USER MANUAL (IN-APP, COMPLETE)

Security & Authorization

Online: mergenhub.envest.com.tr/docs/manual-security

ON THIS PAGE

Roles & Permissions: who does what, how permissions are given
Action reference: what every permission and every action allows
Factory examples: which boxes for whom
Frequently asked questions (permissions)
Permissions page by page: which button needs which permission and a
Passwords, forgot password and sessions
HTTPS / Public Exposure
Hardening the Server: data folder lock, backup password, disk encryptic

Roles & Permissions: who does what, how permissions are given

VERSION 3.10.1

Four things decide what a user can see and what they can change: whether the account is **Root**, the **View** / **Manage** permissions per 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, screens). A user without the permission does not see that page in the menu at all; 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.

Location: **Settings** → **Access** → **Users**. Only the **Root** (super administrator) account sees this tab. It has two cards: **Users** and **User Groups**. The **Permissions** button on a user row opens that user's permission window, the **Permissions** button on a group row opens the **Group Permissions** window; both are the same editor.

More in this chapter Action reference: 31 permissions, 95 actions Factory examples Frequently asked questions Permissions page by page

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 permission window; for a super administrator the Root box in the user list is ticked. In short, the "roles" are three things: the four presets, Root and your own groups. In the user list, in the permission window and in the profile, the **?** button next to the badge opens the **Presets and Root** window, which explains them.

Viewer preset. Who gets it: those who only watch (managers, visitors, dashboard screens). 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. Every new account created in the interface starts with these permissions.

Operator preset. Who gets it: shift operators. Runs the plant (writes to tags, acknowledges alarms, sees the modules) but changes no definition.

Maintenance preset. Who gets it: maintenance and automation staff. On top of the Operator preset defines channels / devices / tags, designs screens and manages the modules. Cannot enter the server settings.

Manager preset. Who gets it: plant or IT managers. Everything except the Root-only jobs (including the server settings). The permissions and actions given with the preset can be turned off one by one afterwards.

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. Who gets it: the owner of the system. At least one, at most a few people; not used for daily operation. Given with the Root box in the user list.

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. When people change only the group membership changes; the permissions are managed in one place.

> **Creating an account and Root** The **Add user** window creates the account as a Viewer; if the **Super-admin (Root) — manage users, permissions & access** box in the window is ticked, the account becomes Root. In the list, the box in the **Super-admin** column gives 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 below the box shows the role of the account: **Viewer** or **Root**. In daily use the role does not need to be changed: what a user does is decided by their **group** and the **Permissions** window.

> **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 (on the badge: **Operator**, **Administrator**). The permission 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.	The 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.	The **Permissions** window: View / Manage boxes
3. Action (95 names)	Which job can they not do in a module they manage (e.g. delete, acknowledge, download)? Actions are managed by **turning them off**: whoever gets the permission does all of its actions, and the administrator turns off the ones they choose.	The **Permissions** window: **Details** on the row
4. Resource access	On which channels, devices, zones and screens do they do these?	The **Access** button (user or group row)

The four are checked together: a user who has Alarms: View and the "Acknowledge alarms" action turned on, but no access to the alarm's tag, does not see that alarm.

WHERE A PERMISSION COMES FROM

SOURCE	WHAT IT DOES
Group (recommended)	The group is given a permission set and the actions that are turned off; 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 untick **No custom permissions (use the group's permissions)** and apply a preset or tick the boxes one by one. A user with their own permissions has a small dot on the button.
If there is neither	If the user has neither a group nor their own permissions, the account works with the permissions of the Viewer preset. On an old account or one created through the API that has the Operator or Administrator role, the set of the role applies (below, "Roles on old accounts and accounts created through the API").

HOW THE USER AND THE GROUP COMBINE

- **Permissions are merged.** If a user has both their own permissions and a group, the union of the two applies: having the permission in one of them is enough.
- **For a grouped user without their own permissions, only the group applies.** The starting permissions of an account without a group (the Viewer preset) are not added to the group; the user has no profile of their own.
- **Actions are merged too.** An action can be done if at least one of the sources allows it. That is why **an action turned off on the user stays on if their group gives the same permission without the restriction**. To really turn an action off, turn it off in the group as well or take the user out of the group.
- **For a grouped user without their own permissions, the action restriction is given to the group.** In this user's permission window the action boxes are locked and show the restrictions of the group; this note appears at the top: "This user has no permission set of their own; the permissions come from the group "...". To turn actions off for this user only, clear "No custom permissions" or edit the permissions of the group." For a user without a group, actions can be turned off while the box is ticked as well (the View / Manage boxes stay locked).
- **An old account with the Administrator (Admin) role is always fully permitted.** Even if permission boxes are unticked or actions are turned off, it does all of them; the action boxes are locked. The window says so: "This account has the Administrator (Admin) role and is always fully permitted. To restrict it, press "Remove role, keep permissions"." The button switches the account to the Viewer role and saves its current permissions as custom permissions: its access does not change, and permissions and actions can then be turned off one by one. A new manager does not need a role: the **Manager** preset or a group is used.
- **Viewing is not a separate action.** The permission itself is entering the module and seeing it. A user with every action turned off still sees the module; if they should not, the View box is unticked.
- **A new action arrives turned on.** Because it is the list of turned-off actions that is stored, an action added in the future is on by itself for everyone who has its parent permission; nobody loses access on an upgrade.
- **A change takes effect immediately.** Permissions and restrictions are recalculated 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, a data access key, an external MCP token and the in-app assistant all pass through the same set of permissions and actions.

THE PERMISSION WINDOW STEP BY STEP

1. **Open the window. Settings** → **Access** → **Users**; **Permissions** on the user or group row. In the user window the **Username** is at the top, with the badge and **?** next to it and the group if there is one; below it are the hint "Grant or revoke permissions for this user; they are combined with the permissions of the user's group." and the **No custom permissions (use the group's permissions)** box. While the box is ticked the user has no permissions of their own and the View / Manage boxes are only shown (the permissions of the group for a grouped user; the permissions of the Viewer preset for a user without a group). If the account has an old Operator or Administrator role, an information line and the **Remove role, keep permissions** button also appear below the hint.
2. **Choose a starting point.** Unticking **No custom permissions (use the group's permissions)** opens the **Preset (click → then fine-tune):** line: **Viewer**, **Operator**, **Maintenance**, **Manager**. A preset fills the boxes with one click and **clears the action restrictions**. If there is a similar user or group, pick it from the **Copy from another user / group...** list: its permissions and turned-off actions are copied (when copying from a user, what that user can actually do together with their group is taken).

3. **Tick the View / Manage boxes.** The window has three sections: **Modules** (each row is a module with two columns: View and Manage; buttons **View all**, **Manage all**, **Clear**), **Operations and tools** and **System** (buttons **All**, **None**). When Manage is ticked, View is ticked automatically; when View is unticked, Manage is unticked too. The **Data Bridge** row has a single box (**View and manage**). The information line below the System section lists the permissions that only Root has.
4. **Turn actions off.** The **Details** button on the right of a row opens the actions of that permission. Objects such as channels, devices and tags are in a grid: the row is the object, the columns are **Add**, **Edit**, **Delete**. The other actions are individual boxes ("Acknowledge alarms", "Download reports", "Write to tags"...). Unticking a box turns the action off. The box of a permission that has an action turned off looks **partial** (a dash) and the row gets a badge of the form **restricted: 2 actions off**. If the box of the permission is unticked, the restrictions of that permission are deleted as well.
5. **Search and filter.** Typing in the box at the top ("Search a permission or an action (e.g. alarm, delete)...") leaves only the matching rows; if the word is the name of an action, the details of the row open and only those actions are shown. The **Show only what is turned off** box lists the rows that have actions turned off and the actions that are off.
6. **Read the summary.** At the bottom of the window there are two boxes: **CAN** and **CANNOT**. They write module by module in plain words ("Alarms: sees; acknowledge alarms", "Alarms: cannot manage (no add, edit, delete)"). If the user has a group, the summary also counts what the group gives and marks it **(from the group)**: if an action you turned off on the user still stands in the CAN box with "(from the group)", the group allows it. In the group window the heading is "Members of this group (as far as the group grants)".
7. **Save. Save**. In the Users list a one-line summary appears under the name: "Alarms: Manage (delete alarm definition off), SCADA: View +5"; the whole of it can be read by hovering. For an old account with the Administrator (Admin) role it says "Administrator: fully permitted". In the group list the same summary is shown as chips.

HELP	WHERE	WHAT IT SHOWS
Badge and preset **?**	Next to the badge (user list, permission window, profile), the preset line and the **My permissions** heading in the profile; all three open the same window	**Presets and Root**: the **What the presets contain** table (a row is a module or a permission, a column is a preset), **Who gets it** and **Cannot** for each preset, Root, the group suggestion (**Suggestion**) and at the bottom the **Roles on old accounts and accounts created through the API** note.
Row **?**	Every module and permission row	The description of the permission, an example and the **Actions inside this permission** table.
Action **?**	Every action box in the details	What the action allows, what happens when it is turned off and which permission it is part of.
Help	The bottom bar of the window	A short summary card for users and groups.

At the bottom of every **?** window there are two links: **Detailed manual** opens this section, **Open on the site** shows the same content in the "Roles and permissions" document on the site.

> **My permissions** Every user sees the **My permissions** heading in the window opened with the **My profile** button (the person icon) next to their name: the permission summary, a **?** next to it (the Presets and Root window) and the **What can I do and what can I not?** line (the CAN / CANNOT boxes). This is the first place to look for a user who says "I cannot see a button".

If the server reports a new permission the interface does not know, it appears at the end of the window under **Other** with its own name and can still be ticked.

PRESETS

PRESET	WHAT IT TICKS

Viewer	View: Connectivity, SCADA, Counters and Metrics, Water Management, Reports, Automation. No Manage, no operation or tool, no system permission. No Alarms and no 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 and no Notification settings.
Manager	Everything in the window except Script execution.

A preset is a starting point: after applying it you change the boxes one by one and turn actions off with **Details**. 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 in the language of the interface. The role decides the permission set that applies while the account has no group and no permissions of its own:

BADGE (NAME ON THE SERVER)	WITH NO GROUP AND NO OWN 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 the account has a group or its own 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 (super administrator)	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, an information line and this button are shown in the permission window, below the hint. A Viewer or Root account does not have the button.

1. Press **Permissions** on the user row and **Remove role, keep permissions** in the window, then confirm the question.
2. The current permissions of the account are saved as custom permissions, 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.
3. 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 with the REST API (`PUT /auth/v1/users/{name}` , body `{ "role": "Viewer" }` ; Root only).

JOBS FOR ROOT ONLY

The following cannot be given to any user or group; only the Root account does them (neither the Manager preset nor an old account with the Administrator role can). They are not in the action list either:

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

OLD PERMISSIONS ON UPGRADE

When upgrading to 3.10.1 nobody loses access. Saved user-specific and group permission sets are widened once; nobody has an action restriction (everyone starts unrestricted):

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 (before, whoever saw alarms could also edit the definitions)
Data Logs	Data Logs: Manage

> **Narrow it down after upgrading** The migration is generous on purpose, so that what could be done yesterday can still be done today. After the upgrade review the groups and the users with their own permissions: untick the Manage boxes that are not needed (e.g. Alarms: Manage for an operator who should only watch alarms) and turn off irreversible actions such as delete with **Details**.

A PERMISSION IS NOT THE SAME AS RESOURCE ACCESS (ACL)

	PERMISSION AND ACTION	RESOURCE ACCESS
Question	Which job can they do (acknowledge an alarm, design a report, delete a channel)?	On which channels, devices, zones and screens?
Where	The **Permissions** button	The **Access** button (user or group row); the **Connectivity** and **SCADA** sections in the window
Default	With no group and no own permissions, the permissions of the Viewer preset	A user who is not Root does not see a channel or device they were not given access to. The **All Connectivity (every channel + device)** box opens all connectivity, the **All SCADA (every zone + screen)** box opens all screens.
Union	User ∪ group	User ∪ group (access that comes from the group is shown in the window with a "group" badge)

The two are checked together: a user with Water Management: View sees on the water pages only the counters of the devices they can access. If a page looks empty, check the **Access** button first. A request such as "this user must not see the devices of that line at all" is met with resource access, not with a permission.

> **Warning** An administrator password is mandatory during installation (it cannot be left blank). The password entered at first installation is added both as the web account `administrator` and as an OPC UA user; the two lists are separate: changing the web password later does not change the OPC UA password. On systems upgraded from older versions the account name stays `admin` and the OPC UA list is left untouched. If a password was entered during installation, it is not asked for again at first sign-in; the default `administrator/admin` is changed at first sign-in only on an untouched development database. Sign-in lockout: locked after 8 failed attempts (HTTP 429). A strong password is essential for an installation exposed to the internet.

See also Action reference Factory examples Frequently asked questions Permissions page by page Passwords and sessions HTTPS / Public Access Assistant and MCP permissions REST API

Action reference: what every permission and every action allows

VERSION 3.10.1

This section is the reference for every row of the permission window and every action box under **Details**: **31 permissions** and **95 actions** in 16 modules. The names are as they appear in the window. The code under the name is the key 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, a Manage or a single box in the window). If the permission is not given, the module is not seen or not managed; its actions are not looked at.
- **The rows below it are the actions of that permission.** When the permission is given they are all on; they are turned off one by one with **Details**. The button, the right-click menu item and the keyboard shortcut of an action that is off do not work; the server rejects the same job through REST, the assistant and MCP as well.
- A permission without actions (e.g. Connectivity: View, SCADA: View, Automation: View, Firewall, Audit log) is only given or not given.
- For Root and for an old account with the Administrator (Admin) role, actions cannot be turned off (on an Admin account press **Remove role, keep permissions** first; see Roles & Permissions).

GENERAL RULES

- **Copying counts as adding** (copy channel = "Add channel"); **bulk delete** needs the "delete" action.
- Adding / editing / deleting a **tag group** and **tag generation** (offline, online, taking nodes from the device) are tag actions.
- **Reports, report pages and counter tracking lists** are one action family (add / edit / delete; no distinction by kind).
- **Three export actions are applied only in the interface** (alarm history, counter data, water reports): the file is produced in the browser and the button is hidden; a user who can see the same data can read it with REST. The Data Logs export and report download, on the other hand, are rejected on the server too.
- **While edit is off the window opens read-only**: the values are visible, **Save** (and Delete) does not appear. Helpers such as validation, preview and selection lists keep working.

- **While reload is off** the user saves a definition; the change does not reach the running system until someone who may reload applies it. The user is told this once per session: "Saved. A user who may reload the runtime is needed to apply the change to the running system."
- **A rejection by the server** is written in the interface with the name of the action: "You have no permission for this action: Delete alarm definition".

CONNECTIVITY

PERMISSION / ACTION	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Connectivity: View `ConfigRead` permission	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 `ConfigWrite` permission	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.

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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
SCADA: View `Scada` permission	Opens and runs SCADA screens.	Example: With only this the user watches screens; giving commands also needs Tag write.
SCADA: Manage `ScadaDesign` permission	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 a screen in design mode and saving it (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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Alarms: View `Alarms` permission	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 `AlarmsManage` permission	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Data Logs: View `DataLogging` permission	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 `DataLoggingManage` permission	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.
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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE

Counters and Metrics: View `Metering` permission	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 `MeteringManage` permission	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.
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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Water Management: View `Water` permission	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 `WaterManage` permission	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Reports: View `Reports` permission	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 it is off, the user's data access keys (report reading by external systems) get 403 as well.	When off, the report opens on screen but the download buttons do not appear.
Reports: Manage `ReportsManage` permission	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Automation: View `Workflows` permission	Sees the automation flows and the run history.	Example: An operator sees which flow ran when but cannot change the flow.
Automation: Manage `WorkflowsManage` permission	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Data Bridge `DataBridge` permission	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 global switches on the Data Bridge tab are saved with this action too.	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.
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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Tag write and services `RuntimeControl` permission	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) depend on this action too.	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
OPC UA client `OpcClient` permission	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Templates and import `Import` permission	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). "Add" actions are not checked separately for the channels, devices, tags and screens it installs.	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 this action too.	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
AI assistant `Ai` permission	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 `Mcp` permission	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 `AiScripts` permission	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 `ai.provider` (inside the Server settings permission)	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 `ai.skills` (inside the Server settings permission)	Adds, edits and deletes the skills of the assistant. The assistant's "save skill" tool depends on this action too.	When off, the Skills tab does not appear in the assistant settings.
Extra instructions `ai.prompt` (inside the Server settings permission)	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Server settings `Settings` permission	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 saved with this action too.	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. It 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.
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 Add-ons › VPN page is view-only: status and the site list are visible, nothing can be changed.
Firewall `Firewall` permission	Opens the required ports in the Windows firewall.	Example: The "open ports" button on Settings › OPC UA server appears with this permission.
Audit log `Audit` permission	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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
Notification settings `Notifications` permission	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 chat notifications (Slack, Telegram, WhatsApp) on / off; sets the Slack webhook, the Telegram bot and chats, the WhatsApp phone number ID, access token, template and recipients, 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	WHAT IT ALLOWS	WHEN OFF / EXAMPLE

Certificates `Certificates` permission	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.
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 & Mobile tab do not appear.

ROOT ONLY (PERMISSIONS THAT CANNOT BE GIVEN)

PERMISSION / ACTION	WHAT IT ALLOWS	WHEN OFF / EXAMPLE
User and group management `Users` permission	Manages users and groups. Root only.	Example: Cannot be given to another user or group.
Resource access (channel / device restriction) `Acl` permission	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 `AiAdmin` permission	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.

See also Roles & Permissions Factory examples Permissions page by page Assistant and MCP tools REST API

Factory examples: which boxes for whom

VERSION 3.10.1

In a factory every area has a different job and a different responsibility. The examples below show step by step, for typical duties, which boxes to tick in the permission window, which actions to turn off under **Details** and how to give resource access. The action names are as written in the window; all of them are in the Action reference. The examples 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 a **Group name** (e.g. Shift operators). A new group opens with the boxes of the Viewer preset.
2. **Apply the preset, adjust the boxes.** Press the preset button named in the example, then tick or untick the View / Manage boxes of the example.
3. **Turn the actions off.** Press **Details** on the row concerned and untick the boxes the example says to "turn off". Read the **CAN** / **CANNOT** summary at the bottom and press **Save**.
4. **Assign the user to the group.** On the **Users** card select the group in the user's **Group** column. If the user has their own permissions (a dot on the Permissions button), open their window and tick the **No custom permissions (use the group's permissions)** box; otherwise their own permissions are merged with the group and an action you turned off in the group may stay on for the user.

5. **Give resource access.** The **Access** button on the group row: tick the channels and devices in the **Connectivity** section and the zones and screens in the **SCADA** section. If no restriction is needed: **All Connectivity (every channel + device)** and **All SCADA (every zone + screen)**.

> **For a single person** It also works without a group: in the user's **Permissions** window untick **No custom permissions (use the group's permissions)** and give the same boxes to that user. If a second person will do the same job, turning it into a group is easier (with **Copy from another user / group...**).

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

STEP	WHAT TO DO
Preset	**Operator**.
View / Manage	As the preset brings them: only View on Connectivity, SCADA, Alarms, Data Logs, Counters and Metrics, Water Management, Reports and Automation; no Manage. Operations and tools: keep **Tag write and services** and **AI assistant**; remove **OPC UA client** if it is not needed.
Actions to turn off	**Tag write and services** › Details: leave only "Write to tags" on; untick "Reload the runtime", "Start / stop services", "Device diagnostics", "File upload" and "Run a flow by hand". Do not touch the Alarms and Reports rows: "Acknowledge alarms" and "Download reports" stay on.
Resource access	The channels and devices of the line the shift is responsible for; in the SCADA section the zone of that line.
Result	Watches the screens, gives commands with the SCADA buttons, acknowledges alarms, looks at the history and the chart. Opens an alarm definition read-only; cannot add a channel, device, tag, screen or log group; cannot stop a service.

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

STEP	WHAT TO DO
Preset	**Operator**, then the boxes below.
View / Manage	**Alarms**: Manage. **Automation**: Manage. **Audit log** in the System section.
Actions to turn off	**Alarms** › Details: on the Alarm definition row untick **Add** and **Delete**, keep **Edit** (changes limits, cannot add or delete a definition). **Automation** › Details: on the Flow row untick **Add**, **Edit**, **Delete**, keep "Enable / disable flows" (stops a flow, cannot change what is inside). **Tag write and services** › Details: keep "Write to tags", "Run a flow by hand" and "Device diagnostics"; untick "Start / stop services" and "File upload".
Resource access	All the lines they are responsible for; in most plants All Connectivity and All SCADA.
Result	In addition to what the operator does, changes an alarm limit, stops and starts a flow or runs it by hand, and follows who wrote which value on the **Settings** → **Audit** tab. The summary in the Users list looks like "Alarms: Manage (add alarm definition, delete alarm definition off)".

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

STEP	WHAT TO DO
Preset	**Maintenance**.
View / Manage	The preset manages every module. Remove what is not the technician's job: Water Management: Manage, Reports: Manage, Data Bridge, MCP, Certificates, Firewall.

Actions to turn off	**Connectivity** › Details: untick the five boxes in the **Delete** column of the grid (Channel, Device, Tag, Virtual Tag, Tag Shortcut). The row gets the badge "restricted: 5 actions off". 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** › keep "Reload the runtime" on (otherwise a tag they add does not reach the running system); untick "Start / stop services".
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 THE COUNTERS AND THE WATER PAGES, ENTERS MANUAL VALUES; CANNOT DEFINE COUNTERS

STEP	WHAT TO DO
Preset	**Viewer**, then the boxes below.
View / Manage	**Counters and Metrics**: Manage. **Water Management**: View (Manage if they will also edit profiles and diagrams). **Reports**: View. Remove SCADA and Automation if they are not needed.
Actions to turn off	**Counters and Metrics** › Details: leave only "Enter manual values" on. Untick **Add**, **Edit**, **Delete** on the Counter row; **Add**, **Edit**, **Delete** on the Metric row; and the "Correct counters" and "Categories and groups" boxes (8 actions). "Export counter data" and "Download reports" under Reports stay on.
Resource access	The channels and devices the counters are bound to (the water pages show only the counters of accessible devices); All Connectivity if it is for the whole plant.
Prerequisite	For the water pages, Water management must be on in **Settings** → **Feature groups**.
Result	Watches consumption, takes it to Excel, enters the monthly invoice, analysis, rainfall and production values (**Enter period value** on a manual counter). The counter and metric windows open read-only; the **Manual adjustment** and **Meter replacement** buttons do not appear. 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

STEP	WHAT TO DO
Preset	**Viewer**, then the boxes below.
View / Manage	**Reports**: Manage. **Connectivity**: View only (can pick tags, cannot add channels or devices). The View permission of every data source used in the reports: **Alarms** for alarm history, **Data Logs** for logged data, **Counters and Metrics** for counters and metrics, **Audit log** for the audit log. A source without the permission is not listed in the editor.
Actions to turn off	**Alarms** › Details: untick the "Acknowledge alarms" box (reads the history, does not acknowledge alarms). If you wish, untick the **Delete** box on the Report row under **Reports** (designs, cannot delete).
Resource access	The request "must not see the devices" 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, in the tag picker or in a report.
Result	Designs and runs reports, report pages and counter tracking lists and downloads Excel / PDF / CSV. Cannot add a channel, device, tag, alarm definition or log group.

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

STEP	WHAT TO DO
Preset	**Viewer**, then the boxes below.

View / Manage	**SCADA**: Manage. **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, the 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). Keep "Symbol library" on: they save their own objects to the library.
Resource access	In the Connectivity section the devices they will bind to screens; in the SCADA section the zones they will edit. They always see a screen they created themselves.
Result	Adds screens, edits them in design mode and saves. Duplicating a screen or importing one from a file counts as adding a screen; full project export / import is Root only.

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

STEP	WHAT TO DO
Account	On an account created in the interface, the permissions given with 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 the permission window.
Preset	**Manager** if they will also manage the field; if they will look after the server only, **Clear** in the **Modules** section, **None** in the **Operations and tools** section, then the boxes below.
View / Manage	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 a settings section and when it is turned off that tab does not appear. Example: keep "OPC UA server settings", "Web and REST API settings", "Mobile access settings", "License", "Data sources", "Services and resource thresholds"; untick "Branding settings", "Feature groups", "AI provider", "Assistant skills", "Extra instructions", "Data access keys". **Notification settings** › Details: "E-mail settings", "SMS settings", "Communication Center" separately. **Certificates** › Details: "Client certificates", "Server certificate", "Web certificate". **Tag write and services** › Details: keep only "Start / stop services"; untick the others, "Write to tags" included.
Resource access	If they will not see the field, no channel is ticked.
Result	On the Settings page they see only the tabs you left on (which tab depends on which action: Permissions page by page). The Users, Retention, Security and Backup tabs and the e-mail / SMS sending server are still Root only.

8. OUTSIDE CONTRACTOR / INTEGRATOR: NARROW AND TEMPORARY

STEP	WHAT TO DO
Account	Create a separate account in the contractor's own name (**Add user**); do not give a shared account: the audit log writes who did what by account.
Preset	**Viewer**, then the boxes below.
View / Manage	**Connectivity**: Manage. **SCADA**: Manage if they will also build screens. Operations and tools: **Tag write and services**, **OPC UA client** (to check the remote server during commissioning), **Templates and import**. Give nothing from the System section; if Counters, Water, Reports and Automation are not their job, untick those View boxes too.
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"; keep "Write to tags", "Reload the runtime", "Device diagnostics" and "File upload".
Resource access	Only the channels and the zone they will work on. They see a channel they added themselves; they do not see the rest of the plant. When installing a template they cannot overwrite an existing resource they cannot access.
Duration	An account has no expiry date field. When the job is finished, untick the account's **Enabled** box in the Users list (the account is disabled: it cannot sign in, and its open session and MCP token stop working too) or delete the account. For a job that is paused, ticking the box again is enough.

9. SENIOR MANAGER WHO ONLY WATCHES

STEP	WHAT TO DO
Preset	**Viewer**. A new user is created with these permissions anyway; nothing special is needed.
View / Manage	**Alarms**: View if they will also see the alarm status; **Data Logs**: View for trend charts.
Actions to turn off	If you gave Alarms: View, **Alarms** › Details: untick the "Acknowledge alarms" box (sees the alarm, cannot acknowledge it). If downloading is not wanted, the "Download reports" box and the export boxes.
Resource access	All Connectivity and All SCADA; or only the plant they are responsible for.
Result	Sees the screens, the counters, the water pages and the reports, and downloads a report. Cannot change anything or write to tags. Watches with the same permissions on the phone too.

10. DEMO / PRESENTATION USER

STEP	WHAT TO DO
Preset	**Viewer**.
View / Manage	The View boxes of the modules you want to show (e.g. Alarms, Data Logs). Give no Manage, no Tag write and services and no System box.
Actions to turn off	If the data must not leave the system: **Reports** › "Download reports", **Counters and Metrics** › "Export counter data", **Water Management** › "Export water reports", **Alarms** › "Acknowledge alarms" and "Export alarm history", **Data Logs** › "Export logged data".
Resource access	Only the channels and screens prepared for the demo; do not tick the 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

1. **Add Group**; press **Clear** in the **Modules** section, then tick the View box on the **Water Management** row only.
2. Press **None** in the **Operations and tools** and **System** sections. **Save**.
3. Assign the user to the group; with **Access** give the devices the water counters are bound to.
4. When the user signs in they see only **Water Management** and the pages below it under the **Plugins** heading in the left menu (if Water management is on in **Settings** → **Feature groups**). The Counters permission is not needed: category and counter names come with the page.

> **Check it** After saving, sign in as that user (or with 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 be the same as what you set up in the window.

See also Roles & Permissions Action reference Frequently asked questions

Frequently asked questions (permissions)

VERSION 3.10.1

WHY CAN I NOT SEE THIS BUTTON?

First look at **My profile** › **My permissions** › **What can I do and what can I not?** in your own account. There are five reasons why a button is not shown:

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 permission window.
That action is turned off	The CANNOT box shows the name of the action (e.g. "Alarms: delete alarm definition"); 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	It is not the button but the channel, device or screen itself that is not shown; the page comes up 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, Backup tabs; full project Export / Import; deleting records.	Cannot be given; 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: the values are visible and cannot be changed.
- **It saves but nothing changes in the field.** The "Reload the runtime" action is off. The user is told once: "Saved. A user who may reload the runtime is needed to apply the change to the running system." Either "Reload the runtime" is turned on for that user under **Tag write and services**, or someone who is permitted reloads.
- **The message "You have no permission for this action: ...".** The server rejected the action; the message names the action that is off.
- **The definition refers to a tag they cannot access.** 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.
- **A section in Settings is not saved.** The action of that section is off (e.g. "Branding settings"); its tab is not shown either.

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 unticking permission boxes nor turning actions off is applied; in the permission window the action boxes are locked and the list says "Administrator: fully permitted".

To restrict it, press **Remove role, keep permissions** in the permission 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 does not need a role: create the user, apply the **Manager** preset in the permission window (or assign the user to a group), then turn off what you do not want.

HOW DO I GIVE A RESTRICTION TO ONE USER IN A GROUP?

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

1. **If the restriction suits everyone**, turn the action off in the permission 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 (**— (none)** in the **Group** column), 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 (copy it and turn the action off) and move these people there.

The other way round, giving one person in a group **more** than the group is easy: in the user's window untick **No custom permissions (use the group's permissions)** and tick the extra box; their own permissions are merged with the group.

I TURNED IT OFF BUT THEY CAN STILL DO IT

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

DID PERMISSIONS CHANGE AFTER THE UPGRADE?

- Nobody lost access. Saved user-specific sets and group sets were widened once with the new View / Manage permissions (the table: Roles & Permissions, "Old permissions on upgrade").
- Nobody has an action restriction: all 95 actions start turned on for everyone who has the parent permission. Narrowing is Root's job.
- Accounts that have no group and no permissions of their own got the new default by themselves.
- What became narrower: the Administrator (Admin) role cannot read the retention counts or the backup and version lists and cannot delete audit and event records (Root only); reading management information now needs the permission to manage it. Details: "Behaviour changes" in the release notes.
- What became wider: the **Categories and groups** window is no longer Root only (see Categories and groups).

ON THE PHONE THE BUTTON IS SHOWN BUT IT SAYS "NO PERMISSION"

MergenHub Mobil does not yet show action restrictions on the buttons: if the module permission is there, the button is shown. When an action that is off is pressed the server rejects the request; the message arrives 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 on the button too (e.g. if "Write to tags" is off, the command buttons do not write).

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

Yes. The permission and action checks are on the server; the way in makes no difference.

WAY IN	WHAT HAPPENS WHEN THE ACTION IS OFF
REST API (cookie or HTTP Basic)	403; the body carries the key of the action: `{ "code": 403, "action": "alarms.ack", "message": "Requires 'alarms.ack' permission." }`
The in-app assistant and an external MCP token	A tool whose action is turned off does not appear in the list; if it is 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 rejects it (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).

WHERE DO I SEE WHO CHANGED WHAT?

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

See also Roles & Permissions · Action reference · Factory examples · REST API

Permissions page by page: which button needs which permission and action

VERSION 3.10.1

This section maps the rows of the permission window to the pages. The general rule: **a page you have no permission for is not shown in the menu, a button you have no permission for is not drawn on the page**. The OPC UA Client, SCADA, Settings, alarm bell and assistant buttons on the top bar are shown according to permissions too. If you arrive at a page you have no permission for through an old link, the Project page opens. If a request is rejected anyway, the message names the required permission ("This action needs these permissions: Counters and Metrics: Manage, Water Management: Manage").

The permission is the door of the module; most buttons on a page also depend on an **action**, and that action can be turned off with **Details** in the permission window. In the tables the name of the action in the window is in quotes, with its key next to it. The button of an action that is off is not shown; if it is rejected, the message names the action ("You have no permission for this action: Delete alarm definition"). The whole list: Action reference. For a button that is not shown, look at **My profile** › **My permissions** first.

PROJECT AND CONNECTIVITY

JOB	REQUIRED
Add, edit and delete channels, devices, tags, Virtual Tags, Tag Shortcuts	**Connectivity: Manage**. Adding, editing and deleting are separate actions for every object (`channel.create` … `alias.delete` , 15 actions). Copying counts as adding; tag groups and tag generation are tag actions; while edit is off the properties window opens read-only. For a saved change to reach the running system the "Reload the runtime" action is needed (`runtime.reload`).
Write a value to a tag, force a device read, device diagnostics, start / stop a service	**Tag write and services**. Actions: "Write to tags" (`tag.write` ; the pencil on the tag row and the SCADA command buttons), "Device diagnostics" (`diag.run`), "Start / stop services" (`service.control`), "Reload the runtime" (`runtime.reload`), "File upload" (`file.upload` ; Browse in the properties window). Forcing a device read has no action of its own.
The **Export** and **Import** buttons (full project; Kepware JSON included), export / import on the SCADA design toolbar	Root only. The buttons are not shown on any other account.
Templates window: **Make Template**, **Import (.mhtpl)**, installing and **Delete**	**Templates and import**. Actions: "Install templates" (`template.install`), "Package templates" (`template.package` ; importing a template file included), "Delete templates" (`template.delete`). It follows resource access: you package only the channels and screens you can access; a template cannot overwrite an existing resource you cannot access. Browsing and **Export file** work with Connectivity: View.
Saving a Virtual Tag	Every tag the expression refers to must be open to you. If the **Output** field is filled (a Virtual Tag that writes to a tag), Tag write and services is needed as well.
The subscription and connected-client window opened by clicking the active tag / client indicator in the status bar	**Server settings** or **Tag write and services**

ALARMS AND DATA LOGS

JOB	REQUIRED
See active alarms, acknowledge them, history	**Alarms: View**. Acknowledging is the "Acknowledge alarms" action (`alarms.ack`): if it is turned off the alarm is visible and the Acknowledge button does not appear. Taking the history to a file is the "Export alarm history" action (`alarms.export`).
Add, edit, delete on the **Definitions** tab	**Alarms: Manage**. Actions: "Add alarm definition", "Edit alarm definition", "Delete alarm definition" (`alarmdef.create` , `alarmdef.edit` , `alarmdef.delete`). A user with only View, or with edit turned off, opens a definition read-only.
Chart, history query, export	**Data Logs: View**. The download buttons depend on the "Export logged data" action (`log.export`).
Add, edit, delete a log group; delete old data; add a tag to logging from SCADA	**Data Logs: Manage**. Actions: "Add log group", "Edit log group", "Delete log group" (`loggroup.create` , `loggroup.edit` , `loggroup.delete`), "Delete old data" (`log.purge`), "Logging target" (`loggroup.target` : creating the table, moving to a data source). Every tag added to the group must be open to you.
Testing the connection in the log group window	Data Logs: Manage is enough to select a saved data source and test it; entering a connection by hand and testing it needs **Server settings**.

COUNTERS AND METRICS, WATER MANAGEMENT, REPORTS

JOB	REQUIRED
Define counters, metrics, manual inputs; manual values and corrections; **Categories and groups**	**Counters and Metrics: Manage**. Actions: "Add counter", "Edit counter", "Delete counter" (`counter.create` ...), "Add metric", "Edit metric", "Delete metric" (`metric.create` ...; a manual input definition counts as a metric), "Enter manual values" (`input.enter` : **Enter period value**), "Correct counters" (`counter.correct` : **Manual adjustment**, **Meter replacement**), "Categories and groups" (`taxonomy.manage` ; also needs access to all connectivity). The export buttons are the "Export counter data" action of the View permission (`metering.export`).
Try in the metric details	Counters and Metrics: Manage. A user who only views can open the breakdown of a period.
The **Data store** button on the Counters page	**Server settings** and the "Data sources" action (`settings.datasources`)
See the Water Footprint, Water Efficiency, Water Flow Diagram pages	**Water Management: View** (the Counters permission is not needed; category and counter names come with the page).
Water profile and diagram settings	**Water Management: Manage**. Actions: "Add water profile", "Edit water profile", "Delete water profile" (`waterprofile.create` , `waterprofile.edit` , `waterprofile.delete`). The export and print buttons are the "Export water reports" action of the View permission (`water.export`).
Entering a manual counter value, rainfall, analysis, production, headcount and area into the table on the water pages	**Counters and Metrics: Manage** and the "Enter manual values" action (`input.enter`). When it is off the value cells cannot be clicked.
Water setup wizard	Water Management: Manage and Counters and Metrics: Manage together; plus the "Water setup wizard" action (`water.setup`). If one of the permissions is missing the wizard says which one.
Open, run and download a report, report page and counter tracking list; refreshing of the live cards	**Reports: View**. The Excel / PDF / CSV buttons are the "Download reports" action (`report.download`): when it is off the report opens on screen and cannot be downloaded; the Excel template of a counter tracking list and the user's data access keys do not work either. A report based on alarms, logged data or the audit log also needs the View permission of that source.

Design a report, preview an unsaved report, delete	**Reports: Manage**. Actions: "Add report", "Edit report", "Delete report" (`report.create` , `report.edit` , `report.delete`); they are the same for table reports, report pages and counter tracking lists. Selecting a source in the editor needs the View permission of that source. Creating a key in the "reading from external systems" window of a report needs the Server settings permission and the "Data access keys" action (`settings.accesskeys`).
The **Excel reports** tab on the Counters and Metrics page	Shown with Reports: View; designing needs Reports: Manage. Changing a group colour needs Counters and Metrics: Manage.

AUTOMATION

JOB	REQUIRED
Flow list and run history	**Automation: View**. The flow opens read-only; there is no **Validate** button, expression check or cron summary.
Add, edit, delete, enable and disable a flow	**Automation: Manage**. Actions: "Add flow", "Edit flow", "Delete flow" (`workflow.create` , `workflow.edit` , `workflow.delete`) and "Enable / disable flows" (`workflow.enable`). With edit off and enable / disable on, the user stops a flow but cannot change what is inside.
The **Run** button	Automation: View + **Tag write and services**; action: "Run a flow by hand" (`workflow.run`). While it is off, scheduled and tag-triggered flows keep running.
Saving a flow that writes to a tag	Automation: Manage + Tag write and services; every tag written and read must be open to you.
Saving a flow that acknowledges alarms	Also the Alarms permission and access to the alarm's tag.
A flow that sends e-mail / SMS to a recipient that is not a registered user's address or an alarm notification recipient	Also **Notification settings**.
A flow that sends an HTTP request to the server itself (`localhost` , `127.x` , `169.254.x`)	Also **Server settings**.

Read-only flow. A flow that refers to a tag you cannot access, or contains a step you may not perform, is shown in the list with a **lock icon**. In the editor the **Read-only** badge and the reason are written; there is no Save, Delete, enable / disable or Run; tag paths, the webhook key, HTTP headers and recipients arrive masked. These rules are applied only **at save time**: saved flows keep running.

Webhook key. In the webhook trigger the **Key** field is read-only: the server generates the key (32 characters, random) and it cannot be typed. **Renew** clears the key; a new one is generated on save and the old address stops working. You give the external system the address in the **Endpoint** field. A warning is shown for an old, short key (it keeps working; replace it with Renew). The `/hooks/` endpoint accepts at most **60** requests per minute from the same IP address; more returns 429. The response body of an HTTP step is not stored in the run history (the status code, duration and byte count remain).

DATA BRIDGE

Seeing the Data Bridge tab and managing the agents needs the **Data Bridge** permission. Actions: "Add agent", "Edit agent", "Delete agent" (`agent.create` , `agent.edit` , `agent.delete`) and "Test agents" (`agent.test` : **Send test request** and the report agent preview). The global switches on the tab are saved with the "Edit agent" action. Every tag an agent sends or serves must be open to the user who saves it.

FIELD	RULE
REST Server agent, **Allow anonymous access**	Starts unticked on a new agent; only **Root** can turn it on. While it is off the `/iotgateway/` endpoint asks for credentials: the reading account needs Connectivity: View and access to the tags it reads, the writing account needs Tag write and services. A tag the account cannot see does not appear in the list.

REST Server agent, **Allow write**; MQTT agent, **Write topic**	Locked if you do not have Tag write and services. Every write made through this endpoint goes to the audit log.
Changing the target (server, port, user)	The saved password / key is not sent to the new target: it is entered again. **Send test request** verifies the target's certificate.

SETTINGS: EVERYONE SEES ONLY THE TABS THEY CAN CHANGE

TAB	REQUIRED PERMISSION	ACTION (WHEN TURNED OFF THE TAB IS NOT SHOWN)
OPC UA Server, **OPC UA Users**	**Server settings**	"OPC UA server settings" (`settings.opcua`)
Web, REST API & Mobile	Server settings	"Web and REST API settings" (`settings.api`)
Data sources	Server settings	"Data sources" (`settings.datasources`)
Mobile push	Server settings	"Mobile access settings" (`settings.mobile`)
Branding	Server settings	"Branding settings" (`settings.brand`)
Feature groups	Server settings	"Feature groups" (`settings.features`)
License	Server settings	"License" (`settings.license`)
Services	Server settings	"Services and resource thresholds" (`settings.services`). The Start / Stop / Restart buttons on the page also need the "Start / stop services" action of the Tag write and services permission.
Trusted Clients	**Certificates**	"Client certificates" (`cert.trust`)
Server Certificate	Certificates	"Server certificate" (`cert.instance`)
The web certificate buttons on the Web, REST API & Mobile tab	Certificates	"Web certificate" (`cert.web`); when it is off the buttons are not shown
Email, **SMS**, **Communication**	**Notification settings** (changing the e-mail / SMS sending server is Root only)	"E-mail settings" (`notify.email`), "SMS settings" (`notify.sms`), "Communication Center" (`notify.comm`)
Data Bridge	**Data Bridge**	The tab is shown with the permission; the buttons depend on the agent actions
Audit	**Audit log**	It has no actions
Users, Retention, Security, Backup	Root only	Cannot be given

The Server settings permission has two more actions that have no tab in the interface: "Scan settings" (`settings.scan` ; changed with REST or MCP) and "Data access keys" (`settings.accesskeys` ; from the report window). The assistant settings are under the same permission too: the Providers and MCP tabs depend on the "AI provider" action (`ai.provider`), the Skills tab on "Assistant skills" (`ai.skills`) and the extra instructions field on "Extra instructions" (`ai.prompt`).

A user with no permission for any tab does not see the **Settings** button. The license fingerprint, owner, activation and new-version information are shown only to a user with the Server settings permission; the license badge and the trial pill are clickable only for that user. In the log group window Data Logs: Manage is enough to **select** a data source; adding and editing a source needs Server settings.

OPC UA CLIENT AND MCP

JOB	REQUIRED
Connecting, disconnecting and discovering servers on the OPC UA Client page	**OPC UA client**; action: "Connect and discover" (`uaclient.connect`)
Subscribing to a node, removing a subscription	OPC UA client; action: "Subscriptions" (`uaclient.subscribe`)
Writing a value to a node on the remote server	OPC UA client; action: "Write to the remote server" (`uaclient.write`)
Creating, disabling and deleting tokens on the MCP (AI) page	**MCP**; action: "MCP tokens" (`mcp.token`)

AUDIT LOG AND EVENT LOG

The **Settings** → **Audit** tab is shown with the Audit log permission. In addition to configuration changes the following are recorded: **tag writes** (tag = value), starting / stopping / restarting a service, running a flow by hand, a write made through the write endpoint of the REST Server agent (who or "anonymous", client address) and webhook calls (key masked). Permission and action restriction changes are written in detail too (who, for whom, permissions added / removed, actions turned off / on). The **Clear History** button on the Audit tab and the **Clear History** button in the Event Log are shown only to Root.

SCADA MACROS

A macro's `MH.query` queries run with the permissions of the user who opens the screen: `alarms` , `alarmDefs` , `alarmHistory` need Alarms: View; `audit` Audit log; `subsystems` Server settings; `agents` Data Bridge; `loggerStatus` , `loggerGroups` Data Logs: View; `opcuaClients` Server settings or Tag write and services. Without the permission the query returns the message "You have no permission for this data" instead of data and no request goes to the server.

See also Roles & Permissions Action reference Factory examples Assistant and MCP Data Bridge

Passwords, forgot password and sessions

VERSION 3.10.1

FORGOT PASSWORD

1. On the sign-in screen click **Forgot password?**; type your username, e-mail or phone and press **Send code**.
2. An **8-digit** verification code arrives at the e-mail or phone saved on your account. The code is valid for **5 minutes**.
3. Type the whole code into the **Verification code** field and your new password below it, then press **Reset password**. A code with missing digits is not sent.

SITUATION	WHAT HAPPENS
You requested a new code	There is one active code per account: the previous code becomes invalid.
You typed the code wrong	After **5** failed attempts in total the code becomes invalid and no new code is issued for **15 minutes**. Requesting a new code does not reset the counter.
No code arrived	The screen looks the same even if the account you typed does not exist (whether the account exists is not revealed). Ask your administrator for the username and the e-mail / phone saved on the account.

> **If you use a custom template** If your password reset e-mail or SMS template says "6-digit code", correct the text: as of 3.10.1 the code has 8 digits.

OTHER SESSIONS ARE CLOSED WHEN THE PASSWORD CHANGES

When you change your own password, when Root resets it, or when it is renewed through forgot password or an invitation, the account's **sessions in other browsers**, **phone (mobile app) sessions** and **MCP tokens** are closed. The session that made the change stays open; the screen tells you how many phone sessions and MCP tokens were closed.

- Sign in to the app on the phone again.
- MCP tokens are **deleted**: create a new token on the **MCP (AI)** page for the external AI client (such as Claude Desktop).
- When a user is deleted their phone sessions, MCP tokens and data access keys are deleted too.

CHANGING THE E-MAIL OR PHONE ASKS FOR THE PASSWORD

In the **My profile** window the **Your current password** row appears when you change the e-mail or the phone; it is not saved without the password. In **Alarms** → **My Alarm Notifications**, if the e-mail or phone is changing, you are asked for your current password when you press Save. If the value does not change (only the notification boxes), no password is asked. The reason: the recovery address must not be changed from a computer whose session was left open, taking over the account.

USERNAME, INVITATION AND SIGN-IN LOCKOUT

TOPIC	RULE
Username	A second account cannot be created with a name that differs only in letter case ("Ömer" / "ömer", "İlker" / "ilker"); an account cannot be renamed to such a name.
Invitation	A user who is not Root can invite only a user with a lower role than their own. An invitation closes the open sessions of the target account. The sign-in address in the e-mail is taken from the **Public address (public URL)** field.
Sign-in lockout	After 8 failed attempts in 5 minutes the account is locked for 5 minutes (HTTP 429). The same limit is applied per username to the REST API's username / password (Basic) sign-in.

See also Roles & Permissions MCP token

HTTPS / Public Exposure

Settings → **Web, REST API & Mobile**: the **Certificate** tab (generate self-signed or upload PFX) and the **Publishing & HTTPS** tab (choosing your case and its steps, HTTPS port, HTTP→HTTPS redirect, public address, check). Step-by-step guide: Publishing on the Web. When exposing to the internet: set the listen address to `0.0.0.0`, point DNS at the server, open the firewall ports, disable AllowAnonymous, and a strong password is mandatory. Changes are applied on restart.

RUNNING BEHIND A REVERSE PROXY (TRUSTED PROXIES)

If there is a reverse proxy (IIS, nginx, load balancer) in front of the server, the client's real address and the fact that the connection is HTTPS are told by the `X-Forwarded-For`, `X-Forwarded-Proto` and `X-Forwarded-Host` headers the proxy adds. As of 3.10.1 these headers are accepted **only from a trusted proxy** (before, they were accepted from anyone: the client address and the "I came over HTTPS" information could be forged).

WHERE THE PROXY IS	WHAT TO DO

On the same computer (IIS, nginx, cloudflared)	Nothing. A proxy on this computer is always trusted.
On another machine	On the **Settings** → **Web, REST API & Mobile** → **Publishing & HTTPS** tab (path C, "Where is the web server?" = On another computer), type the proxy's address into the **Trusted proxies** field: one IP address or CIDR network per line (e.g. `10.0.0.5` or `10.0.0.0/24`). Save and **restart the service**. An invalid address is not saved; the message says which line is invalid.
A cloud proxy connects directly to the server	Type the provider's address ranges. Not needed if you use a `cloudflared` tunnel (the tunnel is local).

Symptom after upgrading. If the proxy is on another machine and the field is empty: the audit log and the active users show the proxy's address instead of the client's; if "Redirect HTTP to HTTPS" is on the page may enter an endless redirect; a data access key (`mhkey_`) may be rejected as "HTTPS only". The fix is the field above.

The **Public address (public URL)** (MCP (AI) page) is a separate setting: the sign-in address in invitation and announcement e-mails and the AI / MCP addresses are derived from it. It is not needed for the origin check below.

A REQUEST COMING FROM ANOTHER SITE (ORIGIN CHECK)

If a page on another site tries to act on your behalf while your session is open, the server rejects the request with 403. The decision is made with the origin reported by the browser; reverse proxy installations and scripts are not affected. Browsers send this information only on **HTTPS** and `localhost` addresses: if you open the interface over plain HTTP by IP address, this check does not come into play. Turn on HTTPS for full protection.

Hardening the Server: data folder lock, backup password, disk encryption

VERSION 3.11.0

MergenHub keeps all of its data in the **data folder** on the server: `C:\ProgramData\MergenHub`. It holds users and permissions, the project, settings (e-mail / SMS password, connection keys), logs, certificates and backups. The database files as a whole are not encrypted; the **passwords inside them are encrypted** (see "Stored passwords are kept encrypted" below). This section explains how to limit access to these files by someone who can reach the server, with **three separate measures**. All three are **optional** and none of them is turned on by itself. The encryption of stored passwords, however, is always on and asks nothing of you.

THREAT	MEASURE	WHERE
The settings file or the database is obtained **on its own** (a file sent to support, a copied file), or a user who is not an administrator opens the settings file	**Encryption of stored passwords** (always on)	By itself. Status: Settings → Security → Stored passwords
A Windows user who can sign in to the server and is **not an administrator** opens and reads the files	**Data folder lock**	Settings → Security → Data folder protection (or the setup wizard)
A backup file leaves the server: network share, e-mail attachment, a disk that is carried away	**Backup password**	Settings → Backup → Backup password
The disk of the server is stolen or removed, or the server is scrapped	**Disk encryption** (BitLocker)	In Windows; MergenHub does not do this itself
Someone who is a Windows **administrator** opens or changes the files	The application cannot prevent this. Limit who is an administrator.	In Windows

> **Default state** If you chose nothing after installation: every Windows user on the server can read the data folder (this is the Windows default permission for `ProgramData`), and backups are plain zip files. The certificate, backup and version history folders and the service key are always open to administrators only. User passwords are not stored as plain text in the file (they are stored as a hash); the e-mail / SMS password, connection keys and driver passwords are stored encrypted too (since version 3.12.0; earlier versions stored them as plain text).

STORED PASSWORDS ARE KEPT ENCRYPTED

VERSION 3.12.0

The passwords you enter in MergenHub are not kept as plain text in the files and the database; they are encrypted with **AES-256**. Scope: the e-mail and SMS password (with a generic SMS provider the address and body template too: the key is usually there), OPC UA users, the passwords and tokens of data bridge agents, AI keys, data source and data logging connections (the password and the whole ODBC connection string), driver passwords (MQTT, OPC UA client, IEC 61850...), webhook keys and headers in automation flows, the backup password and the password of the HTTPS certificate. Configuration version history files and project files saved through the API (the projects folder) are encrypted as a whole.

Nothing is asked of you. You enter passwords as usual; the interface and the API do not change (passwords are shown masked as before). If you upgraded from an earlier version, the plain-text passwords left by that version are encrypted once when the service first starts, and the event log gets a "Kayıtlı parolalar şifrelendi" (stored passwords encrypted) entry.

Seeing the status (Root user only). The **Stored passwords** card at the bottom of the **Settings** → **Security** page says "Stored passwords are ENCRYPTED" and shows the name of the key file. If there is a problem the same card states the reason: "Some stored passwords cannot be opened", or the names of the files that still contain plain-text passwords.

Where is the key? Every installation creates its own random key; the key is not built into the program. Its file is in the data folder: `C:\ProgramData\MergenHub\keys\secrets-XXXXXXXX.key` (XXXXXXXX is the identifier of the key). The `keys` folder can be read only by **SYSTEM** and **Administrators**, even when the data folder lock is off. **Do not delete or change** this file.

QUESTION	ANSWER
What does it protect against?	A Windows user who is not an administrator and can read the settings file or the database but not the key folder; a file obtained on its own (a settings file sent to support, a copied database); someone looking inside a backup that has no password.
What does it not protect against?	A Windows administrator, and someone who obtains the **whole** data folder or the **whole of a backup without a password**: the key is in there too. For those use a backup password and disk encryption (below).
If I restore the backup on another server, do I enter the passwords again?	No. The backup contains the `keys` folder as well; the passwords open by themselves on the new server. The new server's own key is not deleted: the two key files sit side by side in the folder.
I copied only the settings file or the database to another server	The passwords in that file cannot be opened: the top bar and the **Stored passwords** card show the "Some stored passwords cannot be opened" warning, and connections that use those passwords do not work (no connection is attempted: a value that cannot be opened is never sent to the other system as a password). Copy the files inside the `keys` folder of the old server into the `keys` folder of the new server as well and restart the service, or enter the passwords again. The passwords are not deleted; they open by themselves once the key is there.
What if the key file is deleted?	The passwords encrypted with that key cannot be opened and must be entered again. The key is also inside your backups: you can put it back from there.
What if I have to go back to an older version (3.11.0 and earlier)?	The older version cannot read the encrypted values. **Before** going back, with the services stopped, turn the passwords into plain text from an administrator command prompt (the command below).

What if I choose "Include credentials" for a project package?	The package carries the passwords as plain text so that it can be imported into another system. That is your explicit choice; store the package accordingly.
What about backups taken before the upgrade?	They stay as they are: the settings file and the database inside them are as they were on the day they were taken, so the passwords are plain text. Delete the ones you do not need or move them somewhere safe; take a new backup after the upgrade.
What is not encrypted?	Logs, event and audit records and assistant conversations are free text. Do not write passwords into description, note and message fields.

Command line (from an **administrator** command prompt on the server):

```
"C:\Program Files\MergenHub\MergenHub.exe" secrets status
"C:\Program Files\MergenHub\MergenHub.exe" secrets decrypt
"C:\Program Files\MergenHub\MergenHub.exe" secrets encrypt
```

`status` reports whether the key is in place and which files still contain plain-text passwords. `decrypt` turns all passwords into plain text: use it only before going back to an older version, with the services stopped. `encrypt` encrypts the remaining plain ones right away (the service already does this at every start).

1. DATA FOLDER LOCK

The lock opens the data folder only to the **SYSTEM** and **Administrators** accounts. Windows users who are not administrators cannot open any file in the folder. The lock is **off by default**; turning it on is your decision.

Check before you turn it on

- **Service account.** The MergenHub services are installed to run as the SYSTEM account; in that case the lock does not affect them. If you changed the account of the service *by hand*, first give that account full control of the data folder, otherwise the service may fail to start.
- **Other software that reads the folder.** If a backup agent or monitoring software reads the folder with an account that is not an administrator, it cannot read it after the lock. Give that account read permission on the folder by hand; the lock **keeps** permissions you granted by hand to a specific account and only removes the permission of broad groups such as "Users".
- **Support.** Collecting the log files (`logs`) now needs administrator rights: File Explorer asks "Continue" when you enter the folder.

Turning it on from the interface (Root user only)

1. Open the **Settings** → **Security** page. At the bottom of the page the **Data folder protection** card shows the state: "Lock is OFF" or "Lock is ON", the path of the folder and the **Who can access the folder right now** table. If the table has a row marked "broad group" (for example `BUILTIN\Users`), users who are not administrators can read the folder.
2. Press the **Lock the folder...** button. The window that opens states what changes, who is affected, what may break, what the lock does not protect against and how to undo it. Read all of it.
3. Tick all **three boxes** below it and press **I have read it, continue**. You cannot go on until the boxes are ticked.
4. In the **Final confirmation** window type the **name of the server** shown on the screen into the box and press **Lock**. If the name does not match nothing is done (so that the lock is not confirmed on the wrong server or out of habit).
5. The card changes to "Lock is ON"; no broad group remains in the table. The operation is written to the audit log.

Turning it on during setup. The setup wizard has a **Data Folder Protection** page; the box "Lock the data folder — only SYSTEM and Administrators can read it" comes **unticked**. If you tick it, the same warnings are shown when you press Next

and you are asked once more (the default button is No). If you do not tick it the permissions are not touched; if the folder was locked before, it stays locked. In a silent installation the lock is turned on with the `/LOCKDATA=1` parameter.

Removing the lock. On the same card: **Remove the lock...** → tick the box → type the name of the server → **Remove the lock**. The folder inherits the permissions of `ProgramData` again: every Windows user on the server can read the files again.

If the interface cannot be reached (for example the service does not start), from an **administrator** command prompt on the server:

```
"C:\Program Files\MergenHub\MergenHub.exe" data-lock status
"C:\Program Files\MergenHub\MergenHub.exe" data-lock off
"C:\Program Files\MergenHub\MergenHub.exe" data-lock on
```

`status` prints the state, `off` removes the lock, `on` locks (it does the same job as the button in the interface; it shows no warning).

QUESTION	ANSWER
Do the tray icon and the desktop app keep working?	Yes. They read the address of the interface from a separate file that contains no secrets (`public\shell.json`); that file stays readable to everyone.
Does an upgrade break the lock?	No. Setup does not touch the permissions unless you tick the box.
Does the lock protect against a Windows administrator?	No. An administrator can open every file and can also change the permissions.
What if the backup folder is somewhere else?	The lock covers the data folder only. The permissions of a backup folder on a network share or on another disk are yours to manage; use a **backup password** for the files there.
The service does not start after the lock	The service account may have been changed by hand. Remove the lock with `data-lock off` from an administrator command prompt, give the account full control of the folder, then lock again.

2. BACKUP PASSWORD

A backup file contains the user accounts, the server settings and the saved connection passwords. If no password is given the backup is written as a **plain zip**: anyone who gets hold of the file can read what is inside. The stored passwords inside it are encrypted, but their key is inside the backup as well so that the backup can be opened on another server; a determined person who obtains the whole backup can open them. If you give a password the backup is written encrypted (its extension is `.mhbak`) and cannot be opened without the password; the copy that goes to a network share, an e-mail attachment or another disk is protected too.

1. On the **Settings** → **Backup** page go to the **Backup password (optional)** part.
2. Type the same password into the **Password** and **Password (again)** fields (at least 8 characters) and press **Save**.
3. Read the warning that opens and, after you have written the password down in a safe place outside the server, press **I wrote it down, save**.
4. Backups taken from now on appear in the list with a lock icon and the `.mhbak` extension. Backups taken earlier stay as they are.

> **If the password is forgotten** The backup cannot be opened; there is no way to recover it, and Envest cannot open it either. Keep the password in a safe place outside the server.

Opening a password-protected backup. There are two ways:

- **From the interface:** Settings → Backup → **Decrypt and download** on the row of the backup → type the password → **Decrypt and download**. A plain zip is downloaded to the browser. The password is used for that request only and is not stored.
- **From the command line** (if the server is not running or the backup was moved to another machine; MergenHub must be installed on that machine):

  ```
  "C:\Program Files\MergenHub\MergenHub.exe" backup-decrypt MergenHub-yedek-20261116-020000.mhbak
  yedek.zip
  ```

  The command asks for the password (it is not shown on the screen) and writes the plain zip.

The restore steps are the same as for a plain backup: first decrypt the backup, then stop the service and extract the zip into the data folder. See Migrating with History and Full System Backup.

> **Where is the password kept?** Because the scheduled backup runs unattended, the password is stored in the settings file of the server, **encrypted** like the other stored passwords. Anyone who can read the key folder (a Windows administrator) can open the password; users who are not administrators cannot. The backup password protects a file that **leaves the server**; for the other files inside the server use the data folder lock. The interface and the API never show the password.

Removing the password. Clear both fields and press **Save**; confirm the warning. Later backups are plain zip files. Password-protected backups taken earlier can still be opened with the old password.

3. DISK ENCRYPTION (BITLOCKER)

The data folder lock and Windows permissions are in force only while Windows is running. If the disk is removed from the server and attached to another machine the permissions mean nothing: the files can be read. The only protection against this is encrypting the disk. MergenHub does not do this itself; use the **BitLocker** feature of Windows.

- On Windows Server add the **BitLocker Drive Encryption** feature; turn it on for the drive that holds the data folder (usually `C:`).
- If you write backups to another disk or to a removable disk, encrypt that disk too or use a backup password.
- Keep the **recovery key** outside the server. If the key is lost the data on the disk cannot be reached.
- On virtual machines the storage that holds the virtual disk and its backup must be protected in the same way.

4. WHO SHOULD BE AN ADMINISTRATOR?

Someone who is a Windows administrator can open the data folder, remove the lock, change the database and give themselves permissions, and stop the service. For this reason the three measures above are meaningful only if the administrator accounts on the server are few and supervised.

- Use an account that is not an administrator for daily work on the server; use administrator accounts for maintenance only.
- If operators do not need to sign in to Windows on the server, do not let them: they use MergenHub from a browser or from the desktop app on their own computers, with their own MergenHub accounts.
- Open remote desktop access (RDP) only to the people and networks that need it.

See also Roles & Permissions · Full System Backup · Publishing on the Web and HTTPS