

# CMIO Manager v2

## Administrator's Guide

v1.3.0



# CMID Manager V2 Administrator's Guide

Version 1.3.0, February 2020



# Table of Contents

1. Introduction to CMID Manager V2 .....	1
1.1. About This Guide .....	1
Revision History .....	1
1.2. Architectural Overview .....	3
1.3. Supported Devices .....	5
1.4. Feature Summary .....	6
2. Installing CMID Manager V2 .....	9
2.1. Installation Overview .....	9
2.2. System Requirements .....	10
2.3. Installing Device Agent .....	11
2.4. Setting up Device Agent .....	12
2.5. Installing Client .....	14
2.5.1. Logging in to CMID Manager V2 .....	14
2.6. Activating CMID Manager V2 .....	17
3. Setting up CMID Manager V2 .....	19
3.1. Setting up General Information .....	19
3.1.1. Adding Company Information .....	20
3.1.2. Adding Departments/Doors/Titles .....	22
3.1.3. Updating Administrator Account Information .....	23
3.2. Adding New Device .....	24
3.2.1. Adding Device Manually .....	24
3.2.2. Searching and Adding Devices .....	25
3.3. Adding New Users .....	27
3.3.1. Registering a User .....	27
3.3.2. Importing Users .....	33
3.3.3. Adding Smart Cards (Template-on-card) .....	37
3.4. Adding Access Groups .....	40
3.4.1. Creating an Access Group .....	40
3.4.2. Adding Users to Access Group .....	41
3.5. Adding Rules .....	42
3.5.1. Adding Work Time Rule .....	43
3.5.2. Adding Work Exception Rule .....	45
3.5.3. Adding Holiday Rule .....	45
3.5.4. Adding User Schedule Rule .....	46
3.5.5. Adding Device Schedule Rule .....	48

3.5.6. Adding Work Schedule Rule .....	50
3.6. Changing System Settings .....	51
4. Using CMID Manager V2 .....	53
4.1. Using Dashboard .....	53
4.1.1. Dashboard Overview .....	53
4.1.2. Monitoring T&A Status .....	55
4.1.3. Monitoring Access Status .....	57
4.1.4. Monitoring Alarm Events .....	57
4.1.5. Monitoring Device Status .....	59
4.1.6. Monitoring Access Events .....	60
4.2. Using Access Control .....	62
4.2.1. Managing Access Events .....	62
4.2.2. Using Door Control .....	64
4.2.3. Using Local Anti-Passback .....	65
4.2.4. Using Global Anti-Passback (Optional) .....	66
4.2.5. Setting up Wiegand Control .....	71
4.3. Using Time & Attendance .....	74
4.3.1. Viewing T&A Events .....	74
4.3.2. Exporting T&A Events .....	78
4.3.3. Managing Overtime .....	78
4.4. Managing Users .....	80
4.4.1. Viewing and Updating User Information .....	80
4.4.2. Exporting Users .....	81
4.4.3. Deleting Users .....	82
4.4.4. Restoring Users .....	82
4.4.5. Protecting Personal Data of Inactive Users .....	83
4.5. Managing Devices .....	84
4.5.1. Viewing Device Information .....	84
4.5.2. Exporting Device List .....	84
4.5.3. Updating Device Information .....	85
4.5.4. Upgrading Device Firmware .....	86
4.5.5. Transferring Device Settings to Other Devices .....	86
4.5.6. Uploading Screensaver to Devices .....	87
4.5.7. Setting up Tamper on Devices .....	87
4.6. Managing Rules .....	88
4.6.1. Viewing and Updating Rule Information .....	88
4.6.2. Applying Rules .....	88

4.6.3. Applying Shift Work Rule .....	95
4.7. Backing Up/Restoring Database .....	101
4.7.1. Backing Up Database .....	101
4.7.2. Restoring Database .....	104
Appendix A: EF-45 Advanced Settings Reference .....	105
A.1. Device Setting .....	105
A.1.1. Device > Configuration .....	105
A.1.2. Device > Bio .....	106
A.1.3. Device > Door .....	107
A.1.4. Device > Interphone .....	109
A.2. Network Setting .....	110
A.2.1. Network > Server .....	110
A.2.2. Network > Serial .....	110
A.2.3. Network > Etc .....	111
A.3. Display Setting .....	111
A.3.1. Display > Display .....	111
A.3.2. Display > Screen Saver .....	112
A.4. Authentication Setting .....	112
A.4.1. Authentication > Mode .....	112
A.4.2. Authentication > T&A .....	112
A.4.3. Authentication > T&A Key map .....	114
A.4.4. Authentication > T&A custom .....	114
A.4.5. Authentication > Admin password .....	114
A.5. Mode Setting .....	114
A.5.1. Mode > Operation .....	114
A.5.2. Mode > Wiegand .....	115
A.5.3. Mode > Card .....	116
A.6. Miscellaneous Setting .....	116
A.6.1. Etc > Device information .....	116
A.6.2. Etc > Firmware .....	117
A.6.3. Etc > Management .....	117
Appendix B: End-User License Agreement (EULA) .....	119
B.1. License Grant .....	119
B.2. Intellectual Property and Ownership .....	120
B.3. Term and Termination .....	120
B.4. Amendments to this Agreement .....	120
B.5. Governing Law .....	121

B.6. Entire Agreement .....	121
B.7. Contact Information .....	121
Appendix C: Copyright Notice .....	123
Appendix D: Disclaimers .....	125
Appendix E: Abbreviations .....	127



# 1. Introduction to CMID Manager V2

CMID Manager V2 is an integrated management system that gives users the ability to manage access control and time & attendance for employees under the biometric security environment. The system offers a client-server architecture that consists of central Device Agent and desktop clients based on Microsoft Windows and MariaDB.

## 1.1. About This Guide

This guide contains the descriptions and operational instructions for CMID Manager V2 system. It is intended and written for system administrators who are in charge of overall operation including installation and management. We recommend you familiarize yourself with this guide to make the most effective use of the software.



- The figures and screenshots in this guide are given for illustration purposes only and may differ from the actual product.
- Due to continuous technological improvements, the guide may not contain the most updated information. For further information not covered in this guide, please contact us at [service@cmi-tech.com](mailto:service@cmi-tech.com) [mailto:service@cmi-tech.com].

### Revision History

Version	Date	Description	Software Version	Note
1.0.0	2019-05-27	Initial public release	2.1.2.0	
1.1.0	2019-09-04	<ul style="list-style-type: none"> <li>• Added <b>User Schedule Rule</b> and <b>Device Schedule Rule</b></li> <li>• Added <b>Overtime Management</b></li> <li>• Updated <b>Anti-Passback Control</b></li> <li>• Updated <b>Work Exception Rule</b></li> </ul>	2.1.3.0	
1.2.0	2019-11-29	Added <b>Using Global Anti-Passback</b> and zone management	2.1.3.1	

---

Version	Date	Description	Software Version	Note
1.2.1	2019-12-18	<ul style="list-style-type: none"><li>Added Automatic Database backup, Automatic Profile Picture Upload, and Manual Event Import</li><li>Updated <b>EF-45 Advanced Settings Reference</b></li></ul>	2.1.3.3	
1.2.2	2020-01-16	Added TOC (Template-on-card), Screensaver upload, Tamper setting	2.1.3.4	
1.3.0	2020-02-20	Added Shift Work	2.1.3.5	

---

## 1.2. Architectural Overview

CMID Manager V2 is based and built upon two main components: Device Agent and Client. The Device Agent works as a core system of the software and provides basic backend functions for main service, device, and database management, whereas the Client provides the interface that allows users to connect to the Device Agent and perform their task by using the software in the front-end.

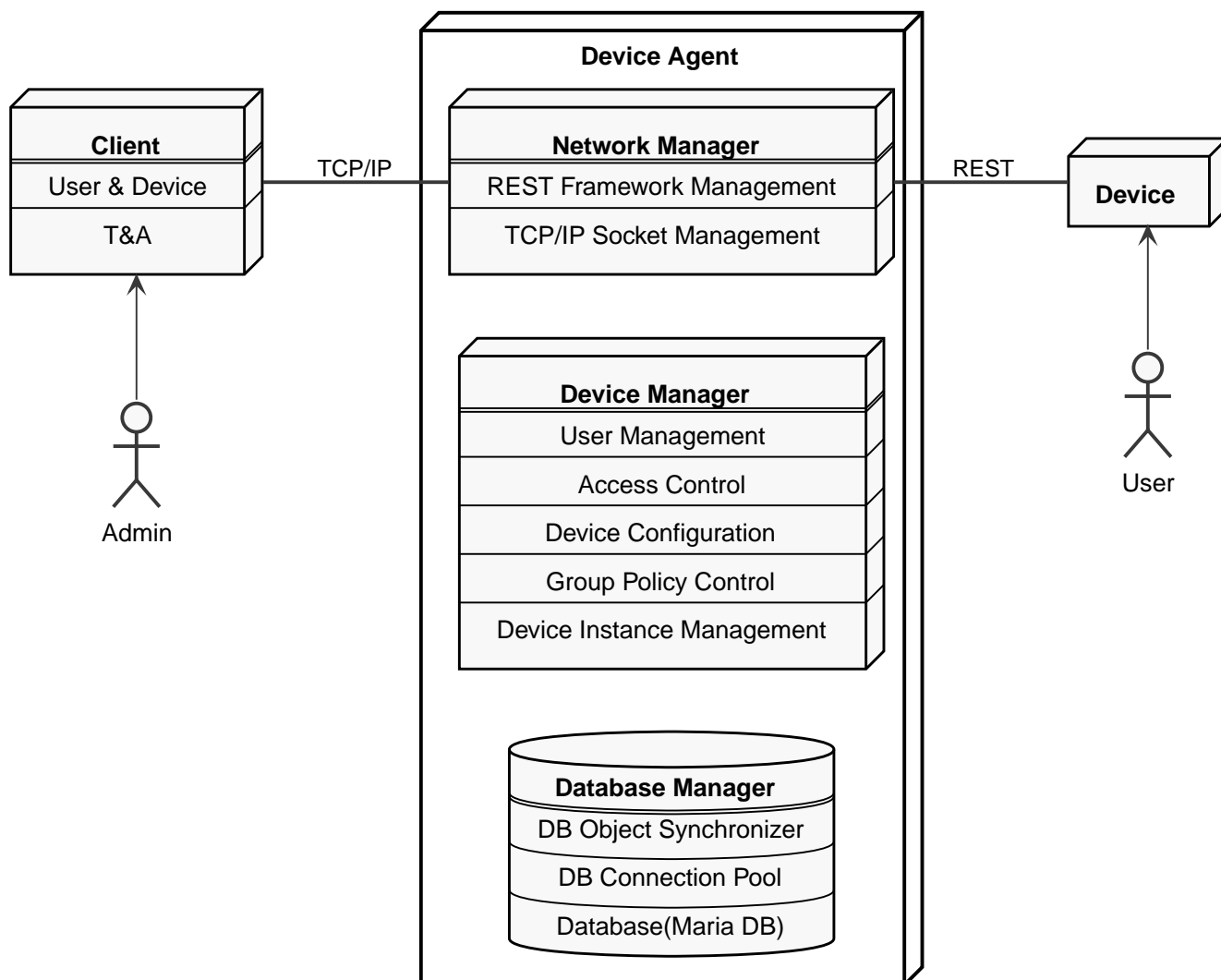


Figure 1. CMID Manager V2 Component Diagram

There are three modules within the Device Agent: Device Manager, Database Manager and Network Manager.

### **Device Manager**

The Device Manager acts as the main service framework of Device Agent and provides a set of components necessary for user and device management. Core capabilities of Device Manager include:

- User Management
- Access Control
- Device Configuration
- Group Policy Control
- Device Instance Management

### **Network Manager**

The Network Manager provides the network interface for CMID Manager V2 clients and devices, transparently handling connections over TCP/IP socket or REST service. It contains two functional components:

- TCP/IP Socket Connection Manager (for clients)
- REST Service Framework (for devices)

### **Database Manager**

The Database Manager provides database service to clients based on Maria DB management system. It maintains a database connection pool to improve performance and synchronize database upon CRUD operations. The Database Manager consists of:

- DB Connection Pool Control
- DB Object Synchronizer
- Database

Each module has access to the database depending on its needs and retrieves and manipulates data when the relevant events occur.

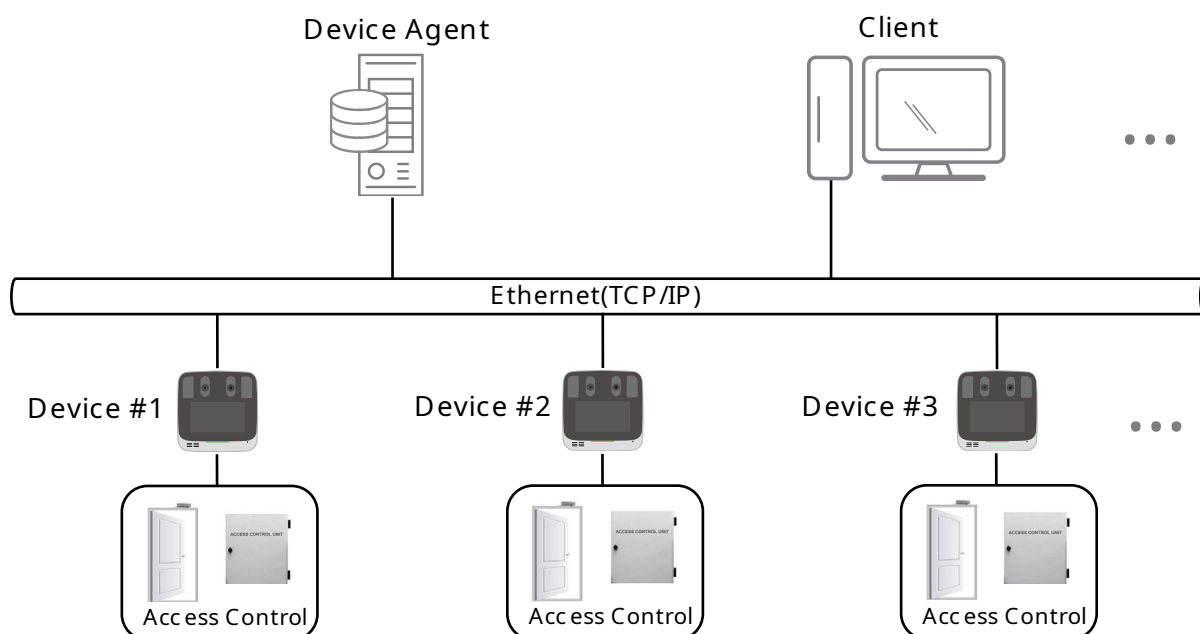


Figure 2. CMID Manager V2 Deployment Diagram

CMID Manager V2 is a server-client application that supports multiple devices. The number of supported devices depends on the product license. The free version offers all the features but allows a single device to be connected. A typical configuration is that multiple access control devices and clients are connected to a central Device Agent via Ethernet. It is also possible that the Device Agent is installed with the Client in the same local system in a smaller environment.

### 1.3. Supported Devices

CMID Manager V2 supports the following device:

- **EF-45:** The EF-45 is a next-generation dual iris imaging system that provides unprecedented subject ease of use through a highly innovative and intuitive user positioning approach. The device offers standard on-board (local) iris data base of 10,000 (maximum 50,000, optional) subjects (iris template-pairs) with matching speed of about 1.0 second in 1:N mode. The normal external communication to host systems and clients is through TCP/IP via an Ethernet connection and USB interface.



## 1.4. Feature Summary

The key features of CMID Manager V2 are as follows:

### Dashboard

CMID Manager V2 provides dashboard and monitoring functions, giving you a quick overview of access events and T&A statistics. The dashboard information includes daily and monthly attendance status in charts and lists. The monitoring pane shows various access events, entrance alerts, connected devices in real time.

### User Management

CMID Manager V2 lets you add new users to the user database including biometric and card information. You can enroll a user through the user interface that the software provides in a device selected as the enrollment machine. The system sends the user data to all the other connected devices with the user's access rights to the devices automatically.

For the case that the user enrollment is done in a local device, CMID Manager V2 provides the synchronization functionality between the master database and the local databases. It can download the user data from the EF-45 in which a new user is registered and upload the data to another device or all other devices.

CMID Manager V2 offers the user data batch import functionality that enables you to register multiple users at once by importing a file which contains the basic user information in a delimiter-separated format (for example, csv, txt, xlsx).

### Access Control and Group Management

CMID Manager V2 gives you the ability to create custom access groups and assign users and devices to a group. You can find all the access events that occur at each device or doors by various information such as group, time period, ID, and name.

It also allows you to perform door control, local and global Anti-Passback control, zone management, and Wiegand configurations.

### Device Management

Device configuration can be performed by CMID Manager V2 remotely. You can read and update almost all the types of settings available in device, which allows for unattended device management. For more information about configurable device settings, see [Appendix A: EF-45 Advanced Settings Reference](#) or relevant device user manual.

The software gives the method to upgrade the firmware in multiple devices at the same time with one click.

### Time and Attendance

CMID Manager V2 supports Time and Attendance feature to let you manage employee's work

hours by creating various time-based rules like work rules, break rules and holiday rules and applying them to companies, departments and individuals. Clock in, Clock out and other T&A event will be calculated automatically based on the rules and shown in the T&A event list in real time.

In addition, a user, who is given with personal password on registration, can sign in to CMID Manager V2 client using ID and password and look up his or her personal T&A events history.





## 2. Installing CMID Manager V2

This chapter gives the information about the system requirements and the prerequisites for installing CMID Manager V2 and the installation procedures.

### 2.1. Installation Overview

The CMID Manager V2 installation package consists of three installers for Device Agent and Client separately. The Device Agent provides service and database functionality while the Client accesses and uses services available by the Device Agent.

- The DA Core installer installs Device Agent Core module.
- The DB installer installs database components of Device Agent.
- The Client installer installs the client application.

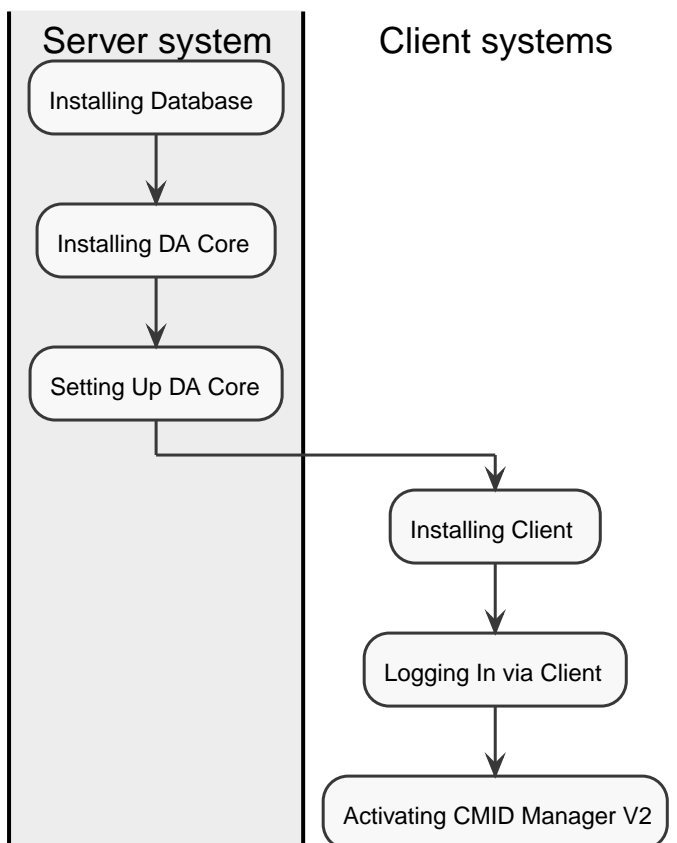


Figure 3. Installation Overview

Before installation, make sure that you check the following prerequisites:


- ☑ Prepare a Workstation or a PC where you install the Device Agent and/or the Client.
- ☑ Make sure that the Workstation or the PC meets the system requirements.
- ☑ Choose a installation type considering your network configuration. You need to decide if you will install Device Agent and Client in the same system or in the different systems connected over the network.



The system where the Device Agent is to be installed must have high reliable and durable software and hardware environment to provide services for long periods without interruption.

## 2.2. System Requirements

The system requirements for operating CMID Manager V2 are as follows:

	Minimum	Recommended	Note
Operating System	Windows 7	Windows 10 (64bit)	Device Agent and Client
CPU	Intel Core i5 series processors or AMD equivalent		
RAM	4GB	16GB or higher	
Disk Drive	100GB HDD	256GB SSD or higher	
Screen Resolution	1440 x 900	1440 x 900 or higher	Client only
	 Make sure that you set the display scaling or text size to 100% in Windows Settings or Control Panel. Otherwise, the screen may not be displayed correctly.		
Database	<ul style="list-style-type: none"> <li>• MariaDB 10.2.12 or higher</li> <li>• MySQL 5.6 or 5.7</li> </ul>		Device Agent only

## 2.3. Installing Device Agent

You must install Device Agent in the Workstation or the PC that you choose as the server machine. You can install the Device Agent by running two installers for Database and DA Core in a row.



- If you have a previous version of CMID Manager installed, remove the old version before running the CMID Manager V2 Installer.
- Do not remove or reinstall the Database Setup Program (**CMV\_DB\_Setup\_x.x.x.x.exe**) if you want to keep the current database. Otherwise, you will lose all the data that are stored in CMID Manager.

1. Double-click **CMV2\_DB\_Setup\_x.x.x.x.exe** to run the Database installer.



- If the User Account Control warning message window appears, click **OK** or **Yes** to continue.
- "x.x.x.x" stands for version identifiers and may vary depending on the software version

2. Click **Next**.

3. Click **Install** to start the installation.

4. Click **Finish** to exit the installer.

5. Double-click **CMV2\_DA\_Core\_Setup\_x.x.x.x.exe** to run DA Core installer.

6. Click **Next > Install > Finish**.

### Antivirus Exclusion Recommended



After installation, we recommend that you add DA Core program (for example, *C:\Program Files (x86)\CMITECH\CMV2\DA\_Core\Bin\CMV2\_DA\_Core.exe*) to the exclusion list of your Antivirus software, if any, to avoid any potential issues. For how to configure antivirus exclusions, refer to your Antivirus software user guide or help.

## 2.4. Setting up Device Agent

When the installation of Device Agent is completed, you should run Device Agent Core Controller program first in the server machine to configure basic Device Agent settings.

1. Open **Control Panel** in Windows.

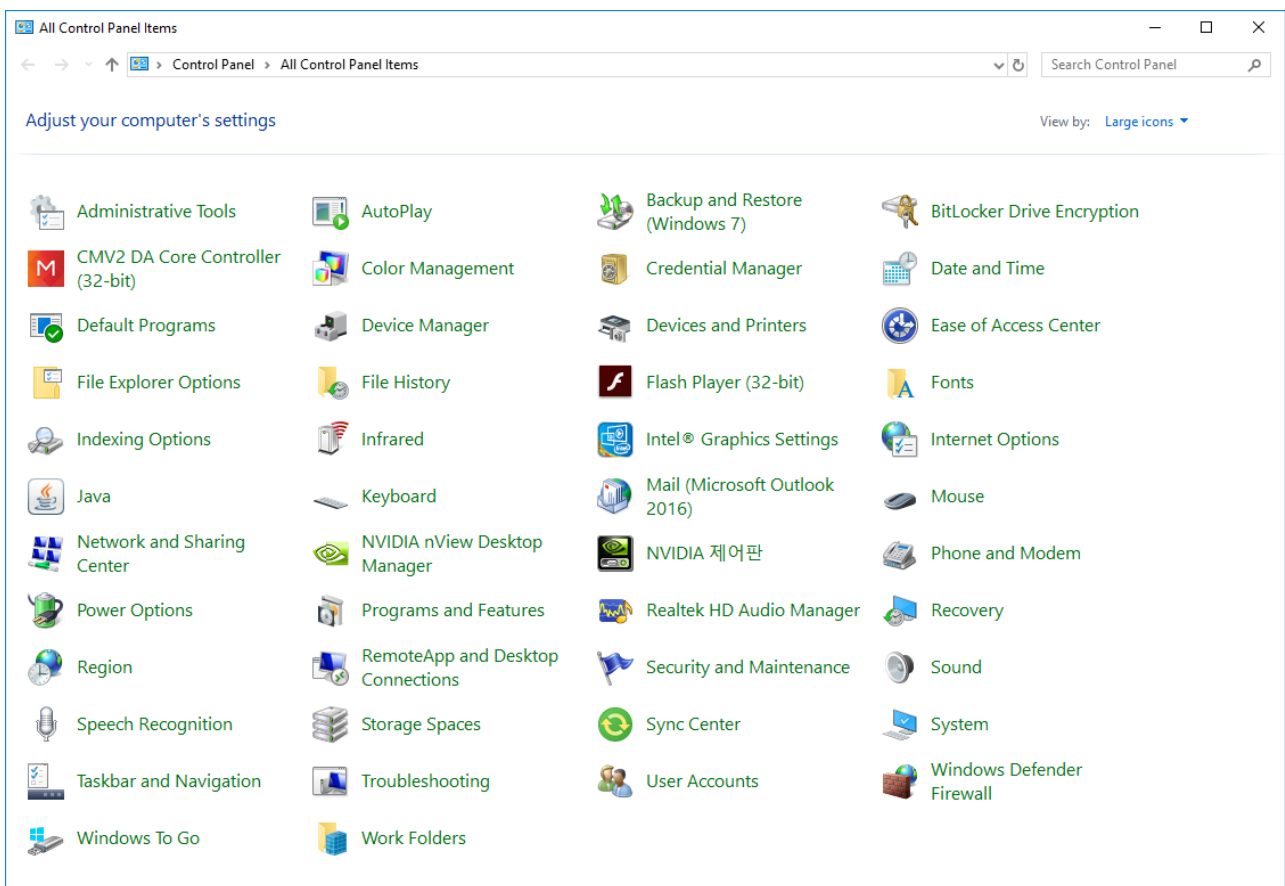


To open Control Panel,

- i) Click the Windows **Start** button on the taskbar in Windows..
- ii) Type "control panel" in the search box.
- iii) Click **Control Panel** in the results.

2. Select **Large icon** or **Small icon** in **View by** drop-down menu.

3. Click **CMV2 DA Core Controller (32-bit)** to run Device Agent Controller.



If the User Account Control warning message window appears, click **OK** or **Yes** to continue.

4. Type the IP address of Device Agent in **IP** box under **DB**.



If you have installed Device Agent and Client together in the same local PC and there is no other client to connect, you can use "127.0.0.1" as the IP address.

5. Click **Save** to save the changes and click **Close**.



Do not change the values in **Database**, **User name**, **Password**, and **Port** under **DB** unless you are advised to do so. Incorrect settings can cause problems in connecting the database.

### To Start/Stop Service Manually

When the installation is completed, the Device Agent Core service should run automatically in the background. But, in some cases, you need to start or stop the service manually. To start or stop the service manually, click **Start** or **Stop** on the **Control** tab.

## 2.5. Installing Client

There are two options you can choose for installing Client. You can install the Client application in another PC or in the same system where the Device Agent is installed depending on your need. You can also install the Client in multiple PCs and each client can access to the Device Agent through a network connection.

1. Double-click **CMV2\_Manager\_Setup\_x.x.x.x.exe** to run the Client installer.



- If the User Account Control warning message window appears, click **OK** or **Yes** to continue.
- "x.x.x.x" stands for version identifiers and may vary depending on the software version

2. Click **Next**.
3. Click **Install** to start the installation.
4. Click **Finish** to exit the installer.

### 2.5.1. Logging in to CMID Manager V2

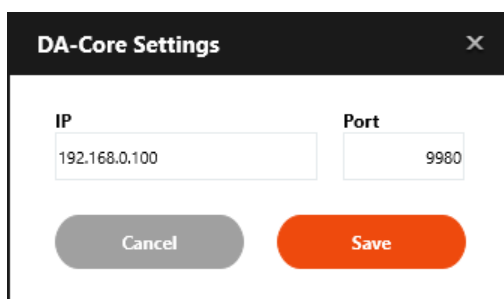
After installation, the first thing you should do is to log in to Device Agent through Client application in a client PC. Once logged in, you can configure and use all the features that CMID Manager V2 provides using the Client software.

1. Double-click **CMV2** on the Desktop to run the client application.

- Click the **Gear** button on the upper-right of the screen to open the connection setting window.



- Type the same IP address that you typed when setting up Device Agent and a port number (default: 9980) and click **Save**.



- Click **Log in**.



- The initial ID and password are as follows: admin / 0000
- You can change the admin password and add admin accounts by using Administrator settings. See [3.1.3. Updating Administrator Account Information](#) for more information.
- If you want to save ID and password and use them again in the next login session, select **Keep me logged in**.

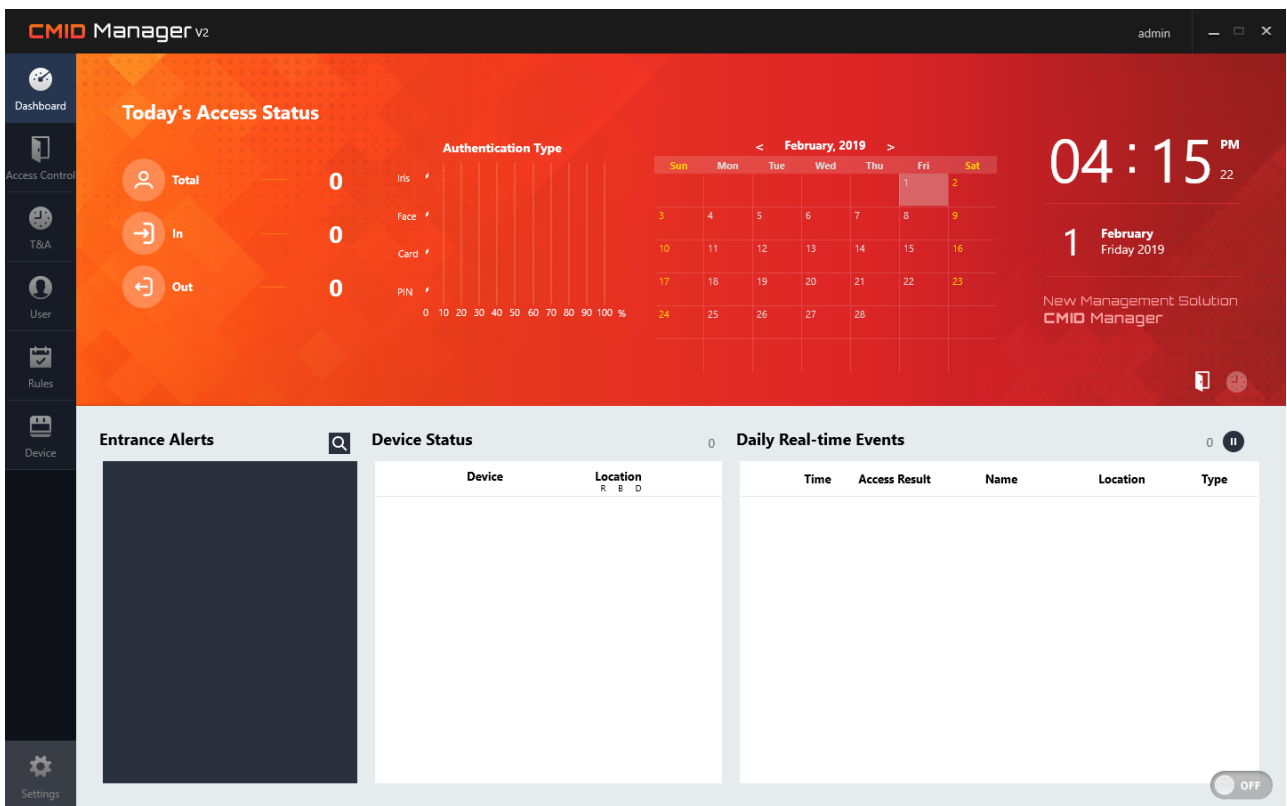
### How to Enable Auto-Login

If you want to log in automatically on every start, do the steps that follow:



1. Before logging in, be sure to select the **Keep me logged in** box on the login screen.
2. After logging in, click **Settings > Manager**.
3. Select the **Auto-Login on startup** box.
4. On the next start, you can use the software without log-in step.

5. The main window appears.





## 2.6. Activating CMID Manager V2

This section gives the instructions for how to activate the software when you purchase the software license. You can still use the software without activation for evaluation purpose with limited device connection capability.

1. Click **Settings** on the lower-left of the screen.
2. Click **License**.
3. Type **Company Name**, **Contact Name**, and **Email** address under **Request Information**.
4. Click **Save to file** and save the request (.req) file in a folder.
5. Send the request file to CMITECH at [sales@cmi-tech.com](mailto:sales@cmi-tech.com) [mailto:sales@cmi-tech.com] to acquire a license file.
6. When you receive the license file (.lic), save the license file in a folder.
7. Click **Load from file** and load the license file from the folder.
8. Click **License-In** to apply the license to the software.



When the software activation is complete, the optional features (for example, Anti-Passback) that are available with the license will appear on the **License** area highlighted in green.



### 3. Setting up CMID Manager V2

After you completed the CMID Manager V2 installation, you must do the initial setup for the software before using. This chapter gives an explanation to add devices, users, groups and rules including general information about company and administrator.

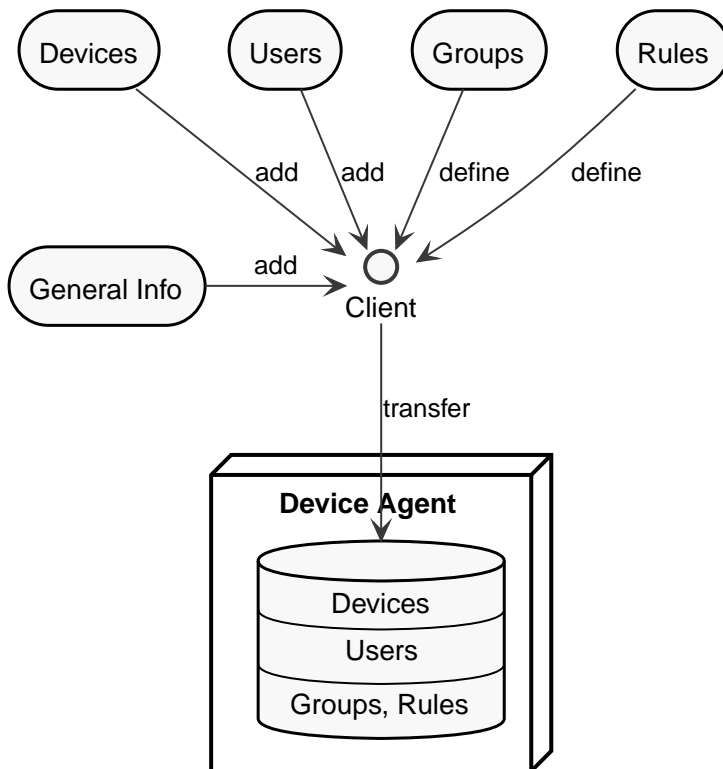


Figure 4. Setup Overview

#### 3.1. Setting up General Information

The general information includes company information and administrator information. These basic information will be used when you add devices and users and assign groups and rules.

### 3.1.1. Adding Company Information

The company information contains company name, location, contacts, doors and employee's titles. Mandatory items to be set up are the company name and basic work rule for the company.

1. Once logged in to the client, click **Settings** in the lower-left corner of the screen.
2. Click **Company** and enter the information as follow:

Name	Description	Required
<b>ID Generation Rule</b>	Type a custom ID format generated by the system automatically. Refer to the <b>Examples</b> section under the <b>ID generation rule</b> box.	Optional



- The auto-generated ID can have total 13 alphanumeric values excluding the percent ("%") sign.
- Once an ID is generated, the ID cannot be used again later even if it is not occupied by a user.





#### Examples Explained

- "%YYYY%000": [year] + [3 digits incremental number] (ex. 2018001,2018002,...,2019001,...)
- "%YYYYMM%0000": [year] + [month] + [4 digits incremental number] (ex. 2018050001,2018050002,...,2018120001,...)
- NT\_%000: [user typed character including symbol] + [3 digits incremental number] (ex. NT\_001, NT\_002,...)



A double-byte character is not allowed such as CJK languages.

Name	Description	Required
<b>Company Name</b>	Type the name of your company	Required
	 <p>A company name can't contain any of the following characters: &amp; (ampersand), \ (backslash), " (quotation mark), ' (apostrophe)</p>	
<b>Address</b>	Type the address of your company	Optional
<b>Phone Number</b>	Type the main phone number of your company	Optional
<b>Select Weekend Days</b>	Select days of week to set as weekend days	Optional
	 <p>In most of the world, the weekend is Saturday and Sunday but it varies depending on countries. For example, some countries observe Friday and Saturday as the weekend. Unless otherwise specified, Saturday and Sunday are set as default weekend and marked as red letter days on the calendars.</p>	

3. Click **Save**.

### 3.1.2. Adding Departments/Doors/Titles

Your company may have one or more departments and doors and the employees may have many job titles. Usually a door name indicates its location or the department that it belongs to. When you add a device to CMID Manager V2, you can assign a door to the device for device location and identification.



A department/title/door name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark), ' (apostrophe)

#### To add departments,

1. Click **Department Management**.
2. Click the **Plus (+)** button.
3. Select a **Parent Department** and click **OK**.



- If you have not created a department, the only **Parent Department** you can select is the company.
- You can create subordinate departments under a parent department as many levels as you want.

4. Type a department name in the **Department** box and click **Save > Close**.
  - To remove the information, select a department and click the **Minus (-)** button > **Delete > Yes**.
  - To change the name, select a department and click the **Pencil** button. Type a new value and click **Save > Close**.

#### To add titles/doors,

1. Click **Title Management** or **Door Management**.
2. Click the **Plus (+)** button, type a name, and press Enter to add the information.
  - To remove the information, click the **Trash** button.
  - To change the value, click the **Pencil** button and type a new value.
3. Click **Save > Close**.

### 3.1.3. Updating Administrator Account Information

This section describes how to change Admin password and how to add Admin account by granting Admin privilege to a user.

#### To change Admin password,

1. Click **Administrator**.
2. Type the current password in **Admin Current Password**.
3. Type a new password in **Admin New Password** and **Admin Confirm Password** in order.
4. Click **Save**.

#### To create more Admin accounts,



To grant Admin privilege to a user, you need to add the user first and give him or her a password on registration. Otherwise, there is no user found on the user list when clicking **Add Privilege**.



When you add a user as Admin for the software, the user will also have the admin rights over the device.

1. Click **Add**. The **Add Admin Privilege** window appears.
2. Select a user who you will add as an admin on the list and click **OK**. Newly added user as Admin appears on the list.
3. Select the items that you will allow the user to have admin privilege over in **Menu Privilege** and click **Save**.
  - To remove a user, click the **Trash** button.
  - To change a user's password, click the **Pencil** button and type a new value.

## 3.2. Adding New Device

The basic settings before using the management software are device setting and user setting. This section gives the procedural information to add devices for device management. There are two ways of device registration: manual input or search & select way.



When registering devices into the software, you can choose whether to download the event logs which are stored within devices. To do the task, select or clear the **Download Event Logs** check box that you can encounter on each context.

### 3.2.1. Adding Device Manually

You can add a device manually by typing its IP address and additional information.



You need to have the network information of the device that you will add. To get the information, refer to the device's user manual. For EF-45, you can find the device IP address at **Settings > Network > TCP/IP > IP Address**.

1. Click **Device** on the main window.
2. Click **Add Device** in the bottom.
3. On the **Manual Add** menu, select the model name of the device in **Device type**. The **Port** number will be entered automatically depending on the device type you select.



If you want to add multiple devices, use the **Manual Add > Manual Batch Add** menu. Click the plus (+) button as many times as the number of devices, enter the information for each device, and click **Register**.

4. Type the IP address in **IP Address**.
5. Select your company in **Company**.
6. Type or select optional information: **Device name**, **Door**, **Direction**, and **Assign Access Group**.



A device name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark)





- If you don't find a company to select, you should add it first as general information. See [3.1. Setting up General Information](#) for more information.
- If you don't find a door to select, you can add it by clicking the **Check (V)** button. See [3.1.2 Adding Departments/Doors/Titles](#) for more instructions.
- If you don't find an access group when clicking **Add** in **Assign Access Group**, you should create access groups first (See [3.4. Adding Access Groups](#)).

7. Click **Register** > **Yes** to apply.

### 3.2.2. Searching and Adding Devices

You can also use the search function that lets you to find devices connected within a specific network domain and register a device with additional information to your device list.

1. Click **Auto Detect**.



When a **Windows Security Alert** window about network security appears, click **Allow access** to continue.

2. Device search starts automatically.



You can search devices manually.

- i) Type the broadcast address of the subnet that the devices belong to. (For example, if the device IP address is 192.168.30.xxx, the broadcast address is 192.168.30.255.)
- ii) Click the **Search** button to find devices

3. Select one or more devices you will add on the list and Click **Register** > **Yes** > **OK**. The devices will be added to your device management list.



You can add more information on each device later by selecting the device on the device list on the left pane.

### Importing Event Log Data From Device

If you want to transfer the existing event logs that the registered devices contain into the CMID software, do the steps that follow:



1. Click **Device** on the main window.
2. Select a device on **Device List** from which you will download the log data.
3. Click **Additional Information** > **Etc** on the **Device Advanced Configuration** pane.
4. Click **Download Event Logs** under **Download Data**, type the admin password, and click **OK**.

## 3.3. Adding New Users

This section gives the procedural information to add users to the software and transfer users between devices for user management.

### 3.3.1. Registering a User




There are two type of user information to add: General information and Biometric information. General Information includes user ID, Name, and other contact information. Biometric information means user's biometric data such as iris, face which can be enrolled by using biometric reader.




#### Adding User Profile





You can register a user by adding general information without biometric information which can be added later.

#### To add General Information


1. Click **User** on the main window.
2. Click **Add User** in the bottom.
3. Enter the general information as follows and click **Save** to apply.

Name	Description	Required
<b>ID</b>	Type a user ID	Required*
	 You can use auto-generated value as ID or you can type the value manually.	
	 When you type a new ID, be sure to click the <b>Search</b> button to do the ID duplication check. Otherwise, you cannot save the user.	
<b>Name</b>	Type a user name	Required*
	 A user name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark)	

Name	Description	Required
<b>Password</b>	<p>Type a password which is needed when logging in CMID Manager V2 client as a user</p> <div style="display: flex; align-items: center; margin-top: 20px;">  <ul style="list-style-type: none"> <li>When a user is given a password, the user can sign in to CMID Manager V2 client by using their ID and Password and look up their personal Time and Attendance events history.</li> <li>The user can change the password by clicking the <b>Gear</b> button on the upper-right corner of the screen after login.</li> </ul> </div>	Optional
<b>PIN</b>	<p>Type PIN</p> <div style="display: flex; align-items: center; margin-top: 20px;">  <p>You can use PIN as a credential that the user can present to a device for access request.</p> </div>	Optional
<b>Phone Number</b>	Type phone number	Optional
<b>Department</b>	<p>Select the department that the user belongs to</p> <ol style="list-style-type: none"> <li>1. Click the <b>Check</b> ( V ) button. The <b>Department</b> window appears.</li> <li>2. Select a department and Click <b>OK</b>.</li> </ol> <div style="display: flex; align-items: center; margin-top: 20px;">  <p>If you have not created a department, you need to register departments first by clicking the <b>Plus</b> (+) button on the <b>Department</b> window. For more instructions, see <a href="#">3.1.2. Adding Departments/Doors/Titles.</a></p> </div>	Optional
<b>Authentication Period</b>	<p>Set a period of time for which the user is allowed to access by selecting the start date and the end date in the Calendar.</p>	Optional

Name	Description	Required
<b>Title</b>	<p>Select the user's title in the company</p> <ol style="list-style-type: none"> <li>1. Click the <b>Check</b> ( V ) button. The <b>Title</b> window appears.</li> <li>2. Select a title and Click <b>OK</b>.</li> </ol> <div data-bbox="536 555 600 613" style="float: left; margin-right: 10px;">  </div> <div data-bbox="683 528 1238 730"> <p>If you have not created a title, you need to register titles first by clicking the <b>Plus</b> (+) button on the <b>Title</b> window. For more instructions, see <a href="#">3.1.2. Adding Departments/Doors/Titles</a>.</p> </div>	Optional
<b>Enabled</b>	<p>Click the button to toggle between the user account activation and deactivation</p> <div data-bbox="536 947 600 1005" style="float: left; margin-right: 10px;">  </div> <div data-bbox="683 943 1238 1055"> <p>You can disable the user to prevent access temporarily without deleting the account.</p> </div>	Optional
<b>Employment date</b>	<p>Select the date that the user was hired by clicking the <b>Calendar</b> button</p>	Optional
<b>Email</b>	<p>Type the user's email address</p>	Optional
<b>Individual</b>	<p>Select an individual authentication mode</p> <div data-bbox="536 1415 600 1473" style="float: left; margin-right: 10px;">  </div> <div data-bbox="683 1388 1238 1635"> <p>To use this feature, make sure that you enable <b>individual authentication</b> first in the device setting. For more information, see <a href="#">A.5.1. Mode &gt; Operation</a> in the <a href="#">Appendix A: EF-45 Advanced Settings Reference</a>.</p> </div> <div data-bbox="536 1711 600 1769" style="float: left; margin-right: 10px;">  </div> <div data-bbox="683 1706 1238 1868"> <p>When enabled and selected, individual authentication mode overrides global authentication mode which is found in <a href="#">A.4.1. Authentication &gt; Mode</a>.</p> </div>	Optional
<b>Bypass card</b>	<p>Select this option to allow the user to get access permission by using a registered card alone regardless of authentication mode</p>	Optional

Name	Description	Required
<b>Current Zone</b> (optional)	Indicates the current zone where the user is. (See <a href="#">4.2.4 Using Global Anti-Passback &gt; Managing Users in Zones</a> )	Optional
<b>Profile Photo</b>	Upload a photo or an image by clicking the <b>Camera</b> button	Optional



When you enroll a user's biometrics, the user's face image captured by the device is selected as default profile photo automatically. You can also upload/delete a photo or an image manually by clicking the **Photo/Trash** button.

### To add devices that you will allow the user to access

1. Click **Assign Doors** tab > **Add** in the **Privilege** area.



When you enroll the user's biometric data to a device, the device will be added automatically as an access allowed device for the user.

2. Select devices on the list and click **Save** to apply.



When an enrollment is completed, the user data gets stored in every registered device. But the devices on which you don't have the permission do not grant access to you.

### To add access groups that you will allow the user to access

1. Click **Assign Access Group** tab > **Add** in the **Privilege** area.



If you don't find a group, you should create groups first (See [3.4. Adding Access Groups](#)).

2. Select access groups on the list and click **Save** to apply.

## Adding User Credentials

When you add user credentials such as cards, biometrics, the credential reader must be available nearby with the enrollee.

### To add card

1. Click **Add** in the **Card** pane.
2. Select a device that you will use as a card reader on the device list.
3. Click **Start** to start the card reader.



Select **Continue** to add several cards. You can register up to eight cards. Once you are done with reading multiple cards, click **Stop** to stop the card reader.

4. Put the card on the device's card reader.
5. The CSN (card serial number) appears on the **Input cards** list.
6. Click **Save** to store the card number.

### To enroll user's biometrics

1. Click **Enrollment** to open **User Biometric Data Registration** window.
2. Select biometric options as follows:
  - **Face:** Select for face enrollment
  - **Glasses:** Select for face enrollment of glasses wearer
  - **Both eyes** or **Either eye:** Select exclusively



**Both eyes** option is highly recommended for enrollment. But you can select **Either eye** if **Both eyes** enrollment is not working.

3. Select a device that you will use as a biometric reader on the device list.
4. Click **Start** to start the biometric reader.
5. Let the user sit or stand in front of the device.
6. Let the user follow the audio and visual instructions that the device provides to capture the biometrics.
7. When the preview images appear, check the images if they are captured correctly.
8. Click **Save** to store the biometric data.

### To delete a user

1. Click **User** on the main window.

2. Select a user to remove on the **User Profile** list.
3. Click **Delete**.
4. Click **Yes** to confirm.



## 3.3.2. Importing Users

The CMID Manager V2 lets you retrieve the user profiles that were made outside the software and reuse them instead of registering users all over again. There are three types of user import: user list import, user data link, and user data download. The user list contains the users with the general information only while the user data includes the user's biometric data.

### Importing User List


If you have an existing staff list or create a user list in a delimiter-separated file format (for example, csv, txt, xls), you can upload the file and register all the users on the list to the database in a batch.

Several types of user information are supported when importing users: ID, Name, Department, Title, Phone Number, and Employment Date. These items serve as the main categories of user information. If the header names of the first row in the file are the same as the main category names, you can import the file as it is. If there is a difference between them, you can link them each other first to match information correctly and then import the file.

*File contents example in csv format*

```
ID,Name,Department,Title,Phone number,Authentication Period,Employment Date
0011,Sean Kim,Sales,Assistant Manager,123-456-7890,2010-06-19 - 2020-06-19,2010-06-19
0012,Lucy Johnston,Marketing,Manager,123-456-7895,2012-06-19 - 2020-06-19,2012-06-19
0013,Gabe Turner,RnD,Manager,123-456-7897,2014-07-02 - 2020-07-02,2014-07-02
```

1. Click **User** on the main window.
2. Click **User Profile** on the left pane.
3. Click **Import** in the lower-right corner of the screen.
4. Click **Upload**.
5. Click the **Search** button in the upper-right corner of the window.
6. Select the file format in **File Type**. Type the delimiter in **Separator**.
 



  - A separator is necessary only when you select *csv* or *text* as a file type.
  - You need to type the correct delimiter character used in the file such as *comma ( , )*, *colon ( : )*, *semi-colon ( ; )*, and *pipe ( | )*.
7. Click the **Search** button in **File Name** section.
8. In the **Load from upload file** dialog box, locate the file and click **Open > OK**.
9. When the **Linked categories** and **Add category** fields appear in **User field mapping**, add or remove the fields in **Linked categories** from **Add category** if necessary by clicking the **Right**

or **Left arrow** button.

- **Main categories** has seven fixed fields: ID, Name, Department, Title, Phone Number, Authentication Period, Date of Entry.
- **Add category** shows the texts of the first row in the file read by the software.
- **Linked categories** shows the linked fields from **Add category** to **Main categories**.



Some fields are linked automatically if the name is matched each other while others are not. For example, if the **Linked categories** field is blank which is next to **Main categories** "ID" field, it means there is no text "ID" found in the first row of the file. Thus, you need to click the associated field like "ID number" in **Add categories** and click the left arrow to map the field to "ID" field in **Main categories**.

10. When **Linked categories** fields are completed, Click **Next**.

11. Make sure that the fields and values are imported correctly on the list and click **Save**.

## Importing User Data by Link

If you have an existing device that keeps the user database within it, the CMID Manager V2 allows you to retrieve the user data from the device and make a link between a newly created user template and the existing user data. Once you make a link between new data and old data and combine them, you can use the employee's data without additional biometric enrollment or any possible conflict.



Before importing user data, you must have users added into the software by registering user manually or importing user list.

1. Click **Device** on the main window.
2. Select a device on **Device List** from which you will import the user data.
3. Click **Link user** in the lower-left corner of the right pane.
  - The user list stored in the device database is shown on the **Users in device** column under the **Unlinked user in device** list. The **User** column is empty by default.
  - The user list added in the Device Agent database is shown on the **Users in DB** list.
4. Select a user in **Unlinked user in device** and select a user in **Users in DB** who you will link together
5. Click the left arrow to combine them. The linked user is shown on the **User** column.



- To view unlinked users only in the list, select the **Unlinked Users** box.
- To remove the link, select a linked user and click the right arrow.
- To delete unlinked users who remain in the list, click **Delete Unlinked Users** in the bottom.



- The user ID in the device and the user ID in the CMID Manager V2 have different meanings. The former shows a UUID and the latter indicates an employee's ID.
- When you merge both users, the old user name in the device will be changed and replaced with the new name in the software database if there is a difference between them.

## Downloading User Data from Device

If you have an existing device that stores the user data within itself and want to use it again in the software, the CMID Manager V2 allows you to download the user data from the device and store it as a database.

1. Click **Device** on the main window.
2. Select a device on **Device List** from which you will download the user data.
3. Click **Additional Information** > **Etc** in the **Device Advanced Configuration** pane.
4. Click **Download Users** under **Download Data** and click **Yes**.



- The software checks whether there is ID duplication of the users between device and software.
  - If there is no ID duplication, only the detected users in the device appear on the left **User in device** column. The users are selected automatically by default.
  - If duplication is found, the users who have the same ID appear side by side on the left **User in device** column and on the right **User** column. The duplicated users are not selected by default.
- To include the users except duplicated ones in the list, click **Unregistered user** in the upper-left corner of the window.

5. Click **Merge** > **Yes** to complete the task.



When you select the users of duplicated IDs and click **Merge**, the user names will be maintained but the biometrics will be overwritten by the ones in device, if any.



### To Add Missing User Pictures

The downloaded users basically don't have the profile picture in the User Information. In this case, you can upload it manually (see **Profile Photo** at [3.3.1 Registering a User > Adding User Profile](#)) or can automate the photo upload by selecting **If there is no user registration image, it is registered as the first authentication image** in **Settings > System > Etc..**

### 3.3.3. Adding Smart Cards (Template-on-card)

You can use an alternative biometric authentication technology, such as TOC (template-on-card) by storing a user's credentials including biometric template within a smart card that has its secure storage. The TOC method retains the biometric reference data on a card, thereby eliminates the need for maintaining the database at the local device side, and enhances security and privacy as a result.



The TOC feature is optional and may not be included in your package depending on your license type. For more information, contact us at [sales@cmi-tech.com](mailto:sales@cmi-tech.com) [mailto:sales@cmi-tech.com].



#### About compatible smart cards and card readers

Only Mifare DESfire EV1 card is supported currently. For the compatible RFID card reader, contact us at [sales@cmi-tech.com](mailto:sales@cmi-tech.com) [mailto:sales@cmi-tech.com].

### Setting Up Template On Card

The first step is to configure the TOC settings. It includes determining a encryption standard and entering the cipher key to be used for encryption and decryption.

1. Click **Settings > System**.
2. Under **TOC**, select an encryption type in **Key Type** and type an encryption key in **Key String(HEX)**.



The key needs to be entered in hexadecimal notation and must not exceed 16 bytes in length except that of **3K3DES** encryption (24 bytes).

- 16 bytes key input range : 0 to FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
- 24 bytes key input range : 0 to FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF



You may leave **Key No** and **File No** unchanged and use the default values for the initial setup. You can change these values later when necessary. (For example, it may be when you have to issue the cards all over again due to a security breach to make the existing cards unusable. Or when you need to issue the cards in another office.)

3. Click **Apply** to save settings in the software and all registered devices.



If you change any of these settings, you cannot use all the cards that have been made earlier in the previous settings because the devices cannot recognize the old cards.

## Storing Template On Card

In TOC scenario, the entire process of data acquisition, feature extraction, and matching is done at the biometric reader side. However, during the enrollment stage, the original template which is constructed at the reader is stored inside the smart card. This section describes how to issue a card that contains the user template thereon.

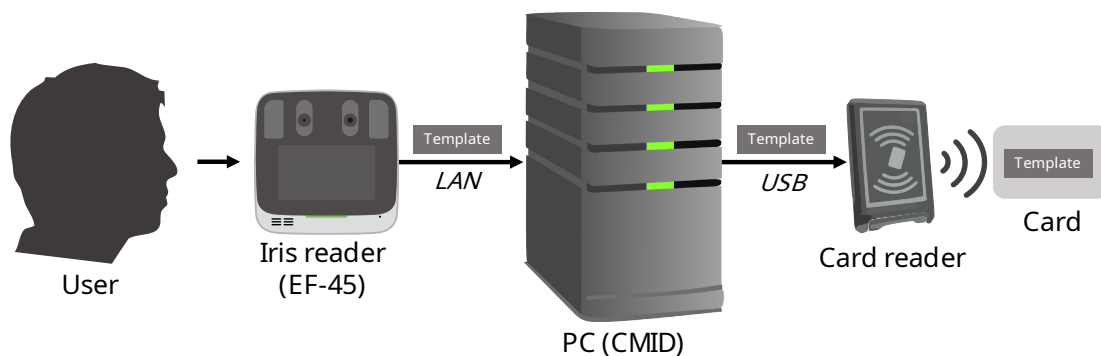


Figure 5. Template-on-card enrollment

Before issuing cards, make sure that you check the following prerequisites:



- Install the RFID card reader driver that the manufacturer provides.
- Connect the card reader to the PC where you installed the CMID Manager client program.
- Place a smart card to write on your RFID card reader correctly.



If you want to allow the users to access through TOC only, you need to withdraw their existing access privilege (if applicable) to the devices.

1. Complete the user registration including biometric enrollment (See [3.3.1 Registering a User](#))
2. Click the user for whom you will issue the card on **User > User Profile**.
3. Click **Issuing TOC** on the **User Information** screen.
4. Enter the card expiration data and time in **Period** by using the **Calendar** icon. The **Card ID** and **PIN** (if it is already present in the user information) are populated automatically.
5. Click **Issue** to write the card information and iris templates to the card.



If you want to read the existing data on the card, click **Read**. If you format the card, click **Format Card**.



Make sure that you always format the card before issuing unless the card is a blank one.

## Using Template On Card

On matching phase, the user presents his or her smart card to the biometric reader to make an authentication request. The original templates are then released from the smart card, transferred to the reader, and stored therein temporarily. The reader concurrently starts its camera to acquire the subject's biometric images and generates query templates from the captured images. Finally, the reader compares the original templates with the query templates and makes an access decision depending on the matching result. Cryptography is used to mutually authenticate the card and the biometric device through the entire process.

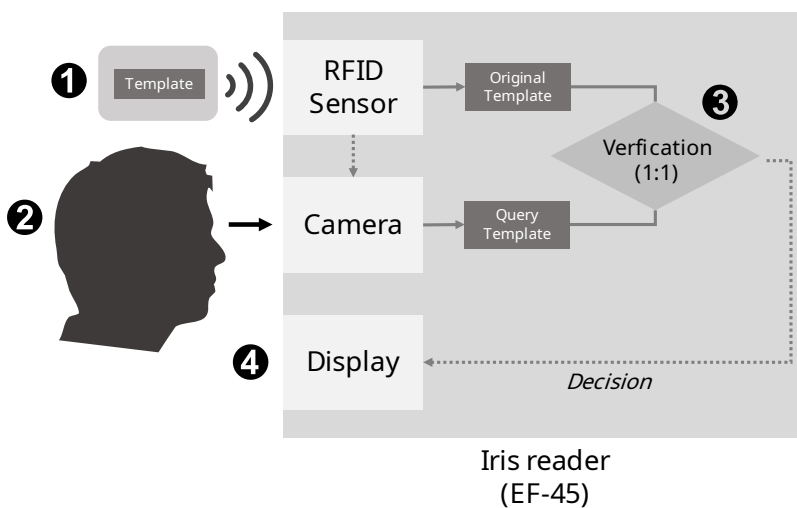


Figure 6. Template-on-card authentication

### Before you begin

Make sure that you meet the minimum firmware requirement for the device and configure the device settings related to TOC.



Device	Setup Instructions	Firmware Version
EF-45	<ol style="list-style-type: none"> <li>Set authentication start mode to <b>BIO</b> (<b>Settings &gt; Authentication &gt; Mode</b>)</li> <li>Enable TOC match functionality (<b>Settings &gt; Mode &gt; Card &gt; Iris template on card match</b>)</li> </ol>	2.1.22 or later <b>(Settings &gt; Device &gt; Device Info. &gt; Application version)</b>

- Put the smart card that you are issued on the RFID sensor of the iris reader.
- When the user interface for a biometric capture appears on the LCD, complete the verification by following the capture guidance.

## 3.4. Adding Access Groups

You can manage users and devices by using present groups or creating a new group. Each user has a department as default group and each device has a door as default group. You can see the user list, attendance list and device list by department and door's location.

In addition, you can create a new access group and assign users and devices to the group. An access group lets you define devices and users who have access permission to the devices within the same group.

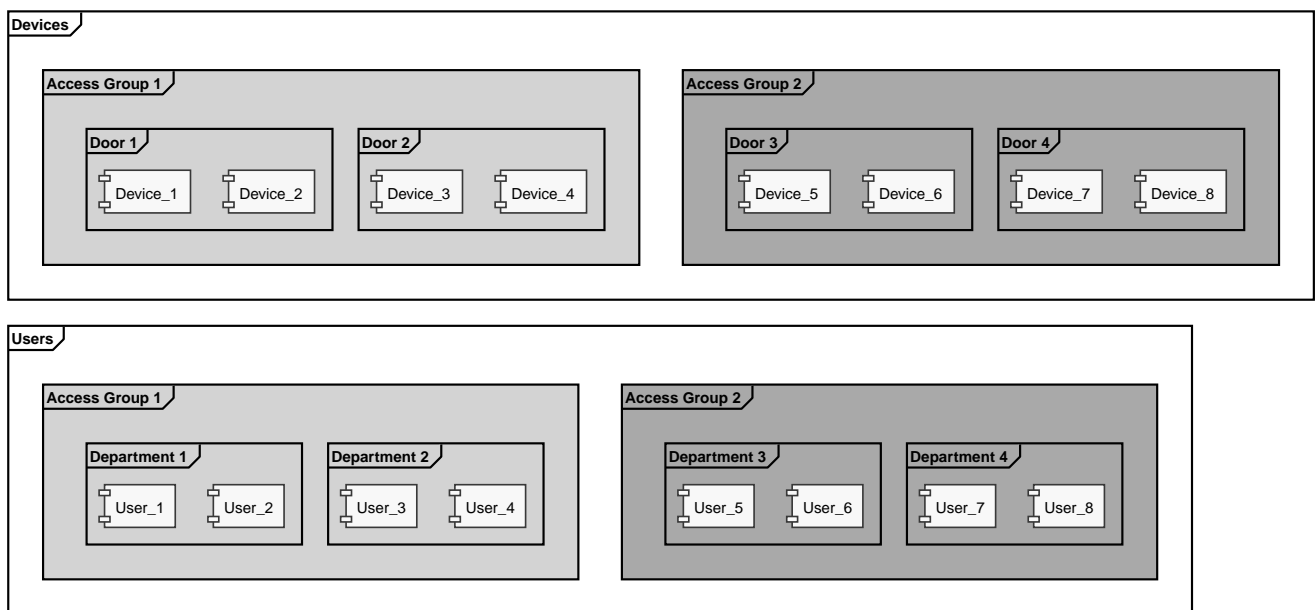


Figure 7. Grouping Example

### 3.4.1. Creating an Access Group

This section gives the procedures for creating a new access group and adding device to the group.



Before adding an access group, you must add devices and users first as described earlier in this chapter (see [3.2. Adding New Device](#) and [3.3. Adding New Users](#))

1. Click **Access Control** on the main window.
2. Click **Add Access Group** in the lower-left corner of the window.
3. Type a group name in the **Access Group Name** box.



A group name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark), ' (apostrophe)

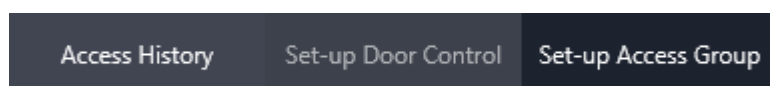


4. Select devices to add on the **Device List** and click **Save**.
5. The devices that you add will be reorganized and appear under the new access group name on the left pane.

### 3.4.2. Adding Users to Access Group

Adding an access group is followed by adding users to the group. You need to define who should access to the devices within the group. You can also add access rights to a user for specific devices in **User Information** as described in [3.3.1. Registering a User](#).

1. Click **Access Control** on the main window.
2. Select a group name on the left **Device List** pane.
3. Click the **Set-up Access Group** tab.



4. Click the **Plus (+)** button on the **Employees in Access Group** area.
5. Select users to add on the **User list** and click **Save**. The added users appears on the **Employees in Group** pane.



- You can also add or remove a device in the group by clicking the **Plus (+)** or **Minus (-)** button on the **Devices in Access Group** area.
- You can remove a user in the group by clicking the **Minus (-)** button on the **Employees in Access Group** area.

6. Click **Save** to apply.

#### To delete an access group







1. Click **Delete** in the lower-left corner of the **Group management** screen.
2. Click **Yes** to apply.

### 3.5. Adding Rules

Adding Rules enables you to create time- or date-based rules for working time management such as work time rule, work exception rule, and holiday rule. Time & Attendance feature operates based on these rules. You have a work time rule called "Day Work" to start with which is selected as Company work rule by default and you can add more rules depending on your need.

The following table presents the different kinds of rules that are available in CMID.

Table 1. Rules Overview

Type	Name	Description	Image
T&A Rule	Work Time Rule	Defines the working hours per day	 Work rule
	Work Exception Rule	Defines the non-working hours per day	 Exception rule
	Holiday Rule	Defines the holidays	 Holiday rule
	Work Schedule Rule	Defines a group of work time rules at designated sequences and intervals	 Work schedule rule
Access Control Rule	User Schedule Rule	Defines access allowed time in terms of users	 User schedule rule
	Device Schedule Rule	Defines access allowed time in terms of devices	 Work schedule rule

### 3.5.1. Adding Work Time Rule

The work time rule defines the working hour which is the period of time that employees spend at work per work day. It includes traditional work schedule that requires employees to check in and check out at designated times and flextime schedule that allows workers to change workday start and finish times.

1. Click **Rules** on the main window.
2. Click **Add Rule** in the lower-left corner of the window.
3. Click **Work rule** in **Rule type**.
4. Type a rule name in **Work Rule Name**.



A rule name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark), ' (apostrophe)

5. Select **Day Start Time** in hours and minutes.



If you clock in before **Day Start Time**, you are not considered as attended for the day. If you clock out after **Day Start Time** (after all night work possibly), your working time for the previous day is not counted.

Thus, make sure that the employees must clock in after **Day Start Time** and clock out before **Day Start Time**.

6. Select **Working Type - Fixed** or **Flexible**.
  - a. If you select **Fixed**, do the steps that follow on the **Fixed Time Settings**.
    - i. Select **Clock-in** and **Clock-out** time in hours and minutes.
    - ii. Type **Grace Time** in **In( min.)** and **Out( min. )** if necessary.



The users who clock in late within the time typed in **In( min. )** is considered as clocked in on time. The users who clock out early within the time typed in **Out( min. )** is considered as clocked out on time.

- b. If you select **Flexible**, do the steps that follow on the **Flexible Time Settings**.
    - i. Select **Working hours per day** in hours and minutes.



The **Working hours per day** is the total working time required of employees on flextime schedules. Users who work less than the hours for one day will appear as "early leave" on the T&A record on another day.

ii. Select **Clock-in Time Limit (Late/Absence)** in hours and minutes.



- The **Clock-in Time Limit (Late)** defines the start time of the core period of the day during which employees are required to be at work. Users who clock in later than this time is considered as "late" for the day.
- The **Clock-in Time Limit (Absence)** defines the end time of the core period of the day. Users who clock in later than this time is considered as "absence" for the day.

7. Select a color in **Color** to highlight the rule in the calendar.

8. (Optional) Type additional information about the rule in **Comments**.

9. Click **Save** to apply.

10. To continue to add the rules, click **Add Rule** in the upper-right corner of the screen.

## Configuring Work Time and Hourly Rate

You can set a few different types of time slots (for example, **Early** and **Midnight**) in a work rule as necessary other than regular work time and exception time.

You can also apply different hourly rates to each time slot in a day. Usually, more than 100% pay rate (for example, overtime rate) is used as an incentive or compensation for extra work of an employee. When you set an hourly rate other than 100, the total work time is recalculated and adjusted by the rate and the employees get paid more (or less) than their regular rate payment.

There are five kinds of configurable time slots – **Basic**, **Over**, **Early**, **Midnight** and **Exception**. The **Exception** time denotes the period that is not calculated as work time.

1. On **Rules > Add Rule > Work Rule > Time Settings**, click **Working time**.

2. Click the **Plus (+)** button to add a time slot.

3. Select **Start Time**, **End Time**, and **Type**.



For **Basic** type, it is a common practice that **Start Time** and **End Time** are identical to **Clock-in** time and **Clock-out** time in **Fixed Time Settings** respectively.

4. Type an hourly rate by percent in **Extra Hour (%)**. Default value is 100.

5. Add more time slots as necessary in the same way. You can also create the exception time rule by clicking **Exception time** next to **Working time**.

### 3.5.2. Adding Work Exception Rule

The work exception rule defines the break time at work which is a period of time that employees are allowed to take time off from their work per day such as meal breaks, rest breaks. It can also include any type of downtime. The downtime including break time will be deducted from working hours when calculating total working time.

1. Click **Rules** on the main window.
2. Click **Add Rule** in the lower-left corner of the window.
3. Click **Exception rule** in **Rule type**.
4. Type a rule name in **Work Rule Name**.
5. Select **Start Time** and **End Time** in hours and minutes in **Advanced Settings**.
6. (Optional) Type additional information about the rule in **Comments**.
7. Click **Save** to apply.
8. To continue to add the rules, click **Add Rule** in the upper-right corner of the screen.

### 3.5.3. Adding Holiday Rule

The holiday rule defines a day or days set aside by law or by custom or by company when employees do not go to work other than weekend days, vacation, and personal leave.

1. Click **Rules** on the main window.
2. Click **Add Rule** in the lower-left corner of the window.
3. Click **Holiday rule** in **Rule type**.
4. Type a schedule name in **Work Rule Name**.



A schedule name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark), ' (apostrophe)

5. In **Advanced Settings**, select a date as follows:
  - If the holiday is scheduled annually on a fixed date, select the **Repeat every year** box and select a date.
  - If the holiday has variable date every year or lasts several days, clear **Repeat every year** and select a date or start/end dates.



You can leave the end date blank if you will select a single date.

6. (Optional) Type additional information about the rule in **Comments**.
7. Click **Save** to apply.

### 3.5.4. Adding User Schedule Rule

A user schedule is a pre-defined list of times when a user is allowed or denied to access devices. Once a user schedule rule is applied to users, they are authorized to access devices only for the time period specified as 'operation' time depending on authentication result. It means that they cannot gain access during the non-operation time, even though their authentication is successful. You can create the user schedule rule on a daily or weekly basis, or on a specific cycle.

#### Adding Daily User Schedule Rule

Daily user schedule rule defines the access time slots for a day.

1. Click **Rules** on the main window.
2. Click **Add Rule** in the lower-left corner of the window.
3. Click **User schedule rule** in **Rule type**.
4. Click **Schedule Type** in **Schedule Settings**.
5. Click the **Plus (+)** button on the upper-right corner of the **Schedule Type** window. The **Schedule Time** window appears.
6. Type a schedule rule name in **Name** and select a color in **Color**.
7. Click the **Plus (+)** button and select **Start Time** and **End Time** in hours and minutes.



- You can add multiple time slots in a day (For example, 08:00–12:00, 13:00–17:00, 20:00–23:00)
- You can delete the time slots by clicking the **Minus (-)** button.

8. Click **Save** to save the rule.
9. When adding rules is complete, click **Save** to save all the rules.

#### Adding User Schedule Rule

Creating daily user schedule rule is followed by adding user schedule rules on a weekly or a cycle basis.

1. In the **Work Rule** window, type a rule name in **Work Rule Name**.



A schedule name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark), ' (apostrophe)

2. Select a **Schedule Type**—**Weekly** or **Daily**.



The **Weekly** type enables you to select and apply an existing daily rule to each day of the week. **Daily** lets you do the same to each day that belongs to a specific cycle.

- a. When you select **Weekly**,
  - i. Select one of present daily rules for each day of the week in **Schedule Settings**
- b. When you select **Daily**,
  - i. Type an interval of time to be repeated in number in **Cycle**.



For example, when you type "3" in **Cycle**, three day slots are created and the rule of each day is cycled from the rule of the day one rule through the rule of the day three.

- ii. Click the **Calendar** icon on the right and select **Start Date**.
  - iii. Select one of present daily rules for each day of the cycle in **Schedule Settings**
3. Select a color in **Color** to highlight the rule in the calendar.
4. (Optional) Type additional information about the rule in **Comments**.
5. Click **Save** to apply.

### 3.5.5. Adding Device Schedule Rule

A device schedule is a list of times during which a device is made to execute a predetermined action. There are three types of the device behavior—Lock, Unlock, and Routine Operation. In the "Lock" mode, the device opens the door all the time within a device schedule time period. The "Unlock" mode cause the device to close the door regardless of authentication result. For the rest of the time to which either "Lock" or "Unlock" is not applied, the device works as usual. You can create the device schedule rule on a daily or weekly basis, or on a specific cycle.

#### Adding Daily Device Schedule Rule

Daily device schedule rule defines the device lock or unlock time slots for a day.

1. Click **Rules** on the main window.
2. Click **Add Rule** in the lower-left corner of the window.
3. Click **Device schedule rule** in **Rule type**.
4. Click **Schedule Type** in **Schedule Settings**.
5. Click the **Plus (+)** button on the upper-right corner of the **Schedule Type** window. The **Schedule Time** window appears.
6. Type a schedule rule name in **Name** and select a color in **Color**.
7. Click the **Plus (+)** button and select **Start Time** and **End Time** in hours and minutes.
8. Select an action to take during the time interval in **Operation—Open** or **Close**.



- You can add multiple time slots in a day and assign different device behavior for each slot (For example, 00:00–06:00 (Close), 12:00–13:00 (Open), 20:00–23:59 (Close))
- You can delete the time slots by clicking the **Minus (-)** button.

9. Click **Save** to save the rule.
10. When adding rules is complete, click **Save** to save all the rules.

#### Adding Device Schedule Rule

Creating daily device schedule rule is followed by adding device schedule rules on a weekly or a cycle basis.

1. In the **Work Rule** window, type a rule name in **Work Rule Name**.



A schedule name can't contain any of the following characters: & (ampersand), \ (backslash), " (quotation mark), ' (apostrophe)



2. Select a **Schedule Type**—**Weekly** or **Daily**.



The **Weekly** type enables you to select and apply an existing daily rule to each day of the week. **Daily** lets you do the same to each day that belongs to a specific cycle.

- a. When you select **Weekly**,
  - i. Select one of present daily rules for each day of the week in **Schedule Settings**
- b. When you select **Daily**,
  - i. Type an interval of time to be repeated in number in **Cycle**.



For example, when you type "3" in **Cycle**, three day slots are created and the rule of each day is cycled from the rule of the day one rule through the rule of the day three.

- ii. Click the **Calendar** icon on the right and select **Start Date**.
- iii. Select one of present daily rules for each day of the cycle in **Schedule Settings**

3. Select a color in **Color** to highlight the rule in the calendar.
4. (Optional) Type additional information about the rule in **Comments**.
5. Click **Save** to apply.



- When you complete adding rules procedure, you must apply the created rules to the targets such as departments, individuals, and devices in order to make the rules to take effect. See [4.6.2. Applying Rules](#) for more information.
- The only exception to this is **Work Exception Rule**. The work exception rules are applied automatically when they are added.

### 3.5.6. Adding Work Schedule Rule

The Work Schedule Rule indicates a group of work time rules that are iterated at designated sequences and intervals. It is useful for making a shift plan.

1. Click **Rules > Add Rules > Work schedule rule**.
2. Type a rule name in **Work Rule Name**.
3. Select a **Schedule Type—Weekly or Daily**.



The **Weekly** type enables you to select and apply an existing daily rule to each day of the week. **Daily** lets you do the same to each day that belongs to a specific cycle.

- a. When you select **Weekly**,
  - i. Select one of present daily work rules or **Holiday** for each day of the week in **Schedule Settings**
- b. When you select **Daily**,
  - i. Type an interval of time to be repeated in number in **Cycle**. Now, you have a number of placeholders for work rules in the **Schedule Settings** area depending on the **Cycle** number.



For example, when you type "3" in **Cycle**, three day slots are created and the rule of each day is cycled from the rule of the day one rule through the rule of the day three.

- ii. Select one of present daily work rules or **Holiday** for each day.
4. Select a color in **Color** to highlight the rule in the calendar.
5. (Optional) Type additional information about the rule in **Comments**.
6. Click **Save** to apply.

## 3.6. Changing System Settings

This section gives information about changing system preferences. You can add a personal touch to the software by changing the skin and change the system language to display depending on your locale.

### To change the display language and the software skin

1. Click **Settings** on the lower-left of the screen.
2. Click **Manager**.
3. Select a language or a skin to change and click **Apply**.

### To view the system logs

1. Click **Settings** > **Logs**.



The system log list gives information about who, when and where the connections have been made to CMID Manager V2 Device Agent Core.



## 4. Using CMID Manager V2

When CMID Manager V2 setup is completed, you can do the management for the users, the devices and T&A by using the software on a regular basis. The management activities you can perform involve monitoring events, creating reports, integrating users, and updating device information.

### 4.1. Using Dashboard

The CMID Manager V2 dashboard provides the quick overview of Time & Attendance and Access status in a daily and monthly basis. It allows you to monitor various alarm events, device status, and access events in real time.

#### 4.1.1. Dashboard Overview

This section gives the information about CMID Manager V2 Dashboard GUI organization and the overview of each presentation. Basically the dashboard supports T&A status mode and Access status mode.

##### T&A Status Mode

To enable T&A Status Mode, click the **Clock** icon on the right side of the screen.

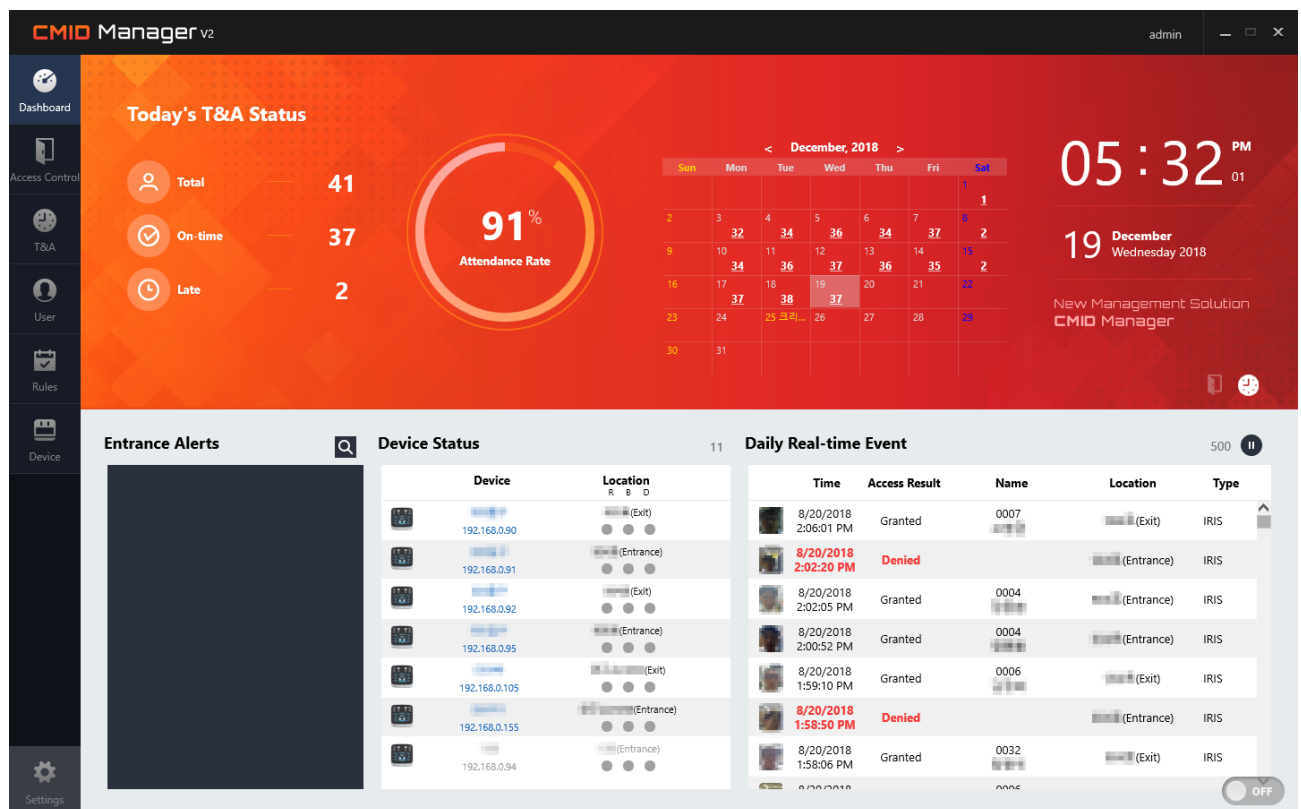


Figure 8. Dashboard Overview (T&A Status)

No.	Name	Overview
1	Today's T&A Status	
2	Attendance Rate	Shows Time & Attendance status in daily and monthly basis
3	Calendar	
4	Entrance Alerts	Shows the alarm events in real time
5	Device Status	Shows the device status in real time
6	Daily Real-time Events	Shows the access events in real time

### Access Status Mode

To enable Access Status Mode, click the **Door** icon on the right side of the screen. 

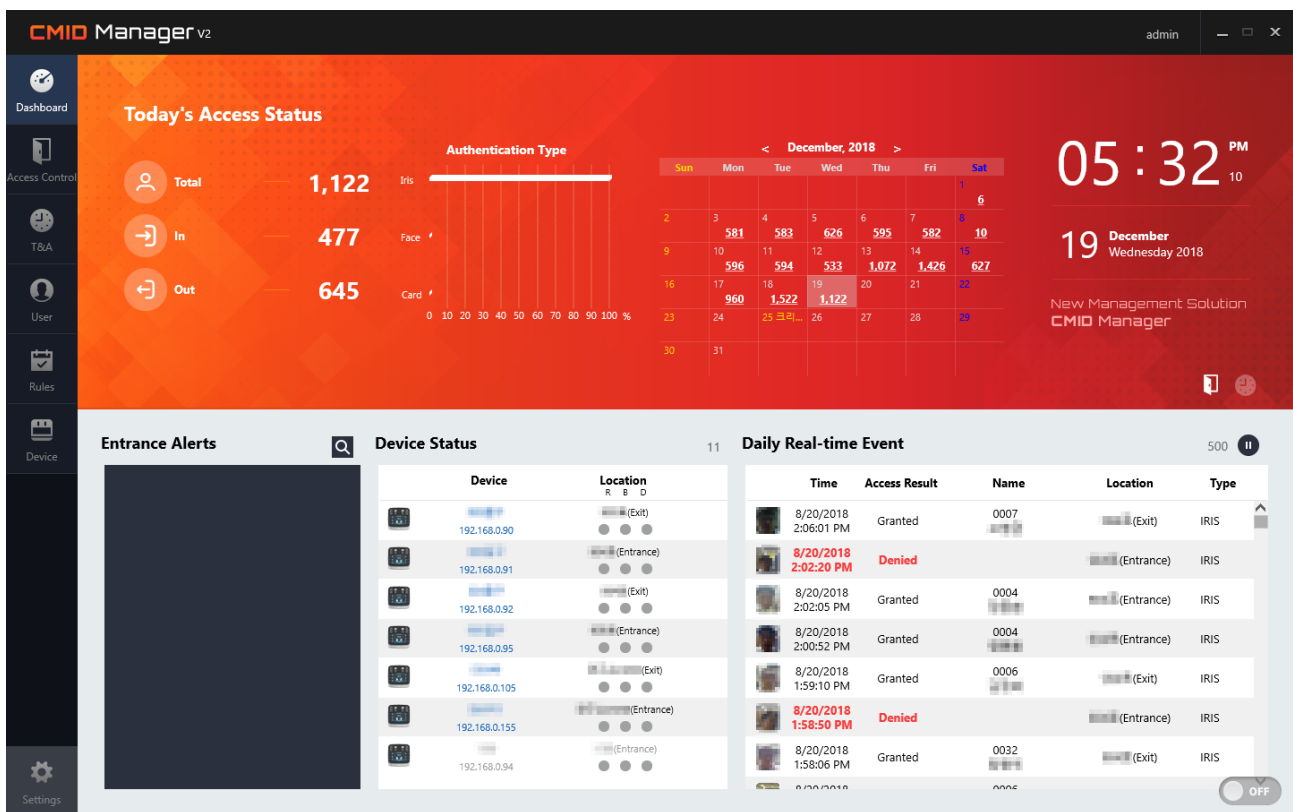


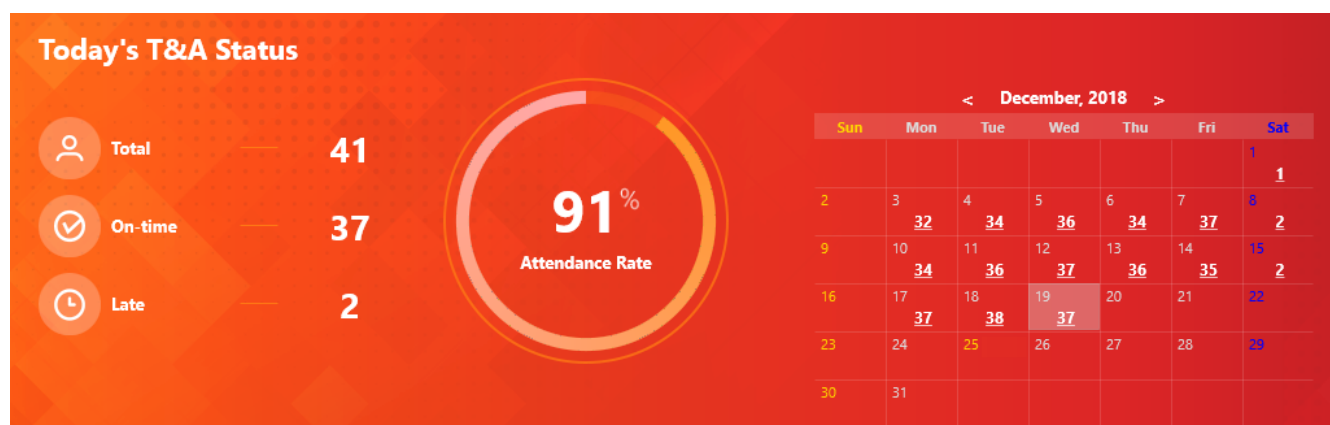
Figure 9. Dashboard Overview (Access Status)

No.	Name	Overview
1	Today's Access Status	
2	Authentication Type	Shows Access status in daily and monthly basis
3	Calendar	

No.	Name	Overview
4	Entrance Alerts	Shows the alarm events in real time
5	Device Status	Shows the device status in real time
6	Daily Real-time Events	Shows the access events in real time

## 4.1.2. Monitoring T&A Status

The T&A Status consists of Today's T&A Status, Attendance Rate, and Calendar.



No.	Name	Description
1	Today's T&A Status	Shows how many employees have attended for the day including late arrivals
2	Attendance Rate	Shows the attendance rate for the day expressed as a percentage
3	Calendar	Shows the date and the number of attended employees in the calendar view

## Viewing Today's T&A Status

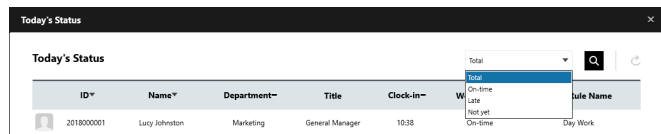
When you click **Total**, **On-time**, **Late** on the dashboard, Today's T&A Status gives more information about T&A of the day.

No.	Name	Description
1	ID, Name, Department, Title	Shows the employee's information
2	Clock-in	Shows the clock-in time of the employee

No.	Name	Description
3	Work Status	Shows the attendance status of the employee such as on-time, late, and not-yet



- When you click **On-time** or **Late** on the dashboard, only **On-time** or **Late** employees appear on the list.
- You can also view the attendance status by **Work Status** by selecting a work status and clicking the **Search** button in the upper-right corner of screen.

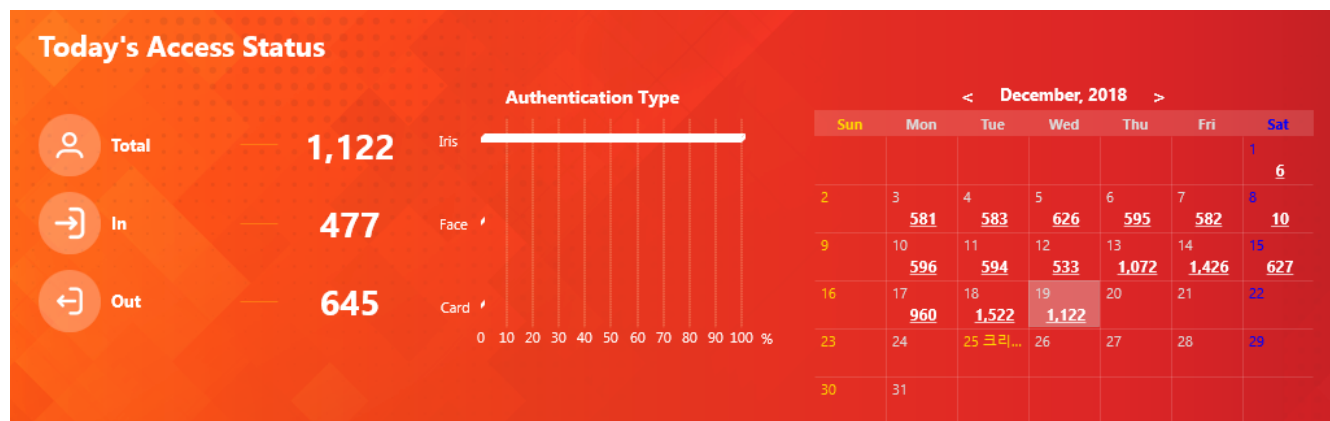


4	Work Rule Name	Show the work rule name which is applied to the employee
---	----------------	--



### 4.1.3. Monitoring Access Status

The Access Status consists of Today's Access Status, Authentication Type, and Calendar.



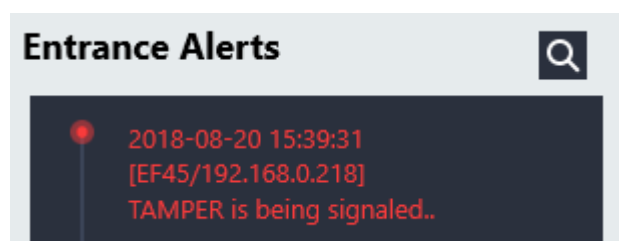
No.	Name	Description
1	Today's Access Status	Shows how many times the employees have been in and out for the day
2	Authentication Type	Shows the authentication rates by credentials for the day expressed as a percentage
3	Calendar	Shows the date and the number of access in the calendar view

### Viewing Today's Access Status

When you click **Total, In, Out** on the dashboard, Today's Access Status gives more information about Access events of the day.

### 4.1.4. Monitoring Alarm Events

The **Entrance Alerts** shows the alarm events such as tampering detection, held or forced open door events, and device disconnection. The event message gives information about alarm type, device type, occurrence time, and location (IP Address).



By clicking the **Search** button, you can open a new Alert List window and view the alarm events history by date, time, IP address, Door, Direction, alarm type, and time period.

## To enable pop-up alerts

You can also receive the alarm events in pop-up messages by doing the steps that follow:

1. Click **Settings > Manager**.
2. Under **Alarm Popup**, select the **Alarm Popup** check box in **TAMPER signaled**, **DEVICE disconnected**, or **FIRE alarm**.
3. Type a value in the **Auto Close(second)** box in **TAMPER signaled** or **DEVICE disconnected** to set a time limit for how long a pop-up message continues.



Selecting the **Sound** check box allows you to choose and to play a sound file along with a pop-up window when the alarm events occur.

1. Select the **Sound** box.
2. Click the **Search** button and locate a sound file with **.wav** file extension, and then click **Open**.



Upon triggering the fire alarm, all the doors will open.


4. Click **Apply**.



In order to make **TAMPER** and **FIRE alarm** to work, you must do the device settings first. The EF-45, for example, has the tamper settings in **Settings > Device > Door > Tamper** and the alarm settings in **Settings > Device > Door > Alarm sensor, Alarm sensor type**. For more information, refer to the EF-45 user guide and installation guide.

## 4.1.5. Monitoring Device Status

The **Device Status** shows the status of registered devices like device type, IP address, device location, and relay & door status.

Device		Location				
		T	R	B	D	S
	<p>① Main 1F</p> <p>② 192.168.0.201</p>	③	④	●	●	●
		Door1(Entrance)				
		●	●	●	●	●

- ① Device name
- ② IP address
- ③ Door address
- ④ Status indicator for tamper, relay, and door
- ⑤ Total number of devices

The relay and door status are represented by four abbreviations (R,B,D,S) and four round indicators below the location name as follows:

- **T** (tamper) shows the tamper status of the device (●(gray): Not used, ●(blue): Normal operation, ●(red): Alarm)
- **R** (relay) shows the internal relay status controlled by the device (●(gray): Idle, ●(green): Active)
- **B** (door button) shows the RTE button status connected to the device (●(gray): Idle, ●(green): Active)
- **D** (door sensor) shows the status of the door sensor connected to the device (●(gray): Idle, ●(green): Active)
- **S** (door status) show the operation mode of the device how it controls the door (●(gray): Not usable or Unknown, ●(yellow): Normal Operation, ●(blue): Always Unlock, ●(red): Always Lock)



### To change the door control mode manually

1. Double-click in the area that the device belongs to in the device list.
2. Select a target device type, click an action that you want to take, and click **OK**.



## 4.1.6. Monitoring Access Events

The **Daily Real-time Event** shows all the access events that happen at all registered devices. The event information includes a thumbnail face image that reveals the person who requests to access, request result (for example, Granted, Denied), and recognition type (for example, IRIS, FACE, CARD).

Daily Real-time Event						303	⏸	⚙
Time	Access Result	Name	Location	Type		3	4	5
8/20/2018 2:06:01 PM	Granted	① 0007	② (Exit)	IRIS				
8/20/2018 2:02:20 PM	Denied		(Entrance)	IRIS				
8/20/2018 2:02:05 PM	Granted	0004	(Entrance)	IRIS				
8/20/2018 2:00:52 PM	Granted	0004	(Entrance)	IRIS				
8/20/2018 1:59:10 PM	Granted	0006	(Exit)	IRIS				
8/20/2018 1:58:50 PM	Denied		(Entrance)	IRIS				

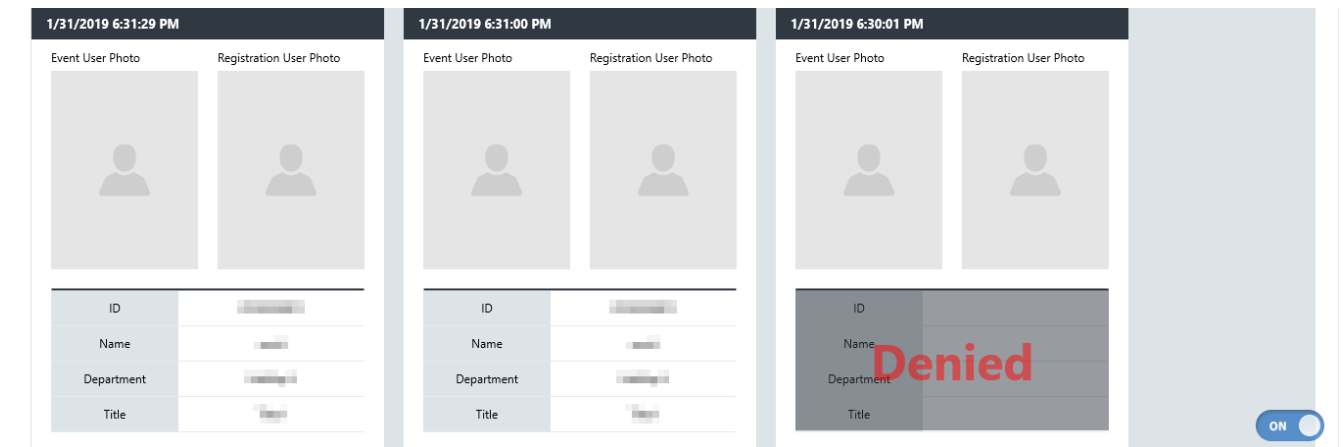
- ① Employee ID
- ② Door name
- ③ Total number of events
- ④ The **Pause/Play** button will stop or start the real time event monitoring
- ⑤ The **Gear** button will open the **Real-time Event Setting** window and allows you to configure various settings such as the limit on the number of events and display mode.




By double-clicking an item in the list, you can see more information about the person who requested to access on the **Access Information** window.

## Monitoring Access Events in Preview Mode

The preview mode gives more information about the users who request to access. It includes the time stamp, user photos, user information, and access result. Event User Photo and Registration User Photo, unlike smaller images in the list, let you identify the person easily and correctly. It also can be used for demonstration purposes.



To enable Preview Mode, click the **OFF** button (  ) in the lower-right corner of the main screen.

To disable Preview Mode, click the **ON** button (  ).



One preview window represents one access event and is displayed newest to oldest, left to right. You can scroll through the events by using the mouse wheel.

## 4.2. Using Access Control

This section gives the information about advanced access event monitoring, door control, local Anti-Passback settings, and Wiegand configurations.

### 4.2.1. Managing Access Events

You can view the entrance request events in details on **Access Control** while the **Real-time Event** on the dashboard tab gives a quick overview.

#### Viewing Access Events

##### To view the access events by device, access group, and location

1. Click **Access Control** on the main window.
2. Select an event view option as follows:
  - Select an access group to see the event list by group.
  - Select a device to see the event list by device.
  - Click **Location** tab on the **Device List** pane and select a door to see the event list by location.
  - Click **Device List** to view all the access events.

##### To view the access events that occurred within a certain period of time

1. Click the left **Calendar** button in the upper-right corner of the **Entrance List** and select a start date.
2. Click the right **Calendar** button and select an end date.
3. Click the **Search** button to view the access events that happened during that period.

##### To search the access events by user ID or user name

1. Type ID and/or Name in the boxes next to calendar area.
2. Click the **Search** button.

##### To sort the access events by various information - Date, Time, Access Type, Name, Location, and Type

1. Click the arrow next to each item title to switch between ascending sort order and descending sort order.



- When you click a user name on the access event list, you can view the user information including the photos for user identification in a pop-up window.
- The user name appears on the list only when the user is registered and recognized correctly.

## Exporting Access Events

You can save the access events in a delimiter-separated file format (for example, csv, txt, xlsx).

1. Select an access group or a door or a device by which you will export the access events on the **Device List**.
2. Click **Export** in the lower-right corner of the **Entrance List** screen.
3. Select a file format in **File Type**. Type a delimiter in **Separator**.



- A separator is necessary only when you select *csv* or *text* as a file type.
- You can type a delimiter character such as *comma( , )*, *colon( : )*, *semi-colon( ; )*, and *pipe( | )* in the **Separator** box.

4. Click the **Search** button in **File Name** section.
5. In the **Save As** dialog box, locate the file path and enter the file name and click **Save**.
6. Click **Export** > **Done** to complete the export.

## Exporting Access Events in Real Time

The CMID Manager V2 provides a way (called **Real-time Events Push**) to transmit the event logs to a compliant client at the time of event occurrence without requests from the client.

1. Click **Settings** > **System**.
2. Click **Enabled** to enable the function under **Real-time Events Push**.
3. Configure the client to get data from DA Core by typing **Host** (e.g. IP address or domain name), **URI** (path component, e.g. /EF-45/events), **Port** (port number) and by selecting a transmission protocol in **Protocol**.
4. Click **Apply**.

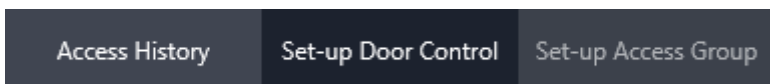


To receive and manipulate the pushed events by DA-Core correctly, you need to set up a host at client side on the network. For more information about event push configuration, contact us a [service@cmi-tech.com](mailto:service@cmi-tech.com) [mailto:service@cmi-tech.com].

## 4.2.2. Using Door Control

When the relay function is enabled in a device and the relay is connected to a door, you can open the door by sending a command to the device to trigger the relay.

1. Click **Access Control** on the main window.
2. Select a device on the left **Device List** pane.
3. Click the **Set-up Door Control** tab.



4. On **Door List**, select a door to control.
5. In the **Door Control** area, type a value in **Duration (sec)** and click **Transfer** to make the relay unlock the door and keep the door unlocked during that time.



When you click **Transfer** with duration time, the door remains unlocked during that time regardless of the default duration time in the device settings.



### 4.2.3. Using Local Anti-Passback

The Anti-Passback feature lets you prevent a valid credential holder from allowing one or more unauthorized persons who are with him or her to gain entry by passing his or her card back or by using his or her biometrics multiple times.

When you enable the local Anti-Passback function on Entrance and Exit devices, the devices updates the users' APB(Anti-Passback) status on each access event and communicate each other through RS-485. When a user try to enter or exit the door, the device refers the user's APB status to see if the user is allowed to enter or exit and grants access or not.

Because a local Anti-Passback works in pairs, the following prerequisites must be met to make Anti-Passback configurable and usable:



- In software
  - You must have at least two devices registered and connected (online) in the device list.
  - The two devices must be assigned to the same door with different directions as **Entrance** (IN) and **Exit** (OUT).
  - You must set RS485 mode correctly for each device: **NET-HOST** for Master device, **NET-SLAVE** for Slave device. For more information about RS485 settings, see [A.2.3. Network > Serial](#). You can select a RS485 mode under **RS485-NET**.
- In hardware
  - The two devices must be wired together through RS-485 interface while they are on the same network.

1. Click **Access Control** on the main window.
2. Select a device to control on the left **Device List** pane.
3. Click the **Set-up Door Control** tab.
4. Click a door in the **Door List**
5. In the **Anti-passback Control** area, click a Anti-Passback mode that you want to set on the device.
  - **Master-Soft** sets the device as Master. "Soft" means that the device allows a user to access even when the user violates the Anti-Passback rule. It just records the violation events in the log.
  - **Master-Hard** sets the device as Master. "Hard" means that the device does not allow a user to access when the user violates the Anti-Passback rule. It also records the violation events in the log.

◦ **Slave** sets the device as Slave.



Usually Entrance (IN) device works as **Master** and Exit (OUT) device as **Slave**.

6. Click **Yes** to apply changes.



**APB Clear User** makes users to be released from Anti-Passback violation status and let them to access again.

### 4.2.4. Using Global Anti-Passback (Optional)

Whereas the local Anti-Passback is enforced for a single access point or door with IN/OUT readers in pairs, the global or regional Anti-Passback establishes an additional set of rules for multiple access points or doors within zones. Generally, a zone is a physically bounded area that contains one or more locations. It can be a building, a story, an office area, or a room. You can group a number of locations together to form an Anti-Passback zone.

When you configure the global Anti-Passback on zones and devices, the devices communicates users' access records among themselves throughout the zones via TCP/IP network. The devices determine whether the user violates the Anti-Passback rule by his or her last known access record and permit access or not accordingly.



The global Anti-Passback feature is optional and may not be included in your package depending on your license type. For more information, contact us at [sales@cmi-tech.com](mailto:sales@cmi-tech.com) [mailto:sales@cmi-tech.com].

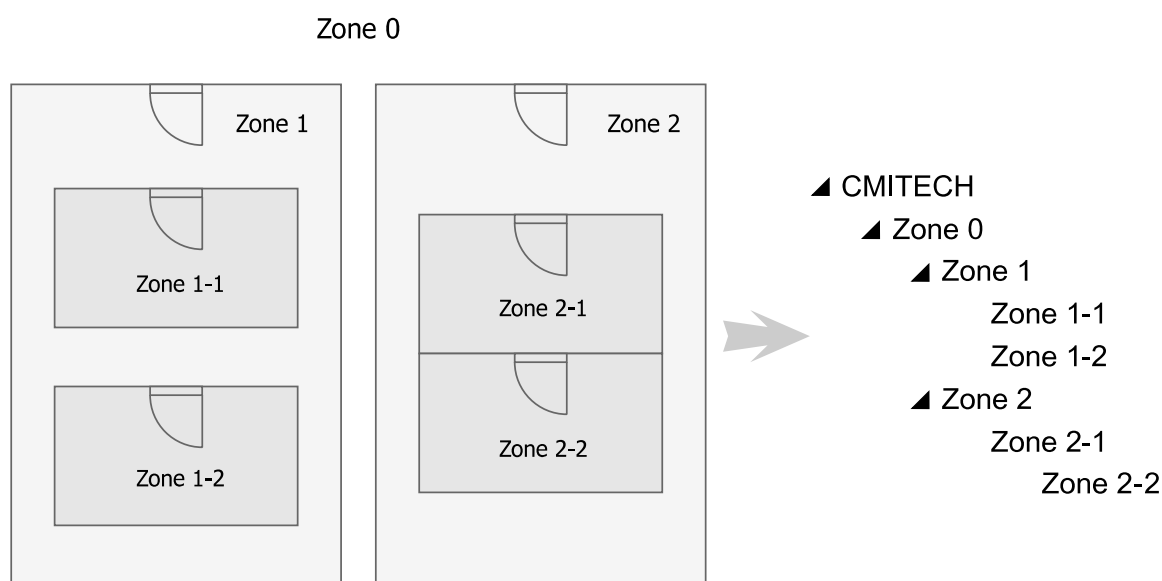


Figure 10. Zone Overview

## Creating Zones

The first step for using regional Anti-Passback (APB) is to form and organize zones. It designates the controlled areas that are subject to the APB rule.

1. Click **Access Control** on the main window.
2. Click the **Anti-passback** tab > **Zone** > **Zone management**.
3. Click **Add**, type a name, and click **Save**.



A zone that you create in the uppermost level is called a *root zone*. It serves as a zone container or a staging area (that is, 'outside' the restricted area) and presumes that there are subordinate zones in the lower levels. And there is no access points between root zones. Thus, you must create one or more subzones under a root zone in order to make the APB rule to work.

4. Select the zone that you created in the previous step and add subzones as necessary in the same way.



The CMID Manager V2 supports nested zone. A zone (child zone) can be contained within another zone (parent zone). A person must enter into a parent zone first in order to gain access to one of its child zones.

## Assigning Devices to Zones

The next step is to set the biometric readers to each zone. It specifies what device to be used on entrance and exit when moving from a zone to another zone.

1. Click **Anti-passback** > **Device**.
2. Click **Add**.
3. Select a target device in **Device List** and set the following options about the device behaviors.

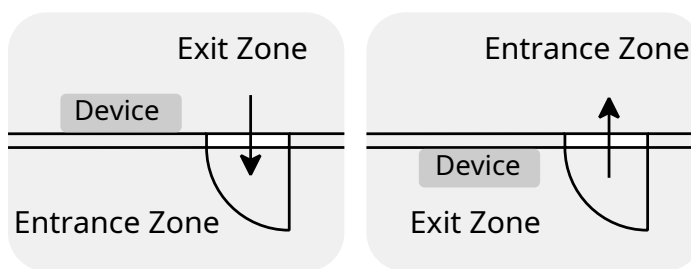
Name	Description
------	-------------

Entrance/Exit Zone	Select <b>Entrance Zone</b> and <b>Exit Zone</b> related to the device
--------------------	--

Generally, the **Exit Zone** is where the device is located. You can easily identify which one to choose by using the sentence:



“A person goes from **Exit Zone** to **Entrance Zone** through this device.”



Type	Select a type of enforcement to be imposed against APB rule violation
------	---

- **Hard:** Deny access and log
- **Soft:** Log only

Network Error	Select an action of the device when a network communication error occurs (that is, when the APB status becomes unknown for all persons due to network failure)
---------------	--

- **Access Denied:** Deny access even if the authentication is successful
- **Access Granted:** Grant access if the authentication is successful

Network Timeout	Type a Network Timeout value in seconds
-----------------	---

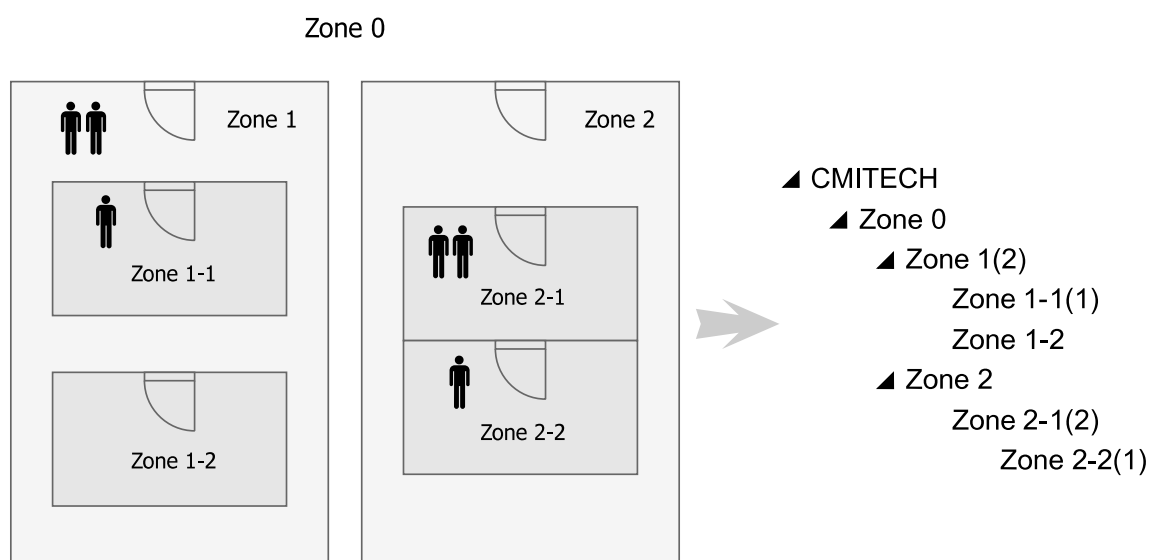
4. Add more devices to zones as necessary.
5. Click **Save** to apply changes.
6. The number of added devices will appear next to the name of zones in parentheses when you click **Zone > Zone management**.

## Managing Users in Zones

After the initial setup for zones and devices, you can monitor the flow of people between zones, track the occupancy of each zone, and check APB violation history. You sometimes need to release the users that misuse their biometric credentials and are trapped in an area consequently. You can also make an exception of some persons from the APB rule.

### To track users in the zones

1. Click **Zone > User list in zone**.
2. On the **Zone** preview pane, you can see the number of people that occupy the zones in parentheses next to the name of zones.



3. When you click a zone to see more, you can identify the persons in the zone on the **Users in the zone** pane.

If you select **Include lower zone**, all the parent zone will include their child zones with regard to the occupancy numbers.



Include lower zone OFF

Include lower zone ON



To see the most recent information, click the Refresh button in the upper-right corner of the **Zone** pane.

### To view the violation history

Click **Anti-passback > Violation History**.



Click the Search button to refresh the list.

### To remove the APB violations

1. Click **Anti-passback > Violation Clear**.
2. Select the target users to release from the list.



Click the Search button to refresh the list.

3. Click **Release**.

### To exempt users from the APB rule

1. Click **Anti-passback > Bypass User**.
2. Click **Add** and select users that you will add to the exception list on **User List**.
3. Click **Save > Save** to apply changes.

## 4.2.5. Setting up Wiegand Control

If a supported device provides Wiegand connections for external card reader or door controller, you can do the Wiegand configuration of the device to send out Wiegand OUT data correctly by using CMID Manager V2.

The supported Wiegand format may vary depending on the device. For example, the EF-45 supports the following data format:



- Wiegand IN: 34 bits (32 bits for ID + 2 parity bits) without Facility bits which are fixed and unchangeable.
- Wiegand OUT: all available formats supported including 26bits and 34 bits

1. Click **Access Control** on the main window.
2. Select a device to set up on the left **Device List** pane.
3. Click the **Set-up Door Control** tab.
4. On the **Wiegand Control** group, in the **Signal** area, type the pulse width and pulse interval values of Wiegand IN/OUT devices such as external RF card reader (IN) and Access Control Unit (OUT) in the **Input/Output** boxes.



For more information about the pulse values, refer to Wiegand IN/OUT device specifications.

5. Type **Total Bits**, **Facility Bits**, and **Facility Code** and Click **Settings**.

*Example 1. How to Set Up Bits (Total Bits = 26, Facility Bits = 8, Facility code = 1, Parity bits)*

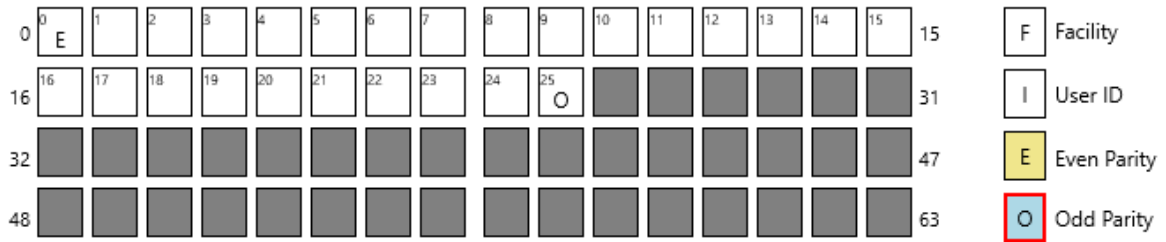
- a. Type the values as shown below and click **Settings**.

Total Bits  Facility Bits  Facility Code

- b. Click **E** and click the first digit **0** to set the even parity.

0	E	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	15	<input type="checkbox"/> Facility
16																	31	<input type="checkbox"/> User ID
32																	47	<input checked="" type="checkbox"/> Even Parity

- c. Click **O** and click the last digit **25** to set the odd parity.



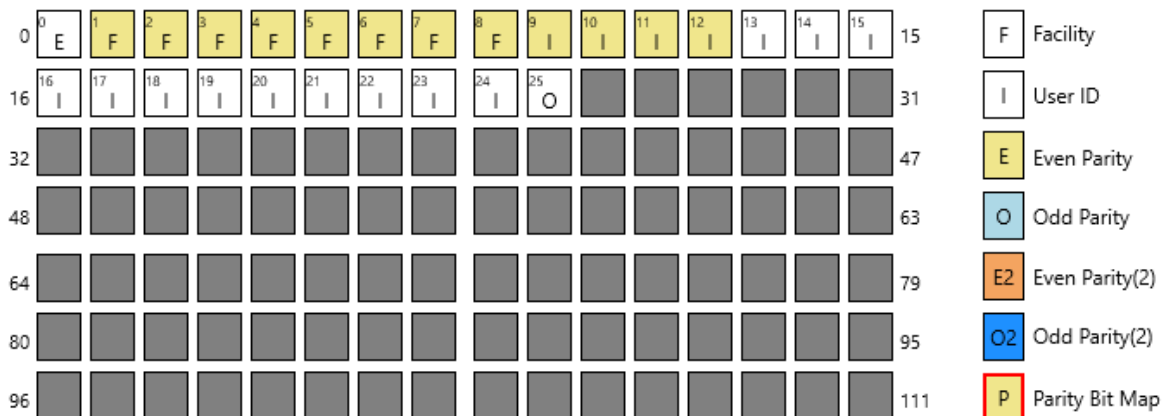
d. Click **F** and click the first 8 digits from **1** through **8** to set the facility bits.



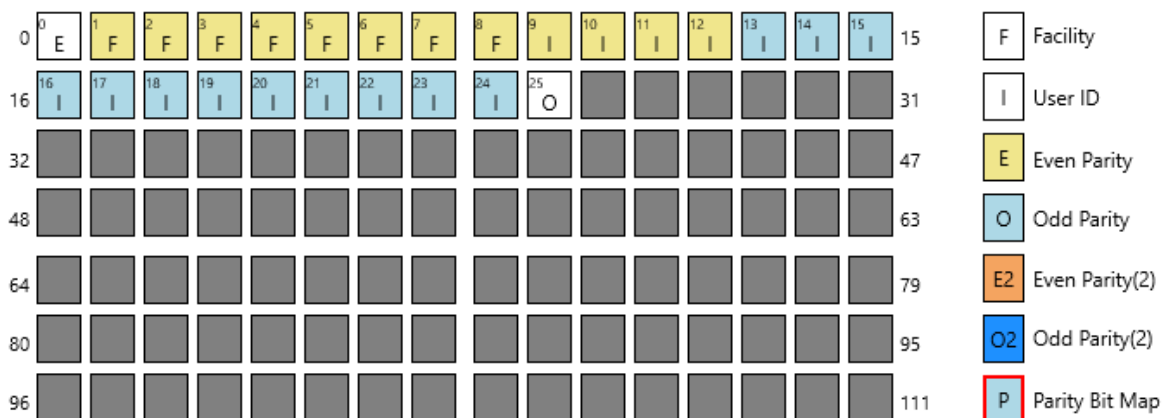
e. Click **I** and click the rest 16 digits (= 26-2-8) from **9** through **24** to set User ID bits.



f. Click **P** to enable parity write mode and click the first half 12 digits except even parity bit.



g. Click **P** again and click the last half 12 digits except odd parity bit.







Alternatively, you can just click **Default set 26Bits** or **Default set 34Bits** to load commonly used Wiegand configuration.

You can also modify the default 26bits or 34bits format as needed.

For example, if you want to remove the Facility bits completely and replace them with ID bits in the default 26 bits format, do the steps that follow:

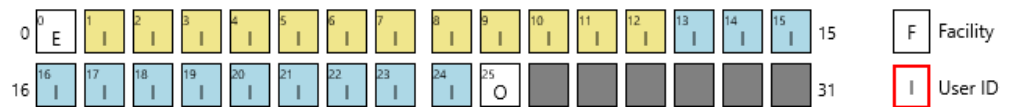
1. Click **I** to enable **User ID** write mode.



2. Click **F** (No.1 - No.8) to replace them with **I**.



3. The Facility bits are replaced with User ID bits.



6. Click **Apply** > **Yes** to write changes to device.

## 4.3. Using Time & Attendance




This section gives the information about advanced T&A event management, T&A report generation, and overtime management.





### 4.3.1. Viewing T&A Events

To view the T&A events by device, access group, and location

1. Click **T&A** on the main window.
2. Select an event view option as follows:
  - Select a department see the event list by department.
  - Select a user to see the event list by user.
  - Click **User Profile** to see all the T&A events.

The descriptions of the items that appear on **Attendance List** and **Individual List** are as follows:

Name	Description
Date	Shows the date when the events occurs
Name	Shows the name of the attendee
Department	Shows the department that the user belongs to
Clock-in	Shows the check-in time of the user
	 <p>CMID Manager V2 records the employee's first recognition time for the day as <b>Clock-in</b> time automatically.</p>
Clock-out	Shows the check-out time of the user
	 <p>CMID Manager V2 records the employee's last recognition time for the day as <b>Clock-out</b> time automatically.</p>
Work Status	Shows the attendance status of the user for the day such as On-time, Late, and Not-yet
	 <p>On flextime rule, the status shows <b>On-time</b> always because it allows flexible arrival and departure.</p>
Working Time	Shows the total amount of working of the user excluding the exception time, the break time, and the overtime.

Name	Description
Exception Time	Shows the total amount of exception time defined in the exception rules
Overtime (Attendance List)	Shows the amount of time during which the user stayed at work later than the designated check-out time for the day
	 <p>On flextime rule, <b>Overtime</b> shows the amount of time during which the user stayed at work longer than the designated <b>Working hours per day</b> in the work time rule (See <a href="#">3.5.1 Adding Work Time Rule</a>).</p>
Overtime (Individual List)	<ul style="list-style-type: none"> <li>• If you configured the <b>Over</b> time interval on <b>Work Rule &gt; Time Settings</b>, it shows the total amount of work time that pertains to the <b>Over</b> time.</li> <li>• If not, it indicates the same information as <b>Overtime</b> on <b>Attendance List</b>.</li> </ul>
Early Time (Individual List)	Shows the amount of work time that pertains to the <b>Early</b> time
	 <p><b>Early Time</b> shows the values only when you configured <b>Early</b> time interval on <b>Work Rule &gt; Time Settings</b>.</p>
Midnight Time (Individual List)	Shows the amount of work time that pertains to the <b>Midnight</b> time
	 <p><b>Midnight Time</b> shows the values only when you configured <b>Midnight</b> time interval on <b>Work Rule &gt; Time Settings</b>.</p>
Break Time	Shows the amount of time when the user took time off from work during the working hours due to coffee breaks, personal calls, and so on.
	<p>The break time needs to be entered by employees manually (Login Required).</p>  <ol style="list-style-type: none"> <li>1. Click in the empty area or click the time under the <b>Break Time</b> row. The <b>Edit Break Time</b> window appears.</li> <li>2. Click the plus button.</li> <li>3. Select the break start and end time, type the break type, and click <b>Save</b>.</li> </ol>

Name	Description
Valid Time	Shows the total amount of working time of the user excluding the exception time and the break time (Overtime hours are included)
Total	Shows the total amount of time when the user stayed at work for the day from <b>Clock-in</b> to <b>Clock-out</b> including all kinds of downtime



If the working type is **Fixed**, it indicates the total amount of time from the defined **Clock-in** time in **Fixed Time Settings** through the employee's last recognition time for the day.

### To view the T&A events that occurred within a certain period of time

1. Click the left **Calendar** button in the upper-right corner of the **Attendance List** and select a start date.
2. Click the right **Calendar** button and select an end date. Or select a period type in the drop-down list box - **Daily, Weekly, Monthly, or Custom**.

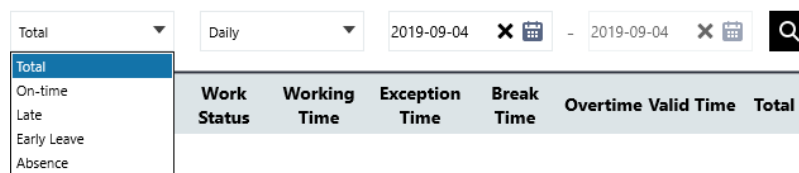


The maximum date range is one year.

3. Click the **Search** button to view the T&A events that happened during that period.



You can also view Attendance List only by a specified work status such as **On-time, Late, Early Leave, or Absence**.



### To sort the T&A events by various information - Date, Name, and Department

- Click the arrow next to each item title to switch between ascending sort order and descending sort order.

## Modifying Worktime Manually

You can change check-in or check-out time of an employee for a day if necessary.



1. Click a value to modify under **Clock-in** or **Clock-out**. The **Edit Time** window appears.
2. Enter a new time value for **Clock-in** or **Clock-out**.
3. Click **Save** to apply.
4. The value that you change manually appears on the list in red.

## To retrieve the list of users who worked more than a certain amount of time by the week

1. Click the **Weekly List** tab next to **Attendance List**.
2. Type a value in the **Working Hour** box and select **Excess**.



You can select **Under** to get the list of users who worked less then the working hours. If you select **Total**, all the employees appear in the list regardless of how long they work in the week.

3. Click the **Calendar** button and select a day that belongs to the week.



You can move through the weeks by clicking the **Right** or **Left arrow** button.

4. Click the **Search** button to view the records that match the condition.

## To get an overview of monthly T&A status by individual or department

1. Click the **Monthly List** tab.
2. Select a user or a department or a company to look up on the left **User Profile** pane.
3. The T&A information of the month appear in the calendar view.



- When selecting a user, the T&A status of each day includes **T&A** (clock-in time - clock-out time), **Working Status**, **Working Time**, **Overtime**, and **Total**.
- When selecting a department or a company, the T&A status of each day includes **On-time**, **Late**, **Early leave**, **Not yet**, and **Total** count. You can see the more information by clicking each number.

4. To search for another month, click the **Arrow** buttons or select a month in the **Calendar** button, and then click the **Search** button.

## To see more information about individual T&A

1. Click the **Individual List** tab.
2. Select a period type in the drop-down list box – **Daily, Weekly, Monthly, or Custom**.



The maximum date range is one year.



Select the **Include Extra Hour** checkbox to view the T&A information with hourly rate applied, if any. When selected, total work time shown on the list might be increased or decreased depending on the rate.

3. Click the **Search** button to view the T&A events that happened during that period.

### 4.3.2. Exporting T&A Events

You can save the T&A events in a delimiter-separated file format (for example, csv, txt, xlsx).

1. Select a department or a user by which you will export the T&A events on the **User Profile**.
2. Click **Export** in the lower-right corner of the **Attendance List** screen.
3. Select a file format in **File Type**. Type a delimiter in **Separator**.



- A separator is necessary only when you select *csv* or *text* as a file type.
- You can type a delimiter character such as *comma( , )*, *colon( : )*, *semi-colon( ; )*, and *pipe( | )* in the **Separator** box.

4. Click the **Search** button in **File Name** section.
5. In the **Save As** dialog box, locate the file path and enter the file name and click **Save**.
6. Click **Export > Done** to complete the export.

### 4.3.3. Managing Overtime

Many nations regulate overtime by law to dissuade or prevent employers from compelling their employees to work excessively long hours. If your country is governed by the maximum working hours law that does not allow the employee to work more than the level specified, you need to manage overtime hours.

The CMID Manager V2 provides ways to keep the working hours under the weekly limit mandated by legislation. For example, the multiple notifications indicating current overtime status through device display and pop-up window serve as reminders for administrators and users.

## Setting Maximum Working Hours

1. Click **T&A** on the main window.
2. Click **Weekly Working Hour Setting** in the lower-left corner of the window.
3. Type the weekly limit hour value in **Max. Working hour** and an hour value when the reminder starts to work in **Alert Start-time**.



For example, if you type 48 in **Max. Working hour** and 45 in **Alert Start-time**, the reminders start to work when an employee's working hours in a week reach 45 hours and to show that how much he or she has worked overtime for the week and how much time left till 48 hours limit.

## Adding T&A Devices

A T&A device gives the additional information about overtime to users on its display when an authentication is done. To assign the registered devices for T&A devices, do the steps that follow:

1. In **T&A Device Setting**, select devices that you want to use for T&A devices in the left **Devices** pane.
2. Click the right arrow to add. The selected devices appear in the right **T&A Devices** pane.
3. Click **Save** to apply.



If you will have the pop-up window notification, select the **Alarm Popup** box under **Alarm Popup** and type the pop-up window duration time in **Auto Close(second)**. Selecting the **Sound** check box allows you to choose and to play a sound file along with a pop-up window.

1. Select the **Sound** box.
2. Click the **Search** button and locate a sound file with .wav file extension, and then click **Open**.
3. Click **Apply**.

## 4.4. Managing Users

This section gives the information about user management including modifying user profile and exporting user data.

### 4.4.1. Viewing and Updating User Information

You can view the user list together by department and look up or update user information individually.

1. Click **User** on the main window.
2. Select a user view option as follows:
  - Select a department to see the user list by department.
  - Select a user name to look up the advanced user information.
  - Click **User Profile (n)** to view all the user list.
3. If necessary, you can update the user information in the **Advanced User Information** window.



For more information about Advanced User Information, see [3.3.1. Registering a User](#).

You can sort the user list by various information - **ID, Name, Department, Title, and Employment Date**.

- Click the arrow next to each item title to switch between ascending sort order and descending sort order.



#### How to identify the users who have biometric information in the list

Sometimes you need to check whether a user is registered with biometric data. You can sort the user list by biometrics by clicking the arrow next to **Iris**.

Date of Entry▼	Card No.	Iris▼
2017-04-21		Y



## 4.4.2. Exporting Users

The CMID Manager V2 lets you do the two types of user export: user list export and user transfer. The "user list export" saves the user list as a file and the "user transfer" transfers users from the software database to other devices over the network.

### Exporting User List

The user list export function allows you to save the existing user list as a delimiter-separated file (for example, csv, txt, xlsx).



Supported fields are "ID", "Name", "Department", "Title", "Phone number", "Authentication Period", "Employment Date".

1. Click **User** on the main window.
2. Click **User Profile** on the left pane to export all the users or  
 Select a department name to export the users in a particular department.
3. Click **Export** in the lower-right corner of the screen.
4. Select a file format in **File Type**. Type a delimiter in **Separator**.



- A separator is necessary only when you select *csv* or *text* as a file type.
- You can type a delimiter character such as *comma( , )*, *colon( : )*, *semi-colon( ; )*, and *pipe( | )* in the **Separator** box.

5. Click the **Search** button in **File Name** section.
6. In the **Save As** dialog box, locate the file path and enter the file name and click **Save**.
7. Click **Export > Done** to complete the export.

### Transferring User Data to Devices

The user transfer function gives you the ability to add the users stored in the software database to other devices at once.

1. Click **Device** on the main window.
2. Click **Transfer and Upgrade** in the lower-left corner of the window.
3. Click **User Transfer**.
4. Select the destination devices for export in the **Devices** pane.
5. Select the users who you will export in the **Employees** pane.



If you want to delete the existing users in the devices, select **Clear users in device before transferring**.



If the application version of the destination device is *1.2.56* or later, you must select **Clear users in device before transferring** before export.

To check the application version of the device, click **Device > Device List**. You can look up the device application version under **App Ver** in the device list.

6. Click **Transfer > Yes** to start export. The transfer status window appears.
7. When the data transfer is completed, click **Close**.

### 4.4.3. Deleting Users

You can unregister multiple users as follows.

1. Click **User** on the main window.
2. Click **Remove User** in the bottom.
3. Select the users to delete in the **User List**.
4. Click **Delete > Yes** to complete the task.

### 4.4.4. Restoring Users

You can easily restore the deleted users without registering the users again.

1. Click **User** on the main window.
2. Click **Restore User** in the bottom.
3. Select the users to restore in the **Deleted User List**.



If you will delete the users permanently, click **Permanently Delete > Yes**.

4. Click **Save** to complete user restoration.

## 4.4.5. Protecting Personal Data of Inactive Users

When you register a user using the software, the user information is stored within the database on premises. It contains sensitive personal data including some identification information that has the security risk of a data breach. According to the related regulations about data protection, such as GDPR, personal data must be kept and restricted to the minimum needed to do the job. Given that the stale and idle but still retained personal data would attract malicious individuals (hackers or rogue employees) in abusing and monetizing the data, you should minimize the data by deleting the user information that is not in use for a certain period of time.

1. Click **Settings > System**.
2. Under **Privacy Protection (Personal data lifecycle)**, select the target data



Two options are allowed to select: "**User data** and **Access event logs**" or "**Access event logs** only".

3. Type a value in **Lifecycle** and select a time unit from the list — **Days**, **Weeks**, or **Months**.



For example, if you type **6** and select **Months**, the personal data of users that have no access record for the past six months will be erased permanently after the six months.

4. Click **Apply**.

## 4.5. Managing Devices

This section gives the information about the advanced device management such as updating device settings and upgrading device firmware.

### 4.5.1. Viewing Device Information

The CMID Manager V2 gets up-to-date device information from each device automatically. You can view the device list together by access group, door or look up each device information individually.

1. Click **Device** on the main window.
2. Select a device view option as follows:
  - Select an access group to see the device list by group.
  - Select a device name to look up the advanced device information.
  - Click **Location** tab on the **Device List** pane and select a door to see the device list by location.
  - Click **Device List** to view all the device list.

You can sort the device list by various information - **Device Type, Device Name, IP Address, Port, SN, Enabled, and Version.**

- Click the arrow next to each item title to switch between ascending sort order and descending sort order.

### 4.5.2. Exporting Device List

The device list export function allows you to save the existing device list as a delimiter-separated file (for example, csv, txt, xlsx).

1. Click **Device** on the main window.
2. Click **Device List** on the left pane to export all the users or
 

Select an access group to export the devices in a particular group.
3. Click **Export** in the lower-right corner of the screen.
4. Select a file format in **File Type**. Type a delimiter in **Separator**.



- A separator is necessary only when you select *csv* or *text* as a file type.
- You can type a delimiter character such as *comma( , )*, *colon( : )*, *semi-colon( ; )*, and *pipe( | )* in the **Separator** box.

5. Click the **Search** button in **File Name** section.
6. In the **Save As** dialog box, locate the file path and enter the file name and click **Save**.
7. Click **Export** > **Done** to complete the export.

### 4.5.3. Updating Device Information

You can update almost all the types of device configuration within CMID Manager V2 without attending to the device physically.



If it takes too long to read device information, check your network environment and settings. Using a proxy server, for example, may make the retrieving slower. Contact your network administrator for more information.

#### To update basic configuration

1. Click **Device** on the main window.
2. Select a device for configuration.
3. Click **Basic information** and change the settings depending on your need.
4. Click **Register** > **Yes** to apply changes to device.

#### To update advanced configuration

1. Click **Device** on the main window.
2. Select a device for configuration.
3. Click **Additional information** and change the settings depending on your need.



- Click **Refresh** to get the updated information from the device.
- Click **Default** to cancel changes and restore the default setting.



For more information about advanced device settings including the description for each item, see [Appendix A: EF-45 Advanced Settings Reference](#).

4. Click **Apply** > **Yes** to apply changes to device.

## 4.5.4. Upgrading Device Firmware

The CMID Manager V2 provides the method to upgrade the firmware in multiple devices at once over the network.

1. Click **Device** on the main window.
2. Click **Transfer and Upload** in the lower-left corner of the window.
3. Click **Firmware Upload**.
4. Select the destination devices for upgrade in the **Devices** pane.
5. Click the **Search** button in the **Firmware** pane.



Select the **Force** box to downgrade the firmware or write the same version of firmware again.

6. In the **Load firmware from** dialog box, locate the firmware file and click **Open**.
7. Click **Upload > Yes** to start firmware upgrade. The **Upload Firmware** window that shows the progress bars appears.
8. When completed, click **Close** to close the window.

## 4.5.5. Transferring Device Settings to Other Devices

When you add a new device to the software, you may want it to have the same settings as the existing device. In this case, you can make a copy of one device settings and use it as a template for other devices.

1. Click **Device** on the main window.
2. Select a source device in the device list.
3. Click **Copy settings** on the right pane.
4. Select destination devices and setting types for copying.



For more information about device setting types, see [Appendix A: EF-45 Advanced Settings Reference](#).

5. Click **Save** to finish. The destination devices will reboot automatically to apply changes.

## 4.5.6. Uploading Screensaver to Devices

You can upload a screensaver to devices by using the CMID Manager V2.



The supported image file format is PNG only and the size must be 854x420 in pixels

1. Click **Device > Transfer and Upload > Screen Saver Upload**.
2. Select the destination devices on the left pane. Locate and open a screensaver file on the right pane.
3. Click **Upload** to apply.

## 4.5.7. Setting up Tamper on Devices

This feature allows you to set the secure tamper protection on multiple devices. If you need all the data and settings to be deleted permanently in devices when a physical tampering is attempted, do the steps that follow:

1. Click **Device > Transfer and Upload > Tamper Setting**.
2. Select the destination devices on the left pane and click the button under **Secure mode** to enable the secure tamper on the right pane.
3. Click **Transfer** to apply.

## 4.6. Managing Rules

This section gives the information about how to apply the various rules about worktime, downtime, and holidays.



Before managing rules, you must create the rules first. See [3.5. Adding Rules](#) for more information.

### 4.6.1. Viewing and Updating Rule Information

You can view the rule list together by type and look up or update rule setting individually.

1. Click **Rules** on the main window.
2. Select a rule view option as follows:
  - Select a rule type such as **Work rules**, **Exception rules**, **Holiday rules**, **User schedule rules**, **Device schedule rules**, and **Work schedule rules** to see the rule list by type.
  - Select a rule name to look up the rule information.
  - Click **Rules** to view all the rule list.
3. If necessary, you can update the rule setting in the **Work Rule** window.

### 4.6.2. Applying Rules

To make rules work, you need to apply the rules to your company, departments, and users. **Day Work** is selected as default company rule and can be changed to other rules. You can assign rules to various targets and in various ways.

Here is the description of how the rules work:

- The company work rule is applied to all the employees and departments by default.
- If you create and apply a work rule to a department, the department rule takes precedence over the company rule. The department members are subject to the department work rule.



If you create departments in multiple levels, the lower level department rule is applied first.

- If you create and apply a work rule to an individual, the individual rule takes precedence over both the company rule and the department rule that the user belongs to. The user is subject to the individual work rule.



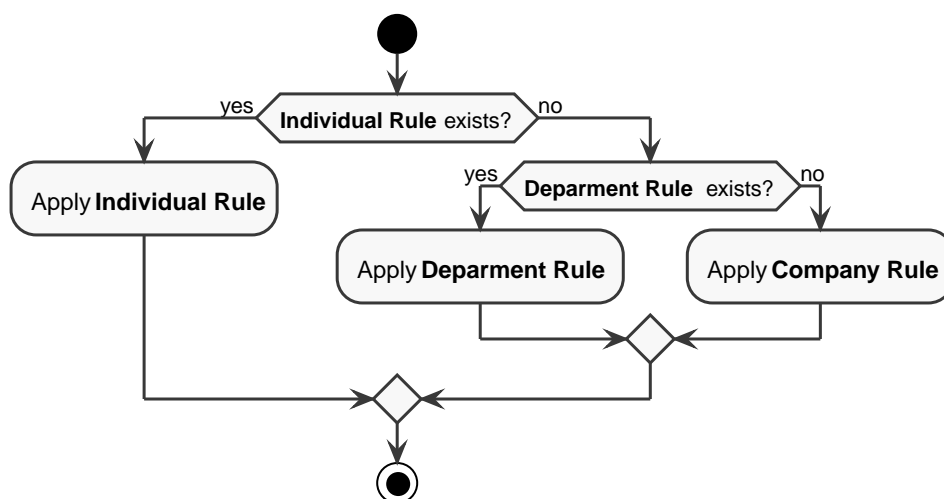


Figure 11. Applying Rules Priority

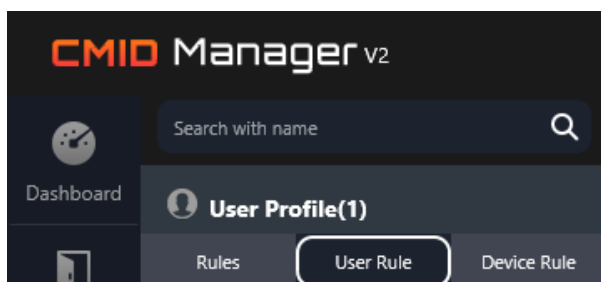


The only rule type that you can apply to departments or individuals selectively is the **Work rule**. The **Exception rule** and **Holiday rule** are required to apply to all the employees when created.

## Applying Department Rules

To apply rules to departments, do the steps that follow:

1. Click **Rules** on the main window.
2. Click **User Rule** tab.



3. Select a department to open **Work Rule by Department** window.
4. Select days that you will apply a work rule on the calendar pane.



- To select all the days in the month, select **Select all working days** box in the upper-left corner of the calendar pane.
- To change month or year, click the **Calendar** button (📅) in the upper-right corner of the pane and select a month or a year.

5. Click a work rule on the **Entire working rules** pane. The new work rule bar appears on the second row below the company work rule bar by the days selected.

6. Click **Save** to apply.

**To apply a work rule to a department on all the work days regardless of month or year,**

1. Click the **Search** button in the **Default Work Rule** box in the upper-right corner of the screen.



2. Click a work rule. The new work rule appears on the second row below the company work rule bar.
3. Click **Save** to apply.
4. To unapply, click the **Cross (X)** button.

To delete the rule from the department, do the steps that follow:

1. Select days that you will delete the work rule on the calendar pane.
2. Click **Delete rule** on the **Entire working rules** pane.
3. Click **Save** to apply.



The default company work rule cannot be deleted.

## Applying Individual Rules

To apply rules to individuals, do the steps that follow:

1. Click **Rules** on the main window.
2. Click **User Rule** tab.
3. Select a user to open **Work Rule by User** window.



If you already applied a work rule to the department that the user belongs to, the department rule as well as the company rule appears on the user work schedule calendar.

4. Select days that you will apply a work rule on the calendar pane.



- To select all the days in the month, select **Select all working days** box in the upper-left corner of the calendar pane.
- To change month or year, click the **Calendar** button in the upper-right corner of the pane and select a month or a year.

5. Click a work rule or absence events such as personal leave (**Day-Off**), vacation (**Vacation**), and business travel (**Business Travel**) in the **Entire working rules** pane. The new work rule or event bar appears on the third row on the selected days.



A newly added individual rule will overwrite the existing individual rule. Thus, if you will add both work rule and absence event for an individual, you should add the work rule first and personal absence events later in most cases.

6. Do the step 4 and 5 until you complete applying individual rules and events.
7. Click **Save** to apply.

### To apply a work rule to a person on all the work days regardless of month or year,



1. Click the **Search** button in the **Default Work Rule** box in the upper-right corner of the screen.
2. Click a work rule. The new work rule appears on the third row below the company work rule bar or the department work rule bar.
3. Click **Save** to apply.
4. To unapply, click the **Cross** (X) button.

To delete the rule from the individual, do the steps that follow:

1. Select days that you will delete the work rule on the calendar pane.
2. Click **Delete rule** on the **Entire working rules** pane.
3. Click **Save** to apply.



The default company work rule and the department rule, if any, cannot be deleted.

## Applying User Schedule Rule

Because the user schedule rule does not have to do with T&A, but Access Control, it does not affect the existing department rules and individual rules in any way that are applied to the user. To apply a user schedule rule to a user, do the steps that follow:



There are two types of access control schedule rule—User schedule rule, Device schedule rule. The device schedule rule takes precedence over the user schedule rule when they conflict with each other.

1. Click **Rules** on the main window.
2. Click **User Rule** tab.
3. Select a user and click the **Schedule Rule** tab next to the **Work Rule** tab.
4. Select days that you will apply a user schedule rule on the calendar pane.



- To select all the days in the month, select **Select all days** box in the upper-left corner of the calendar pane.
- To change month or year, click the **Calendar** button in the upper-right corner of the pane and select a month or a year.

5. Click a user schedule rule on the **Entire user schedule rules** pane. The new schedule rule bar appears on the third row by the days selected.



When a user schedule rule is applied, the existing rule will be always replaced with the new rule.

6. Click **Save** to apply.



**To apply a user schedule rule to a user on all the work days regardless of month or year,**

1. Click the **Search** button in the **Default User Schedule Rule** box in the upper-right corner of the screen. The weekly or cycle-based rules will be listed.
2. Click a user schedule rule. The new work rule appears on the third row replacing the existing one, if any.
3. Click **Save** to apply.
4. To unapply, click the **Cross (X)** button.

To delete the rule from the user, do the steps that follow:

1. Select days that you will delete the work rule on the calendar pane.
2. Click **Delete rule** on the **Entire user schedule rules** pane.
3. Click **Save** to apply.

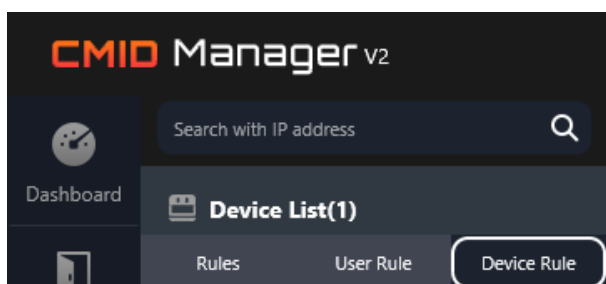
## Applying Device Schedule Rule

To apply a device schedule rule to a device, do the steps that follow:



There are two types of access control schedule rule—User schedule rule, Device schedule rule. The device schedule rule takes precedence over the user schedule rule when they conflict with each other.

1. Click **Rules** on the main window.
2. Click **Device Rule** tab.



3. Select a device.
4. Select days that you will apply a device schedule rule on the calendar pane.



- To select all the days in the month, select **Select all days** box in the upper-left corner of the calendar pane.
- To change month or year, click the **Calendar** button in the upper-right corner of the pane and select a month or a year.

5. Click a device schedule rule on the **Entire device schedule rules** pane. The new schedule rule bar appears on the third row by the days selected.



When a device schedule rule is applied, the existing rule will be always replaced with the new rule.

6. Click **Save** to apply.



**To apply a device schedule rule to a device on all the work days regardless of month or year,**

1. Click the **Search** button in the **Default Device Schedule Rule** box in the upper-right corner of the screen. The weekly or cycle-based rules will be listed.
2. Click a device schedule rule. The new work rule appears on the third row replacing the existing one, if any.
3. Click **Save** to apply.
4. To unapply, click the **Cross (X)** button.

To delete the rule from the device, do the steps that follow:

1. Select days that you will delete the work rule on the calendar pane.
2. Click **Delete rule** on the **Entire device schedule rules** pane.
3. Click **Save** to apply.

### 4.6.3. Applying Shift Work Rule

In this section, you will learn how to set up your shift work schedule through CMID Manager V2 by an example. Before you begin, you need to design a reasonable shift schedule depending on your work environment.

#### Introducing Sample Shift Schedule

This guide assumes that you have the following shift schedule:

- **Number of crews:** 4 (A, B, C, D)
- **Shift system:** 2W:2F, where W represents work days and F represents free days
- **Shift length:** 12 hours (that is, two shifts within a day – day shift, night shift)
- **Shift change time:** Day shift from 6 a.m. to 6 p.m., Night shift from 6 p.m. to 6 a.m.
- **Cycle length:** 4 days
- **Shift plan** (that is, the sequence of work and free days) for each crew: DNOO NOOD ODNO OODN, where DNOO represents day shift (D), night shift (N), and days off (O) respectively

The following tables demonstrate how the example shift schedule is weekly organized.

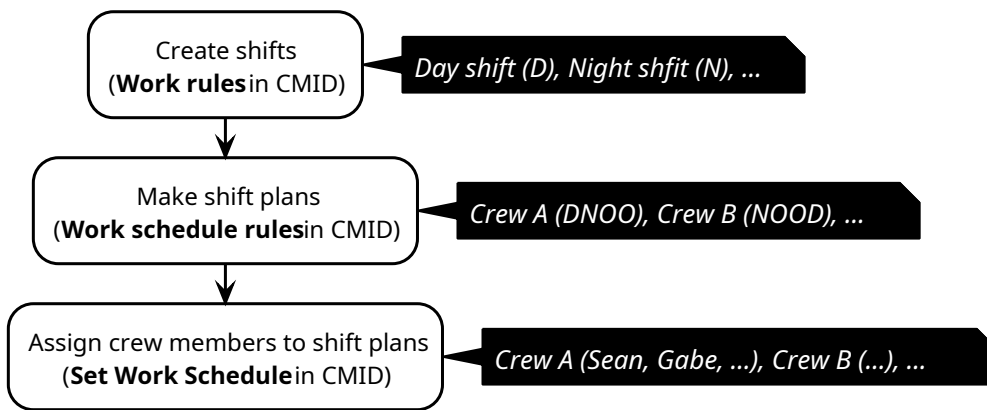
Time	Week1				Week2				Week3				Week4											
	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun			
D (0600-18:00)	A	C	D	B	A	C	D	B	A	C	D	B	A	C	D	B	A	C	D	B	A	C	D	B
N (1800-06:00)	B	A	C	D	B	A	C	D	B	A	C	D	B	A	C	D	B	A	C	D	B	A	C	D

Figure 12. Shift plan example by time (12-hour, 4-crews, 4-days)

Crew	Week1				Week2				Week3				Week4											
	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun			
A	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O
B	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D
C	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O
D	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N	O	O	D	N

Figure 13. Shift plan example by crew (12-hour, 4-crews, 4-days)

The workflow is shown in the following figure.



## Creating Shifts

To add a shift, you have to create a work time rule in CMID. In the preceding example, two shifts need to be added. For more information, see [3.5.1. Adding Work Time Rule](#).



The following steps are presented as an example and intended to help your understanding. Actual configurations and procedures may vary depending on your shift schedule.

1. Add a day shift (06:00–17:59) as shown in the figure.

### Work Rule

<b>Work Rule Name</b> *	Day Shift	<b>Color</b>	<span style="background-color: red; color: white; padding: 2px;"> </span>																																																
<b>Rule Type</b> *	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc;"> <div style="background-color: #0056b3; color: white; padding: 5px; text-align: center; width: 15%;">Work rule</div> <div style="background-color: #e0e0e0; padding: 5px; text-align: center; width: 15%;">Exception rule</div> <div style="background-color: #e0e0e0; padding: 5px; text-align: center; width: 15%;">Holiday rule</div> <div style="background-color: #e0e0e0; padding: 5px; text-align: center; width: 15%;">Device schedule rule</div> <div style="background-color: #e0e0e0; padding: 5px; text-align: center; width: 15%;">User schedule rule</div> <div style="background-color: #e0e0e0; padding: 5px; text-align: center; width: 15%;">Work schedule rule</div> </div>																																																		
<b>Comments</b>	<input type="text" value="Comments"/>																																																		
<b>Working Type</b> *	<input checked="" type="radio"/> Fixed <input type="radio"/> Flexible	<b>Day Start Time</b> *	04 : 00																																																
<b>Fixed Time Settings</b> *	Clock-in - Clock-out	06 : 00 - 17 : 59																																																	
	Grace Time	In( min.)    In( min.)    Out( min.)    Out( min.)																																																	
<b>Time Settings</b> *	<div style="display: flex; justify-content: space-between; font-size: small;"> <span>Basic</span> <span>Over</span> <span>Early</span> <span>Midnight</span> <span>Exception</span> </div> <table border="1" style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td> </tr> <tr> <td style="background-color: #e0e0e0;"></td><td style="background-color: #e0e0e0;"></td><td style="background-color: #e0e0e0;"></td><td style="background-color: #e0e0e0;"></td><td style="background-color: #90ee90;"></td><td style="background-color: #90ee90;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #ff0000;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #00b0f0;"></td><td style="background-color: #008080;"></td><td style="background-color: #008080;"></td><td style="background-color: #e0e0e0;"></td><td style="background-color: #e0e0e0;"></td><td style="background-color: #e0e0e0;"></td><td style="background-color: #e0e0e0;"></td> </tr> </table>			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23																								
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23																												
	<input type="button" value="Working time"/> <input type="button" value="Exception time"/>																																																		



2. Add a night shift (18:00–05:59) as shown in the figure.

**Work Rule**

<b>Work Rule Name</b> *	Night Shift		<b>Color</b>	[Blue]																																													
<b>Rule Type</b> *	<input checked="" type="radio"/> Work rule <input type="radio"/> Exception rule <input type="radio"/> Holiday rule <input type="radio"/> Device schedule rule <input type="radio"/> User schedule rule <input type="radio"/> Work schedule rule																																																
<b>Comments</b>	Comments																																																
<b>Working Type</b> *	<input checked="" type="radio"/> Fixed <input type="radio"/> Flexible		<b>Day Start Time</b> *	16 : 00																																													
<b>Fixed Time Settings</b> *	Clock-in - Clock-out		18 : 00 - 05 : 59																																														
	Grace Time		In( min.)	In( min.)	Out( min.)																																												
<b>Time Settings</b> *	<div style="display: flex; justify-content: space-between; font-size: small;"> <span>Basic</span> <span>Over</span> <span>Early</span> <span>Midnight</span> <span>Exception</span> </div> <table border="1" style="width: 100%; text-align: center; font-size: x-small;"> <tr> <td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td> </tr> <tr> <td colspan="6">Basic</td> <td colspan="2">Over</td> <td colspan="2">Early</td> <td colspan="2">Midnight</td> <td colspan="2">Exception</td> <td colspan="6"></td> </tr> </table>					0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Basic						Over		Early		Midnight		Exception							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23																									
Basic						Over		Early		Midnight		Exception																																					
Working time		Exception time																																															

## Making Shift Plans

A shift plan is the sequence of shifts and free days. To make a shift plan, you need to create a work schedule rule by determining the order of work rules and holidays in CMID. In the example shift schedule, you need to make four different work schedules (shift plans) with four cycles because the number of crews is four and the cycle length is four days. For more information, see [3.5.6. Adding Work Schedule Rule](#).

1. Make a plan for crew A as shown in the figure (DNOO).

### Work Rule

<b>Work Rule Name</b> *	Crew A	<b>Color</b>																																																																																																																														
<b>Rule Type</b> *	<input type="checkbox"/> Work rule <input type="checkbox"/> Exception rule <input type="checkbox"/> Holiday rule <input type="checkbox"/> Device schedule rule <input type="checkbox"/> User schedule rule <input checked="" type="checkbox"/> Work schedule rule																																																																																																																															
<b>Comments</b>	Comments																																																																																																																															
<b>Schedule Type</b> *	<input type="radio"/> Weekly <input checked="" type="radio"/> Daily	<b>Cycle</b> *	4																																																																																																																													
<b>Schedule Settings</b> *	<table border="1"> <thead> <tr> <th></th> <th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th> </tr> </thead> <tbody> <tr> <td>1 Day Shift</td> <td></td><td></td><td></td><td></td><td>Basic</td><td>Over</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td> </tr> <tr> <td>2 Night Shift</td> <td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td> </tr> <tr> <td>3 Holiday</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>4 Holiday</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </tbody> </table>				0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	1 Day Shift					Basic	Over	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	2 Night Shift	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	3 Holiday																									4 Holiday																								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23																																																																																																								
1 Day Shift					Basic	Over	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic																																																																																																								
2 Night Shift	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic																																																																																																								
3 Holiday																																																																																																																																
4 Holiday																																																																																																																																

2. Make a plan for crew B as shown in the figure (NOOD).

### Work Rule

<b>Work Rule Name</b> *	Crew B	<b>Color</b>																																																																																																																														
<b>Rule Type</b> *	<input type="checkbox"/> Work rule <input type="checkbox"/> Exception rule <input type="checkbox"/> Holiday rule <input type="checkbox"/> Device schedule rule <input type="checkbox"/> User schedule rule <input checked="" type="checkbox"/> Work schedule rule																																																																																																																															
<b>Comments</b>	Comments																																																																																																																															
<b>Schedule Type</b> *	<input type="radio"/> Weekly <input checked="" type="radio"/> Daily	<b>Cycle</b> *	4																																																																																																																													
<b>Schedule Settings</b> *	<table border="1"> <thead> <tr> <th></th> <th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th> </tr> </thead> <tbody> <tr> <td>1 Night Shift</td> <td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td> </tr> <tr> <td>2 Holiday</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>3 Holiday</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>4 Day Shift</td> <td></td><td></td><td></td><td></td><td>Basic</td><td>Over</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td><td>Basic</td> </tr> </tbody> </table>				0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	1 Night Shift	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	2 Holiday																									3 Holiday																									4 Day Shift					Basic	Over	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23																																																																																																								
1 Night Shift	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic																																																																																																								
2 Holiday																																																																																																																																
3 Holiday																																																																																																																																
4 Day Shift					Basic	Over	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Basic																																																																																																								

3. Make a plan for crew C as shown in the figure (ODNO).

**Work Rule**

<b>Work Rule Name</b> *	Crew C	<b>Color</b>																																																																																																																														
<b>Rule Type</b> *	<input type="button" value="Work rule"/> <input type="button" value="Exception rule"/> <input type="button" value="Holiday rule"/> <input type="button" value="Device schedule rule"/> <input type="button" value="User schedule rule"/> <input checked="" type="button" value="Work schedule rule"/>																																																																																																																															
<b>Comments</b>	<input type="text" value="Comments"/>																																																																																																																															
<b>Schedule Type</b> *	<input type="radio"/> Weekly <input checked="" type="radio"/> Daily	<b>Cycle</b> *	4																																																																																																																													
<b>Schedule Settings</b> *	<div style="display: flex; justify-content: space-around; font-size: small;"> <span> Basic</span> <span> Over</span> <span> Early</span> <span> Midnight</span> <span> Exception</span> </div> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th></th> <th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th> </tr> </thead> <tbody> <tr> <td>1</td> <td colspan="24">Holiday</td> </tr> <tr> <td>2</td> <td colspan="4">Day Shift</td> <td colspan="2">Early</td> <td colspan="4">Basic</td> <td colspan="1">Exception</td> <td colspan="4">Basic</td> <td colspan="2">Over</td> <td colspan="2">Day Shift</td> <td colspan="4"></td> </tr> <tr> <td>3</td> <td colspan="4">Night Shift</td> <td colspan="4">Basic</td> <td colspan="2">Over</td> <td colspan="4"></td> <td colspan="2">Early</td> <td colspan="4">Basic</td> <td colspan="1">Exception</td> <td colspan="4"></td> </tr> <tr> <td>4</td> <td colspan="24">Holiday</td> </tr> </tbody> </table>				0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	1	Holiday																								2	Day Shift				Early		Basic				Exception	Basic				Over		Day Shift						3	Night Shift				Basic				Over						Early		Basic				Exception					4	Holiday																							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23																																																																																																								
1	Holiday																																																																																																																															
2	Day Shift				Early		Basic				Exception	Basic				Over		Day Shift																																																																																																														
3	Night Shift				Basic				Over						Early		Basic				Exception																																																																																																											
4	Holiday																																																																																																																															

4. Make a plan for crew D as shown in the figure (OODN).

**Work Rule**

<b>Work Rule Name</b> *	Crew D	<b>Color</b>																																																																																																																														
<b>Rule Type</b> *	<input type="button" value="Work rule"/> <input type="button" value="Exception rule"/> <input type="button" value="Holiday rule"/> <input type="button" value="Device schedule rule"/> <input type="button" value="User schedule rule"/> <input checked="" type="button" value="Work schedule rule"/>																																																																																																																															
<b>Comments</b>	<input type="text" value="Comments"/>																																																																																																																															
<b>Schedule Type</b> *	<input type="radio"/> Weekly <input checked="" type="radio"/> Daily	<b>Cycle</b> *	4																																																																																																																													
<b>Schedule Settings</b> *	<div style="display: flex; justify-content: space-around; font-size: small;"> <span> Basic</span> <span> Over</span> <span> Early</span> <span> Midnight</span> <span> Exception</span> </div> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th></th> <th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th> </tr> </thead> <tbody> <tr> <td>1</td> <td colspan="24">Holiday</td> </tr> <tr> <td>2</td> <td colspan="24">Holiday</td> </tr> <tr> <td>3</td> <td colspan="4">Day Shift</td> <td colspan="2">Early</td> <td colspan="4">Basic</td> <td colspan="1">Exception</td> <td colspan="4">Basic</td> <td colspan="2">Over</td> <td colspan="2">Day Shift</td> <td colspan="4"></td> </tr> <tr> <td>4</td> <td colspan="4">Night Shift</td> <td colspan="4">Basic</td> <td colspan="2">Over</td> <td colspan="4"></td> <td colspan="2">Early</td> <td colspan="4">Basic</td> <td colspan="1">Exception</td> <td colspan="4"></td> </tr> </tbody> </table>				0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	1	Holiday																								2	Holiday																								3	Day Shift				Early		Basic				Exception	Basic				Over		Day Shift						4	Night Shift				Basic				Over						Early		Basic				Exception				
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23																																																																																																								
1	Holiday																																																																																																																															
2	Holiday																																																																																																																															
3	Day Shift				Early		Basic				Exception	Basic				Over		Day Shift																																																																																																														
4	Night Shift				Basic				Over						Early		Basic				Exception																																																																																																											

## Assigning Workers to Shift Plans

The last step is to add your crew members to each plan that they belong to.

1. Click **Rules** on the main window.
2. Click **Set Work Schedule** in the lower-left corner of the window.
3. On the left **Schedule** pane, click the target shift plan (schedule or crew).

By clicking the **Pencil** button on the right, you can edit additional settings for the schedule.



- **Start Day** is the start date of the schedule.
- **Holiday Use** means whether to allow the holiday break when a holiday comes on a work day.
  - "Y": The work team members don't have to work on the holidays.
  - "N": The work team members have to work regardless of the holidays.
- **Holiday Work** denotes the work rule that needs to be applied on their holiday work. Generally, it is a common practice that a holiday work rule has higher hourly rates than those of regular work rules when **Holiday Use** is Y.

4. On the right **Users in the schedule** pane, click the **Plus (+)** button.
5. On the **User list** that opens, select the crew members (users) and click **Apply**.
6. Click **Save**.
7. Do the same steps for other plans.

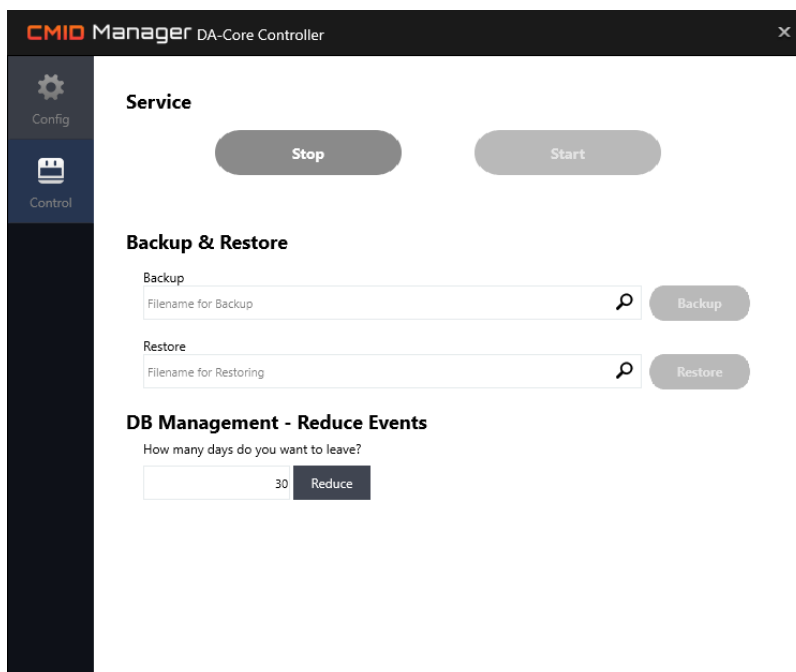
## 4.7. Backing Up/Restoring Database

The DA Core controller involves a built-in database backup/restore tool that lets you to perform a manual backup and restore against a data loss event or system reinstallation. There are various types of target data to work with such as user information, device information, and event logs.

### 4.7.1. Backing Up Database

To back up the current database, do the steps that follow:

1. Open **Control Panel** in Windows.
2. Select **Large icon** or **Small icon** in **View by** drop-down menu.
3. Click **CMV2 DA Core Controller (32-bit)** to run Device Agent Controller.
4. Click **Control** tab.



5. Click the **Search** button in the **Backup** area.
6. Locate a folder where you will save the backup file and type the name of the file.



The file extension (that is, *dbk*) and file name (with file creation date suffix) are generated automatically.

7. Click **Open** to select the file.

8. Click **Backup** and select data types to back up.

Select Target Group

√	Group Name	Total Records
<input type="checkbox"/>	System	5
<input type="checkbox"/>	Codes	55
<input checked="" type="checkbox"/>	Device	6
<input checked="" type="checkbox"/>	Employee	11
<input type="checkbox"/>	Event	0
<input type="checkbox"/>	System Log	11

Cancel
OK

9. Click **OK** whenever prompted to complete backup.

## Reducing Backup Time

If you have a large number of events in the database, it will take a quite long time for backup. By deleting old and unnecessary event records, you can speed up the backup process.

1. Under **DB Management - Reduce Events**, type a value in days.



If you type 60, the recent 60 days event records will be kept and the other older ones will be deleted.

2. Click **Reduce**.

## Backing Up Database Automatically

The automatic backup function allows you to create a backup file at a designated time and location.

1. On the CMID Manager main window, click **Settings > System**.
2. Under **CMV2 DB Backup**, click **Enable** to enable the function.
3. Complete the following forms about backup time and save location:

- Under **Remote PC Backup Folder(DA-Core)**, type the backup file save location of the PC where the DA Core is installed.
- Under **Backup Cycle**, type a value in **Cycle** and select a time unit from the list — **Days**, **Weeks**, or **Months**.



For example, if you type **3** and select **Days**, the first backup will start in three days from when you apply the changes and then the backup will be performed every three days periodically.

- Under **Backup Start Time**, select hours and minutes to specify the backup start time of the day.
- Under **Target**, select the data types to back up.

4. Click **Apply**.

## 4.7.2. Restoring Database

To restore the database, do the steps that follow:

1. Run DA-Core Controller.
2. Click **Control** tab.
3. Click the **Search** button in the **Restore** area.
4. Locate a folder where the backup file is stored and click the file.
5. Click **Open** to select the file.
6. Click **Restore** and select data types to restore under **Backup Information**.

Restore Options

**DB**

<b>IP</b> <input type="text" value="127.0.0.1"/>	<b>Database</b> <input type="text" value="CMID"/>
<b>User name</b> <input type="text" value="cmid"/>	<b>Password</b> <input type="password" value="*****"/>

**Backup Information**

	Group Name	Total Records
<input checked="" type="checkbox"/>	Device	6
<input checked="" type="checkbox"/>	Employee	11

7. Click **OK** whenever prompted to complete restore.



# Appendix A: EF-45 Advanced Settings Reference

This appendix gives the details about advanced setting menus of EF-45 device that include the functional description for each device configuration.





## A.1. Device Setting

The device setting contains the configurations about Biometrics, Access Control, and Audio.

### A.1.1. Device > Configuration

Item	Description
User Positioning Interface	Select a guide display UI when enrollment and recognition <ul style="list-style-type: none"> <li>• <b>Color Overlay:</b> Color overlay type guide UI display</li> <li>• <b>Box:</b> Tracking box type guide UI display</li> </ul>
Enroll notices timeout	Select notice time out time during enrollment process
Motion detection wait time	Select motion detection delay time from last recognition operating
Motion detection	Select motion detection enable/disable for starting recognition
Debug	Select Debug mode enable/disable that captures image stream for off-line analysis
Speaker volume	Select speaker volume for instruction sound and interphone voice
MIC volume	Select microphone volume for interphone voice
Power line frequency	Select power line frequency of device power supply

## A.1.2. Device > Bio

Item	Description
Security Level	<p>Select a combination mode of Face and Iris</p> <ul style="list-style-type: none"> <li>• <b>Face or Iris:</b> Two stages “Face or Iris” recognition mode</li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Face recognition first, and then automatic switch-over to Iris upon Face recognition non-match)</p> </div> <ul style="list-style-type: none"> <li>• <b>Face only:</b> Face only recognition mode</li> <li>• <b>Iris only:</b> Iris only recognition mode</li> <li>• <b>Face and Iris:</b> Face and Iris recognition mode</li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>The EF-45 reader captures Iris and Face at the same time from the Iris capture distance. If it finds the matches both in Iris and Face of the user, it will grant access to the user.</p> </div> <ul style="list-style-type: none"> <li>• <b>Iris first and Face:</b> One stage “Face or Iris” recognition mode for faster recognition</li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>The EF-45 reader captures Iris and Face at the same time from the Iris capture distance. If it finds a match in Iris or Face of the user, it will grant access to the user.</p> </div>
Cover glass IR transmission(%)	<p>Adjusts IR transmission attenuation if a cover glass is in front of the EF-45</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Do not change this value unless advised to do so</p> </div>

## Device > Bio > IRIS

Item	Description
Enroll iris usable area (%)	Select usable area for Iris enrollment
Recog false accept rate	Select false accept rate for Iris recognition
Fast recog mode	Select enable/disable for fast recognition mode

Item	Description
Recognition: allow either eye	Select enable/disable for either eye recognition mode
Enroll: allow either eye	Select enable/disable for either eye enrollment mode
Min distance(cm)	Select min distance for Iris recognition

## Device > Bio > Face




Item	Description
Fake face	Select enable/disable fake face detection (For example, face photo)






With Fake face enabled, it may take a little more time to recognize face than when disabled

## A.1.3. Device > Door

Item	Description
Relay	Select a relay type <ul style="list-style-type: none"> <li>• <b>Not used:</b> Relay not used</li> <li>• <b>Internal Relay:</b> EF-45's internal relay</li> <li>• <b>Smart Relay:</b> External relay</li> <li>• <b>Common Relay:</b> Common relay</li> </ul>
Relay ID	Type Relay ID when using Smart Relay
Driven by	Select an event mode for door open relay <ul style="list-style-type: none"> <li>• <b>All Events:</b> Door opens for all events</li> <li>• <b>Authentication:</b> Door opens for authentication event</li> <li>• <b>T&amp;A Event:</b> Door opens for T&amp;A event</li> <li>• <b>Authentication + T&amp;A Event:</b> Door opens for authentication plus T&amp;A event</li> <li>• <b>Disabled:</b> Door open events disabled</li> </ul>
Duration (sec)	Select time duration for door open relay operation

Item	Description
RTE(Exit button)	Select an option for Door exit button <b>(Not used, GPI1, GPI2, GPI3, EFIO GPI 1, EFIO GPI 2)</b>
RTE Type	Select relay operation type of RTE <b>(N/O, N/C)</b>
Door sensor	Select an option for door sensor input <b>(Not used, GPI1, GPI2, GPI3, EFIO GPI 1, EFIO GPI 2)</b>
Door sensor Type	Select door sensor type <b>(N/O, N/C)</b>
Held open period(sec)	Type acceptable Door held open period
Alarm sensor	Select an option for Alarm sensor input <b>(Not used, GPI1, GPI2, GPI3, EFIO GPI 1, EFIO GPI 2)</b>
	<div style="display: flex; align-items: center;">  <div> <p><b>Alarm sensor</b> monitors an input port and causes the output relay to open the door on an event (e.g. Fire alarm) basis.</p> </div> </div>
Alarm sensor type	Select Alarm sensor type <b>(N/O, N/C)</b>
Tamper	Select an option for tamper protection type <b>(Not used, Beep mode, Secure mode)</b>
	<div style="display: flex; align-items: center;">  <div> <p>If a physical tampering is attempted in <b>Secure mode</b>, all the data and settings in device will be deleted.</p> </div> </div>
Interlock sensor	Select an option for Interlock sensor input <b>(Not used, GPI1, GPI2, GPI3, EFIO GPI 1, EFIO GPI 2)</b>
	<div style="display: flex; align-items: center;">  <div> <p><b>Interlock sensor</b> monitors an input port and causes the output relay to open or close the door depending on an interlock status after successful authentication and displays the “Wait” message while the interlock is activated.</p> </div> </div>
Interlock sensor type	Select Interlock sensor type <b>(N/O, N/C)</b>

Item	Description
Prohibition sensor	Select an option for Prohibition sensor input ( <b>Not used, GPI1, GPI2, GPI3, EFIO GPI 1, EFIO GPI 2</b> )
	 <p><b>Prohibition sensor</b> monitors an input port and causes the output relay to close the door on an event basis after successful authentication and displays a message that informs the device is not available</p>
Prohibition sensor type	Select Prohibition sensor type ( <b>N/O, N/C</b> )
Recognition start sensor	Select an option for Recognition sensor input ( <b>Not used, GPI1, GPI2, GPI3, EFIO GPI 1, EFIO GPI 2</b> )
	 <p><b>Recognition start sensor</b> monitors an input port and causes device to start recognition procedure on an event (e.g. pressing a button) basis.</p>
Recognition start sensor type	Select Recognition start sensor type ( <b>N/O, N/C</b> )
LED feedback sensor	Select an option for LED feedback sensor input ( <b>Not used, GPI1, GPI2, GPI3, EFIO GPI 1, EFIO GPI 2</b> )
	 <p><b>LED feedback sensor</b> monitors an input port from an access control unit and causes the device to display a message that shows whether a person is permitted depending on the type of input signal.</p>
LED feedback sensor type	Select LED feedback sensor type ( <b>N/O, N/C</b> )

## A.1.4. Device > Interphone


Item	Description
Interphone	Select enable/disable for interphone use
IP Address	Type IP address of the PC where interphone program is installed

## A.2. Network Setting

The network setting contains the configurations about TCP/IP connection, USB port, server functionality, serial communication, and local Anti-Passback.

### A.2.1. Network > Server

Server functionality works based on push dedicated data from device (for example, event/log, image/template for server match) to network. If you will use to this function, contact [service@cmi-tech.com](mailto:service@cmi-tech.com) [mailto:service@cmi-tech.com]

Item	Description
User server	Select enable/disable server functionality
Use manual command	Select enable/disable manual command functionality
	<div style="display: flex; align-items: center; gap: 10px;">  <div> <p><b>Manual command</b> allows for device control by using REST commands. It is an experimental function, not intended for general use.</p> </div> </div>
Server authentication	Select enable/disable server matching <ul style="list-style-type: none"> <li>• <b>Not used</b></li> <li>• <b>Image mode</b> sends original biometric image to server</li> <li>• <b>Template mode</b> sends biometric template extracted from image to server</li> </ul>
Server IP	Type server IP address
Port	Type server port
Commute Uri	Type server URI to receive T&A event logs from device
Sync Uri	Type server URI to receive T&A event logs backed up by device while server is offline.
Acceptable Uri	Type server URI where device sends request to check periodically if server is online

### A.2.2. Network > Serial

Item	Description
RS485-PC	Select a baud rate for RS485 (optional, on demand)

Item	Description
RS485-NET	Select an operating mode for RS485 (optional, on demand)
RS485-ID	Type device ID when the operating mode is SLAVE
RS232	Select a baud rate for RS232 (optional, on demand)

### A.2.3. Network > Etc

Item	Description
USB enable	Select enable/disable device USB port for USB drive

## A.3. Display Setting

The display setting contains the configurations about date and time representation, timeout settings, display language, and screen saver.

### A.3.1. Display > Display

Item	Description
Voice Instruction	Select when to use the voice instructions <ul style="list-style-type: none"> <li>• <b>Not used</b> disables all voice instructions</li> <li>• <b>Use all</b> enables all available voice instructions</li> <li>• <b>Except for recognition position guide</b> enables voice position guide for recognition only</li> <li>• <b>Except for recognition result</b> enables recognition result voice only</li> </ul>
Central Timer	Select device time display enable/disable and time notation <ul style="list-style-type: none"> <li>• <b>Not Used</b> disables Central Timer</li> <li>• <b>12 Hours</b> enables Central Timer in 12-hour clock format</li> <li>• <b>24 Hours</b> enables Central Timer in 24-hour clock format</li> </ul>
Menu Timeout(sec)	Select timeout for auto exit from menu display after leaving it untouched
Pop-Up Timeout(sec)	Select pop-up message window (recognition complete etc.) display duration

Item	Description
Backlight Timeout(sec)	Select timeout for auto-off of LCD backlight after leaving unused
Date Display	Select date notation <ul style="list-style-type: none"> <li>• <b>YYYY/MM/DD</b> uses year/month/day date format</li> <li>• <b>DD/MM/YYYY</b> uses day/month/year date format</li> </ul>
Language	Select language

### A.3.2. Display > Screen Saver

Item	Description
Use screensaver	Select enable/disable screensaver
Time display position	Select time display position in the screensaver
Wait time	Select the amount of idle time

## A.4. Authentication Setting

The authentication setting contains the configurations about basic authentication mode, T&A settings, and Admin password.




### A.4.1. Authentication > Mode

Item	Description
Start mode	Select a primary recognition method
Combination mode	Select a secondary recognition method if necessary


### A.4.2. Authentication > T&A

Item	Description
Use T&A	Select enable/disable T&A mode
T&A mode	Select a T&A mode



Item	Description
T&A value	<p>Select a T&amp;A value: In, Out, Leave, Return</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p><b>T&amp;A value</b> is available for selection when <b>T&amp;A mode</b> is <b>Fixed(by device)</b> or <b>Manual Fix(by key input)</b></p> </div>
T&A order	<p>Select a T&amp;A order: <b>Recognition &gt; T&amp;A</b>, <b>T&amp;A &gt; Recognition</b>, <b>T&amp;A Anytime</b></p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p><b>T&amp;A order</b> is available for selection when <b>T&amp;A mode</b> is <b>Manual(by key input)</b></p> </div> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>The <b>T&amp;A Anytime</b> option allows you to attend directly by pressing the function buttons on the device LCD.</p> </div>

## Authentication > T&A > T&A mode

Item	Description
Fixed(by device)	When selected, authentication is available only with the fixed T&A event. You can define a fixed T&A event in T&A value menu.
Manual(by key input)	When selected, you can press a Function key that is assigned to a T&A event you want. The selected T&A event is released after authentication.
Auto(by time schedule)	<p>When selected, the time schedule that defines the permitted time zones for a door or a user will be applied automatically. Users can obtain or Doors can provide an access permission on this period only.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>The relevant time schedule should be uploaded first to the device for this function to work.</p> </div>
Manual Fix (by key input)	<b>Manual Fix</b> works like <b>Manual</b> . However, in <b>Manual Fix</b> mode, once a T&A event is selected, the event is kept until another T&A event is selected.

### A.4.3. Authentication > T&A Key map

**T&A Key map** lets you to assign EF-45's Function Keys (F1~F5) to a T&A event (In, Out, Leave, Return, Other, Custom) that you want.



The value should be exclusive for each event. Only **Custom** event can have a duplicate value.

### A.4.4. Authentication > T&A custom

**T&A Key custom** lets you to assign a custom T&A event messages for a Function Keys (F1~F5) instead of default T&A event message (In, Out, Leave, Return) on the main screen and authentication result screen.



To make the customized T&A message to appear, make sure that you select **Custom** for the Function keys in the **T&A Key map** setting.

### A.4.5. Authentication > Admin password

Item	Description
Use admin password	Select enable/disable admin password
Password	Type admin password

## A.5. Mode Setting



The mode setting contains the configurations about advanced authentication mode, Wiegand output, and card.

### A.5.1. Mode > Operation

Item	Description
Individual authentication	Select enable/disable for permission of individual authentication




When enabled, the authentication mode of the user will be determined by Individual mode selection in the **User** setting of the device.  
When disabled, the authentication mode will be determined by the global authentication mode settings of the device at **Settings > Authentication > Mode**.

Item	Description
Dual authentication	Select a dual authentication method that requires two person authentication successively
	 Currently, it works only when <b>Everyone</b> selected.
Match timeout	Set a recognition trying timeout
Face image log	Select to include face image file in the log
Continuous recognition	Select enable/disable continuous recognition mode
	 When enabled, the system does not return to the home screen after each recognition.


## A.5.2. Mode > Wiegand

Item	Description
Output type	Select Wiegand output type

### Mode > Wiegand > Output type

Item	Description
Wiegand	Select to send customized Wiegand data out
	 Do not select <b>Wiegand</b> as Wiegand output type unless you will use and set a custom-based Wiegand data for each subject by using a software application. Otherwise, you will get no data in Wiegand Output.
Card	Select to send card CSN out
ID	Select to send user ID out

### A.5.3. Mode > Card

Item	Description
Use CSN	Select to enable/disable card CSN read functionality
	<div style="display: flex; align-items: center;">  <p>When disabled, the card reader tries to read the specific data (for example, ID) stored in writable card memory area instead of CSN. If there is no data on card memory, the card reader does not read anything.</p> </div>
CSN order	Select a card CSN read order <ul style="list-style-type: none"> <li>• <b>MSB</b> reads CSN's most significant bit first (Reverse)</li> <li>• <b>LSB</b> reads CSN's least significant bit first (Forward)</li> </ul>

## A.6. Miscellaneous Setting

The miscellaneous setting contains the information about advanced device information such as application version and the configurations about firmware upgrade, device reboot, and clearing data in device.

### A.6.1. Etc > Device information

Item	Description
MAC	Shows MAC address of this device
Model name	Shows model name of this device
Firmware file	Shows version name Firmware installed
Kernel	Shows revision number of kernel
Hardware	Shows revision number of hardware board
Boot	Shows revision number of boot loader
Root	Shows revision number of root file system
Recovery	Shows revision number of recovery firmware
FPGA	Shows revision number of Camera FPGA firmware
Version	Shows revision number of Launcher application

## A.6.2. Etc > Firmware

The device firmware upgrade procedures are as follows:

1. Click the search button in the **Firmware** section.



Select the **Force** box to downgrade the firmware or write the same version of firmware again.

2. In the **Load firmware from** dialog box, locate the firmware file and click **Open**.
3. Click **Upgrade > Yes** to start firmware upgrade. The **Upgrade firmware** window that shows the progress bars appears.
4. When completed, click **Close** to close the window.

## A.6.3. Etc > Management

Item	Description
Re-boot	Click to restart device
Clear all	Click to delete log data ( <b>Logs</b> ) or user data ( <b>Users</b> ) stored in device



## Appendix B: End-User License Agreement (EULA)

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and CMITech Co., Ltd.

This EULA agreement governs your acquisition and use of our CMID Manager V2 software ("Software") directly from CMITech Co., Ltd. or indirectly through a CMITech Co., Ltd. authorized reseller or distributor (a "Reseller").

Please read this EULA agreement carefully before completing the installation process and using the CMID Manager V2 software. It provides a license to use the CMID Manager V2 software and contains warranty information and liability disclaimers.

If you register for a free trial of the CMID Manager V2 software, this EULA agreement will also govern that trial. By clicking "accept" or installing and/or using the CMID Manager V2 software, you are confirming your acceptance of the Software and agreeing to become bound by the terms of this EULA agreement.

If you are entering into this EULA agreement on behalf of a company or other legal entity, you represent that you have the authority to bind such entity and its affiliates to these terms and conditions. If you do not have such authority or if you do not agree with the terms and conditions of this EULA agreement, do not install or use the Software, and you must not accept this EULA agreement.

This EULA agreement shall apply only to the Software supplied by CMITech Co., Ltd. herewith regardless of whether other software is referred to or described herein. The terms also apply to any CMITech Co., Ltd. updates, supplements, Internet-based services, and support services for the Software, unless other terms accompany those items on delivery. If so, those terms apply.

### B.1. License Grant

CMITech Co., Ltd. hereby grants you a revocable, non-transferable, non-exclusive licence to download, install, and use the CMID Manager V2 software on your devices in accordance with the terms of this EULA agreement.

You are permitted to load the CMID Manager V2 software (for example a PC, laptop, mobile or tablet) under your control. You are responsible for ensuring your device meets the minimum requirements of the CMID Manager V2 software.

You are not permitted to:

- Edit, alter, modify, adapt, translate or otherwise change the whole or any part of the Software nor permit the whole or any part of the Software to be combined with or become incorporated in any other software, nor decompile, disassemble or reverse engineer the

Software or attempt to do any such things

- Reproduce, copy, distribute, resell or otherwise use the Software for any commercial purpose
- Allow any third party to use the Software on behalf of or for the benefit of any third party
- Use the Software in any way which breaches any applicable local, national or international law
- Use the Software for any purpose that CMITech Co., Ltd. considers is a breach of this EULA agreement

## B.2. Intellectual Property and Ownership

CMITech Co., Ltd. shall at all times retain ownership of the Software as originally downloaded by you and all subsequent downloads of the Software by you. The Software (and the copyright, and other intellectual property rights of whatever nature in the Software, including any modifications made thereto) are and shall remain the property of CMITech Co., Ltd..

CMITech Co., Ltd. reserves the right to grant licences to use the Software to third parties.

## B.3. Term and Termination

This EULA agreement is effective from the date you first use the Software and shall continue until terminated. You may terminate it at any time upon written notice to CMITech Co., Ltd..

It will also terminate immediately if you fail to comply with any term of this EULA agreement. Upon such termination, the licenses granted by this EULA agreement will immediately terminate and you agree to stop all access and use of the Software. The provisions that by their nature continue and survive will survive any termination of this EULA agreement.

Upon termination of this Agreement, you shall cease all use of the Software and delete all copies of the Software from your computer or from your mobile device.

Termination of this Agreement will not limit any of CMITech Co., Ltd.'s rights or remedies at law or in equity in case of breach by you (during the term of this Agreement) of any of your obligations under the present Agreement.

## B.4. Amendments to this Agreement

CMITech Co., Ltd. reserves the right, at its sole discretion, to modify or replace this Agreement at any time. If a revision is material we will provide at least 30 days' notice prior to any new terms taking effect. What constitutes a material change will be determined at our sole discretion.

By continuing to access or use our Software after any revisions become effective, you agree to



be bound by the revised terms. If you do not agree to the new terms, you are no longer authorized to use the Software.

## **B.5. Governing Law**

This EULA agreement, and any dispute arising out of or in connection with this EULA agreement, shall be governed by and construed in accordance with the laws of the Republic of Korea excluding its conflicts of law rules.

## **B.6. Entire Agreement**

The Agreement constitutes the entire agreement between you and CMITech Co., Ltd. regarding your use of the Software and supersedes all prior and contemporaneous written or oral agreements between you and CMITech Co., Ltd..

You may be subject to additional terms and conditions that apply when you use or purchase other CMITech Co., Ltd.'s services, which CMITech Co., Ltd. will provide to you at the time of such use or purchase.

## **B.7. Contact Information**

If you have any questions about this Agreement, please contact CMITech at [sales@cmi-tech.com](mailto:sales@cmi-tech.com) [<mailto:sales@cmi-tech.com>].



## Appendix C: Copyright Notice

All rights reserved. The documentation, brand name, and logo used in this guide are copyrighted by CMITech Co., Ltd. No part of this guide may be reproduced, transmitted, or transcribed without the expressed written permission from CMITech Co., Ltd. All other product names, trademarks, or registered trademarks are property of their respective owners.

We reserve the right to make any alterations which may be required due to technical improvement. For the most current information, contact your CMITech representative.



## Appendix D: Disclaimers

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



## Appendix E: Abbreviations

Item	Description
CJK	Chinese, Japanese, Korean
CRUD	Create, Read, Update, Delete
CSN	Card Serial Number
DHCP	Dynamic Host Configuration Protocol
GPI	General Purpose Interface
LSB	Least Significant Bit
MSB	Most Significant Bit
N/O	Normally Open
N/C	Normally Close
PIN	Personal Identification Number
REST	Representational State Transfer
RTE	Request To Exit
T&A	Time & Attendance
TCP/IP	Transmission Control Protocol/Internet Protocol
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier



**CMITech Company, Ltd.**

5th Floor, 38, Burim-ro, 170beon-gil, Dongan-gu, Anyang-si, Gyeonggi-do,  
14055, Republic of Korea

**CMITech America, Inc.**

2033 Gateway Place, Suite 500, San Jose, CA 95110

[www.cmi-tech.com](http://www.cmi-tech.com)