MODULES

Roles and permissions

What each role does, View / Manage permissions per module and actions that can be turned off one by one: the permissions window, a reference table of 31 permissions and 95 actions, factory examples, FAQ.

Online: mergenhub.envest.com.tr/docs/roles-and-permissions

ON THIS PAGE

- Who does what: the short answer
- How permissions work
- The permissions window in short
- Reference: 31 permissions and 95 actions
- Factory examples
- Frequently asked questions
- See also

In MergenHub four things decide what a user can see and what they can change: whether the account is **Root**, the **View** / **Manage** permissions of each module, the **actions** inside a permission that can be turned off one by one (add, edit, delete, acknowledge, download...) and **resource access** (which channels, devices and screens). A user without the permission does not see that page in the menu; a user with an action turned off does not see that button. The server applies the same rule on every request: hiding things in the interface is not the only safeguard.

This page is for version 3.10.1 and later. In the application the **?** button next to the badge, the preset row, a permission row and an action box opens a short explanation; the **Open on the site** link at the bottom of that window comes to this page, and **Detailed manual** opens the same chapter of the in-app manual (Security & Authorization). For accounts, password and session policy, HTTPS and auditing see Users, groups and security.

Who does what: the short answer

There is no role selector in this interface. The permissions of an account come from a **preset** or from its **group** and are adjusted one by one in the permissions window; for a super administrator tick the Root box in the user list. In short, "roles" are three things: four presets, Root and your own groups. In the user list, in the permissions window and in the profile, the **?** button next to the badge opens the **Presets and Root** window that explains them.

WHAT	WHAT IT DOES	WHO GETS IT
Viewer preset	Sees the project tree and live values, SCADA screens, counters, the water pages, reports and automation flows. Cannot change anything or write to tags; does not see alarms or data logs.	Those who only watch: managers, visitors, dashboard screens. Every new account created in the interface starts with these permissions.
Operator preset	Runs the plant (writes to tags, acknowledges alarms, sees the modules) but changes no definition.	Shift operators.

WHAT	WHAT IT DOES	WHO GETS IT
Maintenance preset	On top of the Operator preset defines channels / devices / tags, designs screens, manages the modules. Cannot enter the server settings.	Maintenance and automation staff.
Manager preset	Everything except the Root-only jobs (including the server settings). The permissions and actions given by the preset can be turned off one by one afterwards.	Plant or IT managers.
Root (super administrator)	Does everything, plus the Root-only jobs: users and groups, resource access, retention, security, backup, full project export / import, deleting audit and event records. Given with the Root box in the user list.	The owner of the system. At least one, at most a few people; not used for daily operation.
Groups	Create a group for each job in the plant (e.g. Shift Operator, Maintenance, Energy): give the permissions to the group and assign the user to it.	Everyone who does the same job. When people change only the group membership changes; the permissions are managed in one place.

Note The **Add user** window creates the account as a Viewer; if the Root box in that window is ticked the account becomes Root. The box in the **Super-admin** column of the list grants or removes Root later (next to the box it says **Make Root** on an account that is not Root and **Root** on a Root account; when it is removed the account becomes a Viewer; the last Root cannot be demoted). The badge under the box shows the role of the account: **Viewer** or **Root**. In daily use there is no need to change a role: what a user does is decided by their group and the **Permissions** window.

Note The server keeps a role name on every account (Viewer, Operator, Admin, Root). An account created in the interface is Viewer or Root; Operator and Admin are seen only on accounts created in an older version or through REST (the badge says **Operator**, **Administrator**). The permissions window of such an account shows the **Remove role, keep permissions** button; the details are below, under "Roles on old accounts and accounts created through the API".

How permissions work

FOUR LAYERS

LAYER	QUESTION	WHERE IT IS SET
1. Root	Is the account Root (super administrator) or an ordinary account? Root does everything; what an ordinary account can do comes from the three layers below.	Users list, **Super-admin** column
2. Permission (31 names)	Which module does the user **view**, which one do they **manage**? The permission is the door of the module: without View the page is not in the menu. Manage carries View with it.	**Permissions** window: the View / Manage boxes
3. Action (95 names)	In a module they manage, which job can they not do (delete, acknowledge, download)? Actions are managed by **turning them off**: whoever has the permission does all of its actions, and the administrator turns off the ones not wanted.	**Permissions** window: **Details** on the row
4. Resource access	On which channels, devices, zones and screens do they do all this?	The **Access** button (user or group row)

All four are checked together: a user who has Alarms: View and the "Acknowledge alarms" action, but no access to the tag of an alarm, does not see that alarm.

WHERE A PERMISSION COMES FROM

- **Group (recommended).** A permission set and the turned-off actions are given to the group and its members inherit them. A user is assigned to a group in the **Group** column of the Users list. Five people doing the same job are managed in one place.
- **User-specific permissions.** In the **Permissions** window of the user row you clear **No custom permissions (use the group's permissions)** and apply a preset or tick the boxes one by one. The button of a user with custom permissions shows a small dot.
- **If there is neither.** If the user has neither a group nor custom permissions, the account works with the permissions of the Viewer preset. On an old account or one created through the API with the Operator or Administrator role, the set of the role applies (below, "Roles on old accounts and accounts created through the API").

HOW A USER AND THEIR GROUP COMBINE

- **Permissions are combined.** If the user has both custom permissions and a group, the union of the two applies: a permission held by either one is enough.
- **For a grouped user without custom permissions only the group applies.** The starting permissions of an account without a group (the Viewer preset) are not added to the group; this user has no profile of their own, and in their permissions window the action boxes are locked and show the restrictions of the group. The note in the window tells the way: to turn actions off for this user only, clear "No custom permissions" or edit the permissions of the group.
- **Actions are combined as well.** An action can be done if at least one of the sources allows it. This is why an action turned off on the user stays on if their group gives the same permission without restriction. To really turn an action off, turn it off in the group too or take the user out of the group.
- **An old account with the Administrator (Admin) role is always fully permitted.** Even if permission boxes are cleared or actions are turned off it does all of them; the action boxes are locked. To restrict it press **Remove role, keep permissions** in the permissions window: the account is switched to the Viewer role and its current permissions are saved as custom permissions; its access does not change, and permissions and actions can then be turned off one by one. A new manager needs no role: use the **Manager** preset or a group.
- **Viewing is not a separate action.** The permission itself is entering and viewing the module. A user with all actions turned off still sees the module; if they should not, clear the View box.
- **A new action arrives turned on.** Because the list of turned-off actions is what is stored, an action added in a later version is open to everyone who has its parent permission.
- **Changes take effect at once.** Permissions and restrictions are evaluated on every request; the user does not have to sign out and in. Every change is written to the audit log (who, for whom, permissions added / removed, actions turned off / on).
- **The same rule on every way in.** The web interface, the REST API, the mobile app, data access keys, external MCP tokens and the in-app assistant all pass through the same set of permissions and actions.

PRESETS

The preset buttons in the permissions window fill the boxes with one click and clear the action restrictions. A preset is a starting point: after applying it you change the boxes one by one and turn actions off with **Details**.

PRESET	WHAT IT TICKS
Viewer	View: Connectivity, SCADA, Counters and Metrics, Water Management, Reports, Automation. No Manage, no operations and tools, no system permission. No Alarms or Data Logs either.
Operator	Viewer + Alarms: View (watch and acknowledge), Data Logs: View, Tag write and services, OPC UA client, AI assistant. Cannot change any definition (no Manage).
Maintenance	Operator + Manage on every module, Data Bridge, Templates and import, MCP, Certificates, Firewall, Audit log. No Server settings or Notification settings.
Manager	Everything in the window except Script execution.

The "Operator" preset and the Operator role on old accounts are not the same thing: the preset changes no definition, the role manages every module (the table below).

ROLES ON OLD ACCOUNTS AND ACCOUNTS CREATED THROUGH THE API

The server keeps a role name on every account (Viewer, Operator, Admin, Root). An account created in the interface is Viewer or Root; Operator and Admin are seen only on accounts created in an older version or through REST. The badge shows the name of the role. The role decides the permission set that applies while the account has neither a group nor custom permissions:

BADGE (NAME ON THE SERVER)	WITHOUT A GROUP AND CUSTOM PERMISSIONS	NOTE
Viewer (Viewer)	The same as the Viewer preset: views Connectivity, SCADA, Counters and Metrics, Water Management, Reports and Automation. No Alarms, Data Logs, Data Bridge, OPC UA client, assistant or Settings.	Every new account created in the interface starts with this role. Permissions are given from a preset or a group and then adjusted one by one in the permissions window.
Operator (Operator)	View and Manage on every module, Data Bridge, Tag write and services, OPC UA client, Templates and import, AI assistant, MCP, Audit log. No Server settings, Notification settings, Certificates or Firewall.	Found only on accounts created in an older version or through REST. If it has a group or custom permissions, those apply. For a new account use a preset or a group for the same scope.
Administrator (Admin)	Everything except the Root-only jobs and Script execution.	Found only on accounts created in an older version or through REST. This role cannot be narrowed: neither permission boxes, nor a group, nor action restrictions are applied. To restrict it: **Remove role, keep permissions**.
Root (Root)	Everything.	Given with the box in the **Super-admin** column of the Users list; the last Root cannot be demoted.

Remove role, keep permissions: if the role of the account is Operator or Administrator, the permissions window shows an information row and this button under the hint; a Viewer or Root account has no such button. When you press the button and confirm the question, the current permissions of the account are saved as custom permissions and then the account is switched to the Viewer role; its access does not change. The message "Role

removed; the permissions were kept as custom permissions." appears and the window opens again. From then on the View / Manage boxes and the actions under **Details** can be turned off one by one on this account too.

The button works even if the system has a single Administrator (Admin) account: while there is an enabled Root account the server allows the role of the last Administrator account to be removed and the account to be disabled or deleted (the last enabled Root is protected separately). The server refuses to change the role of the last enabled Administrator (Admin) account only if there is no enabled Root account: in that case the account keeps its role and its access still does not change. The role can also be changed through the REST API (`PUT /auth/v1/users/{name}` , body `{ "role": "Viewer" }` ; Root only).

ROOT-ONLY JOBS

The following cannot be given to any user or group; only a Root account does them (neither the Manager preset nor an old account with the Administrator role can):

- User and group management, resource access (channel / device restriction), assistant and MCP security administration.
- The **Retention**, **Security** and **Backup** tabs in Settings; the backup list, the configuration version history and reverting to a version; changing the e-mail / SMS sending server.
- Deleting the audit log and the event history.
- Exporting and importing the full project (**Export** / **Import** on the Connectivity page; Kepware JSON import included).
- Turning on anonymous access for a REST Server agent of the Data Bridge.

PERMISSIONS AND RESOURCE ACCESS ARE NOT THE SAME THING

Permissions and actions answer "which job can they do"; resource access answers "on which channels, devices, zones and screens". A user who is not Root does not see a channel or device they were not given access to; in the **Access** window the **All Connectivity (every channel + device)** box opens all connectivity and the **All SCADA (every zone + screen)** box opens all screens. Both are checked together: a user with Water Management: View sees on the water pages only the counters of the devices they can reach. A request like "this user must never see the devices of that line" is met with resource access, not with a permission.

The permissions window in short

Location: **Settings › Access › Users**. Only a Root account sees this tab. It has the **Users** and **User Groups** cards; the **Permissions** button on a row opens the permissions window (**Group Permissions** for a group).

1. **Choose a starting point.** For a user clear **No custom permissions (use the group's permissions)**; click one of the presets (**Viewer**, **Operator**, **Maintenance**, **Manager**) or pick a similar record from the **Copy from another user / group...** list. While the box is ticked the user has no custom permissions and the View / Manage boxes are only shown (for a grouped user the permissions of the group; for a user without a group the permissions of the Viewer preset).
2. **Tick the View / Manage boxes.** The window has three sections: **Modules** (one row per module, two columns: View and Manage; buttons **View all**, **Manage all**, **Clear**), **Operations and tools** and **System**. Ticking Manage ticks View as well; clearing View clears Manage. The Data Bridge row has a single box (**View and manage**).

3. **Turn actions off.** The **Details** button at the right of a row opens the actions of that permission. Objects such as channels, devices and tags are in a grid: one row per object, columns **Add**, **Edit**, **Delete**. The other actions are single boxes ("Acknowledge alarms", "Download reports", "Write to tags"...). Clearing a box turns the action off; the row gets a badge such as "restricted: 2 actions off".
4. **Search and filter.** The search box at the top filters by permission or action name; **Show only what is turned off** lists the actions that are turned off.
5. **Read the summary.** The **CAN** and **CANNOT** boxes at the bottom of the window state the result in plain text, module by module; what the group gives is marked "(from the group)".
6. **Save.** In the Users list a one-line summary appears under the name: "Alarms: Manage (delete alarm definition off)". For an old account with the Administrator (Admin) role it says "Administrator: fully permitted".

> **Tip** Every user sees the **My permissions** heading in their own **My profile** window: the permission summary, a **?** next to it (the Presets and Root window) and the **What can I do and what can I not?** row. This is the first place to look when a user says "I cannot see a button".

Reference: 31 permissions and 95 actions

The tables below are the reference for every row of the permissions window and every action box under **Details**: **31 permissions** and **95 actions** in 16 modules. Names are as they appear in the window. The Key column is the name used in the REST API, in the 403 response and in the audit log: a permission name looks like `AlarmsManage`, an action key like `alarms.ack`.

How to read the tables:

- **A bold row is a permission** (a View box, a Manage box or a single box in the window). Without the permission the module is not seen or not managed; its actions are not looked at.
- **The rows under it are the actions of that permission.** When the permission is granted they are all on; they are turned off one by one with **Details**. For an action that is off, the button, the right-click menu item and the keyboard shortcut do not work; the server also refuses the same job over REST, the assistant and MCP.
- A permission without actions (e.g. Connectivity: View, SCADA: View, Automation: View, Firewall, Audit log) is simply granted or not.
- Actions cannot be turned off for Root or for an old account with the Administrator (Admin) role (on an Admin account first use **Remove role, keep permissions**; see "Roles on old accounts and accounts created through the API" above).

General rules:

- **Copying counts as adding** (copying a channel = "Add channel"); bulk delete needs the "delete" action.
- Adding / editing / deleting a **tag group** and **tag generation** are tag actions.
- **Reports, report pages and counter tracking lists** are one family of actions (add / edit / delete; no distinction by kind).
- **Three export actions are applied in the interface only** (`alarms.export`, `metering.export`, `water.export`): the file is produced in the browser and the button is hidden; a user who can see the same data can read it over REST. Data Logs export and report download are refused on the server as well.
- **With edit turned off the window opens read-only**: values are visible, Save and Delete are not shown.

- **With reload turned off** the user saves a definition; the change does not reach the running system until someone who may reload applies it.
- **A refusal by the server** is shown in the interface with the name of the action: "You have no permission for this action: Delete alarm definition".

CONNECTIVITY

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Connectivity: View (permission)	`Config Read`	Sees the project tree (channels, devices, tags), the Virtual Tag and Tag Shortcut pages, live values and the event log.	Example: Without it the user signs in but the project tree stays empty; most modules also need it.
Connectivity: Manage (permission)	`Config Write`	Adds, edits and deletes channels, devices, tags, Virtual Tags and Tag Shortcuts. In the details Add / Edit / Delete can be turned off per object.	Example: A maintenance technician can keep tag add / edit on and have channel and device delete turned off.
Add channel	`channel.create`	Adds a new channel. Copying a channel also counts as adding.	When off, the add button does not appear; existing items stay visible.
Edit channel	`channel.edit`	Changes the settings of an existing channel.	When off, the window opens read-only: the Save button does not appear.
Delete channel	`channel.delete`	Deletes a channel. When a channel is deleted, "Delete device" / "Delete tag" are not checked separately for the devices and tags inside it.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Add device	`device.create`	Adds a new device. Copying a device and importing devices from a file also count as adding.	When off, the add button does not appear; existing items stay visible.
Edit device	`device.edit`	Changes the settings of an existing device.	When off, the window opens read-only: the Save button does not appear.
Delete device	`device.delete`	Deletes a device. When a device is deleted, "Delete tag" is not checked separately for the tags inside it.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Add tag	`tag.create`	Adds a new tag. Tag groups and bulk / CSV tag operations are included.	When off, the add button does not appear; existing items stay visible.
Edit tag	`tag.edit`	Changes the settings of an existing tag. Tag groups and bulk / CSV tag operations are included.	When off, the window opens read-only: the Save button does not appear.
Delete tag	`tag.delete`	Deletes a tag. Tag groups and bulk / CSV tag operations are included.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Add Virtual Tag	`vtag.create`	Adds a new Virtual Tag.	When off, the add button does not appear; existing items stay visible.
Edit Virtual Tag	`vtag.edit`	Changes the settings of an existing Virtual Tag.	When off, the window opens read-only: the Save button does not appear.
Delete Virtual Tag	`vtag.delete`	Deletes a Virtual Tag.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Add Tag Shortcut	`alias.create`	Adds a new Tag Shortcut.	When off, the add button does not appear; existing items stay visible.
Edit Tag Shortcut	`alias.edit`	Changes the settings of an existing Tag Shortcut.	When off, the window opens read-only: the Save button does not appear.
Delete Tag Shortcut	`alias.delete`	Deletes a Tag Shortcut.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.

SCADA

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
SCADA: View (permission)	`Scada`	Opens and runs SCADA screens.	Example: With only this the user watches screens; giving commands also needs Tag write.
SCADA: Manage (permission)	`ScadaDesign`	Designs screens: adds, edits and deletes screens; manages the library, artwork and the zone tree.	Example: A designer can keep screen edit on and have screen delete turned off.
Add screen	`screen.create`	Adds a new screen. Duplicating a screen and importing one from a file also count as adding.	When off, the add button does not appear; existing items stay visible.
Edit screen	`screen.edit`	Changes the settings of an existing screen. Editing and saving a screen in design mode (adding objects, drawing) is this action; so are the assistant tools that change a screen.	When off, the window opens read-only: the Save button does not appear.
Delete screen	`screen.delete`	Deletes a screen.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Symbol library	`scada.library`	Adds, renames and deletes own objects and symbols in the library.	When off, the designer uses library objects but cannot save new ones.
Screen artwork	`scada.art`	Uploads the background artwork files of screens to the server. Artwork is uploaded while a Device Library package is installed.	When off, the screens of a package installed from the library are created but the artwork files are not uploaded; the install report says so.
Zone tree	`scada.zones`	Adds, edits and deletes the zones (area / plant tree) that group the screens.	When off, the zone editor does not open; screens are added to existing zones.
Watch cameras	`camera.view`	Watches the live video in the Camera component of SCADA screens and takes snapshots. Part of SCADA: View.	When off, the screen opens and the camera box says "You have no permission to watch cameras"; no video leaves the server.

ALARMS

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Alarms: View (permission)	`Alarms`	Sees active alarms and the alarm history; acknowledges alarms and exports the history.	Example: For a watch-only dashboard acknowledging can be turned off: the alarm is visible, Acknowledge is not.
Acknowledge alarms	`alarms.ack`	Acknowledges an active alarm.	When off, the user sees the alarm but the Acknowledge button does not appear.
Export alarm history	`alarms.export`	Downloads the alarm history as a file (CSV / Excel). This restriction is applied in the interface: the file is produced in the browser, so there is no separate block on the server.	When off, the history is visible on screen but the download button does not appear.
Alarms: Manage (permission)	`AlarmsManage`	Adds, edits and deletes alarm definitions.	Example: A shift operator can keep definition edit (changing limits) on and have add and delete turned off.
Add alarm definition	`alarmdef.create`	Adds a new alarm definition.	When off, the add button does not appear; existing items stay visible.
Edit alarm definition	`alarmdef.edit`	Changes the settings of an existing alarm definition.	When off, the window opens read-only: the Save button does not appear.
Delete alarm definition	`alarmdef.delete`	Deletes an alarm definition.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.

DATA LOGS

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Data Logs: View (permission)	`DataLogging`	Queries the logged history, views trend charts and exports data.	Example: A quality officer sees and downloads the history but cannot define log groups.
Export logged data	`log.export`	Downloads the logged history as CSV / Excel.	When off, the chart and table are visible but the download buttons do not appear.
Data Logs: Manage (permission)	`DataLoggingManage`	Adds, edits and deletes log groups; chooses the logging target; deletes old data.	Example: With delete old data turned off the user defines groups but cannot delete logged data.
Add log group	`loggroup.create`	Adds a new log group.	When off, the add button does not appear; existing items stay visible.
Edit log group	`loggroup.edit`	Changes the settings of an existing log group.	When off, the window opens read-only: the Save button does not appear.
Delete log group	`loggroup.delete`	Deletes a log group.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Delete old data	`log.purge`	Permanently deletes the records of a log group older than a date.	When off, the "delete old data" row does not appear.

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Logging target	`loggroup.target`	Creates the table in the target database for a log group, moves an old group to a data source.	When off, the "Create table" and "Move to data source" buttons do not appear in the group window.

COUNTERS AND METRICS

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Counters and Metrics: View (permission)	`Metering`	Sees the counter and metric lists, their status, period data and events; exports data.	Example: An energy officer watches consumption and takes it to Excel.
Export counter data	`metering.export`	Downloads the counter period report as Excel / CSV. This restriction is applied in the interface: the file is produced in the browser, so there is no separate block on the server.	When off, the tables are visible but the download buttons do not appear.
Counters and Metrics: Manage (permission)	`MeteringManage`	Defines counters and metrics, enters manual values, makes corrections, manages categories and groups.	Example: With only "Enter manual values" on, the user enters invoice and analysis values and cannot touch definitions.
Add counter	`counter.create`	Adds a new counter.	When off, the add button does not appear; existing items stay visible.
Edit counter	`counter.edit`	Changes the settings of an existing counter.	When off, the window opens read-only: the Save button does not appear.
Delete counter	`counter.delete`	Deletes a counter.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Correct counters	`counter.correct`	Makes a manual adjustment on a measured counter, records a meter replacement, sets the total, decides on a reset.	When off, the "Manual adjustment", "Meter replacement", "Set total" and reset decision buttons ("Count from zero", "Take as new base") do not appear in the counter window.
Add metric	`metric.create`	Adds a new metric. Manual input DEFINITIONS also count as metrics.	When off, the add button does not appear; existing items stay visible.
Edit metric	`metric.edit`	Changes the settings of an existing metric. Manual input DEFINITIONS also count as metrics.	When off, the window opens read-only: the Save button does not appear.
Delete metric	`metric.delete`	Deletes a metric. Manual input DEFINITIONS also count as metrics.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Enter manual values	`input.enter`	Writes period values to manual inputs and manual counters (including rainfall, analysis, production, personnel and invoice entries on the water pages).	If only this is left on, the user enters monthly invoice and analysis values but cannot define counters or metrics.

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Categories and groups	`taxonomy.manage`	Adds, renames, deletes and colours the counter / metric categories and the group tree. For users who can reach all connectivity; users with restricted resource access cannot use it.	When off, the "Categories and groups" button does not appear.

WATER MANAGEMENT

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Water Management: View (permission)	`Water`	Sees the Water Footprint, Water Efficiency and Water Flow Diagram pages; exports reports. The feature group must also be on.	Example: A user with only this sees only the Water Management pages in the menu.
Export water reports	`water.export`	Downloads the Water Footprint, Water Efficiency and Water Flow Diagram tables as Excel / CSV / PDF. This restriction is applied in the interface: the file is produced in the browser, so there is no separate block on the server.	When off, the pages are visible but the download buttons do not appear.
Water Management: Manage (permission)	`WaterManage`	Defines, edits and deletes water profiles and diagrams; runs the setup wizard.	Example: A water officer edits profiles; defining counters also needs Counters and Metrics: Manage.
Add water profile	`waterprofile.create`	Adds a new water profile. Water Footprint and Water Efficiency profiles and Water Flow Diagrams.	When off, the add button does not appear; existing items stay visible.
Edit water profile	`waterprofile.edit`	Changes the settings of an existing water profile. Water Footprint and Water Efficiency profiles and Water Flow Diagrams.	When off, the window opens read-only: the Save button does not appear.
Delete water profile	`waterprofile.delete`	Deletes a water profile. Water Footprint and Water Efficiency profiles and Water Flow Diagrams.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Water setup wizard	`water.setup`	Asks for sources and uses and sets up counters, the diagram and the reports. Also needs Counters and Metrics: Manage.	When off, the "Setup wizard" button does not appear.

REPORTS

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Reports: View (permission)	`Reports`	Opens, runs and downloads reports, report pages and counter tracking lists.	Example: A manager opens a report and downloads the PDF but cannot change its design.
Download reports	`report.download`	Downloads a report, a report page and a counter tracking list as Excel / PDF / CSV. While off, the data access keys of the user (reports read by external systems) also get 403.	When off, the report opens on screen but the download buttons do not appear.

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Reports: Manage (permission)	`ReportsManage`	Designs, edits and deletes reports, report pages and counter tracking lists.	Example: A reporting specialist can keep design on and have delete turned off.
Add report	`report.create`	Adds a new report. Table reports, report pages and counter tracking lists; no distinction by kind.	When off, the add button does not appear; existing items stay visible.
Edit report	`report.edit`	Changes the settings of an existing report. Table reports, report pages and counter tracking lists; no distinction by kind.	When off, the window opens read-only: the Save button does not appear.
Delete report	`report.delete`	Deletes a report. Table reports, report pages and counter tracking lists; no distinction by kind.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.

AUTOMATION

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Automation: View (permission)	`Workflows`	Sees the automation flows and the run history.	Example: An operator sees which flow ran when but cannot change the flow.
Automation: Manage (permission)	`WorkflowsManage`	Defines, edits, deletes and enables / disables flows.	Example: Enable / disable can stay on with edit off: the user stops a flow but cannot change it.
Add flow	`workflow.create`	Adds a new flow.	When off, the add button does not appear; existing items stay visible.
Edit flow	`workflow.edit`	Changes the settings of an existing flow.	When off, the window opens read-only: the Save button does not appear.
Delete flow	`workflow.delete`	Deletes a flow.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.
Enable / disable flows	`workflow.enable`	Enables or disables a flow.	When off, the on / off switch does not appear in the list or the editor.

DATA BRIDGE

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Data Bridge (permission)	`DataBridge`	Sees, adds, edits, deletes and tests the data bridge agents (MQTT, REST). A single permission.	Example: An integration officer can keep agent edit on and have delete turned off.
Add agent	`agent.create`	Adds a new agent.	When off, the add button does not appear; existing items stay visible.
Edit agent	`agent.edit`	Changes the settings of an existing agent. The general switches on the Data Bridge tab are also saved with this action.	When off, the window opens read-only: the Save button does not appear.
Delete agent	`agent.delete`	Deletes an agent.	When off, the Delete button and Delete in the right-click menu do not appear: accidental deletion is prevented.

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Test agents	`agent.test`	Sends a trial request to the target of an agent, previews a report agent.	When off, the "Test request" and preview buttons do not appear.

TAG WRITE AND SERVICES

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Tag write and services (permission)	`RuntimeControl`	Writes values to tags, reloads the runtime, starts / stops services, runs device diagnostics, runs flows by hand.	Example: A shift operator keeps only "Write to tags" on; stopping services is turned off.
Write to tags	`tag.write`	Writes a value to a tag from the interface, a SCADA screen or REST (start a pump, set a setpoint).	When off, the pencil icon on tag rows and the command buttons on SCADA screens do not work; values stay visible.
Reload the runtime	`runtime.reload`	Applies a configuration change to the running system (scanning is rebuilt).	When off, the user saves a definition but the change does not reach the running system until someone who may reload applies it.
Start / stop services	`service.control`	Starts, stops and restarts the scan engine and the OPC UA server; turns auto-restart on and off.	When off, the Start / Stop / Restart buttons do not appear on Settings › Services.
Device diagnostics	`diag.run`	Watches the raw packets exchanged with a device (the diagnostics window). The assistant's network diagnostics tools (ping, TCP, DNS, local ports) are also tied to this action.	When off, Diagnostics does not appear on the device page or in the right-click menu.
File upload	`file.upload`	Uploads a certificate or an SCL / ICD file for a channel / device setting.	When off, the Browse buttons do not appear in the properties window.
Run a flow by hand	`workflow.run`	Starts an automation flow immediately with the Run button. Also needs Automation: View.	When off, the Run button does not appear; scheduled and tag-triggered flows keep running.

OPC UA CLIENT

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
OPC UA client (permission)	`OpcClient`	Uses the built-in OPC UA Client page: connects, browses, subscribes, writes.	Example: A commissioning engineer connects to a remote server and checks values; writing to it can be turned off.
Connect and discover	`uaclient.connect`	Connects to and disconnects from a remote OPC UA server, discovers servers, scans the network.	When off, the connection state and subscriptions are visible but the Connect button does not appear.
Write to the remote server	`uaclient.write`	Writes a value to a node on the connected OPC UA server.	When off, the node can be read but the Write button does not appear.
Subscriptions	`uaclient.subscribe`	Subscribes to nodes and removes subscriptions.	When off, existing subscriptions are watched but new ones cannot be added.

TEMPLATES AND IMPORT

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Templates and import (permission)	`Import`	Installs and packages templates, does partial imports. Full project export / import is Root only.	Example: An outside contractor can keep template install on and have template delete turned off.
Install templates	`template.install`	Installs a template into the project (adds channels, devices, tags and screens). The "add" actions are not checked separately for the channels, devices, tags and screens it creates.	When off, templates are visible but the install button in the template window does not work.
Package templates	`template.package`	Builds a reusable template from part of the project; imports a template from a file (.mhtpl). Editing a saved template is also this action.	When off, the "Make Template" and "Import (.mhtpl)" buttons do not appear.
Delete templates	`template.delete`	Deletes a saved template.	When off, the Delete button does not appear in the template window.

AI AND MCP

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
AI assistant (permission)	`Ai`	Uses the AI assistant. Every tool the assistant runs also needs the permission for that job.	Example: The assistant cannot do on the user's behalf what the user cannot do.
MCP (permission)	`Mcp`	Uses the MCP (AI) page: creates tokens for an external AI client.	Example: A token does only what its owner is permitted to do.
MCP tokens	`mcp.token`	Creates and deletes personal connection tokens for an external AI client.	When off, the MCP page is visible but new tokens cannot be created.
Script execution (permission)	`AiScripts`	The assistant may run Python / PowerShell in the sandbox on behalf of this user. Dangerous; granted only explicitly.	Example: The feature must also be enabled by the system administrator; every run asks for confirmation.
AI provider (inside the Server settings permission)	`ai.provider`	Defines and tests the provider and model profile the assistant uses.	When off, the Providers and MCP tabs do not appear in the assistant settings; the user talks to the assistant but cannot define a provider or an API key.
Assistant skills (inside the Server settings permission)	`ai.skills`	Adds, edits and deletes the skills of the assistant. The assistant's "save skill" tool is also tied to this action.	When off, the Skills tab does not appear in the assistant settings.
Extra instructions (inside the Server settings permission)	`ai.prompt`	Writes plant-specific extra instructions for the assistant.	When off, the extra instructions field in the assistant settings is read-only; the text cannot be changed.

SERVER SETTINGS AND SYSTEM

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Server settings (permission)	`Settings`	Manages the server settings. In the details every settings section can be turned off separately.	Example: A corporate communications officer can be left with only the Branding section.
OPC UA server settings	`settings.opcua`	Endpoints, security policies and OPC UA users.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Web and REST API settings	`settings.api`	Listen address, HTTPS and trusted proxies.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Mobile access settings	`settings.mobile`	Mobile app sign-in, push notifications and device sessions.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Branding settings	`settings.brand`	Logo, name, login screen and e-mail appearance. The SCADA map tile address is also saved with this action.	If only this is left on, the user sees only the Branding tab on the Settings page.
Feature groups	`settings.features`	Turns the feature groups of the left menu (e.g. Water Management) on and off.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
License	`settings.license`	Activates and releases the license, checks for updates.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Data sources	`settings.datasources`	Manages external database connections and the mirroring of counter data to an external database (data store).	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Services and resource thresholds	`settings.services`	Manages the service status page, the resource warning thresholds and Windows service startup. Covers the Monitoring (resource thresholds) and Service settings sections; starting / stopping a service is a separate action (Start / stop services).	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Data access keys	`settings.accesskeys`	Creates and deletes keys that let external systems read reports.	When off, keys cannot be created in the "reading from external systems" window of a report.
Scan settings	`settings.scan`	Changes the scan engine settings.	This section has no tab in the interface; the setting is changed through REST or MCP. When off, the user can neither read nor change this section.

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Camera settings	`settings.cameras`	Defines the IP cameras (RTSP address, user, password) and the video engine.	When off, the Settings › Cameras tab does not appear; cameras on screens can still be watched.
VPN management	`vpn.admin`	Turns MergenHub VPN on / off; adds, changes and revokes field modems; issues one-time configuration links.	When off, the Plug-ins › VPN page is view-only: status and the site list are visible, nothing can be changed.
Firewall (permission)	`Firewall`	Opens the required ports in the Windows firewall.	Example: The "open ports" button on Settings › OPC UA server appears with this permission.
Audit log (permission)	`Audit`	Sees the audit log (who did what and when). Deleting records is Root only.	Example: A shift supervisor follows who wrote which value here.

NOTIFICATION SETTINGS

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Notification settings (permission)	`Notifications`	Manages the e-mail, SMS and Communication Center settings (on / off, sender name, recipients, test, templates). The sending server is set by Root only.	Example: With only the Communication Center on, the user edits message templates but cannot touch the e-mail and SMS settings.
E-mail settings	`notify.email`	Turns e-mail notification on / off, sets the sender name and the recipients, sends a test e-mail. The sending server (address, port, credentials) is set by Root only.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
SMS settings	`notify.sms`	Turns SMS notification on / off, sets the sender name and the recipients, sends a test SMS. The provider connection (address, credentials) is set by Root only.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Communication Center	`notify.comm`	Edits message templates, sends user invitations and bulk messages.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Slack / Telegram settings	`notify.chat`	Turns Slack and Telegram notification on / off, sets the Slack webhook, the Telegram bot and chats, sends a test message.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.

CERTIFICATES

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Certificates (permission)	`Certificates`	Manages the OPC UA trust list, the server certificate and the web certificate.	Example: A commissioning engineer trusts a new client's certificate; the web certificate can be left off.
Client certificates	`cert.trust`	Trusts, rejects, imports and deletes OPC UA client certificates.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
Server certificate	`cert.instance`	Shows the OPC UA server's own certificate.	When off, the tab of this section does not appear on the Settings page; the user can neither see nor change these settings.
Web certificate	`cert.web`	Generates, uploads and removes the HTTPS certificate.	When off, the web certificate buttons (generate, upload, remove) on the Settings › Web, REST API & Mobil tab do not appear.

ROOT ONLY (PERMISSIONS THAT CANNOT BE GRANTED)

PERMISSION / ACTION	KEY	WHAT IT OPENS	WHEN OFF / EXAMPLE
User and group management (permission)	`Users`	Manages users and groups. Root only.	Example: Cannot be given to another user or group.
Resource access (channel / device restriction) (permission)	`Acl`	Decides which channels / devices users and groups can reach. Root only.	Example: Cannot be given to another user or group.
Assistant and MCP security administration (permission)	`AiAdmin`	Manages the assistant and MCP security settings (script sandbox, approval mode, external MCP servers). Root only.	Example: Cannot be given to another user or group.

Factory examples

In a factory every area has a different job and responsibility. The examples below show, for typical duties, which boxes to tick in the permissions window, which actions to turn off under **Details** and how to give resource access. They are a starting point: add and remove boxes to suit your own plant.

Steps common to every example:

1. **Create a group. Settings › Access › Users**, **Add Group** on the **User Groups** card; type the group name (e.g. Shift operators).
2. **Apply the preset and adjust the boxes.** Click the preset button named in the example, then tick or clear the View / Manage boxes.
3. **Turn actions off.** Click **Details** on the row and clear the boxes the example says to turn off; read the **CAN** / **CANNOT** summary at the bottom and click **Save**.
4. **Assign the user to the group.** On the **Users** card pick the group in the user's **Group** column. If the user has custom permissions (a dot on the Permissions button), open their window and tick **No custom permissions (use the group's permissions)**; otherwise their custom permissions are combined with the group and an action you turned off in the group may stay on for that user.
5. **Give resource access.** The **Access** button on the group row: tick the channels, devices, zones and screens.

1. SHIFT OPERATOR: WATCHES, ACKNOWLEDGES ALARMS, WRITES TO TAGS; DOES NOT TOUCH DEFINITIONS

- **Preset:** Operator. View only on every module; no Manage. Remove OPC UA client if it is not needed.
- **Actions to turn off:** Tag write and services › Details: leave only "Write to tags" on; clear "Reload the runtime", "Start / stop services", "Device diagnostics", "File upload" and "Run a flow by hand". "Acknowledge alarms" and "Download reports" stay on.

- **Resource access:** the channels, devices and SCADA zone of the line the shift is responsible for.
- **Result:** watches screens, gives commands with SCADA buttons, acknowledges alarms, looks at history and trends. Opens an alarm definition read-only; cannot add channels, devices, tags, screens or log groups; cannot stop a service.

2. SHIFT SUPERVISOR: WHAT THE OPERATOR DOES + CHANGING LIMITS, STOPPING FLOWS, AUDITING

- **Preset:** Operator; in addition Alarms: Manage, Automation: Manage and Audit log.
- **Actions to turn off:** Alarms › Details: on the alarm definition row Add and Delete off, Edit on (changes limits, cannot add or delete definitions). Automation › Details: on the flow row Add, Edit and Delete off, "Enable / disable flows" on (stops a flow, cannot change it). Tag write and services › Details: "Write to tags", "Run a flow by hand" and "Device diagnostics" on; "Start / stop services" and "File upload" off.
- **Resource access:** all the lines they are responsible for.
- **Result:** in addition to what the operator does, changes alarm limits, stops and starts a flow or runs it by hand, and follows who wrote which value on the **Settings › Audit** tab.

3. MAINTENANCE / AUTOMATION TECHNICIAN: ADDS AND EDITS CHANNELS, DEVICES AND TAGS; CANNOT DELETE

- **Preset:** Maintenance. Remove what is not their job: Water Management: Manage, Reports: Manage, Data Bridge, MCP, Certificates, Firewall.
- **Actions to turn off:** Connectivity › Details: the five boxes in the Delete column of the grid (channel, device, tag, Virtual Tag, Tag Shortcut). If you wish, in the same way SCADA › screen Delete, Alarms › alarm definition Delete, Data Logs › log group Delete and "Delete old data", Templates and import › "Delete templates". Tag write and services › leave "Reload the runtime" on (otherwise a tag they add does not reach the running system); "Start / stop services" off.
- **Resource access:** the channels of the lines they are responsible for. They always see a channel and a screen they added themselves.
- **Result:** adds channels, devices and tags, changes their properties, runs device diagnostics, installs templates. The Delete button, Delete in the right-click menu and the Delete key do not work. Turn the three delete boxes off together: if "Delete channel" stays on, a channel can be deleted together with the devices and tags inside it.

4. ENERGY / WATER OFFICER: WATCHES COUNTERS AND THE WATER PAGES, ENTERS MANUAL VALUES; CANNOT DEFINE COUNTERS

- **Preset:** Viewer; in addition Counters and Metrics: Manage, Water Management: View (Manage if they will also edit profiles and diagrams), Reports: View.
- **Actions to turn off:** Counters and Metrics › Details: leave only "Enter manual values" on. On the counter and metric rows Add, Edit, Delete; "Correct counters" and "Categories and groups" off (8 actions). "Export counter data" and "Download reports" stay on.
- **Resource access:** the channels and devices the counters are connected to (the water pages show only the counters of the devices that can be reached).
- **Prerequisite:** for the water pages, Water management must be on under **Settings › Feature groups**.

- **Result:** watches consumption, takes it to Excel, enters monthly invoice, analysis, rainfall and production values. The counter and metric windows open read-only. The water setup wizard needs Water Management: Manage and Counters and Metrics: Manage together.

5. QUALITY / REPORTING: DESIGNS AND DOWNLOADS REPORTS; SEES ONLY THE DEVICES THEY REPORT ON

- **Preset:** Viewer; in addition Reports: Manage, Connectivity: View only, and the View permission of every data source used in a report (Alarms for alarm history, Data Logs for logged data, Counters and Metrics for counters and metrics, Audit log for audit records).
- **Actions to turn off:** Alarms › Details: "Acknowledge alarms" (reads the history, does not acknowledge). If you wish, Reports › Delete on the report row (designs, cannot delete).
- **Resource access:** the "must not see the devices" request is met here: in the **Access** window tick only the channels and devices they will report on. A device that is not ticked does not appear in the project tree, the tag picker or a report.
- **Result:** designs and runs reports, report pages and counter tracking lists and downloads Excel / PDF / CSV. Cannot add channels, devices, tags, alarm definitions or log groups.

6. SCADA DESIGNER: DESIGNS SCREENS; GIVES NO COMMANDS TO THE PLANT

- **Preset:** Viewer; in addition SCADA: Manage and Connectivity: View (to bind tags to objects). Do not give Tag write and services: the command buttons on a screen do not work for them, values are visible.
- **Actions to turn off:** if needed SCADA › Details: Delete on the screen row (designs, cannot delete); "Zone tree" (adds screens to existing zones, cannot change the tree). Leave "Symbol library" on.
- **Resource access:** the devices they will bind to screens and the zones they will edit. They always see a screen they created themselves.
- **Result:** adds screens, edits them in design mode and saves. Full project export / import is Root only.

7. IT / SYSTEM ADMINISTRATOR: SERVER SETTINGS, TAB BY TAB

- **Account:** on an account created in the interface the permissions given by a preset can be turned off one by one. An account with the Administrator (Admin) role that comes from an older version or was created through REST cannot be restricted: first press **Remove role, keep permissions** in its permissions window.
- **Boxes:** in the System section Server settings, Notification settings, Certificates, Firewall, Audit log. Tag write and services if they will start and stop services.
- **Actions to turn off:** Server settings › Details: every box is one settings section, and when it is off that tab does not appear. Example: "OPC UA server settings", "Web and REST API settings", "Mobile access settings", "License", "Data sources", "Services and resource thresholds" on; "Branding settings", "Feature groups", "AI provider", "Assistant skills", "Extra instructions", "Data access keys" off. Tag write and services › Details: only "Start / stop services" on.
- **Result:** sees on the Settings page only the tabs left on. The Users, Retention, Security and Backup tabs and the e-mail / SMS sending server remain Root only.

8. OUTSIDE CONTRACTOR / INTEGRATOR: NARROW AND TEMPORARY

- **Account:** create a separate account in the contractor's own name; do not hand out a shared account: the audit log records who did what by account.

- **Preset:** Viewer; in addition Connectivity: Manage (SCADA: Manage if they will also build screens), Tag write and services, OPC UA client, Templates and import. Give nothing from the System section.
- **Actions to turn off:** Connectivity › Details: the whole Delete column. Templates and import › "Delete templates". OPC UA client › "Write to the remote server". Tag write and services › "Start / stop services".
- **Resource access:** only the channels and the zone they will work on. They see a channel they added; they do not see the rest of the plant. When installing a template they cannot overwrite an existing resource they cannot reach.
- **Duration:** an account has no expiry date field. When the job is done clear the account's **Enabled** box in the Users list (it cannot sign in, and its open session and MCP token stop working too) or delete the account.

9. SENIOR MANAGER WHO ONLY WATCHES

- **Preset:** Viewer (a new user is created with these permissions anyway). Alarms: View if they should also see the alarm state; Data Logs: View for trend charts.
- **Actions to turn off:** if you gave Alarms: View, "Acknowledge alarms" (sees the alarm, cannot acknowledge). "Download reports" and the export boxes if downloading is not wanted.
- **Result:** sees screens, counters, the water pages and reports. Cannot change anything or write to tags. Watches with the same permissions on the phone.

10. DEMO / PRESENTATION USER

- **Preset:** Viewer; the View boxes of the modules you want to show. Give no Manage box, no Tag write and services and no System box.
- **Actions to turn off:** if data must not leave, "Download reports", "Export counter data", "Export water reports", "Acknowledge alarms", "Export alarm history" and "Export logged data".
- **Resource access:** only the channels and screens prepared for the demo; do not tick real production lines.
- **Result:** browses the screens and pages you chose; cannot change or download anything. Change the password of a shared demo account after the presentation (the other sessions are closed).

11. A USER WHO SEES ONLY WATER MANAGEMENT

- **Boxes:** create a group; click **Clear** in the **Modules** section and tick only the View box on the Water Management row. Leave no box ticked in the other two sections.
- **Resource access:** the devices the water counters are connected to.
- **Result:** the user sees in the left menu only Water Management and the pages under it (if Water management is on under **Settings › Feature groups**). The Counters permission is not needed: category and counter names come with the page.

> **Tip** After saving, sign in as that user (or as a test account in the same group) and open **My profile** › **My permissions** › **What can I do and what can I not?**: the list must match what you set up in the window.

Frequently asked questions

WHY DO I NOT SEE THIS BUTTON?

First look at **My profile** › **My permissions** in your own account. There are five reasons a button does not appear:

REASON	HOW TO TELL	WHO FIXES IT
No Manage permission for the module	The CANNOT box says "...: cannot manage (no add, edit, delete)".	Root: the Manage box in the permissions window.
That action is turned off	The CANNOT box names the action; the summary in the Users list shows "(... off)".	Root: **Details** on the row. If the user is in a group, the action must be on in the group as well.
No access to the resource	Not the button but the channel, device or screen itself is missing; the page is empty.	Root: the **Access** button.
The feature group is off	The Water Management pages are not in the menu.	Someone with the Server settings permission: **Settings › Feature groups**.
The job is Root only	The Users, Retention, Security and Backup tabs; full project Export / Import; deleting records.	Cannot be granted; Root does it.

THE USER SEES THE SCREEN BUT CANNOT SAVE

- **The window opens read-only, there is no Save.** The "edit" action of that object is off (e.g. "Edit tag"). This is the expected behaviour.
- **It saves but nothing changes in the field.** The "Reload the runtime" action is off. Either turn on Tag write and services › "Reload the runtime" for that user, or someone who may reload does it.
- **The message "You have no permission for this action: ...".** The server refused the action; the message names the action that is off.
- **The definition refers to a tag the user cannot reach.** When a Virtual Tag, a flow, a data bridge agent or a log group is saved, every tag it refers to must be open to the user who saves it; a definition that writes to a tag also needs Tag write and services.

WHY CAN I NOT RESTRICT AN ADMINISTRATOR?

An account whose badge says **Administrator** has the Administrator (Admin) role on the server: it comes from an older version or was created through REST. This role is always fully permitted: neither clearing permission boxes nor turning actions off is applied; in the permissions window the action boxes are locked and the list shows "Administrator: fully permitted".

To restrict it, press **Remove role, keep permissions** in the permissions window of the account and confirm: the account is switched to the Viewer role and its current permissions are saved as custom permissions; its access does not change. Then turn off the permissions and actions you do not want. The button works even if the system has a single Administrator (Admin) account: while there is an enabled Root account the role of the last Administrator account can be removed.

A new manager needs no role: create the user, apply the **Manager** preset in the permissions window (or assign the user to a group), then turn off what you do not want.

HOW DO I RESTRICT ONE USER IN A GROUP?

An action is on if the user's own profile or their group allows it. This is why clearing a box on the user is not enough to make one person narrower than their group. There are three ways:

1. **If the restriction suits everyone**, turn the action off in the permissions window of the group: it is off for all members.

2. **If it is for one person only**, take that user out of the group, copy the permissions of the group with **Copy from another user / group...** in the **Permissions** window, then turn the action off with **Details**.
3. **If it is for a few people**, create a second, narrower group and move them there.

The other way round is easy: to give one person more than their group, clear **No custom permissions (use the group's permissions)** in the user's window and tick the extra box; their custom permissions are combined with the group.

I TURNED IT OFF BUT THE USER CAN STILL DO IT

Three possibilities: the user's group gives the same permission without restriction (the summary at the bottom of the window shows that action as "(from the group)"); the account has the Administrator (Admin) role (see the question above); or it is one of the three export actions (alarm history, counter data, water reports) and the user reads the data over REST: these three only hide the button in the interface, so remove the View permission to stop the data being seen.

DID PERMISSIONS CHANGE AFTER THE UPGRADE?

Nobody loses access when upgrading to 3.10.1. Saved permission sets of users and groups are widened once; nobody has an action restriction (all 95 actions start on for everyone who has the parent permission). Accounts with neither a group nor custom permissions get the new default by themselves.

IF THE OLD SET HAD	ADDED
Connectivity: View (configuration read)	Counters and Metrics: View, Water Management: View, Reports: View, Automation: View
Connectivity: Manage (configuration write)	Counters and Metrics: Manage, Water Management: Manage, Reports: Manage, Automation: Manage, Data Bridge
Alarms	Alarms: Manage (a user who saw alarms could also edit the definitions before)
Data Logs	Data Logs: Manage

What became narrower: the Administrator (Admin) role cannot read the retention counts, the backup list or the version list and cannot delete audit and event records (Root only); reading management information now needs the permission to manage it. The migration is generous on purpose; after upgrading review your groups, remove Manage boxes that are not needed and turn off irreversible actions such as delete with **Details**. Details: release notes.

A BUTTON SHOWS ON THE PHONE BUT IT SAYS "NO PERMISSION"

MergenHub Mobile does not yet show action restrictions on buttons: if the module permission is there, the button is shown. When an action that is off is tapped the server refuses the request; the message is in English (`Requires 'alarms.ack' permission.`). There is no difference for security: the restriction is applied on the server. A SCADA screen opened inside the app is the web interface itself: there the restriction is applied to the buttons as well.

DO THE API, MCP AND ACCESS KEYS FOLLOW THE SAME RULE?

Yes. Permissions and actions are checked on the server; the way in does not matter.

WAY IN	WHAT HAPPENS FOR AN ACTION THAT IS OFF
REST API (cookie or HTTP Basic)	403; the body carries the action key (example below).
In-app assistant and external MCP tokens	A tool whose action is off is not in the tool list; if called it does not run. A token cannot exceed the permissions and restrictions of its owner.
Data access key (`mhkey_`)	If the owner's "Download reports" action is off, the key cannot read reports either (403).
Mobile app	The server refuses (see the question above).
OPC UA clients	These permissions are for the web interface and the REST API; OPC UA users are a separate list (Settings › OPC UA Users).

```
{ "code": 403, "action": "alarms.ack", "message": "Requires 'alarms.ack' permission." }
```

The action catalogue is returned in the `actions` field of `GET /auth/v1/capabilities`, the actions turned off for the caller in the `denied` field of `GET /auth/v1/me`; on user and group records the turned-off actions are given in the `restrict` field. See REST API.

WHERE DO I SEE WHO CHANGED WHAT?

Settings › Audit. Permission and restriction changes are written in detail under the "Security" category: who, for whom, permissions added and removed, actions turned off and on. An attempt at an action that is off is not recorded; the change itself is.

See also

- Users, groups and security: accounts, passwords and sessions, HTTPS, auditing, the hardening checklist
- User Manual: Security & Authorization: the same chapter of the in-app manual (including permissions page by page)
- AI assistant (MCP server) and In-app AI assistant: how tools map to permissions and actions
- REST API: the 403 response and the permission fields