Permissions

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

In this lesson, we will explore how permissions are set and managed within the C4 System.

Understanding these principles will allow us to fully leverage the potential of the C4 to ensure secure and efficient management of resources.

Users of the C4 System are often responsible only for specific buildings, floors or departments within their company. Therefore, permissions must be set individually for each user, to ensure they can only access the information they are authorized to see.

In data security and access control, there are generally two main strategies of managing access to information.

The first strategy is a role-based security.

It restricts access based on user's roles within an organization. Roles are defined during the application's design phase, reflecting the responsibilities and needs of users.

Each role has associated permissions that determine access to various parts of the system.

For example, an Installation Manager can access all installations, a Product Manager can access all products, and an Administrator has access to all data.

This strategy is also called a column-level security.

Permissions are assigned to roles, and users acquire these permissions through their roles.

This approach is easier to implement and manage, but offers less detailed permission settings.

Therefore, complex systems often use a concept of record-based security, which controls access to individual records within the system. This approach is also known as a row-level security.

This concept is used also by the C4 System which features highly dynamic and detailed permissions settings at the row level.

If there are three Installation Managers, each assigned to a different customer, then each manager is able to view only the rows related to the installations of his respective customer.

Record-based security approach allows for very precise control over who can access or modify specific rows of data within a database.

The C4 System uses for permission management a hierarchical structure, which is a combination of both tree hierarchy and flat group hierarchy.

A tree hierarchy is a multi-level hierarchy allowing an unlimited number of levels. Each entity appears here only once and has one parent.

A flat group hierarchy is single-level, and all items within it are equal.

Let's now take a closer look at how permissions are set in the C4 System environment.

Permissions in the C4 System are managed in the Permissions tab.

In the C4 environment, a permission represents a relationship between a person and any data object managed within the system. The available data objects for which permissions can be set are listed on the left side.

In our lesson, we will use Devices as an example to demonstrate how to set permissions.

In the columns for each subsystem, you'll find various types of permissions, such as Create, Read, Edit or Delete. The number and types of these permissions reflect the extent of C4 functionality utilized by the user. Additional permissions can be added as needed in the future.

Each permission type can be assigned a value of Allow or Deny.

Access is one of the permission types, but to simplify the process for the user, access rights management is handled in its own separate tab. This tab contains only the endpoints where permissions are evaluated (typically doors and alarm areas).

Each type of permission is evaluated separately, but the same principles apply to all of them. In this lesson, we'll explain these principles using a permission of type Read as an example.

In the upcoming animations, a line will represent a Read permission assigned to a person for a device.

Permissions with an Allow value are shown in green colour, while permissions with a Deny value are shown in red. Additionally, permissions can be set with or without inheritance.

So let's now take a more detailed look at these different types of permissions and the combinations that can arise.

The basic option for setting permissions is to set it directly on the respective endpoint.

Although it is advisable to use hierarchical structures and inheritance to simplify permission management, you can also set permissions on a specific individual entity if needed.

For example, we assign permission with the Allow value directly on the card reader 102.

Permissions set directly on the entity always have the highest priority and cannot be changed by inheritance.

In the C4 System, permissions set in this way are displayed in full colour.

Another option is to set permissions with inheritance. Hierarchical system as used by the C4 allows for quick evaluation of inheritance and supports an unlimited number of levels.

This enables the user to set permissions that are automatically inherited by subordinate entities quickly and easily.

For example, if we assign permission with an Allow value on the control panel 1, it will also be inherited by all doors and card readers under this control panel.

In the C4 System, inherited permissions are displayed in faded colour.

If we want to enable permission inheritance but exclude certain nodes, we assign a permission with a Deny value on the nodes we wish to exclude.

For example, if we set an Allow value with inheritance on control panel 1, and Deny value with inheritance on door 102, then the Allow value will apply to all subordinate nodes, except for door 102 and card reader 102.

A common question regarding inheritance is, which of the permissions takes precedence when different permissions are assigned within the hierarchical structure.

For example, control panel 1 has an Allow value with inheritance, and door 102 has a Deny value with inheritance. Which value applies to card reader 102? The rule is that the permission closest to the node being evaluated takes precedence. In this case, the closest node is door 102, so the Deny value will apply.

The same rule applies in the reverse order of Allow and Deny values. In this case, card reader 102 will inherit the Allow value from door 102, which is the closest parent node.

We also have the option to set permissions without inheritance. Such permissions apply only to the specific node on which they are set and do not extend to subordinate nodes.

For example, if we set an Allow value with inheritance on control panel 1, but a Deny value without inheritance on door 102 then door 102 will have a Deny value, while card readers and other doors under this control panel will inherit the Allow value.

The same rule also applies in the reverse order of Allow and Deny values.

To simplify the assignment of permissions, the C4 System also enables creation of the so-called groups, which will be described in more detail in the upcoming part of the video.

Imagine a situation where the physical layout of subsystems in a building doesn't enable easy permission settings based on logical units. For example, we want to set permissions for all doors on a specific floor, but those doors are managed by multiple control panels. The basic device tree doesn't support this kind of organization.

Therefore, the C4 System enables creating additional logical structures called groups, which allow us to organize the entities according to our needs.

When we want to grant a person access to the first floor, we create a group consisting of all doors on that floor. We place doors 101, 102 and 103 into this group. Now we can assign the person permission to this group.

Permissions assigned to the group are also applied to the corresponding entities in the original tree.

As indicated by an arrow in the lower corner of the icons, all entities in the group are references to the existing entities in the original tree. Groups cannot contain any new entities.

There is no hierarchy within a group. All entities are at the same level. Therefore, you have to add each node directly, it is not possible to add a node along with its child nodes to the group.

In the case of devices, these groups are called access levels. They allow for the logical grouping of devices from different control panels, making access management simpler.

How are permissions calculated when groups are involved?

Think of the group as if it was placed just before the entity which is evaluated.

When control panel 2 has a Deny value that is inherited by subordinate nodes, but the first-floor group has an Allow value, then Allow value will be applied to the door 101, as the group is considered as if it was the closest node to the door.

In groups, it is recommended to work only with the Allow value. Applying Deny values for groups can significantly complicate the permission calculation process.

For certain devices, it is possible to create a special type of group called an alarm area, which contains detectors. These detectors must all be managed by the same control panel.

While the same rules apply to this group as to regular groups, there is one exception: an alarm area can be placed within the hierarchical structure of the tree, as it is an integral component of the device's configuration.

With the insights from this lesson, you are ready to set up permissions in the C4 System effectively and according to your needs.