User Profiles in the Remote

User profiles allow you to diversify access to selected elements of the **Remote** application menu structure. With user profiles you can easily restrict access to sensitive areas of installation to unauthorized persons or even create a different configuration for individual users of an intelligent building. A few examples of profiling applications:

- Parental control (restriction of access to heating, air conditioning, ventilation, alarm status, etc.).
- Access levels for employees in company.
- Access for persons from outside regularly present in the installation, eg child care, security, cleaning staff, etc.
- Temporary access for guests.
- Control of intelligent installation in hotel rooms.

User profiles can be applied to the **Page** and **Section** elements.

1. Profiles Configuration

In order to create profiles, run the **Base configurator** and go to the **Settings** tab, and then click the **Remote Authorizations** button.

Before you start creating profiles, it's worth taking the time to give paired devices names that will make it easier for you to identify them when creating profiles. Devices with the iOS after pairing are presented with the names given to them in the device settings. However, devices with the Android are visible only as a device model and a fragment of the serial number of a given device. While in the iOS we have an influence on the name of the device, unfortunately, the Android does not give us such control. However, in case user didn’t change the default device name in the iOS does or when many identical devices are paired, then we have a list of devices where it is difficult to clearly identify particular devices.
That's why in the **List of currently paired devices** we have added the **Description** column, so that you can give your own names to devices. In the description you can use spaces. Once the descriptions are ready, you can proceed to creating profiles.

At the bottom of the window you can see the profiles table. Pay attention to the information, which is written in red. Profiles are closely related to the **Remote** tab and saving profiles will cause all unsaved changes in the **Remote** tab to be discarded. Saving the profiles settings is immediately reflected in the **Remote** menu structure on mobile devices (configuration is reloaded and the view is refreshed according to the profile assignments).

1. To add a new profile, click the **Add profile**.
2. In the **User Profiles** column, enter the name of the profile (double click to start editing the field). **The name must be unique and cannot contain any special character and spaces (can use underscore character)**.
3. In the right part of the window you can see the list of paired mobile devices. The list uses names given in the **Description** column - if entered, otherwise it uses default na-

mes. From this list, please select devices to be assigned to the profile is being created.

4. Create as many profiles as you need.
5. Click the **Save** button to save settings.

The next step is assigning profiles to the elements of the **Remote** structure.

1. Go to the **Remote** tab and double click on the structure element (**Page** or **Section**) that you want to edit.
2. In the bottom part of the window there is the **Access Control** checkbox. This option is unselected by default, which makes the given structure element visible to all devices. After selecting this option, a table with defined user profiles will become active.
3. Select profiles that should have access to the edited item.
4. Click the **OK** to close the edit window.
5. Click the **Save** button to save the settings you have made. Saving the settings will automatically reload the configuration on mobile devices and will update the visibility of the edited element according to assigned user profiles.

2. How user profiles work?

The following list contains a detailed description how **Remote** user profiles work.

1. The **Page** and **Section** elements have the **Access Control** checkbox. For a newly added element and for existing configurations, it is unselected by default, which means that the given element is visible to all paired devices.
2. Selecting the **Access Control** requires to select profiles that should have access to a given structure element. If none profile is selected, then the item will be invisible on all paired devices. Nested structure elements will be invisible too (even if they have valid profiles assignment).
3. After pairing a device, assign it to the profile/profiles. All structure elements that are assigned to a given profile will automatically be visible on this device.
4. Unpairing of a device automatically removes it from all profiles to which it was assigned. Pairing the same device later requires reassignment to profiles.
5. When an element of the menu structure already has profiles assignments and then a new profile has been added, which should also have access to this element, you have to edit the configuration of the element and select the newly created profile.
6. When all profiles to which the given structure element has been assigned are deleted, then the element becomes invisible. To make it visible again, you must create at least one profile and assign the element to this profile (the element will be visible only for devices assigned to this profile) or uncheck the **Access Control** option (then the item will be visible on all paired devices).
7. Deselecting all profiles for a given structure element makes it invisible to all devices.
8. Structure elements that have modified access control preferences are marked in the configurator with a different label style of the element.
    1. Elements that are assigned to at least one profile have a green label.

2. Elements that have the option **Access Control** checked but no profile is selected are marked in orange (the item is not visible for any paired device).
3. Elements with the **Access Control** disabled have a black label (default color).
4. Elements that contain children with modified access control have bolded labels. The effect is visible only after saving the configuration in the **Remote** tab.

We hope this feature will make your smart home even smarter.