C4 Quick Guide

Hi Everybody, welcome to the human soul of your security engine!

After the successful installation of the C4 System and registration of the installation, we can begin with the implementation of the system for the client. This lesson will guide you through the whole process at the end of which is handover of the system to the customer.

We will start by creating a supplier account. Under this account we will perform all the steps necessary to complete the implementation of the System.

Creating a Supplier

1. Engineer account

The first step involves adding a supplier company and a person to the C4 System, creating a user account and assigning user permissions.

Start by adding a supplier company. Then add a person under it.

The C4 System is a client-server solution, and therefore all changes made in the C4 Client must be transferred to the server.

And since the C4 System is modular, it enables processing of data in the forms developed by independent developers. Therefore, to ensure secure data processing, each form must be saved separately. This naturally results in very frequent requirements for data saving. For this reason, the C4 System offers the possibility of automatic data saving when switching between different parts of the client. This function can be activated by ticking the checkbox in each saving request. This setting can be turned off any time in the application settings.

Now, we will create a user account and set permissions for it.

Each person who will be working in the C4 Client must have their own account with a secure password created.

The easiest way to define permissions is through assigning a role, which will automatically determine permissions within the C4 System.

The roles can be mutually combined and resulting permissions are the sum of permissions from the individual roles.

An engineer is a role assigned to a person trained for installation and connection of devices to the C4 System.

An administrator is a role for a person managing the entire C4 System installation and setting up permissions for individual users.

Combination of these two roles gives the person the highest possible permissions.

As soon as the supplier account is created and all the necessary permissions are set, you can log out from the Support account and start working under your personal supplier account.

2. **Access to the Portal Services**

In the next step, we will allow access to the Portal Services.

In order to be able to download Drivers directly from the C4 Client environment, we need to allow access to the Portal Services from the C4 Client.

The C4 System enables to allow access to the Portal Services for all users. However, for more transparent management of the C4 System, it is recommended to explicitly define the persons who will have access to the Portal Services.

The next step is adding devices to the C4 System.

Adding devices

1. **Installation of the Driver**

In order to implement a device, it is necessary to install a Driver first.

All extensions of the C4 System, called Plugins, are located exclusively on Gamanet's Plugin Store. One of the categories of Plugins is Driver, which is designed to integrate external systems into C4. They can be acquired in two ways.

If you don't have an internet connection from your computer with the C4 Client, you can download the package for the particular Driver on the address *https://my.c4portal.com*, section Plugin Store. You can find there all available Drivers, grouped into categories according to the scope of functionalities they offer. Clicking on the Driver will display all information about it, and you can also download it from here.

In the C4 Client, you will import and install the downloaded Driver.

The second possibility of obtaining a Driver is directly from the C4 Client environment. The available Drivers will be displayed upon checking the Show Available option.

To be able to download Drivers this way, it is necessary to have enabled logging in to the Portal Services, as explained at the beginning of this lesson.

If you want to be logged in to the Portal Services automatically, you can link your account in the Portal Services with your account in the C4 System. This way you won't be asked to enter your credentials every time reaching the Portal Services.

The only exception is the Support account, which cannot be accessed through automatic login.

Now select the desired Driver and click on the Install button.

The person installing the Driver must be trained for the particular device.

In case you are prompted, restart the C4 Client.

2. Adding device configuration

After downloading the Driver, we can proceed to the next step which is adding device configuration to the C4 System.

For each device which we want to manage, it's necessary to define its configuration specific to the particular customer. In the C4 System, this configuration is represented in the form of a tree. Some Drivers allow automatic loading of configuration from devices, and the trees are created automatically. In other cases, the tree needs to be created manually.

We begin by adding a Bus Controller, which represents a connection point to the device.

Fill in the required information such as the name of the device, IP address and set the correct port.

Then we add the subsystems, in this case it's an access panel, a door and a card reader. For each subsystem, enter the hardware address. This address uniquely identifies a subsystem within the device topology. Usually, it's a physical address defined directly on the subsystem. In certain cases serves as an address a logical address generated within the configuration of the device in the software of the manufacturer.

The C4 System enables to define various parameters depending on the subsystem and the possibilities of the communication protocol provided by the device manufacturer. The names of the connection and configuration parameters usually match the names found in the device manual provided by the manufacturer, or in the device integration manual provided by the Driver developer.

This way you will implement all devices from your installation to the C4 System. In our case the installation consists of two demo devices, the first one is an input/output device and the second one is an access control device.

In the case of access control and security devices that manage credentials, it is necessary to disable the *Credential Upload Enabled* parameter in this phase, which turns off uploading of credentials to the device. This parameter can be found either in the settings for the Control Panel of the access control system or in the Bus Controller settings.

Location of the parameter depends on the device type and its implementation by the developer.

By initial launch of the communication with the device - by issuing a Start command, the C4 System takes control of the device within the allocated range of the device memory. As the very first step, it uploads to the device all credentials defined in the C4 System for the particular device. The rest of the memory space which is under control of the C4 System will be cleared of old records. This ensures transparency in the information subsequently received by the C4 System from the device in the form of logs. In the case of adding a new device, it is thus necessary before uploading the credentials, to create these first, assign them to the

respective persons, define their permissions and then we can upload them to the device.

Therefore, we will enable uploading of credentials only after completing the employee settings in the following step.

After implementing the device configuration, we will initiate communication of the C4 System with the device. We will thoroughly check correct functioning of all subsystems of the device. We will also verify whether the individual statuses of the device are displayed correctly in the C4 System and whether all events are being received from the device.

The next important part of implementation of the C4 System for the customer is creating organizational structure of the company and setting up credentials.

Employee Management

1. **Adding persons**

The first step is adding the persons to the C4 System.

To be able to use the benefits which the C4 System offers in management of access rights, it is strongly recommended to implement the organizational structure of the company in the personnel management. Therefore, before we start adding persons, we need to create a company and individual departments. Such created structure has a significant impact on transparency of the access rights management. Adding employees directly under the Root is not advisable. Persons added in this way cannot subsequently be processed in bulk when assigning accesses. Organizational structure considerably speeds up processing of access rights for uploading to devices.

When creating an organizational structure of the company, it's important that it is created by one person only. If two users of one system create the same company or department in their C4 Clients at the same time, these are registered twice in the C4 System after being saved.

The organizational structure should reflect the policy of defining the access rights as much as possible. It means that persons with the same sets of access rights should be placed in one organizational unit.

Considering these aspects will allow us to significantly simplify the access rights management within the C4 System in the future.

In the C4 System, it is also possible to create employee groups. However, the access rights settings are more complicated in this case, because all groups are considered equal. That's why it is highly recommended to define only the access rights of "Enable" type in the groups. Differences between the settings of access rights for persons in the organizational structure and for persons in the groups will be further described in a separate lesson.

2. Credentials

Next, for each employee we register their credentials used within the scope of access rights.

Before that, however, we need to add into the C4 System a list of all types of credentials that will be used in our system.

A big challenge in the credential management is diversity of their types and formats, as well as the fact that each access control system works with its specific format of credentials. Therefore, Gamanet created a central library, which registers all types of supported formats of credentials and their conversion into formats compatible with devices integrated in the C4 System. When importing a type of credentials, converters for individual devices are imported as well.

For each employee we register all credentials used within the access management which are assigned to them. In our case, it's a PIN code, type PIN 4 and a card, type HID 26.

3. Access rights

Then we can proceed to defining the access rights.

Accesses can be configured for each person separately, or for the whole department. All settings defined within the organizational structure are

automatically inherited and reflected on the persons. If we move a person from one department to another, they will take on the rights defined for the department they are currently in.

When the accesses are defined, we will go back to the device and enable the option *Credential Upload Enabled.* Any changes in the device configuration will take effect only after restarting the device.

In the case of the first start of the communication with the device with the Credential management enabled, the process of uploading credentials to the device will be started automatically in the next step. This process may take longer, depending on the computer and network speed, number of cards or configuration and type of the device.

When the uploading is finished, we will check how much are the uploaded entries of allowed accesses for the persons projected in the real installation. For this, it is necessary to check a few credentials to see how much the access rights settings in the C4 System match the reality. That means, if a person has defined access to the door in the C4 System, whether the access system will actually allow this person to enter. Of course, any activity of a person on the access system will be displayed in the C4 in the form of an event in the list of events.

4. User permissions

Next, we define user permissions.

If the person will be an active user of the C4 System, we need to create for them a user account under which they will be working.

Then we assign each person a role based on the permissions they should have in the C4 System.

The first person with assigned Administrator permissions will be an installation manager from the customer's perspective.

Assigning a role to the person automatically determines their permissions within the C4 System.

If we need to configure more specific permissions for a particular person in various areas, we can do that in the Permissions tab.

This topic is explained in details in a separate lesson.

Next, we proceed with creating regions and visualization.

Regions and Visualization

1. Creating the structure of regions

The first step is creating regions and adding devices to them.

Regions are an essential part of the core of the C4 System. They enable extension of functionalities regarding access and visitor management systems, such as in the case of people counting, anti-passback, or time and attendance.

Hierarchy of regions enables intelligent processing of information from devices and persons, their pairing and subsequent evaluation at various levels.

Hierarchical structure of regions is also a basis for visualization.

When creating regions, we always start with a region that represents the entire installation, whether it's a building, city, country or continent. The individual regions should reflect the logical structure of the installation. The more detailed the hierarchy, the easier it is for an operator to navigate and implement any changes within it.

As soon as the regions are created, we can start adding devices to them by drag and dropping with the mouse.

2. Visualization of regions and devices

We can now proceed with creating a visualization and placing objects to it.

Hierarchical structure of the visualization divides the entire installation into small visualization blocks. This allows to visualize only the specific part of the building in which we need to work.

To create a block, we start with visualization of a region in the form of an underlying picture, and continue by visualization of devices to the positions representing their real location.

The C4 System supports any public raster format for images. In the case of a request for vector-based visualization, Gamanet provides a separate visualization module.

Subsequently, in the Monitoring module, we can monitor and control the devices. Any change on the device is projected in the visualization.

In our case, by switching on the detector, we simulate that a window has been opened.

If we want an incident to be generated in such situations, we can set it up using Smart Routines.

In this part of the lesson we will explain how to activate incidents and create a workflow.

Incidents and Workflow

1. **Activating incidents**

Incidents can be activated in two ways. Customers can use an Incident Creator, or they can set up their own custom Smart Routine that will generate incidents based on the conditions defined by them.

Incident Creator is a Smart Routine provided by Gamanet, which generates incidents from all alarm-type events, regardless of the device type.

We can also expand incidents based on the conditions defined through any Smart Routine installed in the C4 System.

In our case, we create an automatic action using Log Routine, which will generate an incident if a window opens.

An incident can be created from any event, change in the status of the device, or scheduled time, depending on the specific needs of the customer.

When the conditions for creating an incident are met, an Alarm Overview window displays. *Input opened* indicates that the window has been opened.

2. Other workflows

The customers can also define various other workflows according to their specific needs.

In the current generation of the C4 System, the basic set of Smart Routines provided by Gamanet can be further extended by the custom routines developed according to the customer's specific requirements.

Smart Routines can be activated by three different sources of signal. The first one is occurrence of a certain event, the second one is change in the state of the particular device, and the third option is scheduling the Smart Routine to be activated at a specific time.

The previous C4 System generations contained so called automatic actions. In the new generation, these are contained within a Log Routine.

A Smart Routine has two parts. The first one is a set of conditions, which are evaluated, and based on the result the system decides whether it should perform a defined action.

To create a condition, we have a set of parameters available.

The range of parameters which the user can set is defined by the developer. For example, for this Log Routine, we can configure the parameters concerning a device, an event, a person or a region.

By specifying conditions in the given Smart Routine we determine the items to which it will apply. For example, in the case of an event, we can exactly define whether it applies only to the specific event or to the subordinate events as well. We can also specify an exact list of events to which the Smart Routine will apply.

Within one condition set, it is possible to combine conditions for various types of items that are included in the event. For example, we can combine alarm with the specific detector 3, too.

In addition to combination of simple conditions, the new generation of the C4 System allows to create also compound conditions with parentheses.

Meeting all the defined conditions triggers the second part of the Smart Routine, which is an action or a set of actions.

The C4 System distinguishes two types of actions, depending on where they are executed. The first type are actions executed on the server side, such as sending a command to the device or sending an e-mail.

In this case, we define that the e-mail is sent to an operator, but it can be sent to any unit within the organizational structure. It is also possible to attach a file with information about the event to the e-mail.

The second type are actions executed on the client side, for example, displaying an instruction set to the operator, or showing a live video.

For a single set of conditions, it is possible to set a combination of both server and client actions.

The list of both client and server actions is open, and it can be expanded according to the client's requirements.

Handover to the Customer

After performing the settings described in this lesson, the system will be ready to be handed over to the customer.

Before the actual handover, there are some steps that need to be taken.

We need to adjust permissions. The supplier retains the role of an engineer. The installation manager at the customer's site will have the role of an administrator.

Then we set a new password for the Support account. This password will be kept by the customer for use in emergency cases.

At the end, an installation protocol will be signed and handed over to the customer together with the Support account password sealed in an envelope.