Bivrost IoT Gateway

彼络物联网关

User Manual

Document Version V1.19.7.22

Bivrost Technologies Company Limited

深圳市彼络科技有限公司

Scan for support on WeChat

Contents

Product Licence Agreement

All products of BIVROST TECHONOLOGIES Company Limited (referred to below as Bivrost), including but not limited to software, hardware devices and documentation, together with all future orders, are governed by this agreement. If you are unwilling to accept these terms, contact customer service within 3 days of receiving the product for a refund. We will refund the purchase price, less shipping and a reasonable handling fee.

1. Permitted Use

You may use this product in the ways described in the documentation Bivrost provides, such as the product manual and the commissioning guide.

You may send commands to the product to perform the corresponding functions by calling the interfaces given in the communication protocol document Bivrost provides.

For additional customisation requirements, or for uses that fall outside the scope of the licence granted here, contact Bivrost before purchasing the product. Bivrost will assess each request on its merits and reply as to whether it can be implemented and what assistance can be offered.

2. Prohibited Use

Except as expressly permitted in Section 1, you may not copy, reverse-engineer, disassemble, decompile, modify, add to or enhance the software, the hardware or any other part of the product. Reverse-engineering any part of the software or the product, or attempting to derive the source code of the software, is prohibited. Installing or running any software not supplied by Bivrost on the hardware device is prohibited. Distributing the software on magnetic or optical media, or over a network, is prohibited.

3. Limited Warranty

Bivrost warrants that, for 12 months from the date the product is delivered and under normal conditions of use, the hardware will be free from material defects in workmanship and materials, and the software will be free from material faults.

4. Limitation of Remedies

When a claim is made under this agreement, Bivrost will provide free replacement or repair of the hardware and remote assistance to repair the software. Shipping and insurance must be prepaid when the product is returned to Bivrost or to a Bivrost authorised dealer.

Other than the warranty given in this agreement, Bivrost makes no further express or implied warranty and accepts no further liability for the products described in this agreement, including their quality, their performance and their fitness for any particular purpose.

5. Limitation of Liability

Whatever the cause, and whether arising under the provisions of a contract or from criminal matters, including negligence, where you or any other party suffers a loss caused by our product, or where the product is the cause of the action or is indirectly related to it, the total liability of Bivrost to you and to any other party shall not exceed the purchase price you paid for the product. Under no circumstances is Bivrost liable for losses arising from your failure to meet your obligations, for loss of data, profits or savings, or for any other consequential or incidental loss, even if Bivrost has been advised of the possibility of such loss, nor for any claim you bring on the basis of a third party’ s claim.

6. Termination

If you fail to comply with the terms set out in this agreement, your licence and this agreement will be terminated. However, Sections 2, 3, 4 and 5 remain in effect.

1. Introduction

Bivrost IoT Gateway Manual · Shenzhen Bivrost Technology Co., Ltd. · Tel: 18824672282

The Bivrost IoT Gateway provides data acquisition and machining program transfer for CNC machine tools, laser welders, robots, PLCs and similar equipment. A single gateway can collect from and manage up to 255 devices of different models. It supports all major machine tool controls, exposes a comprehensive software API, is flexible to configure and works out of the box. It reconnects automatically after a dropped link, resumes interrupted transfers, polls multiple machines in parallel from one unit, collects data at millisecond resolution, and forwards data over a range of protocols.

The current version can collect data from the following CNC machine tool brands:

System [Model]	Basic Data	Axis Data	OEE Monitoring	PLC Data	DNC	Tool Data
Bosunman	√	√	√	√	√	√
Brother	√	√	√	√	√	√
Citizen	√	√	√	√	√	√
Delta	√	√	√	√	√	√
Dmg Mori	√	√	√	√	√	√
Fagor	√	√	√	√	√	√
Fanuc	√	√	√	√	√	√
Gsk	√	√	√	√	√	√
Haas	√	√	√	✗	√	✗
Heidenhain	√	√	√	√	√	√
Hnc	√	√	√	√	√	√
Jingdiao	√	√	√	√	√	√
Kede	√	√	√	√	√	√
Knd	√	√	√	√	√	√
Lnc	√	√	√	√	√	✗
Lynuc	√	√	√	√	√	√
Mazak	√	√	√	√	√	√
Makino	√	√	√	√	√	√
Mitsubishi	√	√	√	√	√	√
Muratec	√	√	√	√	√	√
Okuma	√	√	√	✗	√	✗
Rexroth	√	√	√	√	√	✗
Siemens	√	√	√	√	√	√

System [Model]	Basic Data	Axis Data	OEE Monitoring	PLC Data	DNC	Tool Data
Syntec	√	√	√	√	√	√

Where:

- **Basic Data**: Count, Alarm, Status, Mode, Tool No., Program Info, Program Block, and so on.
- **Axis Data**: Actual Feedrate, Feedrate Override, Spindle speed, Spindle Override, Position, Spindle Load, Servo Axis Load, and so on.
- **OEE Monitoring**: Autorun Time, Manual Time, Wait Time, Emergency Time, Off Time, Availability, and so on.
- **Data Handling**: Forwarding over the MQTT, MODBUS and HTTP protocols; writing to a database.

2. Networking

2.1. Gateway Network

The Bivrost IoT Gateway has two wired Ethernet ports, LAN1 and LAN2, plus a built-in wireless adapter.

LAN1 is dedicated to the data-acquisition network. Its default IP address is 192.168.100.1 and its default subnet mask is 255.255.0.0. If several gateways share the same internal network, change the gateway network settings so that no two static IP addresses collide (see 3.7.1. Wired Network). To collect machine data, connect LAN1 directly to the Ethernet port of a CNC machine with a network cable for one-to-one acquisition, or connect LAN1 and the CNC machines through a switch or similar device so that they share one acquisition network for parallel acquisition.

LAN2 is the external communication port. If you need to upload data to the cloud or to receive remote assistance, contact Bivrost first, then connect LAN2 to the external network.

The **wireless adapter** can join a WiFi network (see 3.7.2. WiFi Settings) and serves the same purpose as LAN2. It is especially useful when testing in a plant that has no network in place: connect the gateway to a phone hotspot and remote assistance becomes much easier to arrange.

2.2. Networking Steps

In a typical customer network architecture, machines of all kinds connect to the gateway over Ethernet, serial over Ethernet, WiFi, a 4G/5G network or other links. Servers running applications such as MES connect to the gateway and read data and issue commands over HTTP, MODBUS, MQTT, a database or other channels.

1. Connect the gateway to the CNC machines, switches, servers and other equipment (see 2.1. Gateway Network).
2. Configure the network settings on the CNC machines (see *Bivrost IoT Gateway — Machine Setup*, referred to below as *Machine Setup*).
3. Start the gateway, sign in, configure it, add the CNC machines and restart the gateway service (see 3.1. Signing In through 3.7. Network).
4. Check that the gateway is receiving machine data (see 3.8. API Test).
5. Following the communication protocol documentation (see *Bivrost IoT Gateway — Communication Protocol*, referred to below as *Communication Protocol*), debug your server-side program and confirm that it receives data from the gateway. If no physical

machine is available, choose the **Mock** machine type when adding a machine so you can test communication between the gateway and the server (see 3.3.1. Adding a Machine).

6. If you need data storage, analysis or dashboard displays, configure them on the Bivrost cloud platform (see *Bivrost Cloud Platform — User Manual*, referred to below as *Cloud Platform Manual*).

To ensure acquisition quality, we recommend shielded Cat 5e or Cat 6 cabling and gigabit network equipment. If a CNC machine has to connect over a wireless network, fit it with a wireless module or a 4G/5G module.

3. Using the Gateway

The gateway is configured to start automatically when power is applied. After connecting the power supply, wait about 1 minute for start-up to finish; the gateway is then ready to use.

You connect to the gateway from a computer and sign in to the gateway management page in a browser.

The first time you connect to the gateway, use an Ethernet cable between the computer’s LAN port and the gateway’s LAN port.

We recommend the latest version of Chrome on the computer used to sign in. Browsers such as 360 or IE may not render the page completely.

To switch the gateway off, use the **Shutdown/Restart Gateway** function button in the top right of the gateway management Home page, and unplug the power cable only after the gateway’s power LED has gone out.

> **Caution**
>
> **Frequent loss of power can make the gateway behave abnormally.** For example, if power is reapplied within 15 seconds of a momentary trip, the gateway may fail to restart automatically, in which case you have to press its power button manually. To avoid frequent power loss, install the gateway where the supply is stable, and fit a UPS if possible.

The navigation bar at the top of the gateway management page contains four menus: **Configurations** (Machines / Group / Task / Communication), **Diagnosis** (API Test / Network Tools / Logger), **App** (DNC / Analysis / Monitor) and **System** (Network / Settings). This chapter covers each function of the gateway management page in turn:

3.1. Signing In

You can connect a computer to the gateway in any of the following ways:

1. Connect the computer’s LAN port directly to the gateway’s LAN1 port, or to LAN1 through a switch, then set the computer’s IP address to an address on the same subnet as the gateway’s LAN1 port, with the same subnet mask.
2. Connect the computer’s LAN port directly to the gateway’s LAN2 port, or to LAN2 through a switch, then set the computer to obtain its IP address automatically.
3. Connect the computer and the gateway to the same wireless network. You must first use method (1) or (2) to connect, sign in and configure the gateway’s WiFi connection.

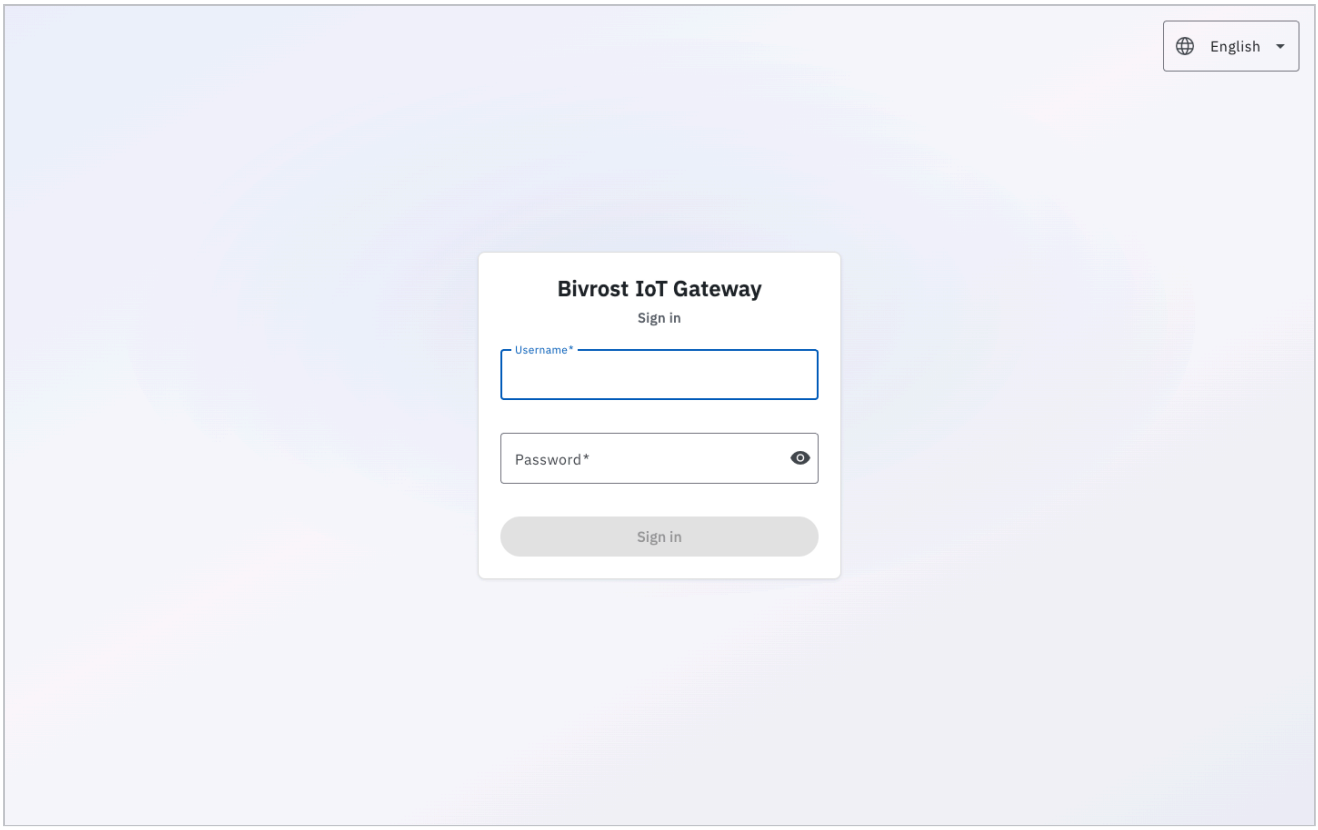
Once connected, you can sign in to the gateway management page in either of the following two ways:

Method 1: Signing In by Domain Name

In the address bar of the computer’s browser (Chrome recommended), enter the following address:

```
http://iotgw.local
```

Press Enter to open the gateway management login page. The initial account and password are both admin. Click **Login**. You can switch the interface language in the top-right corner.



If sign-in fails, disconnect any other devices so that the computer is connected to only one gateway, check the network cabling, and try again.

On some early gateway models, if `iotgw` does not work, replace `iotgw` with BIV-[first part of the gateway UID]. The gateway UID is printed on the label on the bottom of the gateway. For example, if the gateway UID is “152KUCG-1TOSJH4-1WXYSON-JY531Q”, the first part of the UID is “152KUCG”, so the address to enter in the browser is:

```
http://BIV-152KUCG.local
```

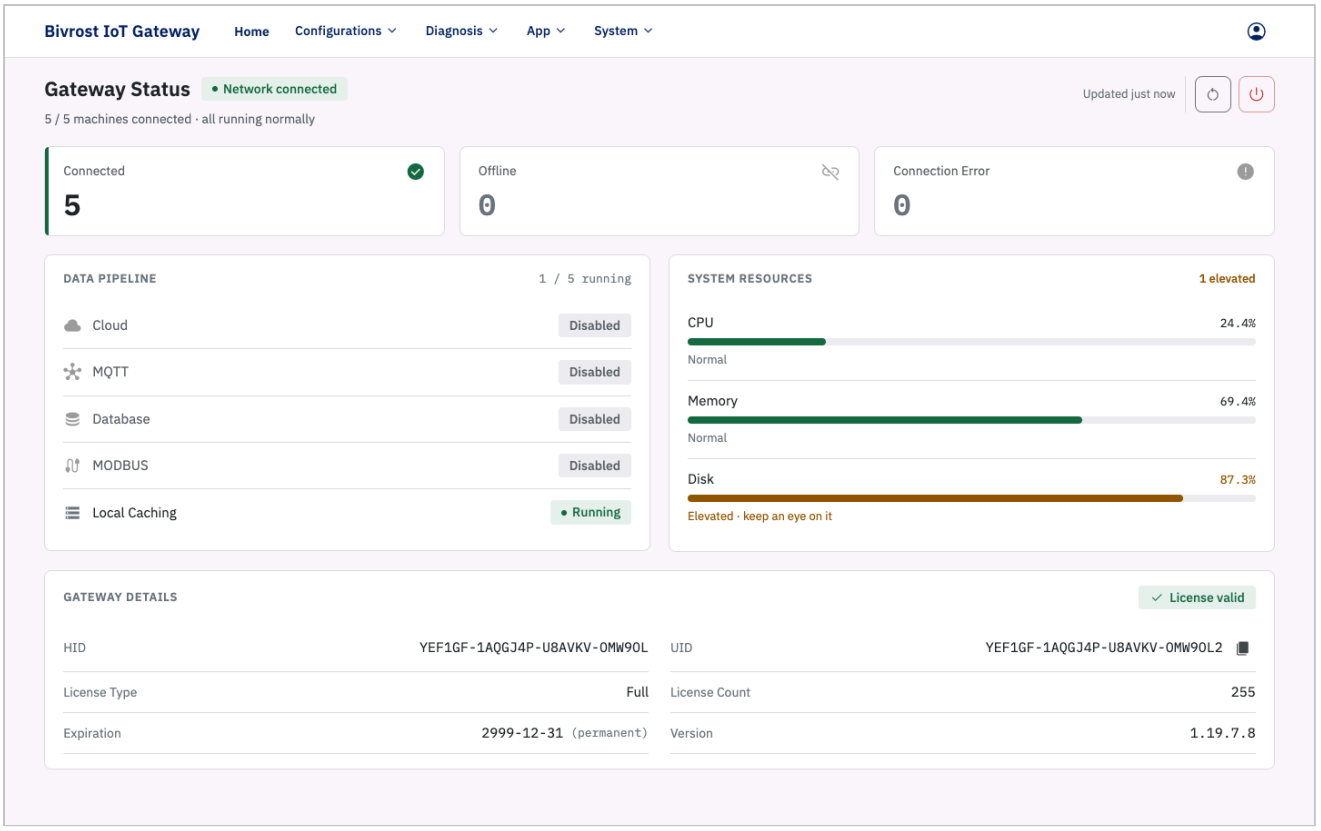
Method 2: Signing In by IP Address

Alternatively, in the address bar of the computer’s browser (Chrome recommended), enter the gateway’s IP address (the initial LAN1 IP is 192.168.100.1) and press Enter to open the login page. The initial account and password are both admin. Click **Login**. You can switch the interface language in the top-right corner.

> **Note**
>
> After changing the LAN1 IP address (see 3.7.1. Wired Network), sign in using the new IP address. If you are connected through the LAN2 port or over WiFi, use the corresponding IP address.

3.2. Home

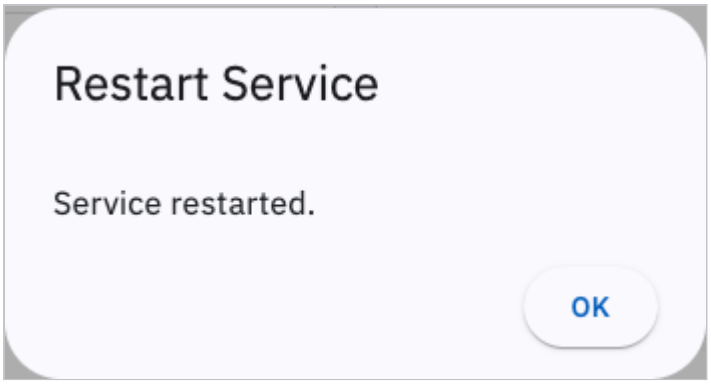
After you sign in, the gateway opens the **Home** page. The navigation bar at the top contains a **Home** link and four menus: **Configurations** (Machines/Group/Task/Communication), **Diagnosis** (API Test/Network Tools/Logger), **App** (DNC/Analysis/Monitor) and **System** (Network/Settings). The **Account** menu is in the top right corner. The page content is shown below the bar.



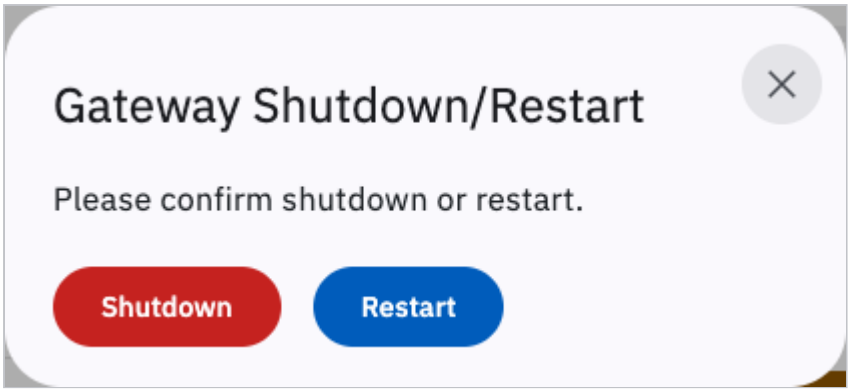
3.2.1. Function Buttons

The function buttons are in the top right corner of the “Gateway Status” panel on the Home page: **Restart Service** and **Gateway Shutdown/Restart**. After you change any configuration, the navigation bar also shows the prompt “Configuration changed. Restart the service for changes to take effect.” — click it to restart the service.

The **Restart Service** button restarts the gateway service. After you change configuration parameters — on the **Machines**, **Groups**, **Communication** or **Tasks** pages, for example — you must click **Restart Service** for the changes to take effect. Clicking **Restart Service** opens the restart dialog; after about 5~10 seconds it reports that the service has restarted, and you can click **Confirm** to close it.



The **Gateway Shutdown/Restart** button powers the gateway hardware down or restarts it.



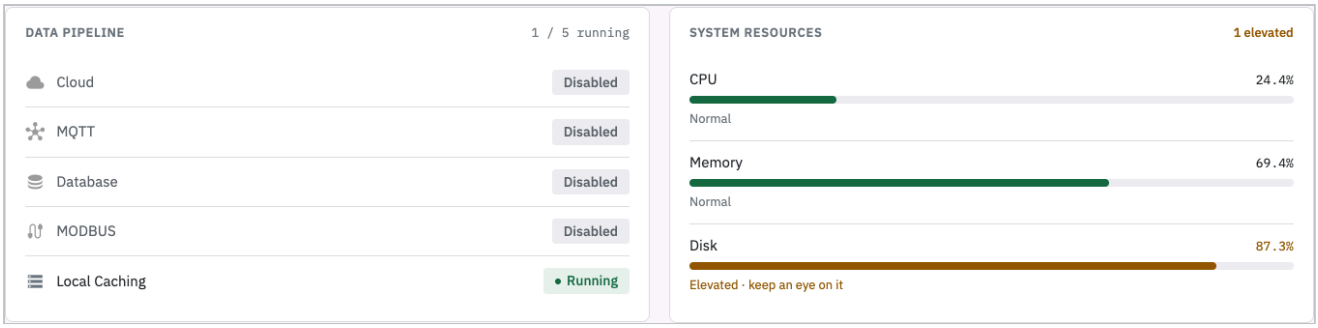
Click **Shutdown** to power the gateway hardware down safely. Wait until the gateway's power LED goes out before unplugging the power cable.

Click **Restart** to restart the gateway hardware. The restart takes about a minute.

3.2.2. Gateway Status

"Gateway Status" shows the gateway's main operating status. At the top is a summary of machine connections (the number of machines that are connected, offline or in connection error):

The "Data Pipeline" card shows the status of the Cloud, MQTT, Database, MODBUS and Local Caching services; the "System Resources" card shows CPU, Memory and Disk usage. All statuses refresh automatically every 5 seconds.



The individual entries under Gateway Status are described below:

Name	Description	Status
Network	Whether the gateway is currently connected to the internet	Connected: connected to the internet Disconnected: not connected to the internet
Cloud	Connection between the gateway and the cloud platform	Running: the Cloud service is on (see 3.6.1. Cloud Settings), correctly configured, and connected to the server Off: the Cloud service is off Delayed: an upload did not complete in time, for example because of network latency Other statuses: the Cloud service has failed
MQTT	Connection between the gateway and the MQTT server	Running: the MQTT service is on (see 3.6.3. MQTT Settings), correctly configured, and connected to the server Off: the MQTT service is off Delayed: an upload did not complete in time, for example because of network latency Other statuses: the MQTT service has failed

Name	Description	Status
Database	Connection between the gateway and the database	Running: the Database service is on (see 3.6.4. Database Settings), correctly configured, and connected to the server Off: the Database service is off Delayed: an upload did not complete in time, for example because of network latency Other statuses: the Database service has failed
MODBUS	Status of the gateway’s local MODBUS service	Running: the MODBUS service is on (see 3.6.2. MODBUS Settings), correctly configured, and the local server is running normally Off: the MODBUS service is off Delayed: an upload did not complete in time, for example because of network latency Other statuses: the MODBUS service has failed
Local Caching	Whether local caching is on or off	Running: local caching is on Off: local caching is off
Machine Connections - Connected	Number of machines connected successfully	0~255
Machine Connections - Offline	Number of machines offline	0~255
Machine Connections - Error	Number of machines with a connection error	0~255

For Cloud, MQTT, Database and MODBUS, the other statuses include “Initiated”, “Waiting for Connection” and “Error”. “Initiated” means the gateway has initialised the service but cannot proceed any further, because of a configuration error or a break in the network. “Waiting for Connection” means no reply has been received from the target server, which may indicate a network fault or a server fault. “Error” means a fault occurred at some stage.

3.2.2.1. Queue Backlog and Discarding It

When a service’s destination (the cloud platform, the MQTT server, the database and so on) is temporarily unreachable, the data waiting to be sent is queued on the gateway and sent once the connection comes back. Anything beyond the in-memory capacity is buffered on disk, so the backlog survives a gateway restart and is still sent afterwards.

Once a backlog reaches 100 items or more, the service's row in the "Data Pipeline" card shows the current backlog size. If the backlog is shrinking, the status reads "Recovering", meaning the connection is back and the data is being sent — no action is needed.

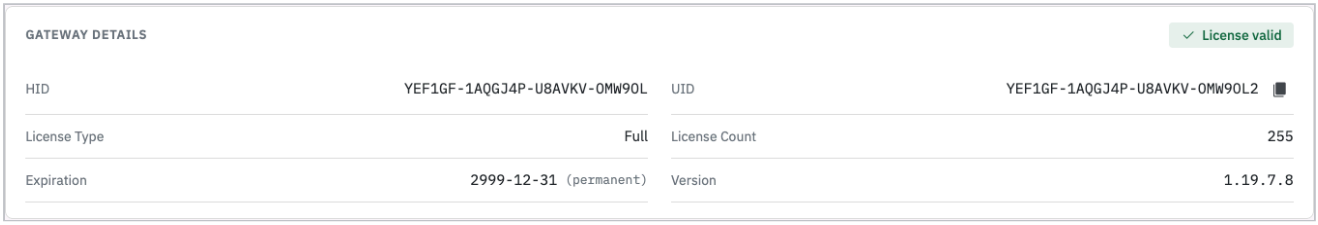
If the target server has been down for a long time (days, say), the backlog may no longer be worth sending, and sending it still costs disk space and bandwidth. In that case click the **Discard queued data** button on that row: after you confirm, everything that service has waiting to be sent, in memory and on disk, is **permanently discarded** and cannot be recovered, so use it with care. Discarding only affects the pending queue; it does not affect data acquisition from the machines or data already uploaded.

> **Caution**
>
> Discarded data cannot be recovered. If it still needs to be uploaded, restore the connection to the target server first and let the gateway send the backlog.

3.2.3. Gateway Details

The **UID** under "Gateway Details" is the device's unique identifier. You need to give it to support when you request help or upgrade your license.

- **Expiration** is the date on which the collection license expires.
- **License Count** is the number of collection licenses configured on the gateway, that is, how many machines the gateway may collect from at the same time.
- **License Type** is the type of collection license. Contact support to find out which features each type provides.
- **License Status** shows whether the current license is valid. "Invalid" means the license has not been assigned, or has expired.
- **Version** is the software version currently running on the gateway.



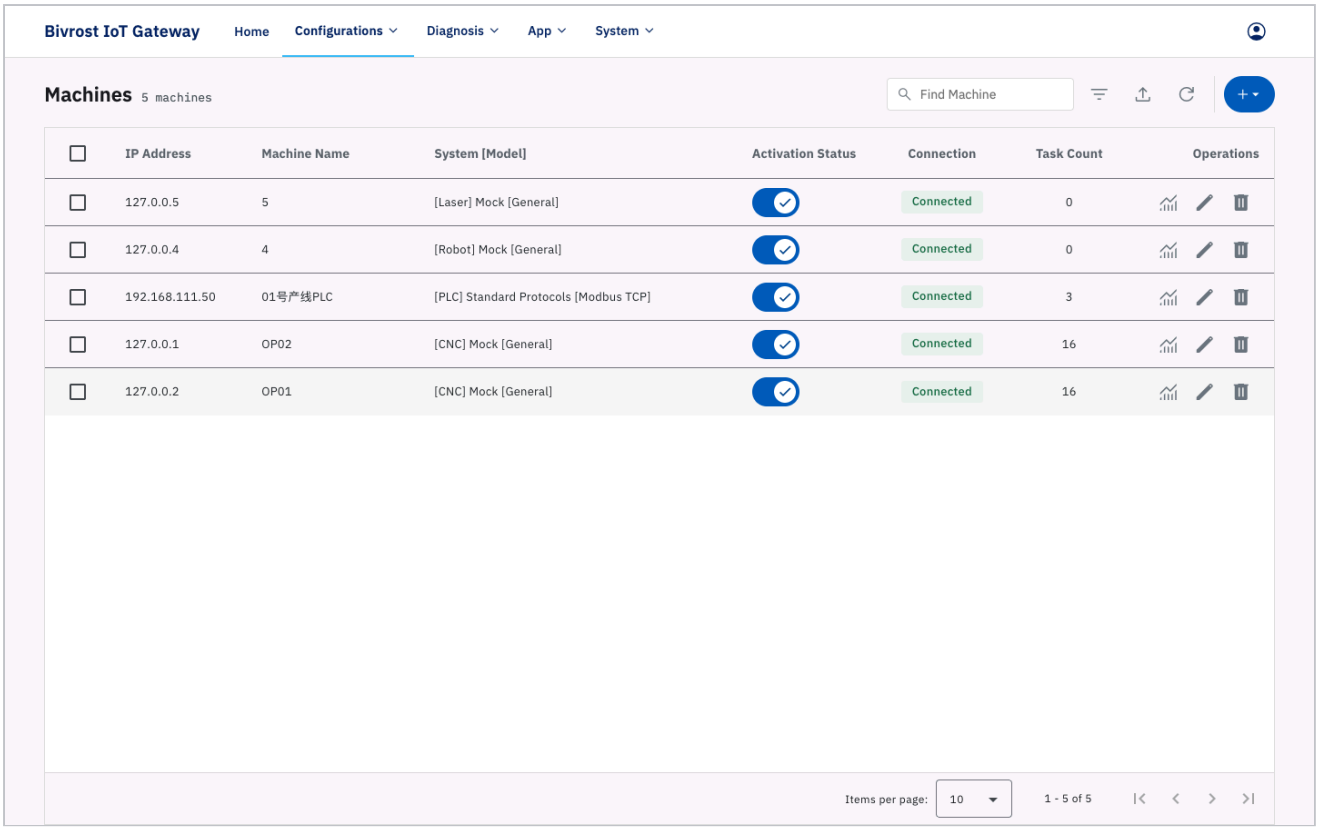
In the screenshot above, the gateway's license type is "Full". The available interfaces include Basic Data (Status, Count, Alarm, current program name, Current Program Block and so on), Axis Data (Position, Feed and Spindle, Load), Cycle Data, OEE Monitoring, PLC Data, tool offset read/write and DNC. The gateway can collect from up to 255 machines at the same time, and the

license expires on 31 December 2999. The current license status is valid. The gateway software version in the screenshot is 1.19.4.19.

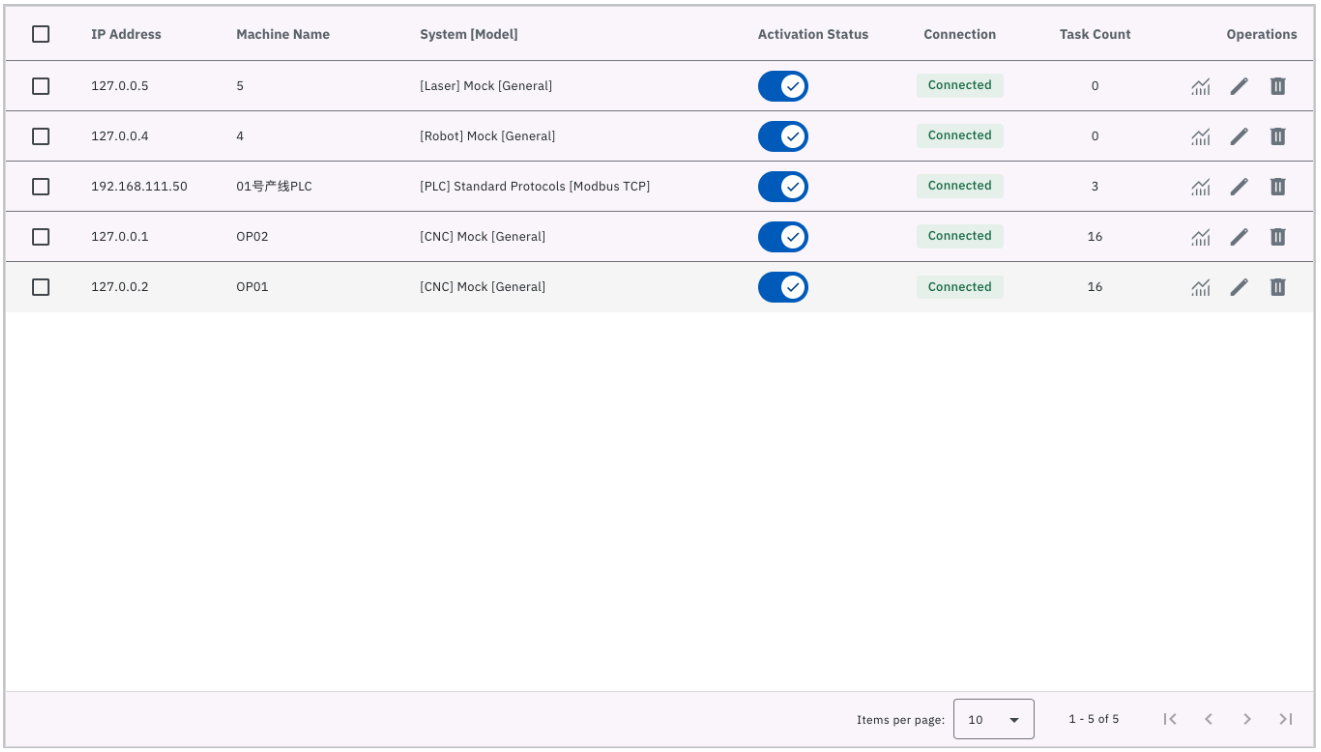
3.3. Machines

The **Machines** page is where you configure the machines you want to collect data from.

After changing anything on the **Machines** page, go back to Home and click **Restart Service** to apply the changes.



The table on this page lists the IP address, machine name, system model, connection status and task count of every configured machine. A green check in the **Connection** column means communication is working; any other icon indicates a problem. Hover over the icon to see an explanation, or refer to the table of common connection icons below. **Task Count** is the number of automatic collection tasks enabled for that machine.



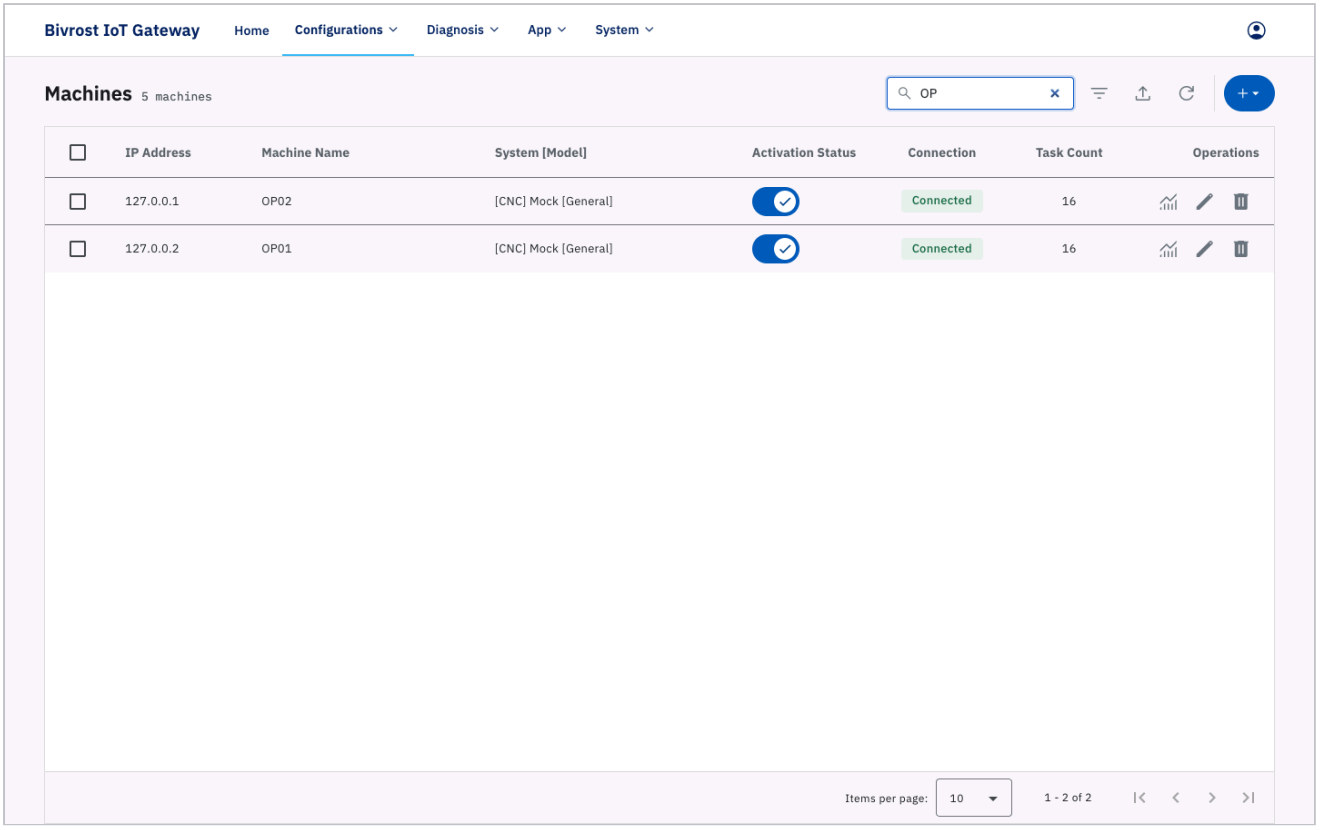
Common connection icons:

Icon	Meaning
✅ Green check	Communication successful.
🚫 Red no-entry	Unactivated. If activation fails in the create/edit machine dialog, the likely causes are: 1. the license type does not match the machine type; 2. the number of activated machines has reached the licensed maximum.
🔄 Yellow circle	Machine not loaded. Likely causes: 1. the gateway is waiting for the result of the first communication attempt after a service restart, which normally takes up to 10 seconds; 2. the machine was activated but the service has not been restarted.
🔗 Broken link	Machine offline. Likely causes: 1. the machine is powered off; 2. the network is not connected; 3. the machine configuration is wrong; 4. the network settings on the machine are incomplete.
❌ Red cross	Task not ready. Likely causes: 1. the machine configuration is wrong (for example the wrong system model); 2. the network settings on the machine are incomplete (wrong port setting, firewall not opened, and so on); 3. the machine’ s IP address conflicts with another device.

> **Note**
>
> The **Connection** column refreshes automatically every 10 seconds. After changing a machine's configuration, click **Restart Service** on Home. Following a **Restart Service** the gateway needs about 10 seconds to initialise its connections to the machines, so a "Not Loaded" status during that period is normal — wait about 10 seconds and the new connection status will appear on its own.

At the top right of the page are, from left to right, the **Find Machine** box and the **Filter**, **Batch Import**, **Refresh** and **Add Machine** buttons.

Type a keyword into the 🔍 **Find Machine** box and the matching machines appear below. The search covers IP address, machine name and system model. Clear the box to show all machines again.

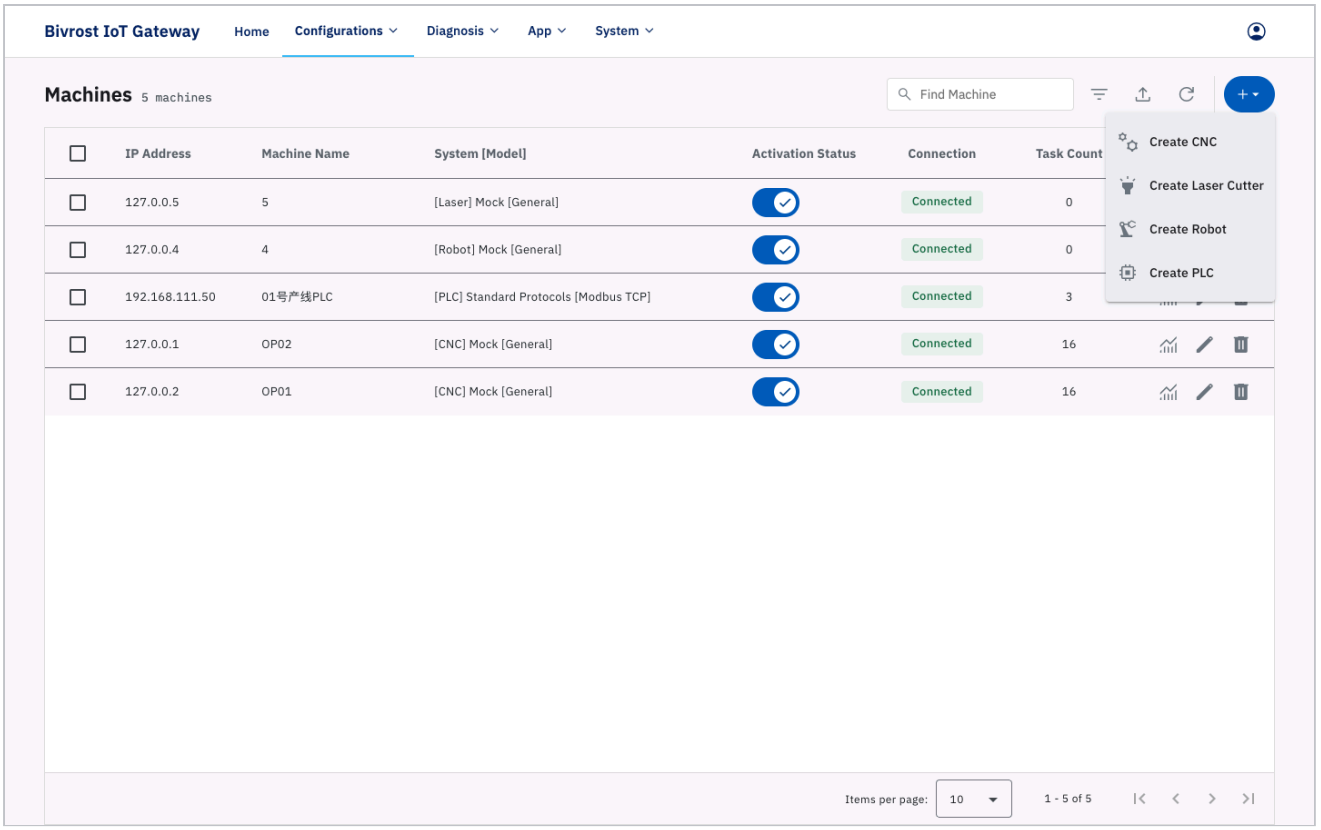


Click ↻ **Refresh** to reload the whole machine list.

Click + **Add Machine** to add a machine — see 3.3.1. Adding a Machine.

3.3.1. Adding a Machine

Click + **Add Machine** at the top right. The drop-down menu contains **Create CNC**, **Create Laser Cutter**, **Create Robot** and **Create PLC**.

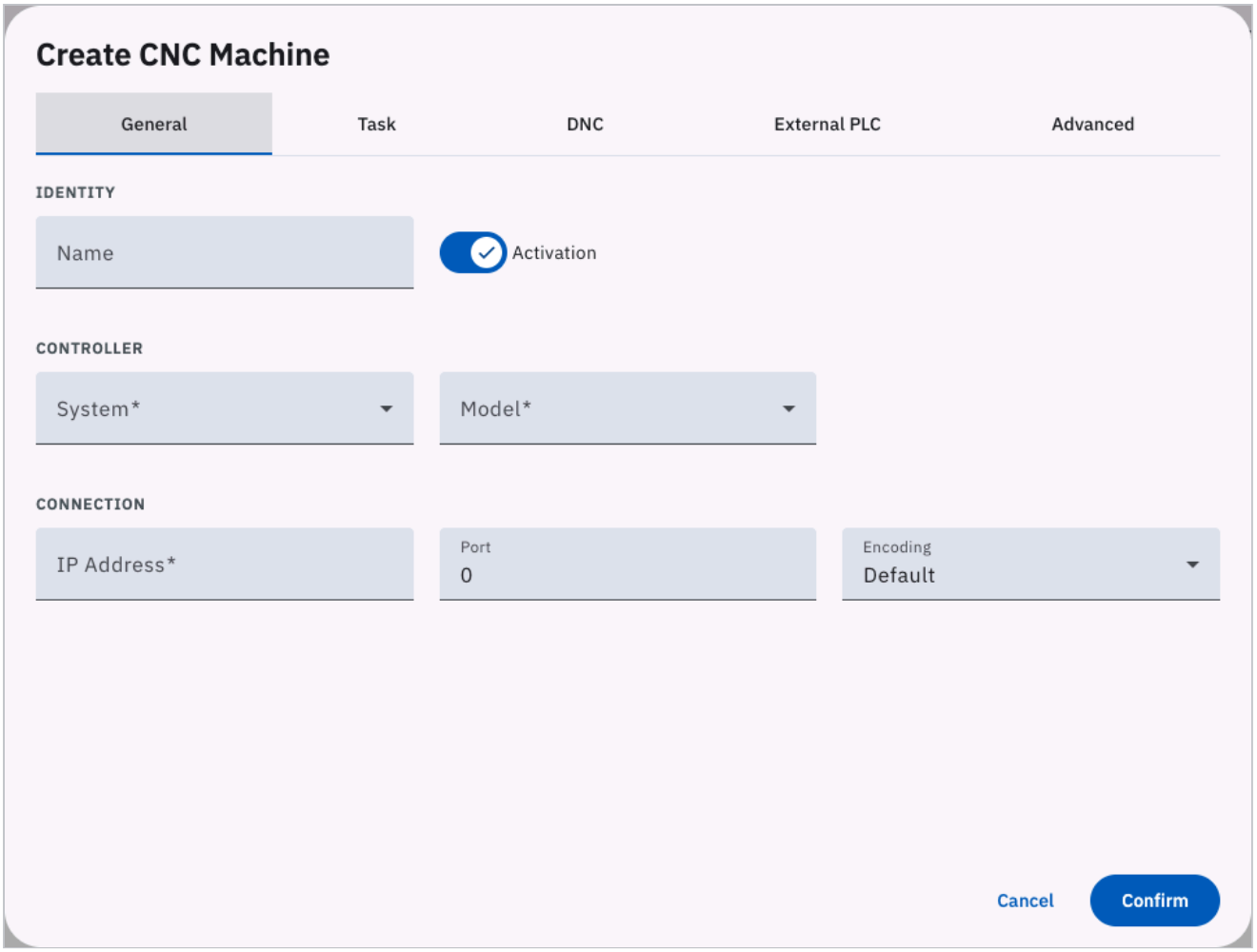


The dialogs for the different machine types are similar. The main differences are:

1. the tasks available on the Task tab differ by machine type;
2. robot and PLC machines have no DNC tab;
3. some machines have special settings (see the machine setup documentation, or contact support).

The example below adds a CNC machine:

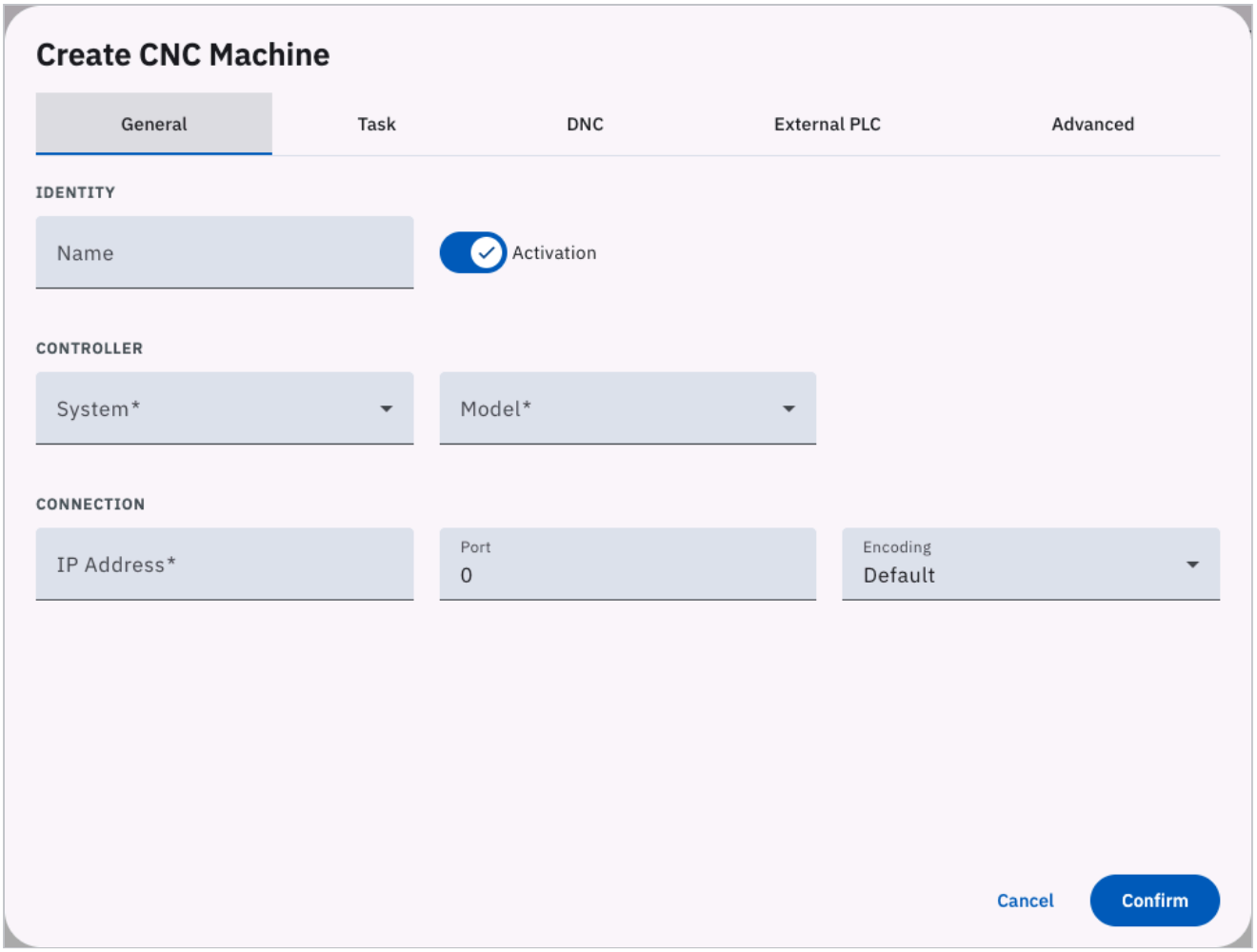
Click **Create CNC**. The “Create CNC Machine” dialog opens with the tabs “General”, “Task”, “DNC”, “External PLC” and “Advanced”. Fill in all of the tabs and click **Confirm** to add the machine. Anything you need to change afterwards can be edited in the “Edit CNC Machine” dialog (see 3.3.2. Editing a Machine).



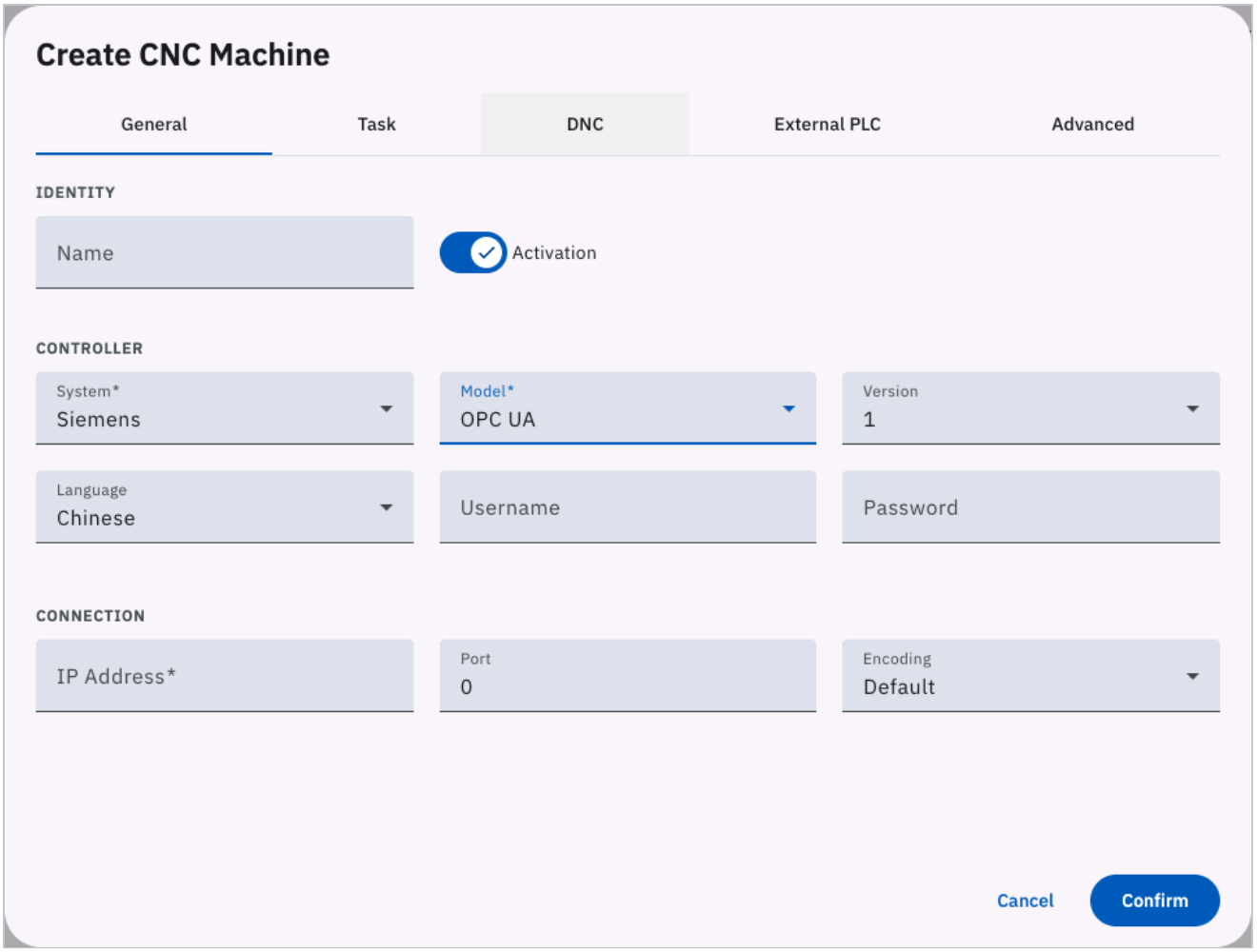
3.3.1.1. General Settings

The “General” tab holds the machine’s connection settings: choose “System” and “Model”, enter the machine’s IP address and machine name, and select an encoding. For the machine-side IP settings, see *Machine Setup*. If you choose Mock as the system, the IP address must be 127.0.0.X, where X is 1–255. Note that when “Activate” is selected in the dialog the machine is license-activated: it uses one collection license and collection is running. Clearing the checkbox withdraws the collection license used by that machine, pauses collection, and makes the withdrawn license available to another machine.

If the communication port on the machine is set to something other than the default listed in *Machine Setup*, set “Port” to the matching value; otherwise leave it at 0 to use the default port. The encoding option is used when parsing text (alarm text, String values in PLC data, file names, the contents of received files, and so on); the wrong encoding produces garbled text. The default is normally correct.

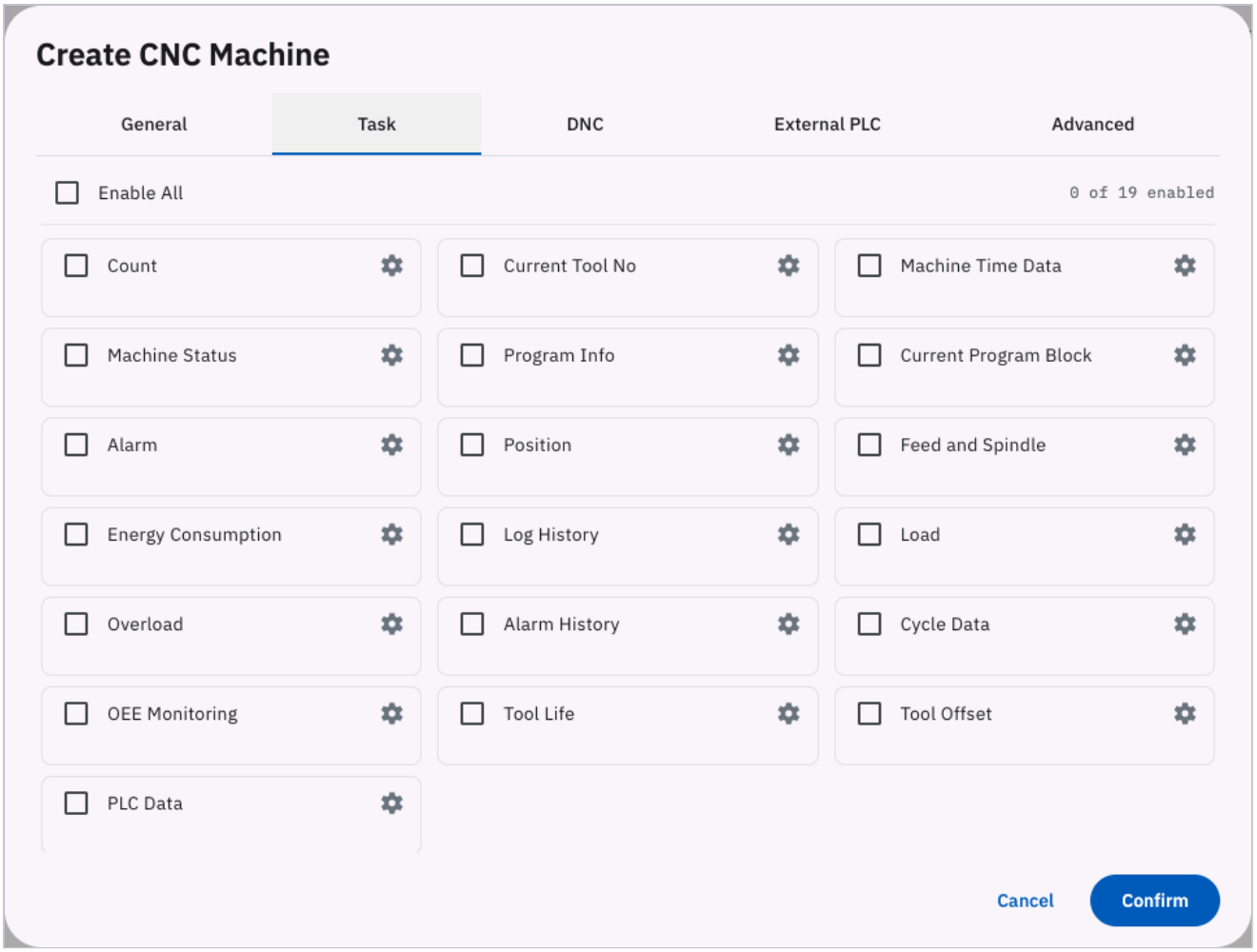


Some models and connection methods — such as Siemens machines that expose an OPC UA service — require the OPC username and password configured on the machine. The fields are hidden for models and connection methods that need no credentials.



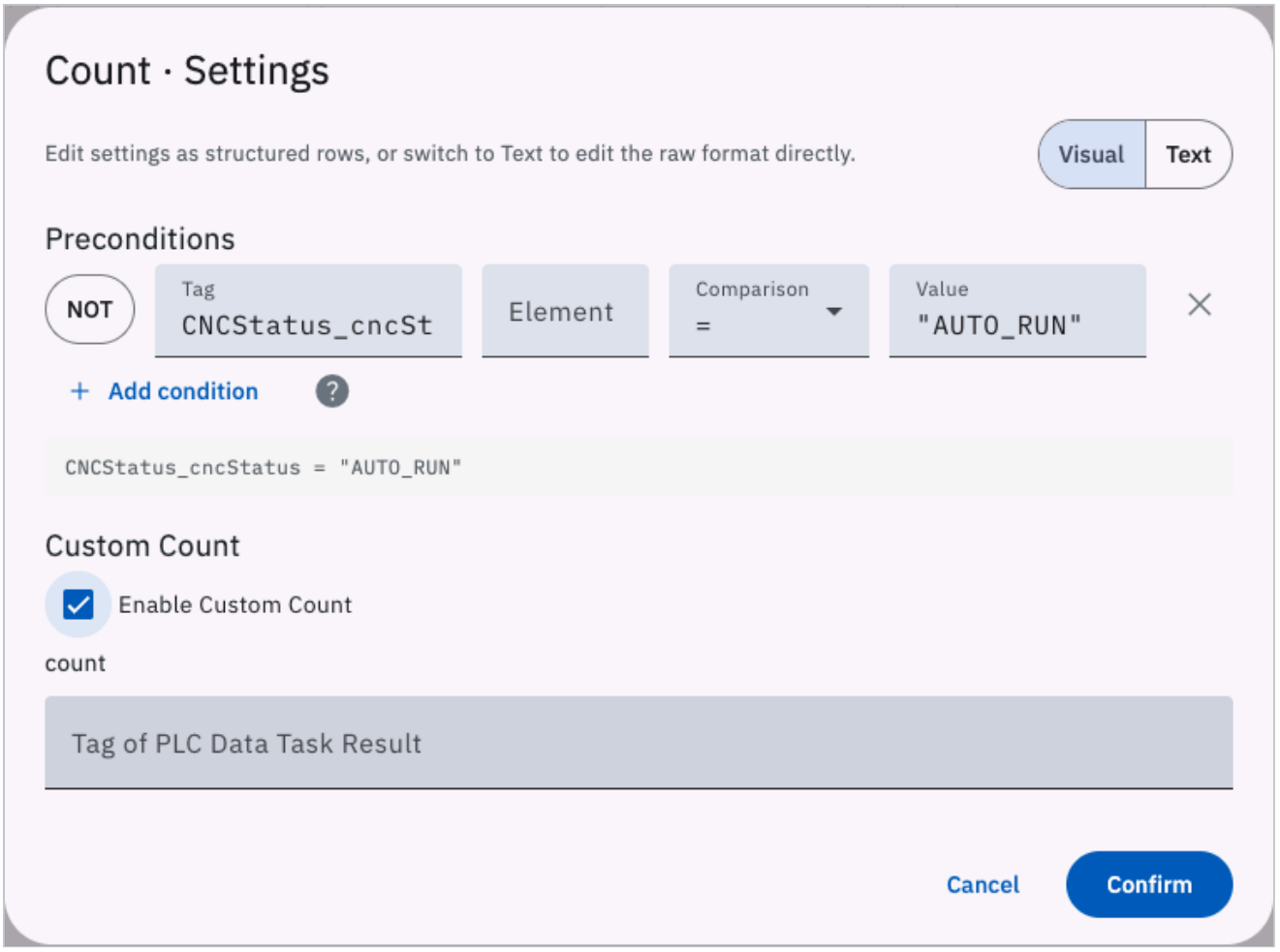
3.3.1.2. Task Settings

The “Task” tab configures the machine’s automatic collection tasks. Select an available interface to turn on automatic collection for the corresponding task. Interfaces not covered by your license are shown as “Unlicensed” and cannot be selected. The number of enabled tasks appears in the “Task Count” column of the **Machines** page.



This tab turns the machine' s automatic collection tasks on and off. Task results can be published through the cloud platform, MODBUS, MQTT or a database. To receive task results you must enable and configure at least one of the cloud, MODBUS, MQTT or database transports in 3.6. Communication. Collection intervals and detailed task settings are configured in 3.5. Tasks. For the format in which task results are published over MODBUS, MQTT and databases, see *Communication Protocol*. Collection through the HTTP interfaces does not require any machine task to be enabled.

The ⚙ button to the right of a task opens its advanced settings — Precondition, Target Channels, Target Tools, Custom Functions, Special Settings and so on.



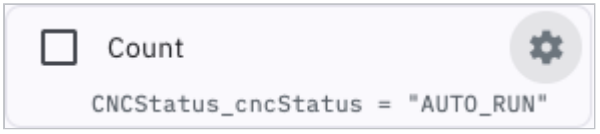
3.3.1.2.1. Precondition

When a precondition is set, the gateway evaluates it before each run of the task and only performs the collection if the condition is met. Left blank, the task has no precondition and always runs. For the precondition syntax, see 4.2.2. Precondition.

For example:

```
CNCStatus_cncStatus = "AUTO_RUN" and Load_spindleLoad[0] > 50
```

Tasks that have a precondition are marked with a blue branch icon to the right of the task name.



3.3.1.2.2. Target Channels

Some machines expose data for several channels — for example channel 1 for the main spindle and channel 2 for the sub-spindle. The default target channel is 0, which collects data from the

main channel only. To collect data from several channels, list them under target channels. The tasks that support this setting include Current Tool No, Machine Status, Program Info, Current Program Block, Position, Feed and Spindle, Load, Overload and Cutter comp.

For example: `0;1-3`

3.3.1.2.3. Target Tools

The Tool Life and Cutter comp tasks require target tools to be entered in the dialog behind the ⚙ button next to the task. How tools are specified depends on the machine's control system; by default no tools are specified. Follow the example in the hint text, or see *Communication Protocol*, 2.5.1.12. readOffsetData (Read Offset Data) and 2.5.1.21. readToolLife (Read Tool Life).

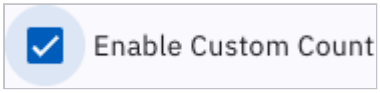
On a Siemens control, for instance, a tool is defined by a tool number (Tool) and an offset number (Offset):

```
1.2;3-5.1;7-9.1-3
```

- `1.2` means tool 1, offset 2;
- `3-5.1` means tool 3 offset 1, tool 4 offset 1 and tool 5 offset 1;
- `7-9.1-3` means tools 7, 8 and 9, offsets 1, 2 and 3 on each of them.

3.3.1.2.4. Custom Functions

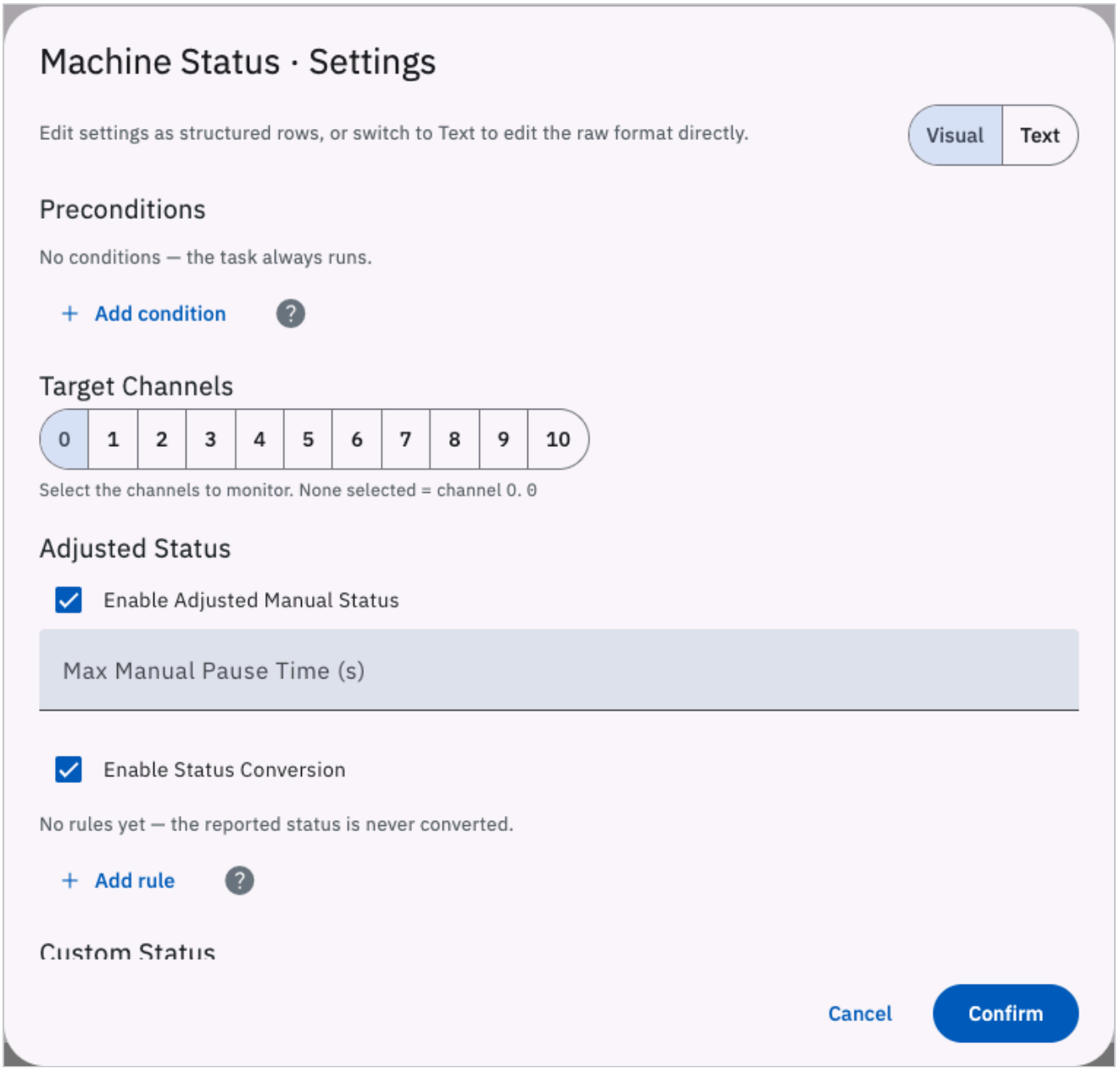
The Count, Machine Status and Alarm tasks support custom functions, which substitute the result of a PLC task for the data returned by the native interface. Custom functions are mainly used on controls where a customised module replaces the native one, or where the control does not support the required communication and the manufacturer supplies an address list so the data can be read from PLC addresses instead.



> **Caution**
>
> The data type of the PLC data task result must be compatible with the data type of the native interface. The `count` field of the Count task, for example, is Int32, so the data behind the tag you enter must be convertible to Int32. If the raw count in the PLC is a string, use the post-processing feature of the PLC data task to convert it to Int32 and enter the tag of the processed value. For an example of the PLC task settings behind a custom status, see example 4 in 4.2.4.2. $POST$ Post-processing.

3.3.1.2.5. Special Settings

The Machine Status task supports adjusted status settings: you can enable manual-status adjustment and status conversion, both off by default. These are the same settings as the ones with the same names in 3.5.8. Machine Status Monitoring Settings; those are global, and enabling them here overrides the global settings for this machine.



With **Enable Adjusted Manual Status** or **Enable Status Conversion** turned on, the status is adjusted according to the corresponding rules and published as `adjustedStatus` (*Communication Protocol*, 1.2.4. CNCStatus: Machine Status). Calculations that involve machine status — OEE, cumulative status time and so on — use the adjusted status in preference to the raw one. With both options off, `adjustedStatus` is identical to the real-time status reported by the machine.

The rules for manual-status adjustment are:

1. the machine is currently in the Manual state;
2. the time since the machine went from a non-Manual state to Manual exceeds the configured Max Manual Pause Time;
3. the machine’s position data has stayed unchanged for longer than the configured Max Manual Pause Time.

Normally `adjustedStatus` matches the machine’s real-time status; when all of the conditions above are met at once, `adjustedStatus` is no longer Manual but is adjusted to Wait.

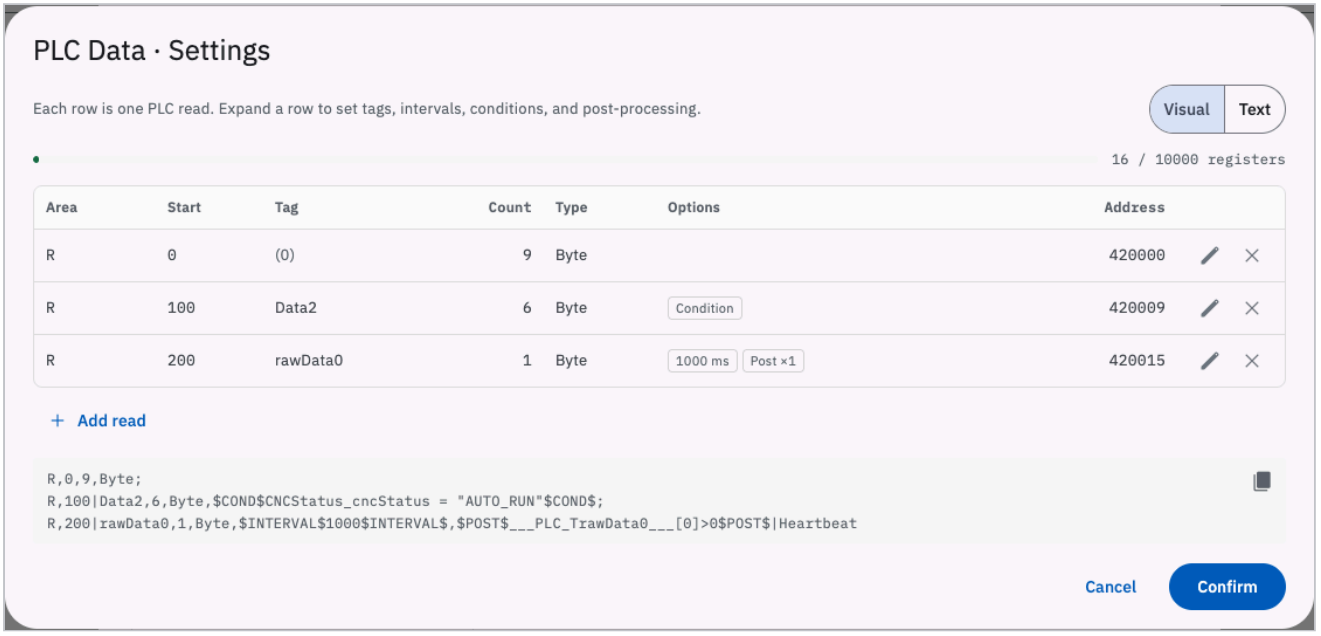
With status conversion enabled, `adjustedStatus` is set according to the commands you enter, for example:

```
CNCStatus_cncStatus = "MANUAL_MDI_RUN" | AUTO_RUN
```

`CNCStatus_cncStatus = "MANUAL_MDI_RUN"` is the precondition (see 4.2.2. Precondition): if the `cncStatus` value (the running status, of type String) returned by this machine’s Machine Status task is “MANUAL_MDI_RUN”, then `adjustedStatus` is set to AUTO_RUN. Separate multiple conversion commands with “;”.

When both options are enabled, manual-status adjustment runs first and status conversion second.

The PLC Data task requires the commands for the target PLC data to be entered in the dialog behind the ⚙ button next to the task — see 4.2.1. PLC Data Task.

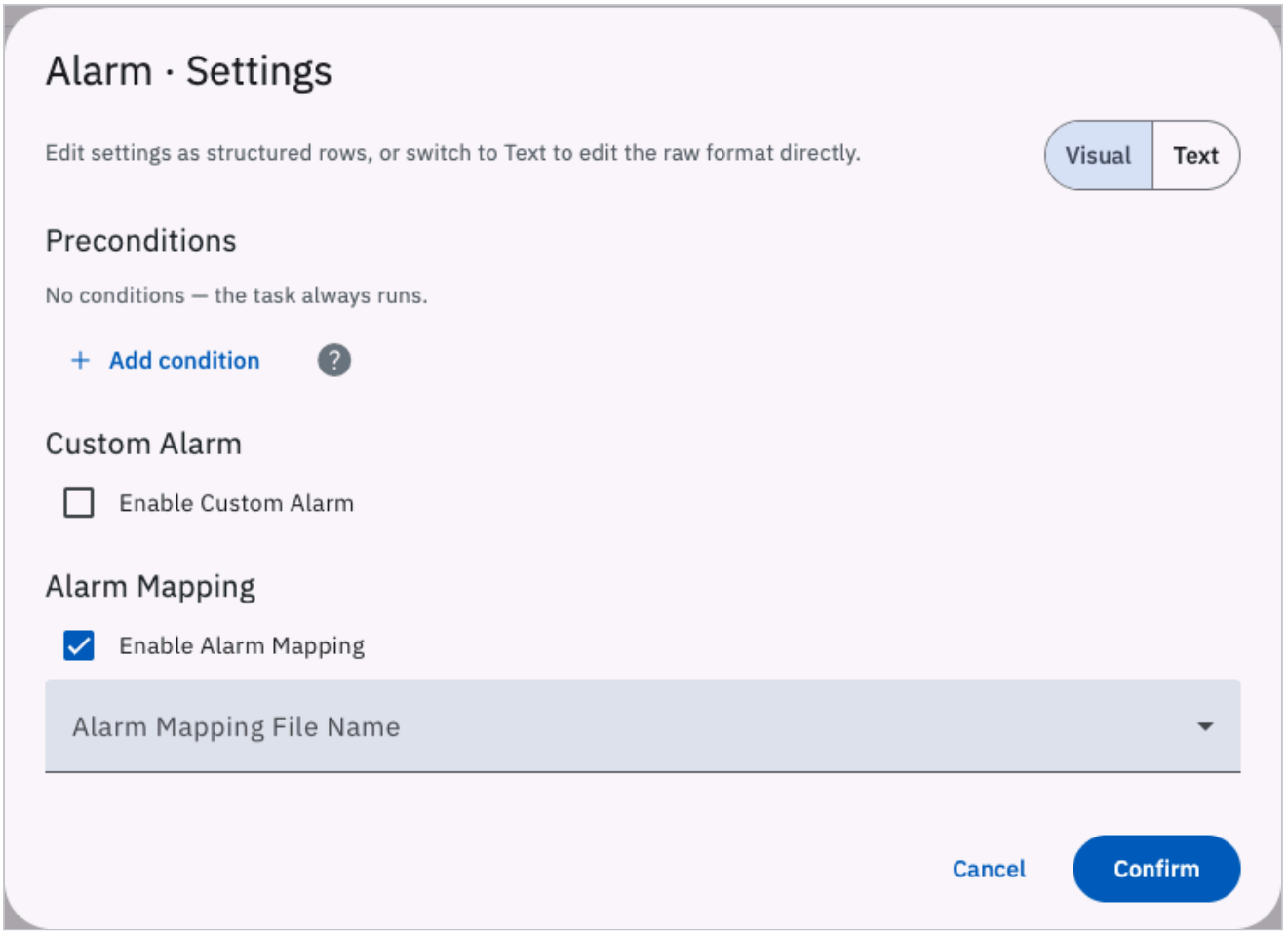


If MODBUS communication is enabled (3.6.2. MODBUS Settings), the reserved MODBUS address space limits a single machine’ s PLC data tasks (including external PLC data) to 10000 address registers after conversion — see *Communication Protocol*, 3.1. Machine-related Data.

3.3.1.2.6. Alarm Mapping

The Alarm task supports alarm mapping, which replaces the alarm numbers reported by the machine with your own alarm text. It suits machines that report only an alarm number and no alarm text, or installations where alarm descriptions need to be standardised.

In the dialog behind the ⚙ button next to the Alarm task, select “Enable Alarm Mapping” and then pick an uploaded mapping file from the “Alarm Mapping File Name” drop-down.



Mapping files are uploaded and managed in 3.5.7.1. Alarm Mapping Files; a file must be uploaded there before it can be selected here. After enabling it, click **Confirm** to save, then go to Home and click **Restart Service** to apply the change.

3.3.1.2.7. Additional Notes

Machine OEE data covers Off Time, Wait Time, Emergency Time, Autorun Time, Manual Time and machine Availability — see 4.1.1. Machine OEE Data. OEE data depends on local caching, so

the “Local Caching” switch under Options in 3.12. Settings must be turned on.

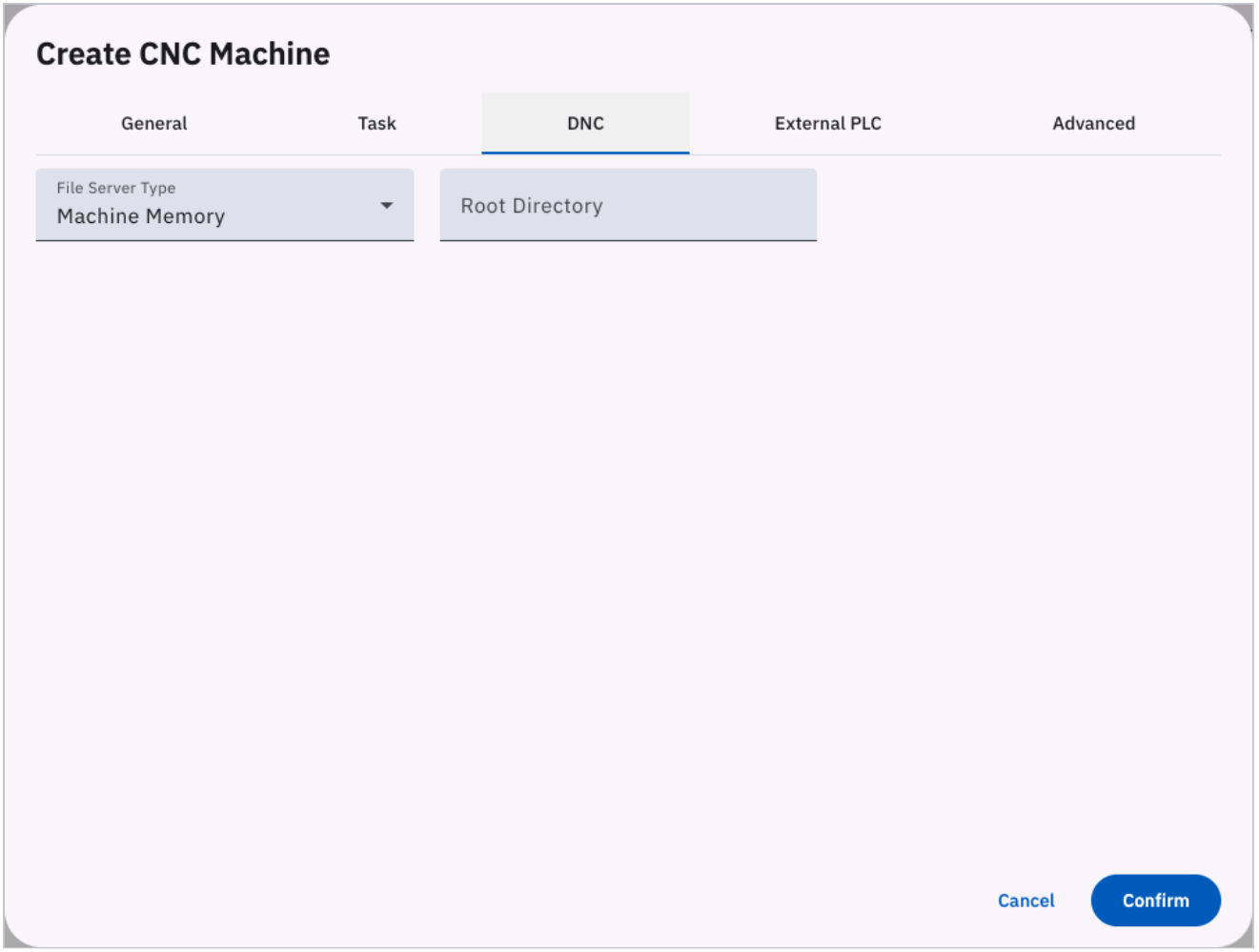
Write Offset Data and DNC are not available as machine tasks; they must be called through the HTTP interfaces or the MQTT RPC interfaces — see *Communication Protocol*.

Cumulative Status Time is the total time spent in each status since the gateway started collecting from the machine, in seconds. The value is stored on the gateway, bound to the machine ID (MachineID), and is never reset.

Cycle Data gives the duration of the last cycle; the gateway derives it from Machine Status, Count and Program Info.

3.3.1.3. DNC Settings

The “DNC” tab sets the file transfer method and target location.

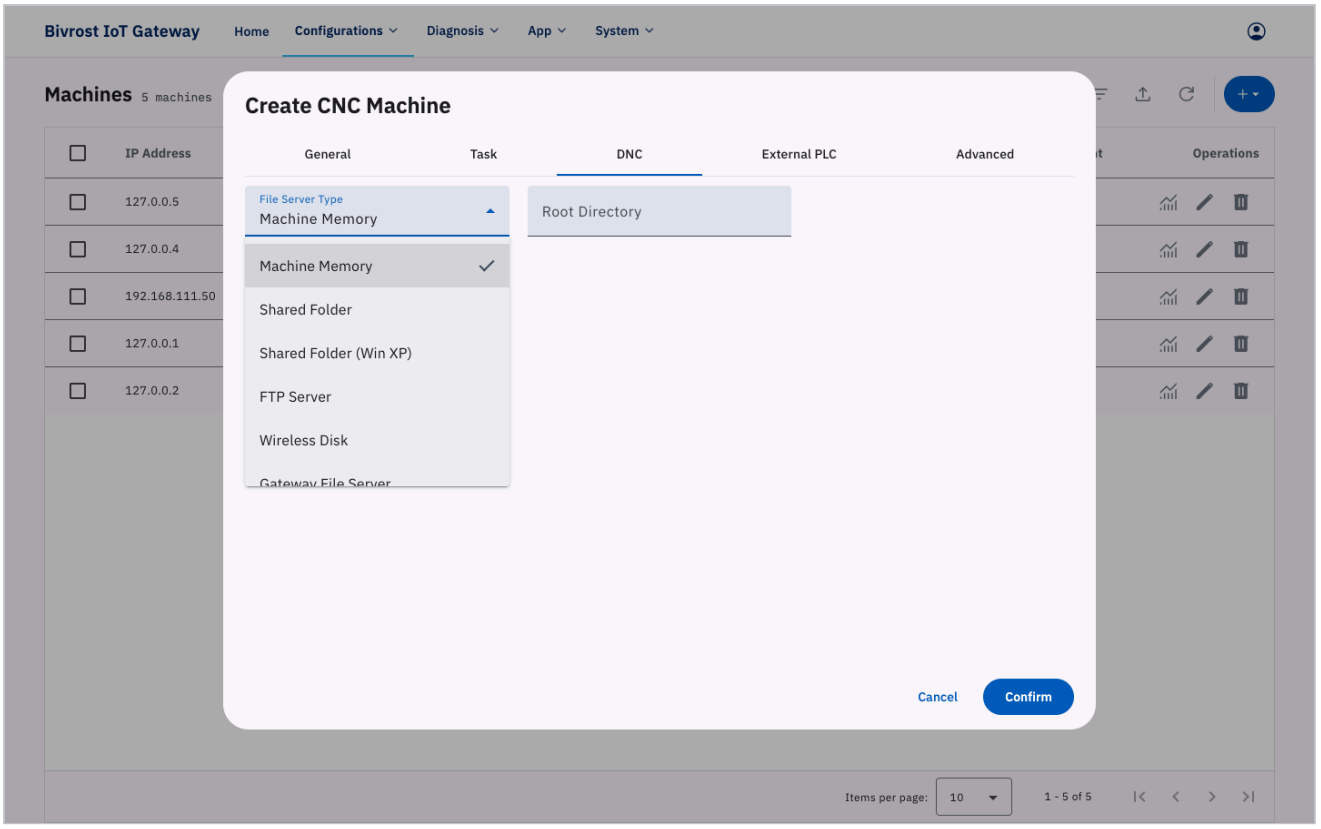


The “File Server Type” options are:

- **Machine Memory** (default), the machine’s built-in storage, including a CF card plugged into the machine (supported on some machines; the root directory must point at the CF

card path);

- **Shared Folder** and **Shared Folder (Win XP)**, which transfer files through a shared folder;
- **FTP Server**, which transfers files over FTP;
- **Wireless Disk**, an external storage device attached to the machine that connects to the gateway over WiFi and to the machine over USB or RS232;
- **Gateway File Server**, a file server hosted on the gateway itself that the machine can reach over FTP or a shared folder — see 3.6.5. Gateway File Server Settings.



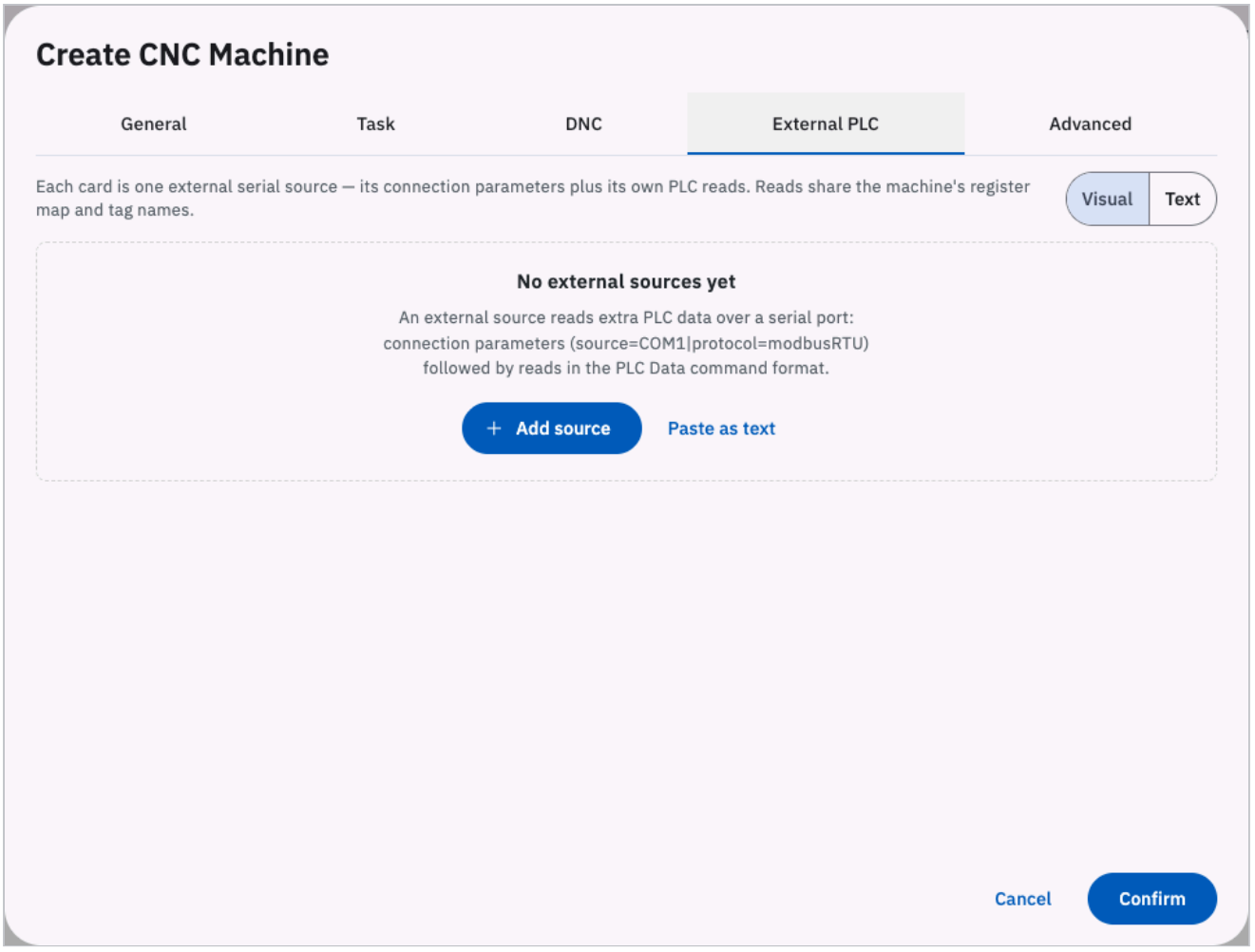
If the machine’s own storage is too small, or the machine does not support transferring programs directly to its internal storage, use the “Gateway File Server” instead. You can also attach file server hardware to the machine and transfer programs through “Shared Folder”, “FTP Server” or “Wireless Disk”.

If the root directory is left blank, the machine’s default path is used. The default path differs by machine model — see *Communication Protocol*, 2.6. File Management Interfaces.

3.3.1.4. External PLC Settings

The “External PLC” tab lets you add commands that collect data from an external PLC attached to equipment around the machine — see 4.2.5. External PLC Data Task. Once a valid external PLC data task has been added, collection starts automatically after a service restart.

The collection interval for external PLC data tasks, and the way their results are retrieved, are the same as for PLC data tasks.

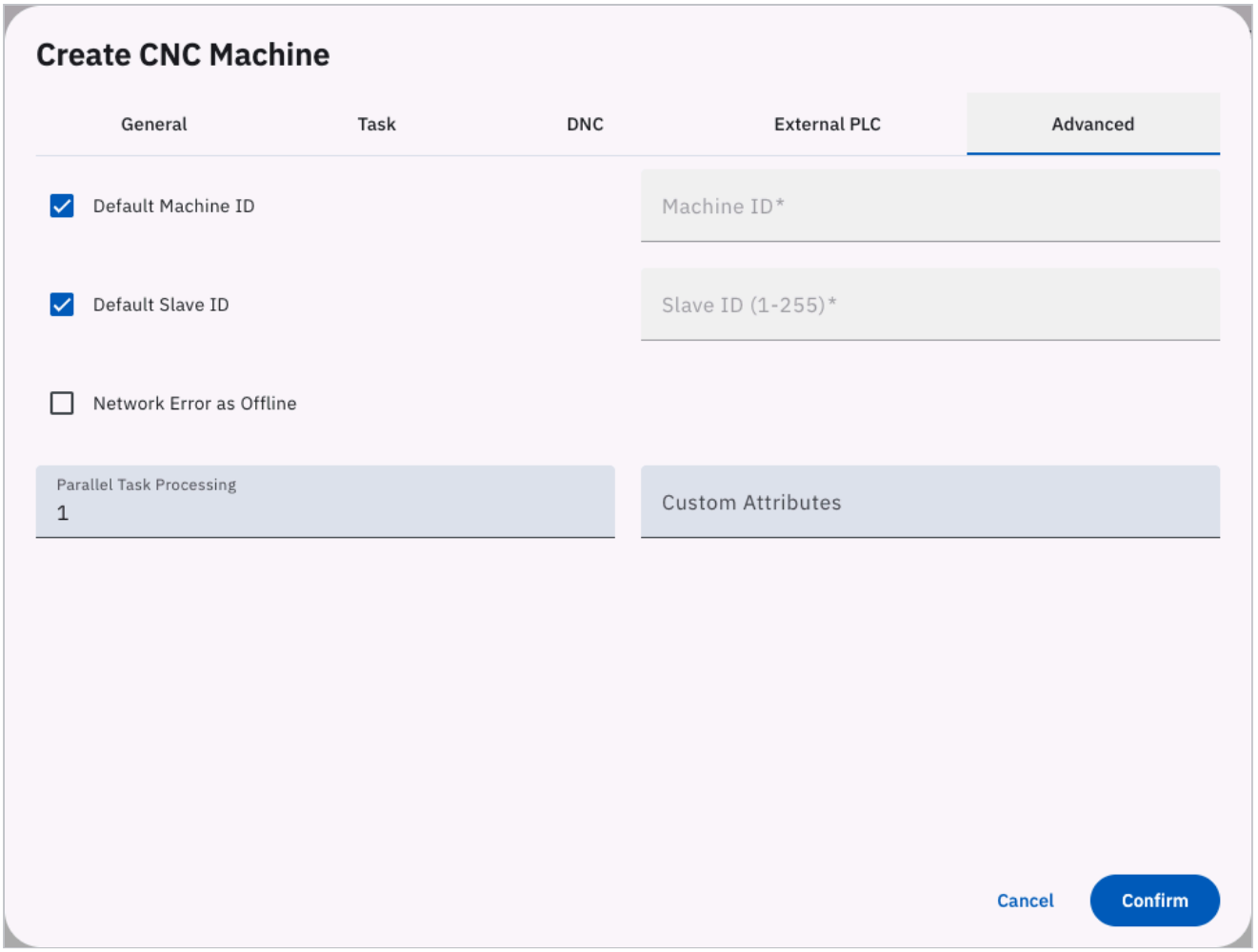


For example:

```
source=COM1|protocol=modbusRTU;4x,0,1,Int16;4x,10,2,Int32
```

3.3.1.5. Advanced Settings

The “Advanced” tab lets you customise the machine ID (MachineID), the slave ID (SlaveID), Network Error as Offline, Parallel Task Processing, and custom attributes.



Machine ID identifies the machine's data on every transport except Modbus. The default machine ID is formed by joining the third and fourth octets of the machine's IP address and stripping the leading zeros. If the third octet is not 0, the fourth octet is padded to three digits. For example, 192.168.0.1 gives a default machine ID of 1, and 192.168.1.12 gives 1012.

Slave ID identifies the machine's data on Modbus. The default slave ID is the fourth octet of the machine's IP address; 192.168.1.12 gives a default slave ID of 12.

Network Error as Offline is off by default. When it is on and the machine fails to connect for network reasons on the first attempt (previously reported as "Network Error"), the gateway treats the machine as offline instead of reporting a connection error. This suits machines that are powered down or lose network connectivity from time to time, where all such unreachable states should be treated uniformly as offline.

Parallel Task Processing is the number of task managers — that is, threads — allocated to the machine. The default is 1. Raising it consumes more system resources, so only raise it when the machine has a large number of tasks with very short intervals and the default setting cannot keep collection up to date. Some control systems do not support multi-threaded connections and must be left at 1. Note that the sum of the Parallel Task Processing values of all activated

machines should be less than the maximum number of task managers (see 3.5.9. Task Manager Settings).

Custom Attributes add user-defined attribute tags to the task data returned by the gateway. The format is:

```
{"attribute":value,…}
```

Example:

```
{"Custom ID":1, "Custom String": "abc123 string"}
```

In the task data, custom attributes are added after the `<entityID>` attribute (MachineID, in the case of a machine).

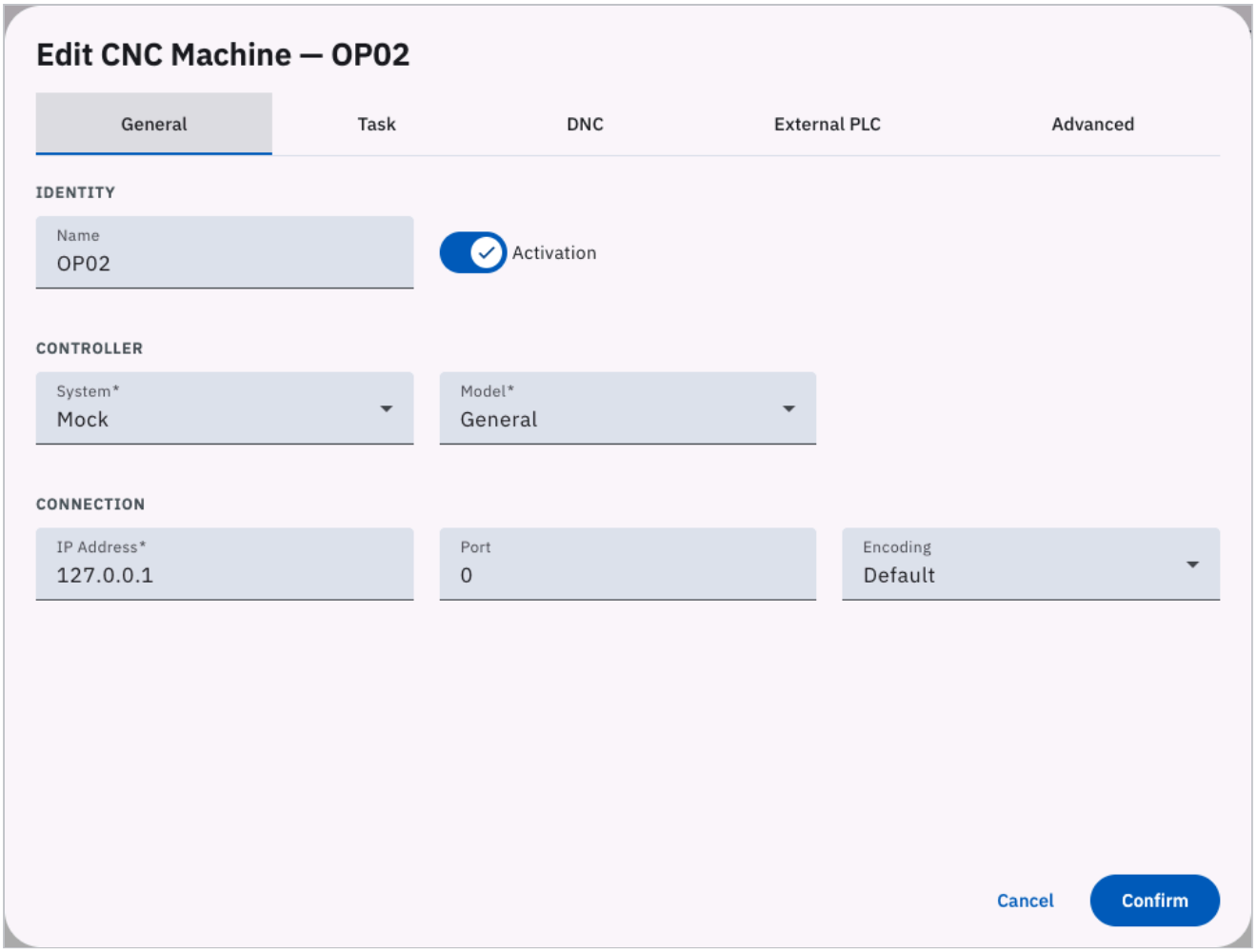
3.3.1.6. Connection Status

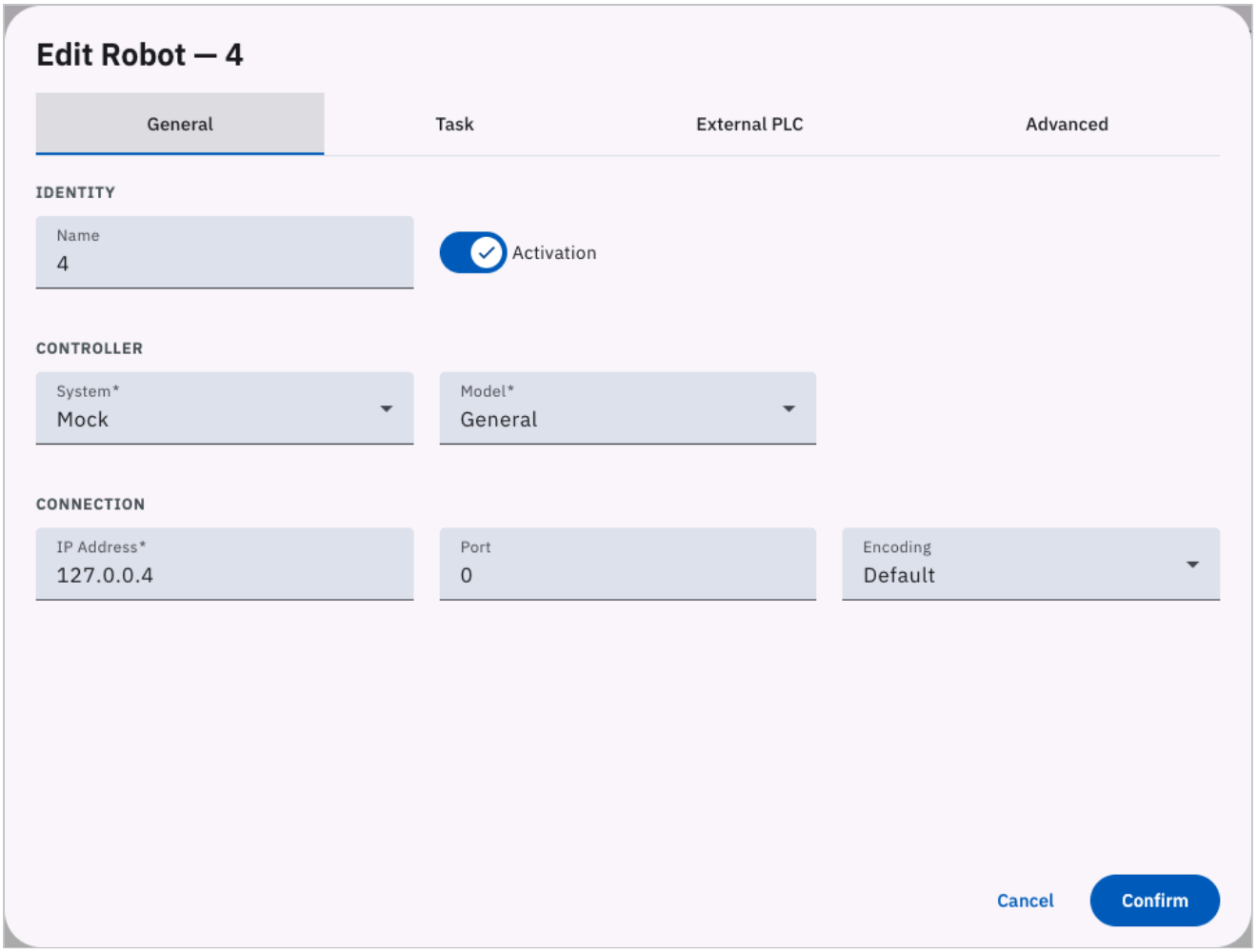
Once everything in the create machine dialog is set, click **Confirm** to save. The new machine appears on the **Machines** page. Note that its "Connection" icon is a yellow circle at this point, meaning the machine is not loaded; go to Home and click **Restart Service** to load the newly configured machine.

After the **Restart Service**, the Connection icon turns into a green check, meaning communication is working. Any other icon means the configuration is wrong or there is a fault in the machine, the gateway or the network — hover over the icon for an explanation, or refer to the table of common connection icons in 3.3. Machines.

3.3.2. Editing a Machine

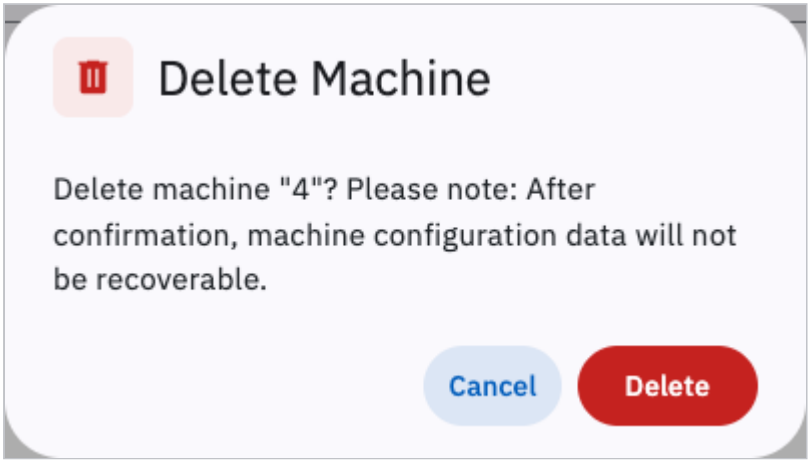
Click the edit button ✏️ in the "Operations" column at the right of a row in the machine list. The "Edit CNC Machine" / "Edit Laser Cutter" / "Edit Robot" / "Edit PLC Machine" dialog opens; it is similar to the corresponding "Create CNC Machine" / "Create Laser Cutter" / "Create Robot" / "Create PLC Machine" dialog. For a description of each tab, see 3.3.1. Adding a Machine. The machine type — CNC, laser cutter, robot or PLC — cannot be changed in the edit dialog.


Edit CNC Machine — OP02
General
Task
DNC
External PLC
Advanced
IDENTITY
Name
OP02
Activation
CONTROLLER
System*
Mock
Model*
General
CONNECTION
IP Address*
127.0.0.1
Port
0
Encoding
Default
Cancel
Confirm



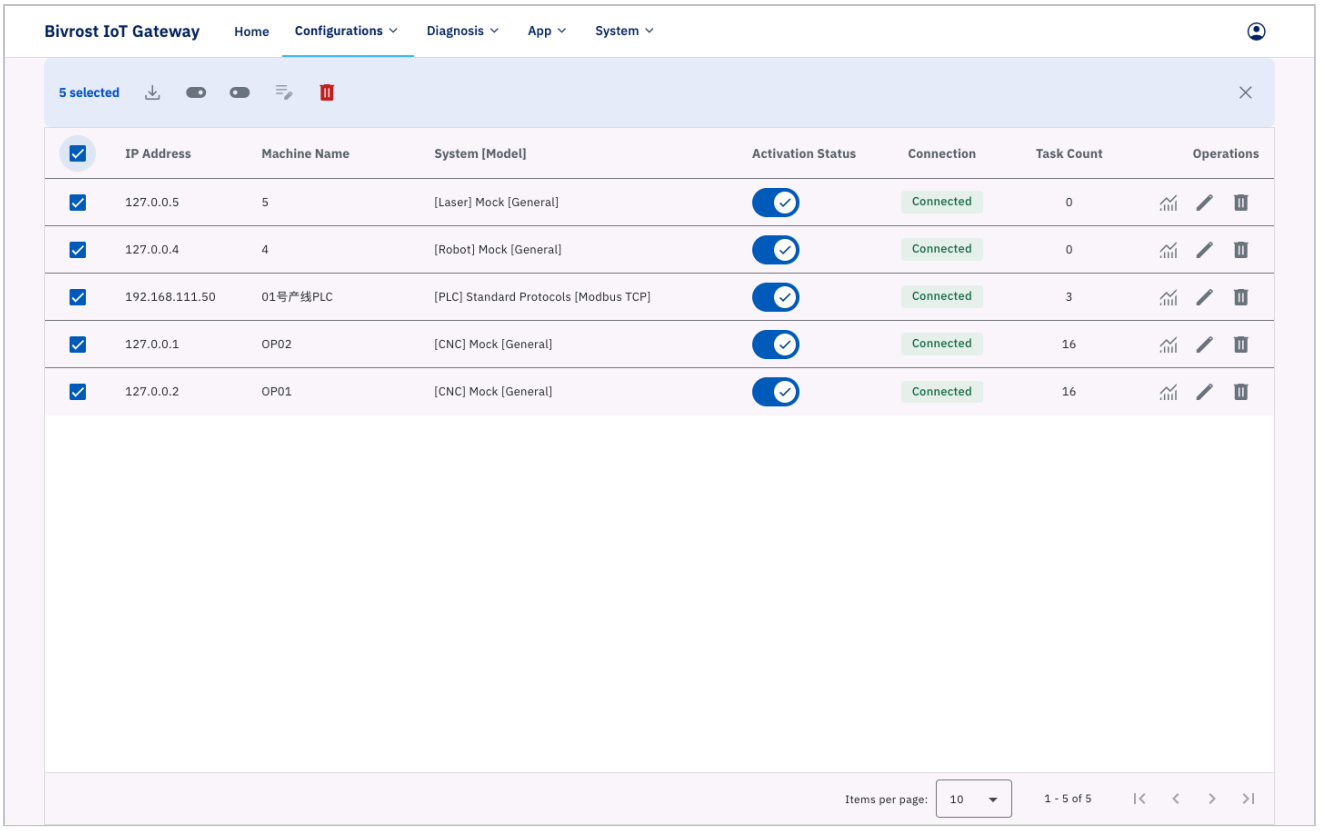
3.3.3. Deleting a Machine

Click the delete button 🗑️ in the “Operations” column at the right of a row in the machine list. The “Delete Machine” dialog appears; click **Confirm** to delete the machine permanently.



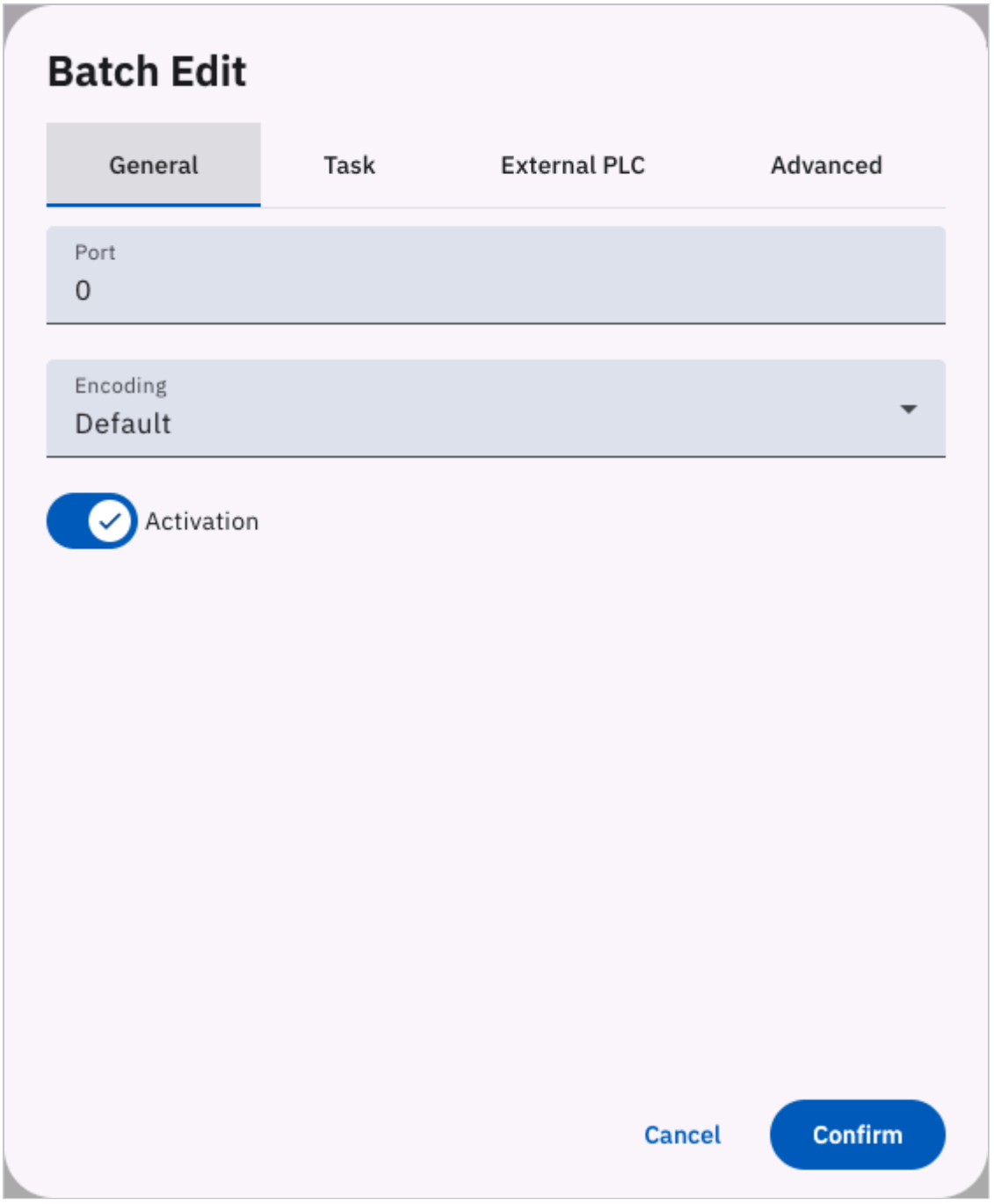
3.3.4. Batch Activation

Select several machines using the checkboxes at the far left of the list, or the select-all button at the top left of the list.



The batch buttons — Batch Activation, Batch Edit and Batch Delete — then appear at the top right.

Click Batch Activation, choose whether to activate, and click Confirm to set the selected machines to activated or unactivated.



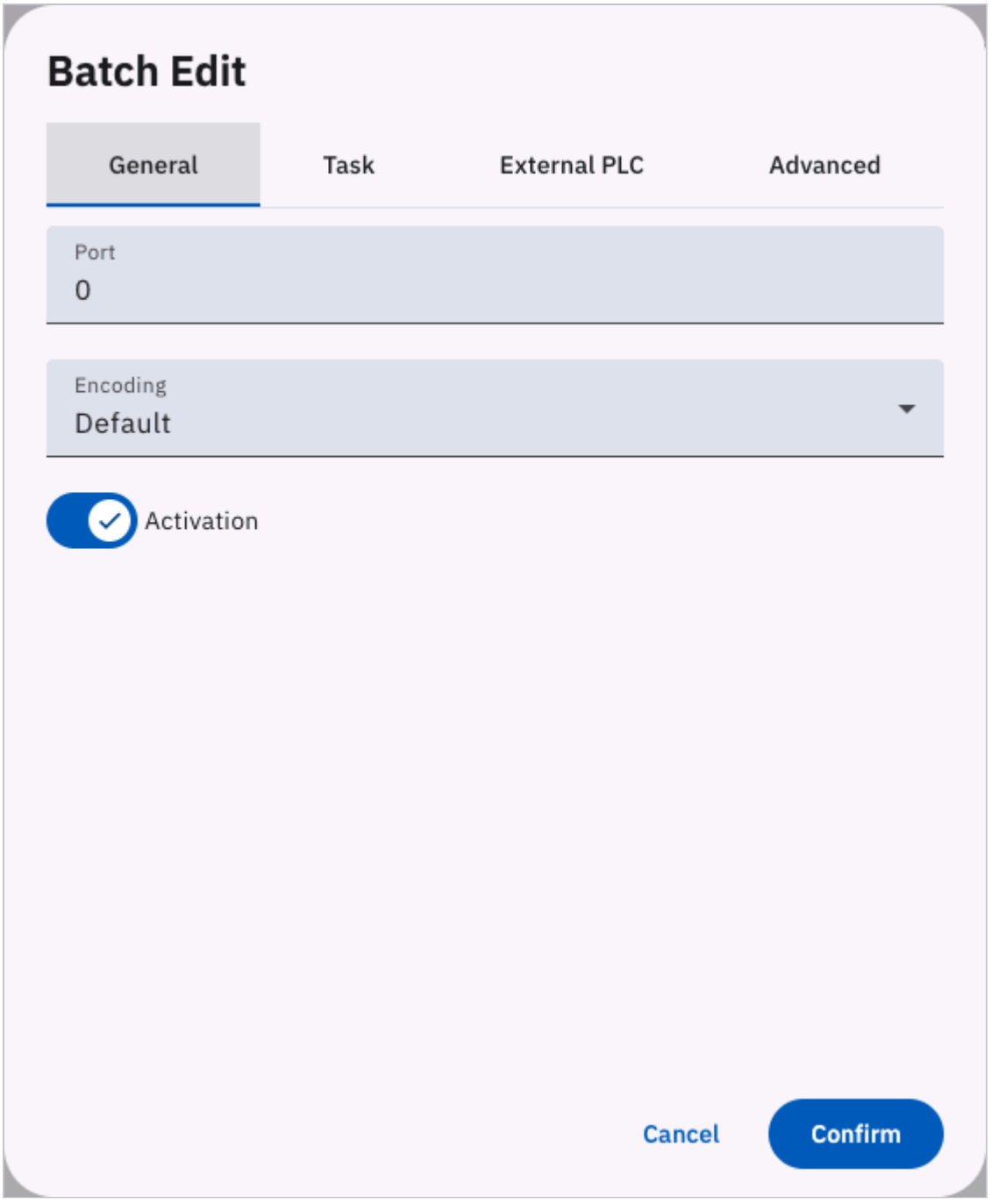
3.3.5. Batch Edit

Select several machines using the checkboxes at the far left of the list, or the select-all button at the top left of the list. Note that they must all have the same system and model.

Click Batch Edit at the top right, set the shared options in the Batch Edit dialog, and click Confirm to save.

Note

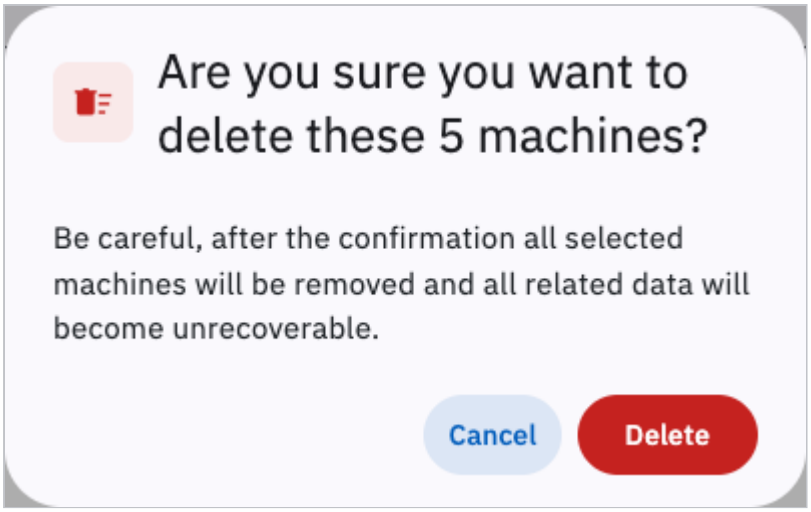
Batch Edit covers shared options only. Options that are specific to a single machine — machine ID, slave ID, machine name, DNC directory, custom attributes and so on — must be edited machine by machine. On every tab of the Batch Edit dialog, options you do not set are initialised to their default values rather than keeping each machine's individual settings.



3.3.6. Batch Delete

Select several machines using the checkboxes at the far left of the list, or the select-all button at the top left of the list.

Click Batch Delete at the top right and click Confirm in the confirmation dialog to delete the selected machines.

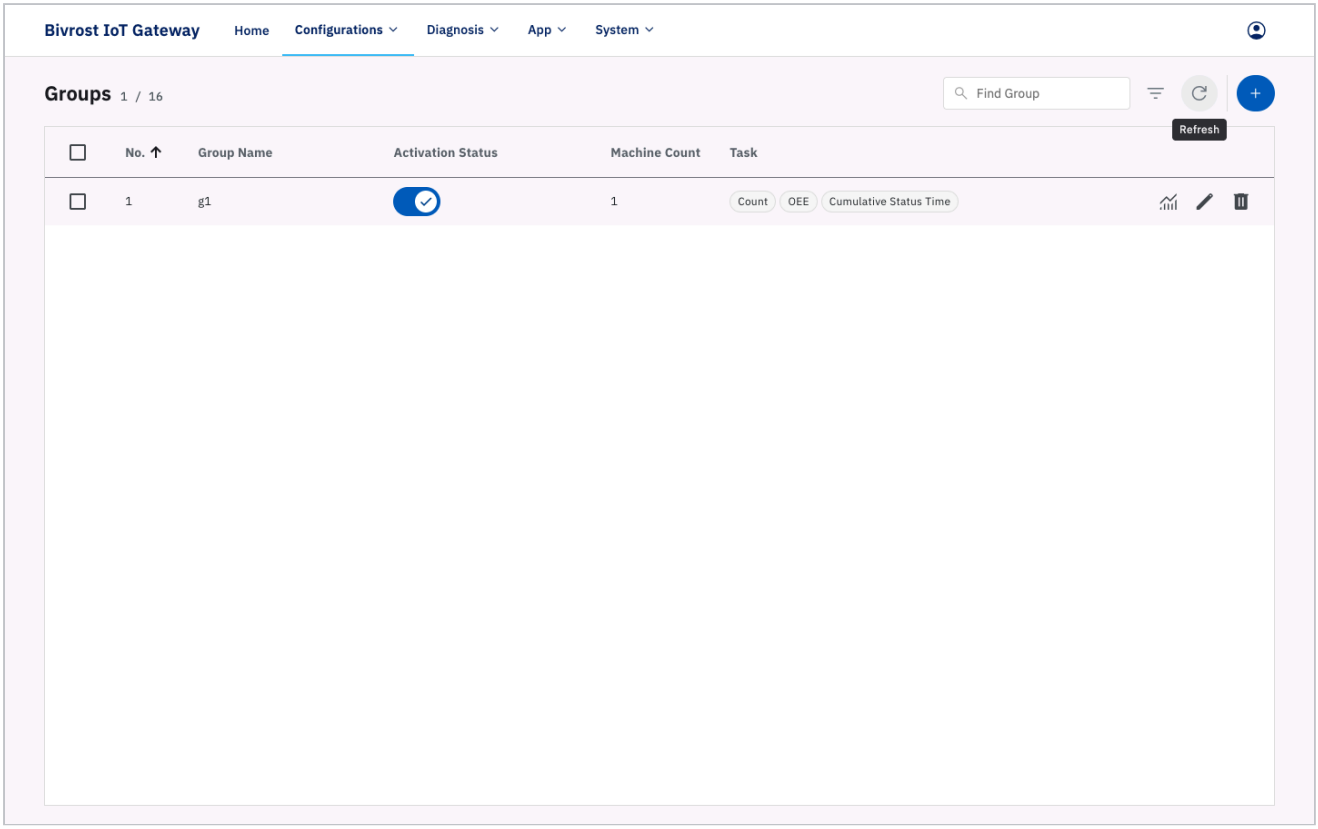


3.4. Groups

On the **Groups** page you can combine the machines defined on the **Machines** page into groups. The gateway then uses the data collected from each machine to calculate group-level statistics and uploads them as a package.

After changing anything on the **Groups** page, return to the home page and click **Restart Service** for the changes to take effect.

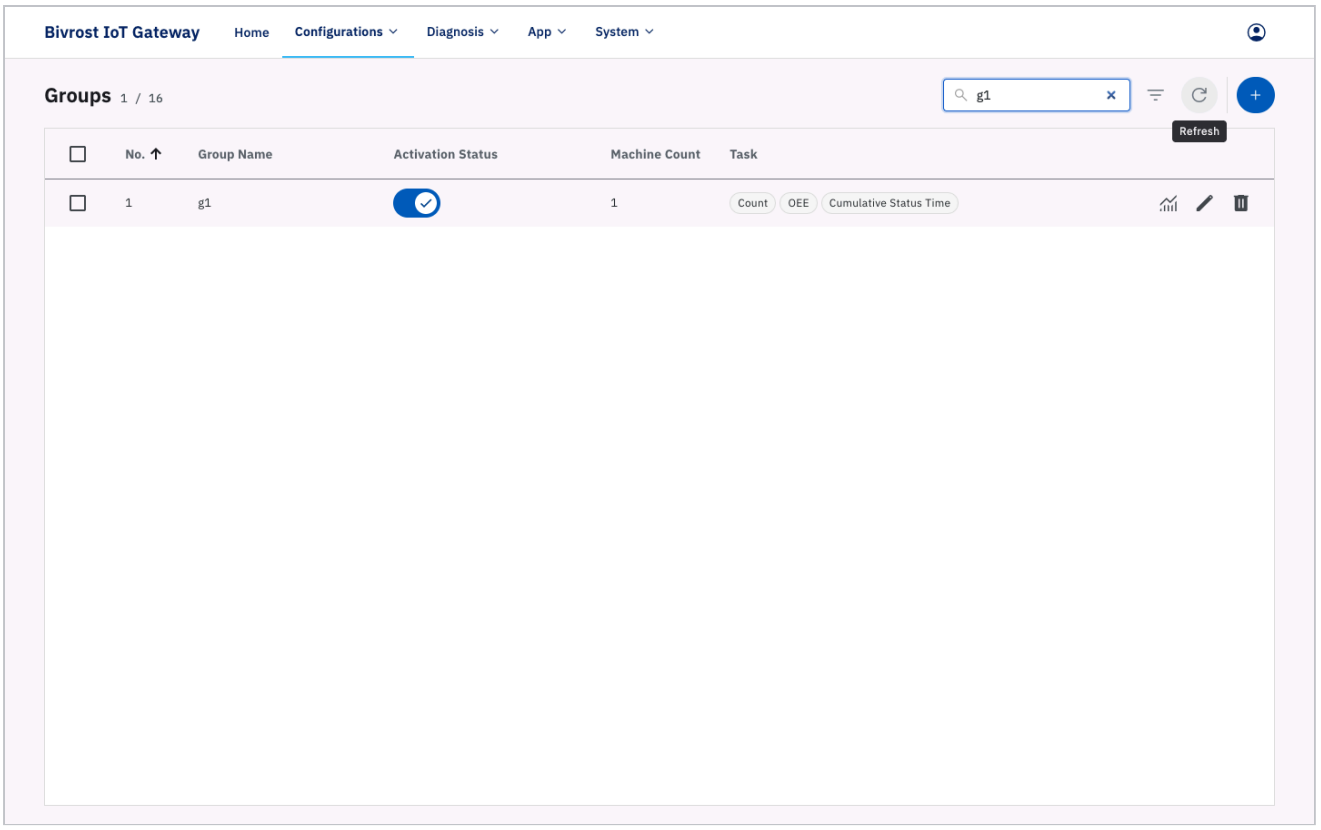
> **Note**
>
> Unlike machine activation, activating a group does not consume a license. An activated group is enabled, and its data is uploaded through the cloud platform (see 3.6.1. Cloud Settings for how to set this up), MODBUS, MQTT and a database (see the *Communication Protocol*). A deactivated group stops collecting statistics for that group and stops uploading them. If a group contains a machine that is not activated (see 3.3. Machines), no data is collected or included in the statistics for that machine.



There are three buttons in the top-right corner of the page: Find Group, Refresh and Create Group.

Click the 🔍 Find Group button and type a keyword into the input field to its left; the matching results appear below. The search covers the group number and the group name. Click the close

button on the right of the search field to show all groups again.

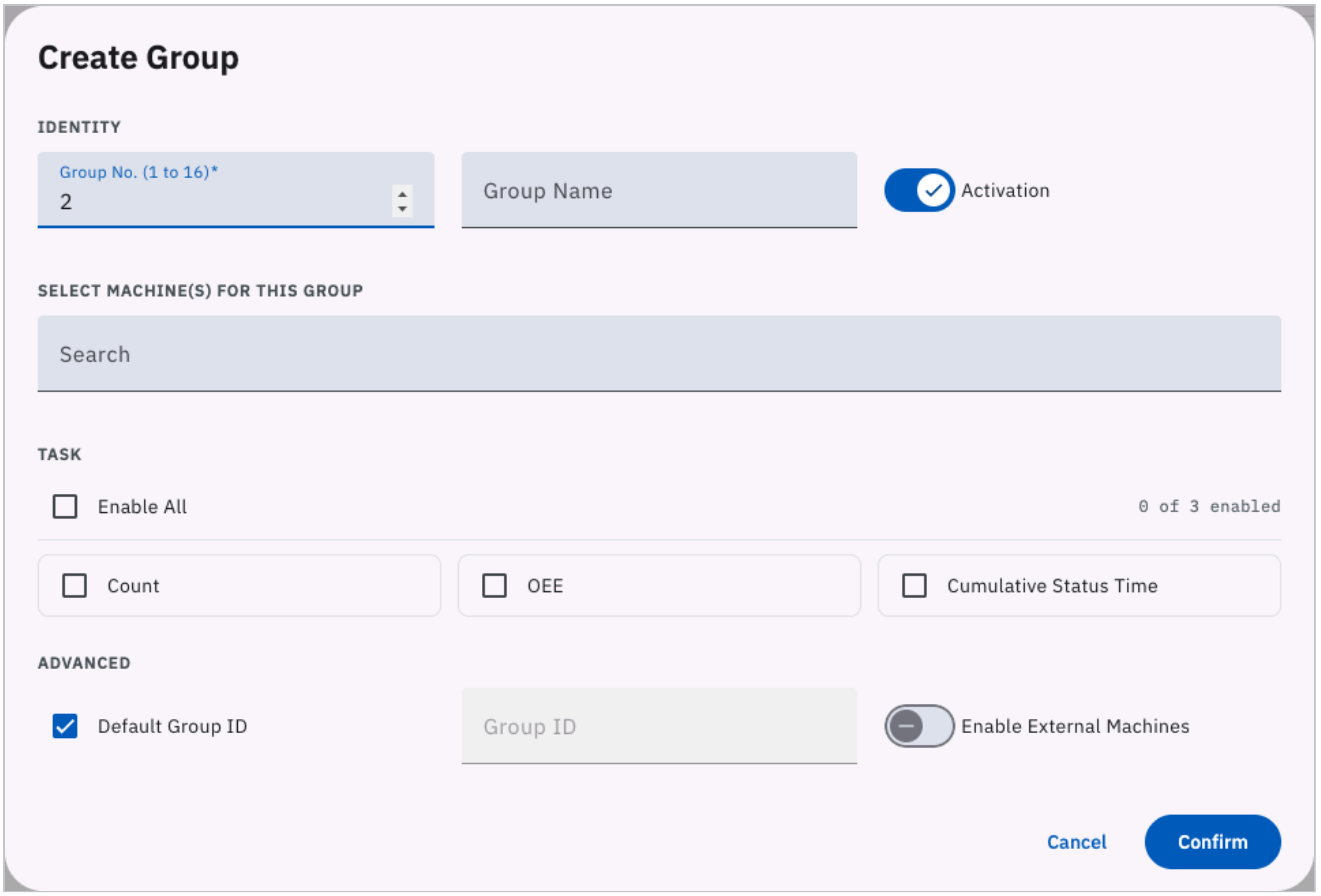


Click the ↻ Refresh button to refresh the whole group list.

Click the + Create Group button to add a group, as described in 3.4.1. Adding a Group.

3.4.1. Adding a Group

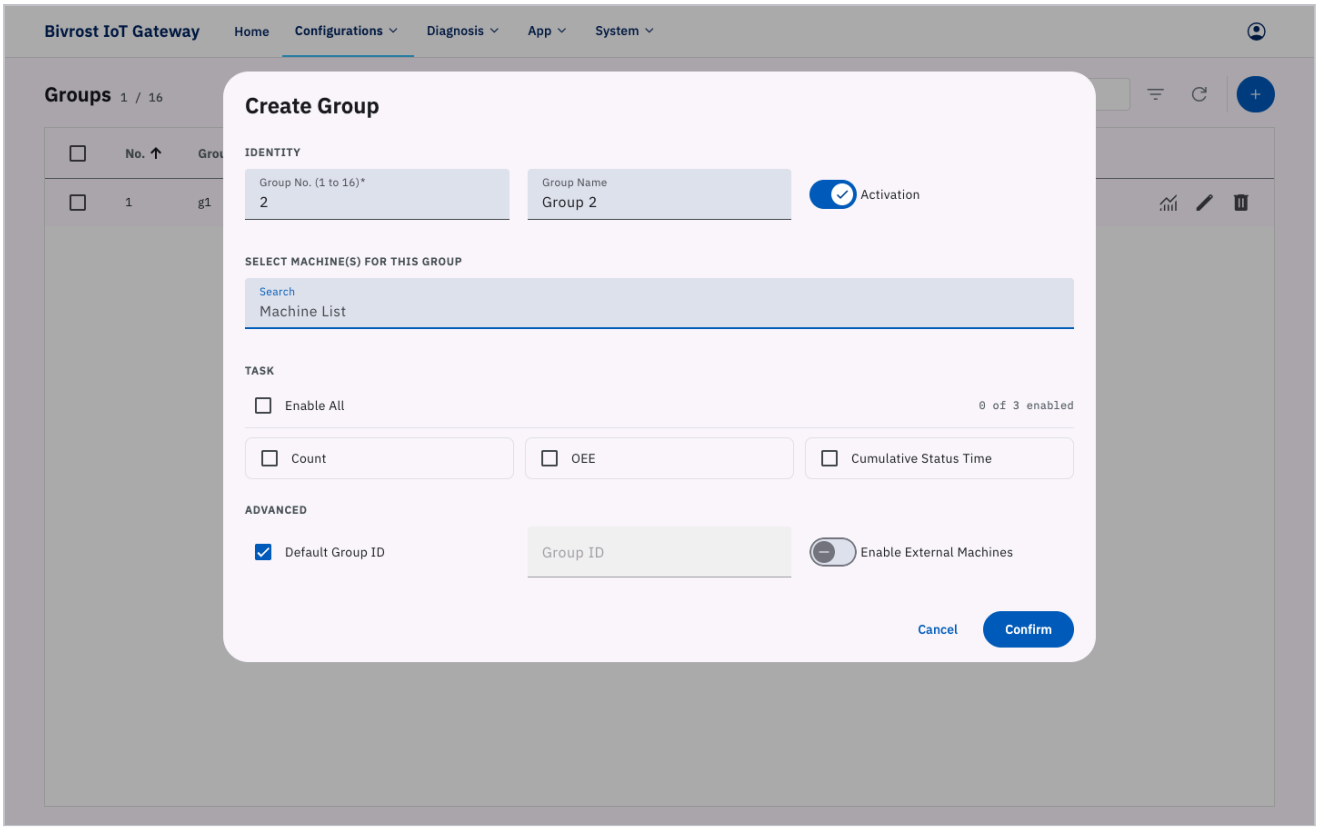
Click the + Create Group button in the top-right corner. The “Create Group” dialog opens, with four sections from top to bottom: “Identity”, “Select Machine(s) for This Group”, “Task” and “Advanced”.



3.4.1.1. Group General Settings

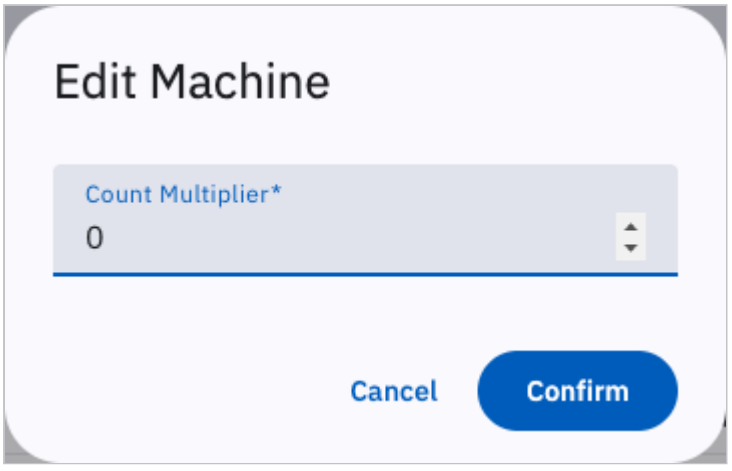
In the “Identity” section, enter the group number and the group name. The group number must currently be an integer between 1 and 16 inclusive, and must not duplicate an existing group number. You can also activate or deactivate the group: statistics are uploaded only while the group is activated. Deactivating it disables the group, and its statistics are no longer uploaded. If the group contains a machine that is not activated (for machine activation, see 3.3. Machines), that machine is not added to the collection list and is neither polled nor included in the statistics.

Click the “Search” box under “Select Machine(s) for This Group” and pick the machines for the group from the machine list. The selected machines are shown as tags, and the number of machines in the group appears in the “Machine Count” column on the **Groups** page.



Each selected machine tag shows the machine IP, the machine name and the count multiplier (for example ×0). Click the × on the right of a tag to remove that machine.

Adjusting the count multipliers of the machines in a group lets you define how the group’s count is calculated. Click a selected machine tag to edit its count multiplier.



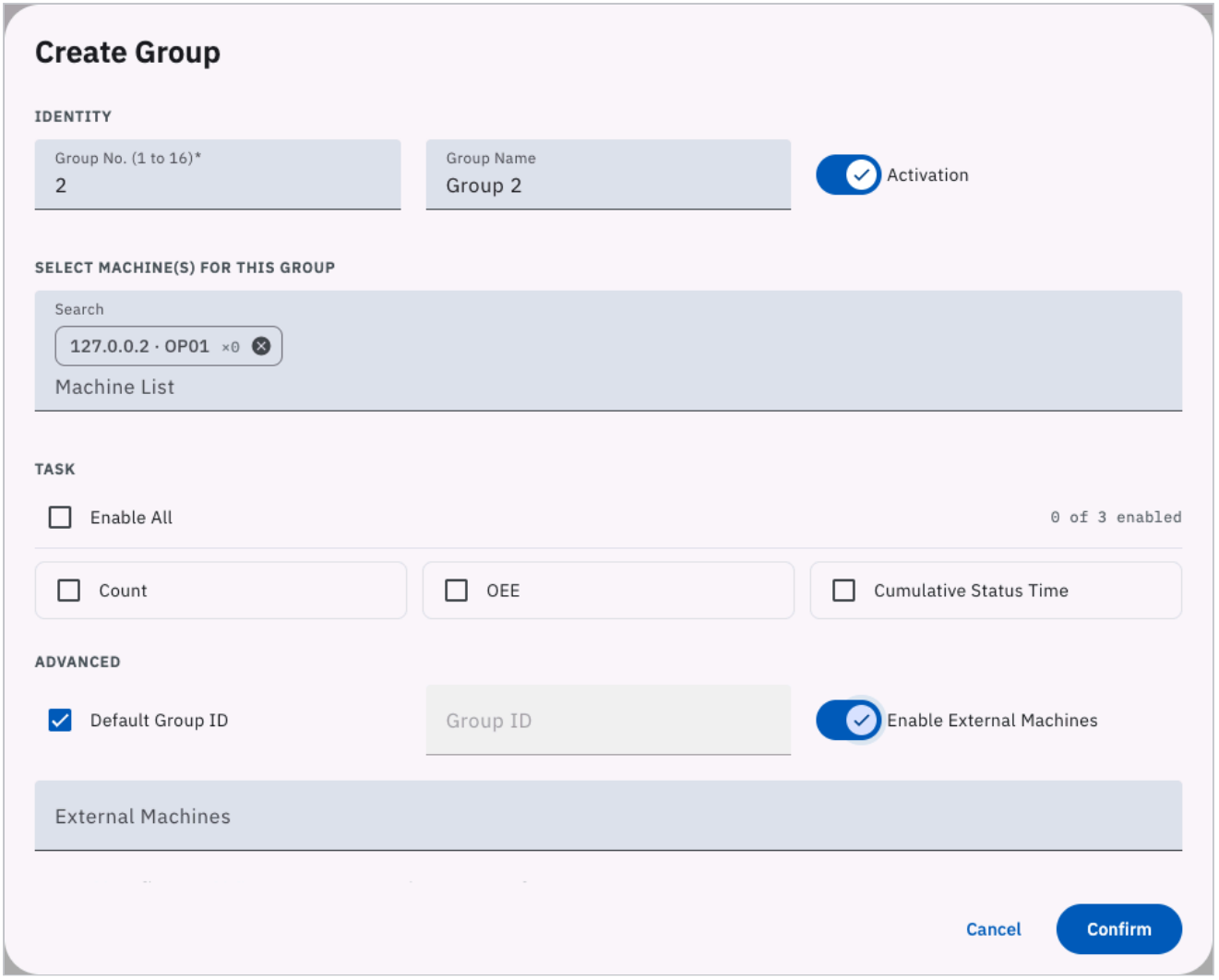
For example, if machine “OP01” and machine “OP02” form a production line and handle two consecutive operations, the output of the line should be taken from the last operation, “OP02”. Set the count multiplier of “OP01” to 0 and that of “OP02” to 1, giving:

```
Group Count = "OP01" Count * 0 + "OP02" Count * 1
```

If the last operation is handled by several machines, set the count multiplier of all of those machines to 1.

If a machine produces several parts per cycle, set its count multiplier to the corresponding number.

By enabling external machines you can add to the group machines that belong to the gateways linked in Cloud Settings or Hub Settings. This requires a command that identifies the gateway and the machine; see 4.2.6. External Machines.



3.4.1.2. Group Task Settings

In the “Task” section, configure the group’s automatic collection tasks. Tick an available interface to turn on automatic statistics collection and upload for the corresponding group task.

The number of enabled tasks appears in the “Task Count” column of the table on the “Groups” page.

Group tasks work in much the same way as machine tasks: their results can be uploaded automatically through the cloud platform, MODBUS, MQTT or a database. To receive group task results, at least one of the cloud platform, MODBUS, MQTT or database communication methods must be enabled and configured in 3.6. Communication. The collection interval and the detailed settings for group tasks are configured in 3.5. Tasks. For the format in which group task results are published over MODBUS, MQTT and a database, see the *Communication Protocol*.

> **Note**
>
> If the group contains a machine that is not activated (for machine activation, see 3.3. Machines), that machine is not on the collection list and is not included in the statistics.

Group OEE data covers all activated machines in the group: total Off time, total Wait time, total Emergency time, total Autorun time, total Manual time, the current number of machines that are Off, Wait, Emergency, Autorun and Manual, and the group availability. See 4.1.2. Group OEE Data.

For the group part count, see 4.1.3. Group Part Count.

Both group OEE and the group part count require local caching, so the “Local Caching” switch under Options in 3.12. Settings must be turned on before you enable them.

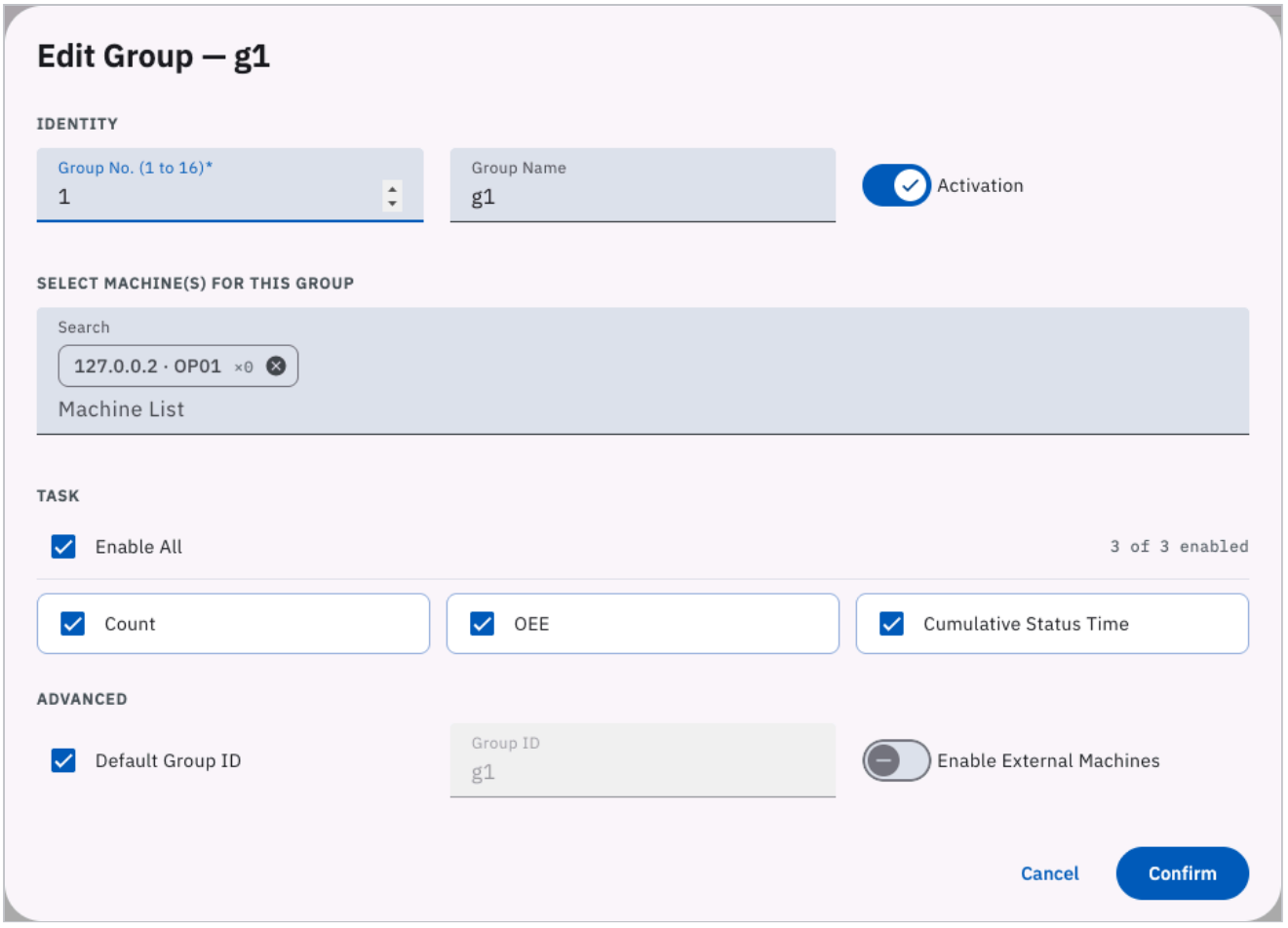
Group Cumulative Status Time is the total time spent in each status, summed over all machines in the group, since the gateway started collecting from those machines, in seconds.

3.4.1.3. Advanced Settings

In the “Advanced” section you can define a custom group ID (GroupID). The group ID identifies the group’s data for every communication method except MODBUS. The default group ID is the letter g followed by the group number, for example “g1”.

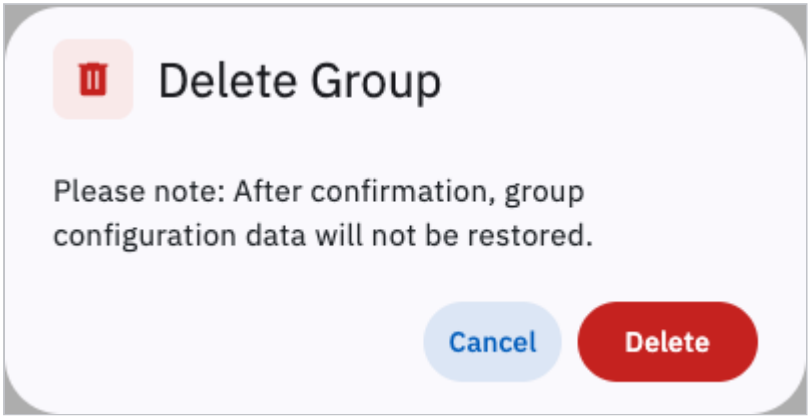
3.4.2. Editing a Group

Click the **Edit** button in the “Operations” column on the right of an existing group row to open the “Edit Group” dialog, which is similar to “Create Group”. Here you can change the group number, group name and activation state, select the machines in the group, adjust their count multipliers, configure group tasks, change the group ID, and so on.



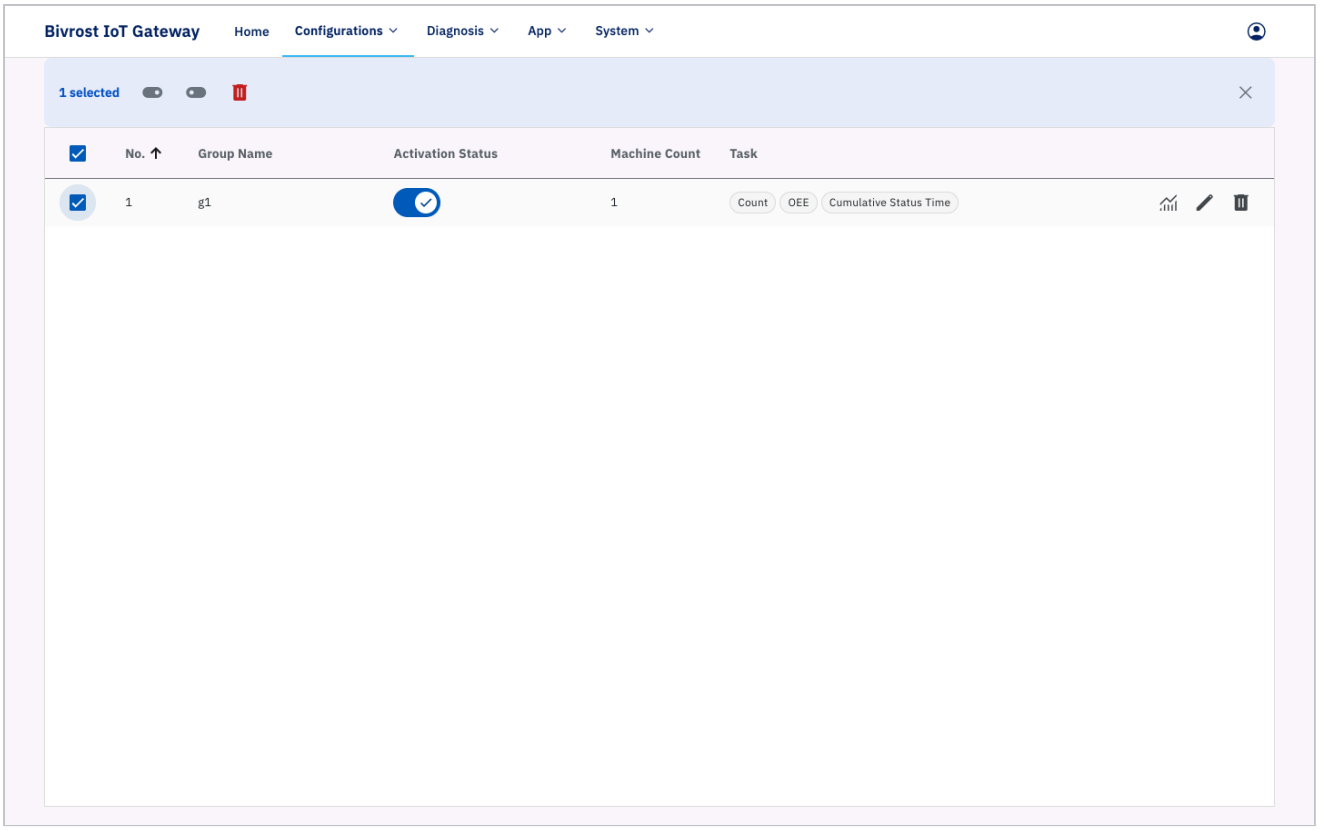
3.4.3. Deleting a Group

Click the **Delete** button in the “Operations” column on the right of an existing group row. The “Delete Group” dialog appears; click **Confirm** to delete the group.



3.4.4. Batch Activation

Select several groups using the checkboxes at the far left of the list, or the select-all button at the top left of the list.



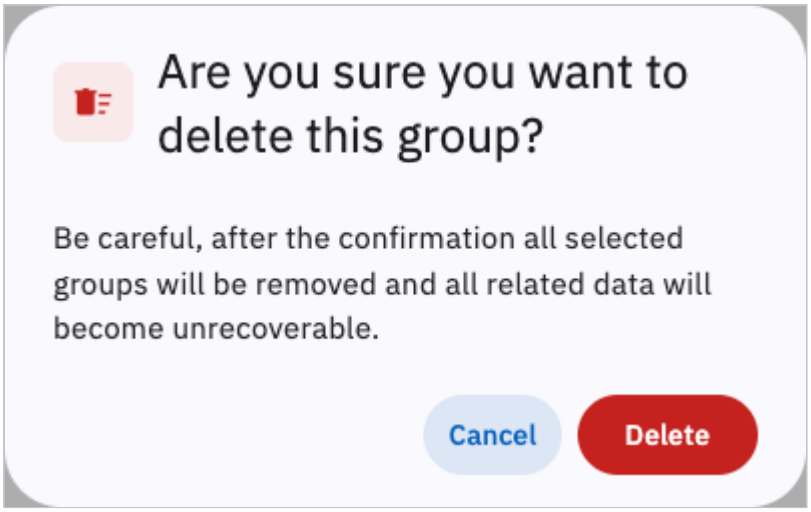
A batch action bar then appears at the top of the page with the **Activate**, **Deactivate**, **Batch Delete** and **Clear Selection** buttons.

Click **Activate** or **Deactivate** to activate or deactivate all the selected groups at once.

3.4.5. Batch Delete

Select several groups using the checkboxes at the far left of the list, or the select-all button at the top left of the list.

Click **Batch Delete** on the batch action bar, then click Confirm in the dialog that appears to delete the selected groups.

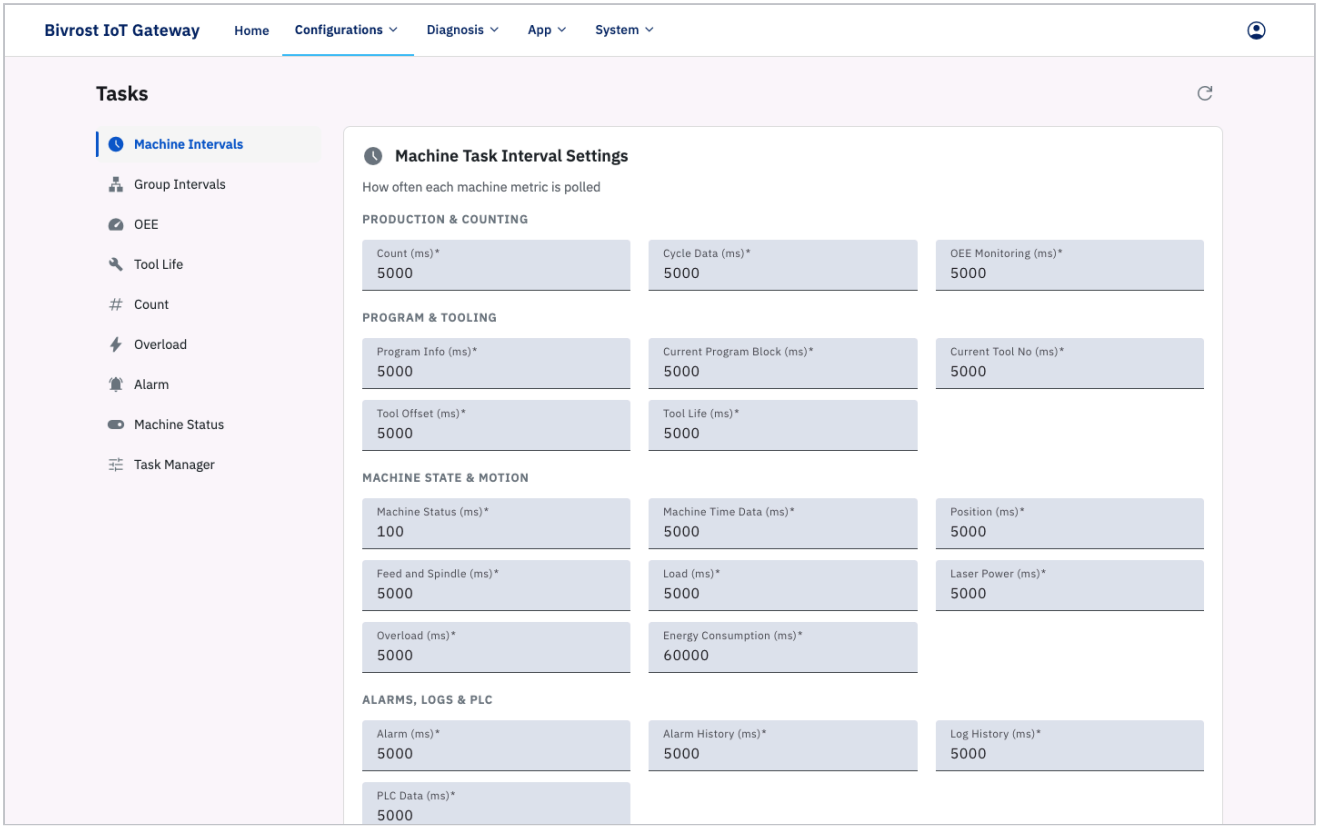

Are you sure you want to delete this group?
Be careful, after the confirmation all selected groups will be removed and all related data will become unrecoverable.
Cancel
Delete

3.5. Tasks

Tasks includes Machine Task Interval Settings, Group Task Interval Settings, OEE Monitoring Settings, Tool Life Monitoring Settings, Count Monitoring Settings, Overload Monitoring Settings, Alarm Monitoring Settings, Machine Status Monitoring Settings and Task Manager Settings.

On the **Tasks** page, click a tab to switch between the setting groups. When you are done, click **Save** below the settings area, then go back to Home and click **Restart Service** to apply the changes.

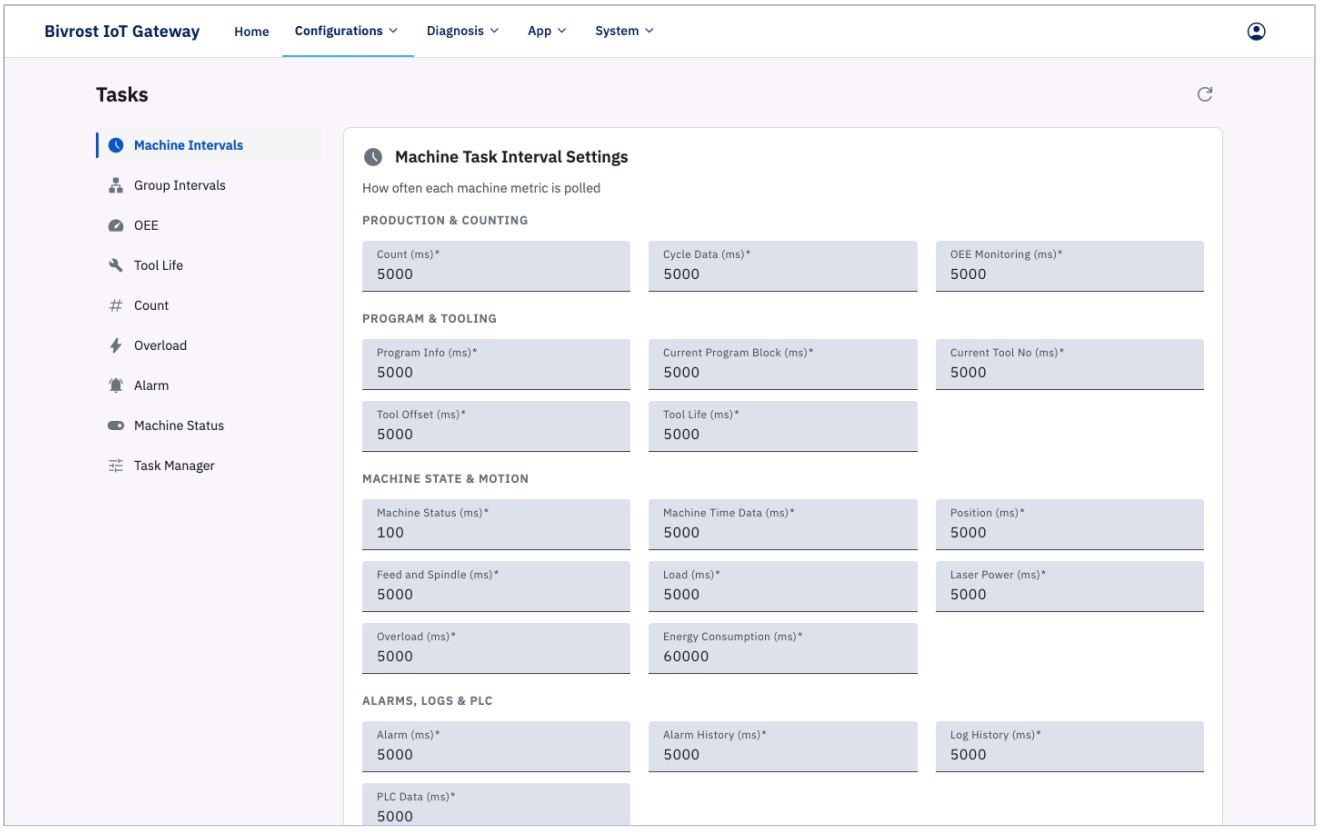
If you are not using automatic data collection tasks, you do not need to configure **Tasks**.



3.5.1. Machine Task Interval Settings

“Machine Task Interval Settings” sets the automatic collection interval for each of the machine tasks described in 3.3.1.2. Task Settings. Intervals are in milliseconds and all default to 5000 ms.

> **Note**
>
> An interval of 5000 ms or longer is recommended. Very short intervals can cause unpredictable faults on machines with limited processing power.



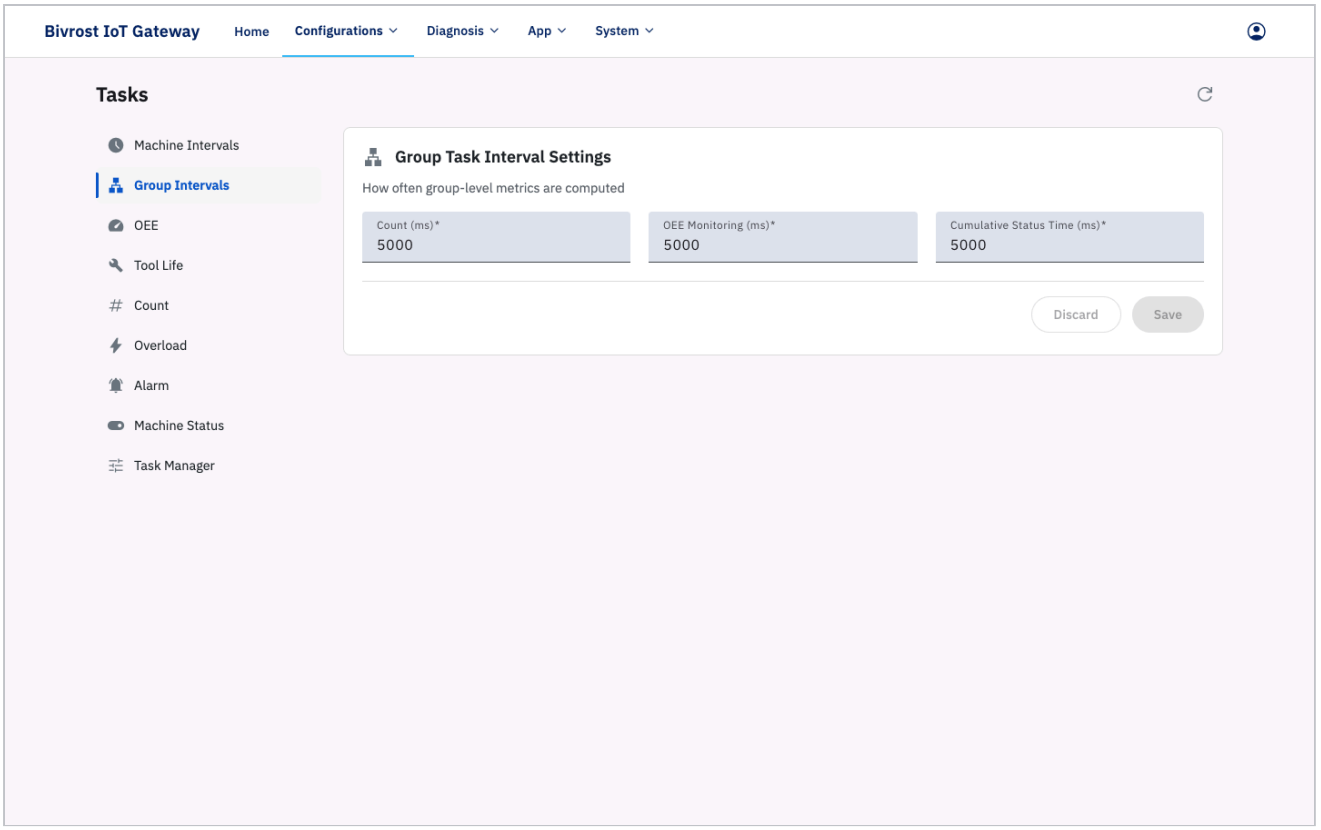
"Overload (ms)" in the screenshot above defaults to 100 ms. Overload events are very short-lived, so a short monitoring interval is needed to capture the data accurately.

"OEE Monitoring (ms)" in the screenshot above is the automatic collection interval for machine OEE data; see 4.1.1. Machine OEE Data.

When you are done, click the **Save** button at the bottom of the page, then click **Restart Service** on Home to apply the changes.

3.5.2. Group Task Interval Settings

"Group Task Interval Settings" sets the automatic collection interval for each of the group tasks described in 3.4.1.2. Group Task Settings. Intervals are in milliseconds and all default to 5000 ms.

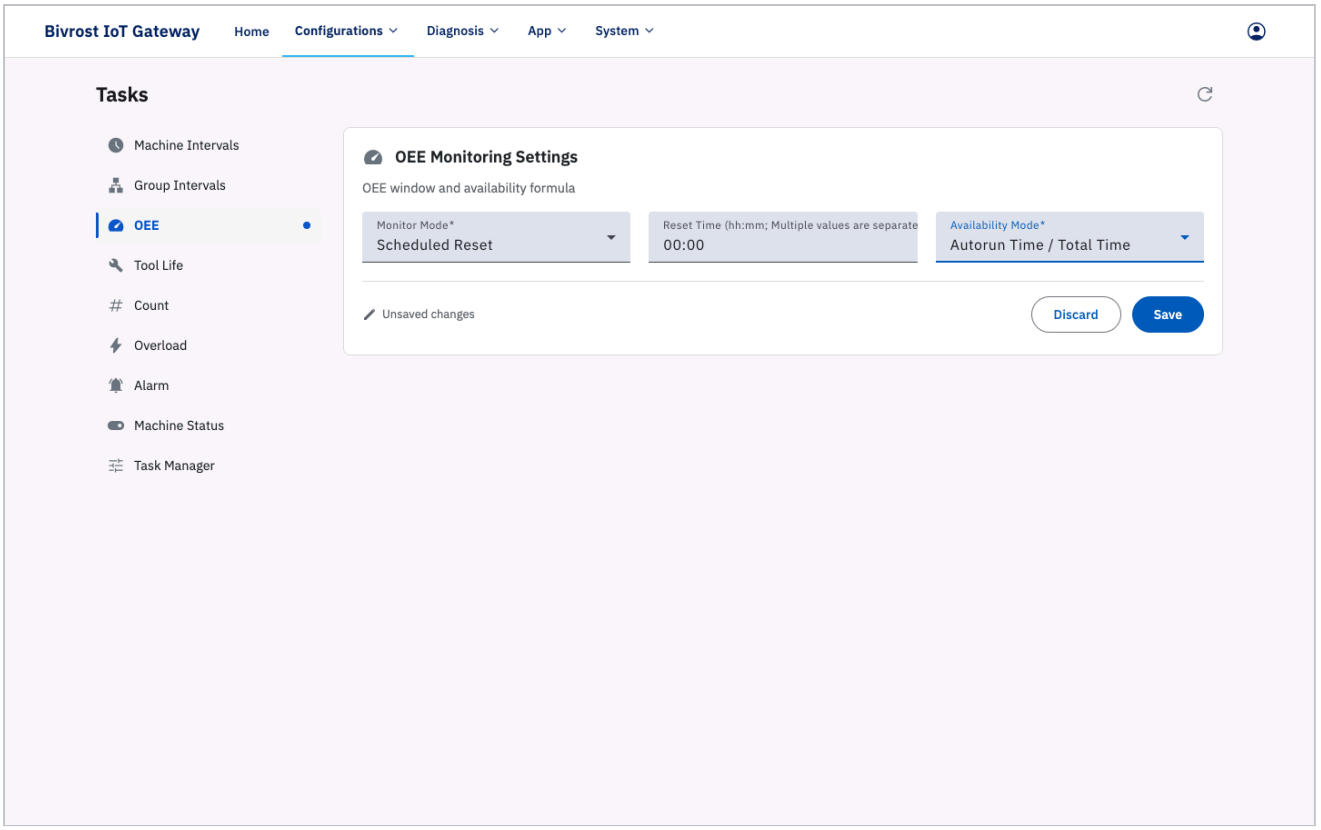


“Count (ms)” in the screenshot above is the automatic collection interval for the group part count; see 4.1.3. Group Part Count. “OEE Monitoring (ms)” is the automatic collection interval for group OEE data; see 4.1.2. Group OEE Data.

When you are done, click the **Save** button at the bottom of the page, then click **Restart Service** on Home to apply the changes.

3.5.3. OEE Monitoring Settings

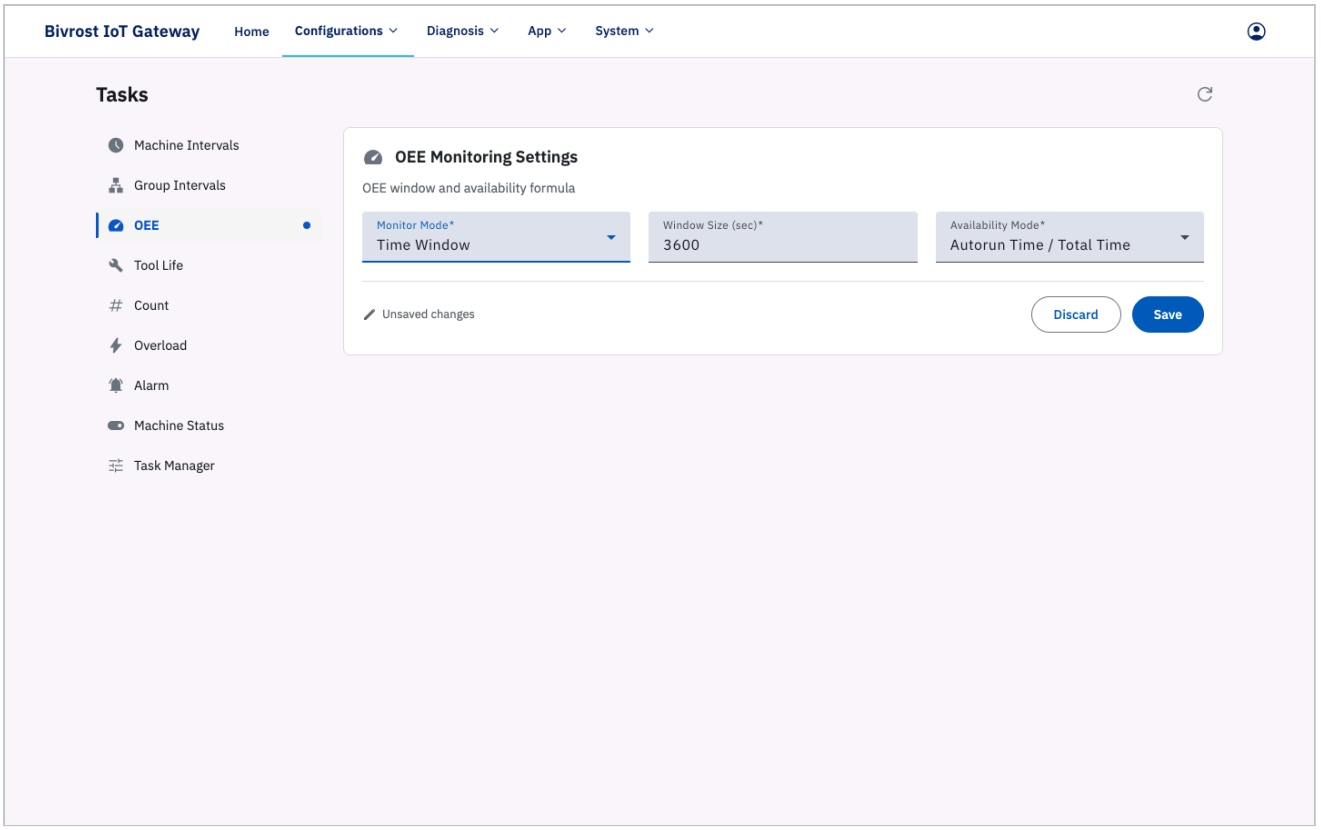
“OEE Monitoring Settings” defines the monitoring period and the availability formula used for machine OEE (see 4.1.1. Machine OEE Data) and group OEE (see 4.1.2. Group OEE Data).



"Monitor Mode" determines how the monitoring period is defined. It offers two options: "Scheduled Reset" and "Time Window".

Scheduled Reset: OEE statistics are calculated over the period that runs from the most recent reset time up to the present moment. "Reset Time" is the time of day at which the daily OEE statistics are reset. You can enter several reset times separated by ";", for example `08:00;12:00;16:00;20:00;`. If no reset time is entered, the default is 00:00, so OEE statistics are reset every day at 00:00.

Time Window: the window size defaults to 3600 seconds, so OEE statistics are calculated over the period that starts 3600 seconds before the present moment and ends at the present moment — that is, the last hour. A window size longer than 86400 seconds (the last day) is not recommended. If this is the first collection and the elapsed monitoring time is shorter than the window size, any time with no machine status data is treated as machine off.



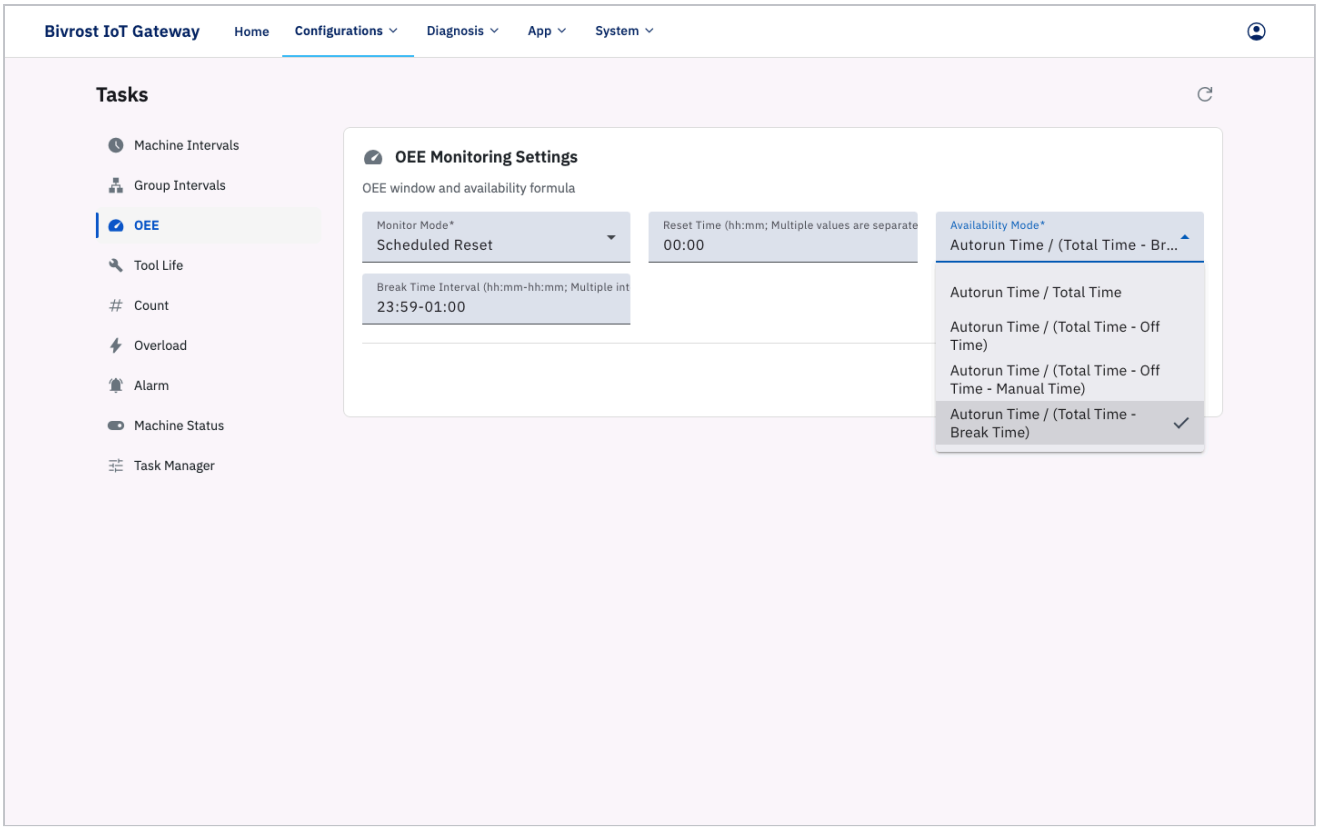
The “Availability Mode” option defaults to “Autorun Time / Total Time”, in which case:

```
Machine Availability = Autorun Time / Total Time
```

Here, autorun time is the machine’s automatic running time within the monitoring period, and total time is the monitoring period itself, as defined by “Monitor Mode”.

```
Group Availability = Autorun Time / Total Time
```

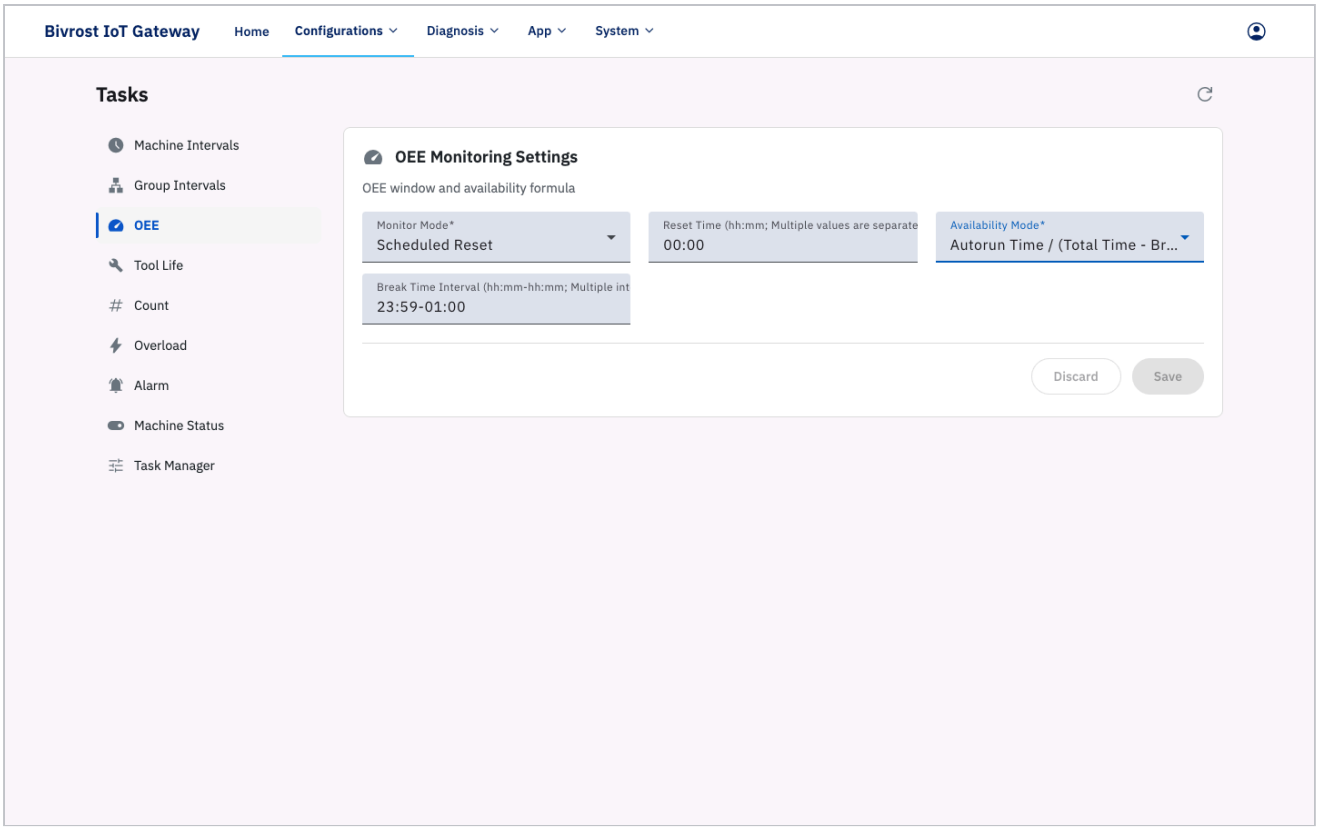
Here, autorun time is the sum of the automatic running time of every active machine in the group within the monitoring period, and total time is the total monitoring time — the monitoring period multiplied by the number of active machines in the group. The monitoring period is defined by “Monitor Mode”.



The “Availability Mode” options are:

- Autorun Time / Total Time
- Autorun Time / (Total Time - Off Time)
- Autorun Time / (Total Time - Off Time - Manual Time)
- Autorun Time / (Total Time - Break Time)

Choose whichever mode suits your needs to exclude off time, manual time or break time from the total time. Off time and manual time are derived from the machine status interface data. When you select “Autorun Time / (Total Time - Break Time)”, you can define the break time intervals, as shown below:

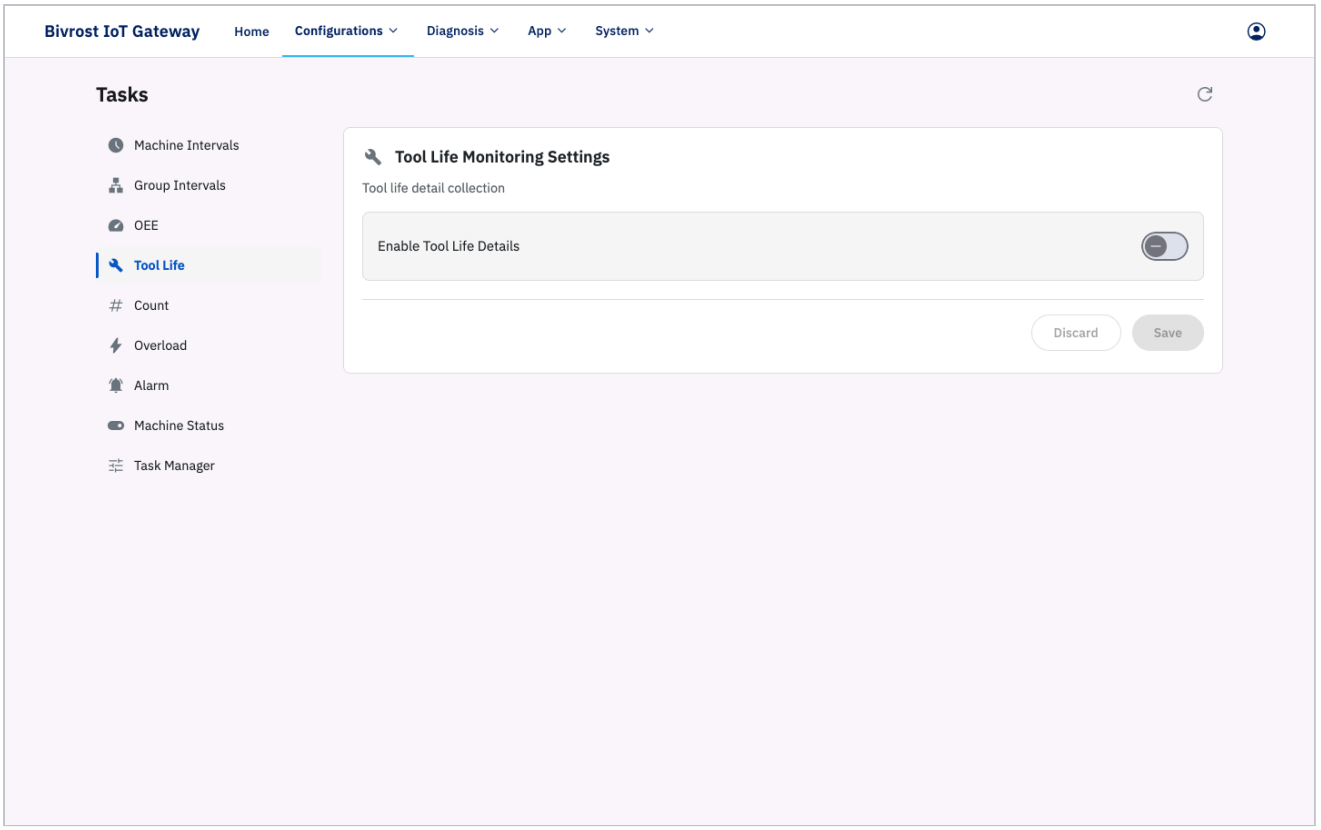


Suppose the break time intervals are set to `07:30-08:00;19:30-20:00;` and the current time is 19:45. With the settings above:

- Total time = 3600 seconds; the monitoring period runs from 18:45 to 19:45 and overlaps part of a break interval.
- Break time = 19:45 - 19:30 = 15 minutes = 900 seconds.

3.5.4. Tool Life Monitoring Settings

"Tool Life Monitoring Settings" configures the tool life data. The "Enable Tool Life Details" option is off by default, in which case the tool life interface returns only normalized data — values converted from the raw data and calculated using a single common definition and unit. With the option enabled, the tool life interface returns both the normalized data and the raw data. For a description of the normalized and raw tool life data, see *Communication Protocol* 1.2.25. ToolLife: Tool Life Data.

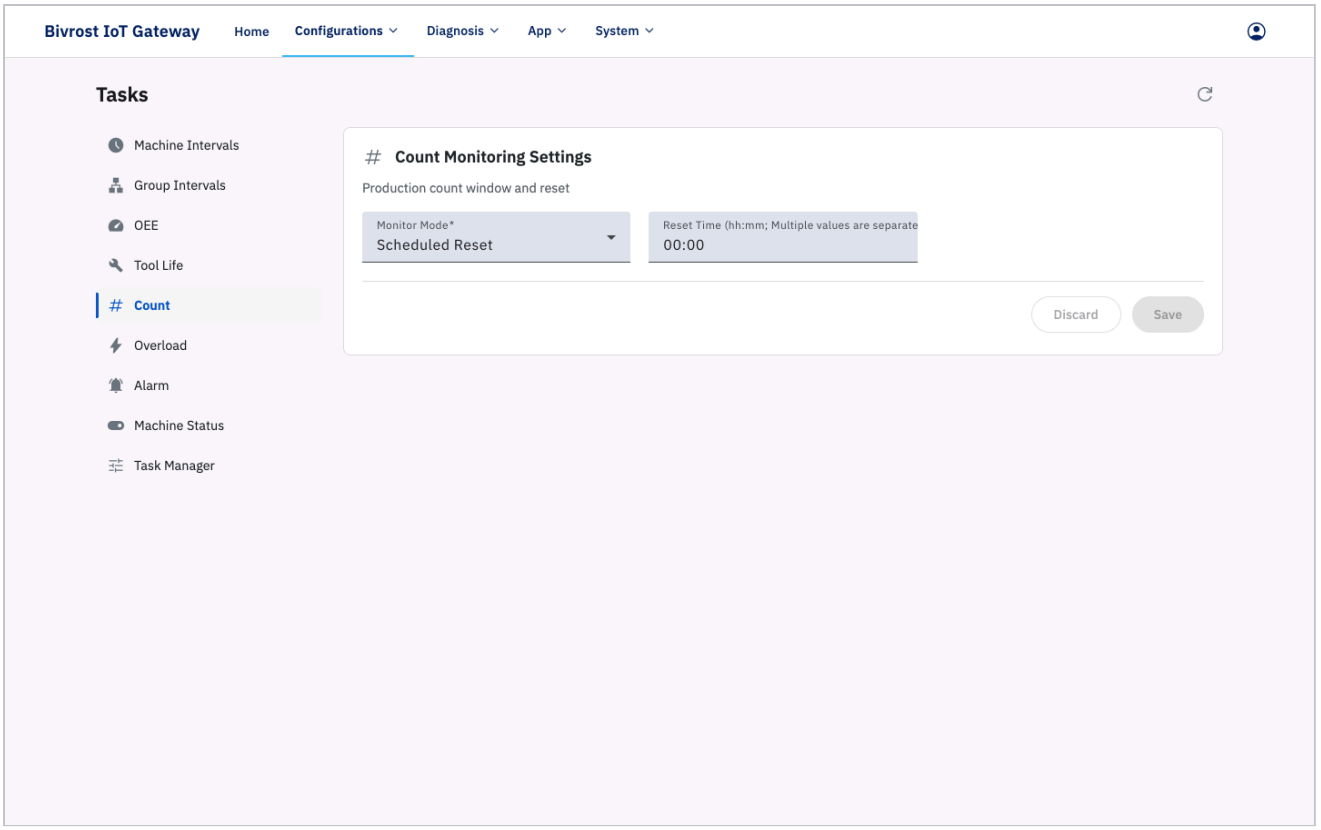


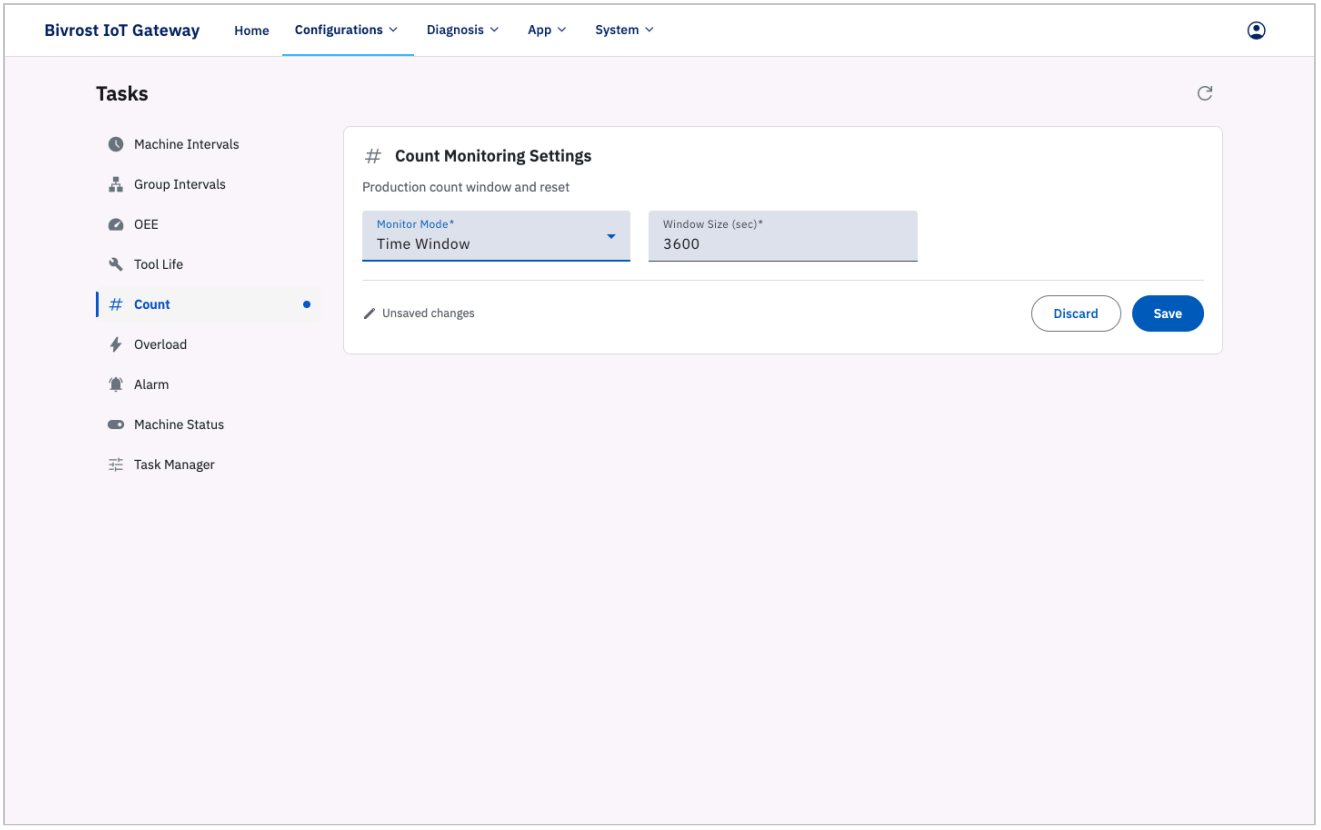
3.5.5. Count Monitoring Settings

“Count Monitoring Settings” defines the monitoring period for the current part count.

The current part count is the machine’s cumulative part count within the monitoring period.

“Monitor Mode” offers “Scheduled Reset” and “Time Window”; the default is “Scheduled Reset” with a default reset time of 00:00. For a description of the two modes, see 3.5.3. OEE Monitoring Settings.

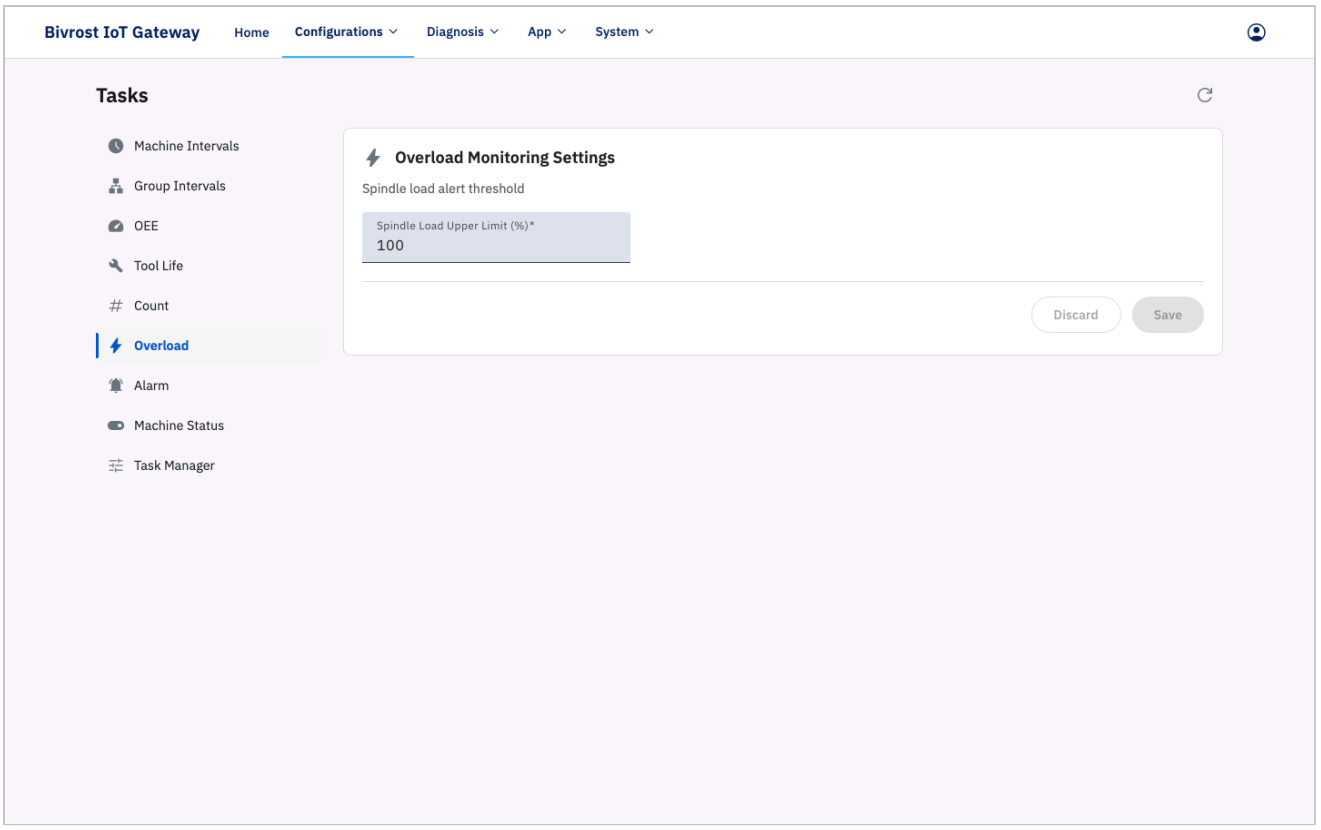




3.5.6. Overload Monitoring Settings

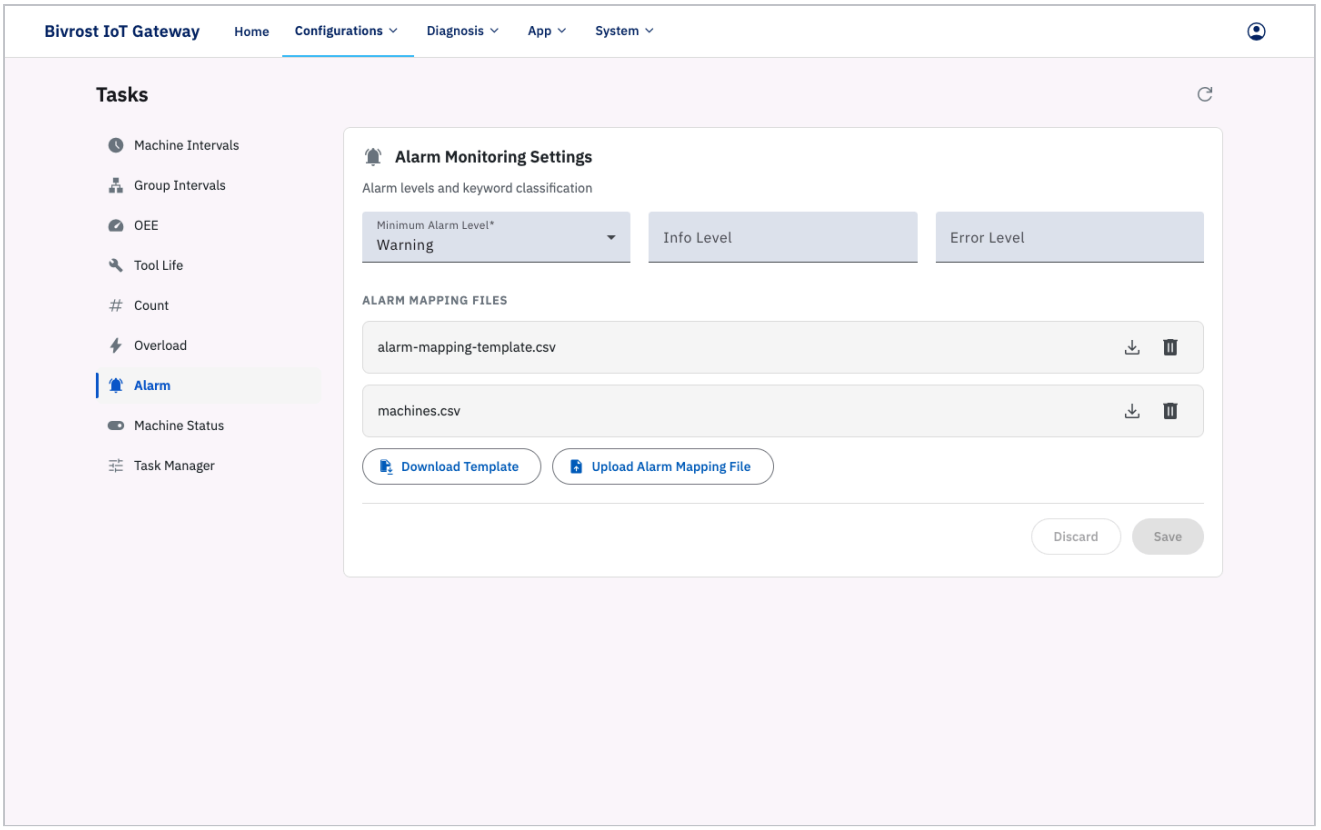
"Overload Monitoring Settings" sets the spindle load upper limit used by the overload task. The default is 100%.

Overload monitoring records the total time the spindle load stays above the limit.



3.5.7. Alarm Monitoring Settings

“Alarm Monitoring Settings” classifies the alarm messages returned by the alarm task into alarm levels and sets the minimum alarm level at which a machine is considered to be in an active alarm state.



Three alarm levels are currently supported, in descending order of priority: Error (ERR), Warning (WRN) and Information (INF). If the minimum alarm level is set to Warning, the gateway automatically ignores information-level alarms and records only error- and warning-level alarms, and uses those two levels to decide whether the machine is in an active alarm state.

In the “Info Level” and “Error Level” input boxes you can enter alarm keywords, separating multiple entries with “;” . Any alarm containing one of those keywords is assigned to the corresponding level.

If no error-level keyword is found in an alarm, the alarm defaults to warning level.

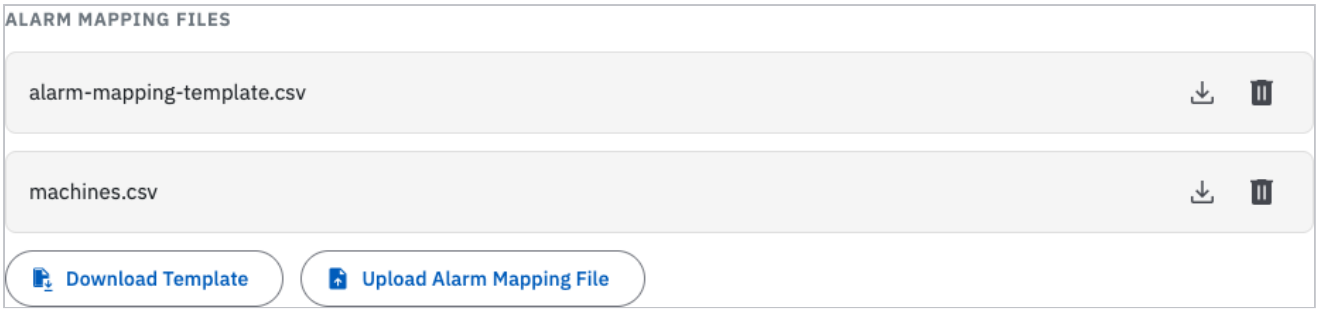
By default, the minimum alarm level for treating a machine as being in an active alarm state is warning level.

3.5.7.1. Alarm Mapping Files

Alarm Mapping maps the alarm numbers reported by a machine to your own alarm messages. It is useful for machines that report only an alarm number and no alarm text, or when alarm descriptions need to be standardized.

Use the “Alarm Mapping Files” area below “Alarm Monitoring Settings” to upload and manage mapping files:

- Click **Upload Alarm Mapping File** and select a local CSV file. Only non-empty CSV files are supported. The uploaded file then appears in the list.
- Each file in the list has a download and a delete button on the right.
- Click **Download Template** to get a sample CSV template (`alarm-mapping-template.csv`).
- When no file has been uploaded, the area shows “No alarm mapping files uploaded.”



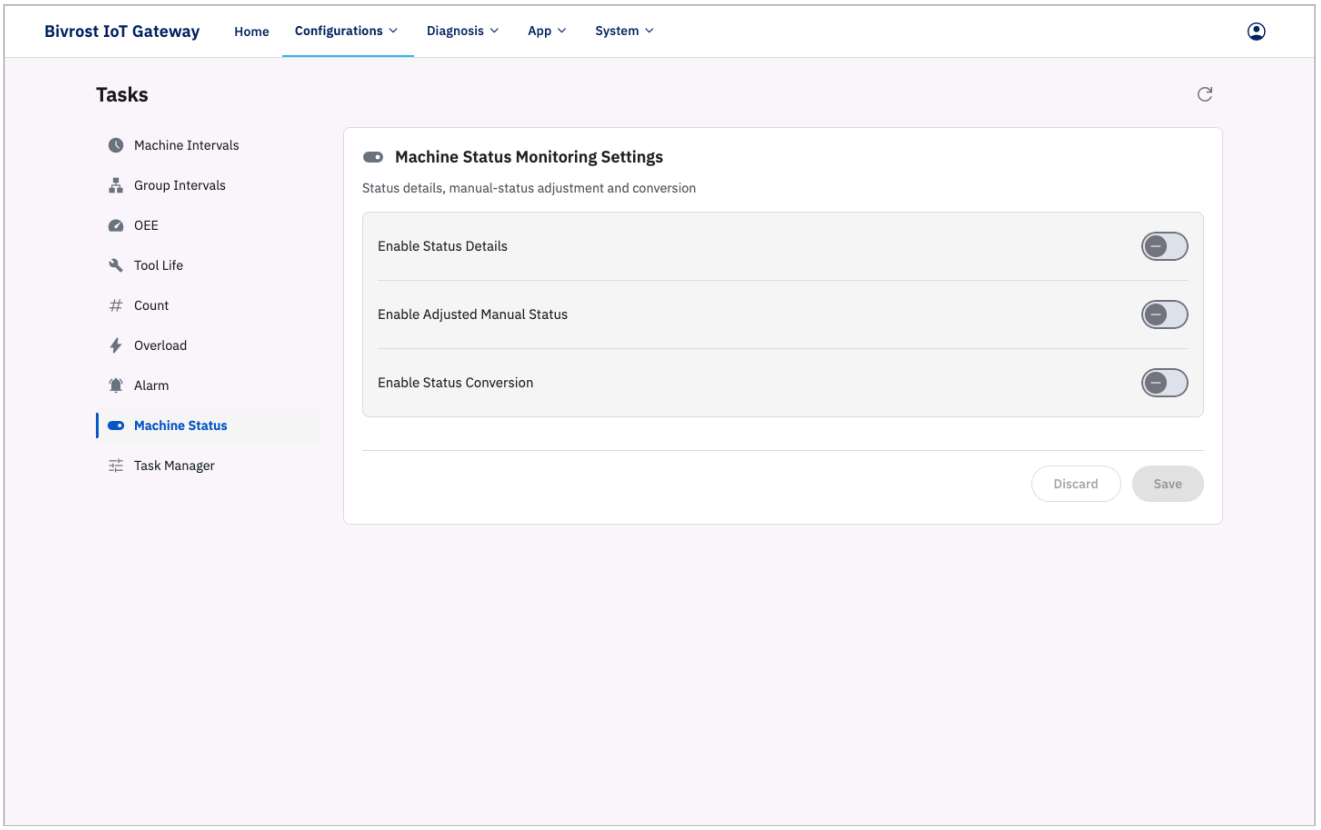
An alarm mapping file is a CSV file with two columns, headed “AlarmNo” and “Content”, for example:

AlarmNo	Content
1000	Emergency stop pressed
2001	Spindle overload

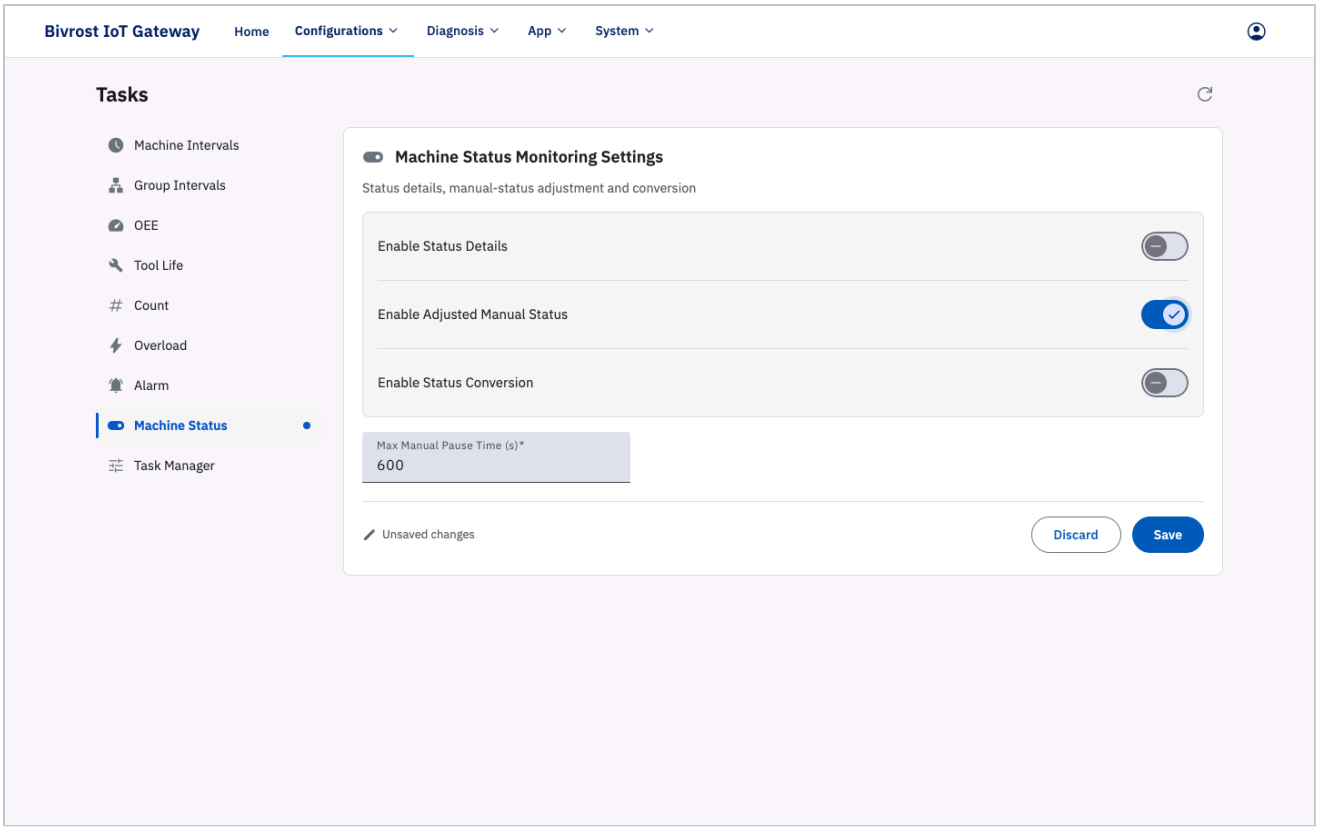
After uploading a mapping file, go to Machines, open the “Alarm” task settings of the machine concerned, enable alarm mapping and select the file; see 3.3.1.2.6. Alarm Mapping.

3.5.8. Machine Status Monitoring Settings

“Machine Status Monitoring Settings” configures the options of the machine status task, including Enable Status Details, Enable Adjusted Manual Status and Enable Status Conversion. For the machine task variables referred to in this section, see *Communication Protocol* 1.2.4. CNCStatus: Machine Status.



The "Enable Status Details" option is off by default, in which case the uploaded status data contains no status details. With the option enabled, the uploaded data includes the status details.

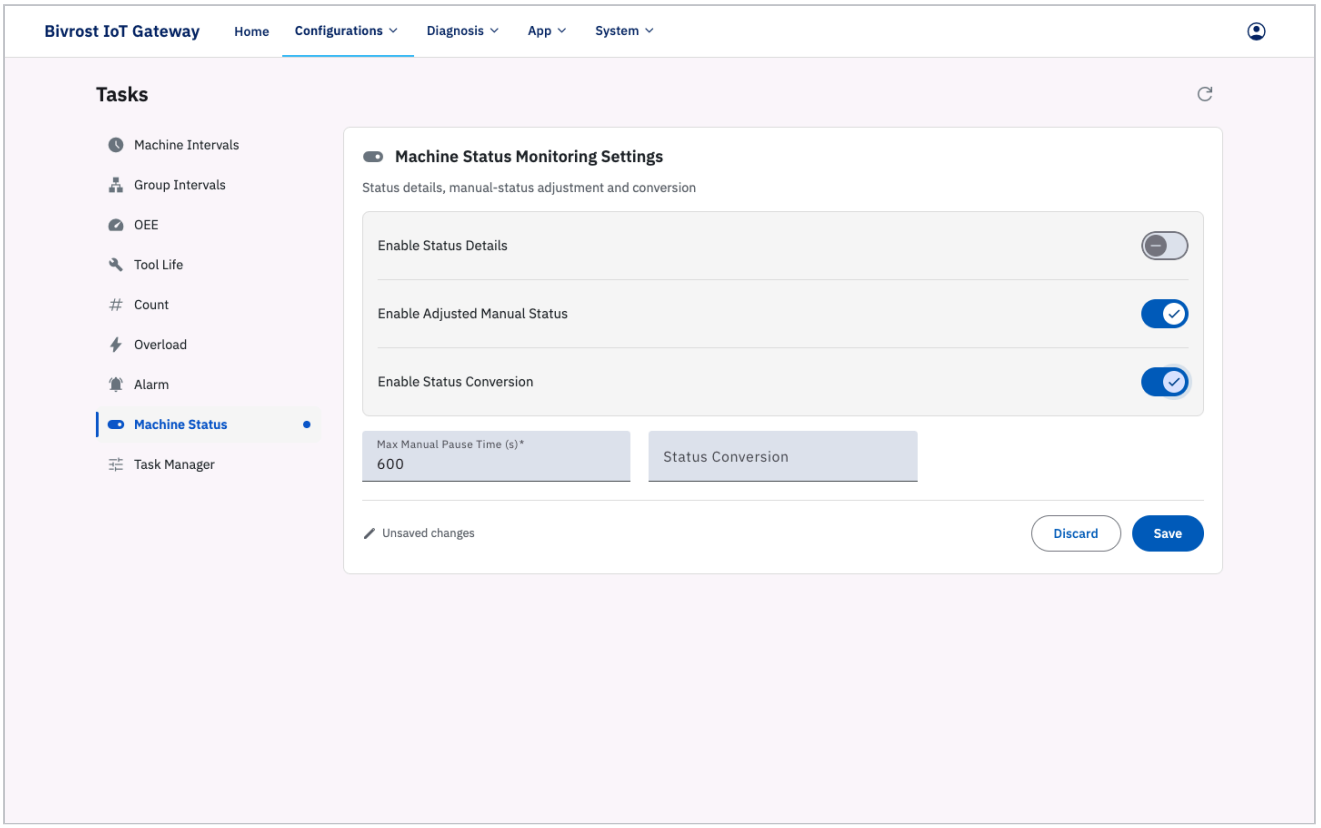


When “Adjusted Manual Status” or “Status Conversion” is enabled, the status is adjusted according to the corresponding rules and reported in adjustedStatus (*Communication Protocol* 1.2.4. CNCStatus: Machine Status). Wherever machine status is involved — OEE statistics, cumulative status time and so on — the adjusted status takes precedence. Both options are off by default, in which case adjustedStatus is identical to the real-time status returned by the machine. “Adjusted Manual Status” and “Status Conversion” here are global settings. Enabling the machine-level settings of the same name in 3.3.1.2.5. Special Settings overrides the global settings.

The rules for adjusting the manual status are:

1. The machine is currently in the Manual state;
2. The time since the machine changed from a non-Manual state to the Manual state exceeds the configured Max Manual Pause Time;
3. The machine’s coordinate data has remained unchanged for longer than the configured Max Manual Pause Time.

Normally adjustedStatus is identical to the machine’s real-time status. If all of the above conditions are met at the same time, adjustedStatus is no longer Manual but is corrected to Wait.



With status conversion enabled, adjustedStatus is set according to the commands you enter, for example:

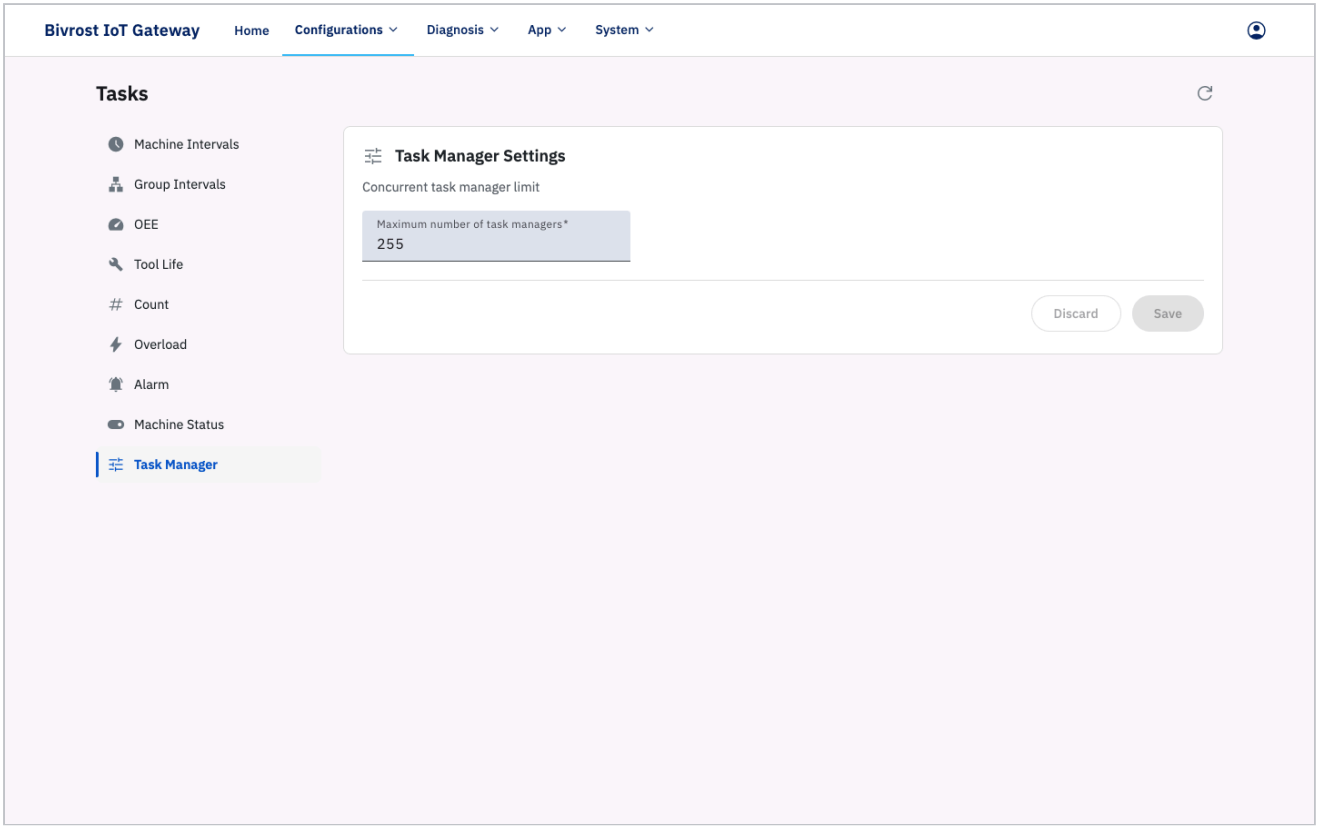
```
CNCStatus_cncStatus = "MANUAL_MDI_RUN" | AUTO_RUN
```

`CNCStatus_cncStatus = "MANUAL_MDI_RUN"` is the precondition (see 4.2.2. Precondition): if the cncStatus (running status, of type String) returned by this machine status task is “MANUAL_MDI_RUN”, then adjustedStatus is set to AUTO_RUN. Separate multiple conversion commands with “;”.

When both options are enabled, the manual status adjustment runs first and the status conversion second.

3.5.9. Task Manager Settings

Each task manager corresponds to one task thread. “Task Manager Settings” sets the maximum number of task managers, that is, the maximum number of task threads.



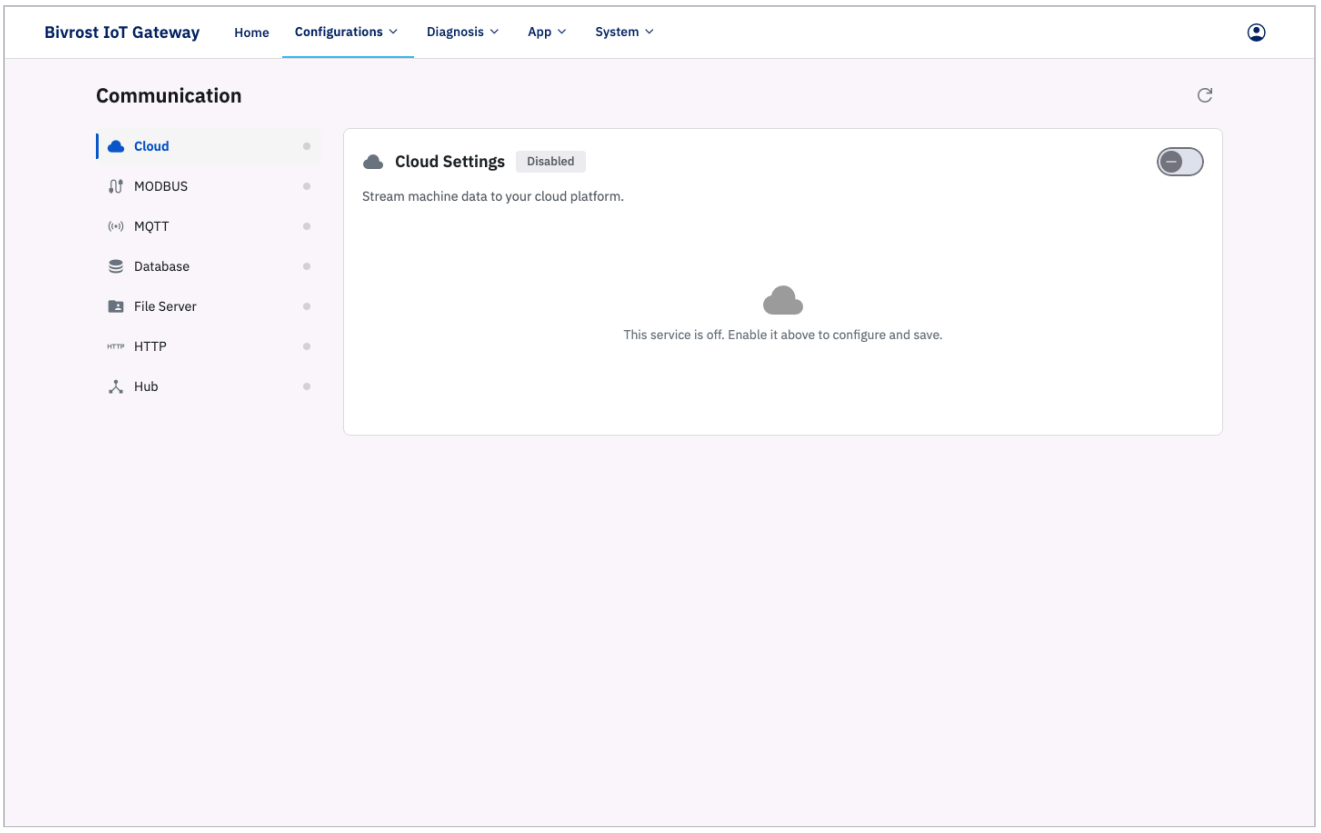
Each machine is allocated one task manager by default. You can assign several independent task managers to improve task throughput (see Parallel Task Processing in 3.3.1.5. Advanced Settings). The more task managers there are, the greater the demands on the hardware, so tune this parameter to your hardware’s capabilities. The maximum number of task managers defaults to 255. When the total number of task managers required by the active machines

exceeds this maximum, task managers are merged automatically to bring the total back below the limit, which reduces task throughput.

3.6. Communication

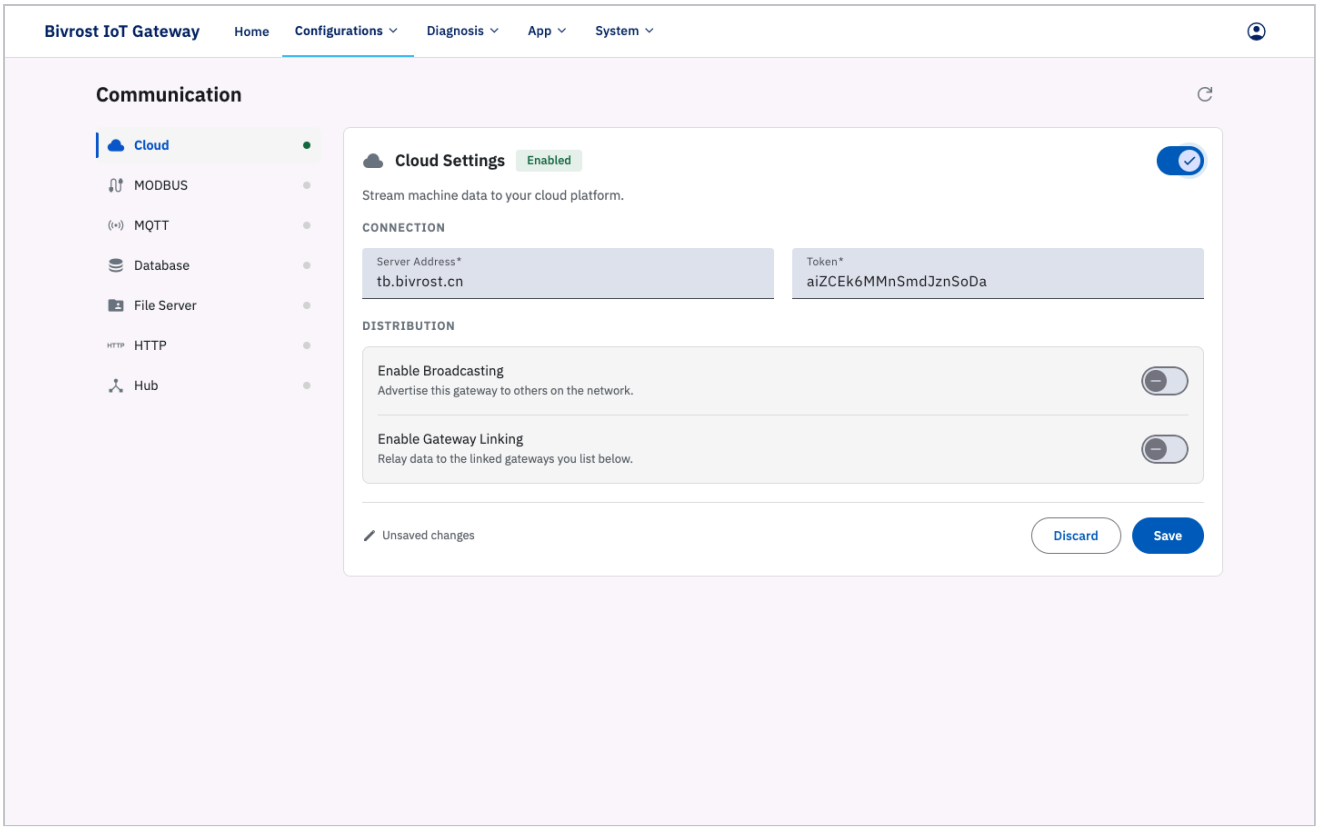
Communication covers Cloud Settings, MODBUS Settings, MQTT Settings, Database Settings, Gateway File Server Settings, HTTP Settings, Hub Settings, MCP Settings and so on. You can turn on one or more of these communication methods as required.

The left side of the **Communication** page lists the available communication methods (and shows whether each one is enabled); the right side holds the settings for the selected method. Turn on the **Enable** switch in those settings to show all of the fields. Except for MCP Settings, after you click **Save** you must go back to Home and click **Restart Service** to apply the changes.



3.6.1. Cloud Settings

Click the **Enable** switch to turn on cloud platform communication.

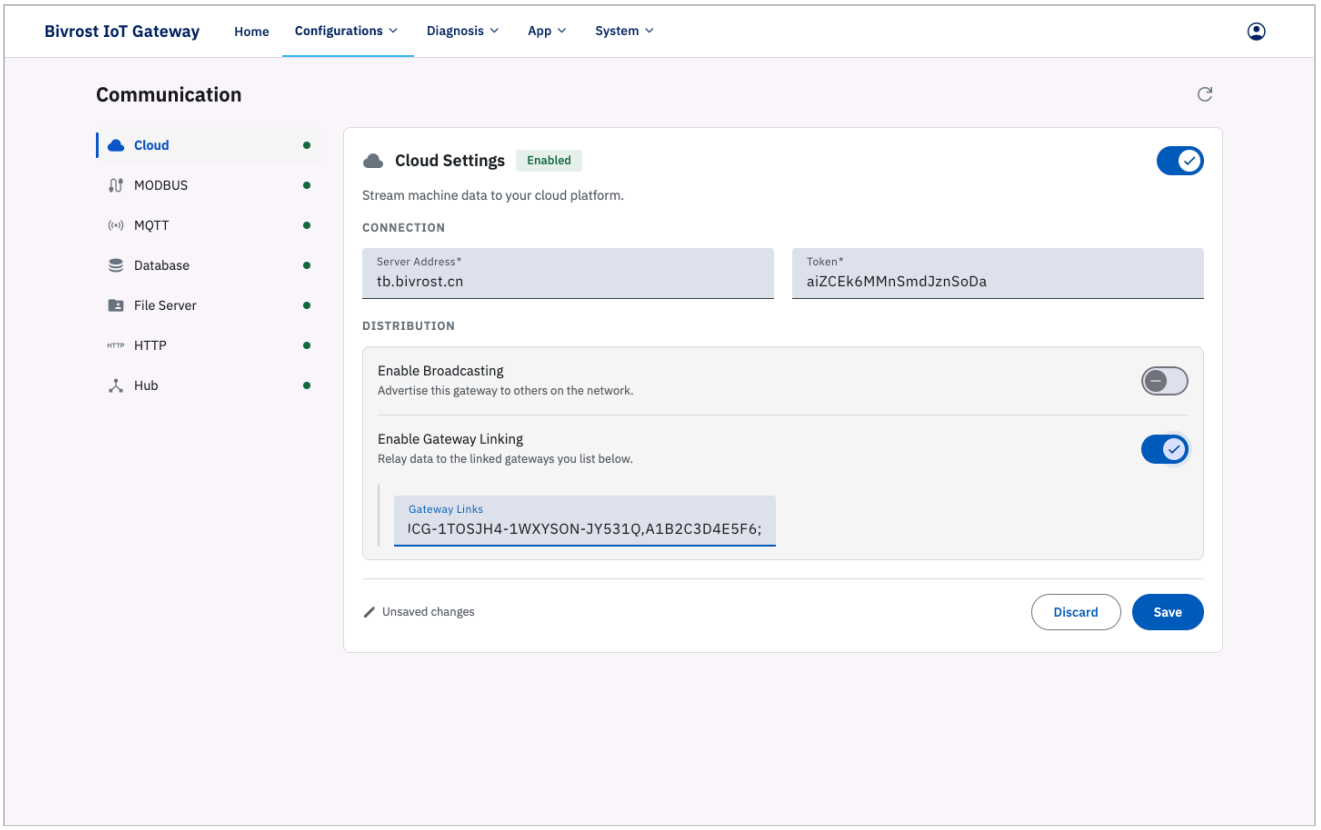


Once cloud communication is enabled, the server settings are complete and the automatic collection tasks of the target machines and groups are switched on (see 3.3.1.2. Task Settings and 3.4.1.2. Group Task Settings), task data is uploaded in real time to the designated standard cloud platform over a standard protocol, where it can be stored, analysed and shown on dashboards. Bivrost runs a standard cloud platform server at tb.bivrost.cn; contact support to arrange a trial (see *Cloud Platform Manual*).

- Enter the cloud platform address in **Broker Address**.
- Enter the token the cloud platform has assigned to the gateway in **Token**.
- With **Enable Broadcasting** on, the gateway broadcasts data through the cloud platform to the other gateways on that platform.
- With **Enable Gateway Linking** on, the gateway receives data broadcast through the cloud platform by the other gateways on that platform. Add the UID and token of each gateway you want to link to under **Gateway Links**, in the following format:

```
UID,token;
```

Separate multiple linked gateways with `;`.

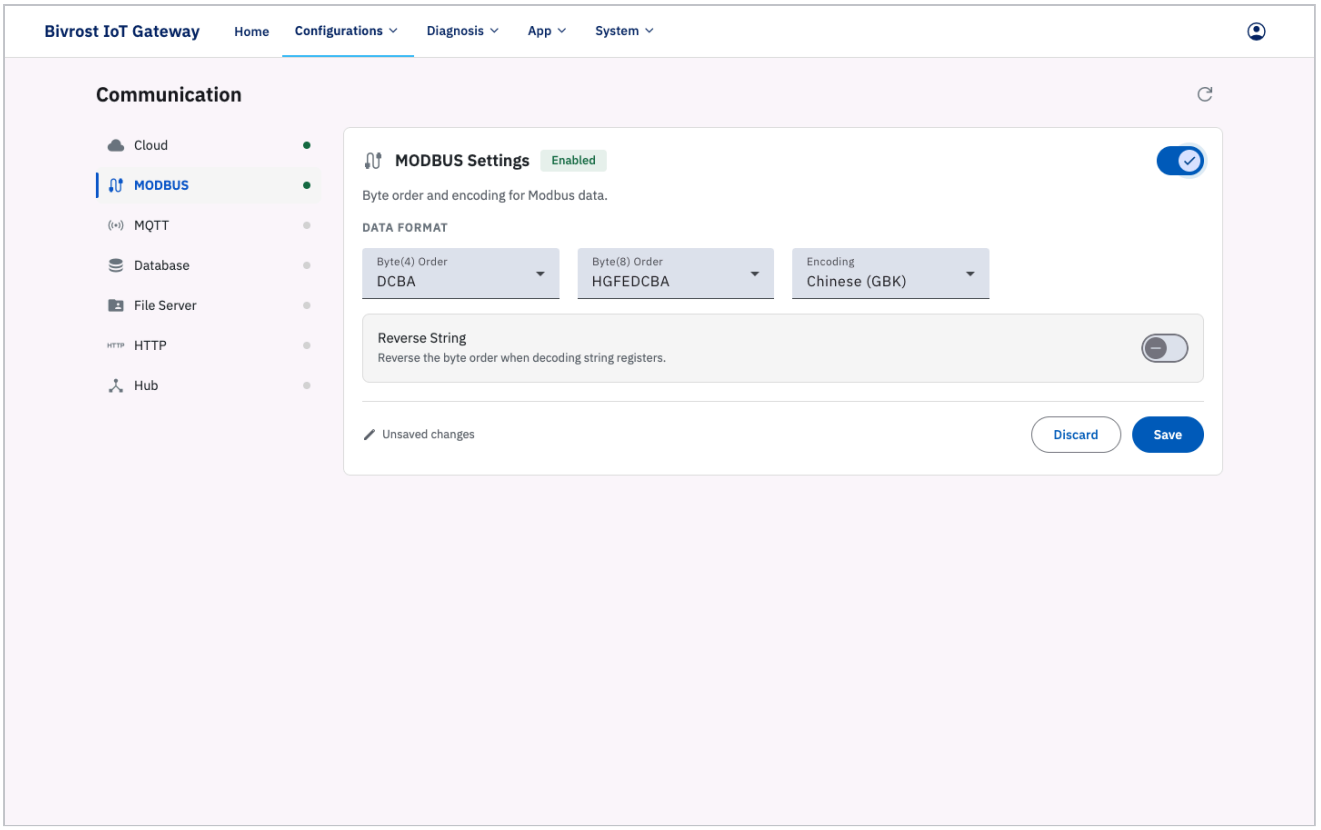


Note

When the settings are complete, click **Save**, then go back to Home and click **Restart Service** to apply the changes.

3.6.2. MODBUS Settings

Click the **Enable** switch to turn on MODBUS communication.



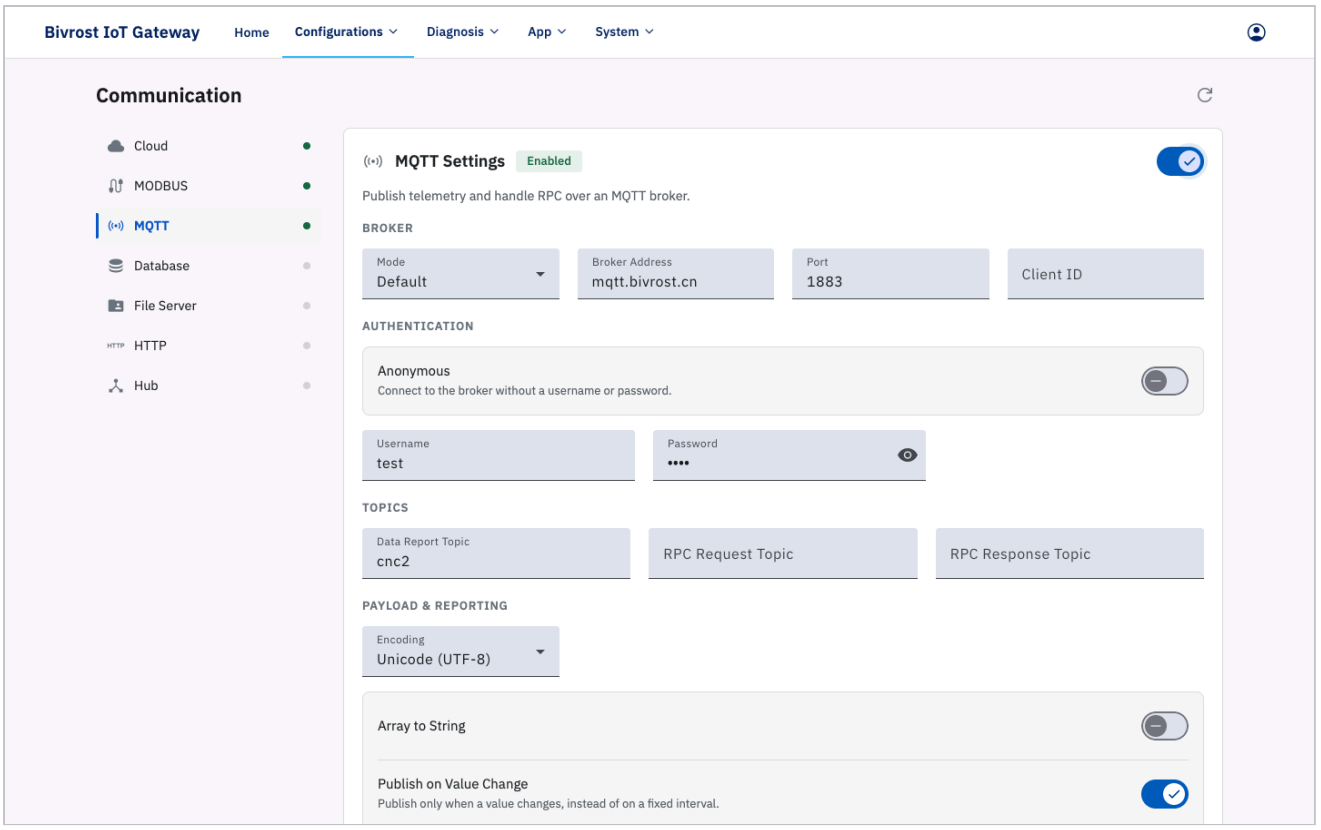
Once MODBUS communication is enabled and the automatic collection tasks of the target machines and groups are switched on (see 3.3.1.2. Task Settings and 3.4.1.2. Group Task Settings), the gateway uses the MODBUS protocol to store the task data in the corresponding address registers — see section 3, MODBUS Communication, of the *Communication Protocol*.

- **Byte(4) Order** selects the decoding format used in MODBUS communication for 32-bit data (long integers such as Int32, single-precision Float and any other type that occupies two register addresses). The default is “DCBA”.
- **Byte(8) Order** selects the decoding format used in MODBUS communication for 64-bit data (double-precision Double and any other type that occupies four register addresses). The default is “HGFEDCBA”.
- **Encoding** selects the string encoding used by the MODBUS protocol. The default is “Chinese (GBK)”.
- With **Reverse String** on, the character order of strings is reversed.

> **Note**
>
> When the settings are complete, click **Save**, then go back to Home and click **Restart Service** to apply the changes.

3.6.3. MQTT Settings

Turn on the **Enable** switch to start MQTT communication.



Once MQTT communication is enabled and the automatic collection tasks of the target machines and groups are switched on (see 3.3.1.2. Task Settings and 3.4.1.2. Group Task Settings), the gateway uses the MQTT protocol to convert the task data into JSON messages and publish them to the designated MQTT broker — see section 4, MQTT Communication, of the *Communication Protocol*.

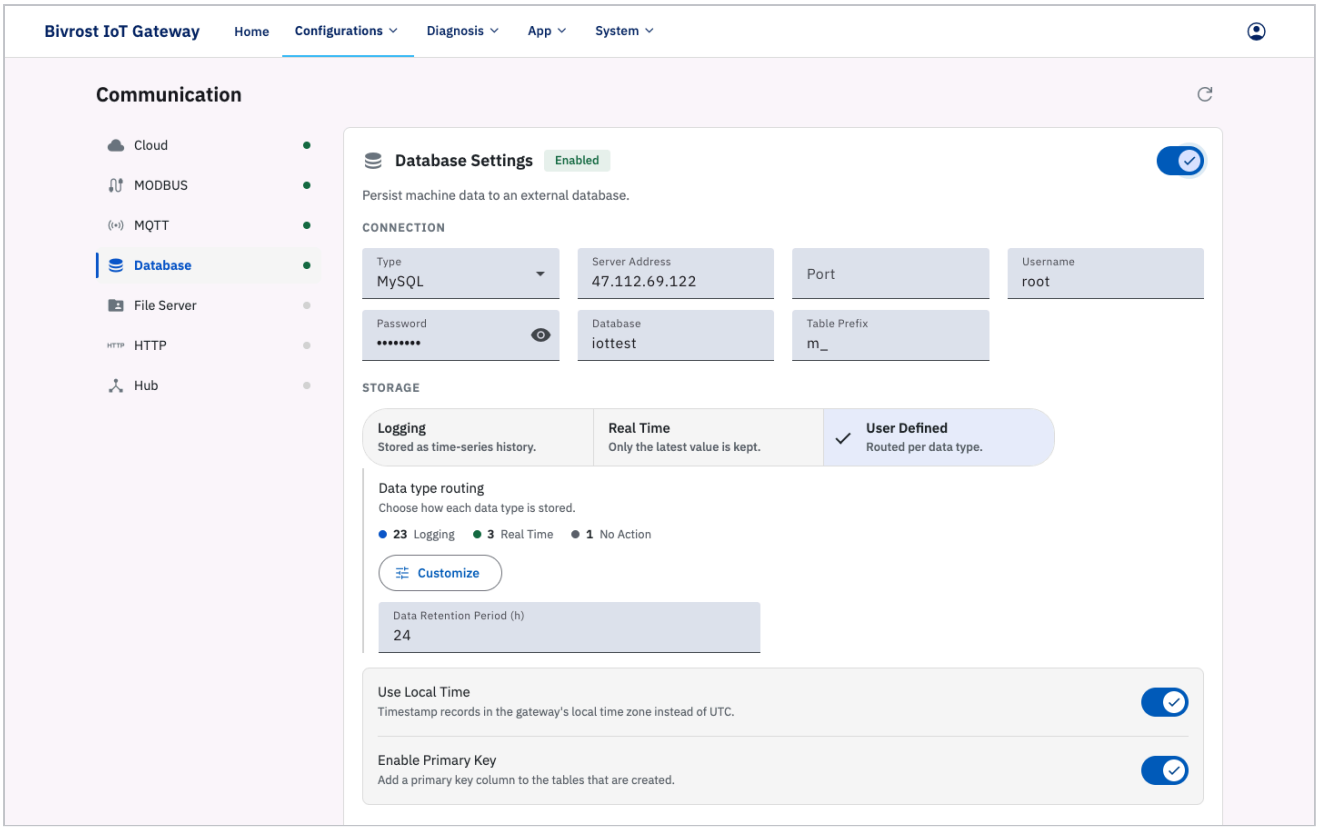
The MQTT settings are: Mode, Broker Address, Port, Client ID, Anonymous, Username, Password, Data Report Topic, RPC Request Topic, RPC Response Topic, Encoding, Array to String and Publish on Value Change.

- **Data Report Topic** is the topic an automatic collection task reports its result on over MQTT. The default is “r”.
- **RPC Request Topic** and **RPC Response Topic** are used by the RPC interface. Both are blank by default, which disables the RPC interface. Once they are set, the gateway subscribes to the RPC request topic and publishes the result of each request to the RPC response topic — see 4.2. RPC Interface of the *Communication Protocol*.
- With **Publish on Value Change** on, the automatic collection tasks enabled in the machine task settings and group task settings only upload a result when the collected value has changed.

> **Note**
>
> When the settings are complete, click **Save**, then go back to Home and click **Restart Service** to apply the changes.

3.6.4. Database Settings

Turn on the **Enable** switch to start database communication.

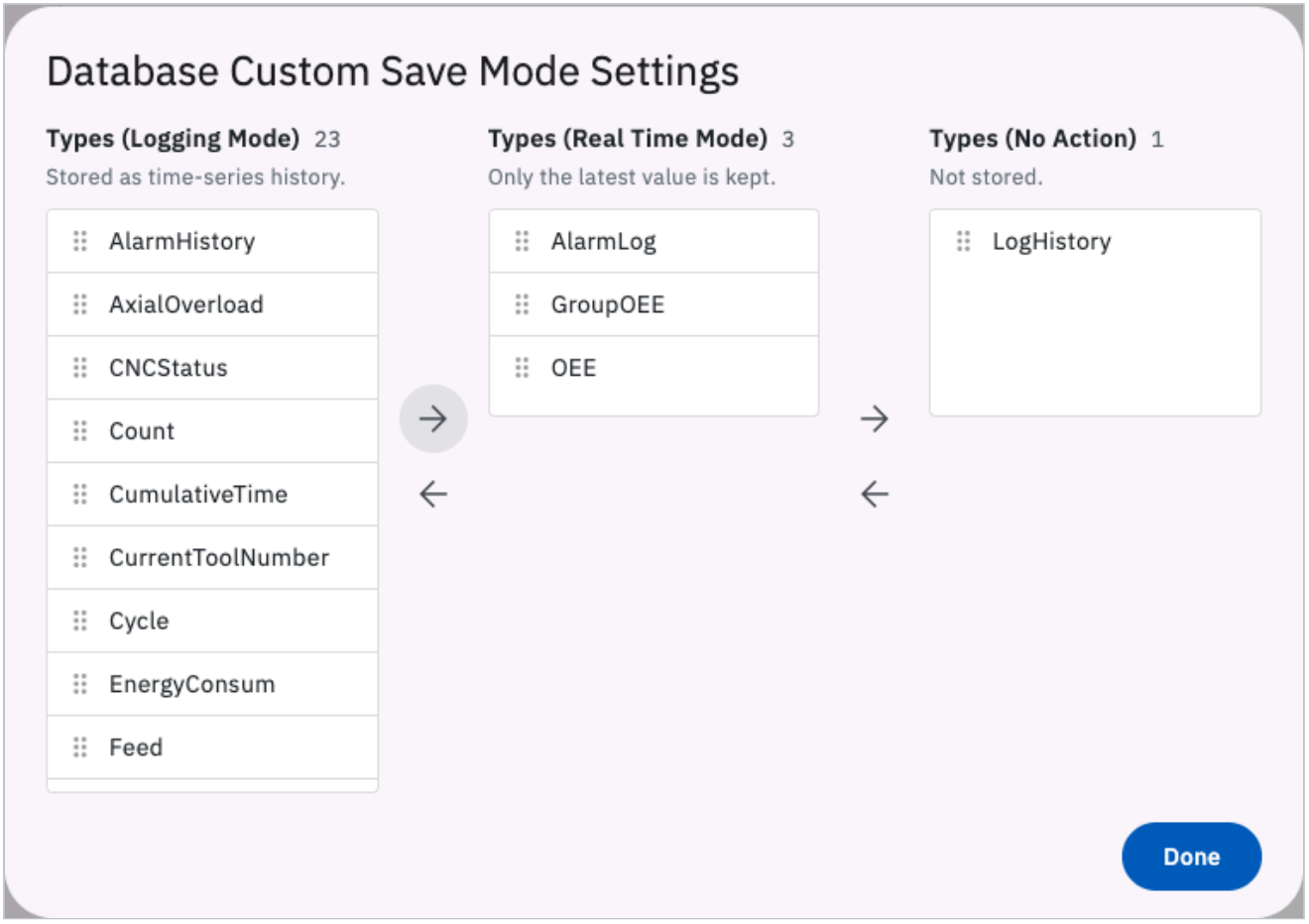


Once database communication is enabled and the automatic collection tasks of the target machines and groups are switched on (see 3.3.1.2. Task Settings and 3.4.1.2. Group Task Settings), the gateway writes the results of those tasks to the designated database. The database types currently supported are SQL Server, MySQL, PostgreSQL and InfluxDB v2.x. See section 5, Database Communication, of the *Communication Protocol*.

The database settings are: Type, Broker Address, Port, Username, Password, Bucket, Table Prefix, Storage Mode, Data Retention Period (h), Use Local Time, Enable Primary Key, Write on Value Change and so on.

- **Type** is the type of database: SQL Server, MySQL, PostgreSQL, InfluxDB v2.x and so on.
- **Broker Address** is the IP address of the server the database runs on.
- **Port** is the port of the server the database runs on.

- **Username** and **Password** are used to sign in to the database.
- **Bucket** is the name of the database.
- **Table Prefix** adds a prefix in front of the default table names.
- **Storage Mode** offers Log, Real Time, User Defined and so on.
    - **Log** mode: every time the gateway reads data from a machine it writes a matching record to the database. The database keeps the complete history.
    - **Real Time** mode: every time the gateway reads data from a machine it finds the matching record for that machine in the database and updates it with the latest data; no history is kept.
    - The default storage mode is **User Defined**: click the **Settings** button on the right and use the "Database Custom Save Mode Settings" dialog to put each individual task into Log mode or Real Time mode. In the dialog, the left column is **Types (Logging Mode)**, the middle column is **Types (Real Time Mode)** and the right column is **Types (No Action)** (not recorded). Drag an interface with the mouse into the mode you want, or click the left and right arrow buttons to move every interface on one side across to the other. Click anywhere outside the dialog to close it, then click **Save** on the page to store your custom settings. By default Alarm, Machine OEE and Group OEE are in Real Time mode and all other data is in Log mode.

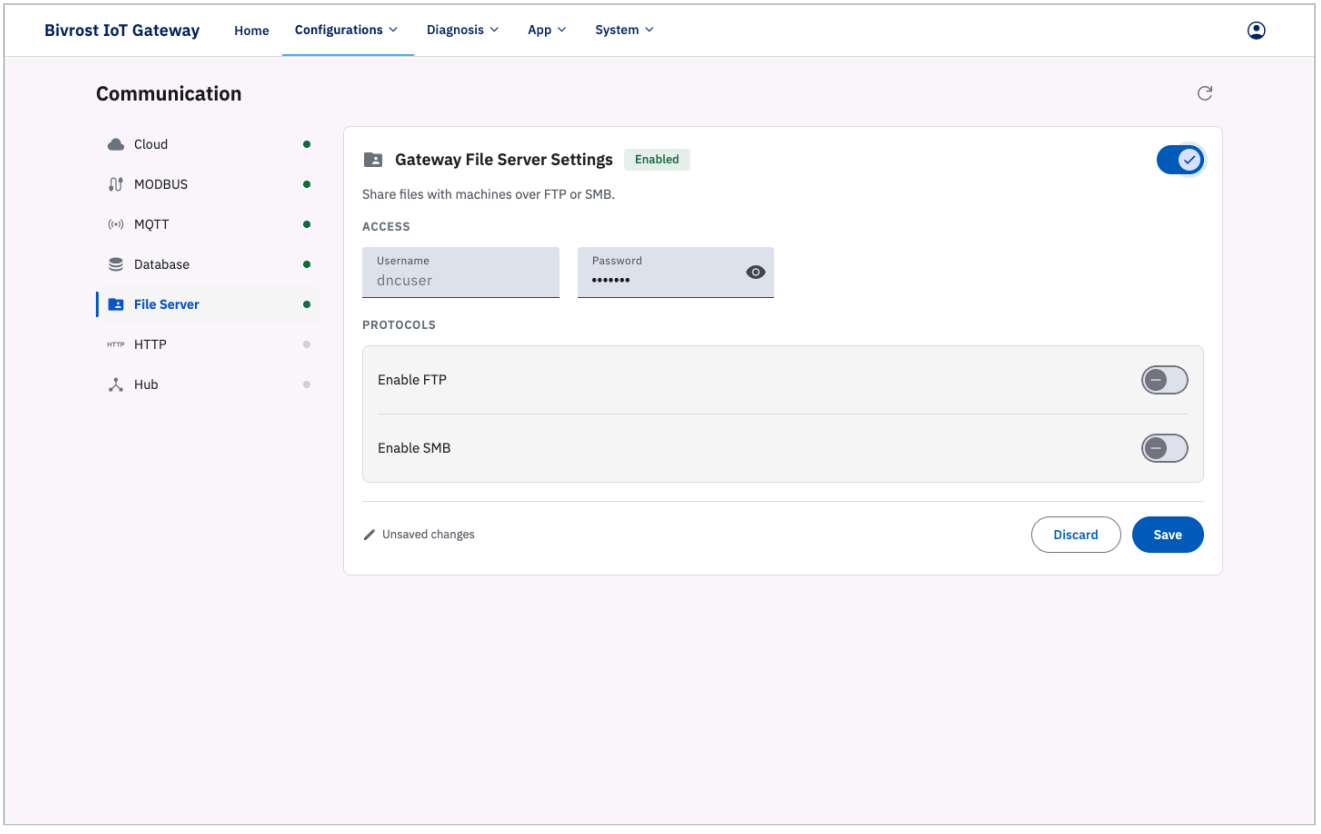


- **Data Retention Period (h)** is how long data is kept in the database, in hours. If it is set to x, the gateway runs a scheduled database cleanup after start-up and automatically deletes data older than x hours. The default is 0, which keeps all data.
- With **Use Local Time** on, data is written using the local time of the time zone set in 3.12. Settings; otherwise UTC is used.
- **Enable Primary Key** adds a primary key column to every table in the database.
- With **Write on Value Change** on, the automatic collection tasks enabled in the machine task settings and group task settings only write a result when the collected value has changed.

> **Note**
>
> When the settings are complete, click **Save**, then go back to Home and click **Restart Service** to apply the changes.

3.6.5. Gateway File Server Settings

Turn on the **Enable** switch to start the gateway file server. The gateway file server is a file server created locally on the gateway that machines can reach over FTP or as a shared folder. Once it is running, the File Server Type option in 3.3.1.3. DNC Settings can be set to “Gateway File Server”.



The username and password are shared by FTP and the shared folder. Both default to dnc_user. At present only the password can be changed.

Turn on **Enable FTP** to allow the gateway file server to be reached over FTP. The FTP address is:

```
ftp://iotgw or ftp://<gateway-IP>
```

Under the FTP home directory each machine has its own folder, named after the machine’s IP address.

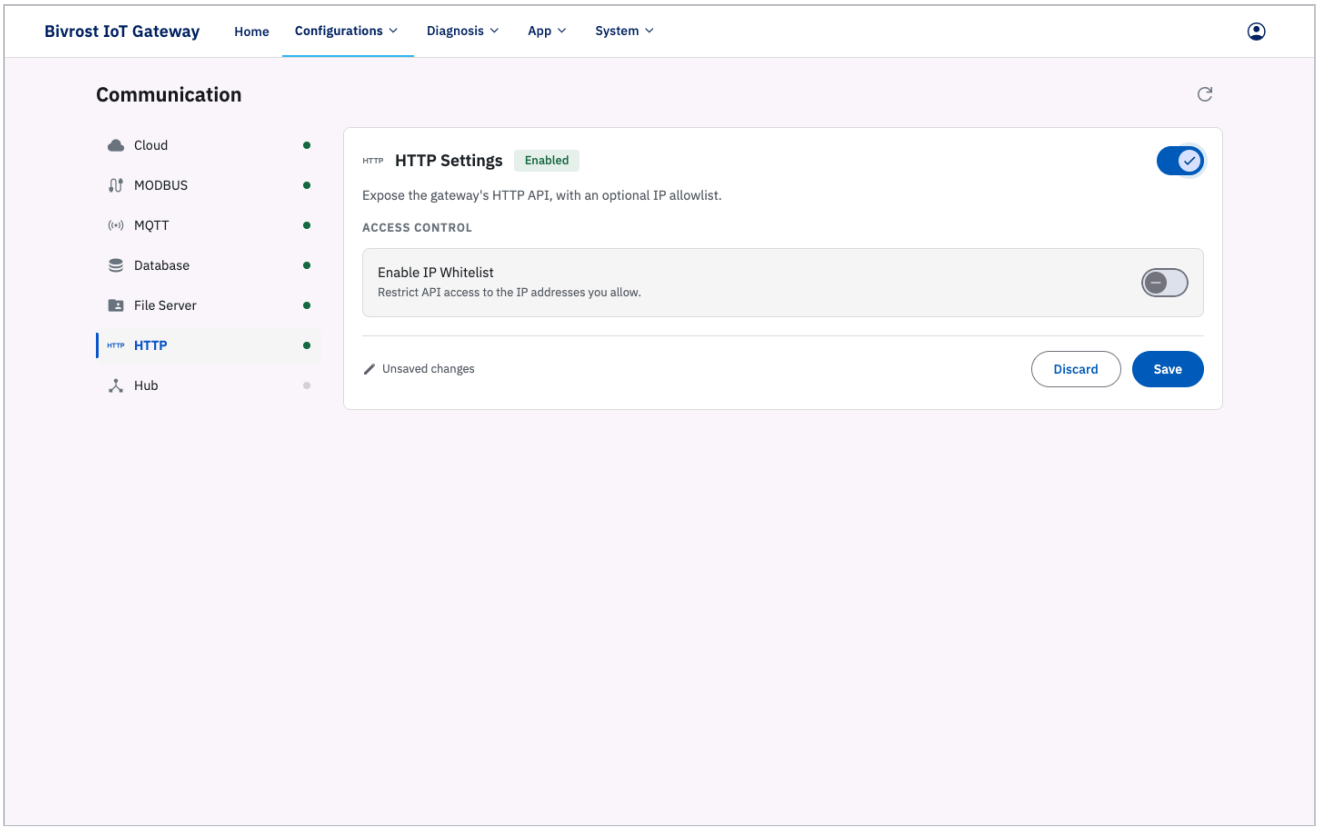
Turn on **Enable SMB** to allow the gateway file server to be reached as a shared folder. Each machine has its own shared folder, named after the machine’s IP address. The shared folder address is:

```
\\iotgw\<machine-IP> or \\<gateway-IP>\<machine-IP>
```

> **Note**
>
> When the settings are complete, click **Save**, then go back to Home and click **Restart Service** to apply the changes.

3.6.6. HTTP Settings

Turn on the **Enable** switch to start the HTTP service.

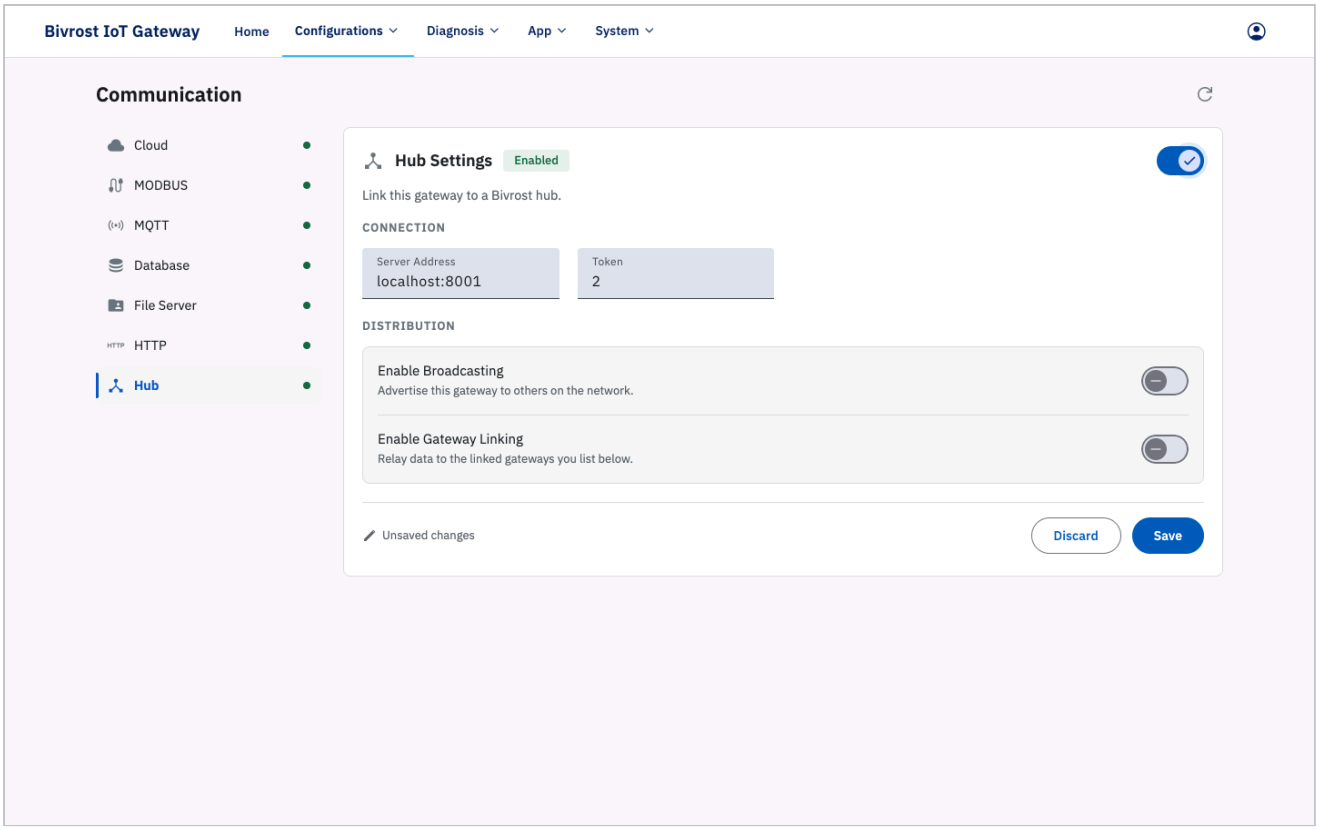


With **Enable IP Whitelist** on, all API requests except those with valid JWT authentication are restricted to whitelisted IP addresses. That is, the login endpoint is not restricted by the whitelist, and requests authenticated with a JWT after login skip the whitelist check; requests authenticated with a SecretKey must still pass the whitelist check. The **Whitelist** can hold several IP addresses, separated by “;” .

> **Note**
>
> When the settings are complete, click **Save**, then go back to Home and click **Restart Service** to apply the changes.

3.6.7. Hub Settings

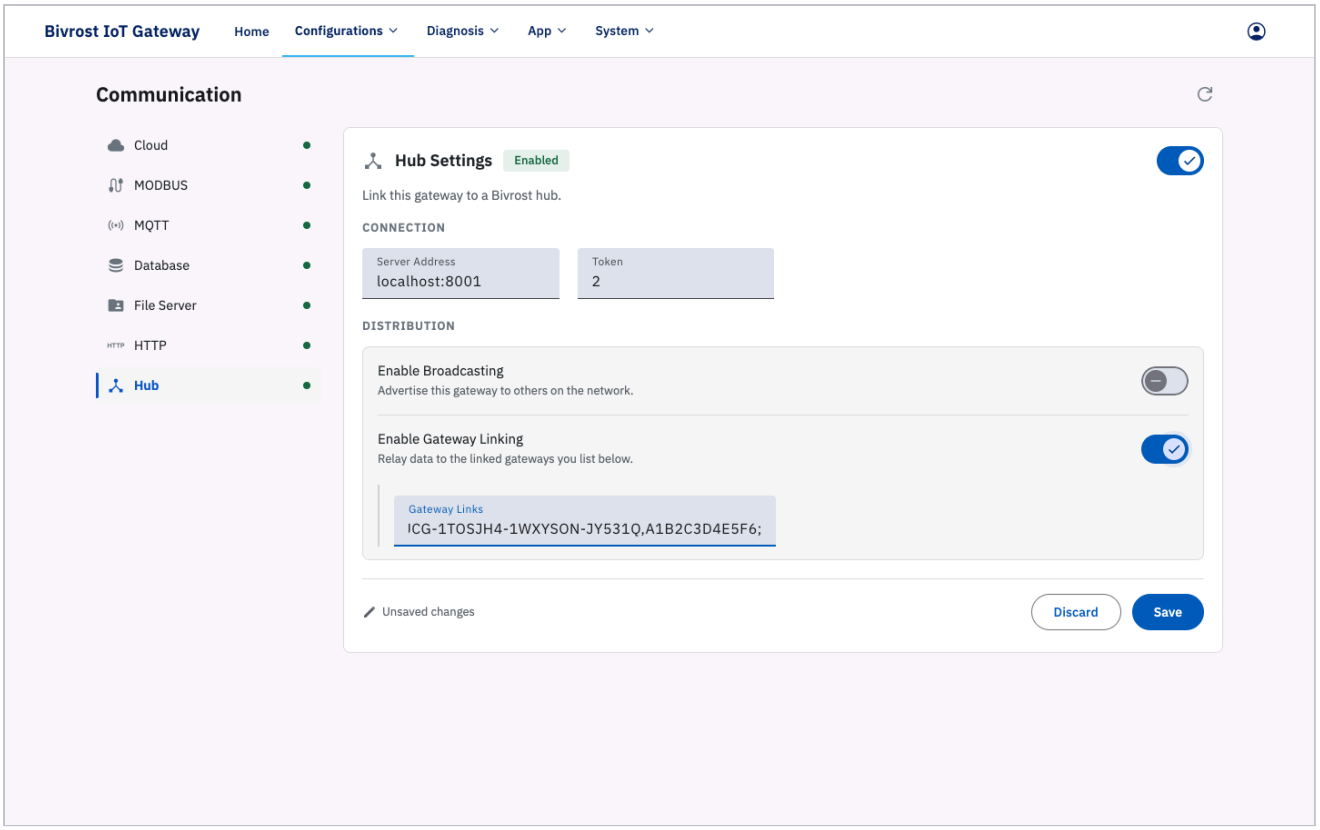
Turn on the **Enable** switch to start the Hub service. A Hub server is used to reach the gateway’ s interfaces remotely, so that configuration can be changed remotely and gateways on different sites can exchange data. Contact support to have one deployed.



- Enter the Hub server address in **Broker Address**.
- Enter the token the Hub server has assigned to the gateway in **Token**.
- With **Enable Broadcasting** on, the gateway broadcasts data through the cloud platform to the other gateways on that platform.
- With **Enable Gateway Linking** on, the gateway receives data broadcast by other gateways through the Hub server. Add the UID and token of each gateway you want to link to under **Gateway Links**, in the following format:

```
UID,token;
```

Separate multiple linked gateways with `;`.



> **Note**
>
> When the settings are complete, click **Save**, then go back to Home and click **Restart Service** to apply the changes.

3.6.8. MCP Settings

Turn on the **Enable** switch and click **Save** to start the MCP service. The MCP (Model Context Protocol) server exposes machine data, data analysis and gateway status as “tools” for MCP-capable AI clients (such as Claude Code and Claude Desktop), so machines can be queried in natural language without calling the interfaces by hand.

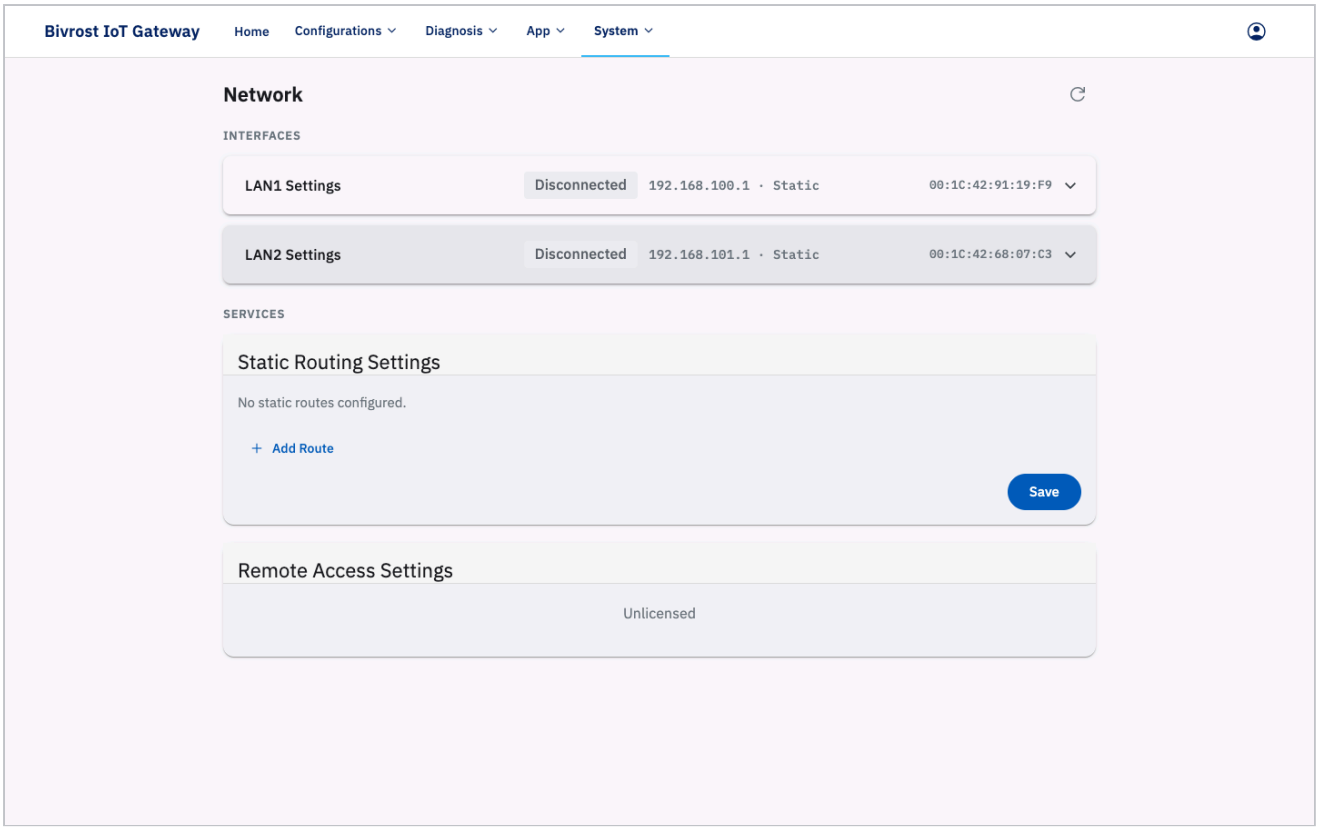
Endpoint shows this gateway’s MCP server address (for example `http://192.168.100.1/mcp`), for use in the MCP client’s configuration. It is read-only.

The MCP service is disabled by default; while it is off, that address returns HTTP 404. It currently exposes 33 read-only tools — anything involving writes, machine control or program transfer has no MCP tool. Authentication and access control follow the HTTP interface settings (secret keys, IP whitelist, authorized APIs) and need no separate configuration on this page. For the full tool list, the authentication methods and client configuration examples, see 4.4. MCP Service.

> **Note**
>
> Unlike the other communication methods, the MCP switch takes effect as soon as you click **Save** — there is no need to go back to Home and restart the service.

3.7. Network

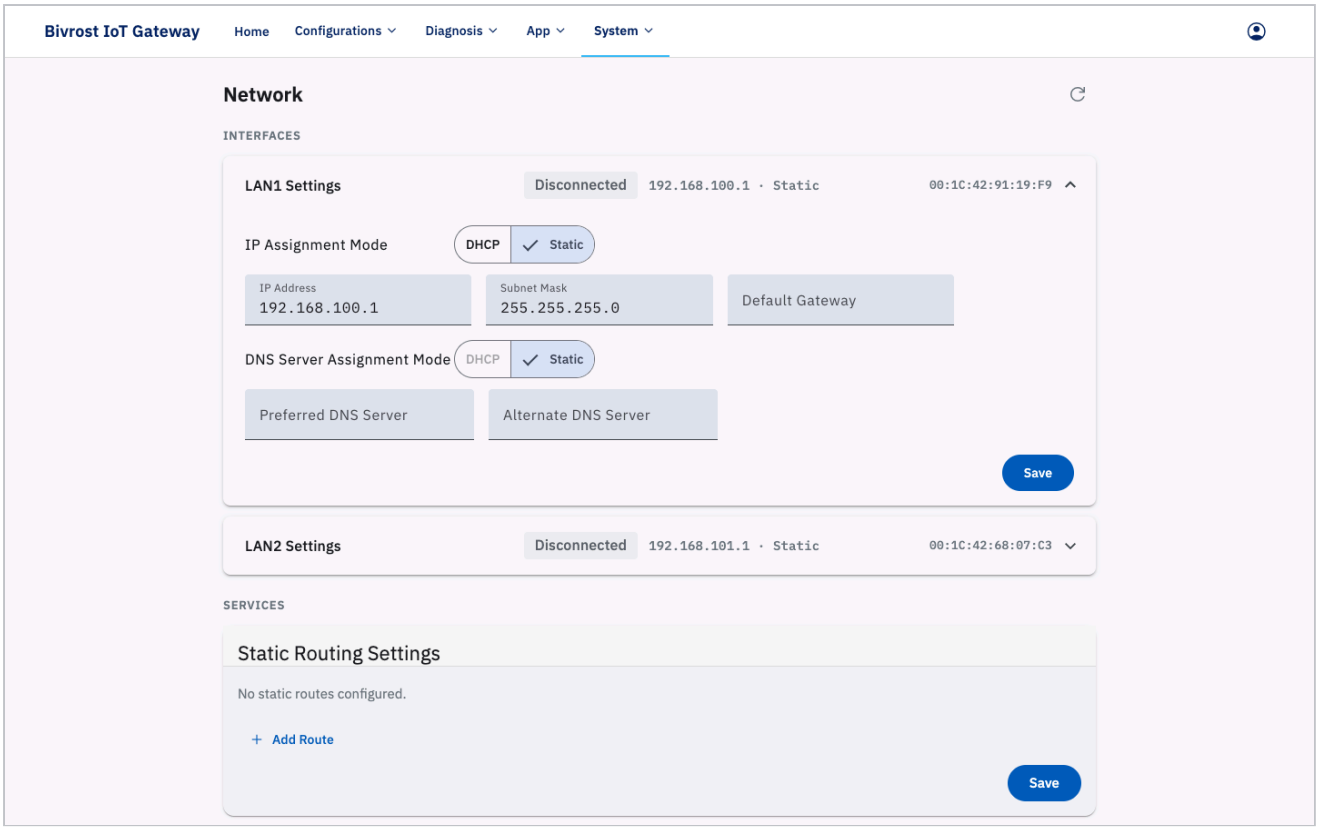
The **Network** page is split into two parts: “Interfaces” (LAN1, LAN2 and the wireless adapter) and “Services” (Static Routing Settings, Remote Access Settings). Click an interface card to expand its settings.



3.7.1. Wired Network

The “Wired Network” section shows the current connection status of the LAN1 port. “Connected” means the LAN adapter has detected a device at the other end of the cable; it does not guarantee that the device can be pinged. You can change the Connection Type of the gateway’s LAN1 port, setting the IP Assignment Mode to DHCP (obtained automatically) or Static (entered manually). LAN1 is normally set to Static, in which case you can edit the IP Address, Subnet Mask, Default Gateway and DNS server settings. The default gateway and DNS server only need to be changed when the company network is restricted; otherwise leave them at their defaults. When you are done, click **Save** to apply the settings.

> **Note**
>
> The settings take effect as soon as you click **Save** — no service restart is required. If you were connecting to the gateway on its LAN1 IP address, you must use the new IP address after changing it.



Once the LAN2 Settings option has been enabled under Settings, LAN2 Settings appears below LAN1 Settings and you can change the Connection Type of the LAN2 port; see 3.12. Settings for details.

3.7.2. WiFi Settings

The gateway is fitted with a wireless adapter and can connect to a WiFi network (models on which the wireless adapter is unavailable do not show this section).

While WiFi is disconnected, click the “WiFi Name” field to scan automatically for nearby networks. You can type a name to narrow the list, then click the network you want to join. For a hidden network, type the full WiFi name manually.

Enter the “WiFi Password” and click **Connect**. If the connection succeeds, the “Status” field shows “Connected: [WiFi name][signal strength]” and the **Connect** button changes to **Disconnect**. Unless you click **Disconnect**, the gateway reconnects automatically whenever it

detects that network again. Clicking **Disconnect** drops the current network and stops the gateway from reconnecting to it automatically.

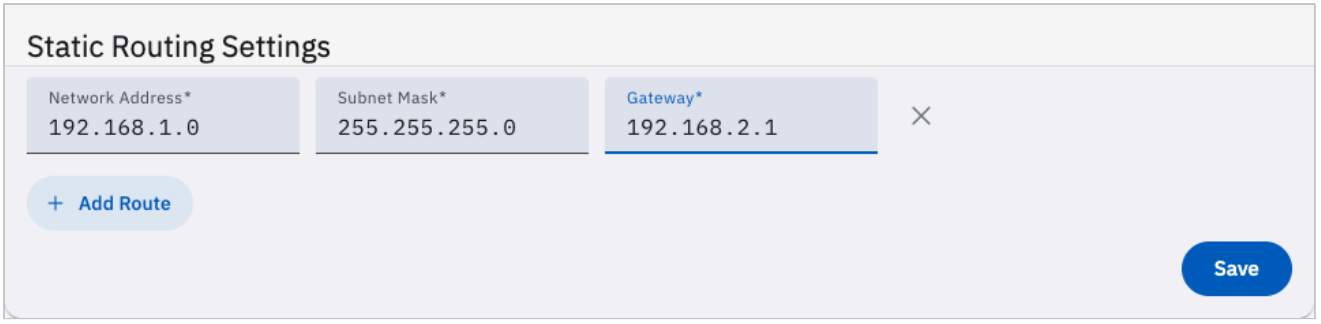
Once connected, click **Configure** to open the "WiFi Settings" dialog. As in 3.7.1. Wired Network, you can change the WiFi IP Address, Subnet Mask and other settings.

3.7.3. Static Routing Settings

You can add static routes here. The route format is:

```
IP network address 1,subnet mask 1,gateway IP address 1;IP network
address 2,subnet mask 2,gateway IP address 2;
```

Separate multiple routes with `;`.



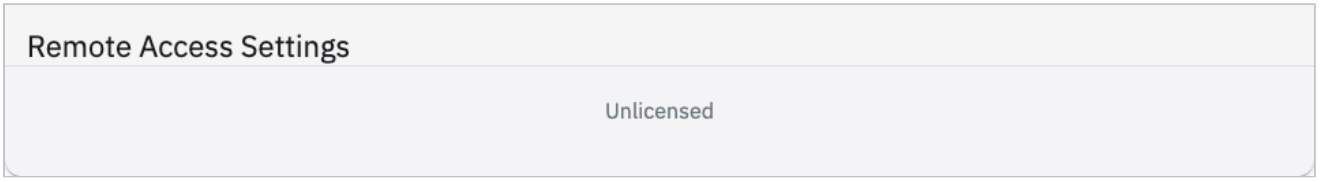
3.7.4. Remote Access Settings

Once remote access is configured, connecting to a remote server provides the following:

1. Remote access to the gateway from outside the local network.
2. Bridging of the LAN1 or LAN2 network, so that debugging software can connect to a machine remotely for commissioning.

Checking the remote access configuration takes a while; the status reads "Detecting" while it runs, as shown below.

This feature is not enabled by default and shows the message below. Contact customer support if you need it enabled.



Once the feature has been enabled, the status is “Disconnected” until it is configured for the first time, as shown below.

Click **Configure** and set up the remote server in the configuration dialog: enter the server address, password and bridge target, then click Confirm. After changing the configuration, you must reconnect to the remote server for it to take effect.

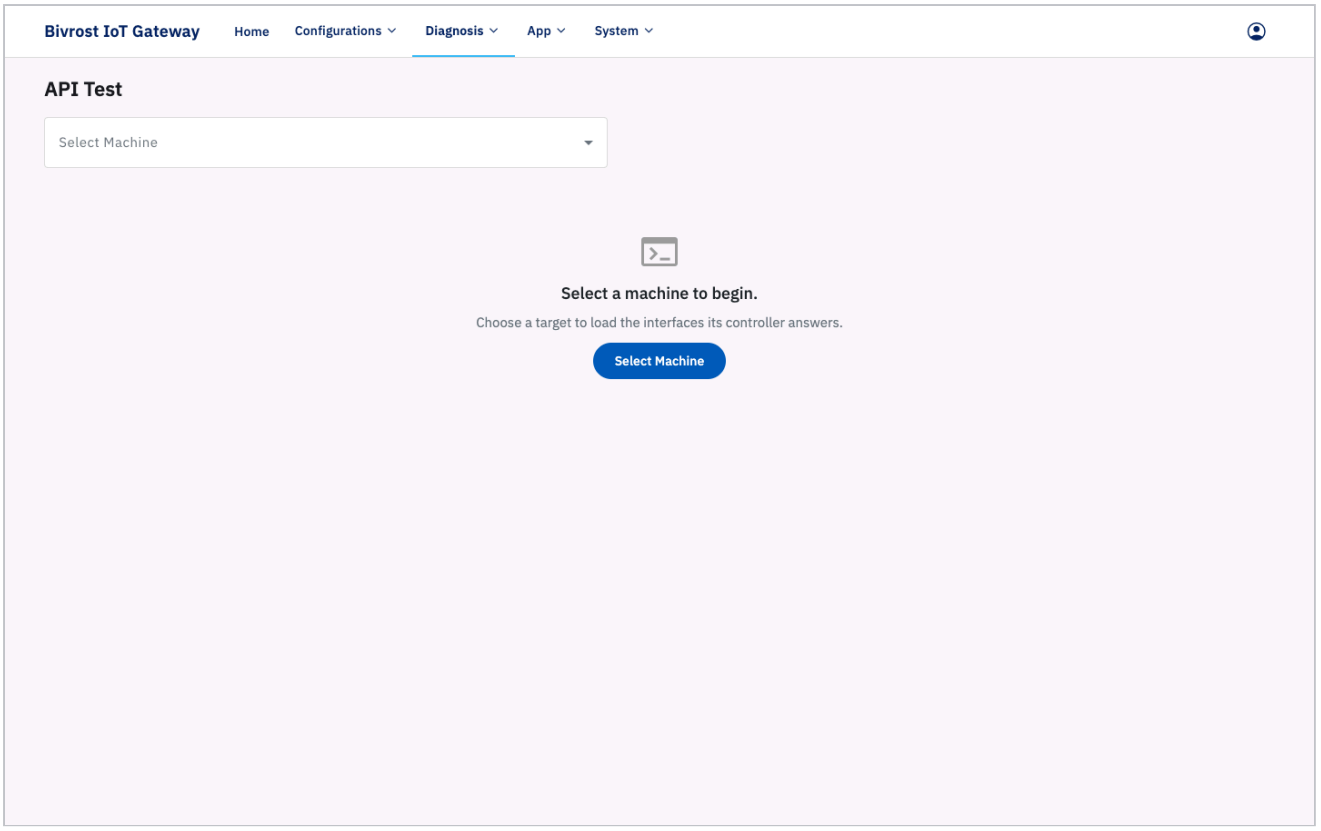
Click the **Connect** button; the gateway starts connecting to the remote server.

Once connected, the gateway connects to the remote server automatically the next time it comes online, as shown below. Click the **Disconnect** button to drop the connection to the remote server immediately and stop it from reconnecting automatically next time.

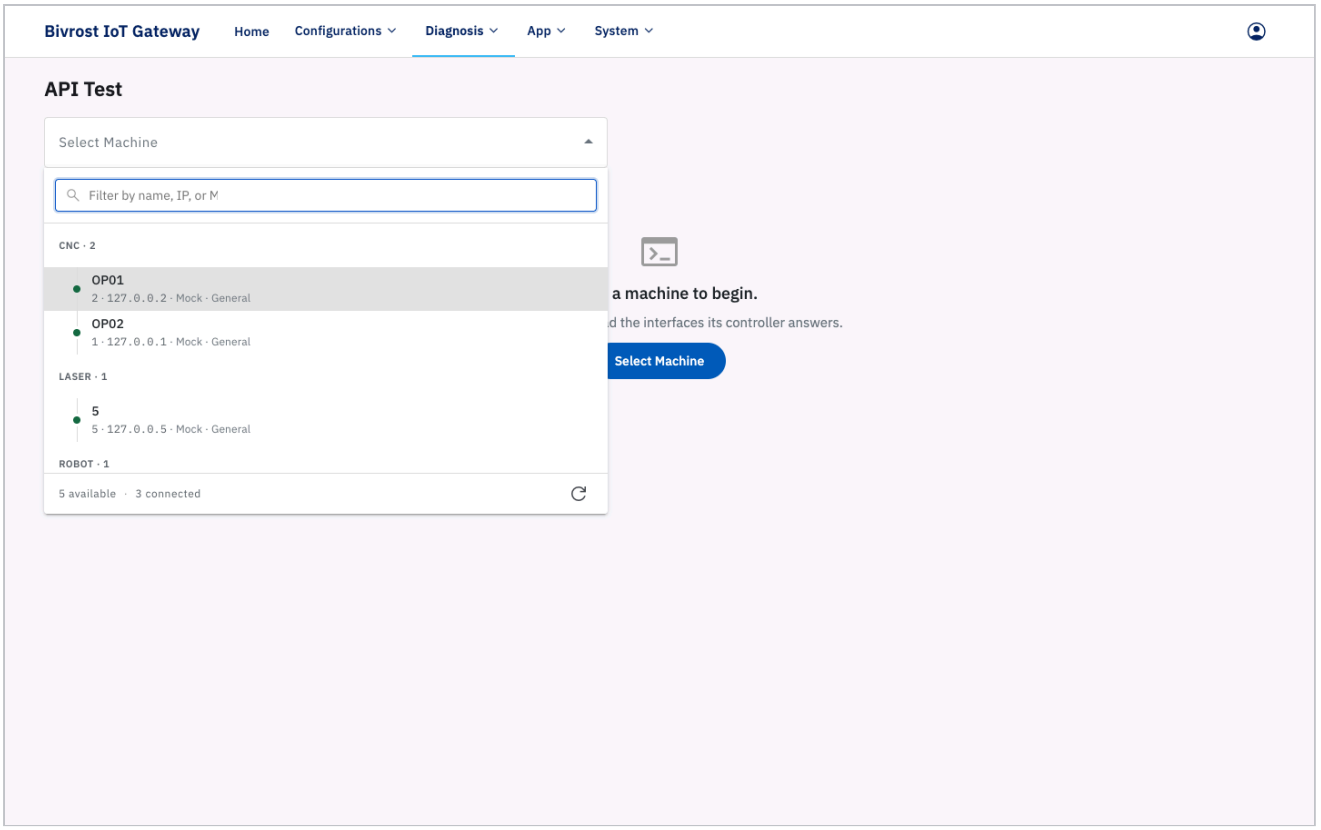
3.8. API Test

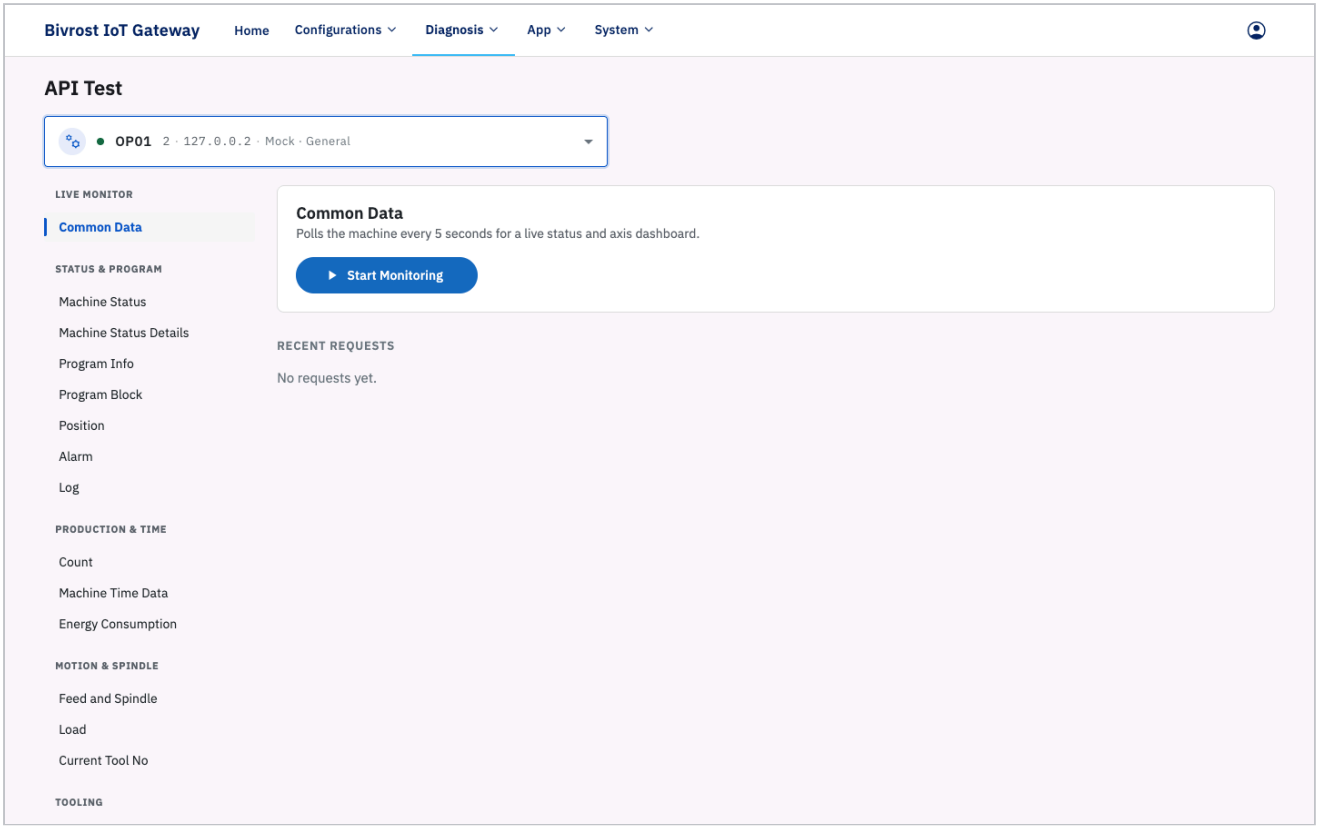
This page exposes a selection of read and write interfaces so you can verify them before going live. Full descriptions of every interface on this page can be found under 2.5.1. Direct Read/Write in the *Communication Protocol*.

Before running an API test, if you have changed any settings on **Machines**, **Groups**, **Tasks** or **Communication**, click **Restart Service** on **Home** first.



In the **Select Machine** box at the top, pick a machine that is activated on the **Machines** page, then pick the HTTP interface you want to test from the interface list (**Common Data** by default). Click **Monitoring/Send** to retrieve data from that interface on that machine.

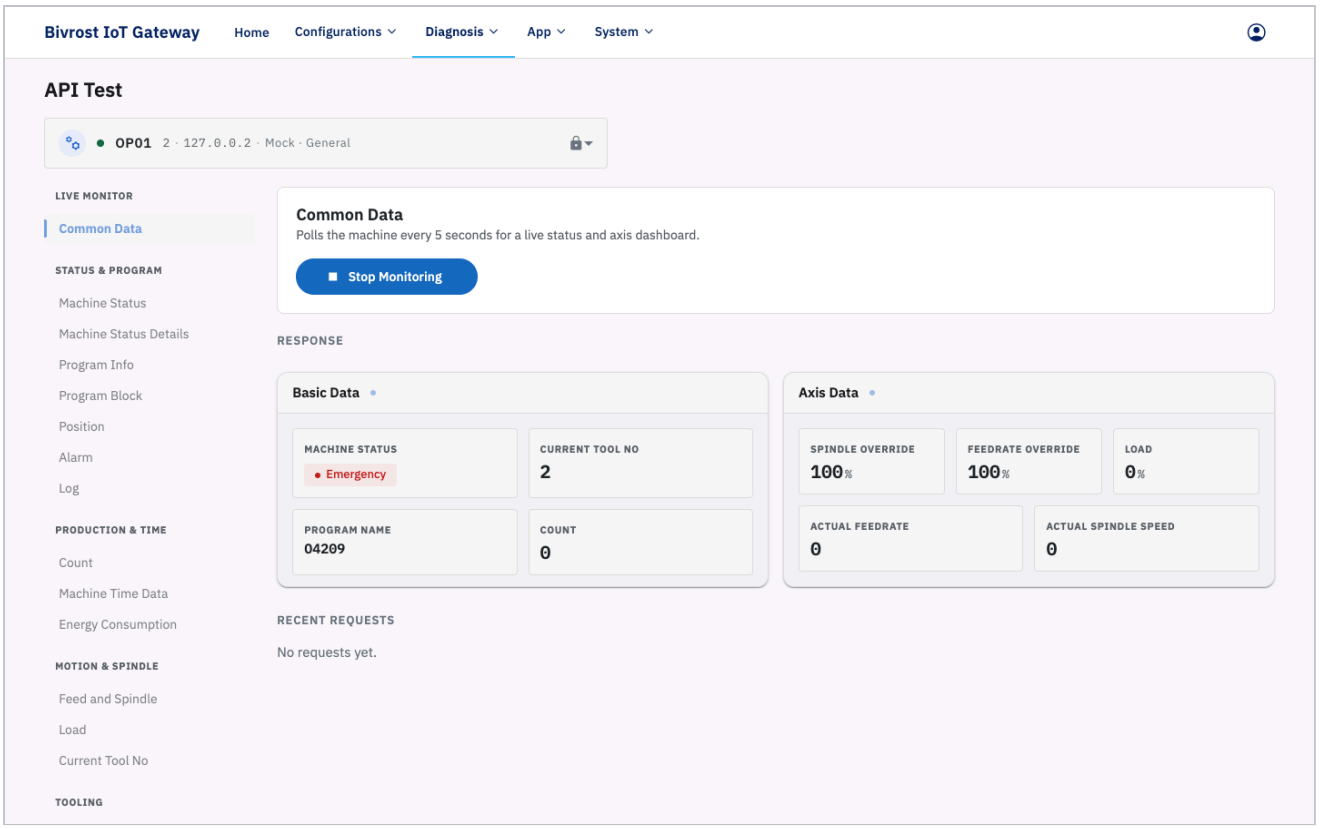




3.8.1. Common Data Interface

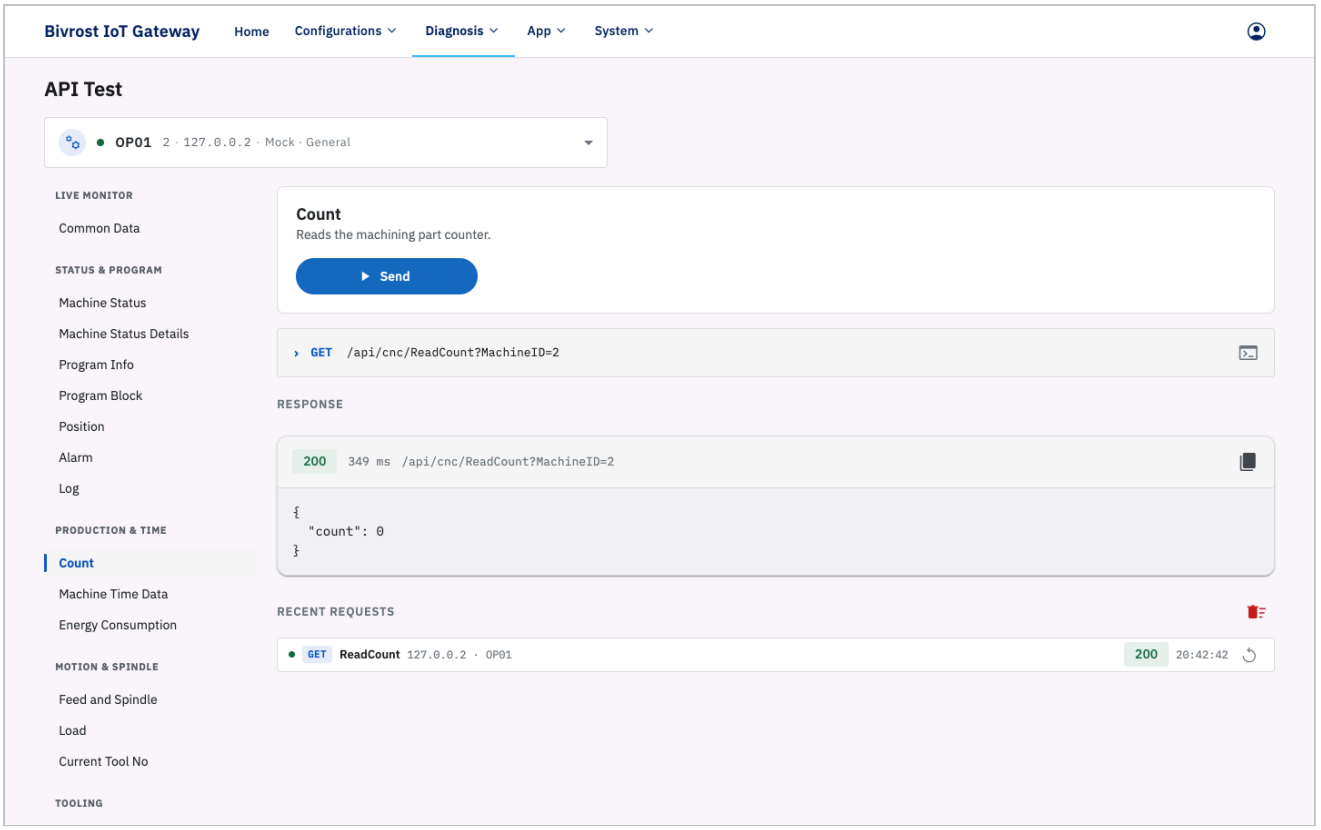
Monitoring common data polls a set of frequently used interfaces at a regular interval (roughly every 5 seconds) — Machine Status, Program Info, Current Tool No, Count, Alarm and so on —

and refreshes the data as shown below. Click **Stop Monitoring** to leave monitoring.



3.8.2. Read Data Interfaces

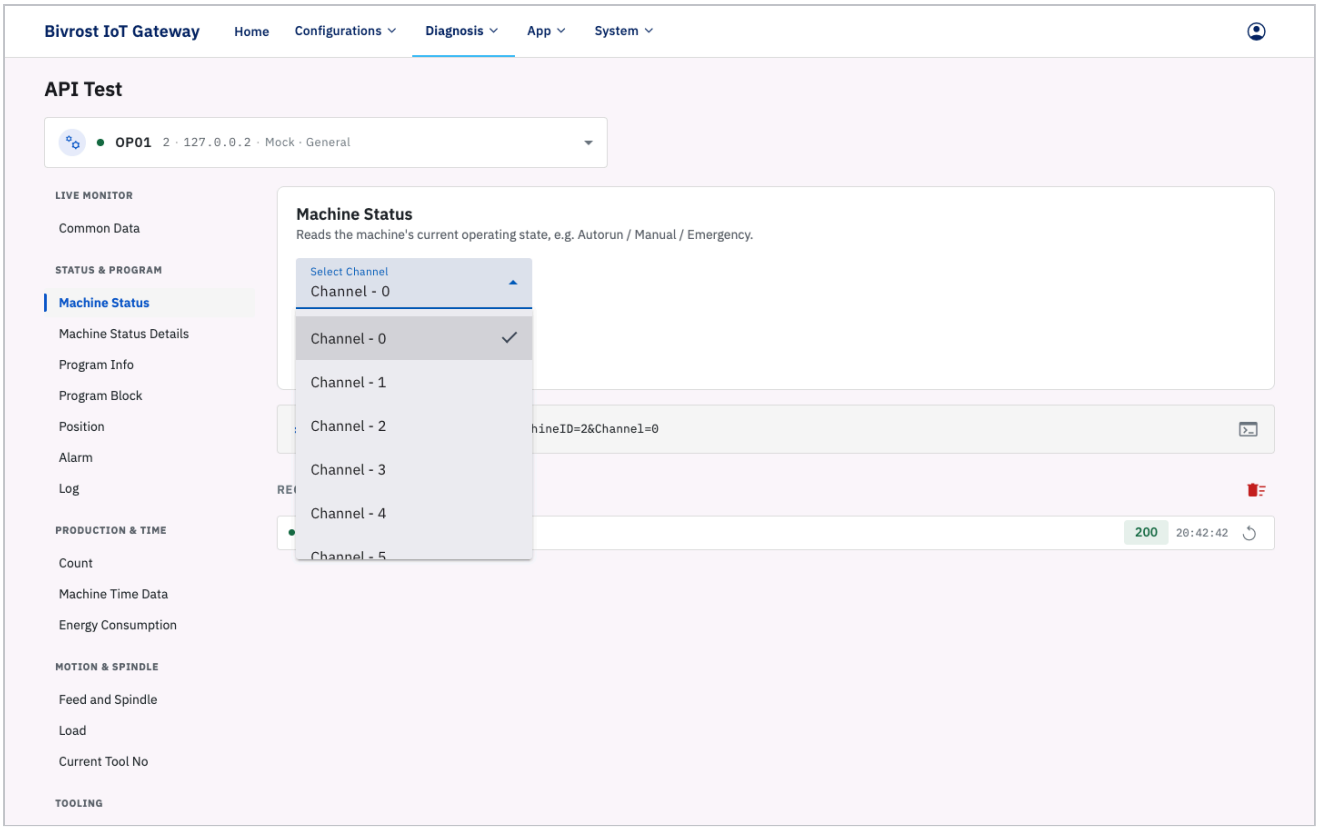
Apart from the **Common Data** interface and the **Write PLC Data** and **Write Offset Data** interfaces, every interface is a read interface. Send a request on a read interface — the **Count** interface, for example — and you get the result shown below. The **Count** interface returns the machine's part count. The line below that begins with `/api/cnc/` is the HTTP interface address. The result is inside `{}`, where "count" is the name and 2806 is the value for that name. For a detailed description of each interface, see the corresponding entry under 2.5.1. Direct Read/Write in the *Communication Protocol*.



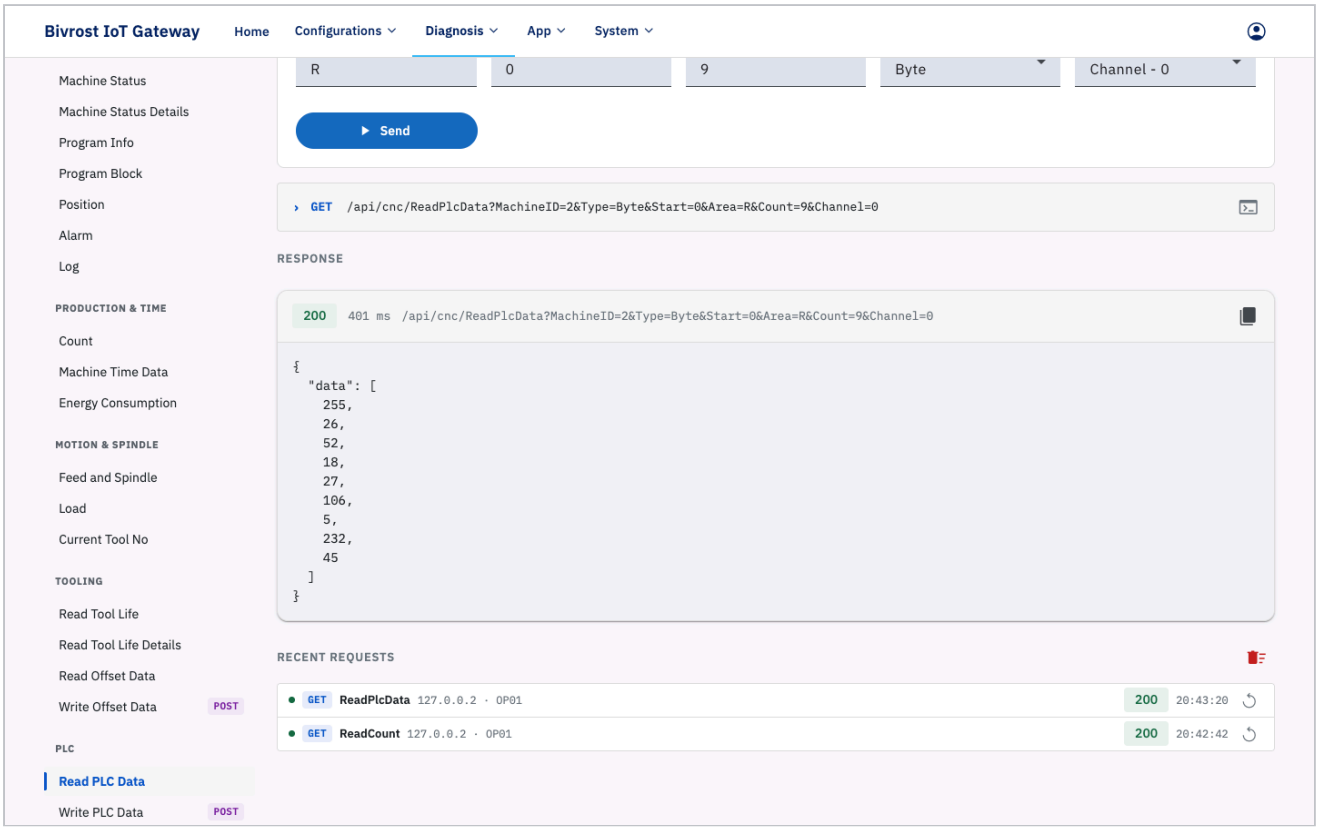

```
/api/cnc/ReadCount?MachineID=2118

{
  "count": 2806
}
```

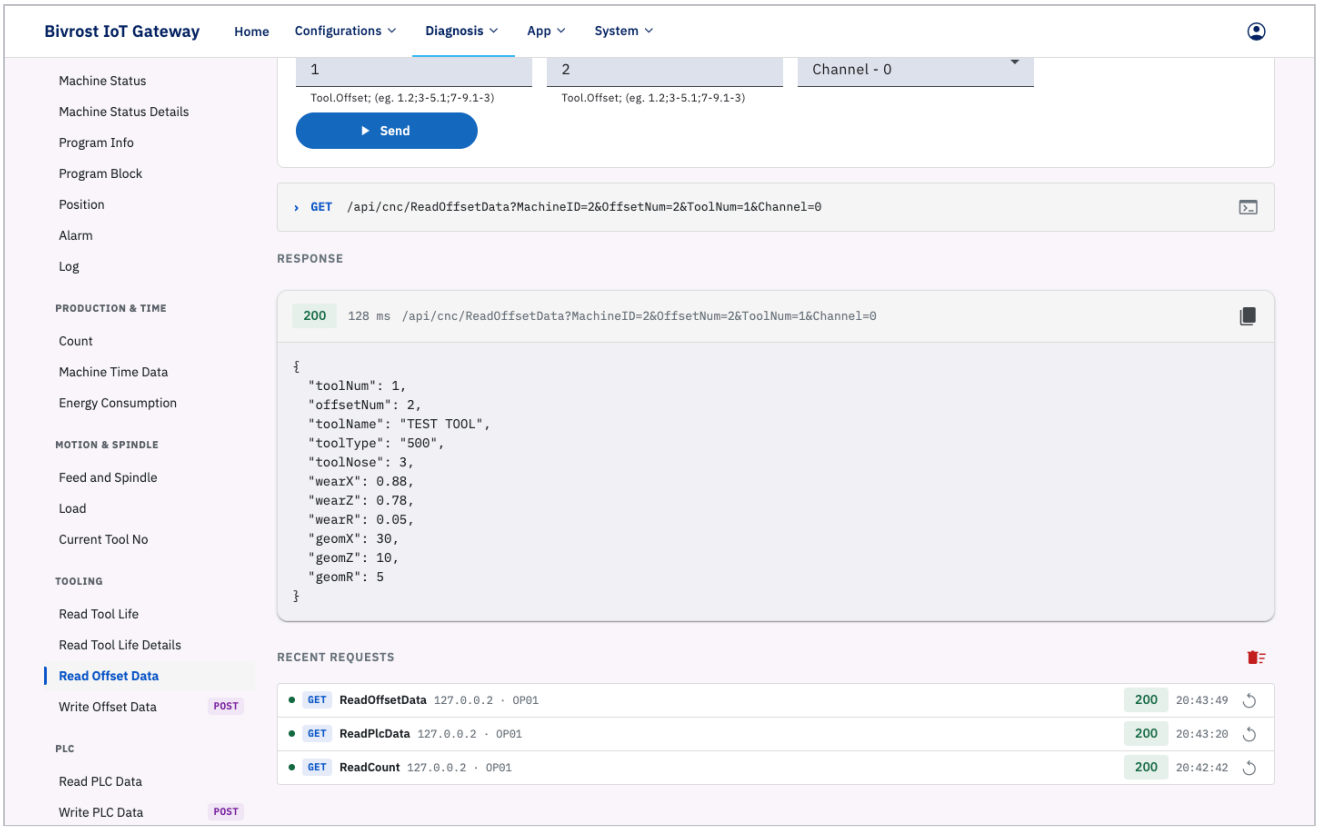
Some interfaces support multi-channel machines and can return data for a specific channel number. The default is channel 0, the main channel. On a single-channel machine, leave it at channel 0. The example below reads the status of a specific channel through the **Machine Status** interface.



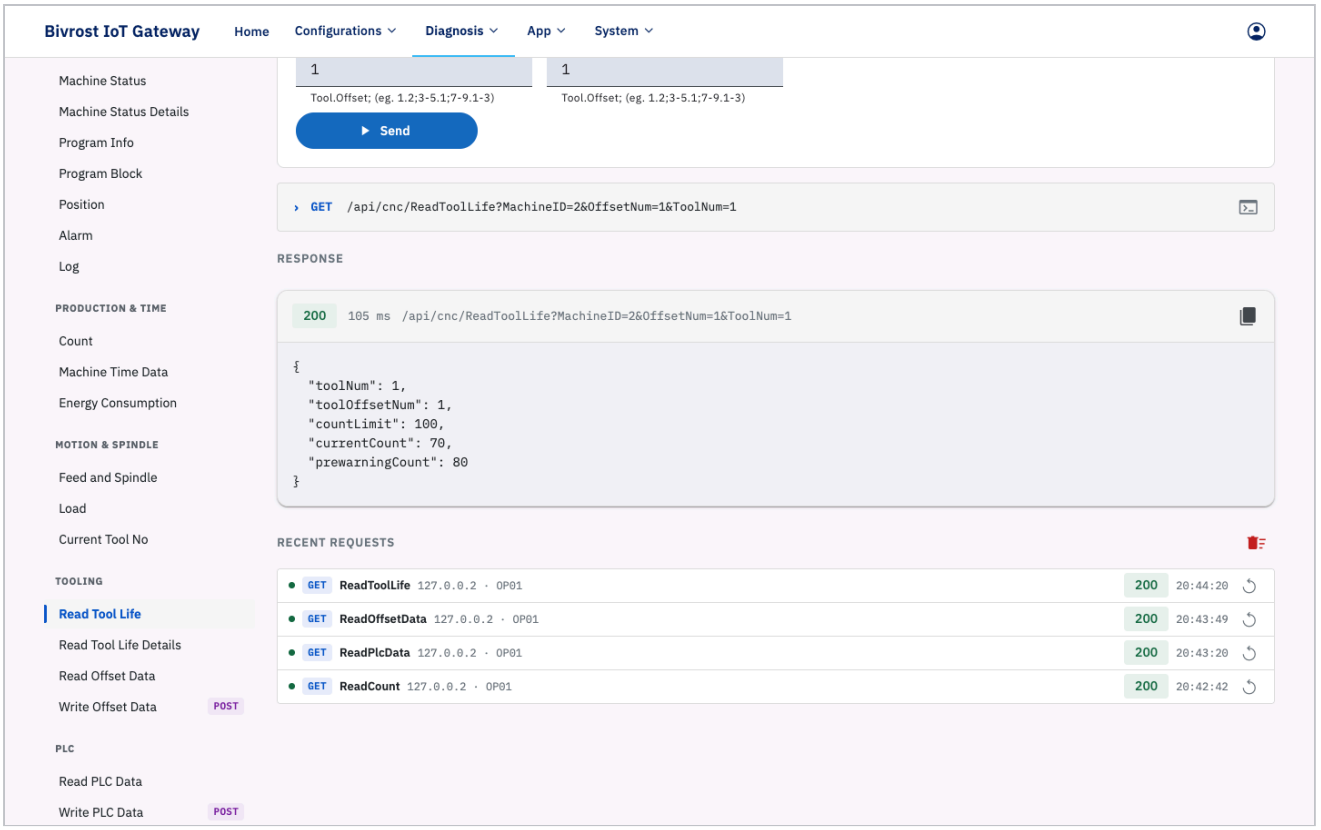
The **Read PLC Data** interface needs additional inputs such as **Area**, **Start Address**, **Data Count** and **Data Type**. See 4.2.1. PLC Data Task and 2.5.1.18. readPlcData — Read PLC Data in the *Communication Protocol*.



The **Read Offset Data** interface needs inputs such as the **Offset Number**; see 2.5.1.12. readOffsetData — Read Offset Data in the *Communication Protocol*.



The **Read Tool Life** and **Read Tool Life Details** interfaces need different inputs depending on the machine's controller model. In this example the controller is a Fanuc, so the tool's **Group Number** and **Tool Index** within that group are required; see 2.5.1.21. readToolLife — Read Tool Life in the *Communication Protocol*.

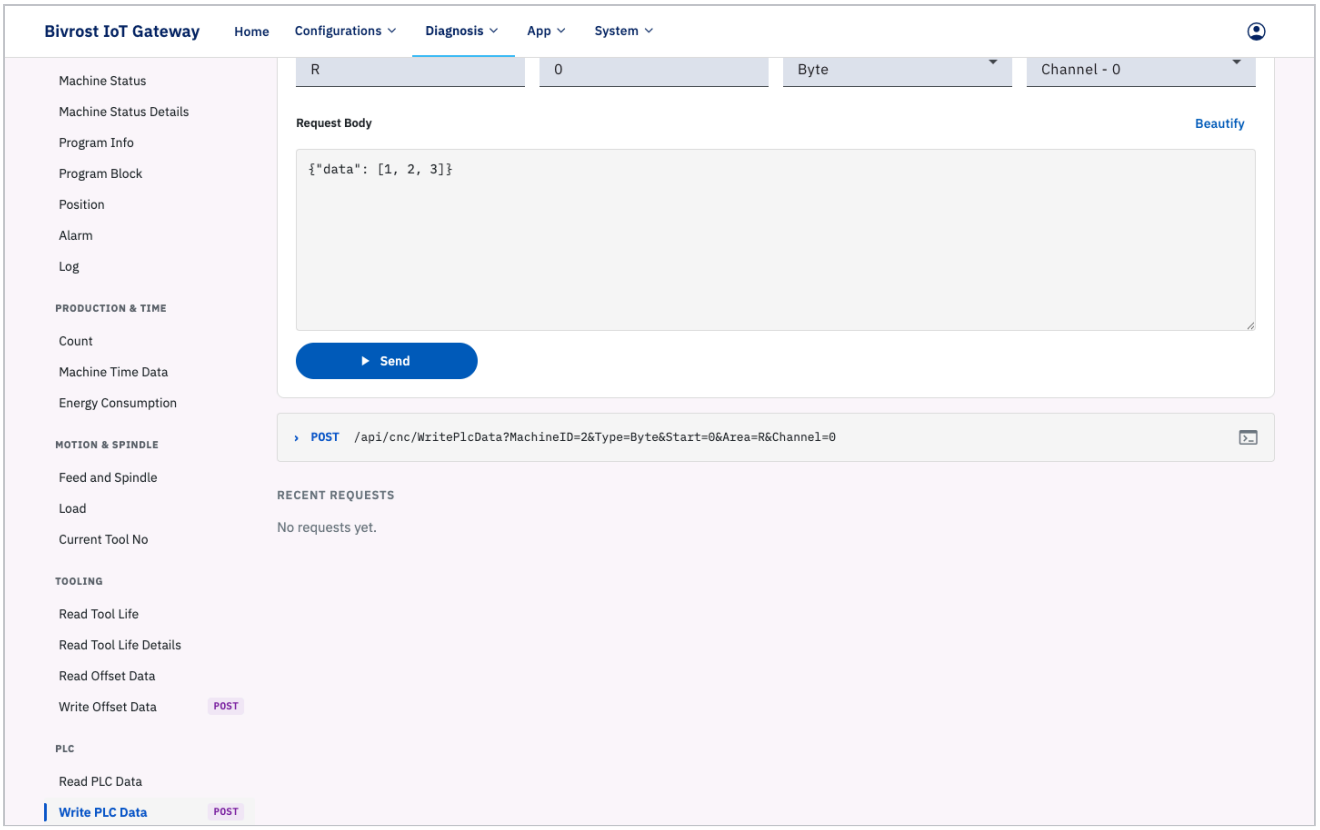


3.8.3. Write Data Interfaces

The write interfaces are **Write PLC Data** and **Write Offset Data**. Like the **Read PLC Data** and **Read Offset Data** interfaces, they need inputs such as **Area**, **Start Address**, **Data Type** and **Offset Number**, and in addition you must supply the data to be written in the request body. See 2.5.1.19. writePlcData — Write PLC Data and 2.5.1.14. writeOffsetData — Write Offset Data in the *Communication Protocol*. Click **Beautify** to reformat the request body into standard JSON.

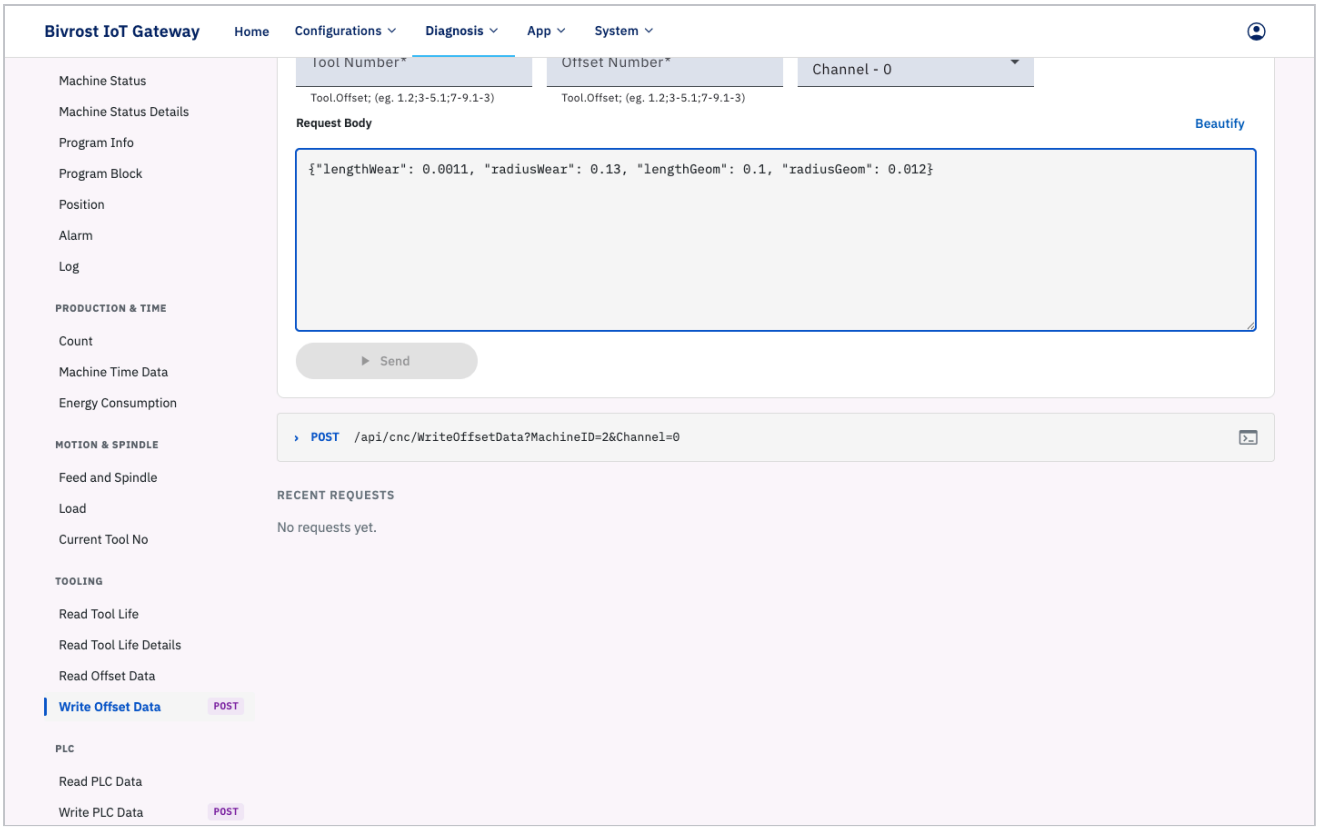
Example request body for writing PLC data:

```
{
  "data": [
    1,
    2,
    3
  ]
}
```



Example request body for writing offset data:

```
{
  "lengthWear": 0.0011,
  "radiusWear": 0.13,
  "lengthGeom": 0.1,
  "radiusGeom": 0.012
}
```

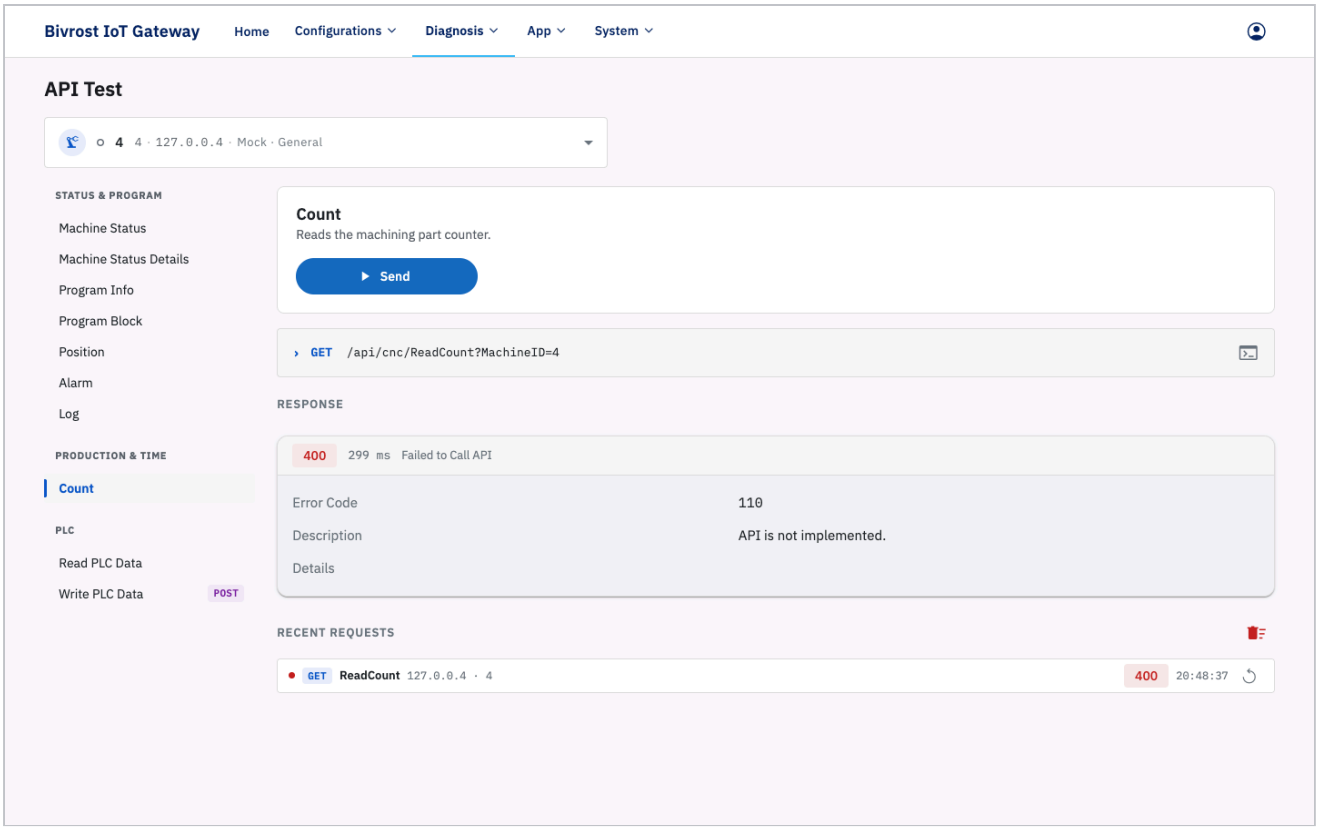


A successful write returns an error code (errorCode, where 0 means success) and an error message (errorMsg); see 2.2. Error Handling in the *Communication Protocol*.

```
{
  "errorCode": 0,
  "errorMsg": "Success"
}
```

3.8.4. Troubleshooting Test Failures

A failed API test returns **Failed to Call API**, as shown below. The response gives an **Error Code**, a **Description**, **Details** and a suggested **Remedy**.



If an API test fails, check the following:

1. The settings on the **Machines** page;
2. Whether you clicked **Restart Service** on **Home** after changing anything on the **Machines** or **Tasks** page;
3. Whether the network settings on the machine are correct (see *Machine Setup*) — on some machines the settings only take effect after the power is switched off for three seconds and back on;
4. Whether the hardware — network cable connections, switches and so on — is properly connected;
5. Whether the machine’s IP address is already in use. When office PCs or other devices share the same LAN, the machine’s IP may be taken, which stops the machine and the gateway from communicating. Try giving the machine an IP address that is not in use. Note: an IP address that does not answer a ping is not necessarily free — some devices disable ping replies for security reasons.
6. Another form of address conflict is a subnet conflict. This is common when the data-acquisition network and another internal network share a switch and both use the same subnet. When this happens, move either the conflicting internal devices or the data-acquisition network to a subnet that is not in use.

3.9. DNC (Program Transfer)

This page lets you list, upload, download, delete and back up machine program files and send files to several machines at once, and it has a built-in toolpath viewer. Use it to verify a setup before it goes live, or as a lightweight file manager for your machines.

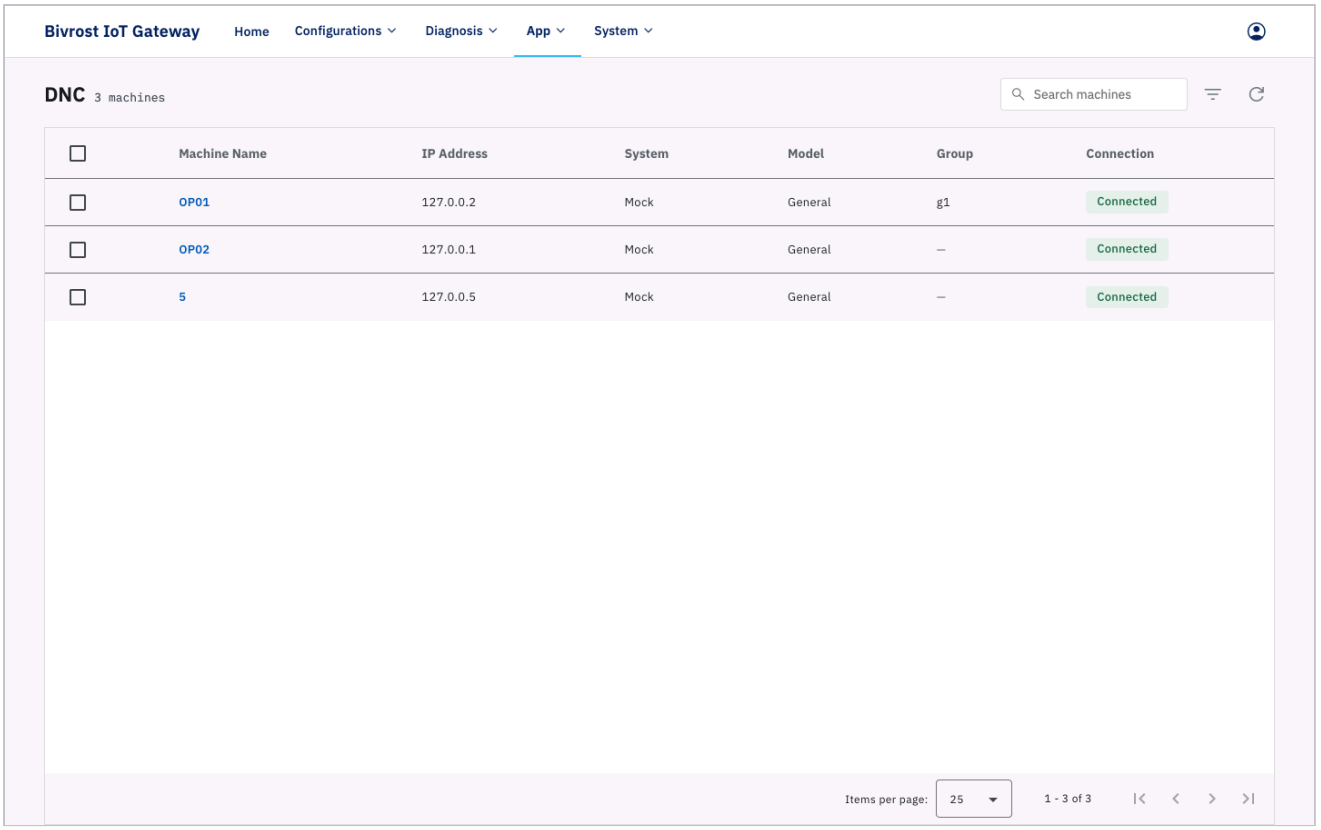
If you have changed any **Machines**, **Groups**, **Tasks** or **Communication** settings, click **Restart Service** on the Home page before transferring programs.

> **Caution**
>
> - A file sent from your computer **cannot overwrite an existing machine file directly**. If you send a file whose name already exists, the gateway asks you to confirm the replacement.
> - Some machines support file locking, write protection and similar features. Once these are enabled, files on the machine cannot be deleted.
> - **A program that is in use cannot be deleted.**

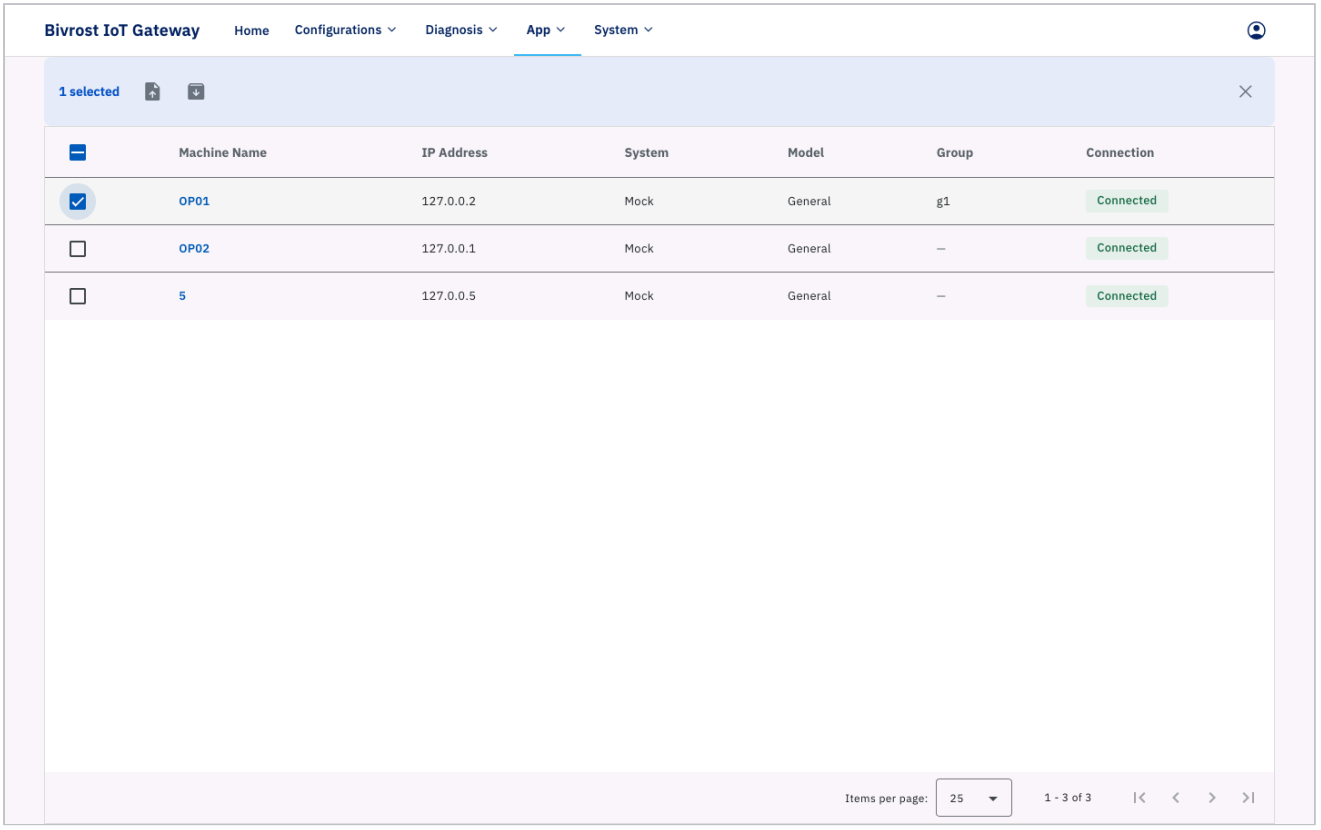
Program transfer uses the file-transfer parts of the HTTP protocol. For details, see section 2.6, File Management Interfaces, of the *Communication Protocol*.

Machine Directory

The **DNC** page opens on the machine directory: every machine that supports program transfer, together with its IP address, system model, group and connection status. DNC is unavailable for offline machines.



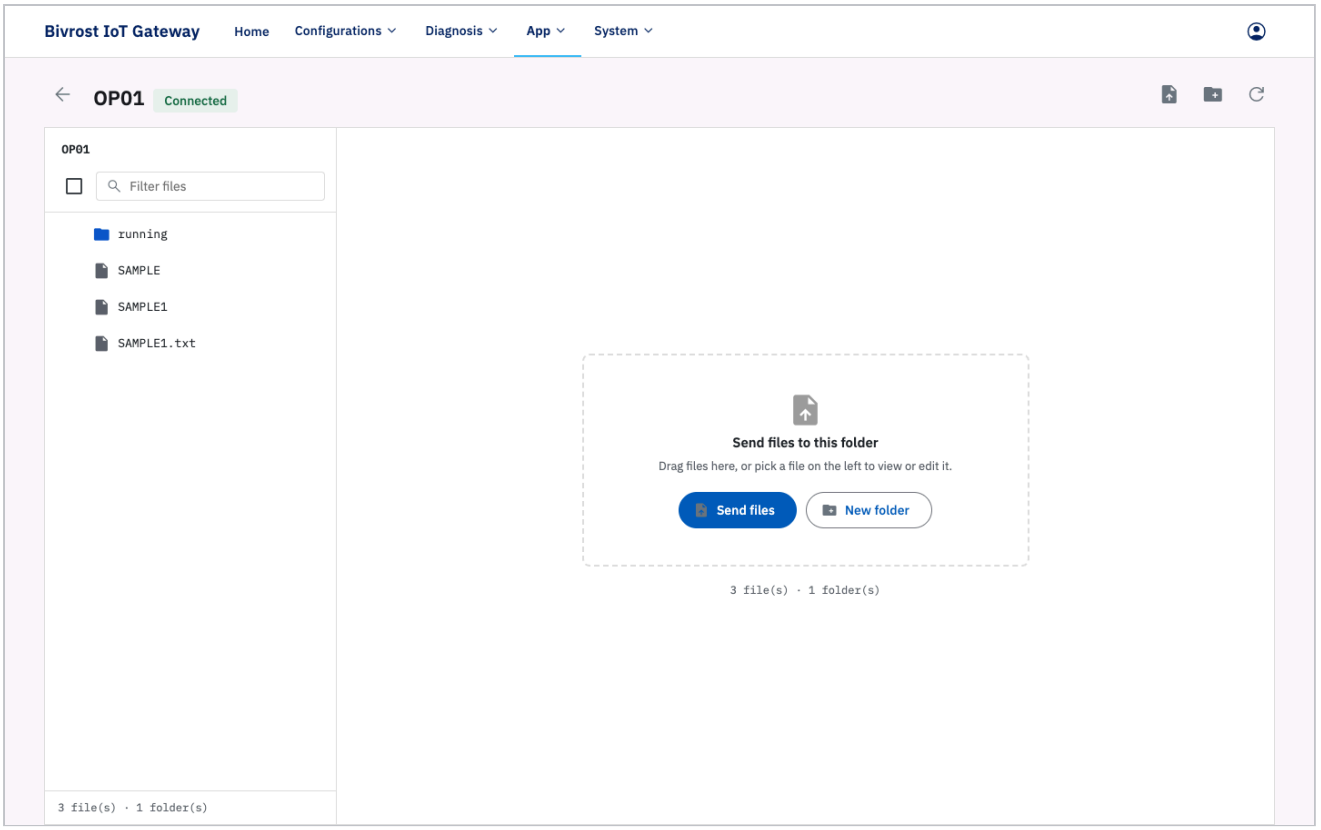
Select one or more machines and the Fleet actions bar appears at the top of the page, offering **Send files** and **Download machine files (backup)** for the selected machines.



Click a machine name to open that machine’s file browser.

3.9.1. Reading a Machine’ s File List

The left-hand panel of the file browser lists the folders and files under the machine’ s root directory (configured in 3.3.1.3. DNC Settings). Click a folder to open it; use the breadcrumb above the list to go back up. A filter box above the list narrows the view by file name.

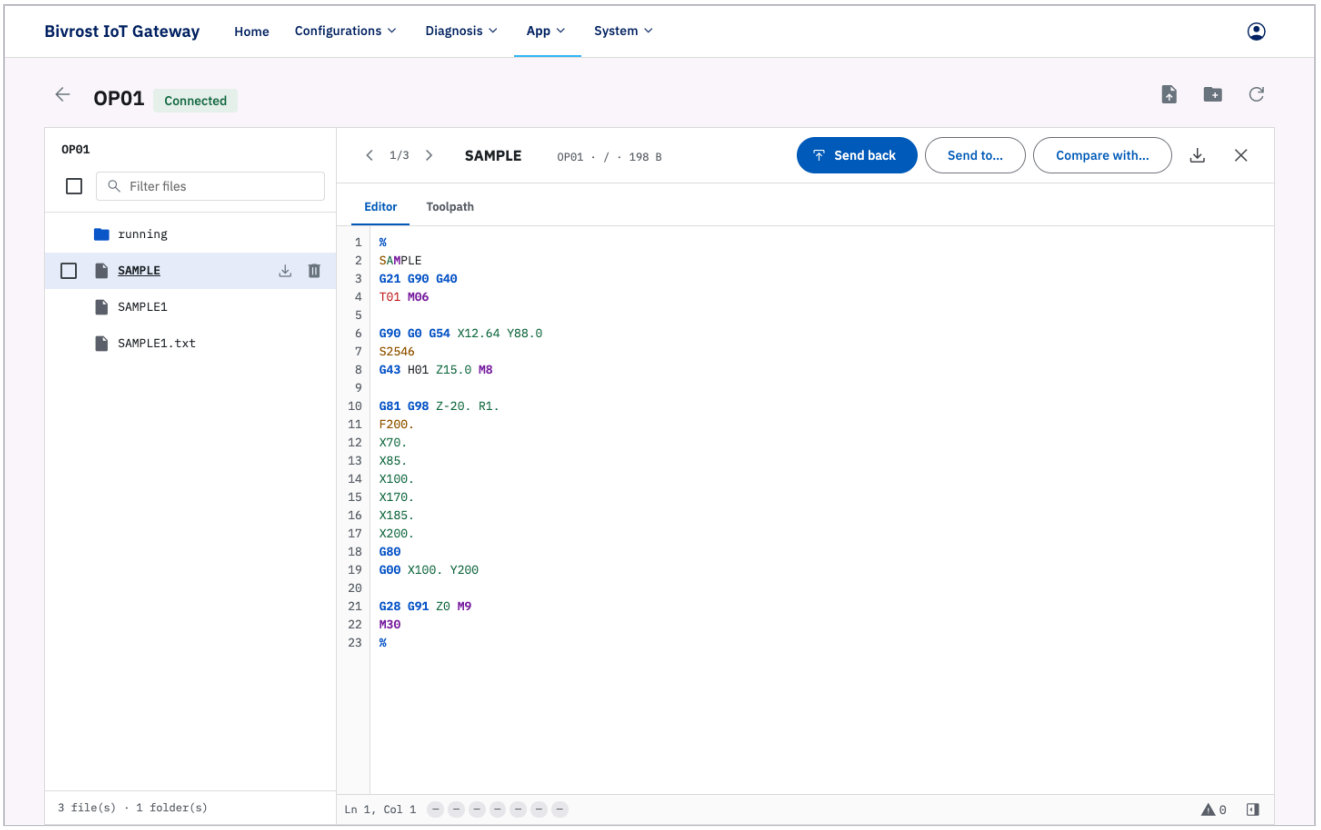


On Mitsubishi controls, a target path holding a large number of files can take a while to list.

If the file list does not respond for a long time and no error appears, go to the API Test page and use the Common Data interface to check that the gateway can talk to the machine.

3.9.2. Receiving a Machine File to Your Computer

Click a file in the left-hand list and the gateway receives it from the machine and shows its contents in the preview pane on the right. The ‹ › buttons at the top left of the preview pane step through the files.



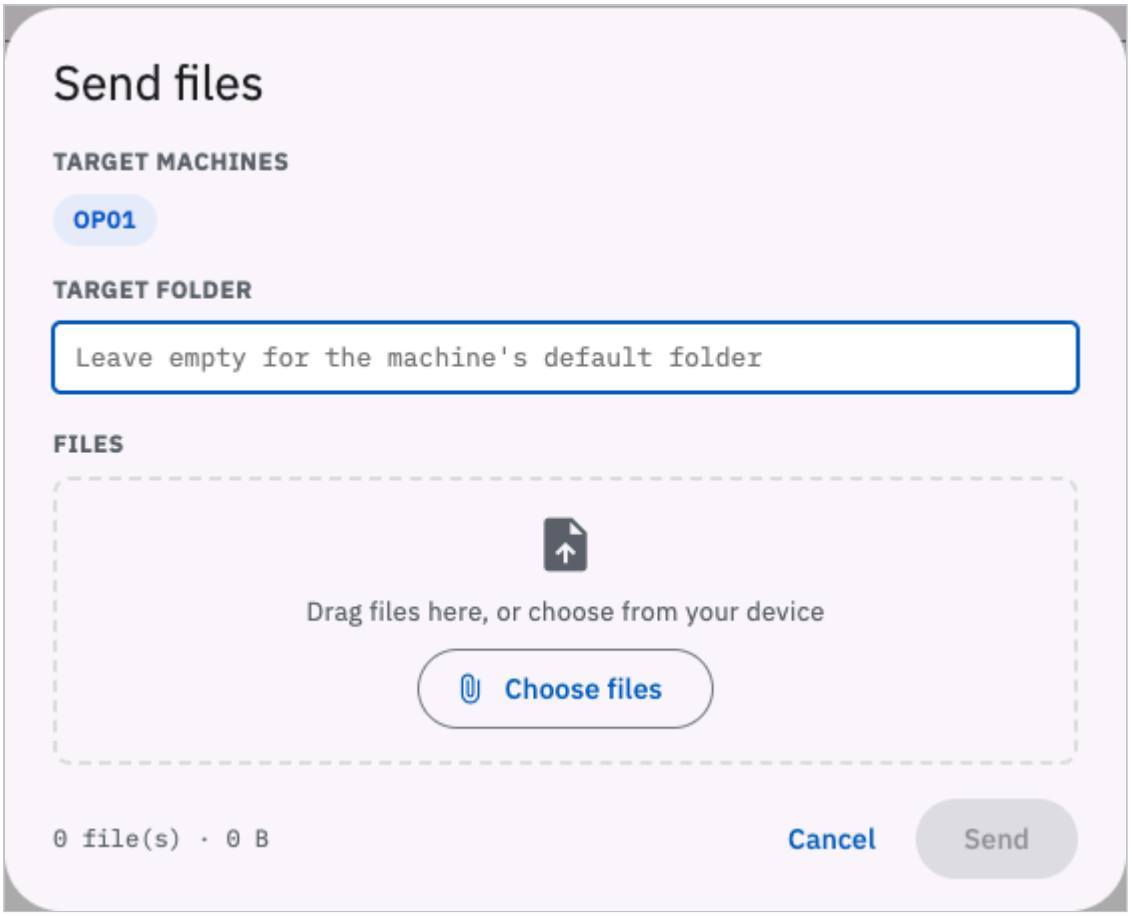
Click the **Download** icon at the top right of the preview pane to save the received file through your browser. The file lands in your browser’ s default download folder. You can also open your browser’ s download settings to change that folder, or have the browser ask you where to save each download. Alternatively, hover over a file in the list and click the **Download** icon on the right of the row to download it directly.

Binary files cannot be shown in the preview pane, but they can still be downloaded.

3.9.3. Sending a Local File to a Machine

Click the **Upload files** button at the top right of the page (or select machines in the machine directory and click **Send files**) to open the “Send files” dialog:

1. Confirm the target machine and the target folder (leave the folder empty for the machine’ s default folder);
2. Drag files into the dialog, or click **Choose files** to pick them from your computer — several files can be selected at once;
3. Click **Send**. The files are sent to the target folder on the machine.



After editing a file in the preview pane, you can also click **Send back** to return the edited contents to the current machine, or **Send to…** to send them to other machines.

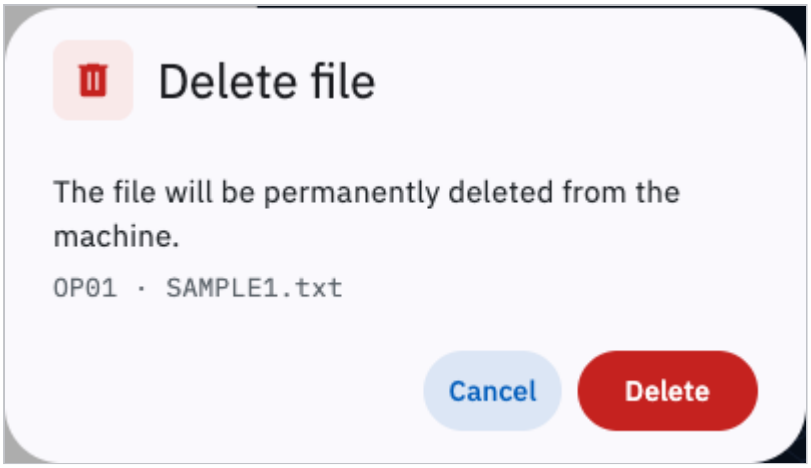
Caution for Fanuc Systems

When you send a file to a Fanuc control, the machine automatically takes the first line of the file’ s contents as the file name, not the name the file had on your computer. You must therefore change the first line to the target file name before sending. With the contents below, the file is named O8003 on the machine after a successful send:

```
%
O8003
T1M06
...
```

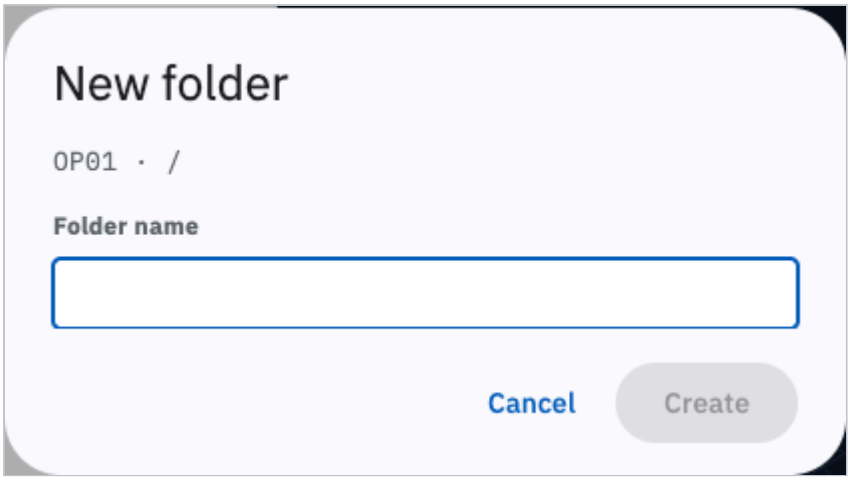
3.9.4. Deleting a Machine File

In the left-hand file list, hover over a file, click the **Delete** icon on the right of the row and confirm in the dialog that appears. The file is then deleted.



3.9.5. Creating a Machine Folder

Click the **New folder** icon at the top right of the page to open the new folder dialog, enter a folder name and click **Create**. The folder is created inside the current folder.



3.9.6. Deleting a Machine Folder

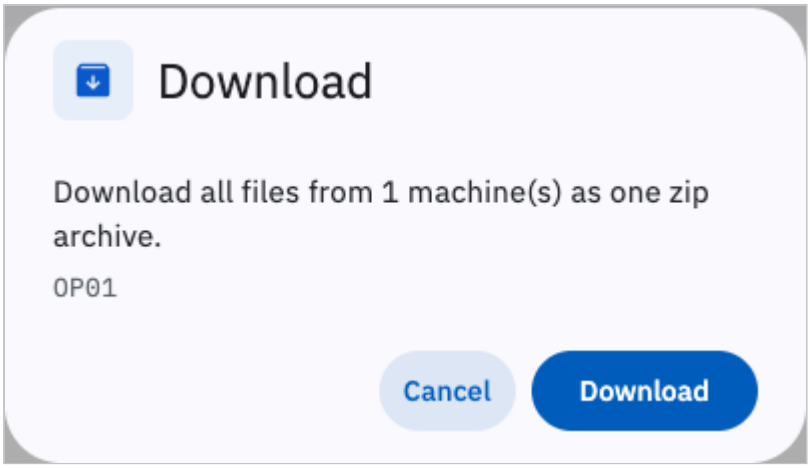
In the left-hand file list, hover over a folder, click the **Delete** icon on the right of the row and confirm in the delete folder dialog. Only empty folders can be deleted at present, so delete all files and subfolders inside it first.

3.9.7. Backing Up Machine Files

This function packs the files of the selected machines — including subfolders and their contents — into a single ZIP archive for you to download. Inside the archive, the first level is a folder named “BackupFiles_” followed by the backup date and time; the second level is one folder

per machine root directory, named “machineID_machineName”; below that are each machine’s files and folders, with the original folder structure preserved.

In the machine directory, select the machines to back up (tick **All machines** in the table header to select every machine), click **Download machine files (backup)** in the Fleet actions bar, then click **Download** in the confirmation dialog to start the backup. Once the archive is ready, it can be downloaded to your computer.



> **Note**
> Backing up a folder that holds a large number of files takes a long time. Back up only the machines you need.

3.9.8. Batch Sending Files

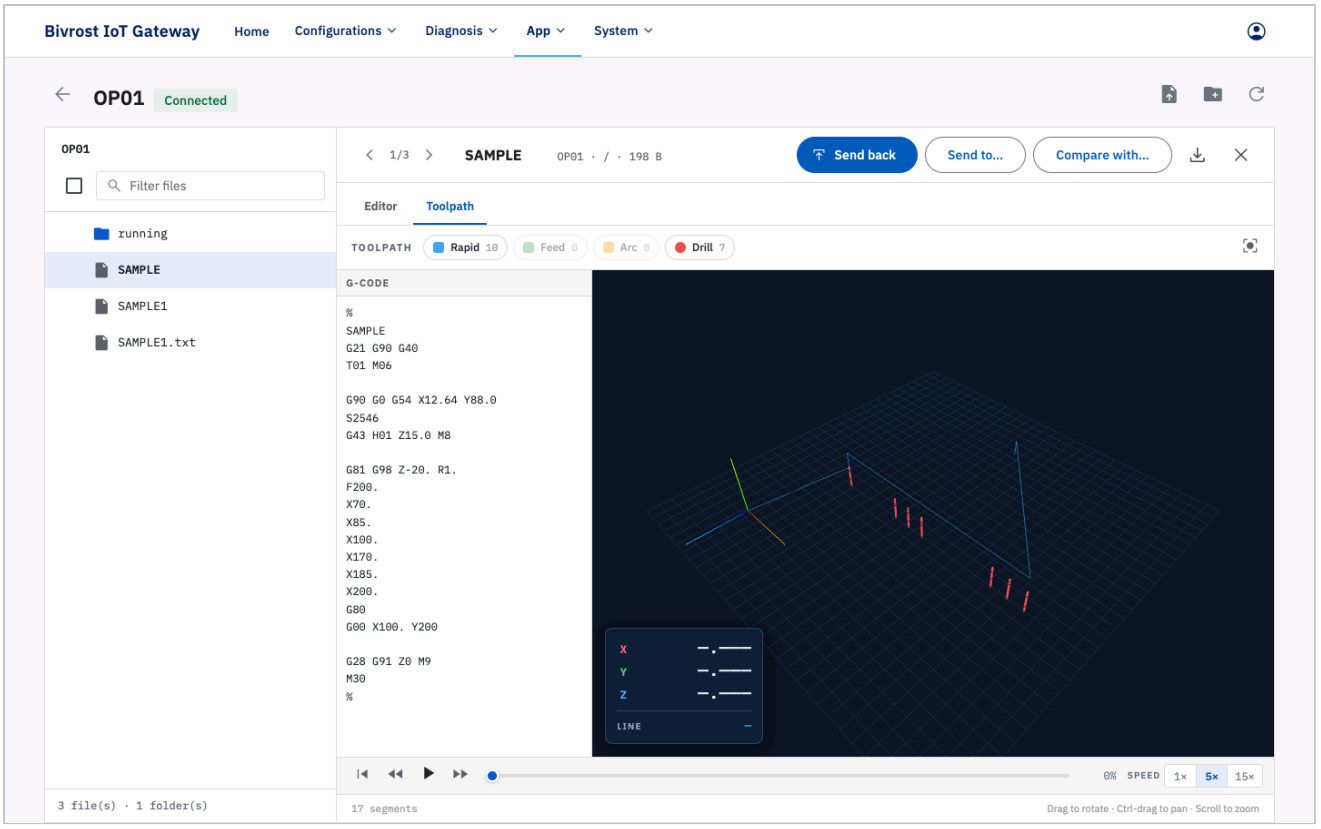
Select several machines in the machine directory and click **Send files** to send the same set of files to a chosen folder on all of them in one go. In the “Send files” dialog you can click **Choose files** repeatedly to add files from different locations; confirm the target folder and click **Send**.

The send runs as a single batch and the gateway transfers to each machine in turn. If a file of the same name already exists at the destination, you are asked to confirm the replacement.

3.9.9. Viewing the Toolpath

Two tabs, **Editor** and **Toolpath**, sit above the file preview pane. Once a G-code file is loaded (received from the machine — see 3.9.2. Receiving a Machine File to Your Computer), switch to the **Toolpath** tab to open the toolpath viewer.

The viewer shows the G-code on the left and an animation of the corresponding toolpath on the right, with X/Y/Z position readouts (DRO) and the current line. The legend above distinguishes toolpath types such as Rapid, Feed, Arc and Drill. Drag to rotate the view, scroll to zoom and adjust the playback speed to study the toolpath directly. If needed, edit the G-code in the code pane on the left and the toolpath on the right updates immediately.

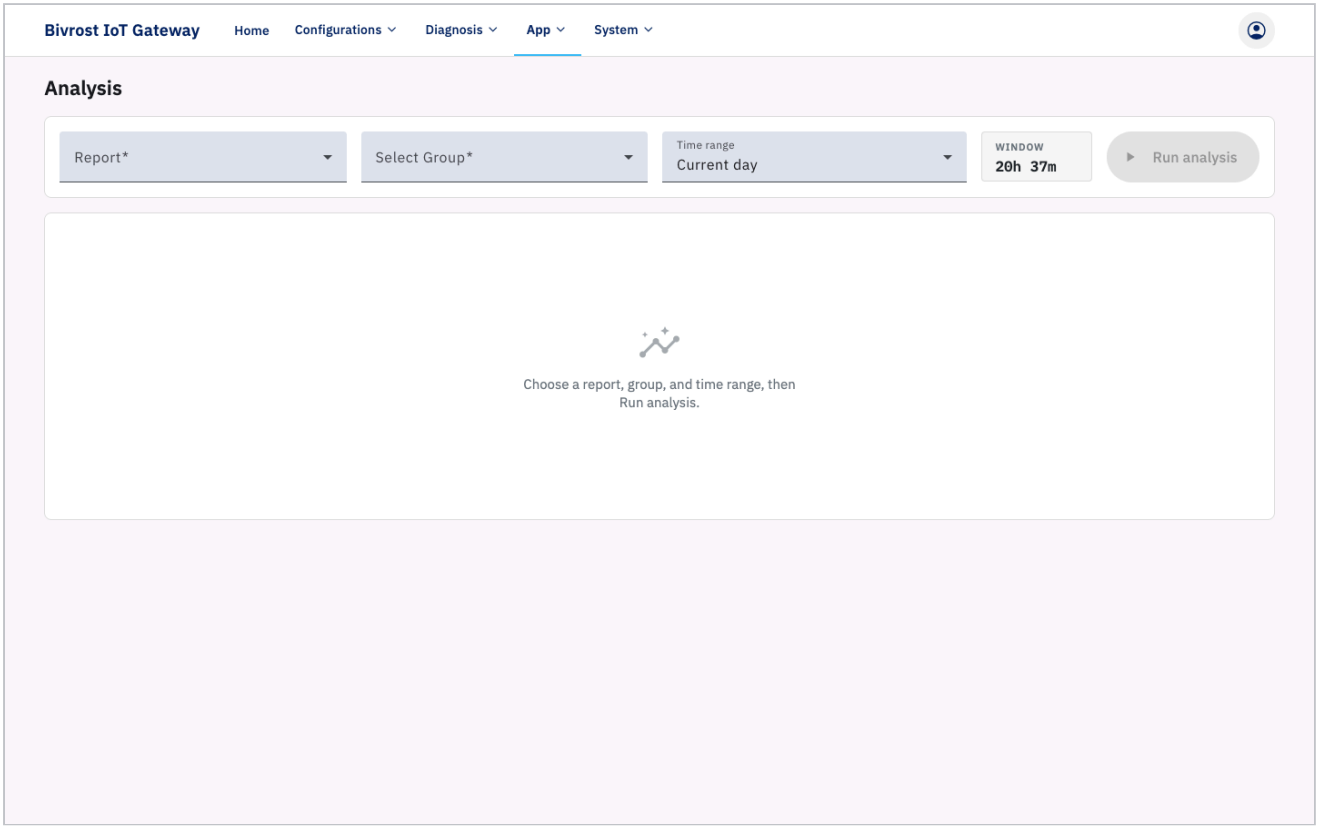


3.10. Analysis

The Analysis page extracts the machine and group data held in the gateway’s local storage and builds a statistics table for a given group, over a given period of time, broken down by grouping interval.

Points to note when using Analysis

- 3.12.2.3. Local Caching must be enabled first, so that machine status history can be kept on the gateway itself. Local history is retained for at most 365 days, so no time option may be set earlier than 365 days before the current time.
- The difference between the start time and the end time (the time range) may not exceed 31 days.
- Machines and groups should already be configured.
- If the end of the time range is later than the current time, the current time is used as the end time.
- If part of the time range contains no machine status data, the status for that gap defaults to **Offline**. Besides the machine actually being off or offline, machine status can be missing for other reasons: local caching was not enabled on the gateway, the gateway lost power, the gateway lost network connectivity, and so on.

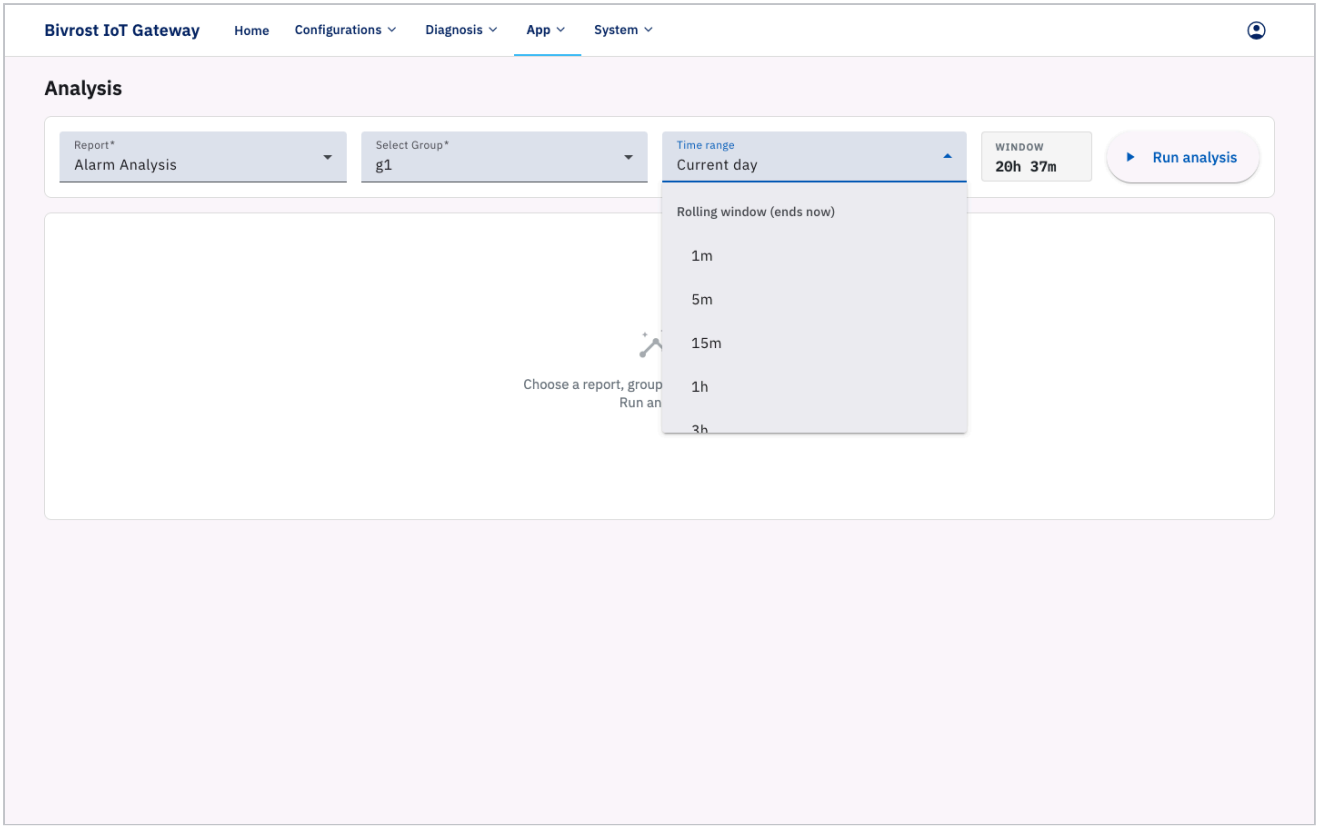


To run an analysis, select an analyzer, select a group, set the time range, and click **Run analysis** to get the result.

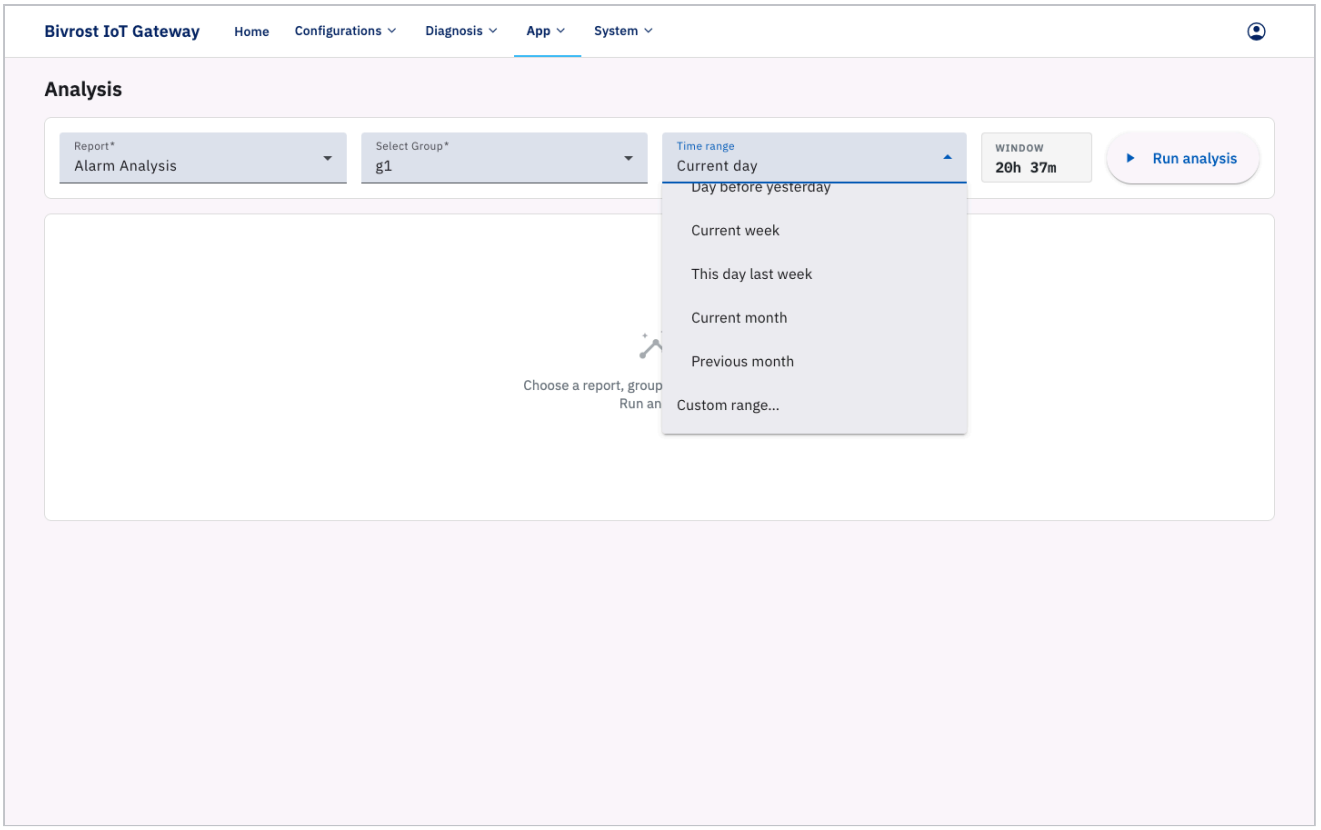
- **Analyzer options**: Alarm Analysis, Count Analysis, Cycle Analysis, OEE Analysis, Overall Analysis, and so on.
- **Group options**: the groups activated on the **Groups** page.

Once the analyzer and the group are selected, the **Time range** list offers three ways to set the period.

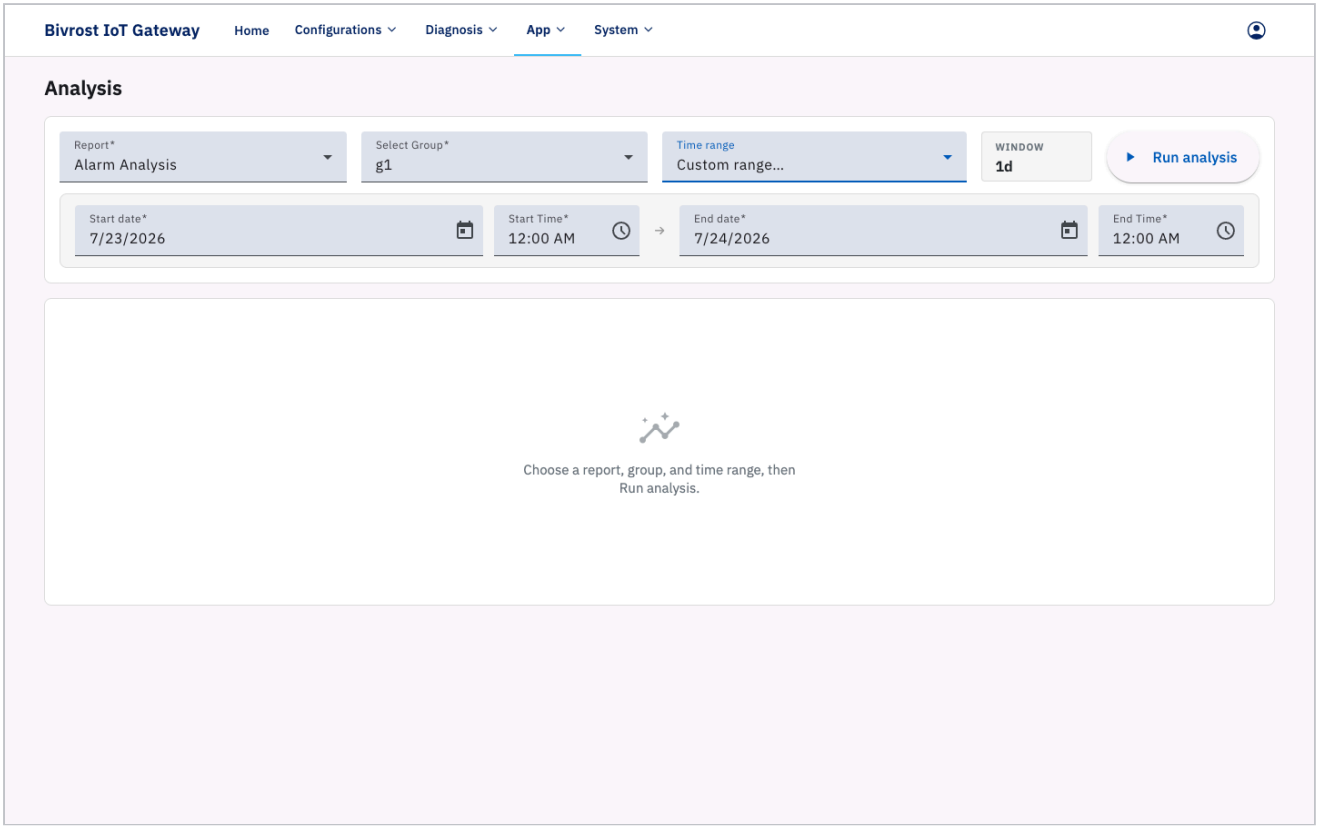
Rolling window (ends now): a period that ends at the current time, chosen from preset lengths such as 5m, 1h, 1d and 30d. Choosing 30d, for example, runs the analysis from 30 days before the current time up to the current time.



Calendar periods: options relative to the present moment, such as Current day, Current week, This day last week and Current month. Current week, for example, sets the start time to midnight on Monday of the current week.



Custom range...: enter the exact start and end date and time by hand.

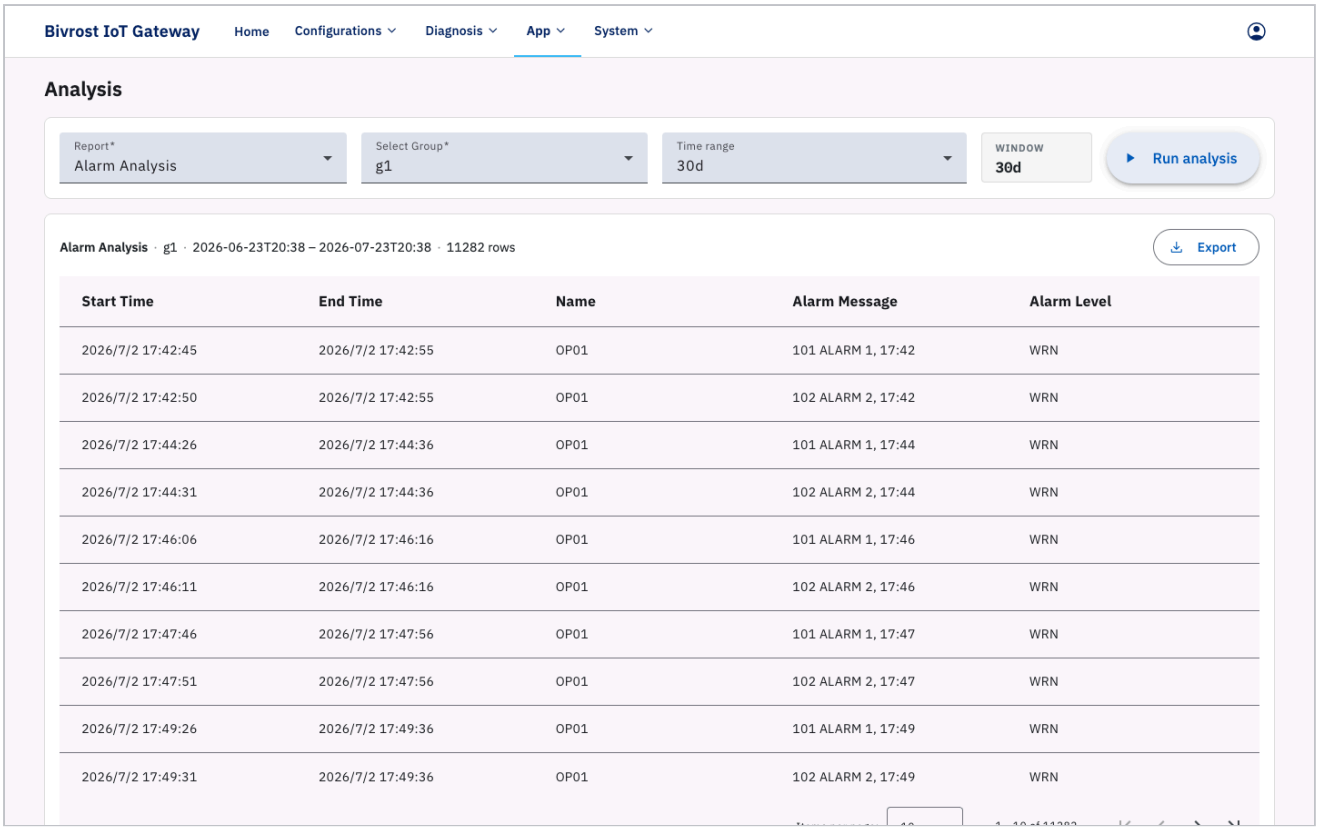


> **Note**
>
> If the end of the time range is later than the current time, it is automatically corrected to the current time.

The options specific to each analyzer, and the results they produce, are described below.

3.10.1. Alarm Analysis

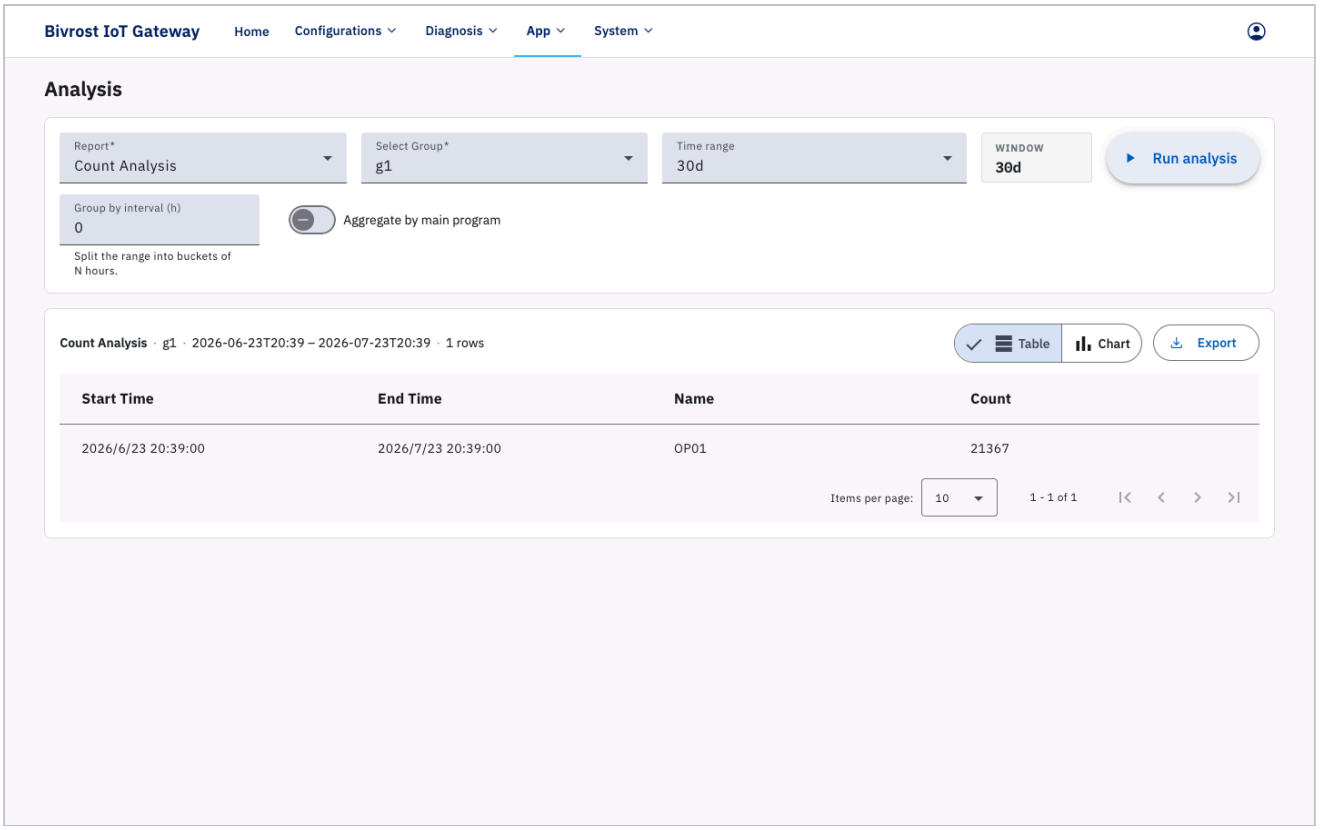
The figure below shows the alarm analysis table for every machine in the selected group, produced by choosing Alarm Analysis, Group 1 and the last 30 days and clicking **Run analysis**. It lists the start and end time of each alarm, its message and its level.



Once the result has been calculated, click **Export** to download it as a CSV file. The file is named automatically as `AnalyzerName-GroupName-StartTime-EndTime.csv`.

3.10.2. Count Analysis

The figure below shows the count analysis table for every machine in the selected group, produced by choosing Count Analysis, Group 1 and the last 30 days and clicking **Run analysis**. Count here means the count produced within the specified time range.



Two settings are specific to this analyzer: **Group by interval (h)** and **Aggregate by main program**.

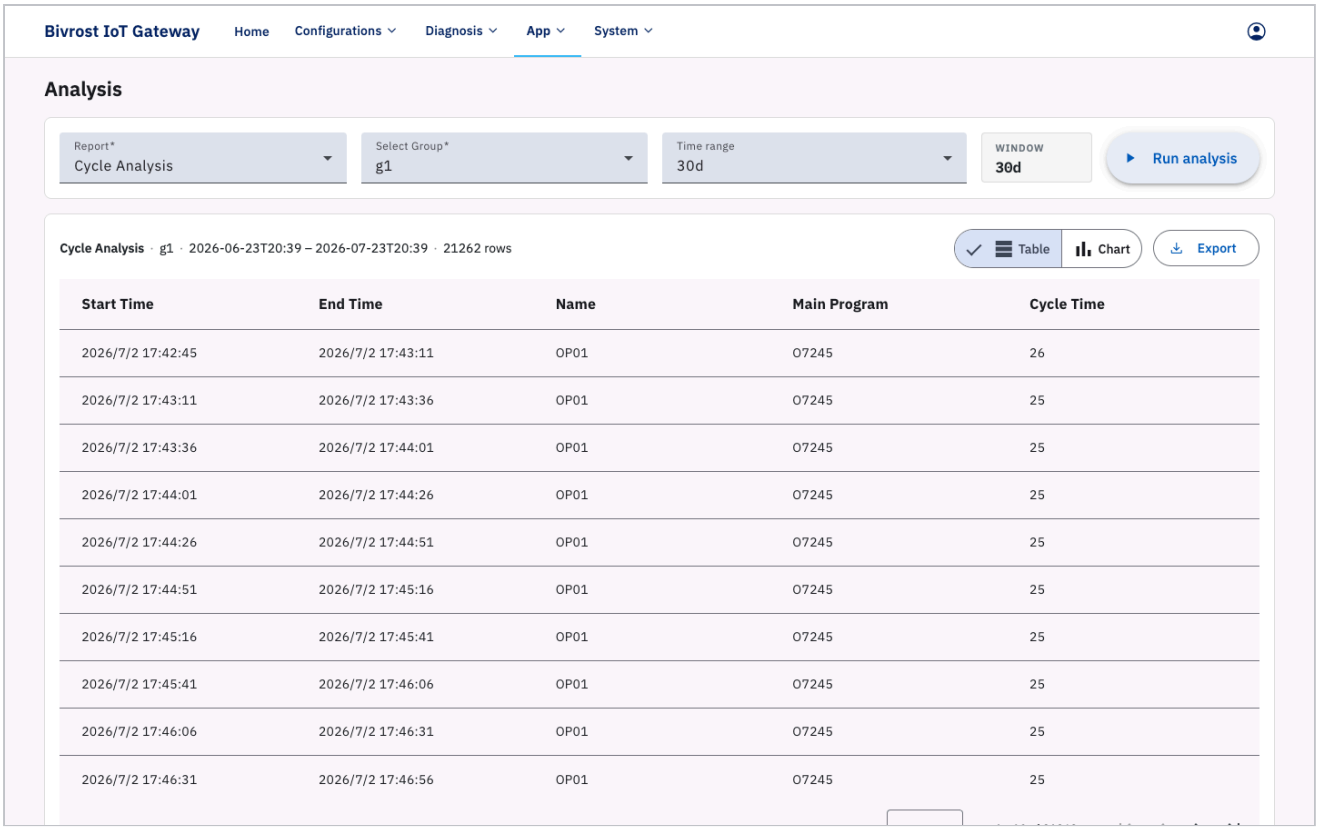
Group by interval (h) splits the time range into buckets: starting from the start time, each interval forms one bucket, and the count is calculated separately for each bucket. The default is 0, which means no grouping — a single bucket. The example below uses a grouping interval of 24 hours, so the count shown is the count within each interval.

Aggregate by main program breaks the count within each bucket down by the main program that was running at the time. In the figure below, mock machine 1 runs two different main programs, so the count is reported separately for each of them.

Once the result has been calculated, click **Export** to download it as a CSV file. The file is named automatically as `AnalyzerName-GroupName-StartTime-EndTime.csv`.

3.10.3. Cycle Analysis

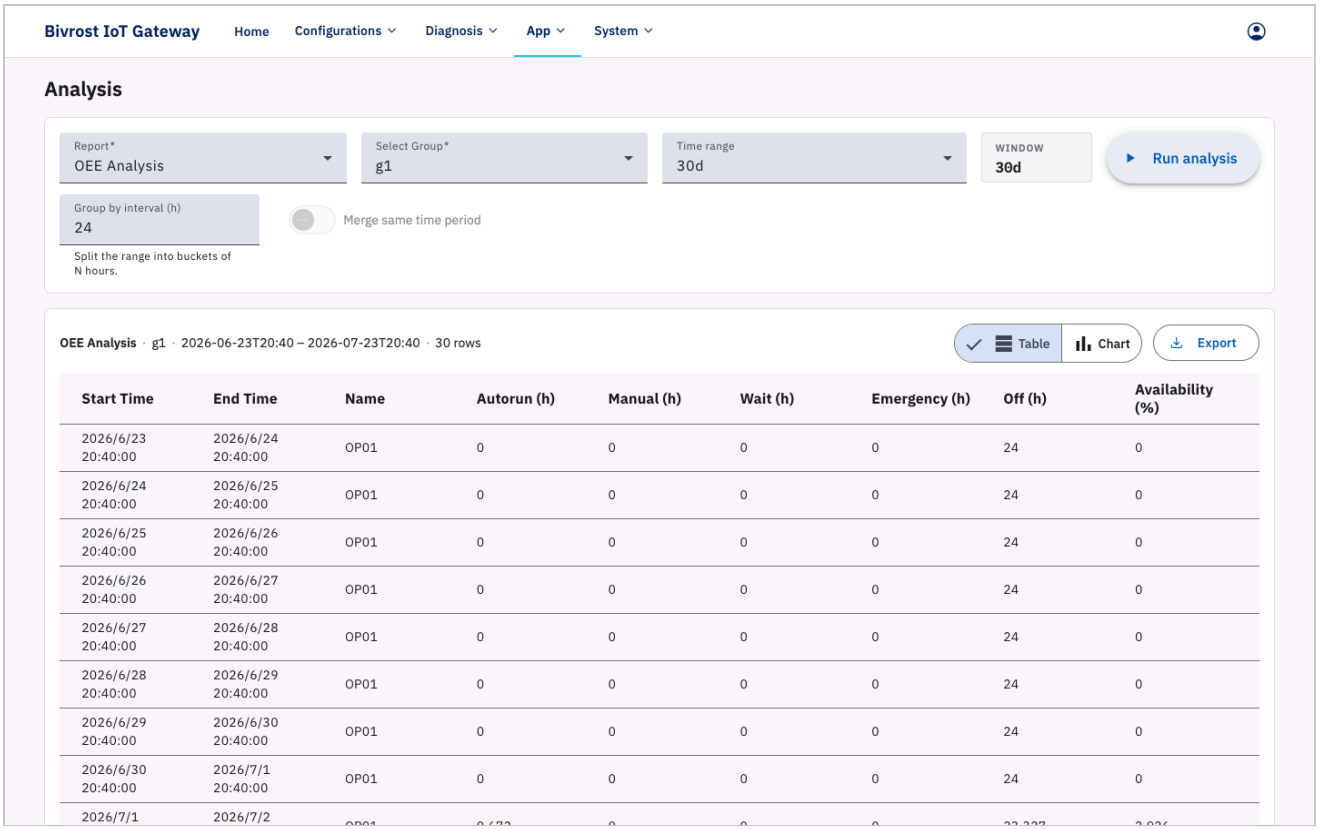
The figure below shows the cycle analysis table for every machine, produced by choosing Cycle Analysis, Group 1 and the last 30 days and clicking **Run analysis**. It shows, for each machine within the period, the start and end time of every cycle, the main program that was running, and the cycle time.



Once the result has been calculated, click **Export** to download it as a CSV file. The file is named automatically as `AnalyzerName-GroupName-StartTime-EndTime.csv`.

3.10.4. OEE Analysis

The figure below shows the OEE analysis table for every machine, produced by choosing OEE Analysis and Group 1, entering an explicit start and end time, setting a grouping interval and clicking **Run analysis**.



Two settings are specific to this analyzer:

Group by interval (h) works exactly as in Cycle Analysis: it splits the time range into buckets, starting from the start time, and calculates OEE separately for each bucket. The default is 0, which means no grouping — a single bucket.

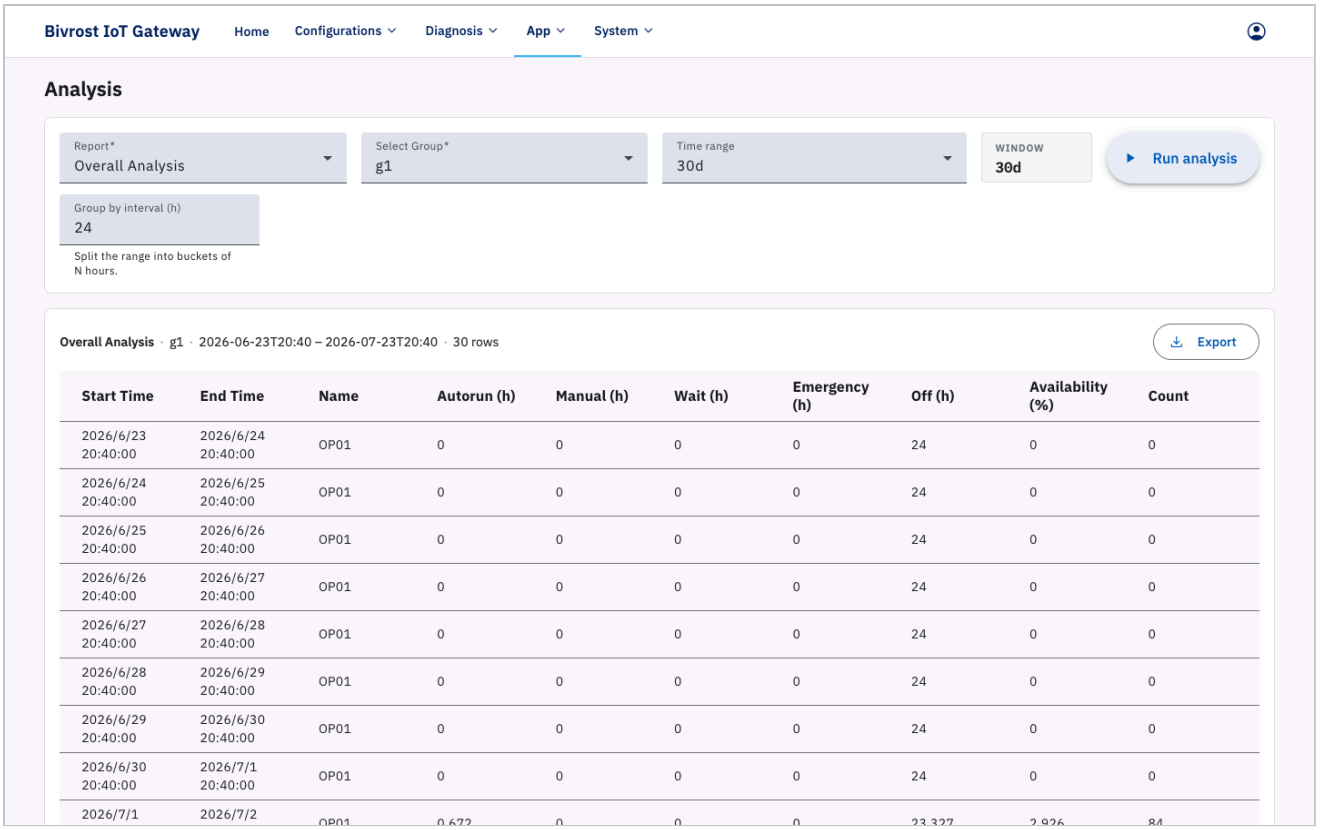
Merge same time period aggregates the OEE data of the buckets that cover the same period of each day. It is typically used to compile OEE data for the several shifts worked each day. You must therefore set the start time to the time a shift begins and set the grouping interval to the length of one shift (greater than 0 and less than 24 hours); only then do you get an OEE summary that matches the shifts. The figure below summarises OEE for two shifts per day (day shift 8:00-20:00, night shift 20:00-8:00) over the specified time range.

Once the result has been calculated, click **Export** to download it as a CSV file. The file is named automatically as `AnalyzerName-GroupName-StartTime-EndTime.csv`.

3.10.5. Overall Analysis

Overall Analysis combines Count Analysis and OEE Analysis.

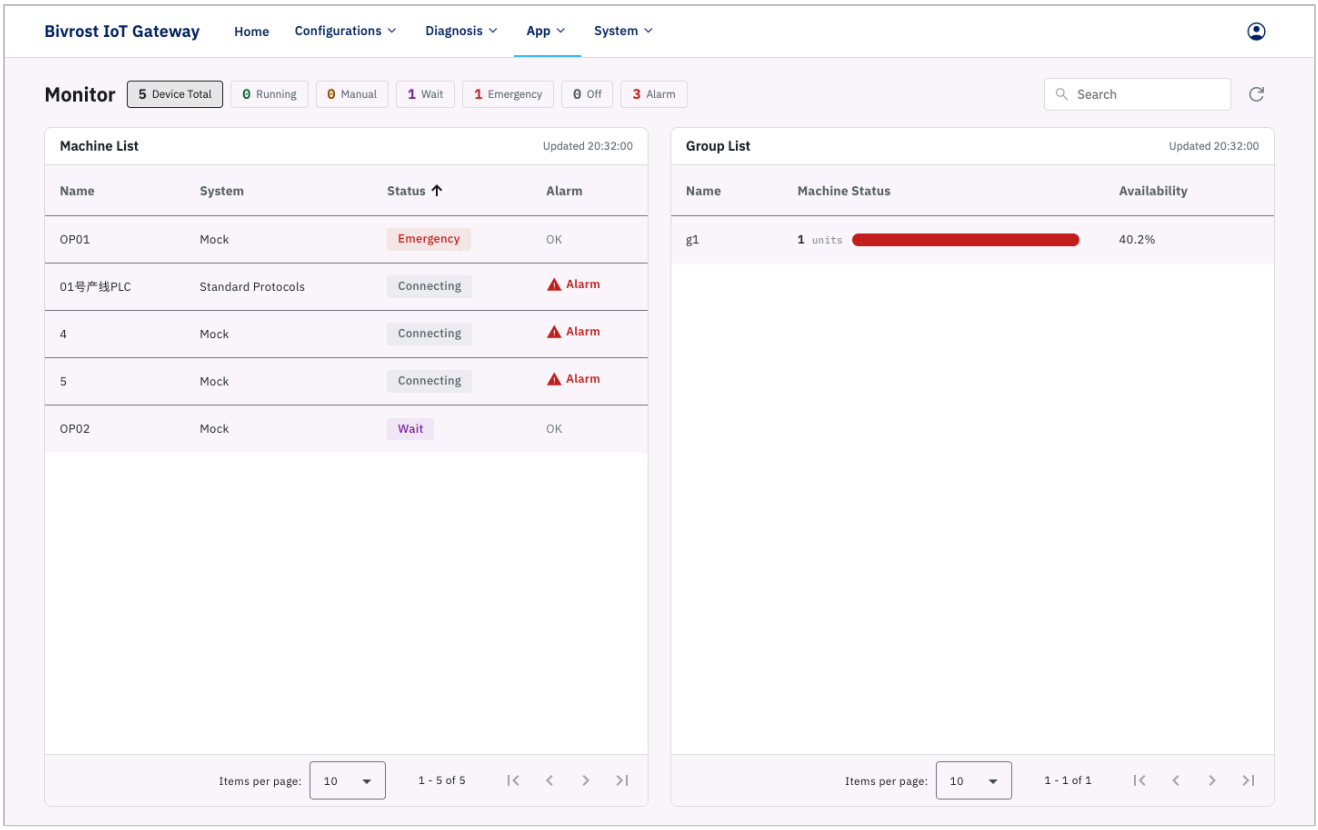
The figure below shows the OEE data and count data for two shifts per day (day shift 8:00-20:00, night shift 20:00-8:00) over the specified time range.



Once the result has been calculated, click **Export** to download it as a CSV file. The file is named automatically as `AnalyzerName-GroupName-StartTime-EndTime.csv`.

3.11. Monitor

The Monitor page shows machine and group status in real time. At the top of the page are device counts summarised by status (Device Total, Run, Manual, Wait, Emergency, Off, Alarm), each of which can be clicked to filter. Below it are the Machine List (Machine Name, System, Status, Alarm Status) and the Group List.

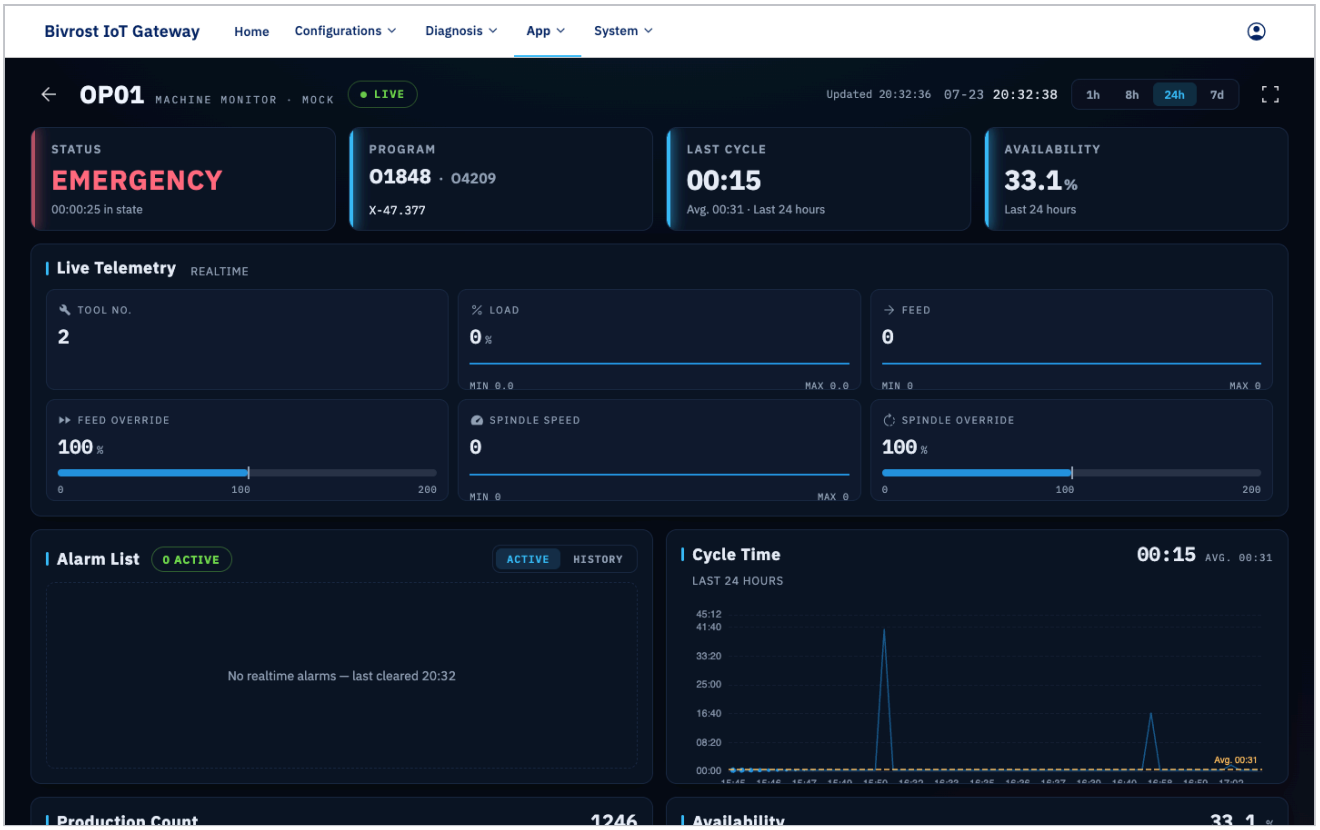


The layout adapts to the screen size: the Machine List and the Group List may be arranged side by side instead of one above the other.

3.11.1. Machine Monitor

Click a machine row in the Machine List to open the Machine Monitor page, which shows the machine’ s live data (Main Program, Sub-program, current Alarm Level, Current Tool No, spindle load, feedrate, Feedrate Override, spindle speed, Spindle Override and so on) together with the Count, Availability, status statistics and Alarm History for the last 24 hours.

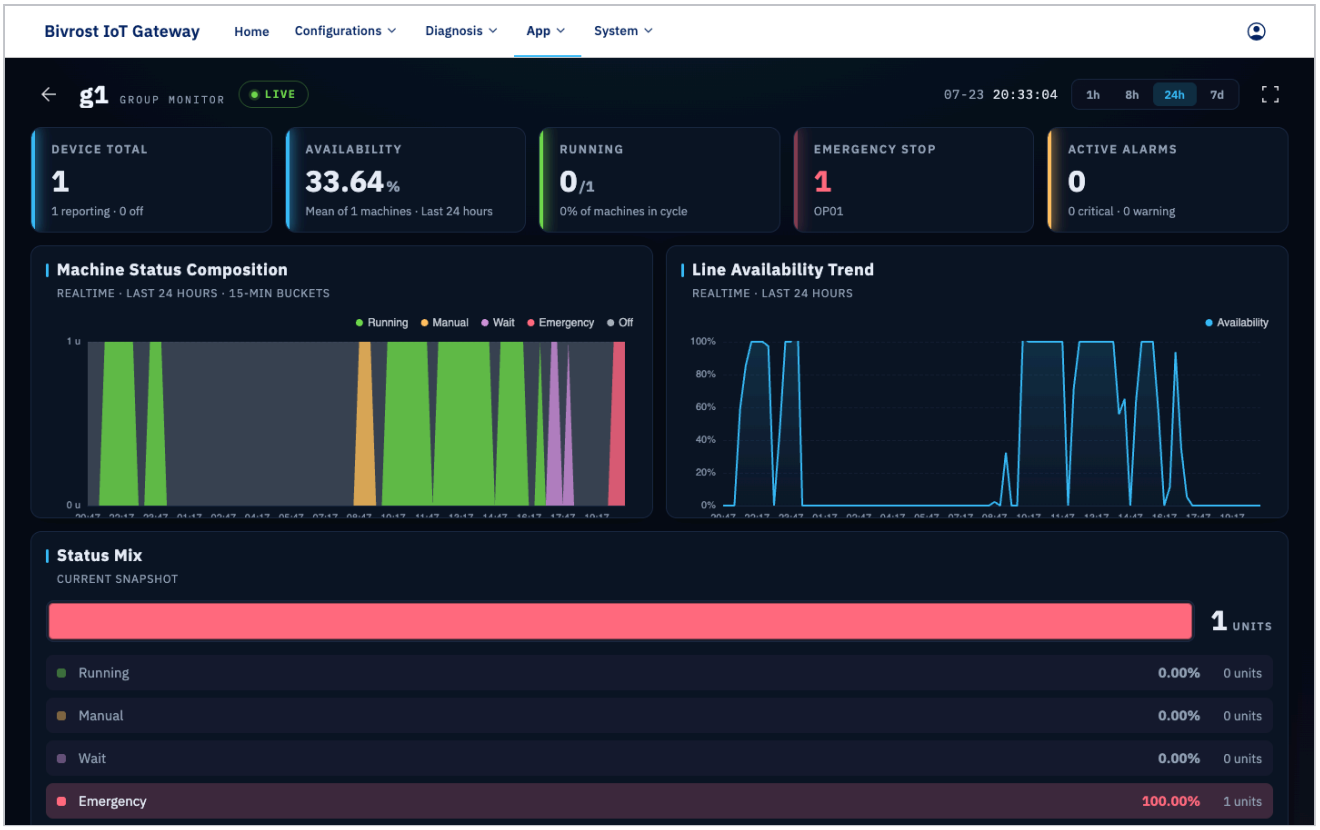
The ‹ button in the top-left corner returns to the Monitor home page.



3.11.2. Group Monitor (Group Overview)

Click a group row in the Group List to open the Group Monitor page, which presents the group’ s live data as an Andon wall (Availability, the number of machines in each status, a status tile for every machine, alarm severity and time, and so on) along with the availability and status trend charts. For groups with a large amount of data, the trend charts take a moment to load.

The ‹ button in the top-left corner returns to the Monitor home page.



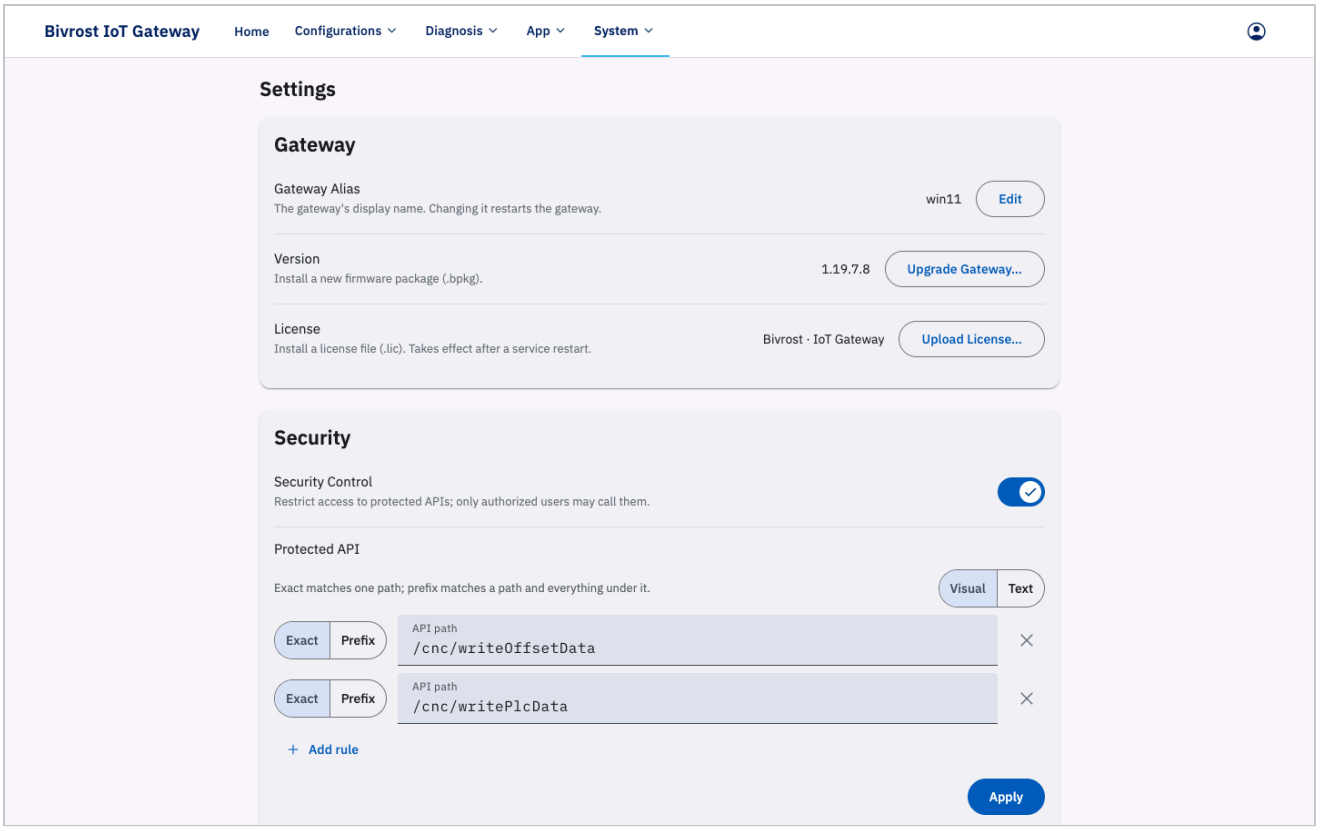
Note

The Availability shown on the page is the cumulative availability over the monitoring period (see 3.5.3. OEE Monitoring Settings). The availability plotted in the availability trend chart is calculated per bucket, using 5-minute buckets within the trend time window.

3.12. Settings

The Settings page is where you configure and maintain the gateway’ s advanced functions: user permissions, license updates, software upgrades, API security, time and region settings, and so on.

When you sign in with an administrator account (for example the initial `admin` account), the Settings page shows the following cards from top to bottom: **Gateway** (Gateway Alias, Version, License), **Security**, **Options**, **Time And Region Setup**, **Backup & Restore** and **Users & Access**.



When you sign in with a standard user account, only the **Change Password** and **Language** items in the account menu at the top right are available.

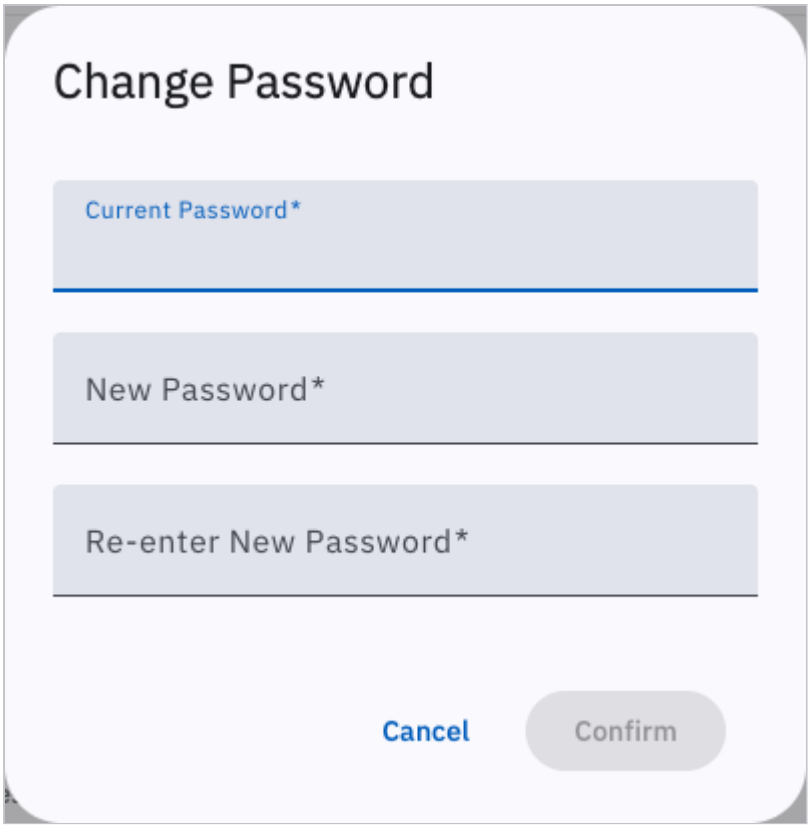
The instructions below describe the interface as seen by an administrator. Unless stated otherwise, a setting can only be changed while signed in as an administrator.

3.12.1. Common Functions

3.12.1.1. Change Password

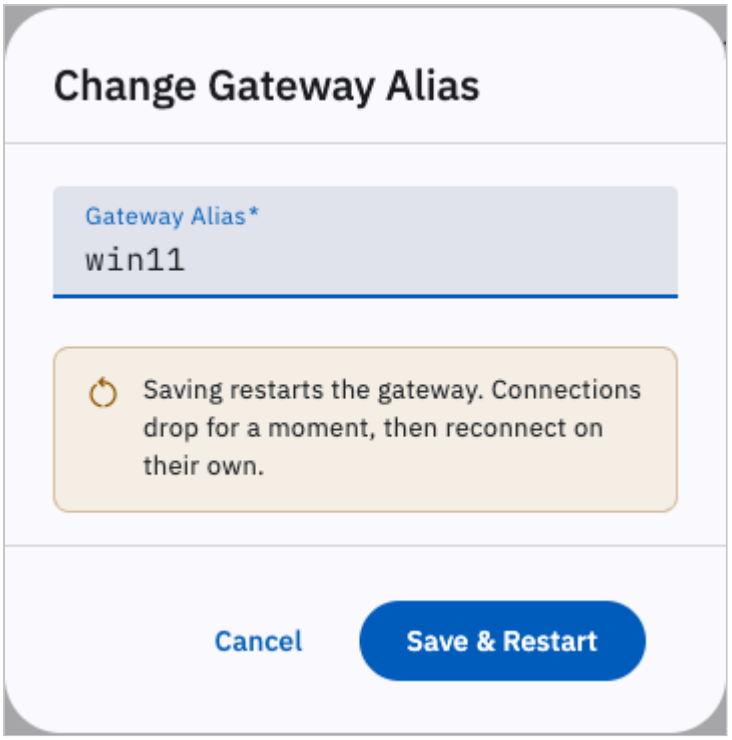
Click the **Account** button at the top right of the page to open the account menu, choose **Change Password**, enter your current password to verify your identity, then enter the new password and

click Confirm to apply the change. Once the change is confirmed, you must use the new password the next time you sign in. This function is available to administrators and standard users alike.



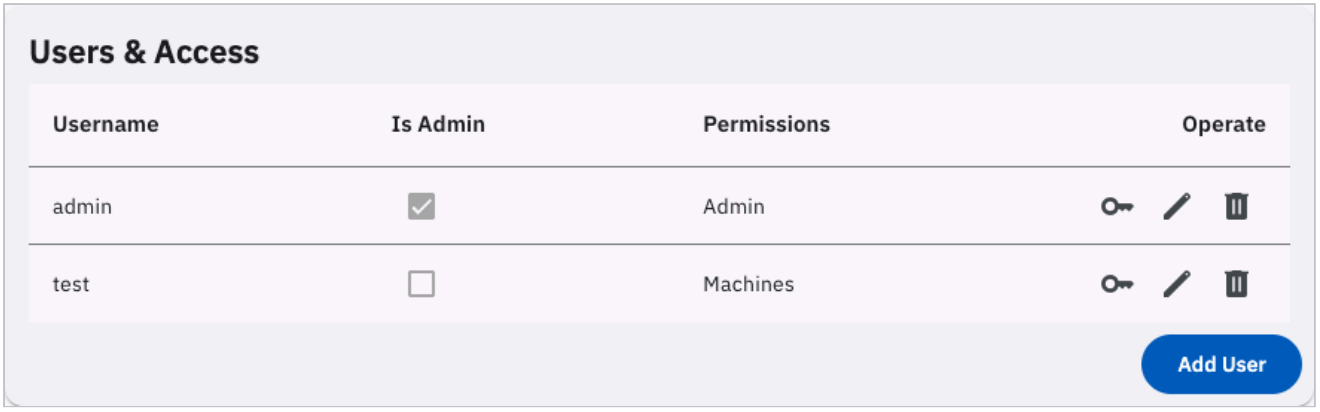
3.12.1.2. Change Gateway Alias

In the “Gateway” card, click the **Edit** button to the right of the Gateway Alias to open a dialog where you can change it. The alias is also the gateway’s domain name, which is used both to reach the gateway and for MQTT communication (see 3.6.3. MQTT Settings). The default alias is iotgw. If you reach the gateway by domain name, use the new domain name to sign in after changing the alias.



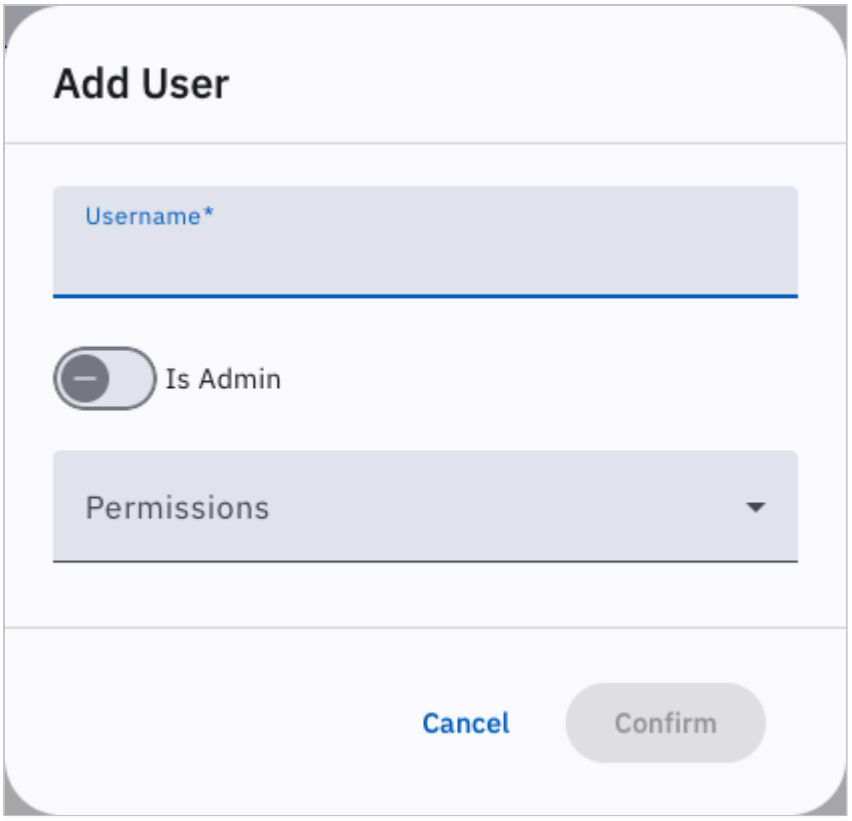
3.12.1.3. Manage Users

The "Users & Access" card lets you add, edit and delete gateway users, and edit their permissions.

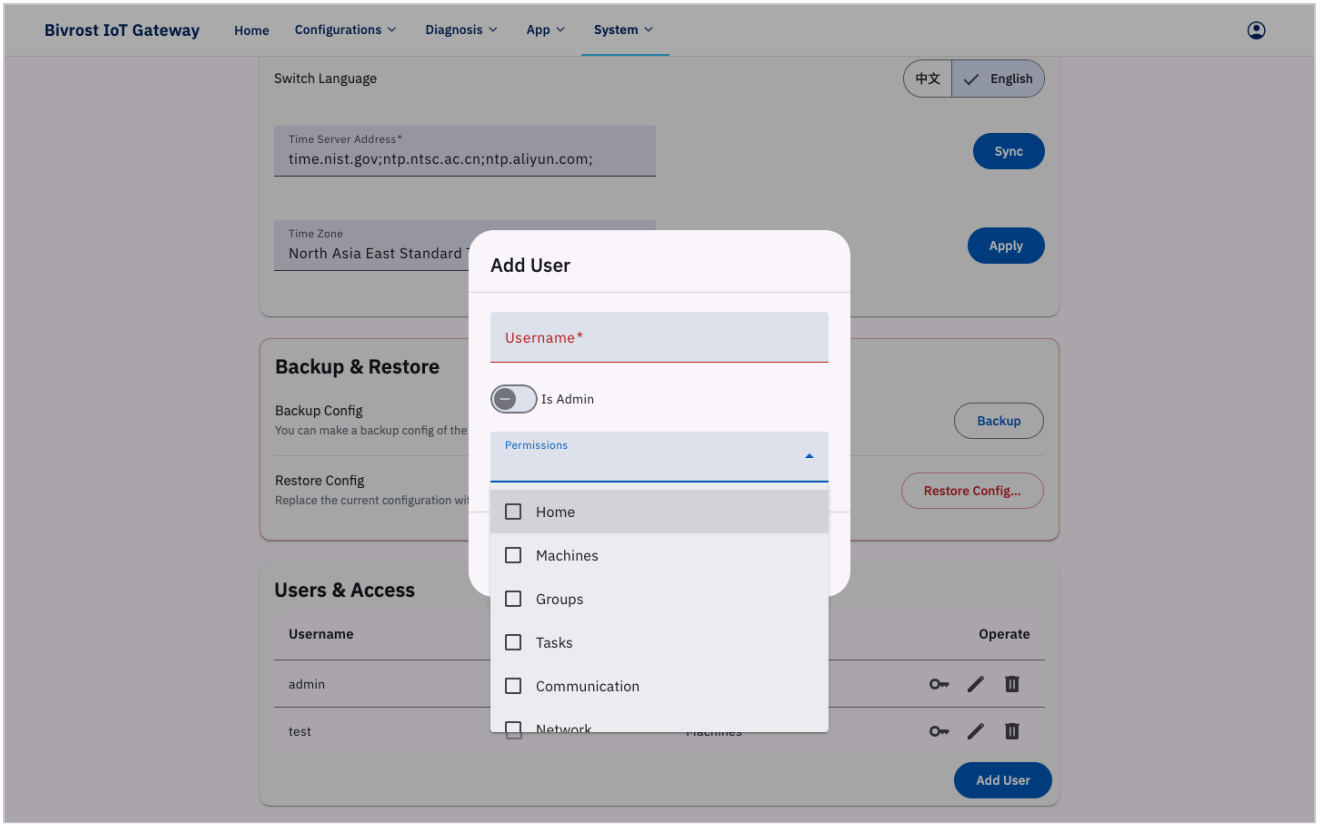


3.12.1.3.1. Add User

Click the **Add User** button on the card to create a new user.

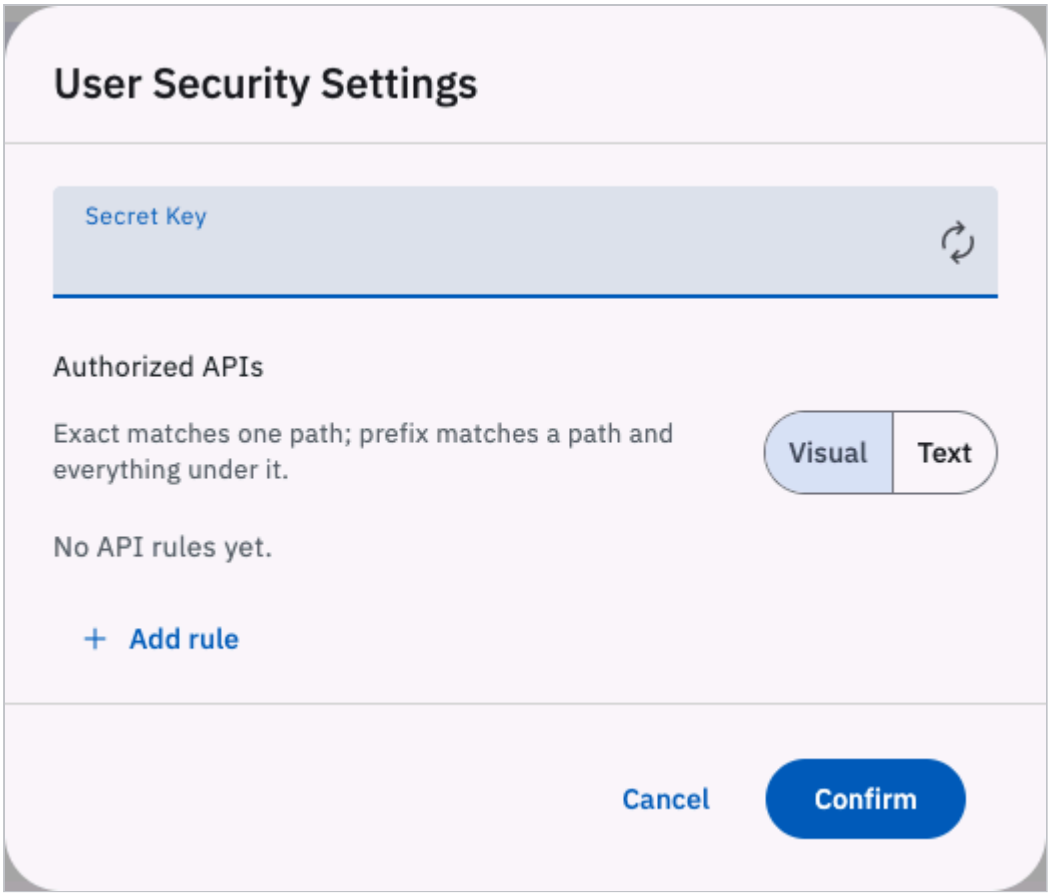


In the dialog that opens, set the username, choose whether the user is an administrator, and assign permissions. A new user’ s initial password is the same as the username. There are two user types: administrator and standard user. An administrator has full access to every page and setting on the gateway. A standard user can only open the pages granted to them; tick those pages in the permissions box. Click Confirm when you are done.



3.12.1.3.2. User Security Settings

In the management dialog, click the shield button 🛡 in the action column of a user’ s row to open the User Security Settings dialog, where you can set a Secret Key and Authorized APIs. User security settings only take effect once the Security Control option is enabled.



The **Secret Key** authenticates a user by key when calling an API; see *Communication Protocol*, 2.3.2. Secret Key. The key must start with “sk-”. Click the **Generate Secret Key** button 🔄 to the right of the Secret Key field to generate a random key.

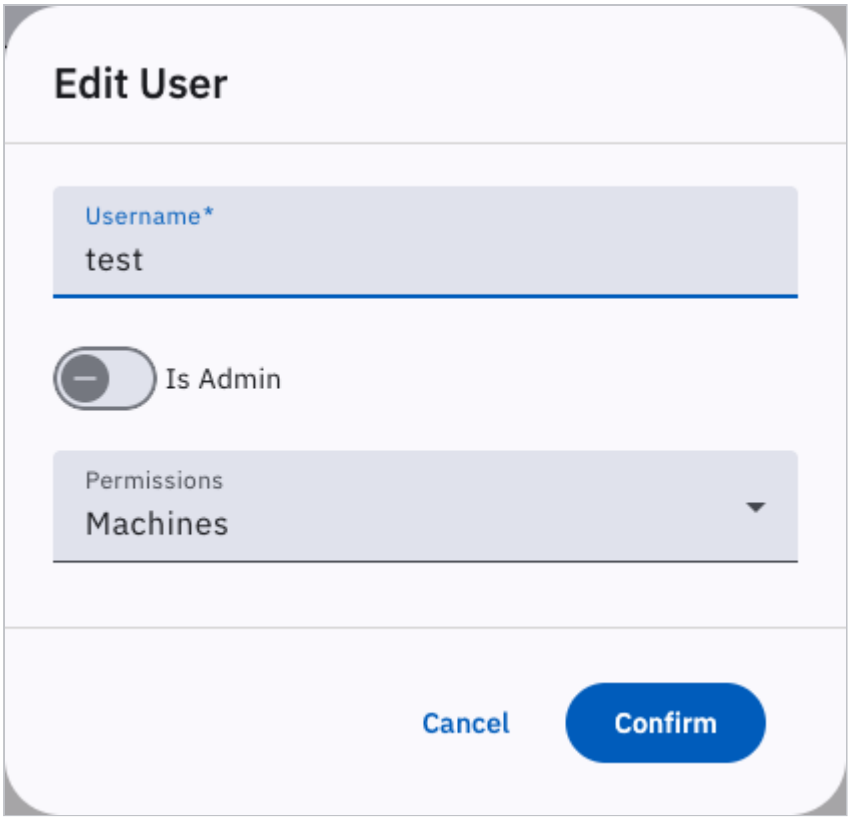
Authorized APIs specifies which interfaces the user may call; see 4.2.7. Protected API and Authorized APIs for how to set them.

> **Note**
>
> Protected APIs take precedence over authorized APIs: if an authorized API is also a protected API, the user cannot call it.

Click Confirm to save your changes.

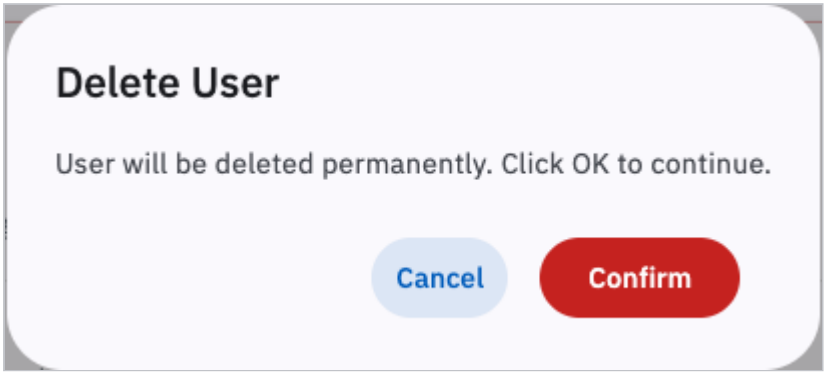
3.12.1.3.3. Edit User

In the management dialog, click the edit button ✏️ in the action column of a user’ s row to change the username, administrator status and page permissions. Click Confirm to apply the change.



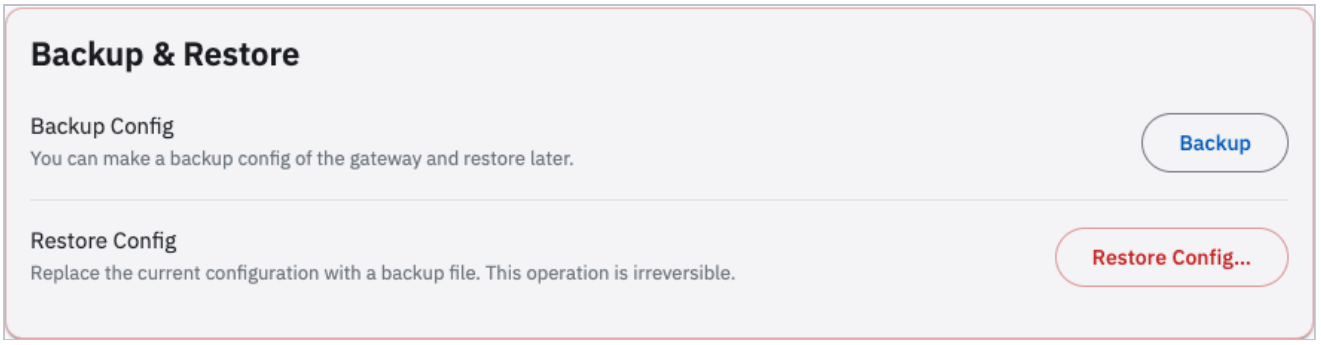
3.12.1.3.4. Delete User

In the Manage Users dialog, click the delete button 🗑 in the action column of a user’ s row and confirm to delete the user.



3.12.1.4. Backup & Restore

The “Backup & Restore” card provides two functions: Backup Config and Restore Config.

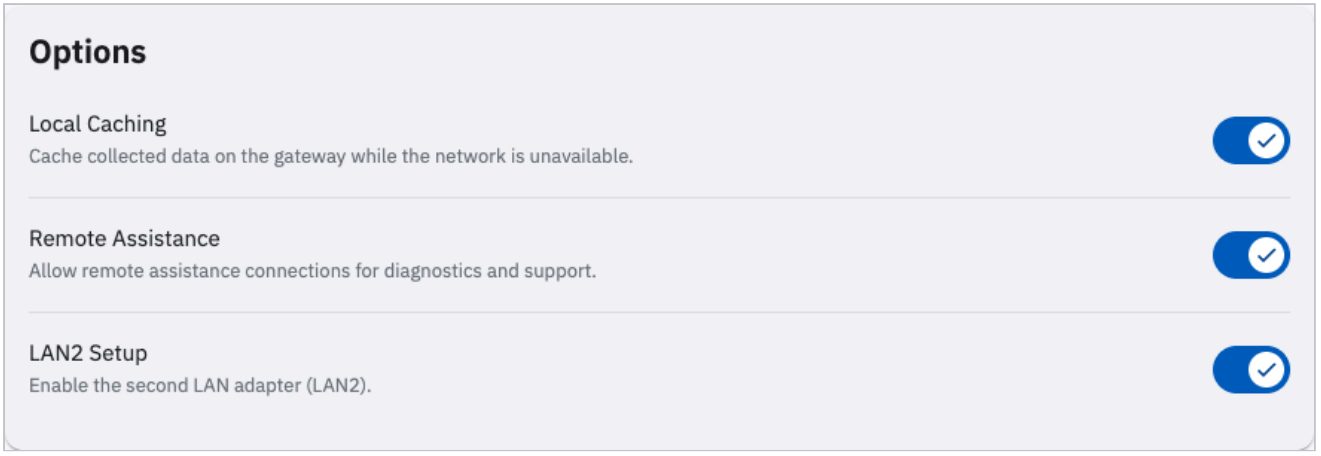


Backup Config backs up the gateway’ s current configuration file. Click the **Backup** button to download it.

Restore Config restores the gateway configuration from a backup file. Click the **Restore Config...** button and upload a gateway configuration backup file to restore the configuration. This operation cannot be undone.

3.12.2. Options

The “Gateway” card provides the Upload License and Upgrade Gateway functions; the “Options” card contains the Local Caching, Remote Assistance and LAN2 Settings switches; the “Security” card contains the Security Control option.



3.12.2.1. Upload License

Upload License... in the “Gateway” card uploads a new license file (.lic) to change the license type, raise the license count and so on. If you need to do this, contact support with the gateway UID (see 3.2.3. Gateway Details) and the license type and count you want. Once you have received the new license file on your computer, click the **Upload License...** button, select the license file in the dialog that opens, and click **Open** to upload it. When the upload finishes, click **Restart Service** on the Home page (see 3.2.1. Function Buttons) for it to take effect. After restarting the service and refreshing the Home page, check that “License Type”, “License

Count” and “License Status” under Gateway Details match what you expect; contact support if anything looks wrong.

3.12.2.2. Upgrade Gateway

Upgrade Gateway... in the “Gateway” card uploads an upgrade package (.bpkg) to update the gateway software.

The procedure is similar to “Upload License”: contact support to obtain the upgrade package, save it on your computer, then click the **Upgrade Gateway...** button to upload it. An upload progress dialog appears — please wait a moment. Once the package has uploaded successfully, a confirmation dialog appears; click **Confirm** to start the upgrade. Wait about 10 seconds, then refresh the Home page and check the gateway version under Gateway Details.

3.12.2.3. Local Caching

The “Local Caching” switch turns local caching on or off; it is on by default. Local caching stores recently collected data and run logs on the gateway so that it can serve historical data and the statistics derived from it, such as machine status statistics and count records for a past period. Data is kept locally for at most 365 days. Turning local caching off disables some gateway functions, so we recommend leaving it on. If you change this switch, click **Restart Service** on the Home page for it to take effect.

3.12.2.4. Remote Assistance

The “Remote Assistance” switch turns remote assistance on or off; it is on by default. When it is on, support staff can reach the gateway over the internet. You can turn this option off for normal operation; if you need remote assistance, contact support first, then turn the option back on once the gateway is connected to the internet. Changes to this switch take effect immediately — no **Restart Service** is needed.

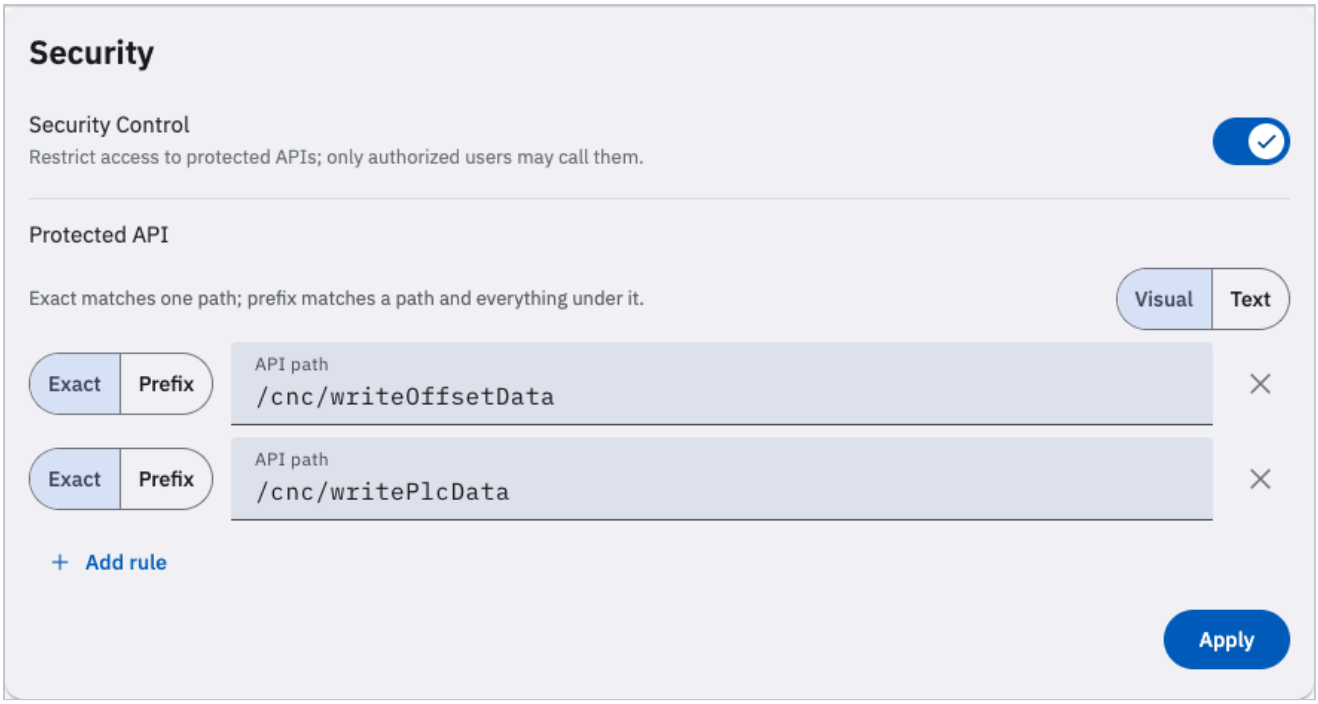
3.12.2.5. LAN2 Settings

The “LAN2 Settings” switch shows or hides the LAN2 settings on the **Network** page; it is off by default. With the switch on, you can change the LAN2 settings on the **Network** page, following the same steps used for LAN1 in 3.7.1. Wired Network.

> **Note**
>
> Turning the “LAN2 Settings” switch off after changing the LAN2 settings does not reset them.

3.12.2.6. Security Control

The “Security Control” switch turns API access control on or off; it is on by default. With the switch on, you can edit the protected APIs.

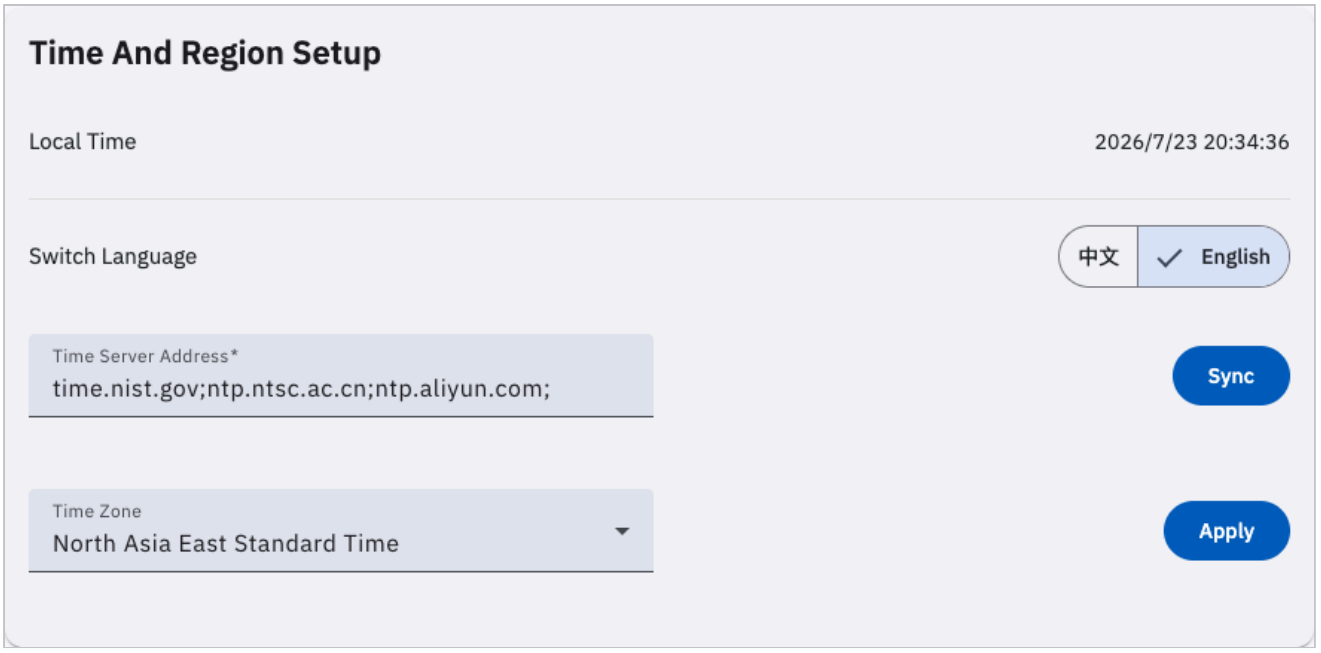


“Protected API” lists the APIs that may not be called. By default, Write Offset Data and Write PLC Data are blocked: writing incorrect data through either interface can cause injury, death or equipment damage, so only use them once you have confirmed it is safe to do so. To change the list, see 4.2.7. Protected API and Authorized APIs, then click **Apply**.

After changing “Security Control” or “Protected API”, click **Restart Service** on the Home page for the change to take effect.

3.12.3. Time And Region Setup

“Time And Region Setup” covers Local Time, Switch Language, Time Server Address and Time Zone.



3.12.3.1. Local Time

"Local Time" shows the gateway's current time.

3.12.3.2. Switch Language

"Switch Language" switches the gateway's web interface between Chinese and English. It does the same thing as the language selector at the top right of the sign-in page and the **Language** item in the account menu.

3.12.3.3. Time Server Address

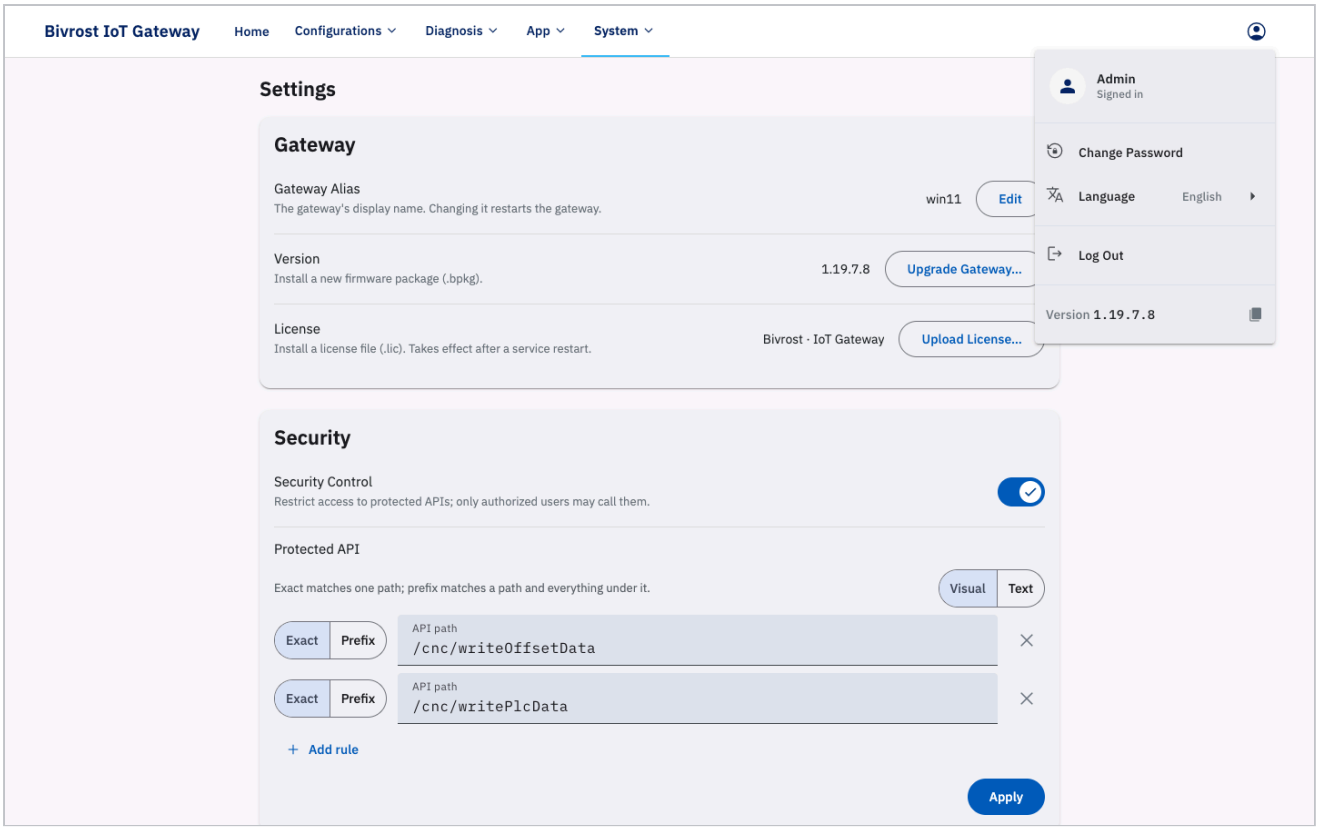
"Time Server Address" takes the addresses of the servers used for time synchronization (separate multiple addresses with ";"). The default is `ntp1.aliyun.com;ntp2.aliyun.com;ntp3.aliyun.com;ntp4.aliyun.com;`, the Alibaba Cloud public time servers, which require an internet connection. Click the **Sync** button on the right to synchronize the time: the gateway starts with the first address and moves on to the next one if it fails, stopping as soon as one succeeds. The current time server address is saved only if synchronization succeeds.

3.12.3.4. Time Zone

"Time Zone" selects the time zone the gateway is in. The default is "China Standard Time", i.e. Beijing time. Click the **Apply** button to save.

3.13. Other

The **Account** button is at the top right of the page. Click it to open the account menu, which contains **Change Password**, **Language**, **Log Out** and other options. The current gateway version is shown at the bottom (click to copy it to the clipboard).



Click **Log Out** to sign out of the current session.

4. Appendices

This chapter has four parts: a glossary, a command format reference, the optional cluster failover feature, and the MCP service:

- 4.1. Glossary: definitions and calculation methods for concepts such as Machine OEE Data, Group OEE Data and Group Part Count.
- 4.2. Command Format: the format of commands such as PLC Data Task, Precondition, Task Interval, Post-processing (DA / $POST$ / $MOCK$), External PLC Data Task, External Machines, Protected API and Authorized APIs.
- 4.3. Cluster Failover (Optional): how the shared standby pool works, how to build it, failover and switch-back behaviour, forced takeover, and what is not replicated.
- 4.4. MCP Service: how to enable and authenticate the gateway’ s built-in MCP server, call it through the cloud platform, and configure clients so AI tools can query machine data in natural language.

4.1. Glossary

4.1.1. Machine OEE Data

Machine OEE (Overall Equipment Efficiency) data includes figures such as the machine’s Off time, Wait time, Emergency time, Autorun time and Manual time, as well as its Availability.

Take machine autorun time as an example: it is the time the machine spent in automatic operation during the monitoring window. The monitoring window is set under “Monitor Mode” in 3.5.3. OEE Monitoring Settings.

```
Machine Availability = Autorun Time / Total Time
```

Here, Autorun Time is the machine’s autorun time and Total Time is the monitoring window.

OEE data requires local caching, so turn on the “Local Caching” switch under 3.12. Settings - Options.

4.1.2. Group OEE Data

Group OEE data includes figures such as the group’s Off time, Wait time, Emergency time, Autorun time and Manual time, as well as its Availability.

Take group autorun time as an example: it is the sum of the time the group’s activated machines spent in automatic operation during the monitoring window. The monitoring window is set under “Monitor Mode” in 3.5.3. OEE Monitoring Settings.

```
Group Availability = Autorun Time / Total Time
```

Here, Autorun Time is the group’s autorun time and Total Time is the total monitoring window, that is, the monitoring window multiplied by the number of activated machines in the group.

OEE data requires local caching, so turn on the “Local Caching” switch under 3.12. Settings - Options.

4.1.3. Group Part Count

The group part count is the group’s cumulative part count. It is calculated as follows:

```
Group Part Count = (Machine 1 Cumulative Part Count - Machine 1
Initial Value) * Machine 1 Count Multiplier
                 + (Machine 2 Cumulative Part Count - Machine 2 Initial
Value) * Machine 2 Count Multiplier
                 + ...
```

The initial value is that machine’s cumulative part count the first time the group part count was collected after the machine joined the group. The group part count is stored on the gateway and bound to the group number, and is never reset.

The group part count requires local caching, so turn on the “Local Caching” switch under 3.12. Settings - Options.

4.2. Command Format

4.2.1. PLC Data Task

A PLC data task has the format below. Separate multiple reads with “;” .

```
Area,Start Address[|Tag],Data Count,Data Type[,Precondition,Task
Interval,Post-processing];
```

Area, Start Address, Data Count and Data Type are mandatory — together they define where the data comes from and what shape it has. Tag, Precondition, Task Interval and Post-processing are optional.

- **Tag** identifies the data in MQTT, database and other communication channels. If you do not set one, the gateway assigns it automatically from the task order and the data length.
- **Precondition** is the precondition for this command. It is evaluated first, and the command runs only if the condition is met; if it is not set, the command always runs. It works exactly like 3.3.1.2.1. Precondition. For the syntax, see 4.2.2. Precondition.
- **Task Interval** is the interval for this command. If it is not set, the gateway uses the matching interval from 3.5.1. Machine Task Interval Settings and 3.5.2. Group Task Interval Settings. For the syntax, see 4.2.3. Task Interval.
- **Post-processing** may appear more than once. Each post-processing expression transforms data returned by this task or by another task and publishes the result under a new tag. See 4.2.4. Post-processing.

Taking [CNC]Fanuc [Oi-F] as an example:

```
R,0,9,Byte;
R,100|Data2,6,Byte,$COND$CNCStatus_cncStatus = "AUTO_RUN"$COND$;
R,200|rawData0,1,Byte,$INTERVAL$1000$INTERVAL$,$POST$___PLC_TrawData0___[0]>
```

- `R,0,9,Byte` reads 9 values of type Byte starting at PLC address R0 (R0 included), with no tag set.
- `R,100|Data2,6,Byte` reads 6 values of type Byte starting at PLC address R100 (R100 included), tagged “Data2” , with the precondition `CNCStatus_cncStatus = "AUTO_RUN"` — that is, only while the machine is in automatic operation. For more on preconditions, see 4.2.2. Precondition.

- `R,200|rawData0,1,Byte` reads one value of type Byte at PLC address R200, tagged "rawData0". `$INTERVAL$1000$INTERVAL$` sets the interval for this command to 1000 milliseconds. `$POST$___PLC_TrawData0___[0]>0$POST$|Heartbeat` is a post-processing expression and its tag: it tests whether the value read into rawData0 is greater than 0 and publishes the result under the tag "Heartbeat". For more on post-processing, see 4.2.4. Post-processing.

Taking [PLC]Simatic [S300] as an example:

```
DB1,1,3,Byte;DB10,100|FloatData,10,Float;
```

- `DB1,1,3,Byte` reads 3 values of type Byte starting at PLC address DB1.1 (DB1.1 included), with no tag.
- `DB10,100|FloatData,10,Float` reads 10 values of type Float starting at PLC address DB10.100 (DB10.100 included), tagged "FloatData".

Some devices support reading data by variable name. Taking [PLC]Allen-Bradley [1783] as an example:

```
$TAG$|name=AB.C[0],,8,Float;
```

`$TAG$|name=AB.C[0],,8,Float` reads elements 0 through 7 of the Float array held in the PLC variable named AB.C, addressed by tag. Note that the field corresponding to Start Address is left empty in this form.

For a fuller description of Area, Start Address, Data Count, Data Type and the other parameters, see the request-parameter section of *Communication Protocol* 2.5.1.18. readPlcData (Read PLC Data).

Consult the device manual or contact the device manufacturer to obtain the area and address of the target PLC data and the type of the target data.

4.2.2. Precondition

A precondition sets the prerequisite for running a task: the collection task runs only when the condition you set is met. If it is left blank, there is no precondition and the task runs directly.

For non-PLC data tasks you set the precondition in 3.3.1.2.1. Precondition. For PLC data tasks you add a precondition command inside the command itself, in this format:

```
$COND$Precondition$COND$
```

A precondition is essentially a logical test. A single precondition command looks like this:

```
a > 100              // variable a is greater than 100
b < 50.0f            // variable b is less than 50.0f
c = "AUTO_RUN"       // variable c is the string "AUTO_RUN"
d <> 0               // variable d is not equal to 0
e >= 12.34f          // variable e is greater than or equal to 12.34f
f <= g               // variable f is less than or equal to variable g
not h in (1,2,3)     // variable h is not one of (1,2,3)
```

Several precondition commands can be combined with and, or and (), for example:

```
a > 100 and (b < 50.0f or c = "AUTO_RUN")
```

The variables currently available for logical tests are `<type>_<tag>` and `prev_<type>_<tag>`, where `<type>` is the data class, `<tag>` is the data tag, and prev refers to the previous value of the data. For details on `<type>` and `<tag>`, see *Communication Protocol* 1.2. Data Description.

4.2.3. Task Interval

The task interval sets the interval for a specific task. If it is not set, the gateway uses the matching interval from 3.5.1. Machine Task Interval Settings and 3.5.2. Group Task Interval Settings. The format is:

```
$INTERVAL$Interval$INTERVAL$
```

Interval is a number, in milliseconds.

4.2.4. Post-processing

Post-processing commands let you transform the raw data you collect. Two kinds are currently available:

4.2.4.1. DA Direct Access

DA takes a single value at a given position out of the data read by the command to its left and publishes it under a given tag. It cannot perform calculations, but it lets you merge PLC tasks whose addresses are adjacent, reducing the number of PLC tasks and improving execution efficiency. For example:

```
R,2036|count,4,Int32,
$DA$0$DA$|Part Count,
$DA$3$DA$|Part Count-Good,
$DA$4$DA$|Part Count-Reject;
```

This reads 4 Int32 values starting at R2036, giving an array of length 4. DA then takes element 0 and tags it Part Count, takes element 3 and tags it Part Count-Good, takes element 4 and tags it Part Count-Reject, and uploads these three values.

If a DA tag is not specified, the default tag is `<raw data tag>_<number>`, where the number is the position given to DA. Had the example above set no tags, the three values would default to `count_0`, `count_3` and `count_4`.

4.2.4.2. $POST$ Post-processing

$POST$ performs calculations, comparisons and similar processing on one or more values that have already been collected, and uploads the result.

The gateway keeps the most recent task data as variables. Variables belonging to the same machine can be referenced inside $POST$ using the format `___VariableName___` — three underscores before and after the variable name to mark its start and end. Take `___PLC_TrawData2_data___`: PLC is the data type, T is the abbreviation for tag, rawData2 is the data's tag, and data is a field of the PLC data class, which is an array. Together the variable name is `PLC_TrawData2_data`, meaning the PLC data class, with tag T set to rawData2 and field data — that array. Adding three underscores at each end per the variable format gives `___PLC_TrawData2_data___`. For details on data classes, data tags and fields, see *Communication Protocol* 1.2. Data Description. This mechanism lets you use, inside $POST$, any data collected by any enabled task.

The gateway keeps at most the two most recent sets of task data. The most recent set is addressed as described above; for the set before it, add the prefix `prev_` to the variable name, for example `___prev_PLC_TrawData2_data___`.

Example 1:

```
R,2000|rawData2,1,Byte,
$INTERVAL$900$INTERVAL$,
$POST$(___PLC_TrawData2_data___[0] and 1>0$POST$|Heartbeat;
```

Every 900 milliseconds, one Byte is read starting at R2000, giving an array of length 1 stored under the tag rawData2. Inside $POST$, the value at position 0 of that rawData2 array is taken; if it is greater than 0 the result is True, otherwise False, and the result is uploaded under the tag Heartbeat.

You can use several $POST$ expressions in a single PLC data task to perform different calculations, as in Example 2 and Example 3.

Example 2:

```
R,3012|rawData3,3,Int32,
$POST$___PLC_TrawData3_data___[0]*0.1f$POST$|Tool-to-Tool Change Time,
$POST$___PLC_TrawData3_data___[1]*0.1f$POST$|Total Tool Change Time,
$POST$___PLC_TrawData3_data___[2]*0.1f$POST$|Tool Machining Time;
```

The raw values are Int32 in units of [0.1 s]; each is multiplied by 0.1f to convert it to a Float in units of [s].

Example 3:

```
R,2003|rawData4,1,Byte,
$POST$(___PLC_TrawData4_data___[0] and (1<<4))>0$POST$|Data Ready,
$POST$(___PLC_TrawData4_data___[0] and (1<<5))>0$POST$|Part Data Ready,
$POST$(___PLC_TrawData4_data___[0] and (1<<6))>0$POST$|Part OK,
$POST$(___PLC_TrawData4_data___[0] and (1<<7))>0$POST$|Part NG;
```

The raw value is a single Byte in which each bit has a different meaning. Bit 4 of the Byte is taken (bit 0 being the least significant bit) and compared with 0, giving True or False, tagged Data Ready; bit 5 is tested for greater than 0 and tagged Part Data Ready; bit 6 is tested and tagged Part OK; bit 7 is tested and tagged Part NG.

Besides the usual +, -, *, /, and, or, <, >, = operators, the gateway also supports nested if tests. Example 4 derives the current status from a PLC value.

Example 4:

```
D,0|rawData0,1,Int16,
$POST$if(___PLC_TrawData0_data___[0] = 1, "AUTO_RUN",
if(___PLC_TrawData0_data___[0] = 2,"MANUAL_HOLD",
if(___PLC_TrawData0_data___[0] = 4, "EMERGENCY", "WAIT")))$POST$|Machine
Status,
$POST$if(___PLC_TrawData0_data___[0] = 4, "ALARM",
if(___PLC_TrawData0_data___[0] = 5, "ALARM", "NO_ALARM"))$POST$|Alarm
Status;
```

The value of D0 represents the state of the machine. D0=1: automatic operation; D0=2: paused; D0=4: emergency stop; D0=5: alarm present; any other value of D0: Wait. D0=4 and D0=5 both count as an alarm state.

4.2.4.3. $POST$ Post-processing Functions

Inside a $POST$ command you can call methods on .NET static members such as Encoding, Enumberable, BitConverter and Math.

The following functions extract a sub-array from a source array; each name applies to arrays holding the corresponding element type:

```
PGetSubBytes,
PGetSubSBytes,
PGetSubChars,
PGetSubShorts,
PGetSubUShorts,
PGetSubInts,
PGetSubUInts,
PGetSubFloats,
PGetSubLongs,
PGetSubULongs,
PGetSubDoubles;
```

Input	Type	Description
source	Object[]	(Required) The source array
startIndex	Int32	(Required) The start position

Input	Type	Description
count	Int32	(Required) The number of elements
isReverse	Bool	Whether to reverse the order; False by default
isSwap	Bool	Whether to swap elements in pairs; False by default
step	Int32	The step, i.e. the gap between the elements taken; 0 by default

These functions build a sub-array out of the source array: they start at the element at the start position, skip the specified number of elements (0 by default) to reach the next one, and continue until the specified number of elements has been collected. The sub-array is then reversed if you asked for it (off by default), and finally its elements are swapped in pairs if you asked for it (off by default).

PGetSubBytes example:

```
source = {0x01, 0x02, 0x30, 0x40, 0x66, 0x88},
startIndex = 1,
count = 3,
isReverse = True,
isSwap = True,
step = 1,
```

Three elements are taken starting at position 1 with a gap of 1, giving `{0x02, 0x40, 0x88}`. Reversing them gives `{0x88, 0x40, 0x02}`. They are then swapped in pairs — note that the length 3 is odd, so the last element takes no part in the pairwise swap. The result is `{0x40, 0x88, 0x02}`.

Functions of this kind suit cases where a single PLC data task reads a large block of data from which each individual value is then parsed out and reported separately as a post-processing result. Handling it this way improves communication efficiency enormously. In the example below, 198 Bytes are read from a Siemens PLC in one go and converted, according to their address offsets, into String / Bool / UInt16 / Float / UInt32 and other types.

```
DB500,0|rawData0,198,Byte,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 0,
8))$POST$|Production Line,
```

```
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 8,
6))$POST$|Process No,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 14,
1))$POST$|Machine No,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 18,
20))$POST$|System Device No,
$POST$ToUInt16(PGetSubBytes(___PLC_TrawData0_data___, 38, 2, true),
0)$POST$|Device Status,
$POST$(___PLC_TrawData0_data___[40] and 1)>0$POST$|Device On,
$POST$(___PLC_TrawData0_data___[40] and (1<<1))>0$POST$|Device Off,
$POST$(___PLC_TrawData0_data___[40] and (1<<3))>0$POST$|Emergency,
$POST$(___PLC_TrawData0_data___[40] and (1<<4))>0$POST$|Device Fault Stop,
$POST$(___PLC_TrawData0_data___[40] and (1<<6))>0$POST$|Other Mode,
$POST$(___PLC_TrawData0_data___[40] and (1<<7))>0$POST$|Pass-Through Mode,
$POST$(___PLC_TrawData0_data___[41] and 1)>0$POST$|Auto Mode,
$POST$(___PLC_TrawData0_data___[41] and (1<<1))>0$POST$|Non-Auto Mode,
$POST$(___PLC_TrawData0_data___[41] and (1<<2))>0$POST$|Cycle Start,
$POST$(___PLC_TrawData0_data___[41] and (1<<3))>0$POST$|Cycle Stop,
$POST$(___PLC_TrawData0_data___[41] and (1<<4))>0$POST$|Special Mode,
$POST$(___PLC_TrawData0_data___[41] and (1<<5))>0$POST$|Dry Run,
$POST$(___PLC_TrawData0_data___[41] and (1<<6))>0$POST$|Material Jam,
$POST$(___PLC_TrawData0_data___[41] and (1<<7))>0$POST$|Waiting for
Material,
$POST$(___PLC_TrawData0_data___[42] and 1)>0$POST$|In Production,
$POST$(___PLC_TrawData0_data___[42] and (1<<1))>0$POST$|Device Alarm,
$POST$(___PLC_TrawData0_data___[42] and (1<<2))>0$POST$|Safety Door Open,
$POST$(___PLC_TrawData0_data___[42] and (1<<3))>0$POST$|Safety Door
Closed,
$POST$(___PLC_TrawData0_data___[44] and 1)>0$POST$|Station 1 Load Request,
$POST$(___PLC_TrawData0_data___[44] and (1<<1))>0$POST$|Station 1 Unload
Request,
$POST$(___PLC_TrawData0_data___[44] and (1<<2))>0$POST$|Station 1 Part
Present,
$POST$(___PLC_TrawData0_data___[46] and 1)>0$POST$|Station 2 Load Request,
$POST$(___PLC_TrawData0_data___[46] and (1<<1))>0$POST$|Station 2 Unload
Request,
$POST$(___PLC_TrawData0_data___[46] and (1<<2))>0$POST$|Station 2 Part
Present,
$POST$(___PLC_TrawData0_data___[48] and 1)>0$POST$|Station 3 Load Request,
```

```
$POST$(___PLC_TrawData0_data___[48] and (1<<1))>0$POST$|Station 3 Unload
Request,
$POST$(___PLC_TrawData0_data___[48] and (1<<2))>0$POST$|Station 3 Part
Present,
$POST$(___PLC_TrawData0_data___[50] and 1)>0$POST$|Station 4 Load Request,
$POST$(___PLC_TrawData0_data___[50] and (1<<1))>0$POST$|Station 4 Unload
Request,
$POST$(___PLC_TrawData0_data___[50] and (1<<2))>0$POST$|Station 4 Part
Present,
$POST$(___PLC_TrawData0_data___[52] and 1)>0$POST$|Station 5 Load Request,
$POST$(___PLC_TrawData0_data___[52] and (1<<1))>0$POST$|Station 5 Unload
Request,
$POST$(___PLC_TrawData0_data___[52] and (1<<2))>0$POST$|Station 5 Part
Present,
$POST$(___PLC_TrawData0_data___[54] and 1)>0$POST$|Load Station Load
Request,
$POST$(___PLC_TrawData0_data___[54] and (1<<1))>0$POST$|Load Station
Unload Request,
$POST$(___PLC_TrawData0_data___[54] and (1<<2))>0$POST$|Load Station Part
Present,
$POST$(___PLC_TrawData0_data___[56] and 1)>0$POST$|Unload Station Load
Request,
$POST$(___PLC_TrawData0_data___[56] and (1<<1))>0$POST$|Unload Station
Unload Request,
$POST$(___PLC_TrawData0_data___[56] and (1<<2))>0$POST$|Unload Station
Part Present,
$POST$ToUInt16(PGetSubBytes(___PLC_TrawData0_data___, 58, 2, true),
0)$POST$|Axis Position_TY,
$POST$ToUInt16(PGetSubBytes(___PLC_TrawData0_data___, 60, 2, true),
0)$POST$|Axis Position_TZ1,
$POST$ToUInt16(PGetSubBytes(___PLC_TrawData0_data___, 62, 2, true),
0)$POST$|Axis Position_TZ2,
$POST$ToUInt16(PGetSubBytes(___PLC_TrawData0_data___, 64, 2, true),
0)$POST$|Axis Position_TX1,
$POST$ToUInt16(PGetSubBytes(___PLC_TrawData0_data___, 66, 2, true),
0)$POST$|Axis Position_TX2,
$POST$(___PLC_TrawData0_data___[68] and 1)>0$POST$|Gripper 1 Clamped,
$POST$(___PLC_TrawData0_data___[68] and (1<<1))>0$POST$|Gripper 2 Clamped,
$POST$ToSingle(PGetSubBytes(___PLC_TrawData0_data___, 70, 4, true),
0)$POST$|Cycle Time (excluding wait),
```

```
$POST$(___PLC_TrawData0_data___[74] and 1)>0$POST$|Data Ready,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 76,
28))$POST$|Part QR Code,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 104,
10))$POST$|RFID_Process No,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 114,
2))$POST$|RFID_Spindle No,
$POST$ToUInt16(PGetSubBytes(___PLC_TrawData0_data___, 116, 2, true),
0)$POST$|RFID_Part Status,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 118,
2))$POST$|RFID_Inspection Info,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 120,
12))$POST$|Machining Time,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 130, 4, true),
0)$POST$|Alarm Code 1,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 134, 4, true),
0)$POST$|Alarm Code 2,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 138, 4, true),
0)$POST$|Alarm Code 3,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 142, 4, true),
0)$POST$|Alarm Code 4,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 146, 4, true),
0)$POST$|Alarm Code 5,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 150, 4, true),
0)$POST$|Alarm Code 6,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 154, 4, true),
0)$POST$|Alarm Code 7,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 158, 4, true),
0)$POST$|Alarm Code 8,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 162, 4, true),
0)$POST$|Alarm Code 9,
$POST$ToUInt32(PGetSubBytes(___PLC_TrawData0_data___, 166, 4, true),
0)$POST$|Alarm Code 10,
$POST$UTF8.GetString(PGetSubBytes(___PLC_TrawData0_data___, 170,
28))$POST$|Station 1 Part QR Code;
```

4.2.4.4. $MOCK$ Mock Task

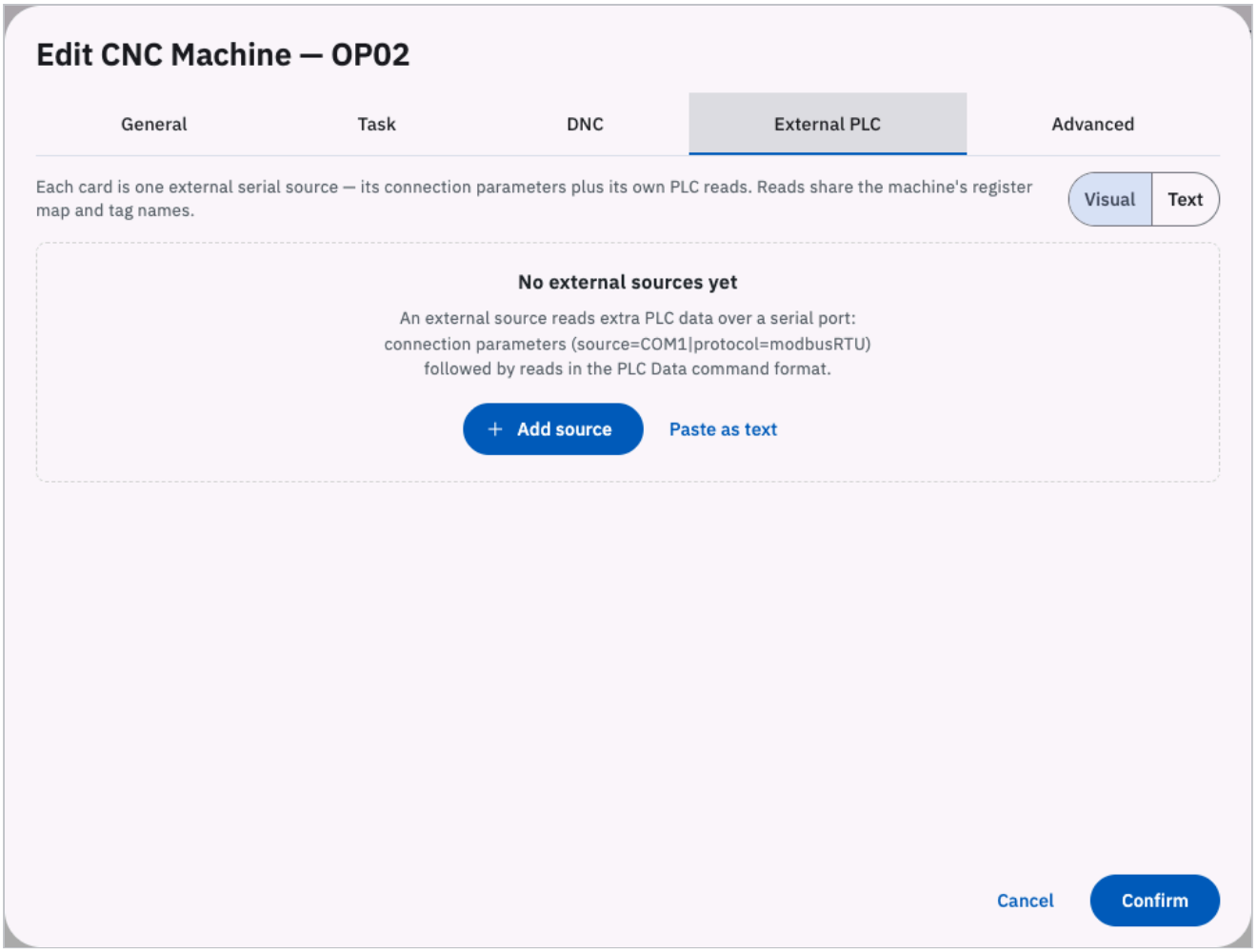
A $MOCK$ task returns the requested number of dummy values of the requested type. The returned values carry no real meaning; they exist only for a few special situations. Post-processing cannot stand on its own — it must follow the mandatory part of a PLC task. In some cases, however, the post-processing needs a different interval from the data read, or for other reasons has to be set up as a task of its own. A $MOCK$ task covers those cases.

```
$MACRO$,500|macro1_500_515,16,Double,
$DA$0$DA$,$DA$1$DA$,$DA$2$DA$,$DA$3$DA$,$DA$4$DA$,$DA$5$DA$,$DA$6$DA$,
$DA$7$DA$,$DA$8$DA$,$DA$9$DA$,$DA$10$DA$,$DA$11$DA$,$DA$12$DA$,$DA$13$DA$,
$DA$14$DA$,$DA$15$DA$;
$MOCK$,1,1,Byte,
$INTERVAL$60000$INTERVAL$,
$POST$(___PLC_Tmacro1_500_515_8_pDouble___ -
___PLC_Tmacro1_500_515_0_pDouble___)<=10$POST$|Cutoff Tool Life Low;
```

Here the first task reads machine macro variables 500 to 515 at the default interval of once every 5 seconds. The second task runs once a minute, subtracts macro variable 500 from macro variable 507 as read by the first task, and tests whether the difference is less than or equal to 10. The result, True or False, is uploaded under the tag “Cutoff Tool Life Low”.

4.2.5. External PLC Data Task

The gateway can collect data from equipment around the machine by adding an external PLC.



The command has three parts: the parameters of the external PLC, the parameters of the communication protocol, and the PLC read commands.

Parameters of the external PLC:

Parameter	Description
source	Data source. Allowed values: COM1, COM2, COM3 and so on, corresponding to serial ports 1-3 on the gateway.
protocol	Communication protocol. Allowed value: modbusRTU.
baudRate	Serial baud rate. Default 9600.
parity	Parity bit. Allowed values: none, odd, even. Default none.
dataBits	Data bits. Default 8.
stopBits	Stop bits. Allowed values: 1, 1.5, 2. Default 1.

Supported communication protocols:

modbusRTU

Parameter	Description
slaveID	Slave ID. Default 1.
plcAddresses	Whether the addresses are PLC addresses. Allowed values: false, true. Default false. When true, Modbus addresses start at 1; when false, Modbus addresses start at 0.
encoding	Encoding. Default GBK.
bit32TypeFormat	32-bit type format (Byte(4) Order). Allowed values: ABCD, CDAB, BADC, DCBA. Default DCBA.
bit64TypeFormat	64-bit type format (Byte(8) Order). Allowed values: ABCDEFGH, GHEFCDAB, BADCFEHG, HGFEDCBA. Default HGFEDCBA.

For the PLC read commands, see 4.2.1. PLC Data Task.

Example:

With a temperature sensor on the machine’s serial port 1 and a smart power meter on serial port 2, you can set up two external PLC task commands to collect the machine’s temperature and energy consumption.

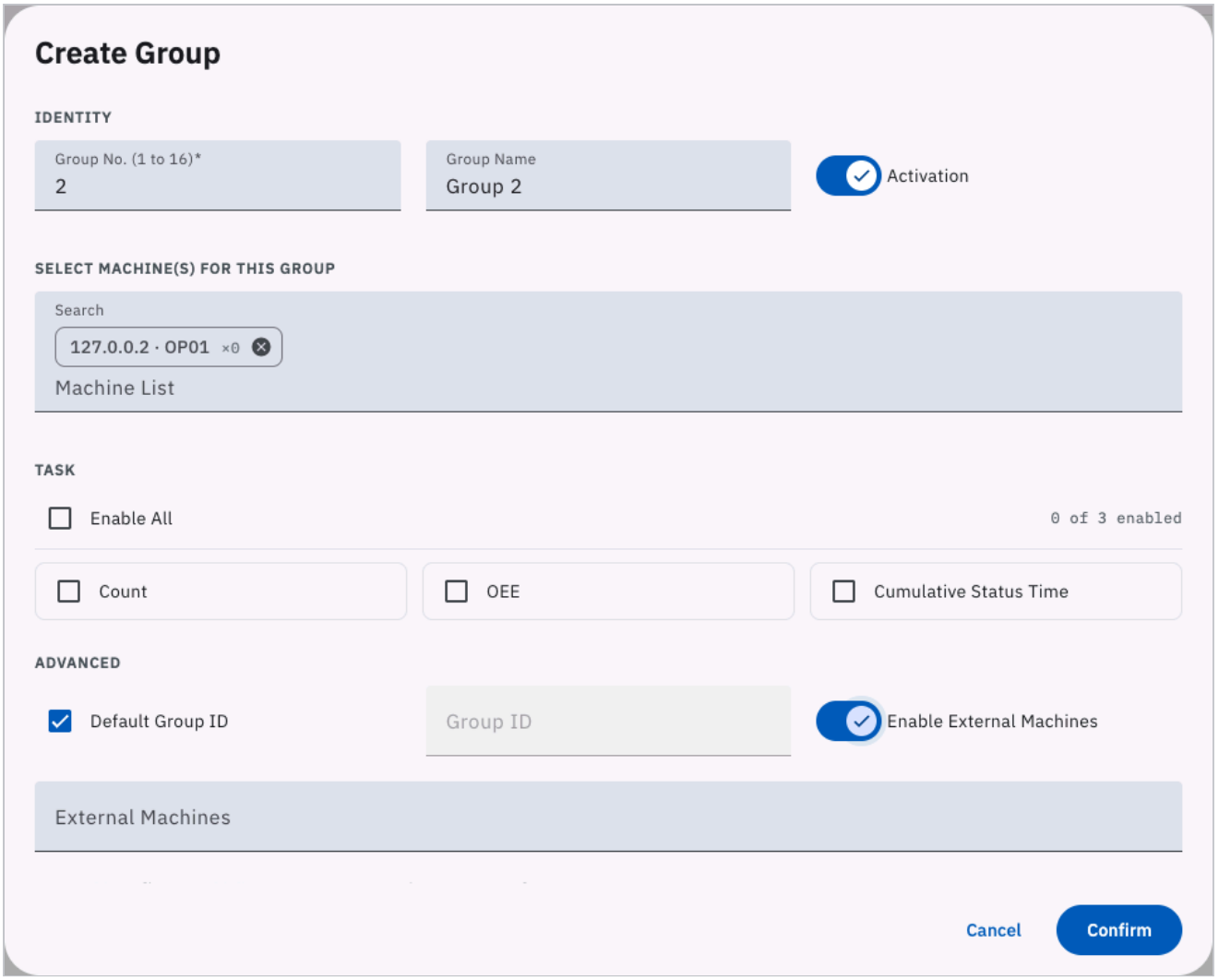
```
source=COM1|protocal=modbusRTU;4x,0,1,Int16;
source=COM2|protocal=modbusRTU|baudRate=14400|encoding=ASCII;4x,0,1,Int16;4x
```

Separate different data sources with a line break.

- First line: over gateway serial port 1, using the modbusRTU protocol, read 1 Int16 from area 4x starting at address 0.
- Second line: over gateway serial port 2, using the modbusRTU protocol with the baud rate set to 14400 and the encoding set to ASCII, read 1 Int16 from area 4x starting at address 0, and 2 Int32 starting at address 10.

4.2.6. External Machines

By adding external machines you can bring machines belonging to other gateways into a group on this gateway. You must first link the other gateway in Cloud Settings or Hub Settings.



The command format is:

```
UID,MachineID[|countMultiplier=COUNTMULTIPLIER|name=NAME,...];...
```

UID is the UID of the other, already linked gateway; MachineID is the machine number of the machine on that gateway; countMultiplier is the Count Multiplier, optional, 0 by default; name is the Machine Name, optional, the same as MachineID by default. Separate multiple external machines with ";". For example:

```
iotgw1,1;iotgw2,100010|countMultiplier=1|name=Machining Center 10;
```

4.2.7. Protected API and Authorized APIs

API commands are used to configure protected APIs and authorized APIs.

The command format is:

```
Command Type,API address prefix or API address;
```

An API address is the part after “/api” of the address of each interface in *Communication Protocol* 2.5. Data Read/Write Interfaces through 2.10. Gateway Function Interfaces. Separate multiple commands with “;” .

There are two command types: prefix match and exact match.

1. Prefix match covers every API address that begins with the given prefix:

```
prefix,/cnc;prefix,/analysis;prefix,/config;
```

Here prefix denotes a prefix match; /cnc covers every API whose address starts with /cnc, that is *Communication Protocol* 2.5. Data Read/Write Interfaces and 2.6. File Management Interfaces; /analysis covers every API whose address starts with /analysis, that is *Communication Protocol* 2.7. Data Analysis Interfaces; /config covers every API whose address starts with /config, that is *Communication Protocol* 2.9. Gateway Configuration Interfaces.

> **Caution**
>
> The following command covers every API:
>
> ```
> prefix,/;
> ```
>
> Leaving it blank covers no API at all.

2. Exact match names the address of one specific API:

```
exact,/cnc/writeOffsetData;exact,/cnc/writePlcData;
```

Here exact denotes an exact match; /cnc/writeOffsetData is the address of the interface that writes tool offset data, see *Communication Protocol* 2.5.1.14. writeOffsetData (Write Offset Data); /cnc/writePlcData is the address of the interface that writes PLC data, see *Communication Protocol* 2.5.1.19. writePlcData (Write PLC Data).

4.3. Cluster Failover (Optional)

Cluster failover is an optional gateway feature that shortens the collection outage caused by a whole-host gateway failure (power loss, hardware fault, system crash). All gateways under the same cloud platform share one pool of standby hosts: when any gateway fails as a whole, the cloud platform assigns an idle standby to take it over and run under that gateway’s identity. Once the original gateway is repaired, comes back online and stays stable, the system switches back automatically and the standby returns to the pool. The standby may sit at a different site, which makes this an off-site disaster-recovery setup.

> **Note**
>
> This feature requires the gateway to be connected to the Bivrost cloud platform. With no standby pool configured, a gateway behaves exactly as in a normal deployment.

4.3.1. How It Works

- **Shared standby pool**: a standby is not tied to one gateway. It is registered in the cloud platform’s standby pool and stands by for every gateway under that cloud platform (N+1).
- **Takeover means switching identity**: a standby does not collect while idle. When it receives a takeover command it imports the failed gateway’s configuration snapshot (machines, groups, tasks, communication settings and user accounts, plus that gateway’s cloud identity) and restarts under that gateway’s identity. The data source on the cloud platform and its dashboards follows the standby automatically — nothing upstream needs to be reconfigured.
- **One takeover at a time**: a standby covers only one gateway at any moment. If every standby is busy when another gateway fails, the cloud platform only records an event and pushes an alarm; it does not switch. As soon as a standby is released it automatically takes over the gateway that is still down. Register several standbys in the pool to cover more simultaneous failures.
- **Switchover time**: about 15 seconds (14–17 seconds measured) from the moment the gateway goes silent to the standby serving requests under that gateway’s identity with its collection engine started. Reconnecting each machine tool afterwards depends on how many machines there are and is not counted in that figure.

4.3.2. Prerequisites

1. The gateways must already be connected to the Bivrost cloud platform. The cloud platform is both the liveness arbiter and the channel used for configuration replication and takeover assignment.
2. A standby is a complete gateway host, with the same hardware and software specification as the gateways it protects.
3. The standby and the protected gateways should run the same software version. A takeover still works across versions, but it records a version-mismatch event; only run that way during a rolling-upgrade window.
4. The standby needs a licence bound to its own hardware, see 3.12.2.1. Upload License.
5. **Every gateway under the cloud platform is protected by default** — there is nothing to configure per gateway. Older gateways (which report neither heartbeats nor configuration snapshots) are not protected and are greyed out on the cluster admin page.

4.3.3. Building the Standby Pool

The pool is configured on the cloud platform's **Gateway Cluster** admin page. Contact Bivrost for the page address and the admin key.

1. Install the gateways as usual and connect them to the cloud platform.
2. Install each standby the way you install an **ordinary gateway**, and note its UID (see 3.2.3. Gateway Details).
3. Open the gateway cluster admin page on the cloud platform and enter the admin key.
4. Under "Standby Pool", click **Generate** to obtain the **pool token**, click + **Standby** to add each standby (UID and name), set the **stability window** (300 seconds by default), then click **Save**.
5. On each standby, enable the cloud platform connection, set the server address to the cloud platform and the AccessToken to the **pool token** generated in the previous step, then restart the service. Once the standby reports a heartbeat it enters the waiting state automatically: collection and cloud upload are suspended, and its own web page becomes read-only and shows a standby banner.
6. Back on the cluster admin page, confirm that the standby shows "Online · Waiting", that each gateway in the protected-gateway table shows "Protected", and that its **snapshot** timestamp refreshes after you change that gateway's configuration — this confirms the replication channel works. Each standby also caches the latest configuration snapshot of every protected gateway locally, for use in the double-fault case.
7. To leave a gateway unprotected, click **Exclude** on its row; click **Protect** to bring it back.

> **Caution**
>
> The pool token is what lets a standby join the pool. Keep it safe, and do not mix it up with a gateway’s own AccessToken.

4.3.4. Failover and Switch-back

Situation	Behaviour
Whole-host gateway failure (power loss, network loss, system crash)	After the heartbeat times out (15 seconds) the cloud platform assigns an idle standby. The standby imports that gateway’s configuration snapshot, restarts, and comes online under that gateway’s identity.
The gateway only loses its link to the cloud platform and keeps collecting locally	**No switchover.** The gateway keeps collecting and uploads the backlog once the link is restored.
Another gateway fails while every standby is busy	Only an event and an alarm are recorded; no switchover. The gateway that is still down is taken over automatically as soon as a standby is released.
The original gateway is repaired and comes back online	It is first put into read-only mode with collection stopped (to prevent dual collection). Once it has been online continuously for the **stability window**, the system switches back: the standby releases the identity and restarts back into the pool, and the original gateway pulls the latest configuration snapshot from the cloud platform (including changes made while it was covered) before resuming.
You need to postpone the switch-back (site maintenance still in progress)	Click **Hold** on that row of the cluster admin page. The original gateway will not switch back automatically even once stable; click **Resume auto switch-back** to cancel.
You need to switch back immediately	Click **Switch back now** (available only while the original gateway is online).

> **Caution**
>
> An off-site standby usually cannot reach the machine tools on the shop floor. In that case it only serves configuration, query and dashboard functions and collects no data, which is expected.

4.3.5. On-screen Notices

The cluster state is shown as a banner at the top of the gateway management page:

Banner	Meaning
This host is a shared standby, waiting in the pool (read-only)	This host is an idle standby in the pool and is not covering any gateway.
This shared standby is currently serving gateway *<name>*	This host is a standby currently running under that gateway’s identity.
This gateway is covered by a standby (read-only); it switches back automatically once stable	This host is the original gateway. It has just come back online and is waiting out the stability window.

A host that is waiting in the pool or is currently covered by a standby serves a **read-only** web page: you can sign in to inspect configuration and status, but every write is rejected, so the two hosts cannot conflict with each other.

In addition, when the browser cannot reach the current gateway the page offers the addresses of alternative nodes to jump to. Those addresses have to be configured in the gateway’s front-end configuration file beforehand — contact Bivrost to set this up.

4.3.6. Double Fault: Forced Takeover

If the site loses its link to the cloud platform **and** a gateway suffers a whole-host failure at the same time, the cloud platform cannot judge liveness or assign a standby, so no automatic takeover happens (without an arbiter, the system will not risk dual collection or a split brain). An administrator can take over manually instead:

1. Sign in to the **standby’s own** gateway management page with an administrator account.
2. Click **Force takeover** on the standby banner (visible to administrators only).
3. Pick the gateway to take over from the list that appears (the list comes from the configuration snapshots cached on the standby). After you confirm, the standby restarts and runs under that gateway’s identity.
4. Once the link to the cloud platform is restored, the cloud platform adopts this takeover automatically and folds it into the normal switch-back flow.

> **Caution**
>
> **Confirm that the target gateway really is down** before forcing a takeover. If that gateway is still collecting, a forced takeover leaves two hosts collecting from the same machines and produces duplicate data.

4.3.7. What Is Not Replicated

- **Historical and time-series data**: this lives on the cloud platform and is not replicated between hosts. A standby starts collecting from the moment it takes over and does not inherit the locally cached history.
- **The part-program directory** used by DNC (the gateway file server directory, e.g. `E:\dnc`): this is outside the product's replication scope and has to be synchronised at the operations level, for example with a scheduled task on each gateway that mirrors the directory to a share on the standby.
- **The local shop-floor entry point**: on-site users normally reach the gateway by its own IP address, which is unavailable after a whole-host failure. The entry point the product guarantees is the address served by the cloud platform, which always points at whichever host currently carries that gateway. If you need the local address to follow the switchover too, configure DNS or a virtual IP at the network layer.

4.3.8. Leaving the Standby Pool

After you **remove** a standby from the pool on the cluster admin page, that host stays exactly as it is; it does not turn itself back into an ordinary gateway (its local configuration may still hold some gateway's settings, and enabling it by hand would cause dual collection). To reuse the host as an ordinary gateway, reinstall the gateway software and configure it from scratch.

4.4. MCP Service

The gateway hosts a built-in MCP (Model Context Protocol) server that exposes machine data, analytics and gateway status as “tools” for MCP-capable AI clients (Claude Code, Claude Desktop, MCP Inspector, and others). Users can query machines in natural language instead of calling the HTTP API by hand. The cloud platform (Hub) offers the same MCP server and forwards calls to the target gateway.

> **Note**
>
> MCP tools go through the exact same processing path inside the gateway as the HTTP API, so the data an MCP tool returns is identical to the matching HTTP endpoint. The full tool list, parameters and return format are in the *Communication Protocol* chapter 6, MCP Service; this section only covers enabling and configuring MCP on the gateway.

4.4.1. Overview

The MCP server is served at `/mcp`, on the same port as the gateway’s HTTP API, e.g. `http://192.168.100.1/mcp`. It currently exposes 33 **read-only** tools covering machine configuration, live status, analytics and gateway system information. Anything involving writes, machine control or program transfer has no MCP tool and still requires the HTTP API.

MCP is **disabled by default**; while it is off, `/mcp` returns HTTP 404. To enable it, open the MCP entry under 3.6.8. MCP Settings, turn the switch on and save. It takes effect immediately — no restart of the gateway or its services is required.

4.4.2. Authentication

The MCP server shares the same authentication and access control as the HTTP API — nothing extra to configure:

- **Key / token**: an MCP client must send `Authorization: Bearer <credential>` in its request header. The credential can be a JWT obtained after login, or a key generated for a user under **User Security Settings** (3.12.1.3.2. User Security Settings). A JWT expires after 24 hours, and MCP client configuration is usually saved long-term, so **a key starting with “sk-” is recommended** to avoid calls silently failing once the JWT expires.
- **IP whitelist**: if the IP whitelist is enabled under 3.6.6. HTTP Settings, `/mcp` requests are subject to it as well.

- **Authorized APIs**: with Security Control turned on, a non-admin user can only call the tools covered by their authorized API list, using the same rule as the HTTP API (see 3.12.1.3.2. User Security Settings); a tool call without permission returns an error. Admin users can call every tool.

4.4.3. Calling Through the Cloud Platform

If the gateway is connected to the Bivrost cloud platform, an MCP client can instead connect to the cloud platform's MCP server (`https://{cloud-platform-address}/mcp`), which forwards the call to the target gateway; the tool list is identical to a direct gateway connection. In this case send `accessToken: <gateway access token>` instead — the same gateway access token entered under 3.6.1. Cloud Platform — which both authenticates the caller and selects which gateway the call runs on.

4.4.4. Client Configuration Examples

Using Claude Code as an example, add the gateway's MCP server:

```
claude mcp add --transport http bivrost-gateway
http://192.168.100.1/mcp --header "Authorization: Bearer <key>"
```

Add the cloud platform's MCP server:

```
claude mcp add --transport http bivrost-hub
https://cloud.example.com/mcp --header "accessToken: <gateway access
token>"
```

Other MCP-capable clients generally use JSON configuration in this shape:

```
{
  "mcpServers": {
    "bivrost-gateway": {
      "type": "http",
      "url": "http://192.168.100.1/mcp",
```

```
      "headers": {
        "Authorization": "Bearer <key>"
      }
    }
  }
}
```

Once configured, ask the client questions in natural language, e.g. “What is the current status of machine 1?” or “Show OEE for group 1 over the last day” — the client picks the matching tool and calls the gateway automatically.

Without a real machine tool on hand, use a mock machine to test the MCP tools.

4.4.5. Limitations

- Every tool is **read-only** — none of them can change configuration, control a machine, or transfer files; use the HTTP API or the web admin UI for writes.
- The data covered by each tool and its field meanings match the corresponding HTTP endpoint; see the full list in *Communication Protocol* chapter 6, MCP Service, section 6.4. Tool List.

5. FAQ

5.1. Cannot Open the Gateway Management Page

Use an Ethernet cable to connect the gateway’s LAN1 or LAN2 port to the LAN port of your computer, either directly or through a switch.

Check the computer’s network settings. Its IP address must be on the same subnet as the gateway’s port, and the subnet mask must be identical. The gateway’s LAN1 port defaults to IP address 192.168.100.1 with subnet mask 255.255.0.0; the LAN2 port obtains both its IP address and its subnet mask automatically. If LAN1’s IP address and subnet mask have been changed and you no longer remember the current values, connect through LAN2 instead.

Check whether the gateway’s power LED is lit steadily and whether the network port LED is blinking. If the power LED is off, the gateway is not powered on. If the port LED is not blinking, check both ends of the Ethernet cable and make sure the computer and the gateway are properly connected.

If the power LED is on and the port LEDs at both ends are blinking, a network connection between the computer and the gateway has been detected. Open the gateway management page on the computer. If it does not open, enter one of the following commands in the computer’s command prompt, depending on the operating system:

```
ping IOTGW -4       (Windows)
ping IOTGW.local    (Linux or Mac)
```

Note

On some early gateway models, if IOTGW does not work, replace IOTGW with BIV-[first part of the gateway UID]. The gateway UID is printed on the label on the bottom of the gateway. For example, if the gateway UID is “152KUCG-1TOSJH4-1WXYSON-JY531Q”, the first part of the UID is “152KUCG”, so on a Windows computer the command is:

```
ping BIV-152KUCG -4
```

If the ping succeeds and the reply shows the IP address of the gateway’s current port, communication between the computer and the gateway is working. If the gateway management page still will not open, contact customer support.

If the ping fails, disconnect all other devices, make sure the computer is connected to a single gateway only, and run the command again.

If the command now succeeds, either the gateway or the computer had an IP address conflict with a device that has since been disconnected from the LAN. Change the conflicting IP address.

If the ping fails again, there is a network fault between the computer and the gateway, usually caused by the network port or the cable.

5.2. The Gateway Page Is Blank or Incomplete in the Browser

The browser you are using does not support the page framework. Use Google Chrome, Microsoft Edge or Apple Safari. If none of these is available, download and install the latest version of Chrome.

5.3. Changing the Gateway’ s LAN1 IP Address

Open the gateway management page and click **Network** in the navigation bar. LAN1’ s IP address can be changed in the network settings; see 3.7.1. Wired Network.

5.4. Finding the Gateway’ s Current LAN2 IP Address

Use an Ethernet cable to connect the gateway’ s LAN2 port to the LAN port of your computer, either directly or through a switch. Follow 5.1. Cannot Open the Gateway Management Page and run the command to obtain the address of the gateway port you are connected to.

> **Note**
>
> LAN2 obtains its IP address automatically by default, so the address may differ every time you connect through LAN2.

5.5. Recovering the LAN1 IP Address

Use an Ethernet cable to connect the gateway’ s LAN2 port to the LAN port of your computer, either directly or through a switch. Sign in from the computer using the domain name (see 3.1. Signing In); alternatively, find LAN2’ s current IP address first (see 5.4. Finding the Gateway’ s Current LAN2 IP Address) and sign in with that IP address.

Go to **Network** and change the LAN1 address (see 3.7.1. Wired Network).

5.6. Resetting the Gateway’s LAN1 Settings

Gateway software version 1.5.6.8 and later supports resetting LAN1. Rename any USB flash drive that is not a system boot disk (used for installing the operating system) to “resetlan1” (case does not matter) and plug it into any USB port on the gateway. After the gateway is shut down and restarted, LAN1’s IP address and subnet mask are automatically reset to the factory settings: IP address 192.168.100.1, subnet mask 255.255.0.0. Remove the USB drive once the reset is complete, otherwise the reset will run again on the next restart.

5.7. Cannot Read Machine Data from API Test

If you cannot read data from the target machine on the **API Test** page, follow the returned error code and its remedy. The main API Test error codes are listed below.

Error Code: 3, Machine off or offline

Remedy: Unable to communicate with the machine. Please check: 1. the machine is turned on; 2. the machine and the gateway are on the same subnet of the same LAN; 3. the machine’s network is properly set ①; 4. the gateway is properly configured ②; 5. network hardware such as ports, cables and switches is working correctly.

Error Code: 102, Machine network error, unable to read data

Remedy: Please ensure the machine’s communication service is started. Check whether another device on the LAN conflicts with this machine’s IP address ③, and try changing the machine’s IP address.

Error Code: 10003, machineID does not exist

Remedy: The machineID is wrong, the corresponding machine is not activated, or the gateway service was not restarted after the machine’s IP address or activation status was edited.

Error Code: 10006, API not authorized

Remedy: Contact Bivrost if you need to use an unauthorized API.

The remaining error codes are described in *Communication Protocol*, section 2.2. Error Handling. If the error code does not let you resolve the problem, contact customer support for remote assistance; see 5.10. Getting Remote Assistance.

Note

① On machines with certain control systems, setting the IP address is not enough: you also have to enable the communication options, configure the firewall and so on before data can be collected. On some models, after the IP address is set, the machine must be powered off for 3 seconds and then powered on again for the setting to take effect. See *Machine Setup*.

② On machines with certain control systems, besides setting the system model and the IP address on the gateway, you also have to set a user name and password. See *Machine Setup*. When you are finished, you must click **Restart Service** on the home page.

③ A machine IP conflict usually means the IP address configured on the machine is already used by another device on the same LAN. Some devices cannot be pinged because of their firewall settings, so their IP addresses are often mistaken for unused ones. In this case, change the machine's IP address to one that is currently free and power-cycle the machine; at the same time, change the machine's IP address to the new one on the gateway's **Machines** page, click **Restart Service**, and run the collection test again.

The other form of address conflict is a subnet conflict. This is common when the acquisition network and another internal network are connected to the same switch and both use the same subnet. When this happens, move either the conflicting internal devices or the gateway and machines to a subnet that is not in use.

To keep IP conflicts from recurring, see 5.11. The Gateway or a Machine Has an IP Conflict with Another Device on the LAN.

5.8. Cannot Get Automatically Collected Machine Data over MODBUS, MQTT or a Database

On the gateway's **API Test** page, check whether the machine's common data can be read; see 3.8. API Test.

If it cannot, follow 5.7. Cannot Read Machine Data from API Test.

If API Test does return machine data, open the **Machines** page, then the "Edit Machine" dialog and its "Task" tab, and check whether the machine's automatic collection tasks are enabled; see 3.3.1.2. Task Settings. Task results are only uploaded automatically over the protocols once the corresponding automatic collection tasks are enabled.

Check the settings for the protocol you are using on the gateway’s **Communication** page; see 3.6. Communication.

Once all of the gateway settings above are confirmed, click **Restart Service** on the gateway’s home page.

If the automatically collected data still does not arrive over MODBUS, MQTT or the database, check the settings of the receiving system and the network connection between it and the gateway.

5.9. Cannot Get Automatically Collected Group Data over MODBUS, MQTT or a Database

First confirm that the target group has been added successfully on the gateway’s **Groups** page and is activated; see 3.4. Groups.

Check the group’s settings in the “Edit Group” dialog on the gateway’s **Groups** page, and make sure the group contains at least one machine; see 3.4.2. Editing a Group.

In the “Group Task Settings” dialog for that group on the gateway’s **Groups** page, check whether the automatic collection tasks are enabled; see 3.4.1.2. Group Task Settings. Task results are only uploaded automatically over the protocols once automatic collection is enabled.

On the gateway’s **API Test** page, check whether the common data of the machines in the group can be read; see 3.8. API Test. If it cannot, follow 5.7. Cannot Read Machine Data from API Test.

Once everything is confirmed, click **Restart Service** on the gateway’s home page and run the collection test again.

5.10. Getting Remote Assistance

Scan the QR code on the cover to contact customer support and describe the problem; support will assign an engineer to work with you.

Once remote assistance has been agreed, connect the gateway’s LAN2 port to the internet (if LAN2’s settings have been changed, make sure the current settings still allow internet access), or connect the gateway to the internet over WiFi (see 3.7.2. WiFi Settings). Then sign in, open **Home**, confirm that “Network” under “Gateway Status” reads “Connected” and that the “Remote Assistance” switch in the “Settings” dialog is turned on, and notify the engineer you are working with.

5.11. The Gateway or a Machine Has an IP Conflict with Another Device on the LAN

An IP address or a whole subnet already being in use is a common problem when connecting the gateway or a machine to a network. It can be resolved as follows:

1. Put the gateway and the machines on their own router, isolated from other devices.
2. When connecting, make sure the gateway and the machines do not use an IP address or subnet mask that is already taken.
3. In the router’s management page, bind the static IP addresses of the gateway and the machines to their MAC addresses so that those IP addresses are not handed out to other devices automatically.

If IP addresses cannot be bound to MAC addresses, apply either of the following settings in the router’s management page:

1. Disable the router’s DHCP server so that IP addresses are no longer assigned automatically and devices can only be connected with manually configured addresses.
2. Restrict the router’s DHCP address pool so that it does not overlap the addresses configured on the gateway and the machines.

For the router settings themselves, refer to the router’s own manual.

5.12. The DNC Page Can List, Receive, Send and Delete Files but the Matching API Calls Fail

The path or file name contains unsafe characters such as special symbols or spaces, which must be converted to URL encoding. For example, the path `TNC:\nc_prog` becomes `TNC%3A%5Cnc_prog`, and `Sinumerik/FileSystem/Part Program` becomes `Sinumerik/FileSystem/Part%20Program`. Most browsers and test tools apply URL encoding automatically, but some software still requires you to convert the path by hand when calling the API.

6. Known Issues

6.1. The LAN Port IP Address Shown on the Gateway’ s Network Page Does Not Match the Actual Setting

Prior to version 1.12.2.0, if a LAN port was not connected the gateway could not determine that port’ s address and assigned it a temporary one instead. This does not affect normal operation: once the port has a working connection again, the actual IP address is displayed.

6.2. A Brief Power Trip Causes the Gateway to Fail to Restart Automatically

If power is restored within 15 seconds of a momentary trip, the gateway may fail to restart automatically, in which case you have to start it manually by pressing the gateway’ s power button. To avoid frequent power interruptions, install the gateway where the supply is stable, and fit it with a UPS if possible.

6.3. The Gateway Is Connected to Several Networks and One Is Restricted, So It Cannot Reach the Internet

When the gateway has a wired network, a WiFi network and an external USB LAN adapter connected at the same time, and all of them can reach the internet, the gateway uses whichever network connected first. If that network is restricted and can only reach a limited set of external hosts, internet access fails even though the other networks are unrestricted.

The correct way to connect to the internet is to disconnect every network first, connect the gateway to the unrestricted network, and only then connect the others. For example, suppose LAN1 is connected to the company intranet (behind a firewall) and an external USB LAN adapter is used to reach the internet for remote assistance. To get remote assistance working, unplug the LAN1 cable, plug in the external adapter, wait until the remote assistance connection is established, and then plug the LAN1 cable back in.

6.4. LAN1 and LAN2 on the Same Subnet Cause a Subnet Conflict and Communication Failure

If the gateway’ s LAN1 and LAN2 ports are on the same subnet, the resulting subnet conflict can cause communication failures. Do not put LAN1 and LAN2 on the same subnet.

Changelog

Version	Change Date	Description	Release Date
1.19.7.29	20260901	1. Added “3.2.2.1. Queue Backlog and Discarding It”, covering the data-pipeline backlog display, the “Recovering” status, and the new button that discards queued data.	20260901
1.19.7.24	20260827	1. The MCP service now has a switch and is disabled by default; it must be enabled under 3.6.8. MCP Settings before it can be reached. Updated “4.4. MCP Service” accordingly.	20260827
1.19.7.22	20260819	1. Added “4.3. Cluster Failover (Optional)”, covering how the shared standby pool works, how to build it, failover and switch-back behaviour, forced takeover, and what is not replicated.	20260820
1.19.7.18	20260803	1. Reworked the Siemens CNC model list: the generic model was split into 828D and 840D sl; 810D/840D (winXP) was split into 810D(winXP) and 840D(winXP); 810D/840D (winNT) was split into 810D(winNT) and 840D(winNT); SINUMERIK ONE was renamed ONE; added the 802D and 808D models. Existing machine configurations are unaffected. 2. Revised the “Enable IP Whitelist” description: the login endpoint is not restricted by the whitelist, JWT-authenticated requests skip the whitelist check, and SecretKey-authenticated requests must still pass it.	20260806
1.19.7	20260719	1. Added Alarm Mapping. 2. Added the “Network Error as Offline” (NetworkErrorAsOffline) option to the machine configuration. 3. Files downloaded from DNC no longer carry a file extension. 4. Added compatibility with older Chromium-based browsers.	20260719
1.19.6	20260702	1. Revised the Monitor documentation.	20260702
1.19.5	20260615	1. Added Toolpath viewing to the “DNC” page.	20260615
1.19.4	20260528	1. Moved to the new UI and updated the content accordingly. 2. Added the Monitor page. 3. Added documentation for PLC task post-processing. 4. Added documentation for custom tasks.	20260528
1.18.0	20240429	1. Reworked the “Settings” dialog: the former “Time Settings” is now “Time And Region Setup”. Added the “Auto Sync Time Interval” and “System Locale” settings. Reworked the “Time Server Address” setting so that several addresses can be configured. 2. On the “Communication” page, the enable toggles for the individual communication protocols were moved.	20240429
1.17.6	20240425	1. Revised the description of DNC (Professional Edition).	20240425
1.17.4	20240328	1. On the “DNC” page, added DNC (Professional Edition).	20240328
1.17.5	20240401	1. On the “Tasks” page, added Machine Status Monitoring Settings.	20240401

Version	Change Date	Description	Release Date
1.16.2	20240301	1. Revised parts of the documentation.	20240301
1.16.1	20240221	1. Updated the section numbers used when referring to the *Communication Protocol*.	20240221
1.16.0	20240205	1. On the “Groups” page, “Create Group” / “Edit Group” gained an “Advanced” tab.	20240220
1.15.8	20240129	1. On the “Network” page, added WiFi scanning and configuration. 2. Gateway management page - Network: added support for WiFi networks with Chinese SSIDs, added support for WPA3SAE networks, and fixed connection problems with common WiFi networks.	20240220
1.15.7	20240127	1. On the “Machines” page, “Create” / “Edit Machine” - “DNC” tab, “File Server Type” gained a “Wireless Disk” option.	20240220
1.15.5	20240122	1. On the “Communication” page - “Gateway File Server Settings”, added the “Enable SMB” toggle. 2. On the “DNC” page, added support for sending several files at once.	20240220
1.15.4	20240117	1. On the “Communication” page - “Gateway File Server Settings”, added the “Enable SMB” toggle. 2. On the “DNC” page, added support for sending several files at once.	20240220
1.15.3	20231226	1. On the “Machines” page, “Create” / “Edit Machine” - “DNC” tab, added the “Gateway File Server” settings. 2. On the “Communication” page, added the “Gateway File Server Settings” section.	20240220
1.15.2	20231218	1. On the “Communication” page, the default value of “Database Settings” - “Storage Mode” changed from “Log” to “User Defined”. This change does not affect your current settings.	20231218
1.15.1	20231206	1. On the “Communication” page, “Database Settings” gained an “Enable Primary Key” toggle. 2. On the “Communication” page, “Database Settings” - “Storage Mode” gained the “User Defined” option, which lets you choose Log mode or Real Time mode for each task individually. 3. On the “Analysis” page, the order of the analyzer options changed. 4. On the “Tasks” page, “Monitor Mode” under “OEE Monitoring Settings” and “Count Monitoring Settings” now defaults to “Scheduled Reset”. This change does not affect your current settings. 5. Revised parts of the documentation.	20231208
1.15.0	20231123	1. On the “API Test” page, the “Program Info” and “Program Block” interfaces gained a channel option. 2. Home - “Gateway Status” panel: removed “License Description” and added “License Status”.	20231123

Version	Change Date	Description	Release Date
1.14.0	20231101	1. On the “Machines” page, “Create” / “Edit Machine” gained an “Advanced” tab where you can set a custom machine ID and Modbus slave ID. 2. The PLC Data task format changed.	20231101
1.13.0	20231023	1. The licensing policy changed: a single gateway can now import licenses for several different device types. When upgrading from an older version to 1.13.0 or later, the license file must be regenerated. 2. Machine types other than CNC can now join a group. 3. On the “Machines” page, the “Task” tab of the “Create PLC Machine” / “Edit PLC Machine” dialog gained the “Machine Status”, “OEE Monitoring” and “Cumulative Status Time” tasks. 4. On the “Machines” page, the “IO Module” option of the System field moved from “Create CNC Machine” / “Edit CNC Machine” to the System field of “Create PLC Machine” / “Edit PLC Machine”. Machines added as “IO Module” in an older version must be configured again.	20231023
1.12.0	20230926	1. On the “DNC” page, added the “New folder” and “Delete folder” buttons. 2. On the “Network” page, “LAN1 Settings” and “LAN2 Settings” gained DNS server settings; a new status indicator shows whether the LAN port is connected (“Connected” means the LAN adapter has detected a device at the other end of the cable; it does not guarantee that the device can be pinged). 3. On the “Machines” page, the “Task” tab of the “Create CNC Machine” / “Edit CNC Machine” dialog gained the “Tool Offset” task. 4. On the “Tasks” page, “Machine Task Interval Settings” gained “Tool Offset (ms)”.	20230926
1.11.0	20230906	1. On the “Machines” page, the layout of the “DNC” tab in the “Create” / “Edit Machine” dialog was reworked.	20230906

Version	Change Date	Description	Release Date
1.10.0	20230822	1. On the “Machines” page, “Create” / “Edit Machine” gained an “External PLC” tab for setting up serial data collection. 2. Added support for laser cutters. The “Machines” page gained a “Create Laser Cutter” button. The “Task” tab of the “Create Laser Cutter” / “Edit Laser Cutter” dialog gained the “Laser Power” task. “Machine Task Interval Settings” on the “Tasks” page gained “Laser Power (ms)”. The “API Test” page gained a “Laser Power” interface option for laser cutters. 3. On the “Machines” page, for laser cutters, robots and PLCs, the System field on the “General” tab of the “Create” / “Edit Machine” dialog gained a “Mock” option. 4. On the “Network” page, WiFi Settings, the “Status” section now shows the current WiFi IP address. 5. On the “API Test” page, some interfaces gained a “Channel” option, which defaults to 0, the main channel.	20230822
1.9.3	20230710	1. Removed the per-machine write option from database communication. Setups that used per-machine write in an older version now run in Log mode.	20230710
1.8.0	20230512	1. On Home, the data upload services in “Gateway Status” gained a “Delayed” state. 2. The top toolbar gained a “Diagnosis” button. 3. On the “Machines” page, the “Task” tab of the “Create CNC Machine” / “Edit CNC Machine” dialog gained the “Tool Life” task. 4. On the “Tasks” page, added “Tool Life Monitoring Settings”. 5. On the “Tasks” page, “Machine Task Interval Settings” gained “Tool Life (ms)”. 6. On the “Tasks” page, “OEE Monitoring Settings” gained the break time settings. 7. On the “Network” page, “WiFi Settings” now shows signal strength. 8. The “API Test” page gained the “Tool Life” and “Tool Life Details” interfaces. 9. The “Analysis” page gained the Overall Analysis analyzer.	20230512

Version	Change Date	Description	Release Date
1.7.5	20230310	1. The “Tasks” page gained an “Alarm Monitoring Settings” section. 2. The “Machines” page gained a “Create Robot” button, adding support for collecting data from robots. 3. Reworked the “Settings” dialog: added a “More” tab, moved the “Default Config” button into it, and added the “Backup Config” and “Restore Config” buttons. 4. Added a “Restart Service” reminder. 5. The shutdown button on Home was merged into the new “Gateway Shutdown/Restart” button. 6. The “Analysis” page gained “Count Analysis”. 7. Added content to the chapter *7. FAQ*. 8. On the “Machines” page, the “Task” tab of the “Create” and “Edit Machine” dialogs gained “Advanced” settings.	20230310
1.7.0	20221212	1. On the “Machines” page, “Count” on the “Task” tab of the “Create CNC Machine” / “Edit CNC Machine” dialog gained the “Overload” task. 2. The “Tasks” page gained “Count Monitoring Settings” and “Overload Monitoring Settings”. 3. On the “API Test” page, the “Read” button became “Send”. 4. On the “API Test” page, the “PLC Data” interface option became “Read PLC Data”. 5. The “API Test” page gained the “Write PLC Data”, “Read Offset Data” and “Write Offset Data” options. 6. “Advanced Options” in the “Settings” dialog gained the permission toggles “Allow Write PLC Data” and “Allow Write Offset Data”.	20221212
1.6.1	20221104	1. The “Settings” dialog gained a “Manage Users” button for adding, editing and deleting gateway users and assigning their permissions.	20221104
1.6.0	20221031	1. On the “Machines” page, the “Create” button was split into “Create CNC” and “Create PLC”. “Create CNC” keeps the behaviour of the original “Create” button; “Create PLC” opens the PLC configuration dialog, adding support for collecting data from PLC devices. 2. Added offline gateway upgrade. 3. On the “Communication” page, “MODBUS Settings” gained a “Byte(8) Order” option. 4. On the “Communication” page, “Database Settings” gained a “Storage Mode” option; the former per-machine write option was folded into “Storage Mode”.	20221031

Version	Change Date	Description	Release Date
1.5.8	20220817	1. On the “Machines” page, the “Task” tab of the “Create” and “Edit Machine” dialogs gained the “Program Block” option. 2. On the “Tasks” page, “Machine Task Interval Settings” gained the “Current Program Block (ms)” setting. 3. The “API Test” page gained the “Program Block” option. 4. The “Analysis” page gained the “Alarm Analysis” option. 5. On the “Communication” page, “Database Settings” gained a “Use Local Time” toggle.	20220830
1.5.7	20220803	1. Moved the FAQ and known issues content from the *User Commissioning Manual* into this document. 2. The “Communication” page gained “Database Settings”. 3. The “Settings” dialog gained the “LAN2 Settings” toggle. 4. The default gateway alias changed to “iotgw”. 5. On the “Machines” page, the “General” tab of the “Create” and “Edit Machine” dialogs gained the “Encoding” setting.	20220809
1.5.6	20220712	1. Rebuilt the table on the “Machines” page: added sorting, search and pagination; the “Status” column became the “Activate” column, which shows the activation state as an icon; added a “Connection” column, which shows the connection state as an icon and refreshes every ten seconds; added a “Task Count” column showing the number of tasks on the machine; the former “Edit” and “Delete” buttons are now icons; hovering over an icon shows a tooltip; the former “Machine Task Settings” dialog moved into the “Task” tab of the “Edit Machine” dialog; the “Edit Machine” dialog gained a “DNC” tab. 2. Rebuilt the table on the “Groups” page: added sorting, search and pagination; the “Status” column became the “Activate” column, which shows the activation state as an icon; added a “Machine Count” column showing the number of machines in the group; added a “Task Count” column showing the number of tasks on the group; the former “Edit” and “Delete” buttons are now icons; hovering over an icon shows a tooltip; the former “Group Task Settings” dialog moved into the “Task” tab of the “Edit Group” dialog. 3. “DNC” gained support for Shared Folder, Shared Folder (Win XP) and FTP Server. 4. On the “API Test” page, “Data Type” for reading “PLC Data” changed from a text field to a dropdown. 5. On the “DNC” page, “Root Directory” is read-only and only shows the “Root Directory” configured on the “Machines” page - “Edit Machine” dialog - “DNC” tab. 6. Updated *3. Specifications*.	20220721

Version	Change Date	Description	Release Date
1.5.5	20220618	1. Reworked the layout of the top toolbar and Home: “Change Username & Password”, “Change Gateway Alias”, “Create Default Config” and “Advanced Options” moved into the new “Settings” dialog. 2. The “Settings” dialog gained “Time Settings”. 3. On the “Communication” page, “MQTT Settings” gained the RPC interface settings.	20220624
1.5.4	20220608	1. Added English language support. 2. Revised the Chinese content. The “Collection” page became the “Tasks” page. On the “Machines” and “Groups” pages, the “Settings” button in the Operations column became the “Task” button. 3. Machine OEE was split out from group OEE and is now enabled and disabled in “Machine Task Settings”. 4. On the DNC page, the “Use” button on a folder in the file list became “Open folder”; clicking it lists the subfolder directly. 5. Revised *4. Networking*. 6. Added *6. Appendices* and moved the glossary into that chapter, adjusting the rest of the document accordingly.	20220617
1.5.3	20220531	1. Revised the support list and added “PLC Data”. 2. Revised *5.1. Signing In*. 3. Adjusted the “PLC Data” documentation to reflect the changes to the “PLC Data” interface.	20220531
1.5.2	20220509	1. On the “Machines” page, the “Auto Collection Settings” dialog gained the “PLC Data” option. 2. On the “Collection” page, “Machine Collection Interval Settings” gained the “PLC Data (ms)” setting. “OEE Monitoring Settings” gained the “Availability Mode” option. 3. On the “Communication” page, “MQTT Settings” gained the “Use Gateway Alias” toggle. 4. The “API Test” page gained the “PLC Data” option. 5. Added the “Analysis” page.	20220509
1.5.1	20220426	1. On the “Collection” page, “Data Statistics Settings” became “OEE Monitoring Settings”. Added “Monitoring Time Settings”, with the options “Time Window” and “Scheduled Reset”.	20220426

Version	Change Date	Description	Release Date
1.5.0	20220418	1. On the “Machines” page, in the “Create” and “Edit Machine” dialogs, the “System” field was split into “System” and “Model”. 2. Reworked the “Auto Collection Settings” dialog on the “Machines” page and added more collection options. 3. On the “Collection” page, “Machine Collection Interval Settings” gained interval settings for the additional collection options. 4. On the “Communication” page, MQTT Settings gained the “Publish on Value Change” toggle. 5. On the Network page, “WiFi Settings” gained a “Disconnect” button.	20220418
1.4.3	20220328	1. Reworked the Home layout: moved the “Restart Service”, “Gateway Shutdown” and “Create Default Config” buttons to the first row of Home. 2. Reworked the content and position of “Network Status” on Home. 3. “Advanced Operations” on Home became “Advanced Options”. 4. The “Local Caching” and “Remote Assistance” toggles moved from “Network Status” on Home to “Advanced Options”. 5. In the navigation bar, the “Collection Test” page became the “API Test” page, with more interfaces available to call. 6. Added the “DNC” page to the navigation bar.	20220328
1.4.2	20220311	1. Extended and revised parts of the “Collection” content.	20220219
1.4.1	20220215	1. Updated the list of supported machines. 2. “Gateway Status” on Home gained an “Enable/Disable Local Caching” toggle. 3. “Gateway Status” on Home gained an “Enable/Disable Remote Assistance” toggle. 4. Added the “Groups” configuration page. 5. Reworked the “Collection” page: it is now split into “Machine Collection Interval Settings”, “Group Collection Interval Settings” and “Data Statistics Settings”, with several new settings. 6. The “Communication” page gained the “Cloud Settings” option.	20220215
1.3.5	20211227	1. Home gained a network status panel. 2. Unified the names and the order of the collected data items across all pages. 3. On the Collection page, “Frequency” was renamed “Interval”. 4. On the Communication page, the MQTT protocol now supports changing the encoding, and the default encoding changed from gb2312 to utf8.	20211227