timeware®
HR, Time and Attendance Software

ON PREMISE SOFTWARE

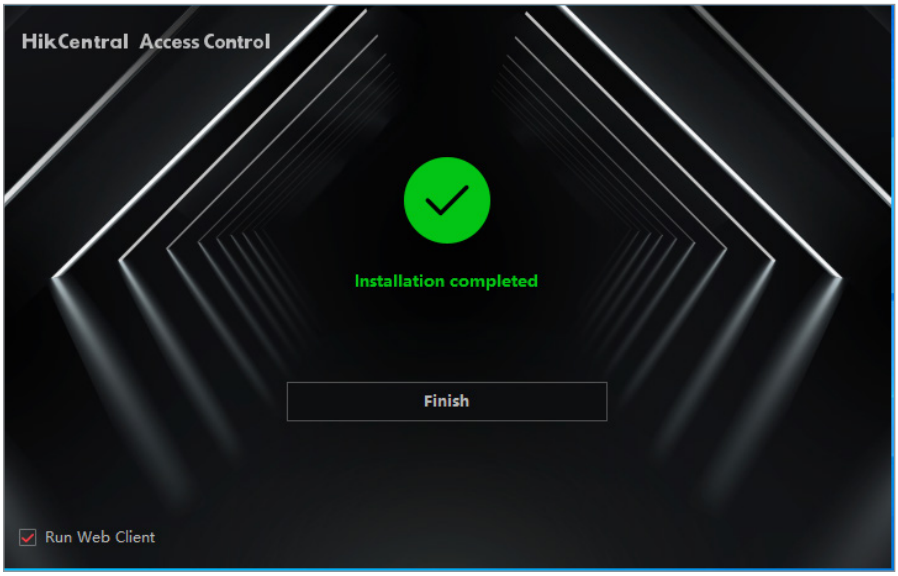
HikVision

Overview:

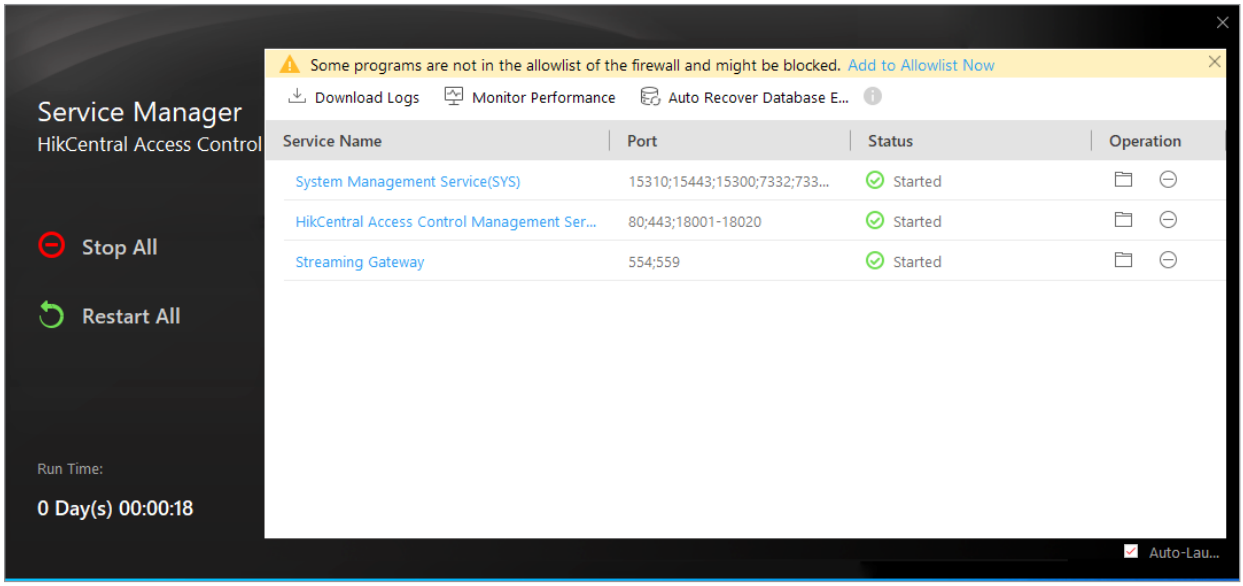
- Supported version of HikCentral Access Control is v2.2.0. With every new release of HikCentral Access Control, the integration will be tested internally.
- There is no annual charge for the integration, the only thing that is required is an upgrade to 2023. There is no connection fee per device, but the license engine allows us to control how many devices can be connected. This is so customers can't add devices to the system as they like without us knowing. We can also control the type of devices, whether it be Access Control or Attendance. An example could be you asking for a license that allows 3 Access Control devices and 5 Attendance devices. If any more devices are added, then a new license will be required.

Installation:

- Requirements
  - HikCentral Access Control software and HikCentral Access Control OpenAPI
  - Please check HikVision's minimum spec documentation for the requirements for HikCentral Access Control and OpenAPIA.
  - timeware® 2023 (23.1.2 or greater)
  - .NET Runtime 7.0.X https://dotnet.microsoft.com/en-us/download/dotnet/7.0
  - timeware® license with the HikVision integration part enabled.
- Instructions
  - Run the HikCentral Access Control installer (not the OpenAPI yet). Agree to the terms and conditions and then click the cross to come back to the main screen.
  - Choose custom installation if you want to change the directory of where it will be installed, if not click install now.
  - Let the installer complete, if ports that are used by HikCentral are already in use, it will ask you to choose a different one. Make a note of the ports you have used and for what service.
  - Once completed you will get the below screen, make sure "Run Web Client" is ticked, and then click "Finish".

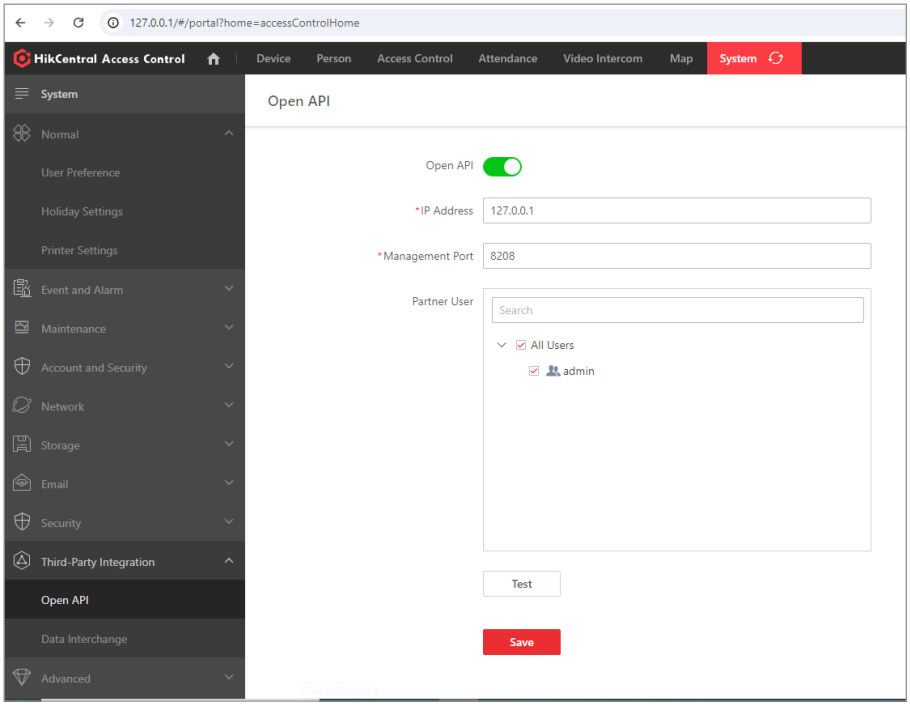


- You should get presented with the below screen, if it mentions allowing apps through the firewall, click the "add to Allowlist Now". Click okay on the next screen, and then the yellow warning should disappear.

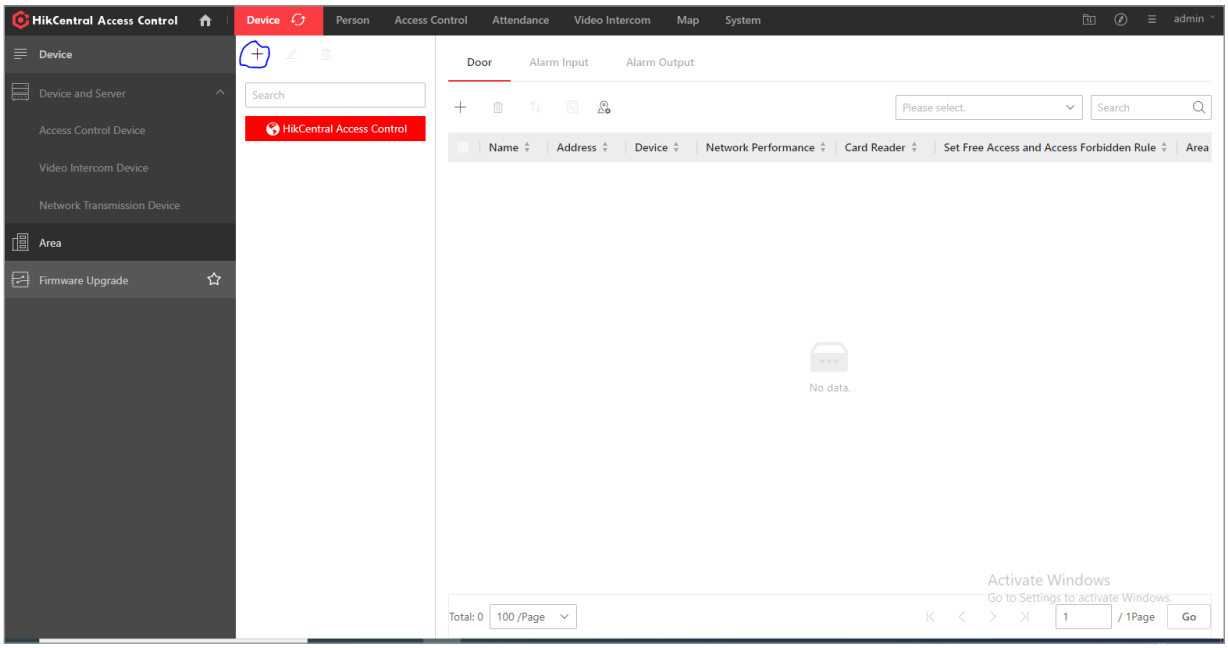


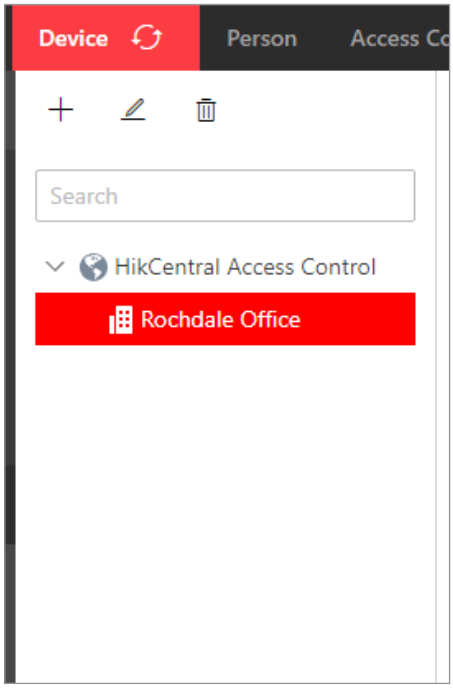
- A browser window should have opened you and taken you to the Web Client. It will ask you to create an admin password. Create one and make sure you remember it. This will be for logging into the HikCentral software. Once completed, you should come to the home screen of the software.
- If at any point you get prompted to install some web controls then go ahead and to do so.
- Next is to install the other .exe, the OpenAPI. Again, agree to the terms, close out and then click on "Install Now". If it says you need to exit "Service Manager", close the application from the system tray and retry. If it asks you to reboot, click yes.

- Reopen the HikCentral Access Control Service Manager and you will now see there are a few more services called Artemis and and then the OpenAPI service, wait until these have changed from "starting" to "stopped".
- Go back into HCAC by either the shortcut on the desktop or the IP:PORT of the server you installed it on and log in with the account you created earlier.
- Click on System at the top and then in the left hand side menu, go to Third-Party Integration->OpenAPI.
- Enable the API, leave the IP and port settings default, and tick the admin user. Click on test, make sure it comes back ok, and then click save.



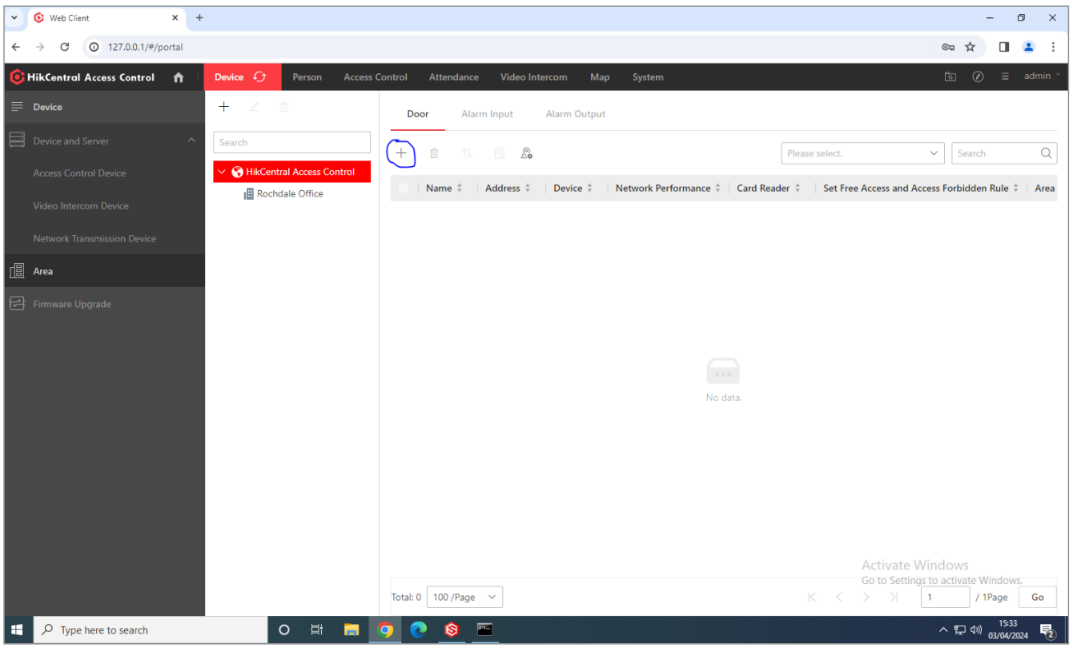
- Next up is to add an Area that the device belongs to. In HCAC there is an "Area", you then add a "Door" to the "Area", and then you add your device(s) against the "Door". We pull swipes from the "Door" record.
- Go to Device up at the top and then Area in the left menu.
- In the section in the middle, click on the circled plus button and create your area.



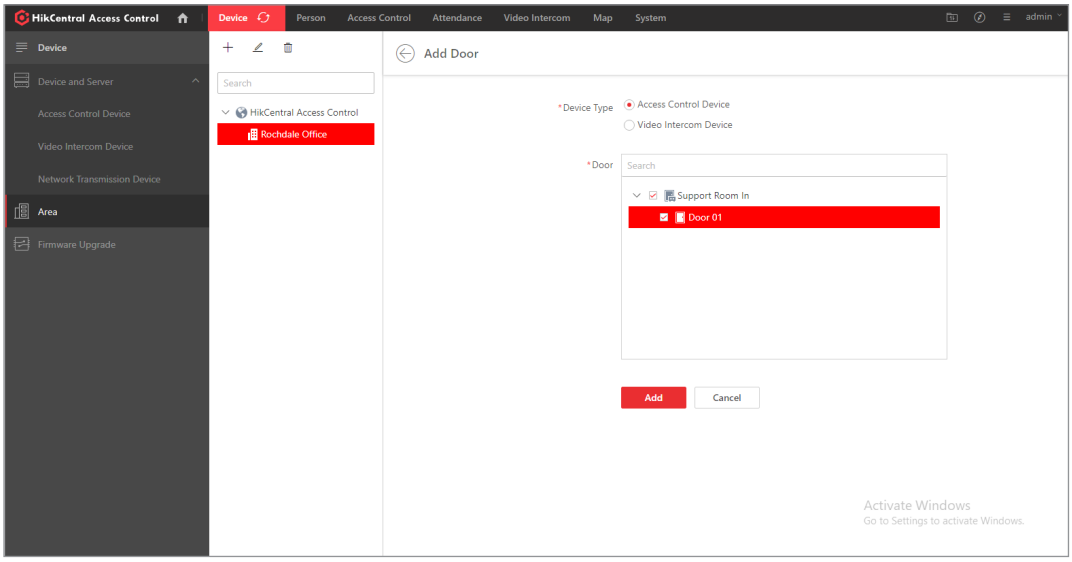


- Next, we want to add the device. This is so when we create the door, we can add it to the correct area, and then assign the device to it.
- Make sure you are still on the Device section at the top, and then on the left-hand side menu go to Device and Server->Access Control Device.
- In the "Online Device" section at the bottom, you should see your device(s).

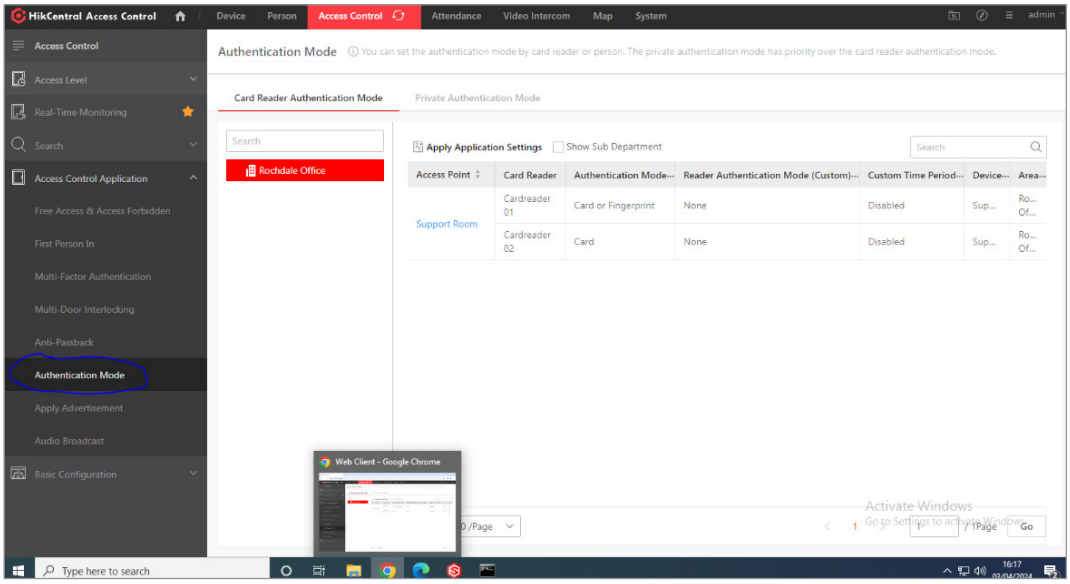
- If you have already activated the device through the device itself, it will show as activated. If not, tick the device on the left-hand side and click on activate.
- Enter a password and click on activate. It should now change to activated at the bottom.
- If you need to change the IP settings, tick the device again, and on the right-hand side under operation click on the "Edit" icon. You can now toggle whether to use DHCP or enter your own static IP address. Once entered press the tick icon under "Operation", enter the admin password you just created, and press save.
- Tick the device again and click on "Add to Device List".
- Give the device a name and set a password for the admin user, in the "Time Zone" section click manually set the time zone and select the correct time zone. The time zone includes the DST changes.
- In the "Resource" section, untick the "Add Resource to Area" option, we will do this manually.
- Click on add.
- If you now go back to the "Area" section on the left-hand side, select the area you created earlier, then in the section in the right-hand side, under the text "Door", click the plus button.



- Select the device added earlier, and it will auto create a "Door 01", make sure this is selected too and then click "Add".

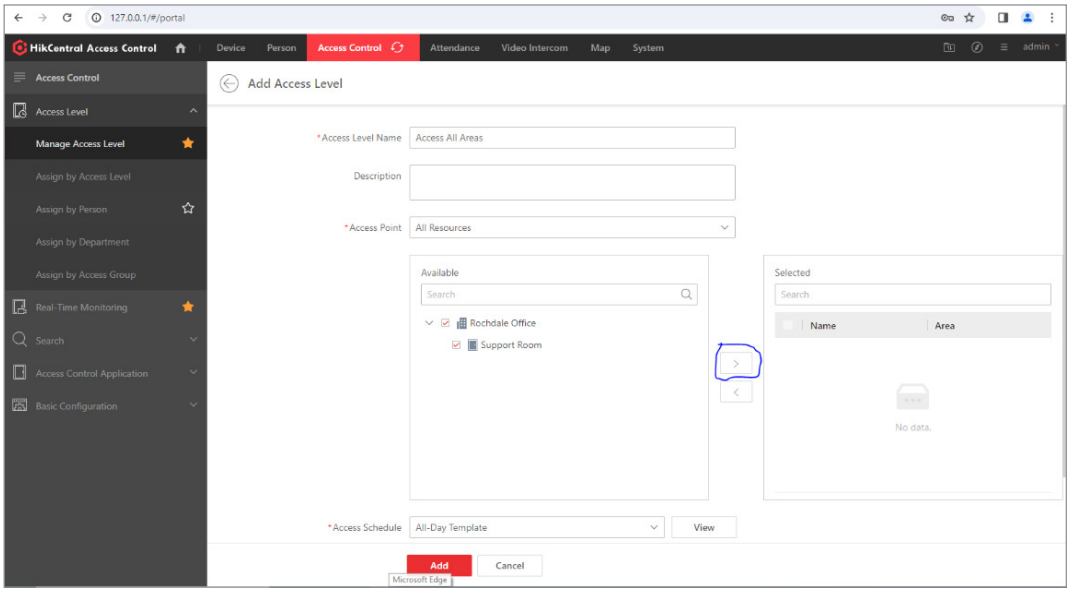


- You will then see it has created a door called "Door 01", if you click this you can rename it to whatever you like. You can then configure all your relay settings from within here.
- Next is to make sure the device has the correct authentication type (card or finger etc).
- Click on "Access Control" in the top menu, and then on the left-hand side select the "Access Control Application" header. Under here, click on "Authentication Mode".

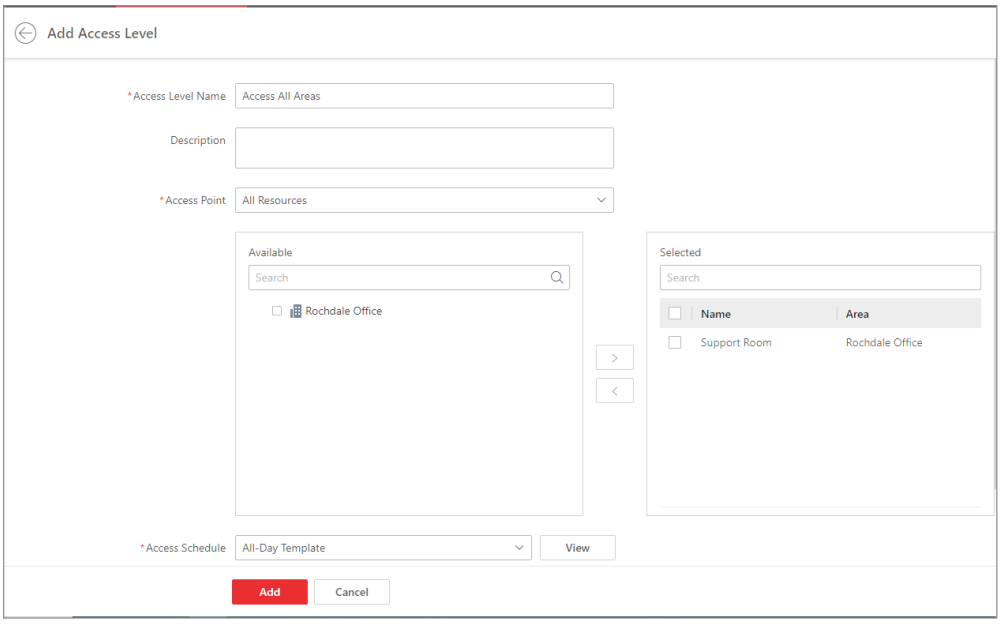


- On the right-hand side section, click on the name of the access point we added previously.
- For "Card Reader 01 Authentication mode", select the option you require. It will usually be "Card or Fingerprint" or "Card or Fingerprint or Face".

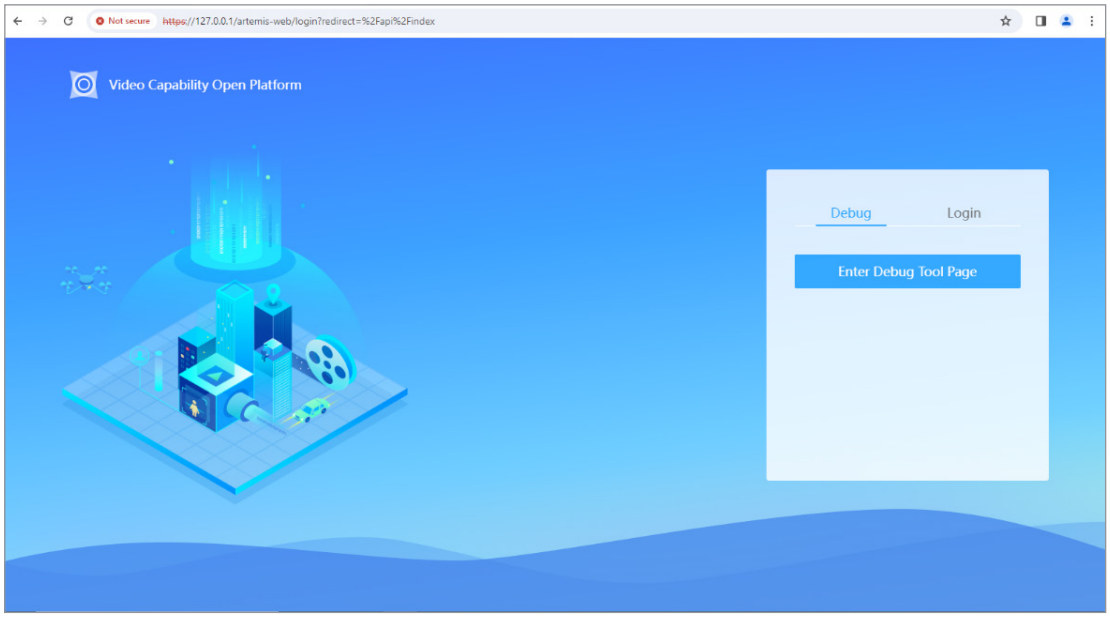
- You can leave Card Reader 2 as it is.
- The last thing to do in HCAC is to create your Access Levels. These are all created and controlled by HCAC, but they are assigned to the employee in timeware.
- Make sure you are on the "Access Control" option at the top still, and then on the left-hand side choose open "Access Level" then select "Manage Access Level".
- Click on the Add button at the top of the main section.
- Give the access level a name, select the door from the area we created earlier, and click on the right arrow to add it to the access group.



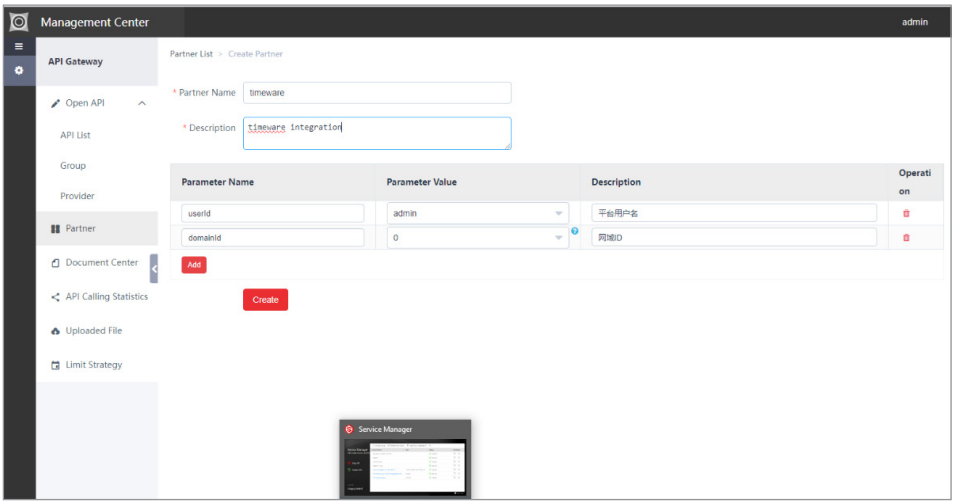
- The door should now show in the selected section on the right-hand side.



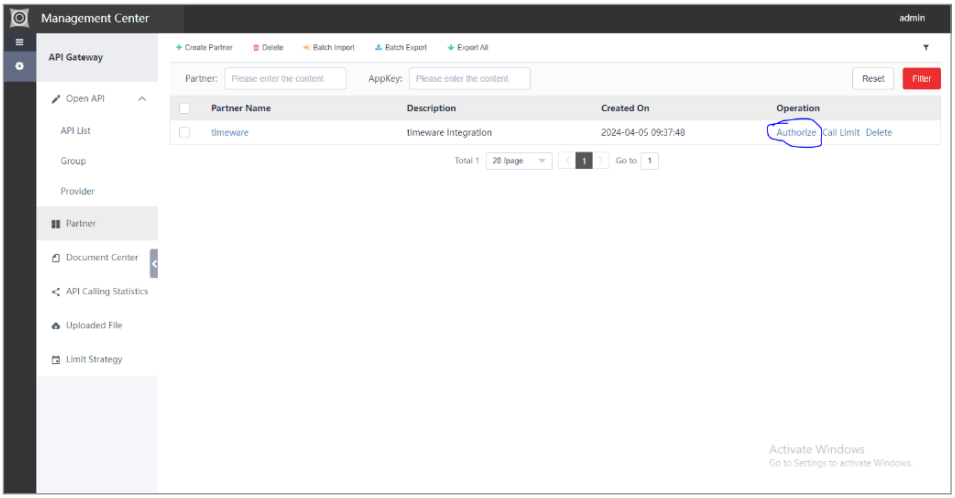
- The "Access Schedule" at the bottom is to set the times of the day the door can be accessed. If you need to customise this then click into the dropdown and then choose "New Access Schedule Template" and configure your schedule.
- We will use the "All-Day Template". Select this and then click on "Add".
- This is pretty much it for the configuration in HCAC, the next step is to setup the API.
- Browse to https://IPADDRESS/artemis-web. You should come to the following screen.



- Click on "Login" and login with the credentials
  - username: admin
  - password: admin@123
- You will be asked to create a new password, do this and then click okay. If you then get presented with an error message, ignore it as the password has still changed.
- Go back and login with your new credentials.
- In the left hand menu click on "Partner", and then at the top click on "Create Partner".
- In more recent versions of the API, partner may show as "User/User Management".

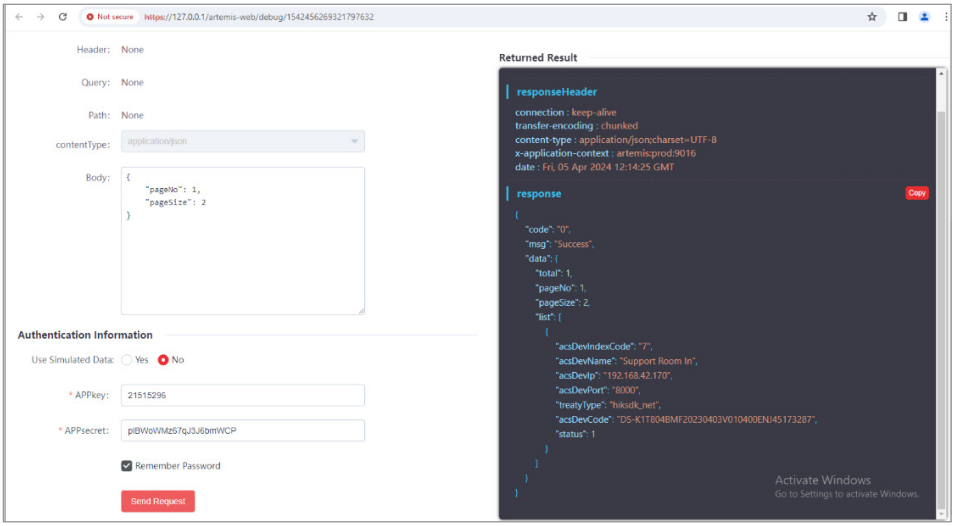


- Give the partner a name and description, doesn't need to be "timeware" but the rest of the settings need to match. The "admin" parameter value assumes you used the admin user when we enabled the OpenAPI earlier on in the guide. If you used a different user, you need to replace "admin" with the username.
- Click on create and it will take you back to the "Partner" screen.
- Click into the partner you just created and make a note of the "Partner Key" and "Partner Secret".
- Go back to the main "Partner" screen, and click on "Authorize on the right hand side

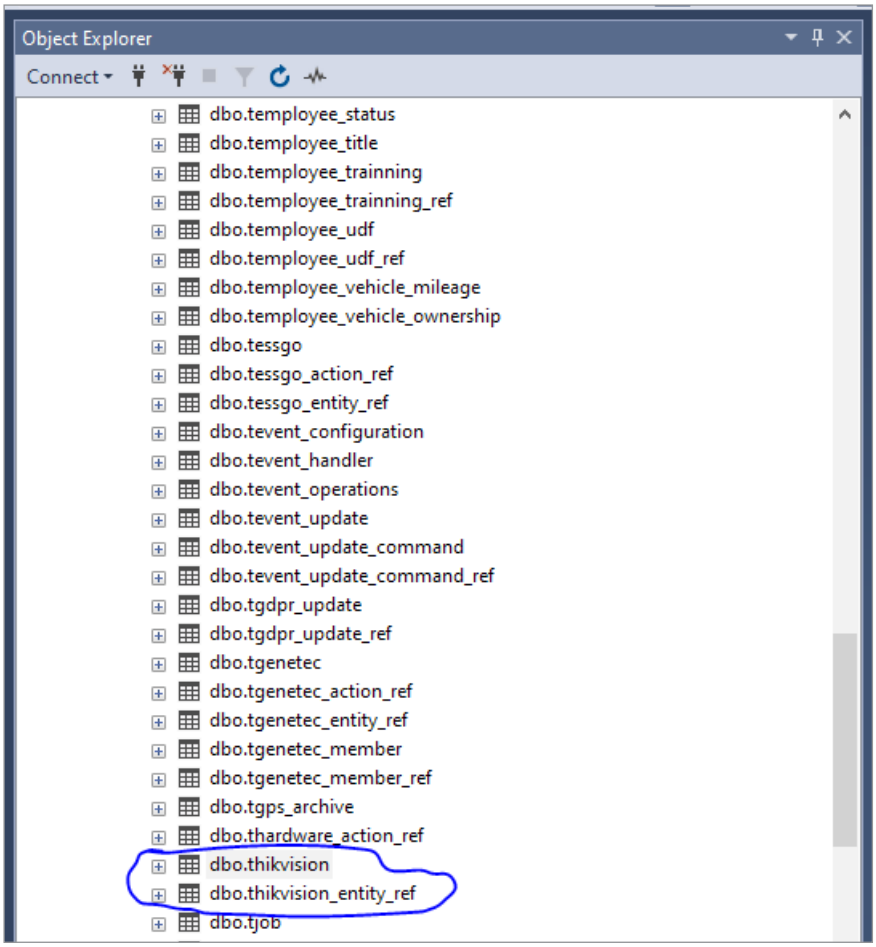


- In here, in the list in the left-hand side, expand "Physical Resources API", and select the "Access Control Device Information".
- In "Logical Resources API", select "Access Point Information" and "Person Information".
- Finally, in the "Access Control API", select "Search for card swiping records".
- Click the right arrow so they copy over to the right-hand side of the screen.

- Click "OK" at the top to save this away.
- To test the API is properly configured, click on "API List" in the left-hand menu.
- In the list of API's find "Get access control device list", click on the "Online debug" link on the right hand side.
- On the new page that opens, scroll to the bottom, and enter the APPkey and APPsecret you made a note of from the partner page we setup earlier. Click on "Send Request"
- If all goes well, you should get a "success" response in the window on the right hand side and a body which shows a list of the doors you have created in HCAC. It should look something like the below.



- If you don't get the success message, then go back through the guide and follow the API setup again.
- That is it on the HCAC and OpenAPI config, next is to add the additional SQL tables and run the Event Agent script.
- From the zip provided, run the 3 sql scripts against the timeware® main database, in order by the name of the script, so starting with 01, then 02, then 03. Reconnect to your databases and make sure that you have the 2 new HikVision tables.



- Once the tables are in place, the last thing to do is to run through the Event Agent Console UI to create the command line for the service.
- Navigate to "C:\Program Files (x86)\timeware Software\timeware\EventAgentBin" and run the Toronto.Event. ConsoleUI.exe.
- Choose number 2 to build a script command line.
- Once the script list has populated, find the EAi-HikVision entry and enter the number it corresponds to.
- Press 0 to read the readme, or 1 to build the command line.
- Choose to run as a service or as a one off operation to be scheduled to run in windows task manager. For testing purpose I would run as a one off.
- If testing or you want it log extra debugging, enable verbose mode.
- Enter the hostname and port of where HCAC is installed, it will be in the format "http://192.168.42.1:8080".
- Enter the appKey that you copied from the partner page in the API earlier.
- Enter the appSecret you copied from the partner page in the API earlier.

- Usually, you won't want to sync employees from HikVision > timeware, so choose "false" for this. I included this option in case we were installing on a site that already had a HikVision system setup.
- Choose "true" if you want to send employees from timeware® > Hikvision.
- Choose "true" for syncing access groups from HikVision > timeware. This is needed to bring the access groups into timeware, so they can then be assigned and sent back across.
- Choose "true" for syncing access groups from timeware® > HikVision. This assigns the employee to the correct Access Group in HikVision. This is handled from the personnel screen in timeware® as usual.
- Choose "true" for syncing terminals. This is so we can save away which terminals the events were made against. The terminals you are pulling data from need to be unsuspended and set to the correct terminal types based on the requirements (access or attendance data).
- Choose "true" if you want to pull "access granted" events from HikVision > timeware. This can be used as Access/ Attendance data based on the requirements.
- Enter your duplicate threshold (Repeat Swipe) duration. I recommend sticking to 2 minutes.
- If you want to limit the integration to certain groupings, enter the grouping number. If not, enter 0.
- Type the names of the groups you want to exclude, if you are not excluding any, leave it empty.
- You can now test your command. Make sure there are no errors before setting it up as a service.
- Next, we need to create the service. Download the following batch file: https://www.dropbox.com/s/lrg49nr1m8injzy/ Event%20Agent%20Service%20Installer.bat?dl=0
- Open the batch file in a text editor, replace the following text:
  - "REPLACENAME" – replace with a name of your service - i.e "timeware/HikVision integration"
  - "REPLACECMD" – replace with copied command line i.e "-c xxxxxxx". Make sure there is a space after the ".exe".
  - "REPLACEDESC" – replace with brief description - i.e "Integration between HikCentral Access Control and timeware Professional".
- Once these have been edited save the file and then run it is an admin, this will install the service for you.
- Start up the service.