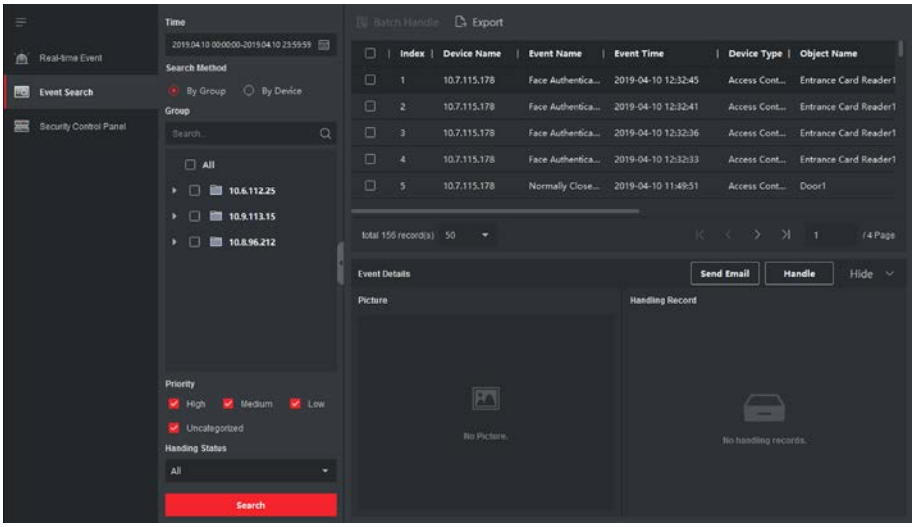

Figure 5-4 Search History Event

2. Set the filter conditions to display the required events only.

Time

The client time when the event starts.

Search by

Group: Search the events occurred on the resources in the selected group.

Device: Search the events occurred on the selected device.

Device Type

The type of device that occurred the event.

All

All the device types, and you can set the following filter conditions: group, priority, and status.

Video Intercom

For the events of video intercom, you need to select searching scope: All Record and Only Unlocking.

- All Records
- : You can filter the events from all the video intercom events, and you need to set the following filter conditions: device, priority, status.
- Only Unlocking
- : You can filter the events from all the video intercom unlocking events, and you need to set the following filter conditions: device, unlocking type.

Access Control

For the events of access control, you can set the following filter conditions: device, priority, status, event type, card reader type, person name, card no., organization.

Note

Click **Show More** to set the event type, card reader type, person name, card no., organization.

Group

The group of the device that occurred the event. You should set the group as condition only when you select the Device Type as **All**.

Device

The device that occurred the event.

Priority

The priority including low, medium, high and uncategorized which indicates the urgent degree of the event.

Status

The handling status of the event.

3. Click **Search** to search the events according the conditions you set.
4. Optional: Right click the table header of the event list to customize the event related items to be displayed in the event list.

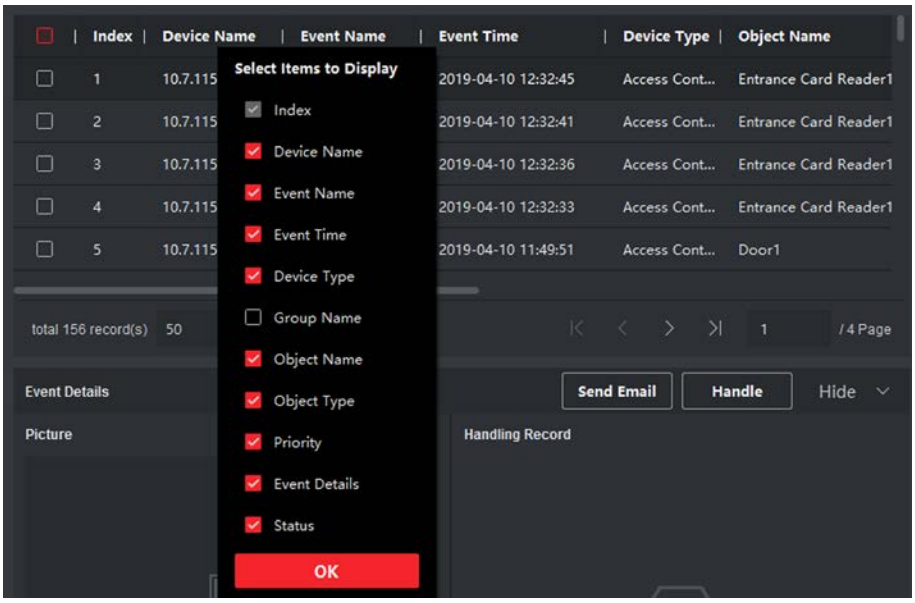

Figure 5-5 Customize Event Related Items to be Displayed

5. Optional: Handle the event(s).
   - Handle single event: Select one event that need to be processed, and then click **Handle** in the event information details page, and enter the processing suggestion.
   - Handle events in a batch: Select the events which need to be processed, and then click **Handle in Batch**, and enter the processing suggestion.

Note

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

6. Optional: Select an event and then click **Send Email**, and the information details of this event will be sent by email.

Note

You should configure the email parameters first, see ***Set Email Parameters*** for details.

7. Optional: Click **Export** to export the event log or event pictures to the local PC in CSV format. You can set the saving path manually.
8. Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

Chapter 6 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

6.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a surbodinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

Note

Up to 10 levels of organizations can be added.

4. Optional: Perform the following operation(s).

Edit Organization	Hover the mouse on an added organization and click to edit its name.
Delete Organization	Hover the mouse on an added organization and click to delete it.

Note

- The lower-level organizations will be deleted as well if you delete an organization.
- Make sure there is no person added under the organization, or the organization cannot be deleted.

Show Persons in Sub Organization	Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

6.2 Add Single Person

You can add persons to the client software one by one. The person information contains basic information, detailed information, profiles, access control information,credentials, custom

information, etc.

6.2.1 Configure Basic Information

You can add person to the client software one by one and configure the person's basic information such as name, gender, phone number, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.
   The Person ID will be generated automatically.
4. Enter the basic information including person name, gender, tel, email address, etc.
5. Optional: Set the effective period of the person. Once expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors.

   Example

   For example, if the person is a visitor, his/her effective period may be short and temporary.
6. Confirm to add the person.
   – Click **Add** to add the person and close the Add Person window.
   – Click **Add and New** to add the person and continue to add other persons.

6.2.2 Issue a Card to One Person

When adding person, you can issue a card with a unique card number to the person as a credential. After issued, the person can access the doors which he/she is authorized to access by swiping the card on the card reader.

Steps

Note

Up to five cards can be issued to one person.

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. In the **Credential** → **Card** panel, click **+**.
4. Enter the card number.
   – Enter the card number manually.

– Place the card on the card enrollment station or card reader and click **Read** to get the card number. The card number will display in the Card No. field automatically.

Note

You need to click **Settings** to set the card issuing mode and related parameters first. For details, refer to ***Set Card Issuing Parameters***.

5. Select the card type according to actual needs.

Normal Card

The card is used for opening doors for normal usage.

Duress Card

When the person is under duress, he/she can swipe the duress card to open the door. The door will be unlocked and the client will receive a duress event to notify the security personnel.

Patrol Card

This card is used for the inspection staff to check the their attendance of inspection. By swiping the card on the specified card reader, the person is marked as on duty of inspection at that time.

Dismiss Card

By swiping the card on the card reader, it can stop the buzzing of the card reader.

6. Click **Add**.
   The card will be issued to the person.
7. Confirm to add the person.
   – Click **Add** to add the person and close the Add Person window.
   – Click **Add and New** to add the person and continue to add other persons.

6.2.3 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.

Note

The picture should be in JPG or JPEG format and smaller than 200 KB.

6. Optional: Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

6.2.4 Take a Photo via Client

When adding person, you can take a photo of the person by the webcam of the PC running the client and set this photo as the person's profile.

Before You Start

Add at least one access control device checking whether the face in the photo can be recognized by the facial recognition device managed by the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. Click **Add Face** in the Basic Information panel.
4. Select **Take Photo**.
5. Connect the face scanner to the PC running the client.
6. Optional: Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Take a photo.
   1) Face to the webcam of the PC and make sure your face is in the middle of the collecting window.
   2) Click to capture a face photo.
   3) Optional: Click to capture again.
   4) Click **OK** to save the captured photo.
8. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.5 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

> **Note**
>
> Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. Click **Add Face** in the Basic Information panel.
4. Select **Remote Collection**.
5. Select an access control device which supports face recognition function from the drop-down list.
6. Collect face.
   1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
   2) Click to capture a photo.
   3) Click **OK** to save the captured photo.
7. Confirm to add the person.
   – Click **Add** to add the person and close the Add Person window.
   – Click **Add and New** to add the person and continue to add other persons.

6.2.6 Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Connect the fingerprint recorder to the PC running the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

> **Note**
>
> Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. In the **Credential** → **Fingerprint** panel, click **+**.

4. In the pop-up window, select the collection mode as **Local**.
5. Select the model of the connected fingerprint recorder.

Note

If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.

6. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
   – Click **Add** to add the person and close the Add Person window.
   – Click **Add and New** to add the person and continue to add other persons.

6.2.7 Collect Fingerprint via Access Control Device

When adding person, you can collect fingerprint information via the access control device's fingerprint module. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure fingerprint collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. In the **Credential** → **Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Remote**.
5. Select an access control device which supports fingerprint recognition function from the drop-down list.
6. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint scanner of the selected access control device to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
   – Click **Add** to add the person and close the Add Person window.
   – Click **Add and New** to add the person and continue to add other persons.

6.2.8 Configure Access Control Information

When adding a person, you can set her/his access control properties, such as setting the person as visitor or as blacklist person, or as super user who has super authorization.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. In the **Access Control** panel, set the person's access control properties.

PIN Code

The PIN code must be used after card or fingerprint when accessing. It cannot be used independently. It should contain 4 to 8 digits.

Super User

If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

Extended Door Open Time

When the person accessing door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.
For details about setting the door's open duration, refer to ***Configure Parameters for Door/Elevator***.

Add to Blacklist

Add the person to the blacklist and when the person tries to access doors/floors, an event will be triggered and send to the client to notify the security personnel.

Mark as Visitor

If the person is a visitor, set the maximum times of authentications, including access by card and fingerprint to limit the visitor's access times.

Note

The maximum times of authentications should be between 1 and 100.

Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.

Note

The Super User, Extended Door Open Time, Add to Blacklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blacklist, or set her/him as visitor.

4. Confirm to add the person.
   – Click **Add** to add the person and close the Add Person window.
   – Click **Add and New** to add the person and continue to add other persons.

6.2.9 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
   1) Click **Custom Property**.
   2) Click **Add** to add a new property.
   3) Enter the property name.
   4) Click **OK**.
3. Set the custom information when adding a person.
   1) Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

   2) In the **Custom Information** panel, enter the person information.
   3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

6.2.10 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. In the **Resident Information** panel, select the indoor station to bink it to the person.

Note

If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

6.2.11 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

6.3 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

6.3.1 Import Person Information

You can enter the information of multiple persons in a predefined template (a CSV file) to import

the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.

Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

7. Click ··· to select the CSV file with person information.
8. Click **Import** to start importing.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 10,000 persons.

6.3.2 Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. Optional: Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click ··· to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.
   The importing progress and result will be displayed.

6.3.3 Export Person Information

You can export the added persons' information to local PC as a CSV file.

Before You Start

Make sure you have added persons to an organization.

Steps

1. Enter the Person module.
2. Optional: Select an organization in the list.

Note

All persons' information will be exported if you do not select any organization.

3. Click **Export** to open the Export panel and check **Person Information** as the content to export.
4. Check desired items to export.
5. Click **Export** to save the exported CSV file in your PC.

6.3.4 Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

Make sure you have added persons and their face pictures to an organization.

Steps

1. Enter the Person module.
2. Optional: Select an organization in the list.

Note

All persons' face pictures will be exported if you do not select any organization.

3. Click **Export** to open the Export panel and check **Face** as the content to export.
4. Click **Export** to start exporting.

Note

- The exported file is in ZIP format.
- The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

6.4 Get Person Information from Access Control Device

If the added access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select the access control device from the drop-down list.
5. Click **Get** to start importing the person information to the client.
   The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

6.5 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.
   The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click **Change Organization**.

5. Select the organization to move persons to.
6. Click **OK**.

6.6 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.
   All the added persons with no card issued will display.
3. Set the card issuing parameters. For details, refer to ***Set Card Issuing Parameters***.
4. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
5. Click the card number column and enter the card number.
   – Place the card on the card enrollment station.
   – Swipe the card on the card reader.
   – Enter the card number manually and press **Enter** key on your keyboard.
   The card number will be read automatically and the card will be issued to the person in the list.
6. Repeat the above step to issue the cards to the persons in the list in sequence.

6.7 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential** → **Card** panel, click on the added card to set this card as lost card.
   After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. Optional: If the lost card is found, you can click to cancel the loss.
   After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

6.8 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.
When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.
Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.
Select the COM the card enrollment station connects to.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.
If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

Chapter 7 Access Control

The Access Control module is applicable to access control devices and video intercom device. It provides multiple functionalities, including access group configuration, video intercom, and other advanced functions.

Note

For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings. For setting the user permission of Access Control module, refer to ***Add User***.

7.1 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to ***Set Access Group to Assign Access Authorization to Persons***.

7.1.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control** → **Schedule** → **Holiday** to enter the Holiday page.
2. Click **Add** on the left panel.
3. Create a name for the holiday.
4. Optional: Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.

Note

Up to 16 holiday periods can be added to one holiday.

1) Click **Add** in the Holiday List field.

2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to one holiday period.

3) Optional: Perform the following operations to edit the time durations.
   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
4) Optional: Select the time duration(s) that need to be deleted, and then click in the Operation column to delete the selected time duration(s).
5) Optional: Click in the Operation column to clear all the time duration(s) in the time bar.
6) Optional: Click in the Operation column to delete this added holiday period from the holiday list.

6. Click **Save**.

7.1.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control** → **Schedule** → **Template** to enter the Template page.

Note

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

All-Day Authorized

The access authorization is valid in each day of the week and it has no holiday.

All-Day Denied

The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.
3. Create a name for the template.

4. Enter the descriptions or some notification of this template in the Remark box.
5. Edit the week schedule to apply it to the template.
   1) Click **Week Schedule** tab on the lower panel.
   2) Select a day of the week and draw time duration(s) on the timeline bar.

   Note

   Up to 8 time duration(s) can be set for each day in the week schedule.

   3) Optional: Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
   4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.

   Note

   Up to 4 holidays can be added to one template.

   1) Click **Holiday** tab.
   2) Select a holiday in the left list and it will be added to the selected list on the right panel.
   3) Optional: Click **Add** to add a new holiday.

   Note

   For details about adding a holiday, refer to ***Add Holiday***.

   4) Optional: Select a selected holiday in the right list and click to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.
7. Click **Save** to save the settings and finish adding the template.

7.2 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Steps

- For one person, you can add up to 4 access groups to one access control point of one device.
- You can add up to 128 access groups in total.
- When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card

number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control** → **Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

Note

You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.

5. In the left list of the Select Person field, select person(s) and the person(s) will be added to the selected list .
6. In the left list of the Select Door field, select door(s) or door station(s) for the selected persons to access, and the selected door(s) or door station(s) will be added to the selected list.
7. Click **OK**.
8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.

      To select multiple access groups, you can hold the **Ctrl** or **Shift** key and select access groups.

   2) Click **Apply All to Devices** to start applying all the selected access group(s) to the access control device or door station.

      Caution

      - Be careful to click **Apply All to Devices**, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may brings risk to the devices.
      - You can click **Apply Changes to Devices** to only apply the changed part of the selected access group(s) to the device(s).

   3) View the apply status in the Status column or click **Applying Status**to view all the applied access group(s).

   The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.
9. Optional: Click to edit the access group if necessary.

7.3 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in

different scene, such as multi-factor authentication, anti-passback, etc.

Note

- For the card related functions(the type of access control card/multi-factor authentication), only the card(s) with access group applied will be listed when adding cards.
- The advanced functions should be supported by the device.
- Hover the cursor on the Advanced Function, and then Click to customize the advanced function(s) to be displayed.

7.3.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter**.

Note

If you can find Device Parameter in the Advanced Function list, Hover the cursor on the Advanced Function, and then Click to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

Upload the pictures captured by linked camera to the system automatically.

Save Pic. After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G

If you enable this function, the device can communicate in 3G/4G network.

4. Click **OK**.
5. Optional: Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door/Elevator

After adding the access control device, you can configure its access point (door or floor) parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter**.
2. Select an access control device on the left panel, and then click to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.

Note

- The displayed parameters may vary for different access control devices.

- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended accesss needs swipes her/his card.

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.
6. Optional: Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).

Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter**.
2. In the device list on the left, click to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Entering PWD

When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click **OK**.
5. Optional: Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Input

After adding the access control device, you can configure the parameters for its alarm inputs.

Steps

Note

If the alarm input is armed, you cannot edit its parameters. Disarm it first.

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. In the device list on the left, click to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm input parameters.

Name

Edit the alarm input name as desired.

Detector Type

The detector type of the alarm input.

Zone Type

Set the zone type for the alarm input.

Sensitivity

Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

Trigger Alarm Output

Select the alarm output(s) to be triggered.

4. Click **OK**.
5. Optional: Click the switch on the upper-right corner to arm or disarm the alarm input.

Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click **OK**.
5. Optional: Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

Passing Mode

Select the controller which will control the barrier status of the device.

- If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.

- If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

Opening/Closing Door Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

Note

The recommended value is 6.

Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .

Note

0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click **OK**.

7.3.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed and set the elevator controller as free and controlled. For example, you can set the door remaining closed in the holiday, and set the door remaining open in the specified period of the work day.

Before You Start

Add the access control devices to the system.

Steps

1. Click **Access Control** → **Advanced Function** → **Remain Open/Closed** to enter the Remain Open/Closed page.
2. Select the door or elevator controller that need to be configured on the left panel.
3. To set the door or elevator controller status during the work day, click the **Week Schedule** and perform the following operations.
   1) For door, click **Remain Open** or **Remain Closed**.
   2) For elevator controller, click **Free** or **Controlled**.
   3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to each day in the week schedule.

4) Optional: Perform the following operations to edit the time durations.
   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
5) Click **Save**.

Related Operations

Copy to Whole Week	Select one duration on the time bar, click **Copy to Whole Week** to copy all the duration settings on this time bar to other week days.
Delete Selected	Select one duration on the time bar, click **Delete Selected** to delete this duration.
Clear	Click **Clear** to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.
   1) Click **Remain Open** or **Remain Closed**.
   2) Click **Add**.
   3) Enter the start date and end date.
   4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to one holiday period.

   5) Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
   6) Optional: Select the time duration(s) that need to be deleted, and then click in the Operation column to delete the selected time duration(s).
   7) Optional: Click in the Operation column to clear all the time duration(s) in the time bar.
   8) Optional: Click in the Operation column to delete this added holiday period from the holiday list.

9) Click **Save**.

5. Optional: Click **Copy to** to copy the door status settings of this door to other door(s).

7.3.3 Configure Multi-Factor Authentication

You can manage the persons by group and set the authentication for multiple persons of one access control point (door).

Before You Start

Set access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons***.

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control** → **Advanced Function** → **Multi-Factor Auth**.
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
   1) Click **Add** on the right panel.
   2) Create a name for the group as desired.
   3) Specify the start time and end time of the effective period for the person/card group.
   4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

   Note

   Make sure you have issue card to the person.
   Make sure you have set access group and apply the access group to the access control device successfully.

   5) Click **Save**.
   6) Optional: Select the person/card group(s), and then click **Delete** to delete it(them).
   7) Optional: Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.
4. Select an access control point (door) of selected device on the left panel.
5. Enter the maximum interval when entering password.
6. Add an authentication group for the selected access control point.
   1) Click **Add** on the Authentication Groups panel.
   2) Select a configured template as the authentication template from the drop-down list.

   Note

   For setting the template, refer to ***Configure Schedule and Template***.

3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

Local Authentication

Authentication by the access control device.

Local Authentication and Remotely Open Door

Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.

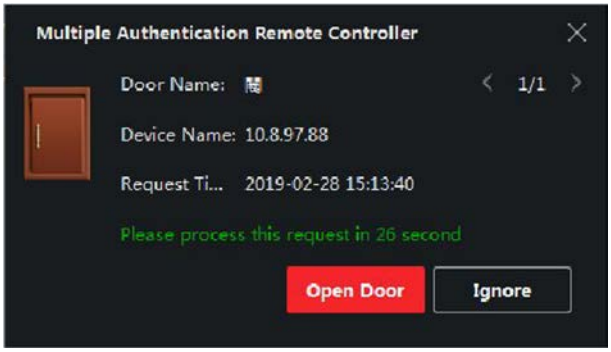

Figure 7-1 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

4) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.

5) Click the added authentication group in the right list to set authentication times in the Auth Times column.

Note

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
- The maximum value of authentication times is 16.

6) Click **Save**.

Note

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
- For the authentication group of which authentication type is **Local Authentication and Super**

Password or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.

7. Click **Save**.

7.3.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Steps

Note

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom Wiegands can be set.
- For details about the custom Wiegand, see ***Custom Wiegand Rule Descriptions***.

1. Click **Access Control** → **Advanced Function** → **Custom Wiegand** to enter the Custom Wiegand page.
2. Select a custom Wiegand on the left.
3. Create a Wiegand name.

Note

Up to 32 characters are allowed in the custom Wiegand name.

4. Click **Select Device** to select the access control device for setting the custom wiegand.
5. Set the parity mode according to the property of the third party card reader.

Note

- Up to 80 bits are allowed in the total length.
- The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
- The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.

6. Set output transformation rule.
   1) Click **Set Rule** to open the Set Output Transformation Rules window.

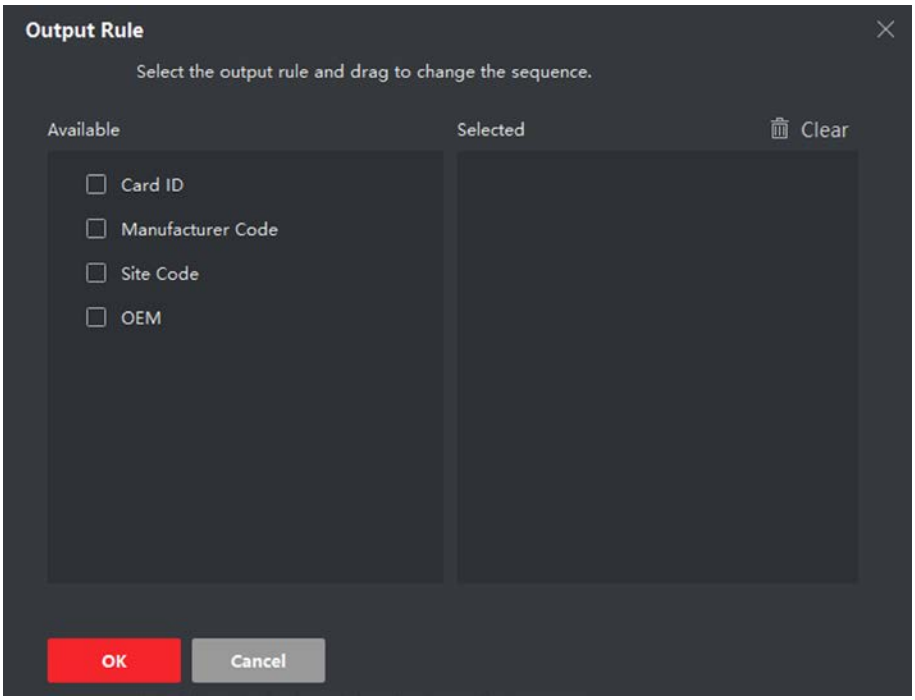

Figure 7-2 Set Output Transformation Rule

2) Select rules on the left list.
   The selected rules will be added to the right list.
3) Optional: Drag the rules to change the rule order.
4) Click **OK**.
5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

7.3.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication** to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
   1) Click **Configuration**.

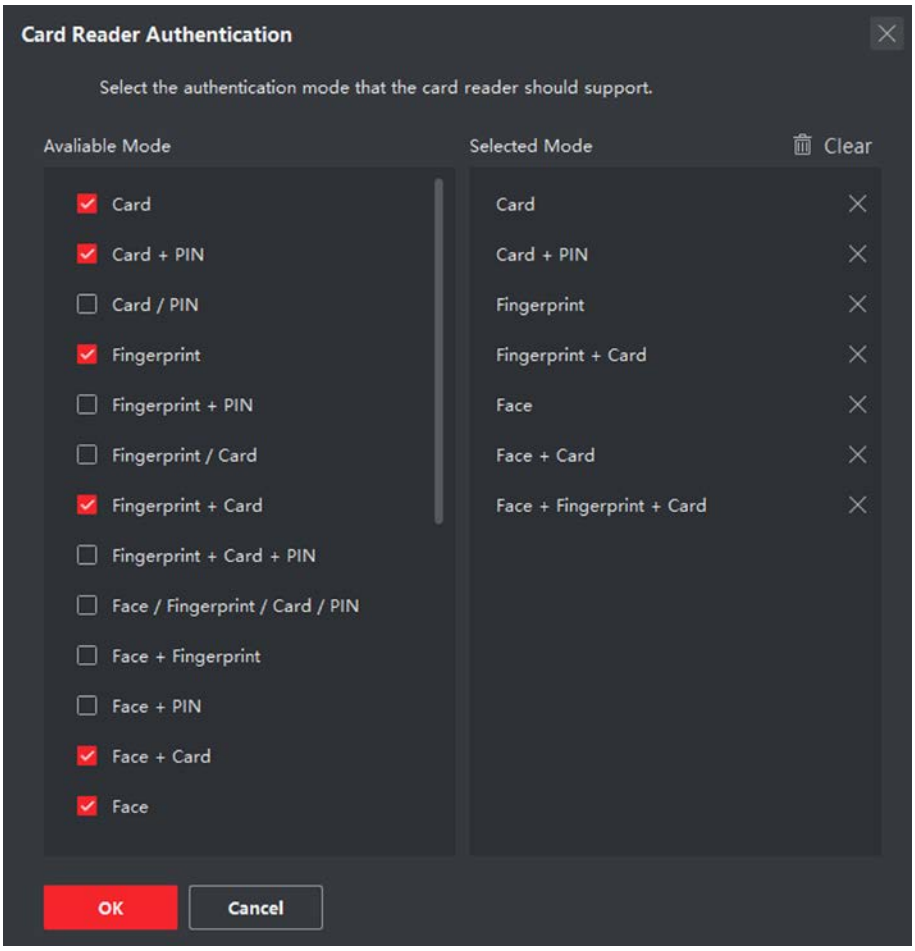

Figure 7-3 Select Card Reader Authentication Mode

Note

PIN refers to the PIN code set to open the door. Refer to ***Configure Access Control Information***.

2) Check the modes in the Available Mode list and they will be added to the selected modes list.
3) Click **OK**.
   After selecting the modes, the selected modes will display as icons with different color.
4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.
5. Repeat the above step to set other time periods.

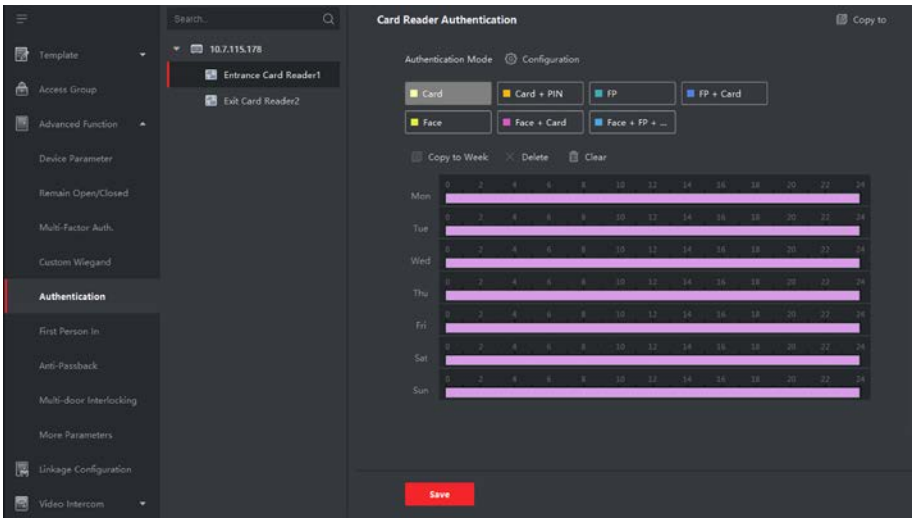

Figure 7-4 Set Authentication Modes for Card Readers

6. Optional: Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. Optional: Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

7.3.6 Configure Person Authentication Mode

You can set the passing rules for person to the specified the access control device according to your actual needs.

Before You Start

Make sure the access control device support the function of person authentication.

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication**.
2. Select an access control device (support the function of person authentication) on the left panel to enter the person Authentication Mode page.
3. Click **Add** to enter the Add window.
4. Select the person(s) need to be configured on the left panel.
   The selected person(s) will be added to the right panel.
5. Select the authentication mode on the drop-down list of **Authentication Mode**.
6. Click **OK**.

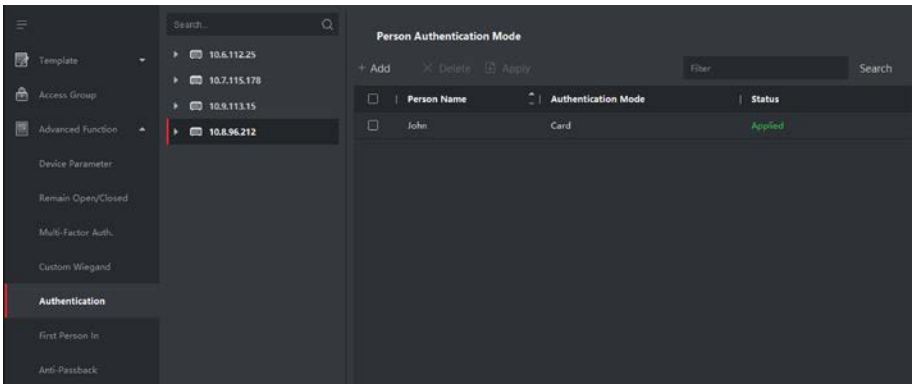

Figure 7-5 Set Authentication Modes for Persons

7. Optional: Select person(s) on the Person Authentication mode page, and then click **Apply** to apply the person authentication mode to the device.

Note

Person authentication has higher priority than other authentication mode. When the access control device has been configured person authentication mode, the person should authenticate on this device via person authentication mode.

7.3.7 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

Set the access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons***.

Perform this task when you want to configure opening door with first person.

Steps

1. Click **Access Control** → **Advanced Function** → **First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

Enable Remaining Open after First Person

The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the remain open duration.

Note

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

Authorization by First Person

All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

Note

You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.
   The added first person(s) will list in the First Person List
6. Optional: Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

7.3.8 Configure Anti-Passback

You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Before You Start

Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.

Steps

Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to ***Configure Multi-door Interlocking***.

1. Click **Access Control** → **Advanced Function** → **Anti-Passback** to enter the Anti-Passpack Settings page.
2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.

4. Click of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
5. Select the afterward card readers for the first card reader.

Note

Up to four afterward card readers can be added as afterward card readers for one card reader.

6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping PathIf you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

7.3.9 Configure Multi-door Interlocking

You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Perform this task when you want to realize interlocking between multiple doors.

Steps

Note

- Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of anti-passing back function, refer to ***Configure Anti-Passback***.

1. Click **Access Control** → **Advanced Function** → **Multi-door Interlocking**.
2. Select an access control device on the left panel.
3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
4. Select at least two access control points(doors) from the list.

Note

Up to four doors can be added in one multi-door interlocking combination.

5. Click **OK** to add the selected access control point(s) for interlocking.
   The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.

6. Optional: Select an added multi-door interlocking combination from the list and click **Delete** to delete the combination.
7. Click **Apply** to apply the settings to the access control device.

7.4 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

7.4.1 Set Multiple NIC Parameters

If the device supports multiple network interfaces, you can set the network parameters of these NICs via the client, such as IP address, MAC address, port number, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **NIC** to enter Multiple NIC Settings page.
4. Select an NIC you want to configure from the drop-down list.
5. Set its network parameters such as IP address, default gateway, subnet mask, etc.

   MAC Address

   A media access control address (MAC address) is a unique identifier assigned to the network interface for communications on the physical network segment.

   MTU

   The maximum transmission unit (MTU) of the network interface.
6. Click **Save**.

7.4.2 Set Network Parameters

After adding the access control device, you can set the device log uploading mode, and create

EHome account via wired or wireless network.

Set Log Uploading Mode

You can set the mode for the device to upload logs via EHome protocol.

Steps

Note

Make sure the device is not added by EHome.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and enter **Network** → **Uploading Mode**.
4. Select the center group from the drop-down list.
5. Check **Enable** to enable to set the uploading mode.
6. Select the uploading mode from the drop-down list.
   – Enable **N1** or **G1** for the main channel and the backup channel.

Select **Close** to disable the main channel or the backup channel

Note

The main channel and the backup channel cannot enable N1 or G1 at the same time.

7. Click **Save**.

Create EHome Account in Wired Communication Mode

You can set the account for EHome protocol in wired communication mode. Then you can add devices via EHome protocol.

Steps

Note

- This function should be supported by the device.
- Make sure the device is not added by EHome.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and enter **Network** → **Network Center**.
4. Select the center group from the drop-down list.
5. Select the **Address Type** as **IP Address** or **Domain Name**.
6. Enter IP address or domain name according to the address type.
7. Enter the port number for the protocol.

Note

The port number of the wireless network and wired network should be consistent with the port number of EHome.

8. Select the **Protocol Type** as **EHome**.
9. Set an account name for the network center.
10. Click **Save**.

Create EHome Account in Wireless Communication Mode

You can set the account for EHome protocol in wireless communication mode. Then you can add devices via EHome protocol.

Steps

Note

- This function should be supported by the device.
- Make sure the device is not added by EHome.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and enter **Network** → **Wireless Communication Center**.
4. Select the **APN Name** as **CMNET** or **UNINET**.
5. Enter the SIM Card No.
6. Select the center group from the drop-down list.
7. Enter the IP address and port number.

Note

- By default, the port number for EHome is ***7660***.
- The port number of the wireless network and wired network should be consistent with the port number of EHome.

8. Select the **Protocol Type** as **EHome**.
9. Set an account name for the network center.
10. Click **Save**.

7.4.3 Set Device Capture Parameters

You can configure the capture parameters of the access control device, including manual capture

and event triggered capture.

Note

- The capture function should be supported by the device.
- Before setting the capture parameters, you should set the picture storage first to define where the event triggered pictures are saved. For details, refer to ***Set Picture Storage***.

Set Triggered Capture Parameters

When an event occurs, the camera of the access control device can be triggered to capture picture(s) to record what happens when the event occurs. You can view the captured pictures when checking the event details in Event Center. Before that, you need to set the parameters for the capture such as number of pictures captured for one time.

Before You Start

Before setting the capture parameters, you should set the picture storage first to define where the captured pictures are saved. For details, refer to ***Set Picture Storage***.

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters** → **Capture**.
3. Select an access control device in the device list and select **Linked Capture**.
4. Set the picture size and quality.
5. Set the capture times once triggered which defines how many pictures will be captures for one time.
6. If the capture times is more than 1, set the interval for each capture.
7. Click **Save**.

Set Manual Capture Parameters

In Status Monitoring module, you can capture a picture manually the access control device's camera by clicking a button. Before that, you need to set the parameters for the capture such as picture quality.

Before You Start

Before setting the capture parameters, you should set the saving path first to define where the captured pictures are saved. For details, refer to ***Set File Saving Path***.

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters** → **Capture**.
3. Select an access control device in the device list and select **Manual Capture**.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as **High**, **Medium**, or **Low**. The higher the picture quality is, the larger size the picture will be.
6. Click **Save**.

7.4.4 Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **Face Recognition Terminal**.
4. Set the parameters.

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blacklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blacklist.
If matched (the person is in the blacklist), the access will be denied and the device will upload an alarm to the client.
If mismatched (the person is not in the blacklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

7.4.5 Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Steps

Note

The RS-485 Settings should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the working mode or connection mode, the device will reboot automatically.

7.4.6 Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand

communication.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

Note

If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the communication direction, the device will reboot automatically.

7.4.7 Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters**.
3. Select an access control device in the device list and click **M1 Card Encryption** to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

   The sector ID ranges from 1 to 100.
6. Click **Save** to save the settings.

7.5 Configure Linkage Actions for Access Control

The events triggered by the access control devices, doors, card readers, and alarm inputs, as well as the card swiping of persons, mobile terminal's MAC address detected, and employee No. detected, can trigger a series of linkage actions to notify the security personnel and record the events.
Two types of linkage actions are supported: client actions and device actions.

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client playing alarm sound and sending an email to notify the security personnel.
- **Device Actions:** When the event is detected, it will trigger the actions of this device, such as buzzing, door open/closed, audio play, etc., to notify the security personnel and allow/forbid access.

7.5.1 Configure Client Actions for Access Event

You can assign client linkage actions to the event by setting up a rule. For example, when the event is detected, an audible warning appears to notify the security personnel.

Steps

Note

The linkage actions here refer to the linkage of the client software's own actions such as audible warning, email linkage, etc.

1. Click **Event Management** → **Access Control Event**.
   The added access control devices will display in the device list.
2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.
   The event types which the selected resource supports will display.
3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.
   1) Select the event(s) and click **Edit Linkage** to set the client actions when the events triggered.

      Audible Warning

      The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.

      Note

      For setting the alarm sound, please refer to ***Set Alarm Sound***.

      Email Linkage

      Send an email notification of the alarm information to one or more receivers.
   2) Click **OK**.

5. Enable the event so that when the event is detected, en event will be sent to the client and the linkage actions will be triggered.
6. Optional: Click **Copy to...** to copy the event settings to other access control device, alarm input, door/elevator, or card reader.

7.5.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. When the event is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Event Linkage**.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Buzzer on Reader

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, and remain close will be triggered.

Note

The target door and the source door cannot be the same one.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save**.
8. Optional: After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

7.5.3 Configure Device Actions for Card Swiping

You can set the access control device's linkage actions for the specified card swiping. When you swipe the specified card, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Card Linkage**.
5. Enter the card number or select the card from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.
   When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).
9. Optional: After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

7.5.4 Configure Device Linkage for Mobile Terminal's MAC Address

You can set the access control device's linkage actions for the specified MAC address of mobile terminal. When access control device detects the specified MAC address, it can trigger the alarm

output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Mac Linkage**.
5. Enter the MAC address to be triggered.

Note

MAC Address Format: AA:BB:CC:DD:EE:FF.

6. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save** to save the settings.
8. Optional: After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

7.5.5 Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Person Linkage**.
5. Enter the employee number or select the person from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support zone function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.
9. Optional: After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

7.6 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to ***Add User***.

7.6.1 Control Door Status

You can control the status for a single door, including opening door, closing door, remaining the door open, and remaining the door closed.

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

Note

For managing the access point group, refer to ***Group Management***.

The doors in the selected access control group will display.

3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.
4. Click the following buttons to control the door.

Open Door

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Close Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Open

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Closed

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to ***Set File Saving Path***.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

7.6.2 Control Elevator Status

You can control the elevator status of the added elevator controller, including opening elevator's

door, controlled, free, calling elevator, etc.

Steps

Note

- You can control the elevator via the current client if it is not armed by other client. The elevator cannot be controlled by other client software if the elevator status changes.
- Only one client software can control the elevator at one time.
- The client which has controlled the elevator can receive the alarm information and view the elevator real-time status.

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

Note

For managing the access point group, refer to ***Group Management***.

The elevators in the selected access point group will display.

3. Click a door icon to select an elevator.
4. Click the following buttons to control the elevator.

Open Door

When the elevator's door is closed, open it. After the open duration, the door will be closed again automatically.

Controlled

You should swipe the card before pressing the target floor button. And the elevator can go to the target floor.

Free

The selected floor's button in the elevator will be valid all the time.

Disabled

The selected floor's button in the elevator will be invalid and you cannot go to the target floor.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

7.6.3 Check Real-Time Access Records

The access records will display in real time, including card swiping records, face recognitions records, fingerprint comparison records, etc. You can view the person information and view the

picture captured during access.

Steps

1. Click **Monitoring** and select a group from the drop-down list on the upper-right corner.
   The access records triggered at the doors in the selected group will display in real time. You can view the details of the records, including card No., person name, organization, event time, etc.
2. Optional: Check the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. Optional: Check **Show Latest Event** and the latest access record will be selected and displayed at the top of the record list.
4. Optional: Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.

Note

You can double click the captured picture to enlarge it to view the details.

5. Optional: Right click on the column name of the access event table to show or hide the column according to actual needs.

Chapter 8 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

Note

In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

8.1 Configure Attendance Parameters

You can configure the attendance parameters, including the general rule, overtime parameters, attendance check point, holiday, leave type, etc.

8.1.1 Configure General Rule

You can configure the general rule for attendance calculation, such as the week beginning, month beginning, weekend, absence, etc.

Steps

Note

The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time & Attendance module.
2. Click **Attendance Settings** → **General Rule**.
3. Set the day as week beginning and the date as month beginning.
4. Select the day(s) as weekend.
5. Set absence parameters.
6. Click **Save**.

8.1.2 Configure Overtime Parameters

You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, attendance status for overtime, etc.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings** → **Overtime**.

3. Set required information.

Overtime Level for Workday

When you work for certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3 . You can set different work hour rate for three overtime levels, respectively.

Work Hour Rate

Set corresponding work hour rates for three overtime levels, which can be generally used to calculate total work hours.

Overtime Rule for Weekend

You can enable overtime rule for weekend and set calculation mode.

4. Click **Save**.

8.1.3 Configure Attendance Check Point

You can set the card reader(s) of the access point as the attendance check point, so that the authentication on the card readers will be recorded for attendance .

Before You Start

You should add access control device before configuring attendance check point. For details, refer to ***Add Device***.

Steps

Note

By default, all card readers of the added access control devices are set as attendance checkpoint.

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **Attendance Check Point** to enter the Attendance Check Point Settings page.
3. Optional: Set **Set All Card Readers as Check Points** switch to off.
   Only the card readers in the list will be set as the attendance check points.
4. Check the desired card reader(s) in the device list as attendance check point(s).
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.
6. Click **Set as Check Point**.
   The configured attendance check point displays on the right list.

8.1.4 Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **Holiday** to enter the Holiday Settings page.
3. Check **Regular Holiday** as holiday type.
4. Custom a name for the holiday.
5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. Optional: Check **Repeat Annually** to make this holiday setting effective every year.
9. Click **OK**.
   The added holiday will display in the holiday list and calendar.
   If the date is selected as different holidays, it will be recorded as the first-added holiday.
10. Optional: After adding the holiday, perform one of the following operations.

Edit Holiday	Click  to edit the holiday information.
Delete Holiday	Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **Holiday** to enter the Holiday Settings page.
3. Click **Add** to open the Add Holiday page.
4. Check **Irregular Holiday** as holiday type.
5. Custom a name for the holiday.
6. Set the start date of the holiday.

   Example

   If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.
7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.

9. Optional: Check **Repeat Annually** to make this holiday setting effective every year
10. Click **OK**.
    The added holiday will display in the holiday list and calendar.
    If the date is selected as different holidays, it will be recorded as the first-added holiday.
11. Optional: After adding the holiday, perform one of the following operations.

Edit Holiday	Click to edit the holiday information.
Delete Holiday	Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

8.1.5 Configure Leave Type

You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **Leave Type** to enter the Leave Type Settings page.
3. Click **Add** on the left to add a major leave type.
4. Optional: Perform one of the following operations for major leave type.

Edit	Move the cursor over the major leave type and click to edit the major leave type.
Delete	Select one major leave type and click **Delete** on the left to delete the major leave type.

5. Click **Add** on the right to add a minor leave type.
6. Optional: Perform one of the following operations for minor leave type.

Edit	Move the cursor over the minor leave type and click to edit the minor leave type.
Delete	Select one or multiple major leave types and click **Delete** on the right to delete the selected minor leave type(s).

8.1.6 Synchronize Authentication Record to Third-Party Database

The attendance data recorded in client software can be used by other system for calculation or some other operations. You can enable synchronization function to apply the authentication record from client software to the third-party database automatically.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings** → **Third-Party Database**.

3. Set **Apply to Database** switch to on to enable synchronization function.
4. Set the required parameters of the third-party database, including database type, server IP address, database name, user name and password.
5. Set table parameters of database according to the actual configurations.
   1) Enter the table name of the third-party database.
   2) Set the mapped table fields between the client software and the third-party database.
6. Click **Connection Test** to test whether database can be connected.
7. Click **Save** to test whether database can be connected and save the settings for the successful connection.
   The attendance data will be written to the third-party database.

8.1.7 Configure Break Time

You can add break time and set start time, end time, duration, calculation mode and other parameters for the break. The added break time can also be edited or deleted.

Steps

1. Click **Time & Attendance** → **Timetable**.
   The added timetables are displayed in the list.
2. Select an added timetable or click **Add** to enter setting timetable page.
3. Click **Settings** in the break time area to enter break time management page.
4. Add break time.
   1) Click **Add**.
   2) Enter a name for the break time.
   3) Set related parameters for the break time.

Start Time / End Time

Set the time when the break starts and ends.

No Earlier Than / No Later Than

Set the earliest swiping time for starting break and the latest swiping time for ending break.

Break Duration

The duration from start time to end time of the break.

Calculation

Auto Deduct

The fixed break duration will be excluded from work hours.

Must Check

The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.

Note

If you select **Must Check** as calculation method, you need to set attendance status for late or early returning from break.

5. Click **Save** to save the settings.
6. Optional: Click **Add** to continue adding break time.

8.1.8 Configure Report Display

You can configure display contents displayed in the attendance report, such as the company name, logo, date format, time format, and mark.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Statistics** → **Report Display**.
3. Set the display settings for attendance report.

Company Name

Enter a company name to display the name in the report.

Date Format / Time Format

Set the date format and time format according to the actual needs.

Attendance Status Mark in Report

Enter the mark and select the color. The related fields of attendance status in the report will display with the mark and color.

Weekend Mark in Report

Enter the mark and select the color. The weekend fields in the report will display with the mark and color.

4. Click **Save**.

8.2 Add Timetable

You can add the timetable for the shift schedule.

Steps

1. Click **Time & Attendance** → **Timetable** to enter timetable settings window.
2. Click **Add** to enter Add Timetable page.
3. Create a name for the timetable.
4. Select calculation method.

First In & Last Out

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

Each Check-In/Out

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.
You need to set **Valid Auth. Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

5. Optional: Set **Enable T&A Status** switch to on to calculate according to attendance status of the device.
6. Set the related attendance time.

Start/End-Work Time

Set the start-work time and end-work-time.

Valid Check-in/out Time

Set the time period during which the check-in or check-out is valid.

Calculated as

Set the duration calculated as the actual work duration.

Late/Early Leave Allowable

Set the time period for late or early leave.

7. Optional: Select break time to exclude the duration from work hours.

Note

You can click **Settings** to manage break time. For more details about configuring break time, refer to ***Configure Break Time***.

8. Click **Save** to add the timetable.
9. Optional: Perform one or more following operations after adding timetable.

Edit Timetable	Select a timetable from the list to edit related information.
Delete Timetable	Select a timetable from the list and click **Delete** to delete it.

8.3 Add Shift

You can add the shift for the shift schedule.

Before You Start

Add a timetable first. See ***Add Timetable*** for details.

Steps

1. Click **Time & Attendance** → **Shift** to enter shift settings page.
2. Click **Add** to enter Add Shift page.
3. Enter the name for shift.
4. Select the shift period from the drop-down list.

5. Select the added timetable and click on the time bar to apply the timetable.

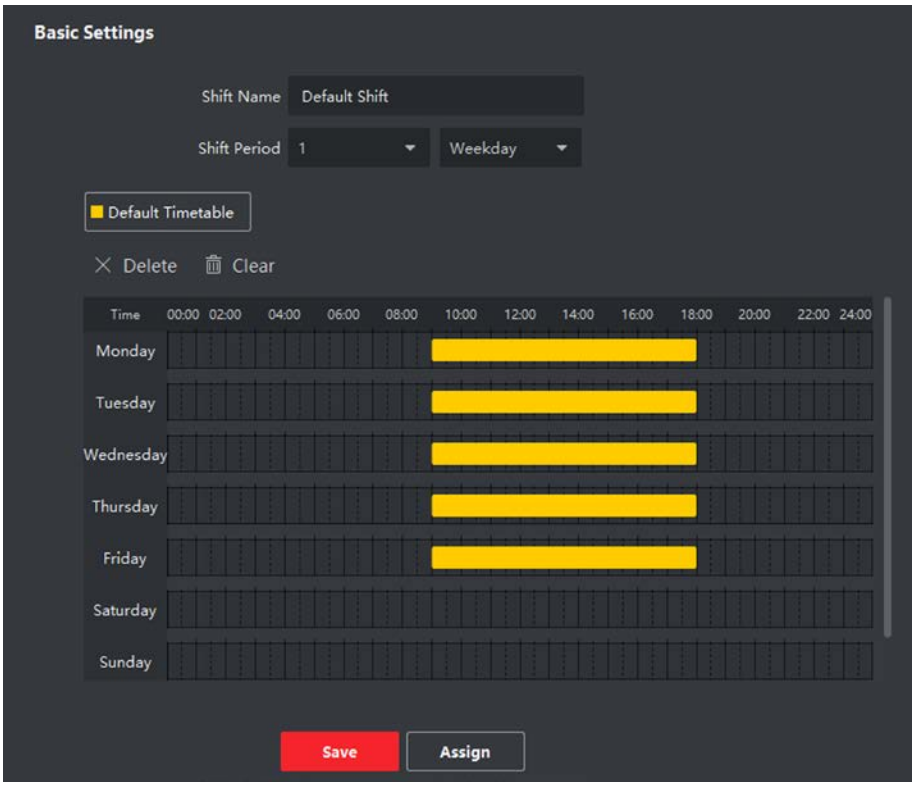

Figure 8-1 Add Shift

6. Click **Save**.
   The added shift lists on the left panel of the page. At most 64 shifts can be added.
7. Optional: Assign the shift to organization or person for a quick shift schedule.
   1) Click **Assign**.
   2) Select **Organization** or **Person** tab and check the desired organization(s) or person(s) box.
      The selected organizations or persons will list on the right page.
   3) Set the effective period for the shift schedule.
   4) Set other parameters for the shift schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.
   5) Click **Save** to save the quick shift schedule.

8.4 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.
You can set department schedule, person schedule, and temporary schedule.

8.4.1 Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

In Time & Attendance module, the department list is the same with the organization. You should add organization and persons in Person module first. See ***Person Management*** for details.

Steps

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Department Schedule** to enter Department Schedule page.
3. Select the department from the organization list on the left.

> **Note**
>
> If **Include Sub Organization** is checked, when selecting the organization, its sub organizations are selected at the same time.

4. Select the shift from the drop-down list.
5. Check the checkbox to enable **Multiple Shift Schedules**.

> **Note**
>
> After checking **Multiple Shift Schedules**, you can select the effective time period(s) from the added time periods for the persons in the department.
>
> **Multiple Shift Schedules**
>
> It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
> If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.
8. Click **Save**.

8.4.2 Set Person Schedule

You can assign the shift schedule to one or more persons. You can also view and edit the person schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Person Schedule** to enter Person Schedule page.
3. Select the organization and select the person(s).
4. Select the shift from the drop-down list.
5. Check the checkbox to enable **Multiple Shift Schedules**.

Note

After checking the **Multiple Shift Schedules**, you can select the effective timetable(s) from the added timetables for the persons.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.
If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.
8. Click **Save**.

8.4.3 Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The temporary schedule has higher priority than department schedule and person schedule.

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Temporary Schedule** to enter Temporary Schedule page.
3. Select the organization and select the person(s).

4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

   If **Non-Workday** is selected, you need to set the following parameters.

   Calculated as

   Select normal or overtime level to mark the attendance status for temporary schedule.

   Timetable

   Select a timetable from drop-down list.

   Multiple Shift Schedule

   It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.
   If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

   Rule

   Set other rule for the schedule, such as **Check-in Not Required**, and**Check-out Not Required**.
6. Click **Save**.

8.4.4 Check Shift Schedule

You can check the shift schedule in calendar or list mode. You ca also edit or delete the shift schedule.

Steps

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule Management page.
2. Select the organization and corresponding person(s).
3. Click  or  to view the shift schedule in calendar or list mode.

   Calendar

   In calendar mode, you can view the shift schedule for each day in one month. You can click the temporary schedule for one day to edit or delete it.

   List

   In list mode, you can view the shift schedule details about one person or organization, such as shift name, type, effective period and so on. Check the shift schedule(s), and click **Delete** to delete the selected shift schedule(s).

8.5 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record.

You can also edit, delete, search, or export the check-in or check-out record.

Before You Start

- You should add organizations and persons in Person module. For details, refer to ***Person Management***.
- The person's attendance status is incorrect.

Steps

1. Click **Time & Attendance** → **Attendance Handling** to enter attendance handling page.
2. Click **Correct Check-In/Out** to enter adding the check-in/out correction page.
3. Select person from left list for correction.
4. Select the correction date.
5. Set the check-in/out correction parameters.

Select **Check-in** and set the actual start-work time.Select **Check-out** and set the actual end-work time.

Note

You can click ⊕ to add multiple check in/out items. At most 8 check-in/out items can be supported.

6. Optional: Enter the remark information as desired.
7. Click **Save**.
8. Optional: After adding the check-in/out correction, perform one of the following operations.

View	Click ▦ or ☰ to view the added attendance handling information in calendar or list mode. **Note** In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.
Edit	● In calendar mode, click the related label on date to edit the details. ● In list mode, double-click the related filed in Date, Handling Type, Time, or Remark column to edit the information.
Delete	Delete the selected items.
Export	Export the attendance handling details to local PC. **Note** The exported details are saved in CSV format.

8.6 Add Leave and Business Trip

You can add leave and business trip when the employee want to ask for leave or go on a business trip.

Before You Start

You should add organizations and persons in the Person module. For details, refer to ***Person Management***.

Steps

1. Click **Time & Attendance** → **Attendance Handling** to enter attendance handling page.
2. Click **Apply for Leave/Business Trip** to enter adding the leave/business trip page.
3. Select person from left list.
4. Set the date(s) for your leave or business trip.
5. Select the major leave type and minor leave type from the drop-down list.

> **Note**
> You can set the leave type in Attendance Settings. For details, refer to ***Configure Leave Type***.

6. Set the time for leave.
7. Optional: Enter the remark information as desired.
8. Click **Save**.
9. Optional: After adding the leave and business trip, perform one of the following operations.

View	Click or to view the added attendance handling information in calendar or list mode. **Note** In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.
Edit	● In calendar mode, click the related label on date to edit the details. ● In list mode, double-click the filed in Date, Handling Type, Time, or Remark column to edit the related information.
Delete	Delete the selected items.
Export	Export the attendance handling details to local PC. **Note** The exported details are saved in CSV format.

8.7 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

8.7.1 Automatically Calculate Attendance Data

You can set a schedule so that the client can calculate the attendance data automatically at the time you configured every day.

Steps

Note

It will calculate the attendance data till the previous day.

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **General Rule**.
3. In the Auto-Calculate Attendance area, set the time that you want the client to calculate the data every day.
4. Click **Save**.

8.7.2 Manually Calculate Attendance Data

You can calculate the attendance data manually by setting the data range.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics** → **Calculate Attendance**.
3. Set the start time and end time to define the attendance data range.
4. Set other conditions, including department, person name, employee No. and attendance status.
5. Click **Calculate**.

Note

It can only calculate the attendance data within three months.

6. Perform one of the following operations.

Correct Check-in/out	Click **Correct Check-in/out** to add check-in/out correction.
Report	Click **Report** to generate the attendance report.
Export	Click **Export** to export attendance data to local PC.

Note

The exported details are saved in CSV format.

8.8 Attendance Statistics

You can check the original attendance record, generate and export the attendance report based on the calculated attendance data.

8.8.1 Get Original Attendance Record

You can search the employee's attendance time, attendance status, check point, etc. in a time period to get an original record of the employees.

Before You Start

- You should add organizations and persons in Person module and the persons has swiped card. For details, refer to ***Person Management***.
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data***.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics** → **Original Records**.
3. Set the attendance start time and end time that you want to search from.
4. Set other search conditions, such as department, person name, and employee No.
5. Optional: Click **Get from Device** to get the attendance data from the device.
6. Optional: Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.
   The result displays on the page. You can view the employee's required attendance status and check point.
8. Optional: After searching the result, perform one of the following operations.

Generate Report	Click **Report** to generate the attendance report.
Export Report	Click **Export** to export the results to the local PC.

8.8.2 Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start

Calculate the attendance data.

Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data***.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics** → **Report**.
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click **Report** to generate the statistics report and open it.

8.8.3 Custom Attendance Report

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

Steps

Note

Set the email parameters before you want to enable auto-sending email functions. For details, refer to ***Set Email Parameters***.

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics** → **Custom Report**.
3. Click **Add** to pre-define a report.
4. Set the report content.

Report Name

Enter a name for the report.

Report Type

Select one report type and this report will be generated.

Report Time

The time to be selected may vary for different report type.

Person

Select the added person(s) whose attendance records will be generated for the report.

5. Optional: Set the schedule to send the report to the email address(es) automatically.
   1) Check the **Auto-Sending Email** to enable this function.
   2) Set the effective period during which the client will send the report on the selected sending date(s).
   3) Select the date(s) on which the client will send the report.
   4) Set the time at which the client will send the report.

      Example

      If you set the effective period as ***2018/3/10 to 2018/4/10***, select ***Friday*** as the sending date, and set the sending time as ***20:00:00***, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

      Note

      Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data***.

   5) Enter the receiver email address(es).

      Note

      You can click **+** to add a new email address. Up to 5 email addresses are allowed.

   6) Optional: Click **Preview** to view the email details.
6. Click **OK**.
7. Optional: After adding the custom report, you can do one or more of the followings:

Edit Report	Select one added report and click **Edit** to edit its settings.
Delete Report	Select one added report and click **Delete** to delete it.
Generate Report	Select one added report and click **Report** to generate the report instantly and you can view the report details.

Chapter 9 Video Intercom

Video intercom is an audiovisual communication system used within a building or a small collection of buildings. With microphones and video camera devices at both sides, it enables the inter-communication via video and audio signals. A video intercom system can provide a safe and easy monitoring solution for apartment buildings and private houses.
Be sure to add video intercom devices to the client and link the indoor stations to the persons beforehand. You should also set the access authorization for the persons to open doors via the linked indoor stations.

Note

- Up to 16 door stations and 512 indoor stations or master stations can be managed in the client. For details about adding video intercom devices, refer to ***Add Device***.
- For details about adding persons, refer to ***Add Single Person***.
- For details about setting person's access authorization, refer to ***Set Access Group to Assign Access Authorization to Persons***.

9.1 Manage Calls between Client Software and an Indoor/Door Station/Access Control Device

You can call the residents by the client, and vice versa. You can also use an indoor station/door station or specified access control device to call the client.
Before making calls, you can set the parameters such as ring duration and speaking duration. For details, refer to ***Set Access Control and Video Intercom Parameters***.

9.1.1 Call Indoor Station from Client

You can call the added indoor station by the client to perform video intercom.

Before You Start

- Be sure to have added a resident to the client. For details, refer to ***Add Single Person***.
- Be sure to have linked the resident with an indoor station and configured the resident information (including floor No. and room No.) in Person module. For details about configuring the linkage and resident information, refer to ***Configure Resident Information***.

Steps

Note

- A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.

- You can remotely configure the Max. Ring Duration and the Max. Speaking Duration.

1. Click **Access Control** → **Video Intercom** → **Contacts**.
2. Unfold the organization list on the left panel and select an organization.
   The information (including resident name, linked device name and device IP address) of all the residents in the selected group will be displayed on the right panel.
3. Select a resident, or enter a keyword in the Filter field to find the desired resident.
4. Click to start calling the selected resident.

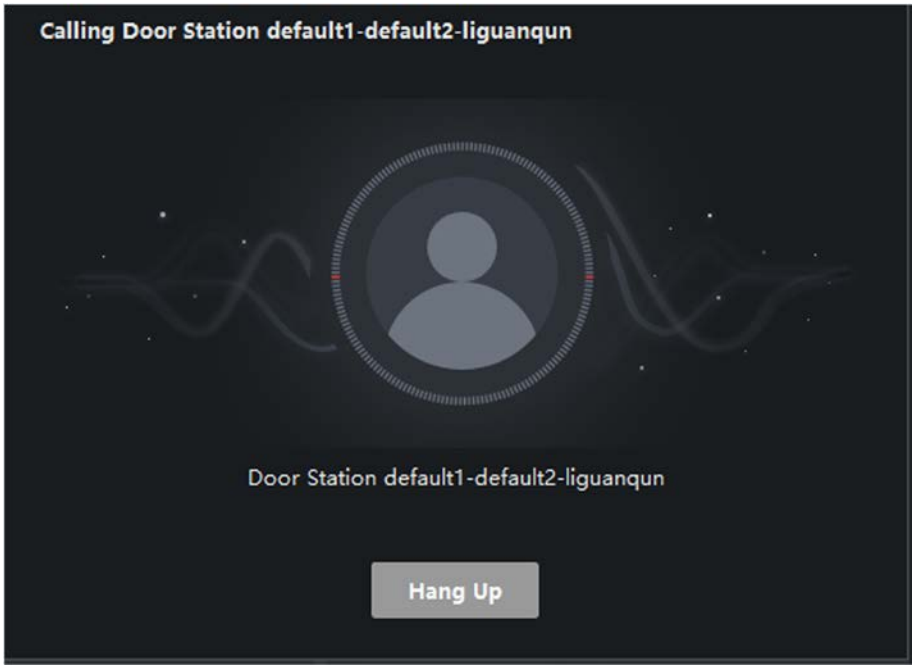

Figure 9-1 Start Calling Window

After the call is answered, you will enter the In Call window.

5. Optional: After the call is answered, perform the following operation(s).

Adjust Loudspeaker Volume	Click to adjust the volume of the loudspeaker.
End Speaking	Click **Hang Up** to end speaking.
Adjust Microphone Volume	Click to adjust the volume of the microphone.

9.1.2 Answer Call via Client

The residents can call the client by an indoor station, door station, or specific access control

devices and perform video intercom with the client.

Before You Start

- Be sure to have added a resident to the client. For details, refer to ***Add Single Person***.
- Be sure to have linked the added resident with an indoor station/outdoor station/access control device and configured the resident information (including floor No. and room No.) in Person module. For details about configuring the linkage and resident information, refer to ***Configure Resident Information***.

Steps

Note

- A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.
- You can remotely configure the Max. Ring Duration and the Max. Speaking Duration.

1. Click **Access Control** → **Video Intercom** → **Contacts**.
2. Unfold the organization list on the left panel and select an organization.
   The information (including resident name, linked device name and device IP address) of all the residents in the selected group will be displayed on the right panel.
3. Click to start calling a desired resident.
   An incoming call dialog will pop up.

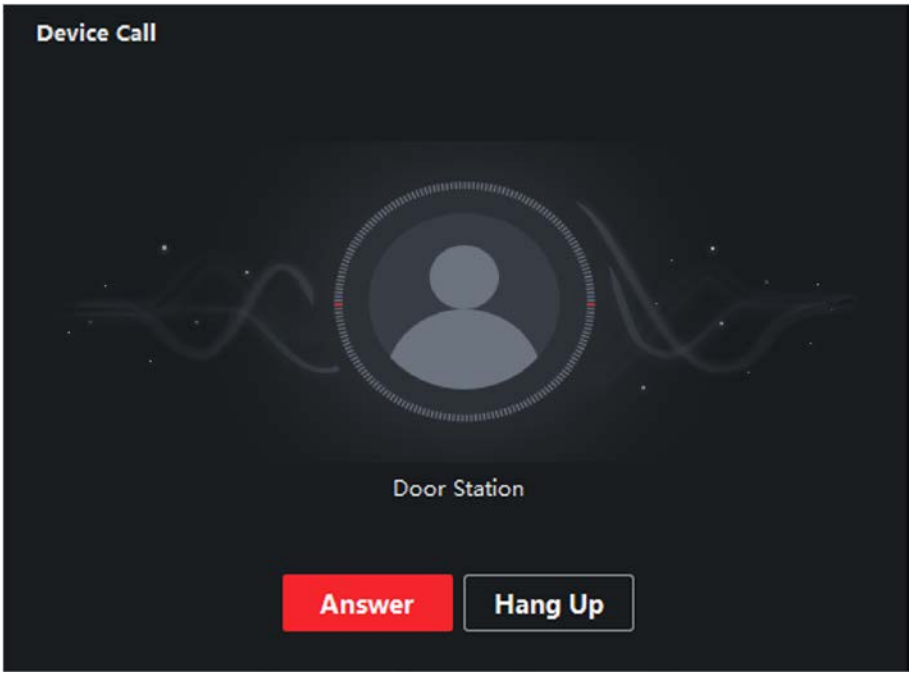

Figure 9-2 Incoming Call

4. Click **Answer** to answer the call.

After the call is answered, you will enter the In Call window.

5. Optional: In the In Call window, perform the following operation(s).

Adjust Loudspeaker Volume	Click to adjust loudspeaker's volume.
End Speaking	Click **Hang Up** to end speaking.
Adjust Microphone Volume	Click to adjust the microphone's volume.
Open Door	When an indoor station is linked with a door station, click to open the door linked with the door station.

9.2 View Real-Time Call Logs

You can view details of all the calls, and you can call the residents or export the logs if they are needed.

Steps

1. Click **Access Control** → **Video Intercom** → **Call Log**.
   Details of all the calls will be displayed on the right panel including call status, start time, speaking duration, device type and name, and organization and name of resident.
2. Optional: Click to re-dial the resident.
3. Optional: Set search conditions (including call status, device type, and time) on the top of the page to filter call logs.
4. Click **Export** to save the logs (a CSV file) in your PC.

9.3 Release a Notice to Resident

You can send a notice to the residents by one-touch. Four notice types are available: advertising, property, alarm, and notice information.

Steps

1. Click **Access Control** → **Video Intercom** → **Notice**.
2. Click **Add** to open the Create Notice panel.
3. Click to select the residents you are going to deliver notice to.
4. Enter the required information.

Note

- Up to 63 characters are allowed in the Subject field.
- Up to 1023 characters are allowed in the Content field.
- You can add up to 6 pictures. Each picture should be in JPG format and smaller than 512 KB.

5. Click **Send** to send the notice to the selected resident(s).
   Information about the sent notices will be displayed on the left panel. Click a notice to view its details on the right panel.
6. Optional: Click **Export** to save all the notices in your PC.

Chapter 10 Log Search

Two log types are provided: operation log and system log. The operation logs refer to the normal operations that the user did on the client, such as add device, log search, and reset password; and the system logs record the system information, such as login, logout, lock and unlock. You can search the log files and view the log details, including time, user, etc.

Steps

1. Enter the System Log module.
2. Click to specify the start time and end time.

Note

You can search the logs within one month.

3. Select a user to search the log files which are generated when this user log into the client.
4. Select **Operation Log** or **System Log** as log type.
5. Click **Search**.
   The log files between the start time and end time will be displayed on the list. You can check the operation time, type and other information of the logs.
6. Optional: Perform one of the following operations.

Filer	Click on each table header and select to filter the logs.
Sort	Click the table header to sort the logs by the time or letter sequence.
Backup	Click **Backup Log** to back up the search result to local PC.

Note

You can view the logs by importing the exported log files. For more details, refer to ***Operation and Maintenance***.

Chapter 11 User Management

To improve the system security, the administrator should create different account for different user, and assign different permissions to the user. To avoid different people sharing the same user account, we recommend you manage the user accounts periodically.

11.1 Add User

The super user and administrator can add new users, and assign different permissions for different users if needed.

Perform this task to add an user account.

Steps

Note

The user account you registered to log in the software is set as the super user.

1. Enter the User Management module.
2. Click **Add User** to show user information area.
3. Select the user type from the drop-down list.

   Administrator

   The administrator account has all permissions by default, and can modify the passwords and permissions of all operators and its own.

   Operator

   The operator account has no permission by default and you can assign the permissions manually. An operator can only change the passwords of its own account and the accounts which are added by it.
4. Enter the user name, password, and confirm password as desired.

Caution

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 following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Check the checkboxes to assign the permissions to the created user.
6. Optional: Click **Default Value** to restore the default permissions of this user.
7. Click **Save**.

Note

Up to 50 user accounts can be added for the client software.

After created user account successfully, the user account is added to the user list on the Account Management page.

8. Optional: Perform the following operations after the user account is created.

Edit User	Click a user from the list to edit the user information. **Note** Only the password of the super user can be edited.
Delete User	Select the user from the list and click **Delete User**. **Note** You cannot delete the super user.

11.2 Change User's Password

The administrator can change normal user's password without entering the old password, while the administrator should enter the old password when changing the password of itself.

Before You Start

Add user to the software client.

Steps

1. Enter the User Management module.
2. Select the user need to be change password, click **Change**.
3. Optional: Enter the old password.

Note

When changing the administrator's password, you need to enter the old password first.

4. Enter the new password and confirm the password.
5. Click **OK**.

Chapter 12 System Configuration

The general parameters, picture storage, alarm sound, email settings, file saving path, video intercom and access control parameters can be configured.

12.1 Set General Parameters

You can configure the frequently-used parameters, including log expired time, network performance, and etc.

Steps

1. Enter the System Configuration module.
2. Click **General** tab to enter the General Settings page.
3. Configure the general parameters.

   Log Expiry Date

   The time for keeping the log files. Once exceeded, the files will be deleted.

   Maximum Mode

   Select **Maximize** or **Full Screen** as the maximum mode. **Maximize** mode can maximize the display and show the taskbar. **Full Screen** mode can display the client in full-screen mode.

   Network Performance

   Set the network conditions to **Normal**, **Better** or **Best**.

   Automatic Time Synchronization

   Automatically synchronize the time of the added devices with the time of the PC running the client at a specified time point.
4. Click **Save**.

12.2 Set Picture Storage

The pictures, captured by the camera of video access control terminal, triggered by events, can be saved in the PC running the Nivian Control Center AC Service.

Steps

1. Enter the System Configuration module.
2. Click **Picture Storage**.
3. Set the **Store Pictures in Server** switch to on.
   All the disks of the PC running the service will show.
4. Select the disk to save the pictures.

Note

The default saving path is: Disk/Nivian Control Center ACalarmPicture

5. Click **Save**.

12.3 Set Alarm Sound

When the event, such as access control event, is triggered, the client can be set to give an audible warning and the sound of the audible warning can be configured.

Steps

1. Open the System Configuration page.
2. Click **Alarm Sound** tab to enter the Alarm Sound Settings page.
3. Optional: Click ··· and select the audio files from the local path for different events.
4. Optional: Add customized alarm sound.
   1) Click **Add** to add customized alarm sound.
   2) Double click the **Type** field to customize the alarm sound name as desired.
   3) Click ··· and select the audio files from the local path for different alarms.
5. Optional: Click for a testing of the audio file.
6. Optional: Click in the Operation column to delete the custom sound.
7. Click **Save**.

Note

The format of the audio file can only be WAV.

12.4 Set Access Control and Video Intercom Parameters

You can configure the access control and video intercom parameters according to actual needs.

Steps

1. Open the System Configuration page.
2. Click the **Access Control & Video Intercom** tab.
3. Input the required information.

Ringtone

Click ··· and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click for a testing of the audio file.

Max. Ring Duration

Specify the seconds that the ring will last for at most. The maximum ring duration can be set from 15s to 60s.

Max. Speaking Duration with Indoor Station

Specify the seconds that the call with indoor station will last for at most. The maximum speaking duration between indoor station and the client can be set from 120s to 600s.

Max. Speaking Duration with Door Station

Specify the seconds that the call with door station will last for at most. The maximum speaking duration between door station and the client can be set from 90s to 120s.

Max. Speaking Duration with Access Control Device

Specify the seconds that the call with access control device will last for at most. The maximum speaking duration between access control device and the client can be set from 90s to 120s.

4. Click **Save**.

12.5 Set File Saving Path

The system configuration files and the pictures manually captured in Status Monitoring are stored on the local PC. The saving paths of these files can be set.

Steps

1. Open the System Configuration page.
2. Click **File** tab to enter the File Saving Path Settings page.
3. Click ··· and select a local path for the files.
4. Click **Save**.

12.6 Set Email Parameters

An email notification can be sent when an event occurs. To send the email to some specified receivers, the settings of the email need to be configured before proceeding.

Steps

1. Enter the System Configuration module.
2. Click **Email** tab to enter the Email Settings interface.
3. Enter the required information.

STMP Server

The STMP server IP address of host name (e.g., smtp.263xmail.com)

Encryption Type

You can check the radio to select **Non-Encrypted**, **SSL**, or **STARTTLS** .

Port

Enter the communication port used for SMTP. The port is 25 by default.

Sender Address

The email address of the sender.

Security Certificate (Optional)

If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

User Name

Enter the user name of the sender email address if **Server Authentication** is checked.

Password

Enter the password of the sender Email address if **Server Authentication** is checked.

Receiver 1 to 3

Input the email address of the receiver. Up to 3 receivers can be set.

4. Optional: Click **Send Test Email** to send an email to the receiver for test.
5. Click **Save**.

Chapter 13 Operation and Maintenance

You can perform maintaining operations in the menu to ensure a smooth and convinient usage of the client.
Click  in the upper-right corner, and then click **File**/**System**/**Tool** to perform the following operations.

Open Log File

You can open a log file saved in your local PC or log files of the client.

Import/Export Configuration File

You can import configuration files (of Nivian Control Center AC V2.7.0 and above) from local PC to the client, and vice versa. The following client modules' configuration files are allowed to be imported/exported: Access Control, Device Management, Event Center, Person, Time and Attendance, and Framework of the client.

Auto Backup

Select day and time to backup configuration files and data in database, or restore the backuped data.

Batch Time Sync

Synchronize selected devices' time with your PC time.

Message Queue

After configuring email linkage, the triggered event(s) will be displayed here. Select an event and cancel sending the an email to the receiver.

A. Custom Wiegand Rule Descriptions

Take Wiegand 44 as an example, the setting values in the Custom Wiegand tab are as follows:

Custom Wiegand Name	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Mode	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Wiegand Data

Wiegand Data = Valid Data + Parity Data

Total Length

Wiegand data length.

Transportation Rule

4 bytes. Display the combination types of valid data. The example displays the combination of Card ID and Manufacturer Code. The valid data can be single rule, or combination of multiple rules.

Parity Mode

Valid parity for Wiegand data. You can select either odd parity or even parity.

Odd Parity Start Bit, and Length

If you select Odd Parity, these items are available. If the odd parity start bit is 1, and the length is 12, then the system will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0. (Bit 0 is the first bit.)

Even Parity Start Bit, and Length

If you select Even Parity, these items are available. If the even parity start bit is 12, and the length is 12, then the system will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

XOR Parity Start Bit, Length per Group, and Total Length

If you select XOR Parity, these items are available. Depending on the table displayed above, the start bit is 0, the length per group is 4, and the total length is 40. It means that the system will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits. (The result length is the same as the length per group.)

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.


NIVIAN

NIVIAN Control Center AC Software

Manual de usuario

V1.0 build 07082019

Información legal

Manual de usuario

Sobre este manual

Se recomienda utilizar este manual bajo la supervision de un profesional.

Marcas Comerciales

Renuncia

Hasta lo permitido por la ley, Nivian no ofrece garantías, expresas ni explícitas, incluyendo sin limitación las garantías implícitas de comerciabilidad y adecuación para un propósito correspondiente a este manual. Nivian no garantiza ni hace ninguna representación con respecto al uso del manual o la correción, precisión o confiabilidad de la información contenida. El uso de este manual, o la correción, exactitud o confiabilidad de la información contenida aquí. El uso de este manual y cualquier confianza en este manual está por lo tanto a su propio riesgo y responsabilidad.

Con respecto al producto con acceso a internet Nivian no tiene responsabilidades por operaciones anormales, fugas de privacidad o otros daños resultantes del ataque cibernético, ataques de hacker, inspección de virus u otros riesgos de seguridad de internet; sin embargo, Nivian proporcionará apoyo técnico a tiempo si se requiere.

Las leyes de vigilancia varían por la jurisdicción. Por favor, comprobar las leyes relevantes en su jurisdicción antes de usar este producto para asegurar que su uso conforme la ley aplicable. Nivian no será responsable en caso de que este producto se utilice con propósitos ilegítimos.
En el caso de cualquier conflicto entre este manual y la ley aplicable, los última se aplica.

Leyenda de Símbolos

Los símbolos que podrás encontrar en este document están definidos de la siguiente manera:

Símbolo	Descripción
Peligro	Indica una situación peligrosa que, si no se evita, ocasionará o podría causar lesiones graves o la muerte.
Precaución	Indica una situación potencialmente peligrosa que, de no evitarse, podría provocar daños en el equipo, pérdida de datos o resultados inesperados.
Nota	Proporciona información adicional para enfatizar o complementar puntos importantes del texto principal.

Contenido

Capítulo 1 Introducción

El software incorpora múltiples funcionalidades, incluyendo gestión del personal, control de accesos, video portero, control de presencia, etc. Para que los dispositivos conectados cumplan con las necesidades específicas de las tareas de monitorización requeridas. Con una estructura distribuida flexible y facilidad de uso de las operaciones, el software es complete para aplicarse a los proyectos de seguridad pequeños o medianos.

Este manual de Usuario describe las funciones, configuraciones y operaciones del software. Para asegurar el uso amigable y la estabilidad del software, se debe referir a los contenidos mostrados a lo largo del manual leyéndolo cuidadosamente antes de la instalación y configuración.

Capítulo 2 Uso automático del software

La utilidad automática de Nivian Control Center AC es principalmente el almacenaje, gestion y cálculo de datos. Con el software ejecutado, se pueden gestionar los datos, tales como eventos y registros de presencia, recibiéndolos a través del Software Nivian Control Center AC. El uso del software también permite la configuración de los permisos de Usuario, dispositivos, grupos, registros, etc.

Se puede ver el estado de funcionamiento del módulo y editar los puertos, incluyendo los puertos HTTP y de la aplicación EHome. Para ello, se necesita reiniciar el software.

Comprobar **Inicio Automático** para habilitar de forma automática que Nivian Control Center AC inicie el auto guardado de datos después de reiniciar el PC.

Nota

- *La utilidad automática del Nivian Control Center AC no se mostrará despues de ejecutarse. Debe entrar en el sistema y hacer click en*  *para abrir la Ventana de utilidad automática.*
- *Después de cerrar la ventana, el software cerrará sesión y volverá a la página de inicio de sesión. Se necesita ejecutar el servicio y volver a registrar.*
- *El servicio y el software cliente deberán ser instalados en el mismo ordenador.*

Capítulo 3 Gestión del Dispositivo

Se pueden gestionar dispositivos incluyendo el añadido, editado y borrado de los mismos. También se pueden realizar otras operaciones como el estado del dispositivo.

3.1 Añadir un dispositivo

Después de ejecutar el software, los dispositivos de control de acceso, videoporteros, etc, se deben añadir al software para la gestion y configuración de forma remota, así como controlar el estado de la puerta, administrar el control de presencia, la configuración de los eventos, etc.

3.1.1 Activar dispositivos

Algunos dispositivos, requieren la creación de una contraseña para activarlos antes de que puedan ser añadidos al software y funcionen de forma correcta.

Pasos

Nota

Esta función deberá ser soportada por el dispositivo.

1. Entre en el modulo Gestión de dispositivo.
2. Opcional: Hacer click en arriba a la derecho de **Gestión de dispositivo** y seleccionar **Dispositivo**.
   Se mostrará un listado con los dispositivos añadidos.
3. Hacer click sobre **Dispositivos en línea** para visualizar los dispositivos en el área de dispositivos en línea.
   La búsqueda de dispositivos son mostradas sobre la lista.
4. Comprobar el estado del dispositivo (mostrado en la columna **Nivel de Seguridad**) y seleccionar un dispositivo inactivo.
5. Hacer click en **Activar** para abrir el cuadro de activación.
6. Crear una contraseña en el campo de contraseña y confirmarla escribiéndola de nuevo.

Precaución

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

7. Pulsar **OK** para activar el dispositivo.

3.1.2 Añadir un dispositivo en línea

Los dispositivos en línea dentro de la misma red local serán visualizados con el software cliente en el área **Dispositivos en línea**.

Nota

*Puede hacer click en **Actualizar cada 60s** para refrescar la información de los dispositivos en línea.*
*La función SADP puede ser habilitada o deshabilitada hacienda click en **Dispositivos en línea**.*

Añadir un dispositivo en línea

Se puede añadir un dispositivo al software.

Pasos

1. Entrar en el módulo Gestión de dispositivos.
2. Opcional: Hacer click en la parte superior izquierda de **Gestión de Dispositivos** y seleccionar **Dispositivo**. Los dispositivos añadidos son mostrados en la lista.
3. Hacer click en **Dispositivos en línea** para mostrarlos en el área de dispositivo.
   La búsqueda de dispositivos es mostrada en la lista.
4. Seleccionar un dispositivo en línea desde el área de **Dispositivos en línea**.

   Nota

   *Para un dispositivo inactivo, se necesita crear una contraseña antes de poder añadir el dispositivo correcto. Para más detalles, ver **Activar Dispositivos**.*

5. Hacer click en **Añadir** para abrir el cuadro de diálogo.
6. Introducir la información requerida.

Nombre

Introducir un nombre descriptivo para el dispositivo.

Dirección

La dirección IP del dispositivo es obtenida automáticamente en el Modo de añadir.

Puerto

El Puerto es obtenido automáticamente.

Nombre del usuario

Por defecto el nombre de Usuario es admin.

Contraseña

Introducir la contraseña del dispositivo.

Precaución

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

7. Opcional: Marque **Sincronizar Hora** para sincronizar la hora en el dispositivo con la del PC en el que se está ejecutando el software en el momento de añadir el dispositivo.
8. Opcional: Marque **Importar a Grupo** para crear un grupo con el nombre del dispositivo.

Nota

Por defecto puede importar todos los canales del dispositivo al grupo correspondiente.

9. Hacer click en **OK** para añadir el dispositivo.

Añadir múltiples dispositivos en línea

Se pueden añadir múltiples dispositivos en línea.

Pasos

1. Entre en el módulo de Gestión de dispositivos.
2. Opcional: Hacer click en la parte superior derecho de **Gestión de dispositivos** y Seleccionar **Dispositivo**.
   Los dispositivos añadidos serán mostrados en la lista.
3. Hacer click en **Dispositivo en línea** para mostrar área de Dispositivo en línea.
   La búsqueda de Dispositivo en línea serán mostrados en la lista.
4. Seleccionar múltiples dispositivos.

Nota

*Para un dispositivo inactivo, se debe crear la contraseña antes de poder agregar el dispositivo. Para obtener información detallada sobre los pasos, consultar **Dispositivos activos**.*

5. Hacer click en **Añadir** para abrir la Ventana de dispositivos añadidos.
6. Introducir la información requerida.

Nombre de usuario

Por defecto el nombre de Usuario es admin.

Contraseña

Introducir la contraseña del dispositivo.

Atención

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

7. Opcional: Marque **Sincronizar Hora** para sincronizar la hora del PC en el que está instalado el software con el dispositivo que se esté añadiendo.
8. Opcional: Marque **Importar a Grupo** para crear un grupo con el nombre del dispositivo.

Nota

Por defecto se pueden importar todos los canales del dispositivo al grupo correspodiente.

9. Hacer click en **OK** para añadir los dispositivos.

3.1.3 Añadir Dispositivo por Dirección IP o Nombre de Dominio

Cuando se conoce la dirección IP o el nombre del dominio del dispositivo que se desea agregar se pueden agregar dispositivos al Software especificando la dirección IP (o el Nombre del Dominio), Nombre de Usuario, Contraseña y otros parámetros relacionados.

Pasos

1. Entre en el módulo Gestión de dispositivos.
2. Opcional: Hacer click en la parte superior del módulo **Gestión de dispositivos** y seleccionar **Dispositivo**.
   Los dispositivos añadidos serán mostrados en la lista.
3. Hacer click en **Añadir** para abrir la Ventana de agregar dispositivo.
4. Seleccionar **IP/Dominio** en el Modo de Añadir.
5. Introducir la información requerida, incluyendo Nombre, dirección, puerto, usuario, y contraseña.

Nombre

Crear un nombre descriptivo para el dispositivo. Por ejemplo, usar el nombre que puede mostrar la localización o parámetro del dispositivo.

Dirección

La dirección IP o nombre del dominio del dispositivo.

Puerto

Los dispositivos a añadir tienen el mismo número de Puerto. El valor por defecto es 8000.

Nombre de usuario

Introducir el nombre de Usuario. Por defecto es admin.

Contraseña

Introducir la contraseña del dispositivo.

Atención

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

6. Opcional: Marcar **Sincronizar Hora** para sincronizar la hora del PC en el que está instalado el software con el dispositivo que se esté añadiendo.
7. Opcional: Marcar **Importar a Grupo** para crear un grupo con el nombre del dispositivo.

Nota

Por defecto se pueden importar todos los canales del dispositivo al grupo correspondiente.

8. Para finalizar el agregado del dispositivo.
   – Hacer click en **Añadir** para agregar el dispositivo y Volver a página que lista los dispositivos.
   – Hacer click en **Añadir y Nuevo** para guardar la configuración y continuar añadiendo otros dispositivos.
9. Realizar las siguientes operaciones despues de añadir dispositivos.

Configuración remota	Hacer click en sobre la Columna Operación para configurar de forma remota el dispositivo correspondiente.

Nota

*Para algunos modelos de dispositivos, se puede abrir una Ventana a través del navegador web. Para abrir la configuración remota original, pulsar **Ctrl** y hacer click en .*
Para los detalles de los pasos de operación para la configuración remota, ver el manual de uso del dispositivo.

Estado del Dispositivo	Hacer click en la columna de operación para ver el estado del dispositivo.

3.1.4 Añadir Dispositivos por rango IP

Si se quiere añadir dispositivos cuya dirección IP esté dentro de un rango IP, se puede especificar las

direcciones inicial y final de IP, nombre de usuario, contraseña, y otros parámetros para añadir.

Pasos

1. Entrar en el módulo Gestión de dispositivos.
2. Opcional: Hacer click en la parte derecho de **Gestión de dispositivos** y Seleccionar **Dispositivo**. Los dispositivos añadidos serán mostrados en la lista.
3. Hacer click en **Añadir** para abrir la Ventana de agregar dispositivo.
4. Seleccionar **Segmento IP** en el Modo de Añadir.
5. Introducir la información requerida.

IP inicial / IP final

Introducir una dirección IP inicial.
Introducir una dirección IP final en el mismo rango que la IP inicial.

Puerto

Introducir el número del Usuario. Por defecto es 8000.

Nombre de usuario

Por defecto el Usuario es admin.

Contraseña

Introducir la contraseña del dispositivo.

Atención

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

6. Opcional: Marque **Sincronizar Hora** para sincronizar la hora del PC en el que está instalado el software con el dispositivo que se esté añadiendo.
7. Opcional: Marque **Importar a Grupo** para crear un grupo con el nombre del dispositivo.

Nota

Se pueden importar todos los canales del dispositivo al grupo correspondiente por defecto.

8. Para finalizar el agregado de los dispositivos.
   – Hacer click en **Añadir** para agregar el dispositivo y Volver a la página de lista de dispositivos.
   – Hacer click en **Añadir y Nuevo** para guardar la configuración y continuar añadiendo dispositivos.
9. Opcional: Hacer click en sobre la Columna de Operación para visualizar el estado del dispositivo.

3.1.5 Añadir Dispositivo por cuenta EHome

Para áreas donde los dispositivos utilizan direcciones IP dinámicas en lugar de estáticas, se puede agregar un dispositivo de control de accesos conectados a través del protocolo EHome especificando la cuenta de EHome.

Antes de empezar

Establacer el parámetro del centro de red primero. Para más detalles, referirse a ***Configuración de parámetros de red***.

Pasos

Nota

Para los dispositivos agregados por EHome, no se admite la carga de eventos con imágenes capturadas por el software.

1. Entrar en el módulo de Gestión de dispositivos.
2. Opcional: Hacer click en sobre la parte derecho de **Gestión de dispositivos** y Seleccionar **Dispositivo**.
   Los dispositivos añadidos serán mostrados en la lista.
3. Hacer click en **Añadir** para abrir una nueva Ventana.
4. Seleccionar **EHome** como el Modo de Añadir.
5. Introducir la información requerida.

   Cuenta del dispositivo

   Introducir el nombre de la cuenta registrado en el protocolo EHome.

   Clave EHome

   Introducir la clave de EHome si se ha configurado cuando se han introducido los parámetros de red del dispositivo.

   Nota

   Esta función deberá ser soportada por el dispositivo.

6. Opcional: Marque **Sincronizar Hora** para sincronizar la hora del PC en el que está instalado el software con el dispositivo que se esté añadiendo.
7. Opcional: Marque **Importar a Grupo** para crear un grupo con el nombre del dispositivo.
8. Para finalizar el agregado de los dispositivos.
   - Hacer click en **Añadir** para agregar el dispositivo y Volver a la página de lista de dispositivos.
   - Hacer click en **Añadir y Nuevo** para guardar la configuración y continuar añadiendo dispositivos.
9. Opcional: Hacer click en sobre la Columna de Operación para visualizar el estado del dispositivo.

3.1.6 Importar Dispositivos en Grupo

Los dispositivos pueden ser añadidos al software en un lote introduciendo la información del

dispositivo en el archivo CSV predefinido.
Los dispositivos pueden ser añadidos al software de la siguiente manera:

Pasos

1. Entre en el modulo de Gestión de dispositivos.
2. Opcional: Hacer click en la parte derecho de **Gestión de dispositivos** y Seleccionar **Dispositivo**.
3. Hacer click en **Añadir** para abrir la Ventana de añadir dispositivos.
4. Seleccionar **Importación por lotes** en el Modo de Añadir.
5. Hacer click en **Exportar Plantilla** y entonces guardar la plantilla pre-definida (archivo CSV) en el PC.
6. Abrir el archivo con la plantilla exportada e introducir la información requerida de los dispositivos para que estos sean añadidos en las columnas correspondientes.

Modo de Añadir

Se puede introducir un ***0*** o un ***1*** lo que indica diferentes modos de añadir. ***0*** indica que el dispositivo es añadido por dirección IP o nombre del dominio; ***1*** indica que el dispositivo es añadido vía EHome.

Dirección

Editar la dirección del dispositivo. Si se establace ***0*** como Modo de Añadir, se debe introducir la Dirección IP o Nombre del dominio del dispositivo; si se establace un ***1*** como Modo de Añadir, este archivo no es obligatorio.

Puerto

Introducir el puerto del dispositivo. El valor por defecto es 8000.

Información del dispositivo

Si se configura con ***0*** como Modo de Añadir, este campo no es requerido. Si se configurar como ***1*** el Modo de Añadir, debe introducir la cuenta EHome.

Nombre de Usuario

Introducir el nombre del Usuario. Por defecto, el Usuario es admin.

Contraseña

Si se establace un ***0*** como el Modo de Añadir, Introducir la contraseña. Si se configura como un ***1*** el Modo de Añadir, Introducir su clave EHome.

Atención

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

Importar al Grupo

Puede introducir un ***1*** para crear un Grupo con el nombre del dispositivo. Todos los canales del dispositivos serán importados al grupo correspondiente por defecto. ***0*** indicaría que se dejaría deshabilitada esta función.

7. Hacer click en ··· y seleccionar la plantilla. hacer click en ··· y seleccionar la plantilla.
8. Hacer click en **Añadir** para importar los dispositivos. hacer click en **Añadir** para importar los dispositivos.

3.2 Editar la Información de Red del Dispositivo

Después de activar el dispositivo, se puede editar la información de la red para el dispositivo en línea.

Antes de empezar

Activar el dispositivo si el estado del dispositivo es inactivo.

Pasos

1. Entre en el módulo de Gestión de dispositivos.
2. Opcional: Hacer click en ▲ la parte derecho de **Gestión de dispositivos** y seleccionar el **Dispositivo**.
3. Hacer click en **Dispositivo en línea** para mostrar el área de Dispositivos en línea.
   Todos los dispositivos en Linea en la misma red local aparecerán mostrados en la lista.
4. Seleccionar un dispositivo activado en el área del **Dispositivo en línea**.
5. Hacer click en ⊕ sobre la Columna de Operación para abrir y Modificar los Parámetros de red del dispositivo.

Nota

*Esta función solo está disponible en el área **Dispositivo en línea.** Se puede cambiar la dirección IP del dispositivo a la misma red local con su ordenador si se necesita agregar el dispositivo al software.*

6. Cambiar la dirección IP del dispositivo a la misma red local con su ordenador.
   – Editar la dirección IP manualmente.
   – Comprobar **DHCP**.
7. Introducir la contraseña creada cuando se active el dispositivo.
8. Hacer click en **OK** para completer las configuraciones de la red.

3.3 Resetear la contraseña del dispositivo

Si se olvida la contraseña de los dispositivos que están en línea, se pueden restablacer la contraseña a través del software.

Pasos

1. Entre en el módulo de Gestión de dispositivos.
2. Opcional: Hacer click en ▲ la parte derecho de **Gestión de dispositivos** y Seleccionar **Dispositivo**.

3. Hacer click en **Dispositivo en línea** para mostrar el área de Dispositivos en línea.
   Todos los Dispositivos en línea en la misma red local estarán mostrados en la lista.
4. Seleccionar el dispositivo desde la lista y hacer click en la columna de operaciones.
5. Resetear la contraseña del dispositivo.
   – En la página con los campos de botón de exportación, contraseña y confirmación de contraseña hacer click en **Exportar** para guardar el fichero del dispositivo en su PC y después enviar el archivo a Soporte Técnico.

   Nota

   Resetear la contraseña para realizar las siguientes operaciones, contactar con el soporte técnico.

   – Si GUID es soportado, se puede importar los archivos GUID que son guardados cuando se activa el dispositivo.

   Nota

   Resetear la contraseña para realizar las siguientes operaciones, contactar con el soporte técnico.

Precaución

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

Capítulo 4 Gestión de Grupos

Los recursos agregados deben organizarse en grupos para una administración conveniente, como los puntos de control de acceso. Puede realizar algunas operaciones adicionales del dispositivo a través del grupo.

4.1 Añadir Grupo

Se puede agregar un grupo para organizar el dispositivo agregado para una Administración conveniente.

Pasos

1. Entre en el módulo de Gestión de dispositivos.
2. Hacer click en → **Grupo** para entrar en la página de gestion de Grupos.
3. Crear un grupo.
   - Hacer click en **Añadir Grupo** e introducir el nombre que se quiera al Grupo.
   - Hacer click en **Crear Grupo con Nombre de dispositivo** y Seleccionar un dispositivo añadido para crear un Grupo nuevo por el nombre del dispositivo seleccionado.

4.2 Importar Recursos a un Grupo

Se puede importar los recursos del dispositivo al grupo en un lote.

Antes de empezar

Añadir un Grupo para la gestion de dispositivos. Ver ***Añadir Grupo***.

Pasos

1. Introducir el módulo de Gestión de dispositivos.
2. Hacer click en → **Grupo** para entrar en la página de gestion de Grupo.
3. Seleccionar un Grupo desde la lista de Grupos y Seleccionar el tipo de Fuente **Punto de Control de Accesos**.
4. Hacer click en **Importar**.
5. Seleccionar los nombres del canal desde que son importados al área.
6. Hacer click en **Importar** para importar los recursos seleccionados del grupo.

4.3 Editar los Parámetros del Recurso

Después de importar los recursos al grupo, se puede editar los parámetros del recurso. Para los puntos de control de acceso, se puede editar el Nombre.

Antes de empezar

Importar los recursos al grupo. Ver en ***Importar Recursos al Grupo***.

Pasos

1. Introducir el módulo de Gestión de dispositivos.
2. Hacer click en → **Grupo** para entrar en la página de gestion del Grupo.
   Todos los grupos añadidos serán visualizados en la izquierda de la pantalla.
3. Seleccionar un Grupo sobre el listado y hacer click en tipo de recurso.
   Los canales del dispositivo serán importados y visualizados en el grupo.
4. Hacer click en la Columna de operaciones para abrir la Ventana de Modificación.
5. Editar la información requerida.
6. Hacer click en **OK** para guardar las nuevas configuraciones.

4.4 Eliminar los Recursos del Grupo

Se pueden eliminar los archivos añadidos desde el grupo.

Pasos

1. Entrar el módulo de Gestión de dispositivos.
2. Hacer click en → **Grupo** para entrar en la página de gestion del grupo.
   Todos los grupos añadidos serán visualizados en la parte izquierda.
3. Hacer click en un Grupo para mostrar los recursos añadidos a este Grupo.
4. Seleccionar los recurso(s) y hacer click en **Borrar** para eliminar los recurso(s) desde el Grupo.

Capítulo 5 Centro de Eventos

Se puede configurar el evento de los recursos agregados y configurar las acciones de vinculación para que, cuando se active el evento, el software pueda notificar al personal de seguridad y registrar los detalles del evento para verificarlos posteriormente.
En la página de Gestión de Eventos, se puede configurar el evento de control de accesos. Para más detalles sobre la configuración de control de evento.
En el centro de eventos, se puede ver los eventos en tiempo real y buscar los eventos históricos. Para obtener más información, ver ***Eventos en Tiempo Real*** y ***Buscar Eventos Históricos***.

5.1 Habilitar la Recepción de Eventos desde Dispositivos

Antes de que el software pueda recibir la información del evento desde el dispositivo, se necesita primero armar el dispositivo.

Pasos

1. Hacer click en → **Herramienta** → **Control de Armado de Dispositivo** abrir la página de Control de Armado de Dispositivo.
   Todos los dispositivos añadidos son mostrados en esta página.
2. En la columna de operación, encienda el interruptor para habilitar el armado automático o hacer click en **Armar Todo** para armar todos los dispositivos.

Nota

Un dispositivo de control de accesos solo puede ser armado por un cliente.

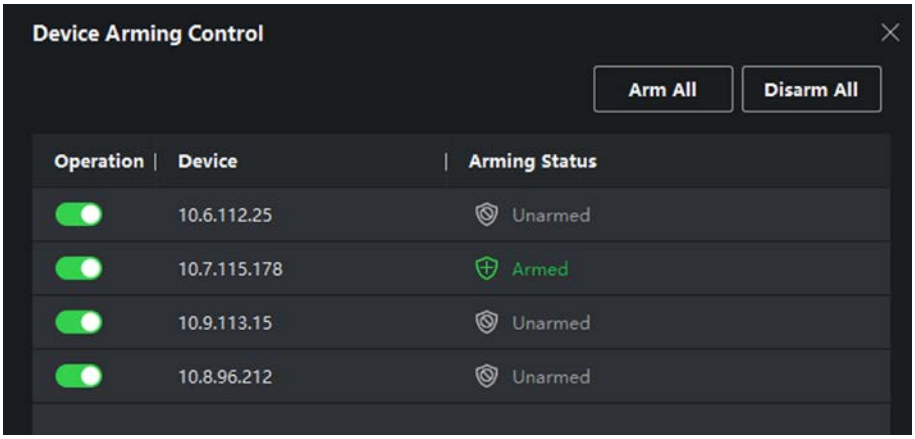

Figure 5-1 Dispositivo armado

3. Ver el estado de armado de cada dispositivo en la Columna de Estado de Armado.

Resultado

Los eventos de dispositivos armados son automáticamente actualizados en el software cuando se desencadena el evento.

5.2 Ver Eventos en Tiempo Real

En el módulo de Evento en Tiempo Real de la página del centro de eventos, se puede ver la información del Evento en Tiempo Real, incluyendo la Fuente del evento, tiempo del evento, prioridad, palabras claves del evento.

Antes de empezar

Habilitar la Recepción de Eventos desde Dispositivos antes de que el software pueda recibir la información del evento desde el dispositivo, ver ***Habilitar la Recepción de Eventos desde Dispositivos*** para más detalles.

Pasos

1. Hacer click en **Centro de Evento** → **Evento en Tiempo Real** para introducir la página Evento en Tiempo Real y poder ver el Evento en Tiempo Real recibido por el software.

   Hora del Evento

   Para un dispositivo de video, la Hora del Evento es el tiempo del software en el que se recibe el evento. Para un dispositivo que no sea de video, la hora del evento es cuando se desencadena el evento.

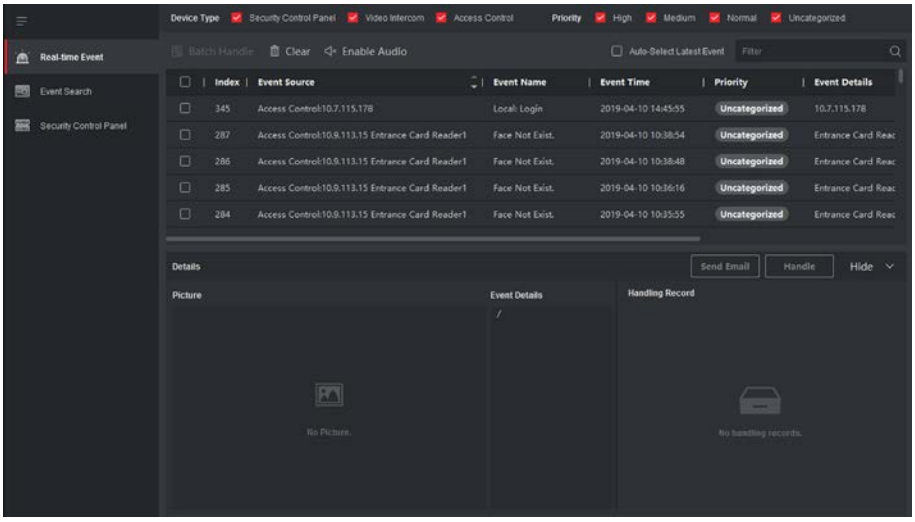

Figure 5-2 Evento en Tiempo Real

2. Configurar las condiciones del filtro o Introducir la palabra clave del evento en el campo de texto Filtro para mostrar solo los eventos requeridos.

   Tipo de dispositivo

   El tipo de dispositivo en el que ocurre el evento.

   Prioridad

   La prioridad del evento que indica el grado de urgencia del evento.

3. Opcional: Hacer click con el botón derecho en el encabezado de la lista de eventos para personalizar los elementos relacionados con eventos que se muestran en la lista de eventos.

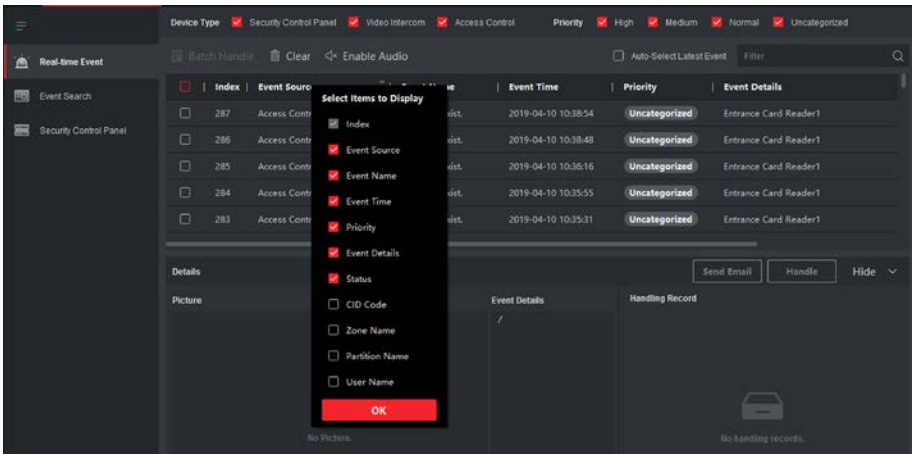

Figure 5-3 Personalizar la información mostrada

4. Ver los detalles de la información del evento.
   1) Selecciona un evento en la lista de eventos.
   2) Hacer click en **Expandir** en la esquina inferior derecha de la página.
   3) Ver la imagen relacionada, descripción del detalle y entrega de registros del evento.
   4) Opcional: Colocar el cursor sobre la imagen relacionada, y después hacer click en el icono de descarga en la esquina superior derecho de la imagen para descargarla en el ordenador local. Se puede configurar la ruta de guardado manualmente.
5. Opcional: Realiza las siguientes operaciones si es necesario.

Manejo de un Solo Evento	Hacer click en **Manejo** para introducir la sugerencia de procesamiento, y después hacer click en **Confirmar**.

Nota

*Después de un evento modificado, el botón **Procesar** se convertirá en **Añadir Observación**. Hacer click en **Añadir Observación** para añadir más información al evento manejado.*

Manejar Eventos en un Lote	Seleccionar los eventos que necesitan ser procesados, y después hacer click en **Manejo en Lote**. Introducir la sugerencia de procesamiento, y después hacer click en **Confirmar**.
Habilita/Deshabilita Alarma de Audio	Hacer click en **Activar Audio/Desactivar Audio** para habilitar/ deshabilitar el audio del evento.
Seleccionar el último evento automáticamente	Comprobar **Auto-Seleccionar el último Evento** para seleccionar el evento más reciente automáticamente y se visualizan los detalles de la información del evento.
Borrar Eventos	Hacer click en **Borrar** para borrar todos los eventos en la lista de eventos.

Enviar email	Seleccionar un evento y después hacer click en **Enviar Email**, y los detalles de la información de este evento serán enviados por email.

Nota

*Se deben configurar los parámetros del email primero, ver **Configurar los Parámetros de Email** para más detalles.*

5.3 Buscar el Histórico de Eventos

En el módulo de Búsqueda de Eventos de la página del centro de eventos, se pueden buscar los eventos históricos por tiempo, tipo de dispositivo, y otras condiciones según el tipo de dispositivo especificado y luego procesar los eventos.

Antes de empezar

Habilitar la Recepción de Eventos desde Dispositivos antes de que el software pueda recibir la información del evento desde el dispositivo, ver ***Habilitar la Recepción de Eventos desde Dispositivos*** para más detalles.

Pasos

1. Hacer click en **Centro de Evento** → **Buscar evento** para introducir la página de búsqueda del evento.

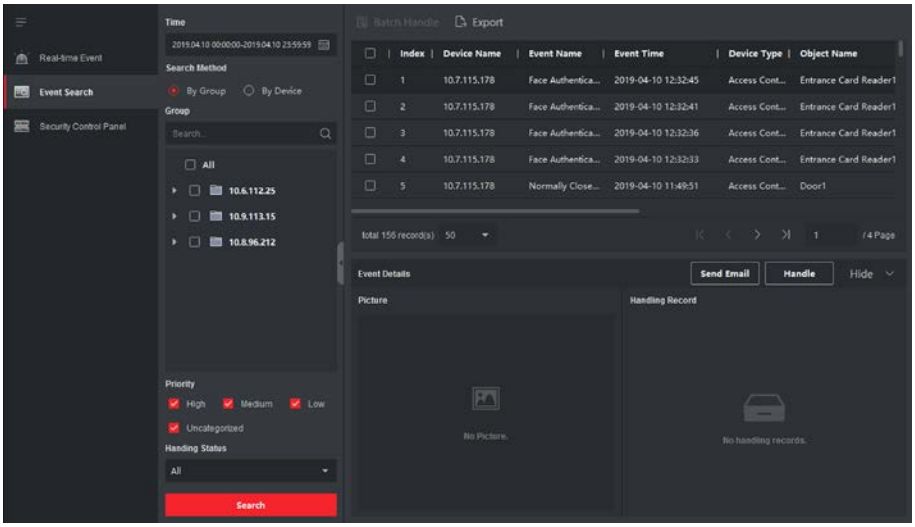

Figure 5-4 Buscar Historial de Eventos

2. Configura los eventos del filtro para seleccionar solo los eventos requeridos.

Hora

La hora del software cuando empieza el evento.

Buscar por

Grupo: Buscar los eventos ocurridos en los recursos de grupo seleccionado.
Dispositivo: Buscar los eventos ocurridos en el dispositivo seleccionado.

Tipo de dispositivo

El tipo de dispositivo en el que ocurre el evento.
Todos los tipos de dispositivos, pueden ser configurados con los siguientes filtros: Grupo, Prioridad y estado.

Videoporteros

Para los eventos de video porteros, se necesita seleccionar el ámbito de búsqueda.

- Todos los registros.
- Se pueden filtrar los eventos desde todos los eventos del video portero, y se necesita configurar las siguientes condiciones de filtro: dispositivo, prioridad, estado.
- Solo desbloqueado.
- Se pueden filtrar los eventos desde todos los eventos desbloqueados de los videos porteros y se necesita configurar los siguientes condiciones de filtro: dispositivo, tipo de desbloqueo.

Control de accesos

Para los eventos de control de accesos, se pueden configurar los siguientes filtros de condiciones: dispositivo, prioridad, estado, tipo de evento, tipo de lector de tarjeta, Nombre de usuario, número de tarjeta, organización.

Nota

*Hacer click en **Mostrar Más** para configurar el tipo de evento, tipo de lector de tarjeta, nombre de usuario, número de tarjeta, organización.*

Grupo

El Grupo del dispositivo donde ocurrió el evento. Se debe configurar el grupo como condición solo cuando se seleccione el tipo de dispositivo como **Todo**.

Dispositivo

El dispositivo en el que ocurrió el evento.

Prioridad

La prioridad incluyendo bajo, medio, alto y sin categorizar los que indican un grado urgente en el evento.

Estado

El estado de manejo del evento.

3. Hacer click en **Buscar** para buscar los eventos acorde a las condiciones de configuración.
4. Opcional: Hacer click con el botón en el encabezado de la tabla de la lista de eventos para personalizar los elementos relacionados con eventos que se mostrarán en la lista de eventos.

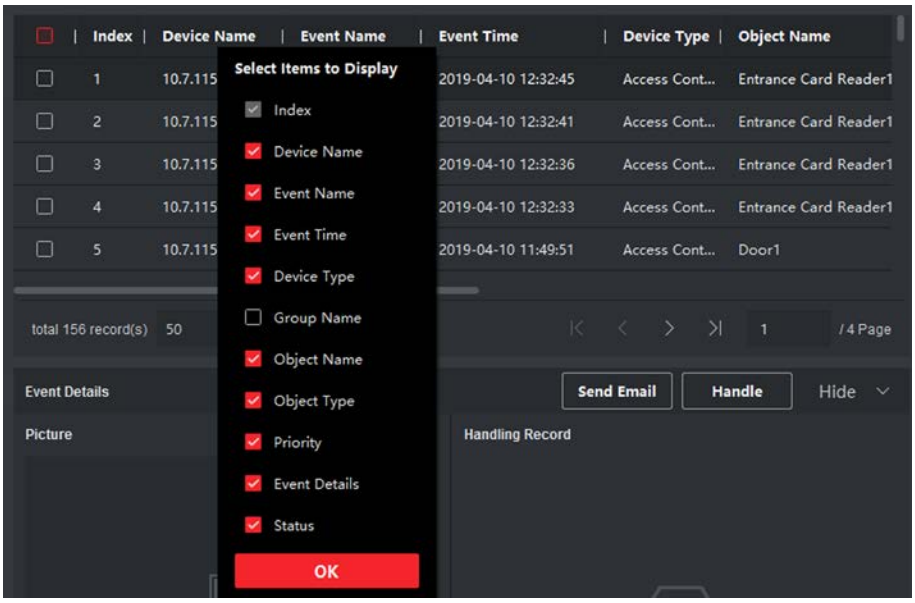

Figure 5-5 Personalizar columnas de los eventos para ser visualizado

5. Opcional: Manejo de eventos.
   - Manejo de un Solo Evento: Seleccionar un evento que necesita ser procesado, y después hacer click en **Procesar** en la página de detalles de información de evento, e introducir los datos de búsqueda.
   - Manejar Eventos en un Lote: Seleccionar los eventos que necesitan ser procesados, y después hacer click en **Manejo en Lote**, e introducir the los datos de búsqueda.

Nota

*Después de un evento modificado, el botón de **Manejo** se convertirá en **Añadir Observación**, hacer click en **Añadir Observación** para añadir más información sobre el evento manejado.*

6. Opcional: Seleccionar un evento y después hacer click en **Enviar Email**, y los detalles de la información del evento será enviado por email.

Nota

*Se deben configurar los parámetros del email antes, ver **Configurar los Parámetros de Email** para más detalles.*

7. Opcional: Hacer click en **Exportar** para exportar el registro de eventos o las imágenes de eventos al ordenador local en formato CSV. Se puede configurar la ruta para guardarlo manualmente.
8. Mover el cursor en la imagen y después hacer click en el icono de descarga en la esquina superior derecha de la imagen para descargarla en el ordenador local. Se puede configurar la ruta para guardarlo manualmente.

Capítulo 6 Gestión de Usuarios

Se puede agregar información de la persona al sistema para otras operaciones como control de accesos, videoporteros, tiempo y asistencia, etc. Se puede gestionar a las personas agregadas añadiendolas tarjetas en un lote, importando y exportando información, etc.

6.1 Añadir organización

Puede añadir una organización e importar la información de los usuarios para la correcta gestión de personas de la compañía. También se pueden añadir organizaciones subordinadas o departamentos.

Pasos

1. Entrar en el módulo de **Usuario**.
2. Seleccionar un departamento superior en la columna de la izquierda y hacer click en **Añadir** en la esquina para superior izquierda para Añadir una organización.
3. Crear un nombre para la organización a añadir.

Nota

Se pueden agregar hasta 10 niveles de organizaciones.

4. Opcional: Realiza las siguientes operaciones.

Editar organización	Selecciona con el ratón sobre la organización o departamento añadido y hacer click en para editar su nombre.
Borrar organización	Selecciona con el ratón sobre la organización o departamento añadido y hacer click en para borrarla.

Nota

- *Los niveles menores de las organizaciones serán eliminados si se borra la organización o departamento Padre.*
- *Debe estar Seguro de que ninguna persona pertenece a un departamento que se quiere eliminar, este no podrá ser borrado*

Mostrar Personas en Suborganizaciones	Seleccionar **Mostrar Personas en una Suborganización** y Seleccione una organización para mostrar las personas de las suborganizaciones.

6.2 Añadir una sola persona

Se pueden añadir los usuarios al software uno a uno. La información del usuario contiene información básica, información detallada, perfiles, información del control de accesos,

credenciales, información personalizada, etc.

6.2.1 Configurar Información Básica.

Se puede añadir la información del usuario uno a uno y configurar la informacion básica como el Nombre, el género, número de teléfono, etc.

Pasos

1. Entre en el modulo de **Personas**.
2. Seleccionar una organización de la lista a la que pertenezca la persona a añadir.
3. Hacer click en **Añadir** para abrir la pestaña de añadido de personas.
   El ID de cada usuario se generará de forma automática.
4. Introducir la información básica de la persona, incluyendo el Nombre, género, teléfono, email, dirección, etc.
5. Opcional: Configure el periodo efectivo que estará la persona en la compañía. Una vez expirado, los credenciales y las configuraciones de control de accesos de ese usuario serán inválidos y la persona no tendrá autorización para acceder a las puertas ni los dispositivos.

   Ejemplo

   Si la persona es un visitante, su periodo efectivo debería ser corto y temporal.
6. Confirmar para Añadir al usuario.
   - Hacer click en **Añadir** para agregar a la persona y cerrar la Ventana de agregado de personas.
   - Hacer click en **Añadir y Nuevo** para agregar al usuario y continuar agregando otros usuarios.

6.2.2 Agregar la Tarjeta a un Usuario

Al agregar una persona, puede emitir una tarjeta con un número único para la persona como credencial. Una vez emitido, la persona puede acceder a las puertas a las que está autorizado para acceder al deslizar la tarjeta en el lector de tarjetas.

Pasos

Nota

Se pueden emitir hasta 5 tarjetas para una misma persona.

1. Entre en el modulo de **Personas**.
2. Seleccionar una organización de la lista para Añadir la persona y hacer click en **Añadir**.

Nota

*Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. En **Credencial** → Panel de **Tarjetas**, Hacer click en **+**.
4. Introducir el número de tarjeta.
   - Introducir el número de tarjeta manualmente.

– Coloque la tarjeta sobre el dispositivo de enrolamiento de tarjetas específico o sobre un lector de tarjetas. Hacer click en **Leer** para obtener el número de tarjeta. Este se mostrará en el campo Número de tarjeta automáticamente.

Nota

*Se necesita hacer click en **Ajustes** para configurar el modo de lectura de tarjeta y parámetros relacionados. Para más detalles, ver **Configurar Parámetros de lectura de tarjeta**.*

5. Seleccionar el Tipo de tarjeta acorde a las necesidades actuales.

Tarjeta Normal

La tarjeta es utilizada para abrir puertas de forma habitual.

Tarjeta Coacción

Cuando la persona se encuentra en una situación de coacción, puede pasar esta tarjeta por la Puerta, esta se abrirá y el software recibirá un evento de coacción para notificar al personal de seguridad.

Tarjeta de Patrol

Esta tarjeta es utilizada por los empleados al realizar una ronda para controlar que estos empleados pasan por los puntos de control de inspección. Al pasar la tarjeta por los lectores específicos, la persona está marcando registros de ronda en un determinado tiempo.

Tarjeta de Disolución

Al pasar la tarjeta por los lectores, esta puede detener el sonido de alarma de ese lector.

6. Hacer click en **Añadir**.
   La tarjetas será agregada a esa persona.
7. Confirmar para Añadir la persona.
   – Hacer click en **Añadir** para Añadir la persona y cerrar la Ventana de agregar personas.
   – Hacer click en **Añadir y Nuevo** para agregar el usuario y a continuación agregar otro.

6.2.3 Cargar una Foto del Usuario desde el PC

Cuando se agrega a una persona, se puede cargar una foto almacenada en el PC para el perfil de usuario de esa persona.

Pasos

1. Entrar en el módulos de Personas.
2. Seleccionar una organización en la lista de la parte izquierda para añadir la persona y hacer click en **Añadir**.

Nota

*Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. Hacer click en **Añadir Cara** en el panel de información básica.

4. Seleccionar **Cargar**.
5. Seleccionar una imagen desde el PC en el que está instalado el software.

> ***Nota***
>
> *La imagen debe ser en formato JPG o JPEG y menor de 200 KB.*

6. Opcional: Habilitar **Verificar por dispositivo** para chequear si el dispositivo de reconocimiento facial administrado en el software puede reconocer la cara desde la foto.
7. Confirmar para Añadir la persona.
   – Hacer click en **Añadir** para agregar al usuario y cerrar la ventana.
   – Hacer click en **Añadir y Nuevo** para agregar al usuario y continuar añadiendo otros.

6.2.4 Hacer una Foto desde el Software

Cuando se está añadiendo un usuario, se puede hacer una foto del usuario desde la webcam del ordenador en el que se está ejecutando el software y configurarla como una foto del perfil del usuario.

Antes de empezar

chequear si el dispositivo de reconocimiento facial administrado en el software puede reconocer la cara desde la foto.

Pasos

1. Entrar en el modulo de Personas.
2. Seleccionar una organización en el listado de la izquierda y hacer click en **Añadir** para agregar el usuario.

> ***Nota***
>
> *Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. Hacer click en **Añadir Cara** en el panel de información.
4. Seleccionar **Hacer Foto**.
5. Conectar el escáner fácial al PC en el que se ejecuta el software.
6. Opcional: Habilitar **Verificar por Dispositivo** para comprobar si el dispositivo de reconocimiento facial gestionado por el software es capaz de reconocer la cara en la foto.
7. Hacer una foto.
   1) Mire a la webcam del PC y asegura que el rostro se encuentra en el medio de la ventana.
   2) Hacer click en para realizar la foto.
   3) Opcional: Hacer click en para realizarlo otra vez.
   4) Hacer click en **OK** en Guardar la imagen obtenida.
8. Confirmar para Añadir el usuario.
   – Hacer click en **Añadir** para agregar al usuario y cerrar la Ventana.
   – Hacer click en **Añadir y Nuevo** para agregar al usuario y continuar añadiendo usuarios.

6.2.5 Capturar Rostros desde el Dispositivo de Control de Accesos

Al agregar a una persona se puede capturar su rostro a través del dispositivo de control de accesos añadido al software que soporta la función del reconocimiento facial.

Pasos

1. Entrar en el modulo de **Personas**.
2. Seleccionar una organización en el listado de la izquierda y hacer click en **Añadir** para agregar el usuario.

> ***Nota***
>
> *Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. Hacer click en **Añadir Cara** en el panel de información.
4. Seleccionar **Captura remota**.
5. Seleccionar un Dispositivo de Control de Accesos el cual soporte la función de reconocimiento facial desde la lista desplegable.
6. Capturar cara.
   1) Mire a la cámara del dispositivo de control de accesos y asegura que el rostro se encuentra en el medio de la ventana.
   2) Hacer click en para hacer la foto.
   3) Hacer click en **OK** para Guardar la foto realizada.
7. Confirmar para añadir al usuario.
   – Hacer click en **Añadir** para agregar al usuario y cerrar la ventana.
   – Hacer click en **Añadir y Nuevo** para agregar al usuario y continuar añadiendo otros.

6.2.6 Capturar huellas dactilares desde el software

Coger localmente huellas dactilares significa que pueden ser recopiladas a través de una grabadora de huellas dactilares, ejecutada por el software, conectada directamente al PC. Las huellas dactilares registradas se pueden utilizar como credenciales de las personas para acceder a las puertas autorizadas.

Antes de empezar

Conectar el grabador de huellas dactilares al ordenador que contiene el software.

Pasos

1. Entrar en el módulo **Usuario.**
2. Seleccionar una organización en la lista de organización para añadir al usuario y hacer click en **Añadir**.

Nota

*Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. En **Credencial** → panel de **Huella dactilar,** hacer click en **+**.
4. En a Ventana emergente, seleccionar el modo de recoger huellas como **Local**.
5. Seleccionar el modelo del grabador de huellas conectado.

Nota

*El grabador de huellas es DS-K1F800-F, se puede hacer click en **Ajustes** para seleccionar el Puerto COM al que está conectado el grabador de huellas.*

6. Capturar la huella dactilar.
   1) Hacer click en **Empezar**.
   2) Colocar y levantar la huella en el grabador de huellas para recoger la muestra.
   3) Hacer click en **Añadir** para guardar la huella capturada.
7. Confirmar para Añadir la persona.
   – Hacer click en **Añadir** para añadir la persona y cerrar la Ventana de añadir persona.
   – Hacer click en **Añadir** para Añadir la persona y continuar para añadir a otras personas.

6.2.7 Capturar huela dactilar desde el dispositivo de Control de Accesos

Cuando se añade una persona se puede coger la información de su huella mediante el módulo de Huella Dactilar en el Dispositivo de Control de Accesos. La huellas grabadas pueden ser usadas como credenciales de las personas para acceder a las puertas autorizadas.

Antes de empezar

Asegurarse de que las huellas dactilares son compatibles con el Dispositivo de Control de Accesos.

Pasos

1. Entrar en el módulo **Persona**.
2. Seleccionar una organización en la lista de organización para añadir la persona y hacer click en **Añadir**.

Nota

*Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. En **Credencial** →panel de **Huella Dactilar**, hacer click en **+**.
4. En la Ventana emergente, seleccionar el modo de recogida de muestras como **Remoto**.
5. Seleccionar un Dispositivo de Control de Accesos que Soporte la función de reconocimiento de Huella Dactilar desde la lista desplegable.
6. Tomar la huella.

1) Hacer click en **Empezar**.
2) Poner y levantar la Huella Dactilar en el escáner del dispositivo de Control de Accesos para coger la Huella Dactilar.
3) Hacer click en **Añadir** para Guardar la Huella Dactilar guardada.

7. Confirmar para Añadir la persona.
   – Hacer click en **Añadir** para Añadir la persona y cerrar la Ventana.
   – Hacer click en **Añadir y Nuevo** para Añadir la persona y continuar para añadir a otras personas.

6.2.8 Configurar información del control de acceso

Cuando se añade una persona se puede configurar las propiedades de su control de accesos, como establacer a la personas como visitante, como persona de la lista negra o como superusuario que tiene autorización maestra.

Pasos

1. Entrar en el módulo de **Persona**.
2. Seleccionar una organización en la lista de organización para añadir a la persona y hacer click en **Añadir**.

Nota

*Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información básica**.*

3. En el panel de **Control de accesos**, configurar las propiedades de control de accesos de la persona.

Código Pin

El Código PIN puede ser usado después de acceder con la tarjeta o Huella Dactilar. No puede ser usado independientemente. Debe contener de 4 a 8 dígitos.

Super Usuario

Si la persona es configurada como Super Usuario, tendrá acceso a todas las puertas/plantas y estará exento de las restricciones de puerta cerrada. Todas anti-passback rules, y paso libre.

Tiempo extendido de puerta abierta

Cuando la persona que accede a la puerta tarde más tiempo en acceder que el tiempo configurado. Utilizar esta función para las personas con movilidad reducida.
Para más detalles sobre la configuración de la duración de la puerta abierta, ver ***Configurar Parámetros para puerta/ ascensor***.

Añadir a la lista negra

Añadir a la persona a la lista negra cuando se trate de acceder a las puertas/plantas. En ese caso se activará un evento y se enviará al software para notificarlo al personal de seguridad.

Marcar como visitante

Si la persona es un visitante, configurar el número máximo de autenticaciones incluyendo el

acceso por tarjeta y huella dactilar para limitar el acceso al visitante.

Nota

El número de veces máximo de autenticaciones debe estar entre 1 y 100.

Operador del Dispositivo

Para una persona con el rol de operador de dispositivo está autorizado a operar en el Dispositivo de Control de Accesos.

Nota

El Super Usuario, el tiempo extendido de puerta abierta, añadir a la lista negra, y marcar como marcar como visitante son funciones que no se pueden habilitar concurrentemente. Por Ejemplo, si un usuario se configura como Super Usuario, no se puede habilitar el tiempo extendido de puerta abierta. Añadirlo a la lista negra y configurarla como visitante.

4. Confirmar para añadir a la persona.
   – Hacer click en **Añadir** para añadir a la persona y cerrar la Ventana de Añadir Persona.
   – Hacer click en **Añadir y Nuevo** para añadir a otra persona y continuar para añadir más personas.

6.2.9 Personalizar Información del usuario

Se pueden personalizar las propiedades del usuario las cuales no están predefinidas en el software actual para las necesidades especiales como lugar de Nacimiento. Después de la personalización cuando se añade una persona se puede acceder a la información personalizada para completarla.

Pasos

1. Entrar en el módulo **Persona.**
2. configurar los campos de la información personalizada.
   1) Hacer click en **Propiedad Personalizada**.
   2) Hacer click en **Añadir** para añadir una nueva propiedad.
   3) Entrar en la propiedad Nombre.
   4) Hacer click en **OK**.
3. Establacer la información personalizada cuando se añada una persona.
   1) Seleccionar una organización en la lista de organización para añadir al usuario y hacer click en **Añadir**.

   Nota

   *Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

   2) En el panel de **Información Personalizada**, introducir la información.
   3) Hacer click en **Añadir** para añadir a la persona y cerrar la ventana de Añadir Persona o hacer click en **Añadir y Nuevo** para añadir a la persona y continuar para añadir otras personas.

6.2.10 Configurar la Información del Residente

Si la persona es residente, para el uso de video portero, se necesita configurar el número de habitación para asignar el monitor interior. Después de enlazar se puede llamar a esta persona mediante Monitor Interior y realizar una video llamada.

Pasos

1. Entrar en el módulo **Persona**.
2. Seleccionar una organización en la lista de organización para añadir la persona y hacer click en **Añadir**.

Nota

*Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. En el panel de **Información de Residencia**, seleccionar el Monitor Interior para asignarselo a un usuario.

Nota

*Si se selecciona **Monitor Interior Analógico**, aparecerá en el campo **Estación de Puerta** y se solicitará que seleccione la Estación de Puerta para comunicarse con el monitor interior analógico.*

4. Introducir la planta y número de piso de la persona.
5. Confirmar para añadir a la persona.
   - Hacer click en **Añadir** para añadir a la persona y cerrar la Ventana de Añadir Persona.
   - Hacer click en **Añadir y Nuevo** para Añadir a la persona y continuar para añadir a otras personas.

6.2.11 Configurar información adicional

Cuando se añade una persona se puede configurar su información adiccional, como el tipo de identidad de la persona, número de identidad, país, etc acorde a las necesidades actuales.

Pasos

1. Entrar en el módulo **Persona**.
2. Seleccionar una organización en la lista de organización para añadir a la persona y hacer click en **Añadir**.

Nota

*Introducir primero la información básica del usuario. Para obtener más detalles sobre dicha configuración, consultar **Configurar Información Básica**.*

3. En el panel de **Información Adiccional**, entrar en la información adicional de la persona, incluyendo tipo de identidad de la persona, número de identidad, título professional etc. Acorde a las necesidades actuales.

4. Confirmar para añadir a la persona.
   – Hacer click en **Añadir** para añadir a la persona y cerrar la Ventana de Añadir Persona.
   – Hacer click en **Añadir y Nuevo** para añadir y continuar para añadir a otras personas.

6.3 Importar y Exportar la Información personal del usuario

Se puede importar la información y las imágenes de varias personas al software en un lote. Mientras tanto, también se puede exportar la información de la persona y las imágenes y guardarlas en el ordenador.

6.3.1 Importar la Información Personal

Se puede introducir la información de múltiples personas en una plantilla predefinida (un archivo CSV) para importar la información en un lote.

Pasos

1. Entrar en el módulo **Persona**.
2. Seleccionar una organización añadida en la lista o hacer click en **Añadir** en la esquina superior izquierda para añadir una organización y después seleccionarla.
3. Hacer click en **Importar** para abrir el panel importado.
4. Seleccionar **Información Personal** como el modo de importación.
5. Hacer click en **Descargar plantilla para importar usuario** para descargar la plantilla.
6. Introducir la Información Personal en la plantilla descargada.

Nota

- *Si el usuario tiene múltiples tarjetas separar el número de la tarjeta con un punto y coma.*
- *Se requieren elementos con asteriscos.*
- *Por defecto la fecha de contratación es la fecha actual.*

7. Hacer click en ··· para seleccionar el archivo CSV con la información personal.
8. Hacer click en **Importar** para comenzar la importación.

Nota

- *Si el número de una persona todavía existe en la base de datos, borrar la información existente antes de importarla.*
- *No se puede importar información a más de 10.000 personas.*

6.3.2 Importar las Fotografías del Usuario

Después de importar las imágenes faciales de las personas añadidas al software, las personas que aparecen pueden ser identificadas mediante un terminal de reconocimiento facial. Se puede

importar imágenes personales una a una o importar varias imágenes según las necesidades.

Antes de empezar

Estar seguro de tener importada la información personal al software.

Pasos

1. Entrar en el módulo de Usuario.
2. Seleccionar una organización añadida en la lista o hacer click en **Añadir** una organización y después seleccionarlo.
3. Hacer click en **Importar** para abrir el panel de Importar y comprobar la **Cara.**
4. Opcional: Habilitar **Verificar por Dispositivo** para comprobar si el dispositivo de reconocimiento facial gestionado en el software puede reconocer la cara en la foto.
5. Hacer click en ··· para Seleccionar un archivo de una imagen facial.

Nota

- *La carpeta de imágenes faciales debe estar en formato ZIP.*
- *Cada archivo de imagen debe estar en formato JPG y no debe supercar los 200 KB.*
- *Cada archivo debe ser nombrado como "ID Personal_Nombre". La identificación de la persona debe ser la misma que la información personal requerida.*

6. Hacer click en **Importar** para comenzar la importación.
   Se mostrará el progreso de la importación y el resultado.

6.3.3 Exportar la información del Usuario

Se puede exportar la información de las personas añadidas al ordenador local como un archivo CSV.

Antes de empezar

Estar seguros de tener añadidas personas a la organización.

Pasos

1. Entrar en el módulo Usuario.
2. Opcional: Seleccionar una organización en la lista.

Nota

La información de todas las personas será exportada si no se selecciona ninguna organización.

3. Hacer click en **Exportar** para abrir el panel exportado y comprobar el contenido de la **Información Personal** para exportar.
4. Marcar los elementos que se desean exportar.
5. Hacer click en **Exportar** para guardar el archivo CSV en su PC.

6.3.4 Exportar imágenes de Usuario

Puede exportar los archivos con la imagen facial de los usuarios añadidos y guardarlas en su PC.

Antes de empezar

Asegurarse de tener añadidos usuarios y sus caras a una organización.

Pasos

1. Entrar en el módulo **Persona**.
2. Opcional: Seleccionar una organización en la lista.

> ***Nota***
>
> *Todas las imágenes faciales de los usuarios serán exportadas sino se selecciona ninguna organización.*

3. Hacer click en **Exportar** para abrir el panel de exportación y comprobar que los **rostros** están como contenido a exportar.
4. Hacer click en **Exportar** para comenzar la exportación.

> ***Nota***
>
> - *El archivo exportado está en formato ZIP.*
> - *La imagen facial exportada se nombra como "Person ID_Nombre_0" ("0"es para una imagen en primer plano).*

6.4 Obtener información del Usuario desde el Dispositivo del Control de Accesos.

Si el dispositivo de control de accesos añadido ha sido configurado con información personal (incluyendo detalles personales, huellas dactilares y la información de tarjetas emitida), Se puede obtener información desde el dispositivo e importarlas al software para facilitar operaciones.

Pasos

> ***Nota***
>
> - *Si el Nombre de la persona almacenada en el dispositivo está vacío, el nombre de la persona será rellenado con el Nº de la tarjeta despues de ser importado al software.*
> - *El género de los usuarios será **Masculino** por defecto.*
> - *Si el Nº de le tarjeta o ID de usuario almacenado en el dispositivo ya existe en la base de datos del software, el usuario con este número de tarjeta o ID no será importada al software.*

1. Entre en el módulo de **Persona**
2. Seleccionar una organización para importar los usuarios.
3. Hacer click en **Obtener del dispositivo**.
4. Seleccionar el Dispositivo de Control de Accesos desde el desplegable.

5. Hacer click en **Obtener** para comenzar a importar la información Personal al software.
   La información personal, incluyendo los detalles de los usuarios, huellas dactilares (si han sido configuradas) y los vínculos con las tarjetas (si han sido configuradas), serán importadas a la organización seleccionada.

6.5 Mover usuarios a otra organización

Si es necesario se pueden mover las personas añadidas a otra organización.

Antes de empezar

- Estar Seguro de tener añadidas al menos dos organizaciones.
- Estar Seguro de tener importada la información del Usuario.

Pasos

1. Entre en el módulo de **Persona**.
2. Seleccionar una organización en el panel de la izquierda.
   Las personas de la organización serán mostradas en el panel de la derecha.
3. Seleccionar el usuario a mover.
4. Hacer click en **Cambiar Organización**.
5. Seleccionar la organización a la que mover el usuario.
6. Hacer click en **OK**.

6.6 Registrar tarjetas de usuarios en Lote

El software proporciona una manera sencilla de registrar tarjetas de múltiples personas en lote.

Pasos

1. Entre en el módulo de Persona.
2. Hacer click en **Registrar Tarjetas en Lote.**
   Todas las personas añadidas con Número de tarjeta serán mostradas.
3. Configurar la configuración de registro de tarjetas. Para más detalles, ver ***Configuración de Parámetros de la tarjeta***.
4. Hacer click en **Inicializar** para encender la estación de enrrolamiento o el lector de tarjeta para que esté listo el registro de tarjetas.
5. Hacer click en la columna número de tarjeta e introducir el número ID de la tarjeta.
   – Colocar la tarjeta en la estación de enrrolamiento de tarjetas.
   – Pasar la tarjeta por encima del lector.
   – Introducir el número de tarjeta manualmente y presionar la tecla **Enter** en el teclado.
   El número de tarjeta será leído automáticamente y la tarjeta será asignada al usuario en la lista.
6. Repetir el paso superior para registrar las tarjetas al resto de personas de la lista en secuencia.

6.7 Informar de Tarjetas Pérdidas

Si el usuario pierde la tarjeta, puede Informar la pérdida de la tarjeta. Entonces la autorización de acceso quedará inactiva.

Pasos

1. Entre en el módulo de **Persona**.
2. Seleccionar el usuario que se quiere Informar la pérdida de la tarjeta y hacer click en **Editar** para abrir la ventaja de edición de Usuario.
3. En las **Credenciales** → Panel de **Tarjeta**, hacer click en  en la tarjeta añadida para configurarla como Perdida.
   Después de Informar la tarjeta Perdida, la autorización de acceso de esta tarjeta quedará inválida e inactiva. Otra persona que adquiera esta tarjeta por error no podrá acceder a las puertas.
4. Opcional: Si la tarjeta Perdida es encontrada, Se puede hacer click en  para cancelar la pérdida.
   Después de la cancelación de la tarjeta, la autorización de acceso de la persona será válido y activo.
5. Si la tarjeta Perdida es añadida en un grupo de acceso y este se aplica al dispositivo, después de Informar la pérdida o cancelación de la tarjeta, se abrirá una nueva Ventana emergente para notificar que se apliquen los cambios en el dispositivo. Después de aplicarlos, estos son cargados y aplicados en el Dispositivo.

6.8 Configurar Parámetros de registro de tarjeta

El software tiene dos modos de realizar la lectura de la tarjeta: A través de la estación de enrrolamiento de tarjeta o mediante el lector de tarjeta del dispositivo. Si la estación está disponible, conectarla al PC que ejecuta el software mediante USB o Puerto COM. Colocar la tarjeta sobre el lector para leer el número de identificación. Si no se dispone, también se puede pasar la tarjeta sobre el lector del dispositivo de Control de accesos para obtener el ID. Como resultado, después de registrar una tarjeta a una persona, se necesitan configurar los parámetros de registro de esta tarjeta incluyendo el modo de registro y los parámetros relacionados.
Cuando se añade una tarjeta a una persona, hacer click en **Ajustes** para abrir la Ventana de Configuración de registro de tarjeta.

Modo Local. Registrar tarjeta con la estación de enrolamiento

Conectar una estación de enrolamiento de tarjetas en el PC que se ejecuta el software. Colocar la tarjeta sobre el lector y obtener el ID de la tarjeta.

Estación de enrolamiento de tarjeta

Seleccionar el módulo de estación conectada

Tipo de tarjeta

Seleccionar el tipo de tarjeta como RFID EM 125KHz o Mifare 13.56MHz de acuerdo con el tipo de tarjeta a leer.

Zumbido

Emitirá un zumbido cuando la tarjeta ha sido leído de forma satisfactoria.

Tipo de Nº de tarjeta

Seleccionar el tipo de tarjeta acorde a las necesidades actuales.

.

Modo remote: Registrar la tarjeta mediante el lector

Seleccionar un Dispositivo de Control de añadido en el software y pasar la tarjeta en el lector para leer el número de tarjeta.

Capítulo 7 Control de acceso

El módulo de Control de accesos es aplicable a los dispositivos de control de accesos y video porteros. Proporciona múltiples funcionalidades, incluido el acceso a la configuración del Grupo, Video portero y otras funciones avanzadas.

Nota

*Para los usuarios con permisos del módulo de control de accesos, el usuario pueden entrar en el modulo y configurar los diferentes parámetros de accesos. Para la configuración de los permisos de usuarios, ver **Añadir Usuario**.*

7.1 Configurar el Calendario

Se pueden configurar plantillas para las vacaciones y la planificación semanal. Después de la configuración se puede acceder a los Grupos para que tenga efecto en el tiempo de duración de las plantillas.

Nota

*Para acceder a las configuraciones de Grupo, ver **Configurar Grupos de acceso para asignar autorizaciones de acceso a los usuarios**.*

7.1.1 Añadir vacaciones

Se pueden crear y configurar los días de vacaciones incluyendo la fecha de inicio y fin, y configuración de festivos.

Pasos

Nota

Se pueden añadir hasta 64 vacaciones en el sistema.

1. Hacer click en **Control de accesos** → **Calendario** → **Vacaciones** para entrar en la página de vacaciones.
2. Hacer click en **Añadir** en el panel izquierdo.
3. Crear un Nombre para las vacaciones.
4. Opcional: Introducir las descripciones o algunas notificaciones sobre las vacaciones en la caja de observaciones.
5. Añadir un periodo de vacaciones en la lista de vacaciones y configurar la duración de las vacaciones.

Nota

Se pueden agregar hasta 16 períodos de vacaciones a un día festivo.

1) Hacer click en **Añadir** en el campo Lista de Vacaciones.
2) Arrastrar el cursor para dibujar la duración del tiempo, lo que significa que en ese período de tiempo, se configura el Grupo de acceso de configuración.

Nota

Se pueden establacer hasta 8 duraciones de tiempo en un período vacacional.

3) Opcional: Realizar las siguientes operaciones para editar las duraciones de tiempo.
   - Mover el cursor hacia la duracción del tiempo y arrastrar la duración en la barra de la línea de tiempo a la posición deseada cuando el cursor gire .
   - Hacer click en la duración de tiempo y directamente editar la hora de inicio y finalización en el cuadro de diálogo que aparece.
   - Mover el cursor al inicio o al final de la duración del tiempo y arrastrar para alargar o acortar la duración del tiempo cuando el cursor se convierta en .
4) Opcional: Seleccionar los tiempos que deben eliminarse y, a continuación, haga clic en la columna de operación para eliminar los tiempos seleccionados.
5) Opcional: Hacer click en en la columna de Operación para borrar los tiempos de duración en la barra de tiempo.
6) Opcional: Hacer click en en la columna de Operación para borrar el período de tiempo añadido desde la lista de vacaciones.

6. Hacer click en **Guardar**.

7.1.2 Añadir plantilla

La plantilla incluye el horario de la semana y las vacaciones. Se puede establacer el horario de la semana y asignar la duración de la autorización de acceso para diferentes usuarios o grupos. También se pueden seleccionar las vacaciones agregadas para la plantilla.

Pasos

Nota

Se pueden añadir hasta 255 plantillas en el sistema del software.

1. Hacer click en **Control de accesos** → **Calendario** → **Plantilla** para entrar en la página de Plantilla.

Nota

Hay dos plantillas predeterminadas: Autorizado durante todo el día y Denegado durante todo el día, y no se pueden editar ni eliminar.

Autorizado todo el día

La autorización de acceso es válida en cada día de la semana y no tiene vacaciones.

Denegado durante todo el día

La autorización de acceso no es válida en todos los días de la semana y no tiene días festivos.

2. Hacer click en **Añadir** en el panel izquierdo para crear una nueva plantilla.
3. Crear un nombre para la plantilla.
4. Introducir las descripciones o alguna notificación de esta plantilla en el cuadro de observación.
5. Editar el calendario mensual para aplicarlo en su plantilla.
   1) Hacer click en la pestaña **Calendario Semanal** en el panel inferior.
   2) Seleccionar un día de la semana y señalar en la barra de tiempo la duración.

   Nota

   Se pueden configurar hasta 8 tiempos para cada día en el calendario semanal.

   3) Opcional: Realiza las siguientes operaciones para editar la duración de tiempo.
      - Mover el cursor a la duración del tiempo y arrastre la duración en la barra de la línea de tiempo a la posición deseada cuando el cursor gire .
      - Hacer click en la duración de tiempo y editar directamente la hora de inicio y finalización en la Ventana que aparece.
      - Mover el cursor al inicio o al final de la duración del tiempo y arrastrar para alargar o acortar la duración del tiempo cuando el cursor se convierte en .
   4) Repetir los dos pasos de arriba para incluir más información en las duraciones de los otros días de la semana.
6. Añadir unas vacaciones para aplicarlo en la plantilla.

   Nota

   Hasta 4 vacaciones pueden ser añadidas en una plantilla.

   1) Hacer click en la pestaña **Vacaciones**.
   2) Seleccionar vacaciones en la lista de la izquierda y se agregará a la lista seleccionada en el panel de la derecha.
   3) Opcional: Hacer click en **Añadir** para Añadir nuevas vacaciones.

   Nota

   *Para más detalles sobre como añadir vacaciones, referir a **Añadir Vacaciones**.*

   4) Opcional: Seleccionar unas vacaciones que ya han sido seleccionadas en a lista de la derecho y hacer click en para eliminar el seleccionado o hacer click en **Borrar** para Borrar todas las vacaciones seleccionadas en la lista de la derecho.
7. Hacer click en **Guardar** para Guardar las configuraciones y añadir la plantilla.

7.2 Configurar grupos de acceso para asignar autorización a usuarios

Después de añadir el usuario y las credenciales de configuración del usuario, se puede crear el acceso Grupos para definir a que puerta puede acceder el usuario/s y aplicar el acceso del grupo al dispositivo de control de accesos para que tenga efecto.

Pasos

- Para un mismo usuario se pueden añadir hasta 4 grupos de Control de accesos de un dispositivo.
- Se pueden añadir hasta 128 Grupos de accesos en total.
- Cuando las configuraciones del grupo de accesos han cambiado, se necesitan aplicar de nuevo los accesos a los dispositivos. Los cambios de acceso al grupo incluyen cambios de plantilla, acceso a la configuración del grupo del usuario y detalles relacionados con el usuario (como el número de la tarjeta, la huella digital, la imagen de la cara, el vínculo entre el número de la tarjeta y la huella digital, el vínculo entre el número de la tarjeta y la huella digital, la contraseña de la tarjeta, etc).

1. Hacer click en **Control de accesos** → **Acceso Grupo** para entrar al interfaz de acceso al grupo.
2. Hacer click en **Añadir** para abrir la Ventana de Añadir.
3. En el campo de texto de **Nombre**, crear un Nombre para el grupo de acceso deseado.
4. Seleccionar una plantilla para el grupo de acceso.

Nota

*Se debe configurar la plantilla antes de las configuraciones del grupo de acceso. Ver **Configurar Calendario y Plantilla** para más detalles.*

5. En la lista izquierda del campo Seleccionar usuario, Seleccionar la persona (s) y se agregarán a la lista Seleccionar.
6. En la lista izquierda del campo de la Puerta Selecionada, seleccione Puerta (s) o estación (es) de Puerta para que las personas que seleccionan acceden, y la Puerta (s) o estación (es) de puerta seleccionada se agregará a la lista seleccionada.
7. Hacer click en **OK**.
8. Después de añadir el grupo de acceso, se necesita para aplicarlos al dispositivo de control de accesos para tener efecto.
   1) Seleccionar el grupo de acceso para aplicar los dispositivos de control de accesos. Para seleccionar los grupos de acceso, pulsar la tecla **Ctrl** o **Turno** y seleccionar el grupo de control de accesos.
   2) Hacer click en **Aplicar Todo en Dispositivos** para empezar aplicar todos los grupos de acceso seleccionado al dispositivo de control de accesos o la Puerta de estación.

Atención

- *Hacer click en **Aplicar Todo a los Dispositivos**, desde este operación se borrarán todos los grupos de accesos de los dispositivos seleccionados y después de aplica los nuevos grupos de accesos, lo que puede suponer un riesgo para los dispositivos.*

- *Se puede hacer click en **Aplicar cambios a los dispositivos** para aplicar solo la parte modificada de los grupos de acceso seleccionados al dispositivo o dispositivos.*

3) Ver todas las opciones aplicadas en la columna de estado o hacer click en **Aplicar Estado** para ver todo lo aplicado en el grupo de acceso.

Los usuarios seleccionados en los grupos de acceso tendrán autorización para entrar o salir de las puertas seleccionadas con las tarjetas vinculadas o las huellas dactilares.

9. Opcional: Hacer click en para editar el acceso al grupo si es necesario.

7.3 Configurar opciones avanzadas

Se pueden configurar las funciones de control de acceso para saber los requisitos especiales para cada caso diferente, como la autenticación multifactor, anti-passback, etc

Nota

- *Para las funciones relacionadas con la tarjeta (tipo de tarjeta de control de accesos / autenticación de múltiples factores), solo se muestran las tarjetas con acceso aplicado por el grupo cuando se agreguen tarjetas.*
- *Las opciones avanzadas deben ser soportadas por el dispositivo.*
- *Mantener el cursor sobre la opción avanzada y luego hacer click en para personalizar las funciones avanzadas que se muestran.*

7.3.1 Configurar parámetros del dispositivo

Después de añadir el dispositivo de control de accesos, se pueden configurar los parámetros de los dispositivos de control de accesos como puntos de control de accesos, Alarma de Entradas, Alarma de Salidas, lectores de tarjetas.

Configurar Parámetros for Dispositivo de Control de Accesos

Después de añadir el dispositivo de control de accesos, se pueden configurar sus parámetros, incluyendo superposición de información del usuario en la imagen, carga de imágenes después de la captura, Almacenamiento de imágenes capturadas, etc.

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Parámetro del Dispositivo**.

Nota

Se pueden encontrar los parámetros del dispositivo en la lista de funciones avanzadas, moviendo el cursor en la Función Avanzada, y después haciendo Click en para Seleccionar los parámetros del dispositivo que se muestran.

2. Seleccionar un acceso del dispositivo para mostrar sus parámetros en la página derecha.
3. Seleccionar el interruptor a ON para habilitar las funciones correspondientes.

Nota

- *Los parámetros mostrados pueden variar para diferentes dispositivos de control de acceso.*
- *Algunos de los siguientes parámetros no se enumeran en la página de información básica, hacer click en **Más** para editar los parámetros.*

RS-485 Comm. Redundancia

Se debe habilitar esta función si se conecta el lector de tarjetas RS-485 al dispositivo de control de acceso de forma redundante.

Mostrar la cara detectada

Mostrar la imagen de la cara al autenticar.

Mostrar el número de tarjeta

Mostrar la información de la tarjeta al autenticarse.

Mostrar información de la persona

Se muestra la información de la persona al autenticar.

Información de la persona superpuesta en la imagen

Se muestra la información de la persona en la imagen capturada.

Mensaje de voz

Si se habilita esta función, el aviso de voz se habilita en el dispositivo. El aviso de voz se puede escuchar cuando el dispositivo está activo.

Actualizar la foto después de ser capturada

Se actualiza las imágenes capturadas por la cámara vinculada al sistema automáticamente.

Guardar la imagen después de ser capturada

Si se habilita esta función, se puede guardar la imagen capturada por la cámara vinculada al Dispositivo.

Presionar la Tecla para introducir el número de la tarjeta

Si se habilita esta función, se puede ingresar el número de la tarjeta presionando la Tecla.

Wi-Fi

Si se habilita esta función, el dispositivo puede sondear la comunicación de la dirección de los dispositivos MAC y actualizer la dirección MAC al sistema. Si la dirección MAC coincide con la dirección especificada, el sistema puede desencadenar algunas acciones de vinculación.

3G/4G

Si habilita esta función, el Dispositivo puede comunicarse en una red 3G / 4G.

4. Hacer click en **OK**.
5. Opcional: Hacer click en **Copiar a**, y después seleccionar el dispositivo de control de accesos para copiar los parámetros en la página de los dispositivos seleccionados.

Configurar los parámetros para Puerta/ Ascensor

Después de añadir el dispositivo de control de accesos, se pueden configurar los parámetros del punto de acceso (puerta o planta).

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Parámetro del dispositivo**.
2. Seleccionar un Dispositivo de Control de Accesos en el panel de la izquierda y después hacer click en para mostrar las puertas y plantas del dispositivo seleccionado.
3. Seleccionar una puerta o planta para mostrar los parámetros en la página derecho.
4. Editar los parámetros de la puerta o planta.

Nota

- *Los parámetros mostrados pueden variar para los diferentes dispositivos de control de accesos.*
- *Algunos de los siguientes parámetros no son listados en la página de información básica, hacer click en **Más** para editar los parámetros.*

Nombre

Editar el nombre del lector de tarjeta como se desee.

Puerta de Contacto

Se puede configurar el sensor de la Puerta como si permaneciera continuamente abierto. Generalmente permanece cerrado.

Tipo de botón de Salida

Se puede configurar el botón de salida como constantemente cerrado o abierto. Generalmente permanece abierto.

Tiempo de Puerta Cerrada

Después de pasar la tarjeta normal y accionar el relé, el temporizador comieza a funcionar para bloquear la Puerta.

Duración de Apertura Extendida

El contacto de la Puerta se puede habilitar en el retraso apropiado después de que la persona con acceso extendido necesita deslizar la tarjeta.

Alarma de puerta abierta fuera de tiempo

La alarma puede activarse si la puerta no se ha cerrado en el período de tiempo configurado. Si se establace en 0, no se activará ninguna alarma.

Bloquear la Puerta cuando esté cerrada

La puerta se puede bloquear una vez que se cierra, incluso si no se alcanza el Tiempo de bloqueo de puerta.

Código de coacción

La puerta puede ser abierta poniendo el Código de coacción cuando hay coacción. Al mismo tiempo, el software puede Informar la duración del evento.

Contraseña Maestra

El usuario específico puede abrir puede abrir la Puerta introduciendo la Contraseña Maestra.

Descartar Código

Crear un código de salida que se pueda usar para detener el zumbador del lector de tarjetas (ingresando el código de salida en el teclado).

Nota

- *El Código de coacción, la super contraseña y el Código de salida deben ser diferentes de la contraseña de autenticación.*
- *La longitud del Código de coacción, la super contraseña y el Código de despido tienen que estar acorde con las características del dispositivo, conteniendo de 4 a 8 digitos.*

5. Hacer click en **OK**.
6. Opcional: Hacer click en **Copiar a** y después seleccionar la puerta/planta para copiar los parámetros en la página de las puerta/planta(s) seleccionadas.

Nota

La duración de los parámetros del estado de la puerta o planta serán copiados en la puerta/planta seleccionada.

Configurar Parámetros para Lector de Tarjeta

Después de añadir el dispositivo del control de accesos, se pueden configurar los parámetros de lectura de la tarjeta.

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Parámetro del Dispositivo**.
2. En la lista de la izquierda del dispositivo, hacer click en para ampliar la Puerta. Seleccionar un lector de tarjeta y se puede editar los parámetros del lector de tarjeta a la derecha.
3. Editar los parámetros básicos del lector de tarjeta en la página de información básica.

Nota

- *Los parámetros mostrados pueden variar para los diferentes dispositivos de control de accesos. Hay parámetros que se enumeran a continuación. Consultar el Manual de Usuario para obtener más información.*
- *Algunos de los siguientes parámetros no están listados en la página de información básica. Hacer click en **Más** para editar los parámetros.*

Nombre

Editar el nombre del lector de tarjeta como se desee.

Polaridad del LED OK/Error Polaridad de LED/Polaridad del Zumbador

Configurar la polaridad del LED OK/ polaridad del LED de error/ polaridad del LED del zumbador de la tarjeta principal acorde con el lector de tarjetas. Generalmente adopta la configuración

por defecto.

Intervalo mínimo para pasar la tarjeta

Si el intervalo entre que se pasa la tarjeta es menor al tiempo establacido, el pase de la tarjeta no es válido. Se puede configurar entre 0 y 255.

Intervalo máximo al entrar con Contraseña

Cuando se introduce la contraseña en el lector de tarjetas, si el interval de tiempo entre presionar dos dígitos es mayor que el valor establacido, los dígitos que se introdujeron anteriormente se borrarán automáticamente.

Alarma de máximos intentos fallidos

Habilitar el informe de alarma cuando los intentos de lectura de la tarjeta alcanzan el valor establacido.

Tiempo máximo de fallo

Configurar los intentos máximos fallidos de la tarjeta.

Detección de Manipulación

Habilitar la detección de manipulación indebida para el lector de tarjetas.

Comunicación con cada controlador

Cuando el dispositivo de control de accesos no se puede conectar con el lector de tarjetas durante más tiempo del tiempo establacido, el lector de tarjetas se apagará automáticamente.

Tiempo de zumbido

Ajustar el tiempo de zumbido del lector de tarjetas. El tiempo disponible varía entre 0 y 5.999 segundos. Un 0 representa zumbido continuo.

Tipo de lector de tarjeta/ Descripción del lector de tarjetas

Obtener el tipo y la descripción del lector de tarjeta. Son solo de lectura.

Nivel de Reconocimiento de huellas dactilares

Seleccionar el nivel de reconocimiento de las huellas dactilares en la lista desplegable.

Modo predeterminado de autenticación del lector de tarjetas

Ver el modo de autenticación predeterminado del lector de tarjetas.

Capacidad de huella digital

Ver el número máximo de huellas digitales disponibles.

Número de huella digital existente

Ver el número de huellas dactilares existentes en el dispositivo.

Resultado

El dispositivo puntuará la imagen captada en relación con el ángulo de giro, el ángulo de inclinación y la distancia pupilar. Si la puntuación es menor que el valor de configuración, se producirá. Si la puntuación es menor que el valor de configuración, se producirá un error en el reconocimiento facial.

Tiempo límite de reconocimiento facial

Si el tiempo de reconocimiento es mayor que el tiempo de configuración, el dispositivo lo indicará.

Intervalo de Reconocimiento Facial

El intervalo de tiempo entre dos reconocimientos faciales continuos. Por defecto es 2 segundos.

Cara 1:1 Umbral de coincidencia

Establacer el umbral de concidencia cuando se autentique a través del modo de concidencia 1:1. Cuanto mayor sea el valor menor será la tasa de aceptación falsa y mayor la tasa de rechazo.

Nivel de seguridad 1:N

Establacer el nivel de seguridad correspondiente al autenticar a través del modo de concidencia 1:N. Cuanto mayor sea este valor menor sera la tasa de aceptación y mayor la tasa de rechazo.

Detección de rostro vivo

Habilitar o deshabilitar la función de detección de rostro vivo. Si se habilita la función, el dispositivo puede reconocer si el usuario está activo o no.

Nivel de seguridad de la detención facial

Después de habilitar la función de la detección facial viva, se puede establacer el nivel de seguridad correspondiente al realizar la autenticación facial en vivo.

Intentos máximos fallidos de autenticación

Configurar el máximo de intentos fallidos de detección de rostro en vivo. El sistema bloqueará la cara del usuario durante 5 minutos si se detecta fallo durante más de los intentos configurados. El mismo usuario no puede autenticarse a través de la cara falsa en 5 minutos. Para desbloquear podrá identificarse con la cara real en los próximos 5 minutos para desbloquear.

Bloqueo de identificación facial errónea

Después de habilitar la función de detección de rostro, el sistema bloqueará el rostro del usuario durante 5 minutos si se pasa del número de intentos permitidos. El mismo usuario no puedo autenticarse a través de la cara falsa en los próximos 5 minutos. Pasado este tiempo para poder desbloquear el usuario debe autenticarse a través de reconocimiento facial dos veces seguidas.

Modo de aplicación

Se puede seleccionar el interior u otros modos de aplicación acorde con el ambiente actual.

4. Hacer click en **OK**.
5. Opcional: Hacer click en **Copiar a**, y después seleccionar el lector de tarjetas para copiar los parámetros en la página al lector seleccionado.

Configurar Parámetros for Alarma de Entrada

Después de añadir el dispositivo de control de accesos, se pueden configurar los parámetros para

sus alarmas de entrada.

Pasos

> ***Nota***
>
> *Si la Alarma de Entrada está armada, no se pueden editar sus parámetros. Desarmar primero.*

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Parámetros del Dispositivo**.
2. En la lista de dispositivos de la izquierda, hacer click en para ampliar la Puerta. Seleccionar en alarma de entrada y se puede editar los parámetros de la alarma de entrada en la derecha.
3. Configurar los parámetros de Alarma de Entrada.

   Nombre

   Editar el nombre de entrada como se desee.

   Tipo de detector

   El tipo de detector de la Alarma de Entrada.

   Tipo de Zona

   Configurar el tipo de zona para la Alarma de Entrada.

   Sensibilidad

   La Alarma de Entrada se active solo cuando la duración de la señal detectada por el detector alcanza el tiempo configurado. Por ejemplo, si se ha configurado la sensibilidad en 10 ms, solo cuando la duración de la señal detectada por el detector alcanza los 10 ms, se activa esta Alarma de Entrada.

   Activación Alarma de Salida

   Seleccionar la Alarma de Salida(s) para ser activada.
4. Hacer click en **OK**.
5. Opcional: Hacer click en el interruptor de la esquina superior derecho para armar o desarmar la Alarma de Entrada.

Configurar Parámetros de la Alarma de Salida

Después de añadir el dispositivo de control de accesos, si el dispositivo enlaza a la Alarma de Salida, se pueden configurar los parámetros.

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Parámetros de Dispositivo** para entrar a la página de configuración de los parámetros del dispositivo.
2. En la lista de Dispositivos de la izquierda, hacer click en para ampliar la Puerta. Seleccionar una alarma de entrada y editar los parámetros de Alarma de Entrada en la derecha.
3. Configurar los parámetros de la Alarma de Salida.

   Nombre

   Editar el nombre del lector de tarjetas.

Tiempo activo de Alarma de Salida

Cuánto tiempo durará la Alarma de Salida después de activada.

4. Hacer click en **OK**.
5. Opcional: configurar el interruptor de la esquina superior derecha a **ON** para activar la Alarma de Salida.

7.3.2 Configurar Permanecer en Abierto / Cerrado

Se puede configurar el estado de las puertas como abierto o cerrado y configurar el controlador del ascensor como libre o controlado. Por ejemplo, se puede configurar que la Puerta permanezca cerrada en vacaciones, y configurar que la Puerta permanezca abierta en un período específico de la jornada laboral.

Antes de empezar

Añadir los dispositivos de Control de accesos al sistema.

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Permanecer Abierto/ Cerrado** para entrar el la página Permanecer Abierto/ Cerrado.
2. Seleccionar la Puerta o ascensor que necesita ser configurada en el panel de la izquierda.
3. Configurar la Puerta o el estado del ascensor durante la jornada laboral. Hacer click en **Calendario Semanal** y realizar las siguientes operaciones.
   1) Para la Puerta, hacer click en **Permanecer Abierta** o **Permanecer Cerrada**.
   2) Para el ascensor, hacer click en **Libre** o **Controlado**.
   3) Arrastrar el cursor para dibujar la duración del tiempo, lo que significa que en ese período de tiempo, se configura el grupo de acceso.

   Nota

   Hasta 8 duraciones de tiempo pueden ser configuradas cada día en el calendario semanal.

   4) Opcional: Realiza las siguientes operaciones para editar las duraciones de tiempo.
   Mover el cursor hacia la duración de tiempo to the time duration y arrastrar la duración del tiempo en la barra de la línea de tiempo hasta la posición deseada cuando el cursor gire  .
   Hacer click en la duración del tiempo y editar directamente la hora de inicio / finalización en el cuadro.
   Mover el cursor  para empezar o acabar la duración de tiempo y arrastrar para alargar o acortar la duración del tiempo.
   5) Hacer click en **Guardar**.

   Operaciones Relacionadas

Copiar toda la Semana Entera	Seleccionar una duración de tiempo en la barra de tiempo. Hacer click en **Copiar toda la Semana Entera** para copiar todos los parámetros de la configuración de la barra de tiempo en los otros días de la semana.
Borrar Selección	Seleccionar una duración de tiempo en la barra. Hacer click en **Borrar**

	Selección para borrar esta duración.
Borrar	Hacer click en **Borrar** para borrar todos los ajustes de duración en la planificación semanal.

4. Ajustar el estado de la Puerta durante las vacaciones. Hacer click en **Vacaciones** y realiza las siguientes operaciones.
   1) Hacer click en **Permanecer Abierto** o **Permanecer Cerrado**.
   2) Hacer click en **Añadir**.
   3) Introducir las fechas de inicio y fin.
   4) Arrastrar el cursor para dibujar la duracción del tiempo, lo que significa que en ese período de tiempo, la configuración del grupo de acceso está activada.

   Nota

   Se pueden establacer hasta 8 duraciones de tiempo en un período de vacaciones.

   5) Realiza las siguientes operaciones para editar las duraciones de tiempo.
      - Mover el cursor de la duración de tiempo y arrastrar la duración de tiempo deseada en la barra de tiempo hacia la posición deseada cuando el cursor gire .
      - Hacer click en la duración de tiempo y editar directamente el tiempo de inicio y fin en la Ventana.
      - Mover el cursor al inicio o fin del tiempo de duración y arrastrar para alargar o acortar la duración del tiempo cuando el cursor se vuelve a .
   6) Opcional: Seleccionar la duración de tiempo que necesita ser eliminada, y después hacer click en en la columna de operación para borrar las duraciones de tiempo seleccionadas.
   7) Opcional: Hacer click en en la columna de operación para borrar toda la duración de tiempo de la barra de tiempo.
   8) Opcional: Hacer click en en la columna de operación para eliminar el período de vacaciones desde la lista de vacaciones.
   9) Hacer click en **Guardar**.
5. Opcional: Hacer click en **Copiar a** para copiar las configuraciones del estado de la puerta a otras puertas.

7.3.3 Configurar Autenticación Múltiple

Se pueden gestionar los usuarios por grupos y configurar la autenticación para varios usuarios de un punto de control de accesos (puerta).

Antes de empezar

Configurar el grupo de acceso y aplicar el grupo de acceso al dispositivo de control de accesos. Para obtener más información consultar ***Establacer grupo de acceso para asignar autorización de acceso a usuarios.***

Realizar esta tarea cuando se desee configurar autenticaciones para varias tarjetas de un punto de

control de accesos (puerta).

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Autenticación Multiple.**
2. Seleccionar un Dispositivo de Control de Accesos en la lista de dispositivos del panel de la izquierda.
3. Añadir un grupo de usuarios o de tarjetas para el dispositivo de control de accesos.
   1) Hacer click en **Añadir** en el panel de la derecha.
   2) Create un nombre para el grupo.
   3) Especifique la hora de inicio y la hora de finalización del período efectivo para el grupo de personas / tarjetas.
   4) Seleccionar los miembros y la tarjeta en la lista y el miembro (s) y la tarjeta (s) seleccionados serán añadidos a la lista seleccionada.

   Nota

   Asegurarse de tener una tarjeta de admisión para el usuario.
   Asegurarse de tener configurado el acceso al grupo y aplicar los accesos de grupo al dispositivo de control de accesos.

   5) Hacer click en **Guardar**.
   6) Opcional: Seleccionar el grupo de usuarios o tarjetas y después hacer click en **Borrar** para borrarlos.
   7) Opcional: Seleccionar el grupo de usuarios o tarjetas y después hacer click en **Aplicar** para reaplicar el acceso al grupo que no se haya aplicado previamente.
4. Seleccionar un punto de control de accesos (puerta) del dispositivo seleccionado del panel de la izquierda.
5. Introducir el intervalo máximo al introducir la contraseña.
6. Añadir una autenticación de grupo para el punto de control de acceso seleccionado.
   1) Hacer click en **Añadir** en el panel de Autenticación de Grupos.
   2) Seleccionar una plantilla configurada como la plantilla de autenticación de la lista desplegable.

   Nota

   *Para configurar la plantilla, consultar **Configurar Programación y plantilla**.*

   3) Seleccionar el tipo de autenticación como **Autenticación Local, Autenticación local y puerta abierta**, o **Autenticación Local y super contraseña** de la lista desplegable.

   Autenticación Local

   Autenticación por el Dispositivo de Control de Accesos.

   Autenticación Local y Puerta Abierta Remotamente

   Autenticación por el Dispositivo de Control de Accesos y por el software. Cuando la persona deslice la tarjeta en el dispositivo se abrirá una Ventana. Se puede desbloquear la puerta a través del software.

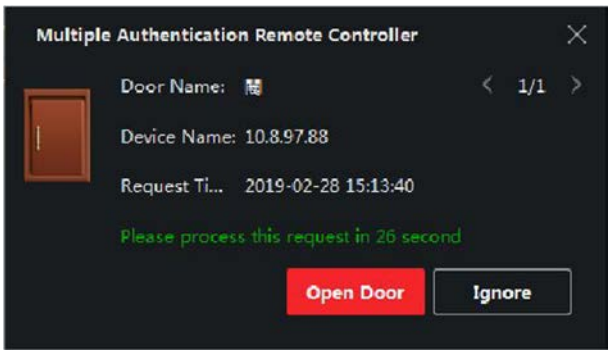

Figure 7-1 Puerta Abierta Remotamente

Nota

*Se puede verificar **Autenticación fuera de línea** para habilitar la Autenticación de Contraseña Maestra cuando el dispositivo de control de accesos es desconectado del software.*

Autenticación Local y Contraseña Maestra

Autenticación por el Dispositivo de Control de Accesos y por la Contraseña Maestra.

4) Seleccionar el grupo de personas/ tarjetas añadidas en la la lista de abajo a la izquierda y se añadirá para la lista de la derecha como grupo de Autenticación.

5) Hacer click en grupo de autenticación añadida en la lista de la derecho para configurar el tiempo de Autenticación en la columna de tiempo.

Nota

- *El tiempo de Autenticación debe ser mayor de 0 y más pequeño que la cantidad de personas añadidas en el grupo personal.*
- *El máximo valor para el tiempo de autenticación es 16.*

6) Hacer click en **Guardar**.

Nota

- *Para cada punto de control de accesos (puerta) hasta 4 grupos de autenticación pueden ser añadidos.*
- *Para el Grupo de Autenticación cuyo tipo de Autenticación es **Autenticación Local**, hasta 8 grupos de personas/ tarjetas pueden ser añadidas por el Grupo de Autenticación.*
- *Para el Grupo de Autenticación cuyo tipo es **Autenticación Local and Contraseña Maestra** or **Autenticación Local and Puerta Abierta Remotamente**, hasta 7 grupos de personas/ tarjetas pueden ser añadidos al Grupo de Autenticación.*

7. Hacer click en **Guardar**.

7.3.4 Configuración personalizada de Wiegand

Basado en el conocimiento de actualización para la configuración Wiegand a terceros, se pueden configurar múltiples reglas de personalización de Wiegand para comunicar entre el dispositivo y el

lector de tarjetas.

Antes de empezar

Conectar los lectores de tarjeta al dispositivo.

Pasos

Nota

- *Por defecto, el dispositivo desactiva la función Wiegand personalizada. Si el dispositivo habilita la función Wiegand personalizada, todas las interfaces Wiegand en el dispositivo utilizarán el protocolo Wiegand.*
- *Se pueden configurar hasta 5 Wiegands personalizado.*
- *Para más detalles sobre el Wiegand personalizado, consultar* ***Descripciones de Reglas Personalizadas de Wiegand****.*

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Wiegand Personalizado** para entrar en la página de configuración de Wiegand.
2. Seleccionar un Wiegand personalizado en la izquierda.
3. Crear un Nombre Wiegand.

Nota

Se permiten hasta 32 caracteres en el nombre de Wiegand.

4. Hacer click en **Seleccionar Dispositivo** para Seleccionar el Dispositivo de Control de Accesos para personalizarlo.
5. Ajustar el modo de paridad acorde a la propiedad del lector de tarjeta.

Nota

- *Hasta 80 bits son permitidos en la longitud total.*
- *El bit de inicio de paridad impar, la longitude de paridad impar, el bit de inicio de paridad par y el rango de longitude de paridad par es de 1 a 80 bits.*
- *El bit de inicio de la ID de la tarjeta, el Código de fabricante, el Código del sitio y el OEM deben oscilar entre 1 y 80 bits.*

6. Establacer la regla de transformación de salida.
   1) Hacer click en **Establacer Regla** para abrir la Ventana de Establacer Reglas.

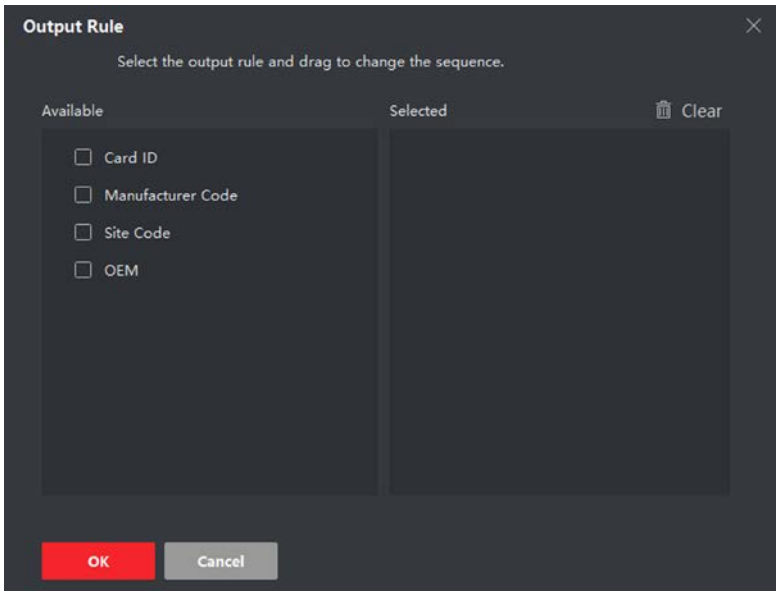

Figure 7-2 Configurar Regla de transformación de salida

2) Seleccionar reglas en la lista de la izquierda.
   Las reglas seleccionadas serán añadidas a la lista de la derecha.
3) Opcional: Arrastrar para cambiar el orden de las reglas.
4) Hacer click en **OK**.
5) En la pestaña personalizado de Wiegand, configurar el bit de inicio, la longitud y el dígito decimal de la regla.

7. Hacer click en **Guardar**.

7.3.5 Configurar el Modo de autenticación del Lector de tarjeta y su esquema

Se pueden configurar las reglas de paso para el lector de tarjeta del Dispositivo de Control de Accesos acorde con las necesidades actuales.

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Autenticación** para entrar en la página de Configuración de Modo de Autenticación.
2. Seleccionar el lector de tarjeta a la izquierda para Configurar.
3. Configurar el modo de lector de tarjeta de Autenticación.
   1) Hacer click en **Configuración**.

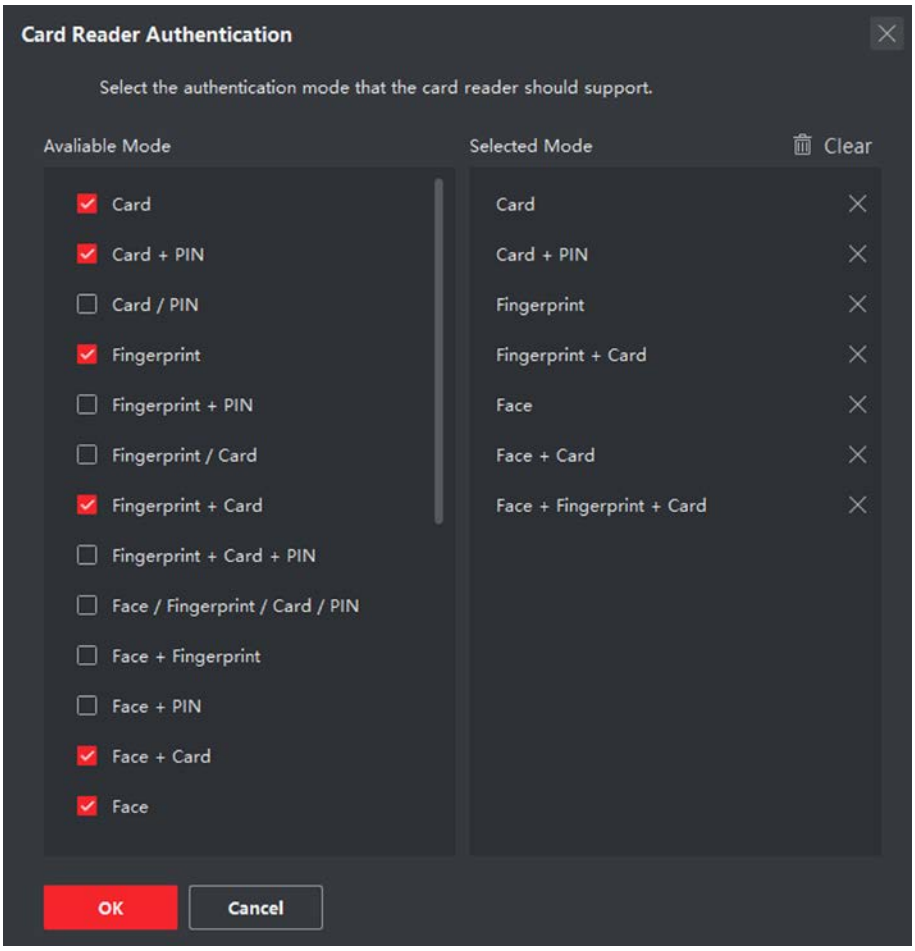

Figure 7-3 Seleccionar modo de autenticación de lector de tarjeta

Nota

El PIN se refiere al Código PIN establacido para abrir la puerta. Ver ***Configurar Información de Control de accesos****.*

2) Comprobar los modos en la lista de modos disponibles y serán añadidos a la lista de modos seleccionables.
3) Hacer click en **OK**.
   Después de seleccionar los modos, estos aparecerán como iconos con diferentes colores.

4. Hacer click en el icono de Seleccionar el modo de autenticación del lector de tarjeta, y dibujar con el cursor una barra de color sobre el esquema, sobre ese period de tiempo, la autenticación del lector de tarjeta será válida.
5. Repetir los pasos anteriores y ajustar los períodos de tiempo.

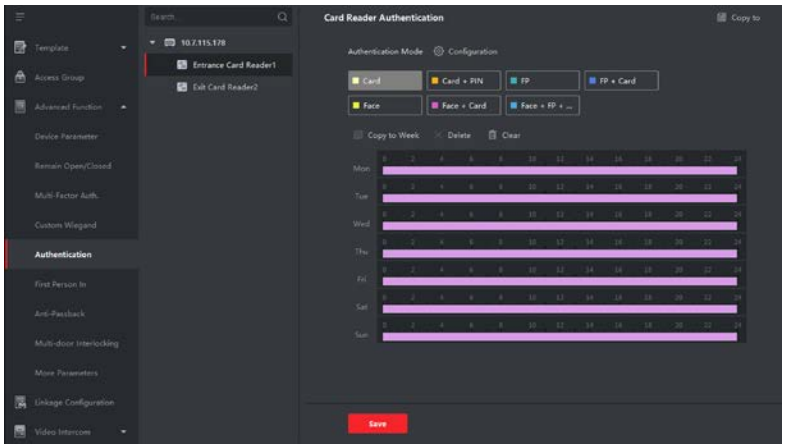

Figure 7-4 Configurar Modos de autenticación para lectores de tarjeta

6. Opcional: Seleccionar un día configurado y hacer click en él. Hacer click en **Copiar a la semana** para copiar la misma configuración al resto de días.
7. Opcional: Hacer click en **Copiar a** para copiar la configuración a otros lector de tarjetas.
8. Hacer click en **Guardar**.

7.3.6 Configurar usuario en el modo de Autenticación

Se puede establacer las reglas de aprobación para la persona según el Dispositivo de Control de Accesos de acuerdo a sus necesidades reales.

Antes de empezar

Asegurarse de que el Dispositivo de Control de Accesos soporta la función de autenticación de personas.

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Autenticación**.
2. Seleccionar un Dispositivo de Control de Accesos (que Soporte la función) en el panel de la izquierda para entrar en la página de configuración.
3. Hacer click **Añadir** para entrar en la Ventana de agregado.
4. Seleccionar la persona que necesita ser configurada en el panel de la izquierda.
   Las personas seleccionadas serán añadidas en el panel de la derecha.
5. Seleccionar el modo de Autenticación en la lista desplegable del **Modo de configuración**.
6. Hacer click en **OK**.

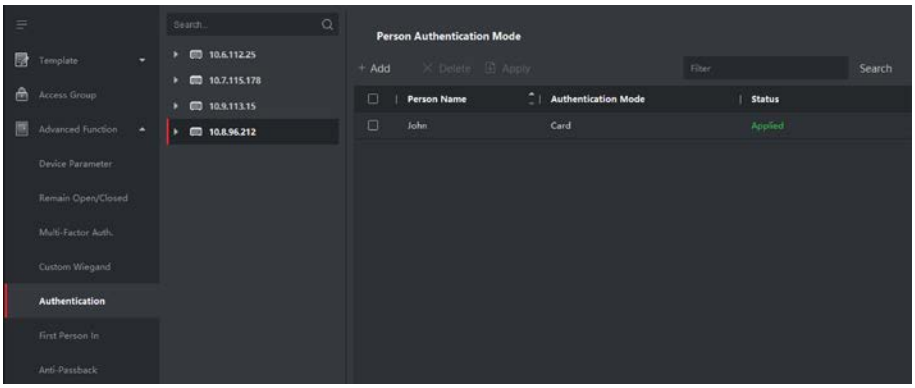

Figure 7-5 Configurar los modos de autenticación para personas

7. Opcional: Seleccionar la persona en la página de Modo de autenticación, y posteriormente hacer click en **Aplicar** para aplicar este modo de autenticación en el dispositivo.

Nota

Autenticación del usuario tiene mayor prioridad que. Cuando el dispositivo de Control de Accesos ha sido configurado con el modo de autentación del usuario, la persona debería autenticarse en el dispositivo con este método.

7.3.7 Configurar Paso Libre

Se puede configurar el acceso a múltiples personas para un punto de control de accesos. Después de ser autorizada la primera persona, se permite el acceso libre al resto de personas.

Antes de empezar

Configurar el grupo de acceso y aplicarlo al Dispositivo. Para más detalles, ***Configurar el acceso al grupo para asignar la autorización de acceso para los usuarios***.

Realiza esta tarea cuando se quiera configurar puerta abierta con paso.

Pasos

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Paso Libre** para entrar en la página de Paso Libre.
2. Seleccionar un Dispositivo de Control de Accesos en la lista del panel de la izquierda.
3. Seleccionar el modo actual como **Habilitar permanecer puerta abierta despues del Paso Libre**, **Deshabilitar Permanecer abierto** o **Autorización por Paso Libre** desde el desplegable para cada punto de control de accesos.

   Habilitar permanecer abierto después de Paso Libre

   La puerta permanece abierta durante el tiempo configurado, después se autoriza el paso libre hasta que la puerta que ha permanecido abierta para el Paso Libre es cerrada cuando se termina el tiempo configurado.

Nota

La duración de permanecer la puerta abierta es entre 0 y 1440 minutos. Por defecto, la puerta permanece abierta una duración de 10 minutos.

Deshabilitar la función de Paso Libre

Deshabilitar la función de Paso Libre, poniendo la autenticación normal.

Autorización por Paso Libre

Toda Autenticación (excepto para la autenticación de tarjeta maestra, Contraseña Maestra, tarjeta y Código de coacción) son permitidos solo después de la autorización de Paso Libre.

Nota

Puede autenticarse como primer usuario para deshabilitar el modo de primer usuario.

4. Hacer click en **Añadir** en el panel de Paso Libre.
5. Seleccionar una persona en la lista de la izquierda y será añadida como usuario seleccionado para el paso libre de las puertas.
   El usuario añadido se verá en la lista.
6. Opcional: Seleccionar un usuario desde la lista y hacer click en **Borrar** para eliminar el usuario de la lista.
7. Hacer click en **Guardar**.

7.3.8 Configurar Anti-Passback

Se puede configurar el paso único por un punto de control de accesos que ha sido especificado y sólo podrá volver a pasar si esta persona cumple las características configuradas de haber salido del recinto.

Antes de empezar

Habilitar la función Anti-passback del dispositivo de control de accesos.

Realizar esta tarea cuando se quiere configurar el anti-passback en el dispositivo de Control de Accesos.

Pasos

Nota

Cada función de Anti-passback o de múltiple esclusas puede ser configurado para un Dispositivo de Control de Accesos a la vez

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Anti-Retorno** para entrar en la página de configuración de Anti-Passback.
2. Seleccionar un Dispositivo de Control de Accesos sobre el panel de la izquierda.
3. Seleccionar un lector de tarjeta para comenzar en el campo **Primer Lector de tarjeta**.

4. Hacer click en de la seleccionado como primer lector de tarjeta en la columna **Lector de tarjeta Posterior** para abrir la selección del lector de tarjeta.
5. Seleccionar el lector posterior de tarjetas para ese primer lector seleccionado antes.

Nota

Hasta 4 lectores posteriores pueden ser añadidos al primer lector de tarjetas para realizar la función de Antipass-back.

6. Hacer click en **OK** en la selección para Guardar.
7. Hacer click en **Guardar** en la configuración de Anti-Passback para Guardar la configuración y que esta resulte efectiva.

Ejemplo

Si se configura que el Lector IN_01 como lector de comienzo, y como lectores posteriores de ese lector, se selecciona los lectores IN_02 y OUT_04. Entonces la única forma de tener acceso, es en primer lugar entrar por el lector In_01, y después continuar por LectorIn_02 y Out_04.

7.3.9 Configurar Esclusas multipuerta

Se puede configurar las esclusas multipuerta entre diferentes puertas dentro del mismo dispositivo de control de accesos. Para abrir una de las puertas, las otras puertas deben permanecer cerradas. Esto significa que las esclusas están combinadas con los grupos de puerta, por lo que sólo una puerta se podrá abrir a la vez.

Realiza esta tarea cuando se necesite realizar Multi Esclusa entre diferentes puertas.

Pasos

Nota

- *La función de esclusas sólo es soportada por los dispositivos de control de accesos que tienen mas de un punto de control de accesos (puertas).*
- *Tanto el antipass-back o las esclusas pueden ser configuradas en un dispositivo de control de accesos a la vez.*

1. Hacer click en **Control de accesos** → **Función Avanzada** → **Interbloqueo de varias puertas**.
2. Seleccionar un Dispositivo de Control de Accesos en el panel de la izquierda.
3. Hacer click en **Añadir** en el panel de esclusas de varias puertas para Añadir puntos de Control de accesos y abrir la pestaña de agregar.
4. Seleccionar al menos dos puntos de control de accesos (puertas) de la lista.

Nota

Hasta cuatro puertas pueden añadidas en una combinación de multi esclusas.

5. Hacer click en **OK** para Añadir la selección de puntos de control de accesos para el esclusamiento.

La configuración de la multi esclusa será listada en el panel de esclusas de varias puertas.

6. Opcional: Seleccionar una combinación de multipuerta desde la lista y hacer click en **Borrar** to eliminar esta combinación the combination.
7. Hacer click en **Aplicar** para asignar la configuración en el dispositivo de control de accesos.

7.4 Configurar otros Parámetros

Después de añadir el Dispositivo de Control de Accesos, Se pueden configurar Parámetros tales como Parámetros de red, Parámetros de capturación, de RS-485, Wiegand, etc.

7.4.1 Set Múltiple NIC Parámetros

Si el dispositivo soporta múltiples interfaces de red, Se pueden configurar los Parámetros de estos NICs a través del software, como por ejemplo, la dirección IP, la MAC, el puerto, etc.

Pasos

Nota

Esta función debe ser compatible con el dispositivo.

1. Entrar en el modulo de Control de accesos.
2. En la barra de navegación situada en la parte izquierda, entrar en **Función Avanzada** → **Más Parámetros**.
3. Seleccionar un Dispositivo de Control de Accesos en la lista de dispositivos y Hacer click en **NIC** para entrar en la página de Configuración NIC.
4. Seleccionar el NIC que se quiere configurar desde el menú desplegable.
5. Configurar los Parámetros de red habituales como Dirección IP, Puerta de enlace, máscara de red, etc.

   Dirección MAC

   La dirección MAC de un dispositivo de control de accesos es un único identificador asignado a la tarjeta de red para las comunicaciones físicas.
6. Hacer click en **Guardar**.

7.4.2 Configurar Parámetros de red

Después de añadir el dispositivo de Control de Accesos, Se puede configurar el modo de carga y crear una cuenta a través de la red cableada o inalámbrica.

Configuración del modo de carga

Se puede configurar el modo en el que un dispositivo carga los registros a través del protocolo

EHome.

Pasos

Nota

Asegurar que el dispositivo no está añadido por EHome.

1. Entrar en el módulo de Control de accesos.
2. En la barra de navegación en la parte izquierda, entrar en **Función Avanzada** → **Más Parámetros**.
3. Seleccionar un Dispositivo de Control de Accesos en la lista de Dispositivos y entrar en **Red** → **Cargando Modo**.
4. Seleccionar el grupo desde el desplegable.
5. Verificar **Habilitar** para activar la configuración del modo de carga.
6. Seleccionar el modo de carga desde el listado desplegable.
   – Habilitar **N1** o **G1** desde el canal principal y el canal de respaldo.

Seleccionar **Cerrar** para deshabilitar el canal principal y el canal de respaldo.

Nota

El canal principal y el de backup no pueden habilitar el N1 o G1 al mismo tiempo.

7. Hacer click en **Guardar**.

Crear una cuenta EHome con comunicación cableada

Se puede configurar una cuenta con el protocolo EHome en el modo de comunicación cableado. Así se añaden dispositivos por el protocolo EHome.

Pasos

Nota

Esta función debe ser compatible con el dispositivo.
Asegurar que el dispositivo no está añadido por EHome.

1. Entrar el en Módulo de Control de accesos.
2. En la barra de navegación en la parte izquierda, entrar en **Función Avanzada** → **Más Parámetros**.
3. Seleccionar un Dispositivo de Control de Accesos en la lista y entrar en **Red** → **Centro de Redes**.
4. Seleccionar el grupo desde la lista desplegable.
5. Seleccionar el **Tipo de dirección** como **Dirección IP Añadida** o **Nombre de Dominio**.
6. Entrar en Dirección IP o Nombre de dominio de acuerdo con el tipo de dirección.
7. Introducir el puerto para el protocolo.

Nota

El puerto de una red cableada e inalámbrica debería ser el mío que el puerto de EHome.

8. Seleccionar el **Protocol Type** como **EHome**.
9. Configurar una cuenta para el centro de red.
10. Hacer click en **Guardar**.

Crear una cuenta EHome con el modo de comunicación inalámbrica

Se puede configurar la cuenta para el protocolo EHome con el modo de comunicación inalámbrica. Así se pueden añadir los dispositivos por este protocolo.

Pasos

Nota

- *Esta función debe ser compatible con el dispositivo.*
- *Asegurar que el dispositivo no está añadido a una cuenta EHome.*

1. Entrar en el modulo de Control de accesos.
2. En la barra de navegación situada a la izquierda, entrar en **Función Avanzada** → **Más Parámetros**.
3. Seleccionar un Dispositivo de Control de Accesos en la lista y entrar en **Red** → **Centro de comunicación inalámbrica**.
4. Seleccionar el nombre de **APN** como **CMNET** o **UNINET**.
5. Introducir el Nº de tarjeta SIM.
6. Seleccionar el grupo desde el desplegable.
7. Introducir la Dirección IP y el puerto.

Nota

- *Por defecto, El puerto de EHome es **7660**.*
- *El puerto de la red inalámbrica o cableada debería coincidir con el puerto EHome.*

8. Seleccionar el **Protocol Type** como **EHome**.
9. Configurar una cuenta para el centro de red.
10. Hacer click en **Guardar**.

7.4.3 Configurar Parámetros de Captura del Dispositivo

Se puede Configurar los parámetros de captura de los dispositivos de control de accesos, incluyendo la captura manual o la captura por evento.

Nota

- *La función de captura debería ser soportada por el Dispositivo.*
- *Antes de configurar los Parámetros de captura, Se debe configurar el almacenamiento de fotografías para definir donde almacenar las imágenes producidas por un evento, para más detalles, ver **Configurar almacenaje de imágenes**.*

Configurar parámetros de Captura por evento

Cuando ocurre un evento, la cámara del dispositivo de control de accesos para comenzar a obtener imágenes y grabar que es lo que está sucediendo en ese evento concreto. Se puede visualizar las imágenes obtenidas cuando se ven los detalles en el Centro de Eventos. Antes, se necesitan configurar los parámetros para obtener el número de imágenes que se capturan en un determinado tiempo.

Antes de empezar

Antes de la configuración de los parámetros de las capturas, se debería configurar primero donde se almacenan. Para ello, ver ***Configurar almacenaje de imágenes***.

Pasos

Nota

Esta función debe ser compatible con el dispositivo.

1. Entrar en el módulo de control de accesos.
2. En la barra de navegación de la izquierda, entrar en **Función Avanzada** → **Más Parámetros** → **Captura**.
3. Seleccionar un dispositivo de Control de Accesos en el lista de dispositivos y seleccionar **Captura Enlazada.**
4. Ajustar el tamaño y la calidad de la imagen.
5. Establacer los tiempos de captura para definer cuentas imágenes pueden ser capturadas.
6. Si el tiempo de captura es mayor a 1, configurar el intervalo para cada captura.
7. Hacer click en **Guardar**.

Configurar los parámetros de Captura Manual.

En el módulo de estado de monitorización, se puede capturar una imagen manualmente en la cámara del dispositivo de control de accesos haciendo click en el botón. Antes es necesario configurar los parámetros da la calidad de la imagen.

Antes de empezar

Antes de configurar los parámetros de captura, se debe configurar la ruta para definir donde son se guardan las imágenes capturadas. Para más detalles ver ***Establacer una ruta para guardar archivos***.

Pasos

Nota

Esta función debe ser compatible con el dispositivo.

1. Entrar en el módulo de control de accesos.
2. En la barra de navegación de la izquierda, entrar en **Función Avanzada** → **Más Parámetros** → **Captura**.

3. Seleccionar un Dispositivo de Control de Accesos en la lista de dispositivos y seleccionar **Captura Manual**.
4. Seleccionar la resolución de las imágenes capturadas de la lista desplegable.
5. Seleccionar la calidad de la imagen como **Alta**, **Media**, o **Baja**. El tamaño será mayor cuánto mayor sea la calidad.
6. Hacer click en **Guardar**.

7.4.4 Configuración de los Parámetros para el Terminal de Reconocimiento Facial.

Para el terminal de reconocimiento facial, se pueden configurar sus parámetros Incluyendo base de datos de las fotografías del rostro, autentificación de Código QR, etc.

Pasos

Nota

Esta función debe ser compatible con el dispositivo.

1. Entrar en el módulo de Control de accesos.
2. En la barra de navegación de la izquierda, entrar en **Función Avanzada** → **Más Parámetros**.
3. Seleccionar un Dispositivo de Control de Accesos en la lista de dispositivos y Hacer click en **Terminal de Reconocimiento Facial**.
4. Configurar los parámetros.

Nota

Estos parámetros varían Según los diferentes módelos de dispositivos.

COM

Selecciona un Puerto COM para la configuración. COM1 se refiere a la interfaz RS-485 y COM2 a la interfaz RS-232.

Base de datos facial

Seleccionar Deep Learning como la Base de datos facial.

Autentificar por Código QR

Si está habilitando, la cámara del dispositivo puede escanear el Código QR para la autentificación. Por defecto esta función está deshabilitada.

Autenticación de la Lista negra

Si está habilitando el dispositivo comparará la persona que desea acceder con las que se encuentran en la Lista negra.
Si coincide (la persona está en la Lista negra) se denegará el acceso y el dispositivo cargará una alarma al cliente.
Si no coincide (la persona no está en la Lista negra), se otorgará el acceso.

Guardar autentificación facial

Si está habilitado, la captura de la imagen facial será guardado en el dispositivo.

Versión MCU

Ver la version MCU del dispositivo

5. Hacer click en **Guardar**.

7.4.5 Configurar los parámetros de RS-485

Se puede configurar los parámetros de RS-485 en el Dispositivo de Control de Accesos. Incluyendo la velocidad de transmission, el bit de paridad, el tipo de paridad, el tipo de control de flujo, el modo de comunicación, el modo de trabajo y el modo de conexión.

Pasos

Nota

Las configuraciones de RS-485 deben ser compatibles con el dispositivo.

1. Entrar en el módulo de Control de accesos.
2. En la barra de navegación izquierda, entrar en **Función Avanzada** → **Más Parámetros**.
3. Seleccionar un Dispositivo de Control de Accesos en la lista de dispositivos y hacer click en **RS-485** para entrar en la página de configuración de RS-485.
4. Seleccionar el número de puerto serie de la lista desplegable para configurar los parámetros de RS-485.
5. Configurar en la lista desplegable la velocidad de transmission, el bit de paridad, el tipo de paridad, el bit de parada, el modo de comunicación, el modo de trabajo y el modo de conexión.
6. Hacer click en **Guardar**.
   - Los parámetros configurados serán aplicados al Dispositivo automáticamente.
   - Después de cambiar el modo de trabajo o el modo de conexión, el dispositivo se reiniciará automáticamente.

7.4.6 Configurar los parámetros Wiegand

Se puede configurar el canal Wiegand y el modo de comunicación en el Dispositivo de Control de Accesos. Después de la configuración de los parámetros Wiegand el dispositivo se puede conectar al lector de tarjeta Wiegand.

Pasos

Nota

Esta función debe ser compatible con el dispositivo.

1. Entrar en el módulo de Control de Accesos.
2. En la barra de navegación izquierda, entrar en **Función Avanzada** → **Más Parámetros**.

3. Seleccionar un Dispositivo de Control de Accesos en la lista de dispositivos y hacer click en **Wiegand** para entrar en la página de configurar Wiegand.
4. Ajusta el interruptor para habilitar la función Wiegand para el dispositivo.
5. Seleccionar el número del canal Wiegand y el modo de comunicación en la lista desplegable.

Nota

*Si se configura la **Dirección de comunicación** como **Enviando**, se requiere configurar el **Modo Wiegand** como **Wiegand 26** o **Wiegand 34**.*

6. Hacer click en **Guardar**.
   - Los parámetros configurados serán aplicados al dispositivo automáticamente.
   - Después de cambiar la dirección de comunicación el dispositivo se reiniciará automáticamente.

7.4.7 Habilitar Encriptación de tarjeta M1

Encriptación de tarjeta M1 puede mejorar el nivel de seguridad.

Pasos

Nota

La función debe ser compatible con el dispositivo del control de accesos y el lector de tarjeta.

1. Entrar en el módulo de control de accesos.
2. En la barra de navegación izquierda, entrar en **Función Avanzada** → **Más Parámetros**.
3. Seleccionar un Dispositivo de Control de Accesos en la lista de dispositivos y hacer click en **M1 Encriptación de tarjeta M1** para entrar en la página de Encriptación de tarjeta M1.
4. Configurar la activación de la función de la encriptación de tarjeta M1.
5. Configurar el sector ID.

   El rango de ID va del 1 al 100.
6. Hacer click en **Guardar** para Guardar la configuración.

7.5 Configurar Vínculos de acción para Control de accesos

Los eventos desencadenados por el Dispositivo de Control de Accesos, lector de tarjetas y alarma de entrada así como el paso de tarjetas de usuario, la detección de la dirección MAC del terminal móvil y el ID de empleados detectados, pueden activar una serie de acciones para notificar al personal de seguridad y el registros de eventos.
Se admiten dos tipos de acciones de vinculación: acciones de cliente y acciones del dispositivo.

- **Acciones del Cliente:** Cuando el evento es detectado, se activan las acciones en el software como emitir un sonido de alarma y enviar un correo electrónico para notificar al personal de seguridad.
- **Acciones del Dispositivos:** Cuando el evento es detectado se activan acciones como zumbidos, puertas abiertas/cerradas, reproducción de audio, etc., para notificar al personal de seguridad y permitir o prohibir el acceso.

7.5.1 Configurar acciones del software para el evento de acceso

Se puede asignar acciones de vinculación del software mediante la configuración de una regla. Por ejemplo, cuando se detecta un evento, aparece una advertencia audible para notificar al personal de seguridad.

Pasos

Nota

Las acciones de vinculación aquí se refieren a la vinculación de las acciones propias del software, como una advertencia Sonora, una vinculación de correo electrónico, etc.

1. Hacer click en **Gestión de eventos** → **Evento de control de accesos**.
   El Dispositivo de Control de Accesos añadido será mostrado en la lista de dispositivos.
2. Seleccionar un recurso (incluyendo Dispositivo, Alarma de Entrada, puerta/ascensor y lector de tarjeta) desde la lista de dispositivos.
3. Seleccionar el evento(s) y hacer click en **Editar Prioridad** para definir la prioridad para los eventos, se puede usar para filtrar eventos en el Centro de Evento.
4. Establacer las acciones de enlace del evento.
   1) Seleccionar el evento (s) y hacer click en **Editar Enlace** para configurar las acciones del software cuando se desencadenan los eventos.

      Advertencia audible

      El software proporciona una advertencia audible cuando se dispara la alarma. Se puede seleccionar el sonido de la alarma deseado.

      Nota

      *Para configurar el sonido de la alarma, hacer referencia a **Configurar Sonido de Alarma**.*

      Enlace de Email

      Enviar una notificación de email con la información de la alarma de uno o más receptores.
   2) Hacer click en **OK**.
5. Habilitar el evento para que cuando sea detectado, se envíe un evento al cliente y se activen las acciones de vinculación.
6. Opcional: Hacer click en **Copiar a...** para copiar las configuraciones del evento a otro dispositivo de control de accesos, Alarma de Entrada, puerta/ascensor, o lector de tarjeta.

7.5.2 Configurar las acciones del Dispositivo para el evento de acceso.

Se puede configurar las acciones de enlace del dispositivo de Control de Accesos para un evento disparado. Cuando el evento se dispara, se puede activar la alarma de salida, zumbador, y otras

acciones en el mismo dispositivo.

Pasos

Nota

Debe ser soportado por el dispositivo.

1. Hacer click en **Control de accesos** → **Configuración de enlace.**
2. Seleccionar el Dispositivo de Control de Accesos desde la lista de la izquierda.
3. Hacer click en el botón de **Añadir** para añadir un nuevo enlace.
4. Seleccionar la Fuente del evento como **Enlace de Evento**.
5. Seleccionar the tipo de evento y el evento detallado para configurar el enlace.
6. En el área de Objetivo de vinculación, establacer el objetivo de propiedad para habilitar esta acción.

Zumbador o Controlador

Se activará la advertencia sonora del Dispositivo de control de accesorios.

Captura

La captura en tiempo real se activará.

Grabación

La grabación se activará.

Nota

El dispositivo deberá soportar la grabación.

Zumbador

Se activará la advertencia audible del lector de tarjeta.

Alarma de Salida

La Alarma de Salida se activará para la notificación.

Alarma de Entrada

Armar o desarmar la Alarma de Entrada.

Nota

El dispositivo deberá soportar la función de Alarma de Entrada.

Punto de Acceso

Se activará el estado de la puerta de abrir, cerrar, permanecer abierto y permanecer cerrado.

Nota

La puerta de destino y la puerta de origen no pueden ser la misma.

Reproducción de Audio

El aviso de audio se activará. Y el contenido de audio seleccionado se reproducirá de acuerdo con el modo de reproducción configuradas.

7. Hacer click **Guardar**.
8. Opcional: Después de añadir el enlace del dispositivo.

Editar Configuración de Enlace	Seleccionar las configuraciones del enlace y sus parámetros de eventos.
Eliminar Configuración de Vinculación	Seleccionar las configuraciones de la vinculación en lista de dispositivos y hacer click en **Borrar** para borrarlo.

7.5.3 Configurar acciones del Dispositivo para desplazar la tarjeta

Se puede configurar las acciones de enlace del Dispositivo de Control para el desplazamiento de la tarjeta especificada. Cuando se desliza la tarjeta especificada, se puede activar la Alarma de Salida, el zumbido, y otras acciones en el mismo dispositivo.

Pasos

Nota

Debe ser soportado por el dispositivo.

1. Hacer click en **Control de accesos** → **Configuración de enlace**.
2. Seleccionar el Dispositivo de Control de Accesos en la lista de la izquierda.
3. Hacer click en el botón **Añadir** para añadir un nuevo enlace.
4. Seleccionar la Fuente del evento como **Enlace de tarjeta.**
5. Introducir el número de tarjeta o seleccionar la tarjeta en la lista desplegable.
6. Seleccionar el lector de tarjeta donde la tarjeta se desliza para activar las acciones vinculadas.
7. En el área Objetivo de vinculación, establacer el objetivo de propiedad para habilitar esta acción.

Zumbador o Controlador

Se activará la advertencia sonora del Dispositivo de control de accesos.

Zumbador en Lector

La advertencia audible del lector de tarjeta se activará.

Captura

La captura en tiempo real se activará.

Grabado

La grabación se activará.

Nota

El Dispositivo debe soportar el grabado.

Alarma de Salida

La alarma de Salida se activará para notificar.

Alarma de Entrada

Armar o desarmar la alarma de Entrada.

Nota

El dispositivo deberá soportar la función de Alarma de Entrada.

Punto de Acceso

El estado de la puerta de abrir, cerrar, permanecer abierto o permanecer cerrado se activará.

Reproducción de audio

El aviso de audio se activará. Y el contenido de audio relacionado con el índice de audio se reproducirá.

8. Hacer click en **Guardar**.
   Cuando la tarjeta (Configurada en el Paso 5) se desliza sobre el lector de tarjeta (Configurada en el Paso 6), se puede activar las acciones vinculadas (Configurada en el paso 7).
9. Opcional: Después de añadir el enlace del dispositivo, se puede realizar las siguientes acciones:

Eliminar la Configuración de Vinculación	Seleccionar las configuraciones del enlace en la lista de dispositivos y hacer click en **Borrar** para borrarlo.
Editar Configuración de Enlace	Seleccionar la configuración del enlace en la lista de dispositivos. Se puede editar sus parámetros, incluyendo fuente de evento y objetivo de enlace.

7.5.4 Configurar enlace del Dispositivo para terminales MAC

Se puede configurar las acciones de enlace del Dispositivo de Control de Accesos para una dirección MAC de un terminal móvil. Cuando el Dispositivo de Control de Accesos detecta la dirección MAC especificada, se puede disparar la salida, el zumbador y otras acciones en el mismo dispositivo.

Pasos

Nota

Deberá ser soportado por el dispositivo.

1. Hacer click en **Control de accesos** → **Configuración del enlace**
2. Seleccionar el Dispositivo de Control de Accesos desde la lista de la izquierda.

3. Hacer click en el botón de **Añadir** para añadir un nuevo enlace.
4. Seleccionar la Fuente de evento como **Enlace MAC**.
5. Introducir la dirección MAC.

Nota

Formato de la dirección MAC: AA:BB:CC:DD:EE:FF.

6. En el área Objetivo de enlace, establacer el objetivo de propiedad para habilitar esta acción.

Zumbador en el Controlador

La advertencia audible del Dispositivo de Control de Accesos se activará.

Zumbador en Lector

La advertencia audible del lector de tarjeta se activará.

Captura

La captura en tiempo real se activará.

Grabado

La grabación se activará.

Nota

El Dispositivo debe soportar el Grabado.

Alarma de Salida

La alarma de Salida se activará para notificación.

Alarma de Entrada

Armar o desarmar la alarma de Entrada.

Nota

El Dispositivo debe soportar la función de Alarma de Entrada.

Punto de Acceso

El estado de la puerta abierto, cerrado, permanecer abierto, o Permanece Cerrado se activará.

Reproducción de Audio

El aviso de audio se activará.

7. Hacer click en **Guardar** para guardar las configuraciones.
8. Opcional: después de añadir el enlace del dispositivo, se pueden realizar una o más de las siguientes acciones:

Editar Configuración de Enlace	Seleccionar la configuración del enlace en la lista de dispositivos. Se puede editar sus parámetros, incluyendo fuente de evento y objetivo de enlace.

Eliminar Configuración de Vinculación	Seleccionar las configuraciones del enlace en la lista de dispositivos y hacer click en **Borrar** para borrarlo.

7.5.5 Configurar acciones del Dispositivo para el ID de usuario

Se puede configurar el enlace del Dispositivo de Control de Accesos para un ID específico de usuario. Cuando el Dispositivo de Control de Accesos detecta el ID de usuario, se puede activar la alarma de salida, el zumbador, y otras acciones en el mismo Dispositivo.

Pasos

Nota

Deberá ser soportado por el dispositivo.

1. Hacer click en **Control de accesos** → **Configuración de enlace**.
2. Seleccionar el Dispositivo de Control de Accesos desde la lista en la izquierda.
3. Hacer click en el botón **Añadir** para Añadir un nuevo enlace.
4. Seleccionar la Fuente de evento como **Vinculación de Persona**.
5. Introducir el número de empleados o seleccionar el usuario desde la lista desplegable.
6. Seleccionar el lector de tarjeta donde la tarjeta se desliza para activar las acciones vinculadas.
7. En el área Objetivo de enlace, establacer el objetivo de propiedad para habilitar esta acción.

Zumbador en el Controlador

La advertencia audible del Dispositivo de Control de Accesos se activará.

Zumbador en Lector

La advertencia audible of lector de tarjeta se activará.

Captura

La captura en tiempo real se activará.

Grabado

La grabación se activará.

Nota

El dispositivo debe soportar la grabación.

Alarma de Salida

La alarma de Salida se activará para notificarlo.

Alarma de Entrada

Armar o Desarmar la alarma de entrada.

Nota

El Dispositivo debe soportar la función de zona.

Punto de Acceso

El estado de la puerta abierto, cerrado, permanecer abierto, o Permanece Cerrado se activará.

Reproducción de Audio

El aviso de audio se activará.

8. Hacer click en **Guardar**.
9. Opcional: después de añadir el enlace del dispositivo, se pueden realizar una o más de las siguientes acciones:

Editar Configuración de Enlace	Seleccionar la configuración del enlace en la lista de dispositivos. Se puede editar sus parámetros, incluyendo fuente de evento y objetivo de enlace.
Eliminar Configuración de Vinculación	Seleccionar las configuraciones del enlace en la lista de dispositivos y hacer click en **Borrar** para borrarlo.

7.6 Control de Puertas o Ascensor

En el módulo de monitorización, se puede ver el estado en tiempo real de las puertas y ascensores manejados por el Dispositivo de Control de Accesos. Se puede también controlar el cierre y apertura de las puertas y ascensores remotamente. El evento de acceso en tiempo real se muestra en este módulo. Se puede ver los detalles de acceso y usuario.

Nota

*Para el usuario con permiso de control de Puerta / ascensor, se puede acceder al módulo de monitoreo y controlar la Puerta/ Ascensor. Los iconos usados para el control no se mostrarán. Para configurar el permiso de usuario, consultar **Añadir Usuario**.*

7.6.1 Control de Estado de las Puertas.

Se puede controlar el estado para una sola puerta, que incluye abrir la puerta, cerrar la puerta, mantener la puerta abierta y permanecer la puerta cerrada.

Pasos

1. Hacer click en **Monitorización** para entrar a la página de estado de motorización.
2. Seleccionar un Punto de Acceso en la esquina superior derecha.

Nota

*Para gestionar el punto de acceso del grupo, ver **Administración del Grupo**.*

3. Hacer click en el icono de la puerta para seleccionar una puerta, o pulsar **Ctrl** y Seleccionar múltiples puertas.
4. Hacer click en los siguientes botones para controlar la puerta.

Puerta Abierta

Cuando la puerta está bloqueada, desbloquearla y se abrirá una vez. Después de la duración abierta, la puerta se cerrará y se bloqueará nuevamente automáticamente.

Puerta Cerrada

Cuando la puerta está desbloqueada, bloquearla y se cerrará. La persona que tiene la autorización de acceso puede acceder a la puerta con credenciales.

Permanece Abierta

La puerta se desbloqueará (no importa si está cerrada o abierta). Todas las personas pueden acceder a la puerta sin necesidad de credenciales.

Permanece Cerrado

La puerta estará cerrada y bloqueada. Ninguna persona puede acceder a la puerta aunque tenga las credenciales autorizadas, excepto los Super Usuarios.

Captura

Capturar una imagen manualmente.

Nota

*El botón de **Captura** está disponible cuando el dispositivo soporta la función de captura. La imagen es guardada en el PC en el que se encuentra el software. Para configurar la ruta para guardar archivos, ver **Establacer una ruta para guardar archivos**.*

Resultado

El icono de las puertas cambiará en tiempo real acorde a la operación.

7.6.2 Estado de Control del Ascensor

Se puede controlar el estado del ascensor del controlador del ascensor, incluyendo la apertura de la puerta del ascensor, etc.

Pasos

Nota

El ascensor no puede ser controlado por otro el software si estado del ascensor cambia.

1. Hacer click en **Monitorización** para entrar en la página del estado de monitorización.

2. Seleccionar un Punto de Acceso en la esquina superior derecha.

> ***Nota***
>
> *Para manejar el punto de acceso, ver **Administración del Grupo**.*

3. Hacer click en el icono de la puerta para seleccionar un ascensor.
4. Hacer click en los siguientes botones para controlar el ascensor.

Puerta Abierta

Cuando la puerta del ascensor está cerrada. Después de un tiempo de apertura determinado la puerta se cerrará automáticamente.

Controlado

Debería pasar la tarjeta antes de presionar el botón de la planta y el ascensor se dirigirá a esa planta.

Libre

Será válido cualquier botón seleccionado del ascensor durante todo el tiempo.

Deshabilitado

El botón de la planta seleccionado en el ascensor será inválido y no se podrá ir a esa planta.

Resultado

El icono de las puertas cambiará en tiempo real acorde a la operación si la operación es satisfactoria.

7.6.3 Comprobación de los grabados en tiempo real

Las grabaciones serán mostradas en tiempo real, incluyendo el registro de los desplazamientos de la tarjeta, registro de reconocimientos faciales, etc. Se puede ver la información personal y ver las imágenes capturadas durante el acceso.

Pasos

1. Hacer click en **Monitorización** y seleccionar un grupo desde la lista desplegable en la esquina superior derecha.
   Los registros de acceso activados en las puertas del grupo seleccionados se mostrarán en tiempo real. Se pueden ver los detalles de los registros, incluidos el número de tarjeta, el nombre de la persona, la organización, hora del evento etc.
2. Opcional: Comprobar el tipo de evento y el estado de los eventos. Los eventos de tipo o estado no marcados no se mostrarán en la lista.
3. Opcional: Comprobar **Mostrar el último evento**.
4. Opcional: Hacer click en el evento y ver los detalles de la persona que ha accedido, incluyendo fotografías, número de persona, nombre de la persona, organización, teléfono, dirección de contacto, etc.

Nota

Se puede hacer doble click en la imagen capturadas para ampliarla y verla en detalles.

5. Opcional: hacer click con el botón derecho en la columna del nombre del evento para mostrar la columna escondida.

Capítulo 8 Tiempo y Asistencia

El módulo de Tiempo y Asistencia proporciona múltiples para realizar un seguimiento y monitorizar cuando empiezan y acaban los empleados su trabajo, y el control total de las horas de trabajo de los empleados, como llegadas tardías, salidas anticipadas, interrupciones y ausentismo.

Nota

En esta sección se introduce las configuraciones antes de obtener informes de asistencia. El acceso a los informes grabados después de estas configuraciones será calculado.

8.1 Configurar Parámetros de Asistencia

Configurar los Parámetros de asistencia, incluyendo la regla general, including the regla general, parámetros de tiempo extra, punto de asistencia, vacaciones, etc.

8.1.1 Configurar Regla general

Se puede configurar el cálculo de asistencia, como el inicio de la semana, el inicio del mes, fin de semana, ausencia, etc.

Pasos

Nota

Los Parámetros Configurados aquí serán ajustados por defecto para los nuevos períodos de tiempo añadidos. No afectará a los asistentes.

1. Entrar en el módulo Tiempo & Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Regla general**.
3. Configurar los días de inicio la semana e inicio de mes.
4. Seleccionar el día/s como fin de semana.
5. Set Parámetros de Ausencia.
6. Hacer click en **Guardar**.

8.1.2 Configurar Tiempo extra Parámetros

Se pueden configurar los parámetros de tiempo extra por día de trabajo y fin se semana, incluyendo nivel de tiempo extra, tarifa de hora de trabajo, horas extras, etc.

Pasos

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Horas Extras**.
3. Establacer la información requerida.

Nivel de Tiempo extra por día de trabajo

Cuando se trabaja durante cierto período después de acabar la jornada laboral se alcanzarán diferentes niveles de tiempo extra: tiempo extra 1, tiempo extra 2, tiempo extra 3. Se pueden ajustar diferentes tarifas de horas de trabajo para los tres tiempos extras relativamente.

Tarifas de horas de trabajo

Configurar las correspondientes tarifas de horas de trabajos durante tres niveles de tiempo extra, los cuales son generalmente usados para calculary el número total de horas trabajadas.

Tiempo extra durante el Fin de semana

Se puede habilitar el tiempo extra durante el fin de semana y configurar el modo de cálculo.

4. Hacer click en **Guardar**.

8.1.3 Configurar Asistencia en el Punto de Control

Se puede configurar desde un punto de accesos la asistencia/s de un punto de control, así la autenticación en el lector de tarjetas será guardada por Asistencia.

Antes de empezar

Se debe Añadir Dispositivo de Control de Accesos antes de configurar el punto de control de asistencia. Para más detalles, ver ***Añadir Dispositivo***.

Pasos

Nota

Por defecto, el lector de tarjetas del Dispositivo de Control de Accesos añadido es configurado como punto de control de asistencia.

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Punto de Control de Asistencia** para entrar en la página de configuración del Punto de Control de Asistencia.
3. Opcional: Configurar el botón de apagar **Configuración de Lector de tarjetas como punto de control**.
   Solo el lector de tarjetas será configurado como el Punto de Control de Asistencias.
4. Comprobar el lector de tarjeta deseado en la lista del dispositivo como Punto de Control de Asistencia(s).
5. Configurar la función punto de control como **Comienzo/ Fin jornada laboral**, **Empezar a Trabajar** o **Terminar de Trabajar**.
6. Hacer click en **Configurar como Punto de control**.
   El Punto de Control de Asistencia se muestra en la lista de la derecha.

8.1.4 Configurar Vacaciones

Se pueden añadir las vacaciones para no registrar la entrada ni la salida.

Añadir Vacaciones Regulares

Se pueden configurar las vacaciones que tendrán efecto anualmente durante un periodo efectivo como Año Nuevo, Navidad, etc.

Pasos

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Vacaciones** para entrar en la página de configuración de vacaciones.
3. Comprobar **Vacaciones Regulares** como vacaciones.
4. Personalizar un Nombre para las vacaciones.
5. Configurar el primer día de vacaciones.
6. Entrar en el número de días de vacaciones.
7. Configurar el estado de la asistencias si los empleados están de vacaciones.
8. Opcional: Comprobar **Repetir Anualmente** para hacer efectiva la configuración de las vacaciones cada año.
9. Hacer click en **OK**.
   Las vacaciones añadidas se mostrarán en la lista de vacaciones y en el Calendario.
   Si la Fecha es selecionada como diferentes vacaciones, se grabarán las vacaciones que han sido grabadas las primeras.
10. Opcional: Después de añadir las vacaciones, realizar una de las siguientes operaciones.

Editar Vacaciones	Hacer click en  para editar la información de las vacaciones.
Eliminar Vacaciones	Seleccionar una o más de las vacaciones añadidas y hacer click en **Borrar** para eliminar las vacaciones de la lista.

Añadir Vacaciones Irregulares

Se puede configurar vacaciones que tendrán efecto anualmente o son días irregulares como permiso para poder ir a un lugar de forma puntual.

Pasos

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Vacaciones** para entrar a la página de ajuste de vacaciones.
3. Hacer click en **Añadir** para abrir la página de las vacaciones.
4. Comprobar que las **Vacaciones Irregulares** están así configuradas.
5. Personalizar un nombre para las vacaciones.
6. Configurar la Fecha de inicio de las vacaciones.

Ejemplo

Si se quiere configurar el Jueves 1 de Noviembre de 2019 como vacaciones por el día de Todos los Santos se debe seleccionar en la lista desplegable.

7. Introducir el número de días de vacaciones.
8. Ajustar el estado de las vacaciones de cada empleados.
9. Opcional: Comprobar la **Repetición Anual** para hacer la configuración de estas vacaciones efectiva cada año.
10. Hacer click en **OK**.
    Las vacaciones serán mostradas en la lista de vacaciones y en el Calendario.
11. Opcional: después de añadir las vacaciones, realizar una de las siguientes operaciones.

Editar Vacaciones	Hacer click en para editar la información de las vacaciones.
Eliminar Vacaciones	Seleccionar una o más de las vacaciones añadidas y hacer click en **Borrar** para borrar las vacaciones de la lista de vacaciones.

8.1.5 Configurar los tipos de ausencia

Se puede personalizar los tipos de ausencias acorde con las necesidades actuales. También se pueden editar.

Pasos

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Tipo de ausencias** para entrar en la página de configuración de Tipo de ausencias.
3. Hacer click en **Añadir** en la izquierda para añadir el tipo de ausencias principal.
4. Opcional: Realizar una de las siguientes operaciones para el tipo de ausencias principales.

Editar	Mover el cursor sobre el tipo de ausencias principales and Hacer click en para editar el tipo de ausencias principales.
Eliminar	Seleccionar un tipo de ausencia principal y hacer click en **Borrar** en la izquierda para borrar el tipo de ausencia principal.

5. Hacer click **Añadir** en la derecha para Añadir un tipo de ausencias menor.
6. Opcional: Realizar unas de las siguientes operaciones para un tipo de ausencia menor.

Editar	Mover el cursor sobre el tipo de ausencia menor y hacer click en para editarlo.
Eliminar	Seleccionar una o múltiples ausencias principales y hacer click en **Borrar** en la derecha para Eliminar el tipo de ausencia menor que ha sido seleccionado.

8.1.6 Sincronización con base de datos de terceros

El dato de Asistencia grabado en el software puede ser usado por otro sistema para calcular algunas operaciones. Se puede habilitar la función de Sincronización para aplicar la autenticación de grabado desde el software a la base de datos de terceros automáticamente.

Pasos

1. Entrar en el Módulo de Tiempo y Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Base de datos de terceros**.
3. Configurar **Aplicar a base de datos** y encender para habilitar la función de sincronización.
4. Configurar los parámetros requeridos de la Base de datos de terceros, incluyendo tipo de base de datos, dirección IP, nombre de la base de datos, nombre de usuario y contraseña.
5. Configurar la tabla de los parámetros de la base de datos acorde con la configuración actual.
   1) Introducir el nombre de la tabla en la base de datos.
   2) Establacer los campos de la tabla entre el cliente y la base de datos.
6. Hacer click en **Prueba de Conexión** para probar si la base de datos puede ser conectada.
7. Hacer click en **Guardar** para probar si la base de datos se puede conectar y guardar la configuración para una conexión exitosa.

8.1.7 Configurar el Tiempo de Descanso

Se puede añadir un tiempo de descanso y configurar el tiempo de inicio, tiempo de fin, duración y otros parámetros. El tiempo de Descanso añadido puede ser editado o borrado.

Pasos

1. Hacer click en **Tiempo & Asistencia** → **Horario**.
   Los horarios añadidos serán mostrados en la lista.
2. Seleccionar un Horario añadido o hacer click en **Añadir** para entrar en la página de configuración del Horario.
3. Hacer click en **Ajustes** en el área del tiempo de Descanso para entrar en la página de gestión del tiempo de Descanso.
4. Añadir tiempo de descanso.
   1) Hacer click en **Añadir**.
   2) Introducir un nombre para el tiempo de Descanso.
   3) Configurar los parámetros relacionados con el tiempo de Descanso.

Tiempo de inicio / Tiempo de Fin

Configurar la hora de inicio y fin del descanso.

No Antes de / No más tarde de

Configurar el tiempo más temprano de registro para el comienzo del Descanso y el tiempo más tarde de registro para finalizar el Descanso.

Duración del Descanso

El tiempo de inicio y fin del Descanso.

Deducción automática

La duracción del Descanso quedará excluida del Horario laboral sin necesidad de que el usuario fiche.

Debe Registrarse

La duración del Descanso se calculará y se excluirá de las horas de trabajo de acuerdo con el Horario real de entrada y salida.

Nota

*Si se selecciona **debe registrarse** como método de cálculo, es necesario configurar los estados de asistencia antes y después de que finalice el descanso.*

5. Hacer click en **Guardar** para Guardar la configuración.
6. Opcional: Hacer click en **Añadir** para continuar con el tiempo de Descanso.

8.1.8 Configurar Mostrar informe

Se puede configurar el contenido de la pantalla que se muestra en el informe de Asistencia, tal y como el nombre de la empresa,, el formato de fecha, el formato de hora y la marca.

Pasos

1. Introducir el Módulo de Tiempo y Asistencia.
2. Hacer click en **Estadística de Asistencia** → **Visualización del Informe**.
3. Configurar el display de ajustes para el Informe de Asistencia.

Nombre de la Compañía

Introducir el nombre de la compañía en el informe.

Formato de Fecha / Formato de Tiempo

Configurar los formatos de Fecha y tiempo acorde con las necesidades actuales.

Asistencia de marca de estado en el registro

Introducir la marca y seleccionar el color. Los campos relacionados con el estado de asistencia se muestra en el informe con la marca y el color.

Fin de semana en el registro

Introducir la marca y seleccionar el color. Los campos de fin de semana en el registro serán mostrados con la marca y el color seleccionados.

4. Hacer click en **Guardar**.

8.2 Añadir Horario

Se puede añadir el Horario para realizar diferentes turnos de trabajo.

Pasos

1. Hacer click en **Tiempo & Asistencia** → **Horario** para entrar en la Ventana de ajustes de Horario.

2. Hacer click en **Añadir** para entrar en la página de añadir Horario.
3. Crear un nombre para el Horario.
4. Seleccionar un método de cálculo.

   Primera entrada y última salida

   La hora de la primera entrada se guarda como el inicio del trabajo y la última salida como el fin de la jornada laboral.

   Cada entrada/ salida

   Cada hora de salida o entrada es válida y la suma de todas ellas se guardan como la duración de la jornada laboral.

   Es necesario configurar el **Intervalo válido de autenticación** para realizar el cálculo. Por ejemplo, si el intervalo entre el deslizamiento de la misma tarjeta es menor que el valor establecido, el deslizamiento de la tarjeta no es válido.
5. Opcional: Configurar el inicio de **Habilitar el estado T&A** para conocer el estado de asistencia del dispositivo.
6. Establecer el tiempo de asistencia.

   Inicio y fin de la jornada laboral

   Configurar la hora de inicio y fin de la jornada laboral.

   Validar la hora de entrada y salida

   Establecer el período de tiempo válido de entrada y salida.

   Calculado como

   Establecer la duración del tiempo real de trabajo.

   Permiso tardío / temprano permitido

   Establecer el período de tiempo para poder salir más tarde o más temprano.
7. Opcional: Seleccionar el tiempo de Descanso excluído de la duración de las horas de trabajo.

Nota

*Se puede hacer click en **Ajustes** para administrar el tiempo de Descanso. Para más detalles sobre la configuración del tiempo de Descanso, ver **Configurar Tiempo de descanso**.*

8. Hacer click en **Guardar** para añadir el Horario.
9. Opcional: Realizar alguna de las siguientes operaciones después de añadir el Horario.

Editar Horario	Seleccionar un Horario desde la lista para editar la información relacionada.
Borrar Horario	Seleccionar un Horario desde la lista y hacer click en **Borrar** para borrarlo.

8.3 Añadir Turno

Se puede añadir el turno para realizar el Horario.

Antes de empezar

Añadir un Horario primero. Ver ***Añadir Horario*** para más detalles.

Pasos

1. Hacer click en **Tiempo & Asistencia** → **Turno** para entrar en la página de ajuste de Turno.
2. Hacer click en **Añadir** para entrar en la página de Añadir Turno.
3. Introducir un nombre para el turno.
4. Seleccionar el turno en la lista desplegable.
5. Seleccionar el Horario añadido y hacer click en la barra de tiempo para aplicar el Horario.

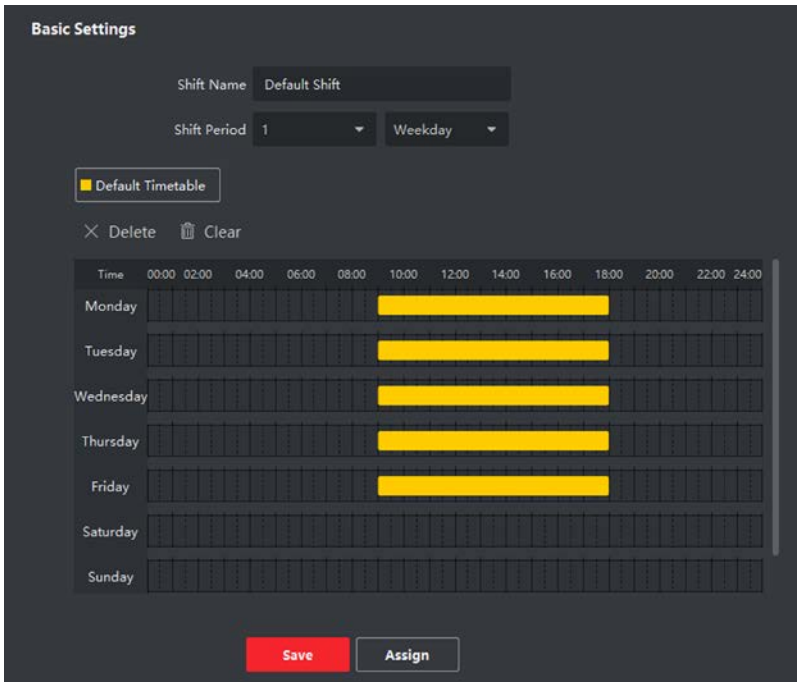

Figure 8-1 Añadir Turno

6. Hacer click en **Guardar**.

La lista de los turnos añadidos se muestra en la parte izquierda. Como máximo se pueden añadir 64 turnos.

7. Opcional: Asignar el turno a la organización o persona.
   1) Hacer click en **Asignar**.
   2) Seleccionar la pestaña de **Organización** o **Persona** y marca la casilla de las organizaciones o personas deseadas.
      Las organizaciones y personas seleccionadas se mostrarán en la página de la derecha.
   3) Configurar el período efectivo para el Calendario de turno.
   4) Configurar otros parámetros para el Calendario de turnos, incluyendo entrada y salida no requeridas, vacaciones o tiempo extra.
   5) Hacer click en **Guardar** para guardar rápidamente el Calendario de turno.

8.4 Manejo del Calendario de turno

El turno de trabajo es una práctica laboral para utilizar las 24 horas del día todos los días de la semana. La práctica habitual es establecer períodos de tiempo realizando diferentes turnos.
Se puede Configurar el Calendario de departamento, calendario Personal, y Calendario Temporal.

8.4.1 Configurar el Calendario departamento

Se puede Configurar el Calendario de turnos para un departamento y todas las personas del mismo.

Antes de empezar

En el Módulo de Tiempo y Asistencia, la lista de departamentos es la misma. Se debe añadir la organización y personas en el módulo de usuario. Ver ***Gestión Personal*** para más detalles.

Pasos

1. Hacer click en **Tiempo & Asistencia** → **Calendario de Turno** para entrar en el manejo del Calendario de turno.
2. Hacer click en **Horario de Departamento** para entrar en la página de Horario de departamento.
3. Seleccionar el departamento desde la lista de organización de la izquierda.

Nota

*Si se marca **Incluir suborganización**, cuando se selecciona la organización, sus suborganizaciones se seleccionan al mismo tiempo.*

4. Seleccionar el turno de la lista desplegable.
5. Marcar la casilla de verificación para habilitar los **Horarios de Turno Múltiple**.

Nota

*Después de seleccionar **Múltiples turnos en el Calendario**, se puede seleccionar el tiempo de periodo efectivo procedentes de los períodos de tiempo añadidos por las personas en el departamento.*

Múltiple Planificación de Turno

Contiene más de un turno. La persona debe marcar la entrada/salida en algunos de esos períodos de asistencia efectivo.
Si la planificación de turno múltiple contiene 3 horarios: 00:00 a 07:00, 08:00 a 15:00 y 16:00 a 23:00. El periodo de asistencia de la persona se hará efectivo en uno de los tres turnos configurados. Si la persona realiza un fichaje a las 07:50, se aplicará el turno más cercano, de 08:00 to 15:00 para el cálculo de asistencia de esa persona.

6. Configurar el tiempo de inicio y fin.
7. Configurar otros parámetros del Calendario, incluyendo entrada o salida no requerida, vacaciones o tiempo extra.
8. Hacer click en **Guardar**.

8.4.2 Establacer el Horario de la persona

Se puede asignar la planificación a una o más personas. Se puede también ver y editar los detalles del Horario.

Antes de empezar

Añadir la persona y departamento en el módulo de persona. Ver ***Gestión Personal*** para más detalles.

Pasos

Nota

El Calendario personal tiene mayor prioridad que el Calendario del departamento.

1. Hacer click en **Tiempo & Asistencia** → Planifiación de **Turno** para entrar en la pagína de configuración de la planificación.
2. Hacer click en **Calendario Personal** para entrar en la página de Calendario Personal.
3. Seleccionar la organización y la persona (s).
4. Seleccionar el turno desde la lista desplegable.
5. Marca la casilla para habilitar la **Planificación de Turnos Múltiples.**

Nota

*Después de seleccionar **Múltiples turnos en el Calendario**, se puede seleccionar el tiempo de periodo efectivo procedentes de los períodos de tiempo añadidos por las personas en el departamento.*

Múltiple Planificación de Turno

Contiene más de un turno. La persona debe marcar la entrada/salida en algunos de esos períodos de asistencia efectivo.
Si la planificación de turno múltiple contiene 3 horarios: 00:00 a 07:00, 08:00 a 15:00 y 16:00 a 23:00. El periodo de asistencia de la persona se hará efectivo en uno de los tres turnos configurados. Si la persona realiza un fichaje a las 07:50, se aplicará el turno más cercano, de 08:00 to 15:00 para el cálculo de asistencia de esa persona.

6. Configurar la Fecha de inicio y fin.
7. Configurar el resto de parámetros del Calendario, incluyendo entradas y salidas no requeridas, tiempo de vacaciones y tiempo extra.
8. Hacer click en **Guardar**.

8.4.3 Configurar el Calendario Temporal

Se puede añadir un Horario temporalmente para la persona que será asignado en el Calendario. También se puede ver y editar los detalles de los horarios temporales.

Antes de empezar

Añadir el departamento y la persona en el módulo de persona. Ver ***Gestión Personal*** para más detalles.

Pasos

Nota

El Calendario temporal tiene más prioridad que el Calendario del departamento o el personal.

1. Hacer click en **Tiempo & Asistencia** → **Calendario de Turnos** para entrar en la página de manejo de turnos.
2. Hacer click en **Calendario Temporal** para entrar en la página de Calendario Temporal.
3. Seleccionar la organización y seleccionar la persona.
4. Hacer click en una Fecha o hacer click y arrastrar varias fechas en el Calendario temporal.
5. Seleccionar **Jornada laboral** o **Jornada no laboral** desde la lista desplegable.

   Si se selecciona la **Jornada no laboral** se necesitan configurar los siguientes parámetros.

   Calcular como

   Seleccionar un tiempo normal o extra para marcar el estado de la asistencia en el Calendario temporal.

   Horario

   Seleccionar un Horario de la lista desplegable.

   Calendario de múltiples turnos

   Contiene más de un Horario. El usuario puede entrar o salir en cualquiera de ellos.
   Si la planificación de turno múltiple contiene 3 horarios: 00:00 a 07:00, 08:00 a 15:00 y 16:00 a 23:00. El periodo de asistencia de la persona se hará efectivo en uno de los tres turnos configurados. Si la persona realiza un fichaje a las 07:50, se aplicará el turno más cercano, de 08:00 to 15:00 para el cálculo de asistencia de esa persona.

   Reglas

   Configurar reglas para el Calendario como **Entrada No Requerida** y **Salida No Requerida**.
6. Hacer click en **Guardar**.

8.4.4 Comprobar el calendario de turnos

Se puede comprobar el turno en el Calendario. También se puede editar o borrar el Calendario de los turnos.

Pasos

1. Hacer click en **Tiempo & Asistencia** → **Planificación de turnos** para entrar en la página de manejo del Calendario.
2. Seleccionar la organización y la persona (s) correspondientes.
3. Hacer click en  o  para ver el turno en el Calendario o en la lista de modos.

   Calendario

   En el modo del Calendario se puede ver el turno para cada día del mes. Se puede hacer click en el Calendario temporar para editar o borrar un día.

Lista

En la lista se pueden ver los detalles de los turnos de cada persona u organización, tal y como el nombre, tipo, período efectivo. Comprobar el Calendario de turnos y hacer clic en **Borrar** para borrar el turno(s) seleccionados.

8.5 Registro correcto Manualmente Entrada/ Salida correcta Record

Nota

Se puede hacer click en ⊕ *para añadir múltiples elementos de entrada / salida. Como máximo se pueden admitir 8 elementos de entrada / salida.*

6. Opcional: Introducir la información que se desee observar.
7. Hacer click en **Guardar**.
8. Opcional: Realizar una de las siguientes operaciones.

Ver	Hacer click en ▦ o ☰ para ver el manejo de la información de la asistencia en el Calendario. ***Nota*** *En el modo de Calendario, se necesita hacer click en **Calcular** para obtener el estado de asistencia de la persona durante un mes.*
Editar	● En el modo de Calendario, hacer click en la etiqueta de Fecha para editar los detalles. ● En el modo de lista, hacer doble click en la columna Fecha, tipo de manejo, Hora u Observación para editar la información.
Borrar	Borrar los términos seleccionados.
Exportar	Exportar los detalles de asistencia al ordenador local. ***Nota*** *Los detalles guardados son exportados en formato CSV.*

8.6 Añadir Ausencias y Viajes de Negocio

Se puede añadir ausencias y Viajes de Negocio cuando el empleados los empleados las realicen.

Antes de empezar

Se debe añadir organizaciones y personas en el módulo de Usuario.

Pasos

1. Hacer click en **Tiempo & Asistencia** → **Manejo de asistencia** para entrar en la página de manejo de asistencia.
2. Hacer click en **Aplicar ausencia/Viajes de Negocio** para entrar en la página de ausencia/ viaje de negocios.
3. Seleccionar a la persona en la lista de la izquierda.
4. Configurar la Fecha de ausencia o Viajes de Negocio.
5. Seleccionar el mayor y menor tipo de ausencia en la lista desplegable.

Nota

*Se puede Configurar el tipo de ausencias en ajuste de asistencia. Para más detalles, ver **Configurar Tipo de ausencias**.*

6. Establacer el tiempo de ausencia.
7. Opcional: Introducir la información deseada.
8. Hacer click en **Guardar**.
9. Opcional: Después de añadir el fin del viaje, realizar las siguientes operaciones.

Ver	Hacer click en  o  para ver la información en los modos de Calendario o lista.
	Nota *En el modo de Calendario, se necesita hacer click en **Calcular** para obtener el estado de la persona en un mes.*
Editar	En el modo Calendario, hacer click en la etiqueta relacionada en la fecha para editar los detalles. El modo lista, hacer doble click en las columnas de Fecha, tipo de manejo, hora u Observación para editar la infomación relacionada.
Borrar	Borrar los términos seleccionados.
Exportar	Exportar los detalles de asistencia al ordenador local.
	Nota *Los detalles exportados son guardados en un formato CSV.*

8.7 Calcular Datos de Asistencia

Se necesita calcular los datos de asistencia antes de buscar y ver el resumen de los datos de asistencia, los datos de asistencia detallados de los empleados, el tiempo extra de trabajo, etc.

8.7.1 Calcular Automáticamente los Datos de Asistencia

Se puede Configurar el Calendario de datos de asistencia automáticamente.

Pasos

Nota

Calculará los datos de Asistencia hasta el día anterior.

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Ajustes de Asistencia** → **Regla general**.
3. En el apartado de cálculo automático de datos de asistencia, configurar la hora que se desea que el software calcule los datos cada día.
4. Hacer click en **Guardar**.

8.7.2 Manualmente Calcular Datos de Asistencia

Se puede calcular los datos de asistencia manualmente configurando el rango de datos.

Pasos

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Estadística de Asistencia** → **Calcular Asistencia**.
3. Configurar el tiempo de inicio y fin para definir el rango de datos de asistencia.
4. Configurar otras condiciones, incluyendo departamento, nombre de la persona, número de empleados y estado de la asistencia.
5. Hacer click en **Calcular**.

Nota

Solo se puede calcular los datos de asistencia en un plazo de 3 meses.

6. Realizar una de las un siguientes operaciones.

Entrada/ Salida correcta	Hacer click en **Entrada/ Salida correcta** para añadir una entrada/salida correcta.
Informe	Hacer click en **Informe** para general el informe de asistencia.
Exportar	Hacer click en **Exportar** para exportar los datos de asistencia al ordenador local. ***Nota*** *Los detalles exportados son guardados en formato CSV.*

8.8 Estadística de Asistencia

Se puede comprobar el informe de asistencia original, generar y exportar el informe de asistencia basado en los datos de asistencia.

8.8.1 Obtener el informe de asistencia original

Se puede buscar el tiempo de asistencia de los empleados, el estado de la asistencia, el punto de control, etc. en un período de tiempo para obtener un informe original de los empleados.

Antes de empezar

- Se deben añadir organizaciones y personas en el módulo de usuarios. Para más detalles, ver ***Gestión Personal***.
- Calcular los datos de asistencia.

Nota

- *El software calculará automáticamente el dato de asistencia desde la 1:00 am del día anterior al día siguiente.*
- *Si los datos de asistencia no se han calculado automáticamente se puede calcular manualmente. Para más detalles, ver **Calcular Manualmente los Datos de Asistencia**.*

Pasos

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Estadística de Asistencia** → **Informes Originales**.
3. Configurar el tiempo de inicio y fin para realizar la búsqueda.
4. Configurar otras condiciones de búsqueda, como departamento, nombre de persona y número de empleados.
5. Opcional: Hacer click en **Obtener del Dispositivo** para extraer los datos desde el dispositivo.
6. Opcional: Hacer click en **Reset** para resetear todas las condiciones de búsqueda y editar las condiciones de búsqueda de nuevo.
7. Hacer click en **Buscar**.
   El resultado se muestra en la página. Se puede ver el estado de la asistencia y el punto de control.
8. Opcional: después de buscar el resultado, realizar una o varias de las siguientes operaciones.

Generar Informe	Hacer click en **Informe** para generar para generar el informe de asistencia.
Exportar Informe	Hacer click en **Exportar** para exportar los resultados al ordenador local.

8.8.2 Generar un informe instantáneo

Soporta la generación de una serie de Informes de Asistencias manualmente para ver los resultados

de Asistencia de los empleados.

Antes de empezar

Calculate los datos de asistencia.

Nota

*Se puede calcular los datos de Asistencia manualmente, o configurar el Calendario así como que el software pueda calcular los datos automáticamente cada día. Para más detalles, ver **Calcular Datos de Asistencia**.*

Pasos

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Estadística de Asistencia** → **Informe**.
3. Seleccionar un tipo de informe.
4. Seleccionar el departamento o la persona para ver el informe de asistencia.
5. Configurar el tiempo de inicio y fin de los datos de asistencia que serán mostrados en el informe.
6. Hacer click en **Informe** para generar la estadística del informe y abrirlo.

8.8.3 Informe Personalizado de Asistencia

El software soporta múltiples tipos de informe y se puede predefinir el contenido del informe y enviarlo automáticamente.

Pasos

Nota

*Configurar los parámetros del email antes de habilitar las funciones del Envío Automático de Email. Para más detalles, ver **Configurar los Parámetros de Email**.*

1. Entrar en el módulo de Tiempo y Asistencia.
2. Hacer click en **Estadística de Asistencia** → **Informe Personalizado**.
3. Hacer click en **Añadir** para predefinir un informe.
4. Configurar el contenido del informe.

   Nombre del informe

   Introducir el nombre para el informe.

   Tipo de informe

   Seleccionar el tipo de informe y se generará.

   Hora del informe

   El Tiempo de selección puede variar en función del tipo de informe.

   Usuario

   Seleccionar la persona (s) añadidas cuyas grabaciones se generaran para el informe.
5. Opcional: Configurar el Calendario y enviar el informe a la dirección del email automáticamente.
   1) Comprobar el **Envío Automático de Email** para habilitar esta función.

2) Establacer el período efectivo durante el cual el software enviará el Informe en las fechas de envío Seleccionadas.
3) Seleccionar la Fecha (s) en la que el software enviará el informe.
4) Configurar la hora en la que el software enviará el informe.

Ejemplo

*Si se configura el período efectivo del **10/3/2018 al 10/4/2018**, Seleccionar **Viernes** como la Fecha de envío a las **20:00:00**, el software enviará el informe todos los Viernes a las 8 p.m. desde el 10/3/2018 al 10/4/2018.*

Nota

*Asegurarse de que los registros de asistencia se calculan antes de la hora de envío. Se puede calcular los datos de asistencia manualmente o establacer el Horario para que el software pueda calcular los datos automáticamente todos los días. Para más detalles **Calcular Datos de Asistencia.***

5) Introducir la dirección del email.

Nota

*Hacer click en **+** para añadir una nueva dirección de email. Se permiten hasta 5 direcciones de email.*

6) Opcional: Hacer click en **Preview** para ver los detalles del email.

6. Hacer click en **OK**.
7. Opcional: después de añadir el informe personalizado, se puede realizar una o más de las siguientes acciones:

Editar Informe	Seleccionar un informe añadido y hacer click en **Editar** para editar sus Ajustes.
Borrar Informe	Seleccionar un informe y hacer click en **Borrar** para borrarlo.
Generar Informe	Seleccionar un informe añadido y hacer click en **Informe** para generar el informe instantáneamente. Se pueden ver los detalles del informe.

Capítulo 9 Video Portero

Video portero es un sistema de comunicación usado dentro de un edificio o un pequeño grupo de edificios. Con micrófonos y cámara de video en ambos lados, habilitando la comunicación visual o auditiva. Un sistema de videoportero puede proporcionar una solución de monitoreo seguro y fácil para edificios de apartamentos y casas privadas.
Asegurarse de agregar los video porteros al software y vincular las estaciones interiors con los usuarios de antemano. También se debe establecer la autorización de acceso para que las personas abran puertas a través de las estaciones interiores vinculadas.

Nota

Se puede gestionar con el software hasta 16 Puertas de estaciones y 512 estaciones interiores. Para obtener más información sobre como añadir video porteros, ser ***Añadir Dispositivo****.*
Para obtener más información acerca de agregar personas, consultar ***Añadir un usuario.***
Para obtener detalles sobre la configuración de la autorización de acceso de la persona, consultar ***Establacer grupo de acceso para asignar la autorización de acceso a persona.***

9.1 Manejo de llamada entre el software y una puerta/Estación de Puerta/Dispositivo de Control de accesos.

Se puede llamar a los residentes mediante el software y viceversa. También se puede usar una estación interior, exterior o un dispositivo de control de accesos para llamar al software. Antes de hacer llamadas, se pueden configurar los parámetros como la duración del timbre y la duracción de la conversación. Para más detalles referirse a ***Configurar los parámetros de Control de Accesos y Video porteros***.

9.1.1 Llamar desde el Monitor Interior al software

Se puede llamar mediante el software del video portero.

Antes de empezar

- Estar Seguro de añadir una residencia al software. Para más detalles, ver ***Añadir un Usuario.***
- Asegurarse de haber vinculado el residente con un Monitor Interior y configurar la información del residente (incluyendo número de piso y número de habitación) en el módulo de usuario. Para obtener más detalles sobre la configuración del enlace y la información del residente, consultar ***Configurar Información del Residente.***

Pasos

Nota

Un dispositivo video portero puede ser añadido a más de un software, pero solo uno al mismo tiempo. Se puede configurar remotamente la duración máxima de llamada y de comunicación.

1. Hacer click en **Control de accesos** → **Video portero** → **Contactos**.
2. Desplegar la lista de organizaciones en el panel izquierdo y seleccione una organización. La información (incluido Nombre de Residente, nombre vinculado al dispositivo, dirección IP) de la llamada de los residentes en el grupo seleccionado que será mostrado en el panel derecho.
3. Seleccionar un residente, o introducir una contraseña en el campo Filtro para encontrar al residente deseado.
4. Hacer click en para empezar la llamada.

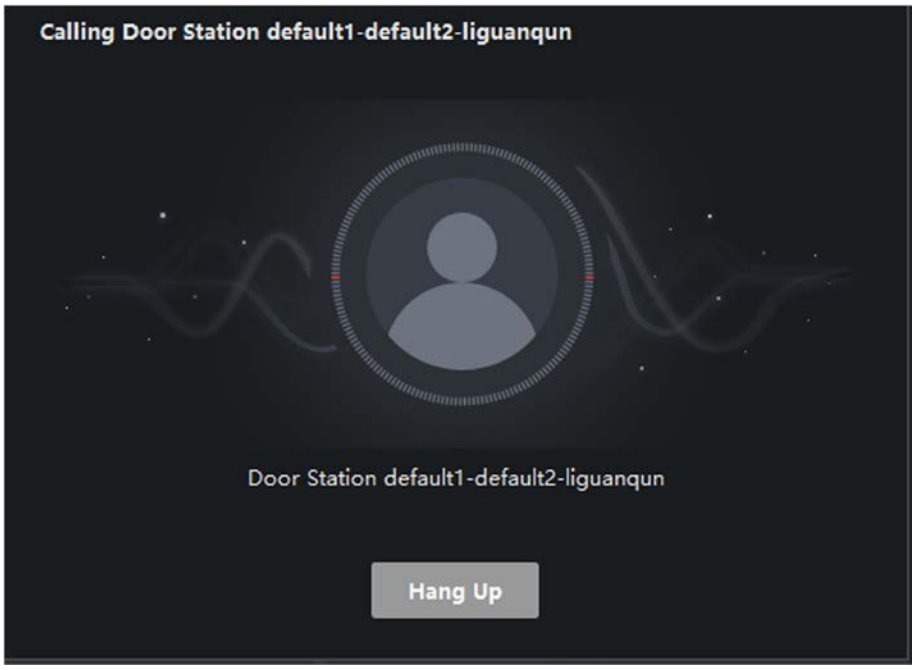

Figure 9-1 Start CTodoing Window

Después de que la llamada sea contestada, se entrará en la Ventana de llamada entrante.

5. Opcional: Después de que la llamada sea contestada, realizar las siguientes operaciones.

Ajustar el volumen del altavoz	Hacer click en para ajustar el volumen del altavoz.
Acabar la llamada	Hacer click en **Colgar** para acabar la llamada.
Ajustar Volumen del Micrófono	Hacer click en para ajustar el volumen del micrófono.

9.1.2 Responder la llamada Via Software

Los residentes pueden llamar mediante un Monitor Interior, una Puerta, o un dispositivo específico de control de accesos y un video portero con el software.

Antes de empezar

- Asegurarse de haber agregado un residente al Sofware. Para más detalles ver ***Añadir un usuario***.
- Asegurarse de haber vinculado al residente añadido con un Monitor Interior/ Puerta o dispositivo de control de accesos y configurar la información del residente (incluyendo planta y piso) en el módulo persona. Para obtener más detalles sobre la configuracón del enlace y la información del residente, consultar ***Configurar Información del Residente.***

Pasos

Nota

- *Un dispositivo video portero puede ser añadido a más de un software, pero solo uno al mismo tiempo.*
- *Se puede configurar remotamente la duración máxima de llamada.*

1. Hacer click en **Control de accesos** → **Video portero** → **Contactos**.
2. Desplegar la lista de organizaciones en el panel izquierdo y seleccione una organización. La información (incluido Nombre de Residente, nombre vinculado al dispositivo, dirección IP) de la llamada de los residentes en el grupo seleccionado que será mostrado en el panel derecho.
3. Hacer click en para empezar la llamada al residente deseado.
   Una Ventana de llamada entrante se abrirá.

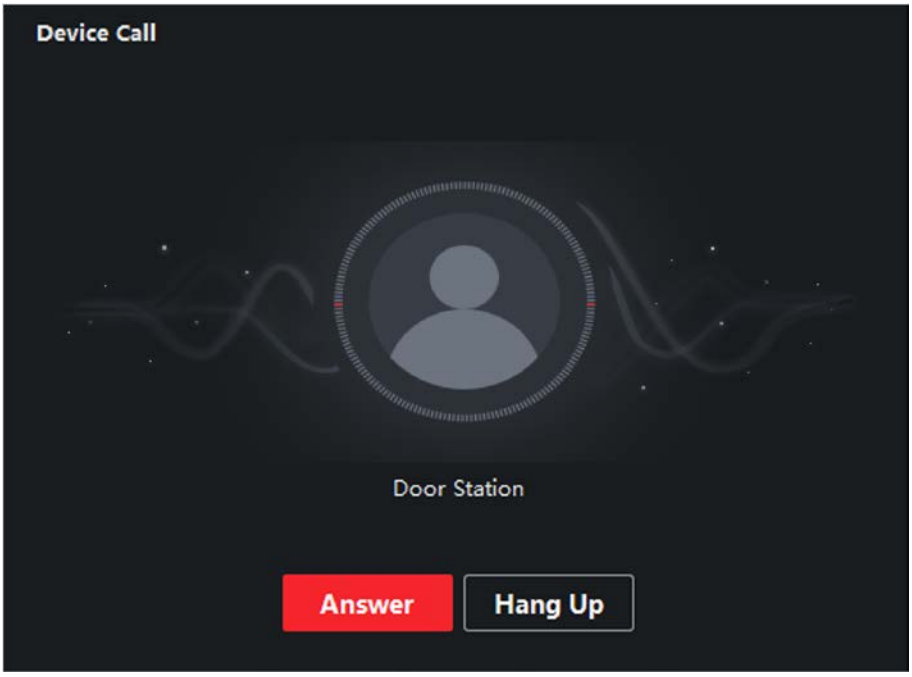

Figure 9-2 Llamada de entrada

4. Hacer click en **Responder** para responder a la llamada.
   Después de ser la llamada contestada, se introducirá en la Ventana de llamada entrante.
5. Opcional: En la Ventana de llamada entrante, realizar las siguientes operaciones.

Ajustar el volumen del altavoz	Hacer click en para ajustar el volumen del altavoz.
Terminar de hablar	Hacer click en **Colgar** para terminar de hablar.
Ajustar volumen del micrófono	Hacer click en para ajustar el volumen del micrófono.
Puerta Abierta	Cuando un Monitor Interior está lincado a una Puerta, hacer click en para abrir la Puerta lincada.

9.2 Visualización del Registro de llamadas en tiempo real.

Se puede ver los detalles de todas las llamadas y se puede llamar a los residentes o exportar los registros si son necesarios.

Pasos

1. Hacer click en **Control de accesos** → **Video portero** → **Registro de llamadas.**
   Los detalles de todas las llamadas se mostrarán en el panel de la derecho, incluido el estado de la llamada, la hora de inicio, la duración de la conversación, el tipo y nombre del dispositivo, la organización y el nombre del residente.
2. Opcional: Hacer click en para Volver a marcar al residente.
3. Opcional: Establacer las condiciones de búsqueda (incluyendo el estado de llamada, el tipo de dispositivo y la hora) en la parte superior de la página para filtrar los registros de llamadas.
4. Hacer click en **Exportar** para guardar los registros (un archivo CSV) en el ordenador personal.

9.3 Comunicar un aviso al residente

Se puede enviar un aviso a los residentes con un solo toque. Hay cuatro tipos de avisos disponibles: publicidad, información de propiedades, alarmas y avisos.

Pasos

1. Hacer click en **Control de accesos** → **Video portero** → **Aviso**
2. Hacer click en **Añadir** para abrir el panel Crear Aviso.
3. Hacer click en para Seleccionar los residentes a los que se les va a enviar la notificación.
4. Introducir la información requerida.

Nota

Se admiten hasta 63 caracteres en el campo Subject.
Se admiten hasta 1023 caracteres en el campo Content.

Se puede añadir hasta 6 imágenes. Cada imagen debería Estar en formato JPG y menor de 512 KB.

5. Hacer click en **Enviar** para enviar el aviso de los residentes seleccionados.
   La información sobre los avisos enviados se mostrará en el panel de la izquierda. Hacer click en el aviso para ver más detalles.
6. Opcional: Hacer click en **Exportar** para guardar todos los avisos en el ordenador personal.

Capítulo 10 Búsqueda de Registros

Se proporcionan dos tipos de registros: registro de operación y registro de sistema. Los registros de operaciones se refieren a las operaciones normales que el usuario realizó en el software como añadir dispositivo, registro de búsqueda, y reseteo de contraseña; y los registros del sistema registran la información del sistema, como el inicio de sesión, el cierre de session, bloqueo y desbloqueo. Puede buscar en los archivos de registro y ver los detalles del registro incluyendo tiempo, usuario, etc.

Pasos

1. Entrar en el módulo Registro del Sistema.
2. Hacer click en para especificar la hora de comienzo y de fin.

Nota

Se pueden buscar los registros de un mes.

3. Seleccionar un usuario para buscar los archivos de registro que son generados cuando el usuario se registra en el software.
4. Seleccionar **Registro de operaciones** o **Registro del sistema** como tipo de registro.
5. Hacer click en **Buscar**.
   Los archivos de registro entre la hora de inicio y la hora de finalización se mostrarán en la lista. Se puede comprobar el tiempo de operación, el tipo y otra información de los registros.
6. Opcional: Realizar una de las siguientes operaciones.

Filer	Hacer click en en el encabezado y seleccionar los registro de filtro.
Ordenar	Hacer click en el encabezado para ordenar los registros por tiempo o secuencia de letras.
Backup	Hacer click en **Backup Log** para hacer una copia de seguridad la búsqueda en el ordenador local.

Nota

Se pueden ver los registros en archivos importados o exportados. Para más informacion, ver ***Operación y Mantenimiento.***

Capítulo 11 Gestión de Usuario

Para mejorar la seguridad del sistema, el administrador debe crear una cuenta diferente para cada usuario y asignar permisos diferentes al usuario. Para evitar que diferentes usuarios compartan la misma cuenta se recomienda administrar las cuentas de usuario periodicamente.

11.1 Añadir Usuario

El Super Usuario y el administrador pueden añadir nuevos usuarios y asignar permisos diferentes para los diferentes usuarios si es necesario.

Realizar esta tarea para añadir una cuenta de usuario.

Pasos

Nota

La cuenta de usuario que se registró para iniciar session en el software se configura como Super Usuario.

1. Entrar en el módulo de Gestión de Usuarios.
2. Hacer click en **Añadir Usuario** para mostrar el área de la información.
3. Seleccionar el tipo de usuario en la lista desplegable.

   Administrador

   La cuenta de administrador tiene por defecto todos los permisos, y se pueden modificar las contraseñas y permisos de todos los operadores.

   Operador

   Por defecto la cuenta del operador no tiene permisos y se pueden asignar los permisos periódicamente. Un operador solo puede cambiar las contraseñas si las cuentas han sido añadidas.
4. Introducir el nombre de usuario, y confirmar la contraseña deseada.

Atención

La fiabilidad de la contraseña del dispositivo se puede comprobar automáticamente. Se recomienda cambiar la contraseña predefinida (con un mínimo de 8 caracteres Incluyendo letras mayúsculas y minúsculas, números y carácteres especiales) para aumentar la seguridad del producto. Se recomienda resetear la contraseña regularmente, especialmente en el sistema de alta seguridad, debido a que resetear la contraseña seminal o mensualmente protege mejor el producto.
La correcta configuración de las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.

5. Marcar las Casillas de verificación para asignar los permisos al usuario creado.
6. Opcional: Hacer click en **Valor por defecto** para restaurar los permisos predeterminados de este usuario.
7. Hacer click en **Guardar**.

Nota

Hasta 50 cuentas de usuario pueden ser añadidas al software.

Después de crear la cuenta de usuario correctamente, la cuenta de usuario se agrega a la lista de usuarios en la página de administración de cuentas.

8. Opcional: Realizar las siguientes operaciones después de crear la cuenta del usuario.

Editar Usuario	Hacer click en un usuario desde la lista para editar la información del usuario.
	Nota *Solo la contraseña Super Usuario puede ser editada.*
Eliminar Usuario	Seleccionar el usuario desde la lista y hacer click en **Eliminar Usuario**.
	Nota *El Super Usuario no puede ser eliminado.*

11.2 Cambiar la Contraseña del Usuario

El administrador puede cambiar la contraseña normal del usuario sin ingresar la contraseña anterior, mientras que el administrador debe ingresar la contraseña antigua al cambiar la contraseña.

Antes de empezar

Añadir usuario al software.

Pasos

1. Entrar en el módulo de Gestión de Usuarios.
2. Si se necesita cambiar la contraseña, seleccionar el usuario y hacer click en **Cambiar**.
3. Opcional: Introducir la contraseña antigua.

Nota

Al cambiar la contraseña del administrador primero debe introducir la contraseña anterior.

4. Introducir una nueva contraseña y confirmar la contraseña.
5. Hacer click en **OK**.

Capítulo 12 Configuración del Sistema

Se pueden configurar los parámetros generales como almacenaje de imágenes, sonido de alarma, configuración de emails, ruta para guardar el archivo, parámetros de video portero y dispositivos de Control de Accesos.

12.1 Configurar los parámetros generales

Se pueden configurar los parámetros más utilizados, incluyendo el tiempo de caducidad del registro, parámetros de red, y etc.

Pasos

1. Ingresar el módulo de configuración del sistema.
2. Hacer click en la pestaña **General** para ingresar a la página de configuración general.
3. Configurar los parámetros generales.

   Registro Fecha de Vencimiento

   El tiempo para mantener los archivos de registro. Una vez superado, los archivos serán eliminados.

   Modo Máximo

   Seleccionar **Maximizar** o **Pantalla Completa** como el modo máximo. El modo maximizar puede maximizar la visualización y mostrar la barra de tareas. En el modo de pantalla completa se puede mostrar al cliente en el modo de pantalla completa.

   Realización de Redes

   Establacer las condiciones de la red en **Normal**, **Mejor** o **el Mejor**.

   Sincronización Automática de la hora

   Sincroniza automáticamente la hora de los dispositivos agregados con la hora del ordenador local que ejecuta el software en un momento específico.
4. Hacer click en **Guardar**.

12.2 Establacer Almacenamiento de Imágenes

Las imágenes, capturadas por la cámara de terminales de control de accesos, desencadenados por eventos, pueden ser guardados en el PC ejecutando Nivian Control Center AC.

Pasos

1. Introducir el Módulo de la Configuración del Sistema.
2. Hacer click en **Almacenamiento de Imágenes.**
3. Poner el interruptor **Almacenar Imágenes en el Servidor** en Activado.
4. Seleccionar la ruta para guardar las imágenes.

Nota

Por defecto se guarda en: Disk/iVMS-4200alarmPicture

5. Hacer click en **Guardar**.

12.3 Configurar el Sonido de Alarma

Cuando se active el evento, como el evento de control de accesos, se puede configurar, el software se puede configurar para que emita una advertencia audible y se puede configurar el sonido de la advertencia audible.

Pasos

1. Abrir la página de configuracion del sistema.
2. Hacer click en la pestaña de **Sonido de Alarma** para entrar en la página de configuración de los Sonidos de Alarma.
3. Opcional: Hacer click en ··· y seleccionar los archivos de audio desde la ruta local para los diferentes eventos.
4. Opcional: Añadir un sonido de alarma personalizado.
   1) Hacer click en **Añadir** para añadir un sonido de alarma personalizado.
   2) Hacer doble click en el campo **Type** para personalizar el nombre del sonido de la alarma como se desee.
   3) Hacer click en ··· y selecciona los archivos de audio de la ruta local para las diferentes alarmas.
5. Opcional: Hacer click en para una prueba del archivo del audio.
6. Opcional: Hacer click en en la columna de operación para borrar el sonido personalizado.
7. Hacer click en **Guardar**.

Nota

El formado del fichero de audio solo puede ser WAV.

12.4 Configuración de los parámetros de Control de accesos y Video porteros

Se pueden configurar los parámetros del control de accesos y video porteros acorde a las necesidades actuales.

Pasos

1. Abrir la página de la Configuración del Sistema.
2. Hacer click en la pestaña de **Control de accesos & Video portero**.
3. Introducir la información requerida.

Tono de llamada

Hacer click en y Seleccionar el fichero de audio desde a ruta local para el sonido del Monitor Interior. Opcionalmente, se puede Hacer click en para testear un archivo de audio.

Max. Duración de llamada

Especifica los segundos que la llamada durará. La duración máxima puede ser configurada entre 15 y 60 segundos.

Max. Duración de conversación con el Monitor Interno

Especifica los segundos que durará como máximo la llamada con Monitor Interior. La duración máxima de conversación entre el Monitor Interior y el software se puede establacer de 120 a 600 segundos.

Max. Duración de conversación con la estación de la Puerta.

Especifica los segundos que durará como máximo la llamada con la estación de Puerta. La duración máxima de la conversación entre la estación de la Puerta y el cliente se puede configurar de 90 a 120 segundos.

Max. Duración de conversación con el dispositivo de Control de Accesos

Especifica los segundos que durará como máximo la llamada con el dispositivo de Control de Accesos La duración máxima de conversación entre el dispositivo de Control de Accesos y el software se puede establacer de 90 a 120 segundos.

4. Hacer click en **Guardar**.

12.5 Establacer una ruta para guardar archivos

Los archivos de configuración del sistema y las imágenes capturadas manualmente en Modo monitorización se almacenan en el PC local. Las rutas de guardado de estos archivos se pueden configurar.

Pasos

1. Abrir la página de configuración del sistema.
2. Hacer click en la pestaña **Archivo** para entrar en la página de Ajustes de la Ruta de Guardado.
3. Hacer click en y seleccionar una ruta local para los ficheros.
4. Hacer click en **Guardar**.

12.6 Configurar los Parámetros de Email

Una notificación por email puede ser enviada cuando ocurre un evento. Para enviar el email a algunos receptores, los parámetros del email necesitan ser configurados antes de procesarlos.

Pasos

1. Entrar en el módulo de Configuración del Sistema.
2. Hacer click en la pestaña de **Email** para entrar en la interfaz de Configuración de Email.

3. Introducir la información requerida.

Servidor STMP

La dirección IP del servidor STMP del host (e.g., smtp.263xmail.com).

Tipo Encriptado

Se puede comprobar la radio para seleccionar **Non-Encrypted**, **SSL**, o **STARTTLS**.

Puerto

Introducir la comunicación del Puerto usado para SMTP. Por defecto el Puerto es 25.

Emisor de dirección

La dirección email desde la que se quiere enviar información.

Certicado de Seguridad (Opcional)

Si el servidor de correo electrónico requiere autenticación, marcar esta casilla de verificación para usar la autenticación para iniciar sesión en el servidor e ingresar el nombre de usuario y la contraseña de su cuenta de correo electrónico.

Nombre de Usuario

Introducir el nombre de la dirección email si la **Autenticación del servidor** está chequeada.

Contraseña

Introducir la contraseña del email si la **Autenticación del servidor** está chequeada.

Receptor 1 a 3

Introducir la dirección email del receptor. Se pueden configurar hasta tres direcciones.

4. Opcional: Hacer click en **Enviar un email de prueba** para enviar un email al receptor para probar.
5. Hacer click en **Guardar**.

Capítulo 13 Funcionamiento y Mantenimiento

Las operaciones de mantenimiento se realizan en el menú para garantizar un uso cómodo y conveniente del software.
Hacer click en  en la esquina superior derecho y luego hacer click en **Archivo** /**Sistema** /**Herramienta** para realizar las siguientes operaciones.

Abrir Archivo de Registro

Se puede abrir un archivo de registro guardado en el PC local o archivos de registro del software.

Importar o Exportar el fichero de Configuración

Se pueden importar archivos de configuración (de Nivian Control Center V2.7.0 y superiores) desde el PC local al software y viceversa. Los siguientes archivos de configuración de los módulos del cliente están permitidos para ser importados/ exportados: Control de Accesos, Gestión de Dispositivos, Centro de Evento, usuario, tiempo y asistencia.

Copia de Seguridad Automática

Seleccionar el día y la hora para hacer una copia de seguridad de los archivos de configuración y los datos de la base de datos o restaurar los datos de la copia de seguridad.

Sincronización de la hora por Lotes

Sincronizar la hora de los dispositivos seleccionados con la hora del PC.

Cola de mensajes

Después de configurar el enlace de correo electrónico, se muestran los eventos.
Seleccionar un evento y cancelar el envío del correo electrónico al destinatario.

A. Descripciones de reglas Wiegand personalizadas

Coger Wiegand 44 como un ejemplo, los valores de configuración de la pestaña Wiegand personalizado son los siguientes:

Nombre Wiegand Personalizado	Wiegand 44				
Longitud Total	44				
Regla de Transformación (Dígito Decimal)	byFormatRule [4]=[1][4][0][0]				
Modo Paridad	Paridad XOR				
Bit de inicio de paridad impar		Longitud			
Bit de inicio de paridad par		Longitud			
Bit de Inicio de Paridad XOR	0	Longitud por Grupo	4	Longitud Total	40
Bit de inicio de la ID de la tarjeta	0	Longitud	32	Dígito Decimal	10
Código de Bit de Inicio		Longitud		Dígito Decimal	
Bit de Entrada OEM		Longitud		Dígito Decimal	
Código de fabricación del Bit de Inicio	32	Longitud	8	Dígito Decimal	3

Datos Wiegand

Datos Wiegand= Datos Válidos + Paridad del Dato.

Longitud Total

Longitud de datos Wiegand.

Regla de transporte

4 bytes. Mostrar los tipos de combinación de los datos válidos. El ejemplo muestra la combinación de la ID de la tarjeta y el Código de fabricación. El dato válido puede contener una sola regla o varias.

Modo de paridad

Paridad válida para los datos de Wiegand. Se puede seleccionar la paridad par o impar.

Bit de inicio de Paridad Impar y longitud.

Si se selecciona paridad impar, estos elementos están disponibles. Si el bit de inicio de paridad impar es 1 y la longitud es 12, entonces el sistema iniciará el cálculo de paridad desde el bit 1. Calculará 12 bits. El resultado estará en el bit 0. (El Bit 0 es el primer bit.)

Bit de arranque de paridad par, y longitud.

Si se selecciona la paridad par, estos elementos están disponibles. Si el bit de inicio de paridad par es 12 y la longitud es 12. Entonces el sistema iniciará el cálculo de paridad a partir de bit 12. Calculará 12 bits. El resultado estará en el ultimo bit.

Bit de inicio de paridad XOR, Longitud por Grupo y Longitud Total.

Si se selecciona paridad XOR, estos elementos están disponibles. Según se muestra en la tabla de arriba, el bit de inicio es 0, la longitude del Grupo es 4 y la longitude total es 40. Esto significa que el sistema calculará a partir del bit 0, calcula cada 4 bits hasta un total de 40 bits (10 Grupos en Total). El resultado estará en los últimos 4 bits. (La Longitud del resultado es la misma que la del Grupo).

ID de la tarjeta Bit de inicio, longitud y dígito decimal.

Si se utiliza la regla de transformación, estos elementos están disponibles. Dependiendo de la tabla que se muestra arriba, el bit de inicio de la ID de la tarjeta es 0, la longitude es 32 y el dígito decimal es 10. Representa que desde el bit 0, hay 32 bits que representan la ID de la tarjeta. (La longitud se calcula por bit). La longitude del dígito decimal es 10 bits.

Bit de inicio del código de sitio, longitud y dígito decimal

Si se usa la regla de transformación, estos items están disponibles. Para más detalles, ver la explicación de la tarjeta ID.

Bit de inicio OEM, longitud y dígito decimal

Si se usa la regla de transformación, estos items están disponibles. Para más detalles, ver la explicación de la tarjeta ID.

Código de inicio Bit de inicio, longitud y dígito decimal

Estos elementos están disponibles si se utilizan las reglas de transformación. Dependiendo de la tabla mostrada arriba, el bit de inicio del Código del fabricante es 32, la longitude es 8 y el dígito decimal es 3. Representa que a partir del bit 32 hay 8 bits del Código de fabricante (la longitud se calcula por bits), siendo 3 la longitud decimal.