SIEMENS

Climatix IC

Remote monitoring and intelligent diagnostic for POL controllers - GettingStarted

User Guide

Contents

Cyber security disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit the following website:

https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html.

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under the following website:

https://www.siemens.com/cert/ => 'Siemens Security Advisories'.

Legal note

Legal note concept

This guide includes notes that must be followed to prevent damage to property.

Notes dealing only with damage to property use the signal word NOTE and an exclamation point.

They are depicted as follows:

NOTICE
!   **Type and source of hazard**   Consequences in the event the hazard occurs   ●   Measures/prohibitions to prevent the hazard

Qualified personnel

Only qualified personnel may commission the device/system. In this regard, qualified personnel have the training and experience necessary to recognize and avoid risks when working with this device/system.

Proper use

The device/system described here may only be used on building technical plants and for the described applications only.

The trouble-free and safe operation of the device/system described here requires proper transportation, correct warehousing, mounting, installation, commissioning, operation, and maintenance.

You must comply with permissible ambient conditions. You must comply with the information provided in the Section "Technical data" and any notes in the associated documentation.

Fuses, switches, wiring and grounding must comply with local safety regulations for electrical installations. Observe all local and currently valid laws and regulations.

Disclaimer

The content of this document was reviewed to ensure it matches the hardware and firmware described herein. Deviations cannot be precluded, however, so that we cannot guarantee that the document matches in full the actual device/system. The information provided in this document is reviewed on a regular basis and any required corrections are added to the next edition.

Software used

All open source software components used in this solution/service (including copyright owners and license agreements) can be viewed at the following link:

● Go to https://www.climatixic.com in the footer on entry "OSS".

● Direct: https://www.climatixic.com/Content/OSS_ClimatixIC.htm

Imprint

About this document:
Edition: 2025-05-07
Document ID: A6V101065428_en--_af

1 About this document

1.1 Getting to know Climatix IC

Videos

Title	URL
Climatix IC on Youtube	https://www.youtube.com/watch?v=5_NuNjhyHyg
Specific user roles in Climatix IC (Youtube)	https://youtu.be/gtZJ9AwfLe0 (German)
	https://youtu.be/kiPp014jrZA (English)

Climatix IC product page

The Climatix IC product pages provide a comprehensive information offering on the product.

Deployment region	URL
Climatix IC	https://www.siemens.com/climatixic

Try out Climatix IC

For Climatix IC	
Start	https://www.climatixic.com
The following test tenants are available	• DEMO.IC.OZW: OZW772, OZW672, OCI670
	• DEMO.IC.S300: S300HRV
	• DEMO.IC.GetConnected: POL
	• DEMO.IC.CLX: POL (AHU, Chiller)
Account names (roles)	• demo@climatixic.com
	• service@climatixic.com
Password	Password.01

2 Climatix IC, remote monitoring and intelligent diagnostic

HVAC plants with Climatix controllers can connect to Climatix IC↑ - 'Cloud-based solution for remote monitoring and intelligent diagnostic'.

Climatix IC↑ supports your organization with remote maintenance 24/7, available anywhere to significantly reduce maintenance costs.

2.1 Key benefits

Climatix IC↑ web applications offer:

● Remote access to plant devices worldwide and 24/7
● Plant owners and managers can analyze:
   – Current status
   – History
   – Access to schedules and settings
● Real-time consumption data (currently available as an history export) helps identify "consumption anomalies" that often point to underlying mechanical problems. This permits preventive maintenance.
● Climatix IC↑ web operation simplifies and modernizes operation at all access levels.

Remote maintenance – at any time from any location

HVAC systems often operate a considerable distance from OEM production centers, supplier or service organizations, resulting in high service and travel costs, especially during warranty periods.

Climatix IC↑ facilitates diagnostics, optimization of settings, or system upgrades from any location. Even if a visit to the plant does prove necessary, however, the available data enables service engineers to work more efficiently.

Connection – straightforward and effective

Today, most Climatix controllers are equipped with a built-in IP interface. The controller connects automatically to the Climatix IC↑ via this interface.

Web-based – always up to date

Climatix IC↑ operates with standard web browsers that support HTML5. The service engineer logs on via a laptop and directly accesses the plant. No special software or cables required.

2.2 Key functions

Climatix IC↑ includes the following key functions:

● Collects alarms and routes them to the responsible service organization.
● Upgrades to installed plants: Application and firmware enhancements or saving control parameters to the cloud. Everything can be scheduled for specific times.
● Process data analysis permits systematic improvements to plant efficiency.
● The application can be used by any PC or laptop; no additional software required.

3 Requirements

3.1 Technical requirements

The current Climatix controllers are preconfigured to automatically connect to Climatix IC↑ as soon as they are connected to the Internet. First review the following system requirements:

Internet access

- The Ethernet cable must be connected to the controller's IP connection (T-IP).
- The controller requires a direct connection to the Internet, i.e. without proxy.
- Port 443 (https) is open, from the device to the outside on the Internet.
- Broadband Internet is recommended for the controller due to the program size.
- It is further important that the Internet connection is stable.

Web browser

The browser must support HTML5.

- The latest versions (as of the publication date) of the following browsers were tested: Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari (based on iOS) by Apple
- Internet Explorer is no longer supported.

Climatix controller BSP↑

- POL63x: VVS11.64 or higher, from January 2023 VVS11.66.
- POL68x: VVS11.64 or higher, from January 2023 VVS11.66.

For support for controllers: See Siemens SIOS Portal:
support.industry.siemens.com/cs/ww/en/view/109747351

- Access to SIOS requires login: support.industry.siemens.com/.

NOTICE	
i	**Additional information** - The upgrade process is documented in "Upgrade". - "Prepare and load current BSP" documents where you can download the current BSP.

SCOPE tool version

The SCOPE tool maps, generates, and uploads to controllers as of VVS 10.32 or higher.

Controller loaded with SAPRO application

- Climatix controllers must be loaded with a valid SAPRO application.
- The ↑BSP LED must be green.

3.2 Scan and use codes

3.2.1 Data Matrix Code

The activation key for your Climatix controller is included in the controller's firmware and can be read there using the SCOPE tool. The activation key is also printed on the actual controller as a DMC.

You can scan the code using a code reader app. The result is a text string.

Example

1PS55396-C488-A100+**31P**POL648.80/STD+**S**160908Z0000000005+**23S**00-A0-03-EB-01-04+**3C**AAAAAA-BBBBB-CCCCC-DDDDD-EEEEE

The text string is subdivided into code letters:

- 1P: Siemens stock number (SSN); fixed
- 31P: Siemens device type (ASN); fixed
- S: Date (YYMMDD), series, serial number, variable
- 23S: MAC address (hex); variable
- **3C: Climatix IC activation key; unique device ID**

Conclusion

Your Climatix supports the automation of your business processes, e.g. during sign-up or pre-registration. You no longer need to connect the controller to get its ID.
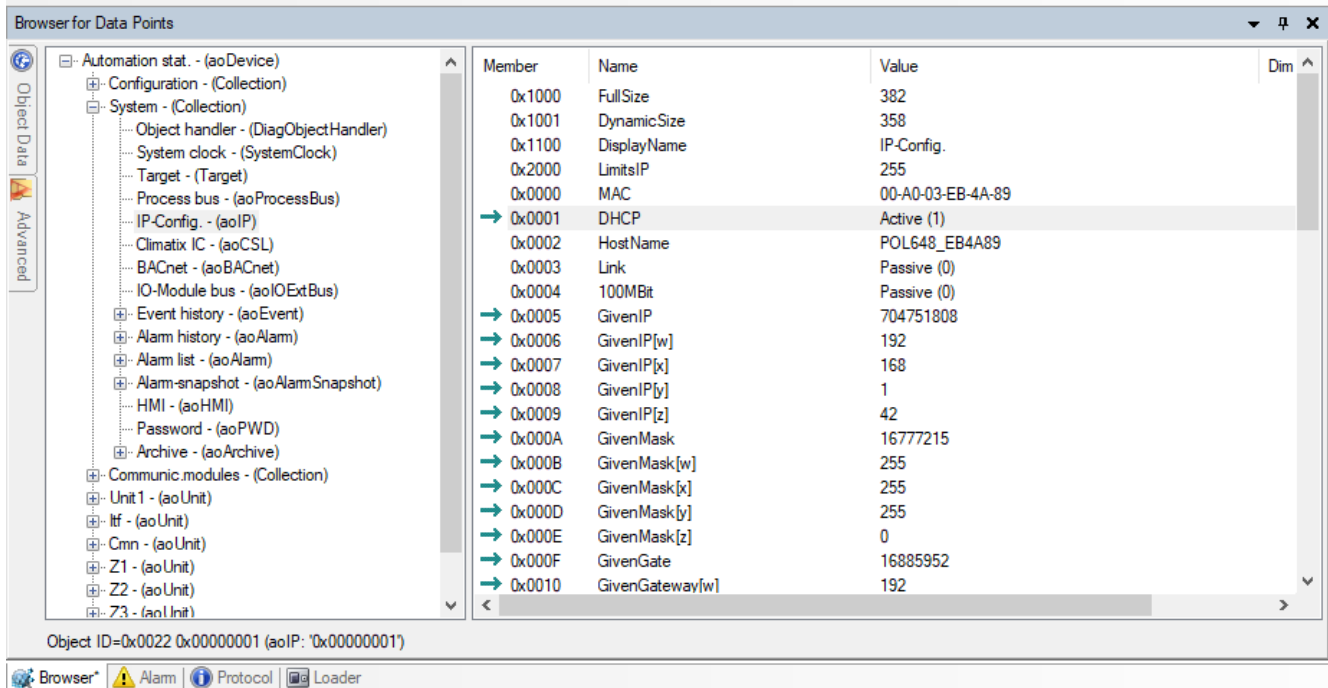
$\boxed{\mathbf{i}}$

The data matrix code on the box includes information such as the Siemens device type (ASN) and date of manufacture. The activation key is not included on the box.

4 Engineering with SCOPE

4.1 Connect and exchange data

4.1.1 Connect to the Internet (IP)

▷ SCOPE tool is connected locally to the target controller.

1. Go to "Menu > View > Browser".

2. In SCOPE, in the "Browser for Data Points", go to "SystemObjects > IP-Config".

3. Check the following member settings

DHCP

The network configuration is taken from the DHCP server, if available.

Member ID	Member name	Setting
0x0001	DHCP	Active

The DHCP server must provide the following information:

- Current controller IP address
- Correct subnet mask
- Gateway IP address, if needed

Fixed IP address

Make the following settings if **no** DHCP server is available:

Member ID	Member name	Setting
0x0001	DHCP	Passive
0x0035	IP	Local controller IP address
0x0036	SubnetMask	Correct subnet mask for the local network
0x0037	Gateway	Gateway IP address or 0.0.0.0, if no Gateway is required
0x0038	PrimaryDNS	Valid DNS server address, e.g. 8.8.8.8 (Public DNS Google*). DNS-Server to resolve Internet domains
0x0039	SecondaryDNS	Backup for PrimaryDNS

Check success

Both members↑ provide a note on success in this step:

● 0x0003: Link: Set to active (1)

● 0x0004: 100MBit: Set to active (1)

The next step "Connect to cloud (CSL) [➜ 12]", lists all other criteria to ensure the controller communicates with Climatix IC (Cloud).

4.1.2 Connect to cloud (CSL)

Table overview

1. In SCOPE, in the "Browser for Data Points", go to "SystemObjects > CSL-Config".

2. Check the following member settings:

Member ID	Member name	Setting
0x0000	ServerIP	Server URL with connection protocol For Climatix IC: ***NOTICE!* As a rule, do not change this value; the proper value comes from the BSP of the controller.** ● https://clx.ccl.climatixic.com (From VVS11.66 and D21) ● https://www.connectivity.ccl-siemens.com (Obsolete, up to VVS11.46)
0x0004	EnableConnection	"Switch" for connecting. Is run as the **last** step.
0x0006	Distributor↑	The distributor key assigns the controller to the correct Tenant↑.
0x0007	ReconnectTime	Wait in seconds between two connection attempts

Workflow in detail and chronologically

▷ You have the Distributor↑ information (compare: "Basic data/tenant key (distributor)").

▷ SCOPE tool is open and connected to the target controller.

1. In SCOPE, in the "Browser for Data Points", go to "SystemObjects > CSL-Config".

2. Check the ServerIP: Do not change the default setting https://clx.connectivity.ccl-siemens.com.

3. Enter the distributor↑/Tenant↑ key in Distributor. The key is provided by the Tenant Administrator↑ or is preset in the SAPRO project (aoCCL Block).

4. The "switch" is used for connecting only at the end: Set EnableConnection to Enabled.
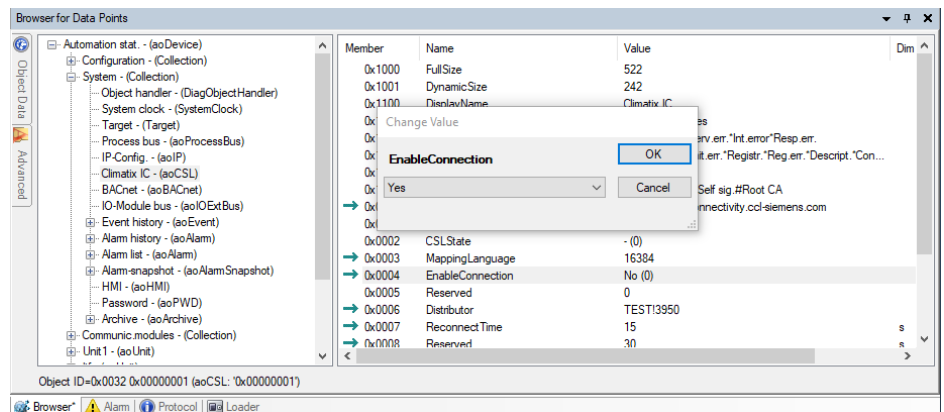
Check success

You can assume, according to the criterion indicated for both member↑ that the controller is communicating with Climatix IC (Cloud):

● 0x0001: ComState must be on OK (0)

● 0x0002: CSLState must be on Connected (7)
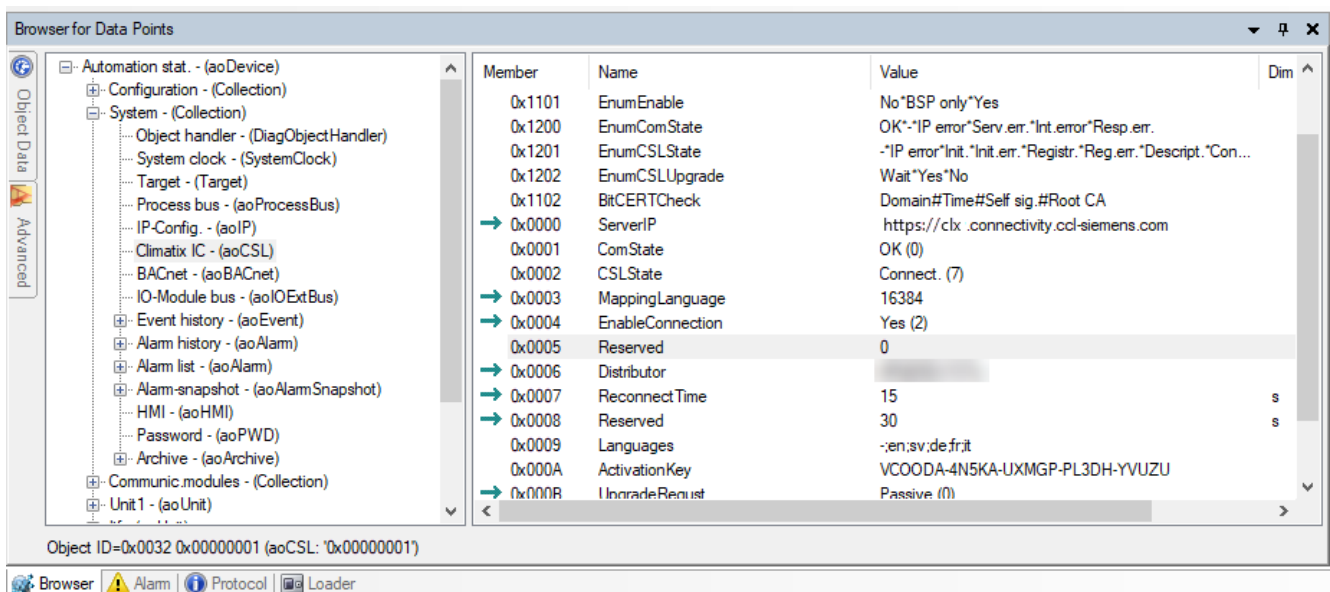
Error messages

Error messages are always displayed in the cloud help. Common errors are:

- **ComState** error - Perr(1): Check the Internet connection

1. Ping www.google.com

2. Ping connectivity URL: clx.ccl.climatixic.com

'**ComState**' describes the state of communication with the cloud.

- **CSLState** error - Perr(1):
▷ GenericCloud mapping available?
▷ OBH created and downloaded?

1. Check the controller's local IP settings and DNS address.

   – Alternatively, use 1.1.1.1 or 8.8.8.8.

2. Check the distributor.

   – Wrong distributor?
   – Distributor does not exist?

3. Check spelling.

   – Blanks at the beginning or end of the connectivity address?

'**CSLState**' describes the CSL state.

4.1.3 Result in Climatix IC

The controller is logged in to Climatix IC with the steps described in "Connect to the Internet (IP) [➜ 10]" and "Connect to cloud (CSL) [➜ 12]" and entered in the list of "Non-assigned plants". Compare the documentation starting at "Plants".

The serial number or the activation key is helpful for finding your controller in Climatix IC; both are always an element of the initial plant name (you change them as a rule). The data is also readable in the SCOPE tool.

Example of the controller in the SCOPE tool:

Example of the same controller in Climatix IC:

The number "161" is also an element of the initial name in Climatix IC.

Result

After performing the various steps described in the complete documentation, you now have the following situation in Climatix IC "Operation > Data points". This information can be used as an example for engineering watch pages and data points:

4.2 Virtual cloud data points VCI and VCP

Virtual Cloud Items (VCIs)

External data (e.g. weather info) is mapped via API to VCIs and read or written by virtual plants↑or a plant with a physical controller.

Virtual Cloud Plant (VCPs)

External data can be saved to VCPs via API. VCPs are listed, in addition to plants with physical controllers, in the plant list. VCPs can, for example, group multiple IoT devices with no relationship to a Climatix controller and operate them in the Cloud.

5 Entering Climatix IC

- Enter Climatix IC at https://www.climatixic.com.
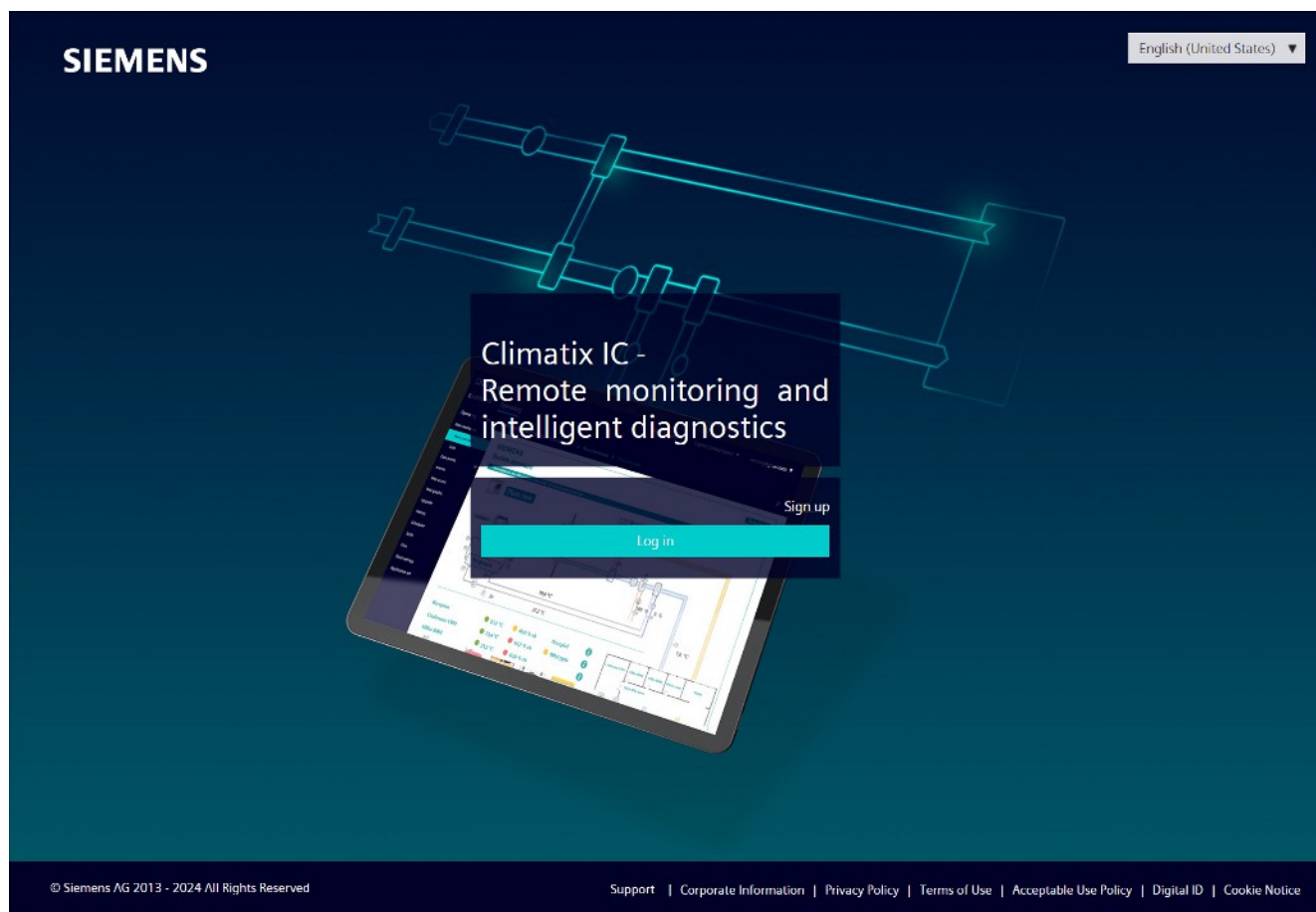
5.1 Assistance on the start page

Accessible documentation

- "Support" on the start page provides an introduction.
- The comprehensive help for reading is located at the same location after login.
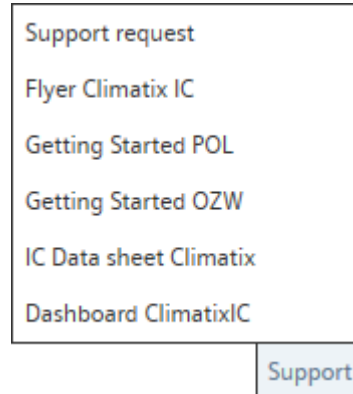
Information on unsupported browsers

An information window indicates when Climatix IC is opened by an unsupported browser.
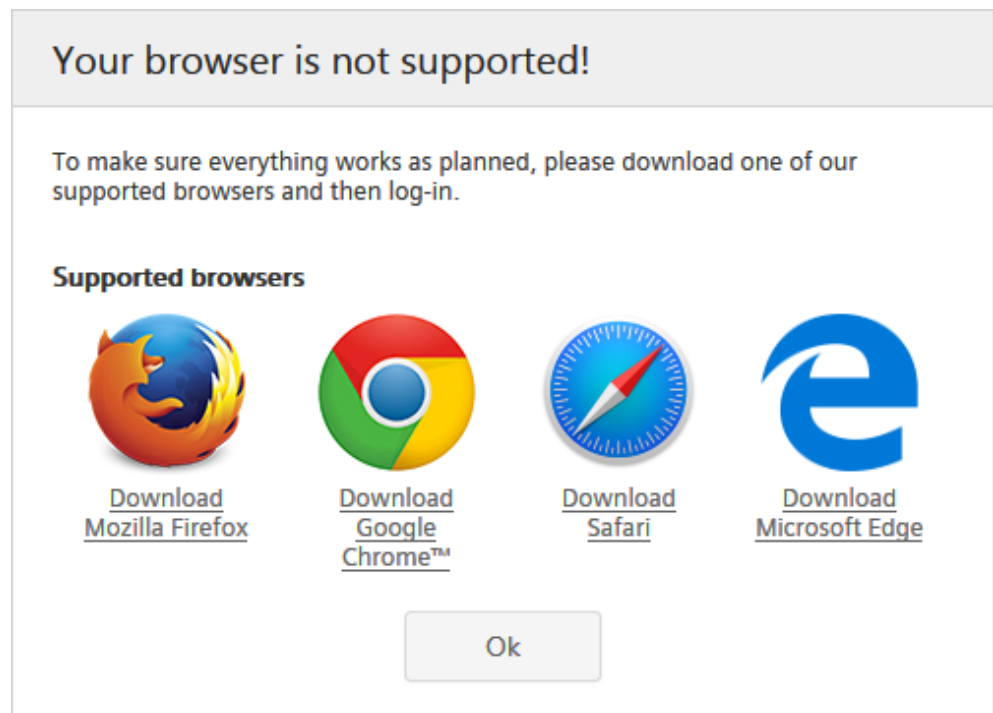
Central maintenance information from the Climatix IC Operations Team

Maintenance and important improvements are prominently displayed on the start page.

A color code (green, yellow, red) intuitively indicates the relevance of the information. Once logged in, you can access the same information at any time using the Info symbol (upper right). The Info symbol flashes for news.

Climatix IC Dashboard

You are investigating an event and want to know whether Climatix IC was online at a specific time? The Climatix IC Dashboard provides easy-to-understand and objective information on what services are or were available. The service can be subscribed to via various channels and media. The URL is: https://status.climatixic.com/

Support   Climatix IC   History   Status   Subscribe To Updates

All Systems Operational

Climatix IC - Remote monitoring and intelligent diagnostics | 远程监控和智能诊断 - siemens.com/climatixic

Uptime over the past 90 days. View historical uptime.

⊞ Global deployment ?   ✔
90 days ago ——— 99.99 % uptime ——— Today

⊞ China deployment | 中国部署 ?   ✔
90 days ago ——— 100.0 % uptime ——— Today

⊟ API services | API服务 ?

Global API Portal ClimatixIC ?   ✔
90 days ago ——— 100.0 % uptime ——— Today

Europe Cloud API ClimatixIC ?   ✔
90 days ago ——— 100.0 % uptime ——— Today

China Cloud API ClimatixIC ?   ✔
90 days ago ——— 100.0 % uptime ——— Today

⊞ External services | 外部服务 ?   ✔
90 days ago ——— 99.35 % uptime ——— Today

✔ Operational   ▢ Degraded Performance   ⚠ Partial Outage   ✖ Major Outage   🔧 Maintenance

← Incident History   Powered by Statuspage

Cookie information

We value your privacy

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in our marketing and performance efforts.

Manage Preferences   Accept All Cookies

The cookie information displays the first time you query Climatix IC in the web browser. You can modify your preferences at any time under 'Footer > Cookie preferences'.

Siemens also wants to evaluate the statistics on the Climatix IC offering to improve user experience. Select "Accept all cookies" to accept.

Siemens respects your privacy. You can modify your preferences under "Manage settings".

Manage Consent Preferences:

+ Strictly necessary cookies	Always active
+ Performance cookies	
+ Marketing cookies	

Language selection

- Set the language in the portal navigation ribbon to the right.

5.2 Access concept to Climatix IC

Systematic security during access

Climatix IC provides two access methods that ensure systematic security.

- A user who already has access to Climatix IC, triggers an invitation e-mail: Access via "Register via e-mail invitation [➜ 25]".
- You possess a device activation key. You can simultaneously activate the device and create a user account. Access via 'Self-registration as plant owner using an activation key [➜ 28]'.

Integrate external logins

NOTICE
ℹ️	• User who want to use the same login for the Cloud API cannot use the external login.

Climatix IC integrates various external login providers. A user, e.g. who often uses Google tools and is logged on to Google, can also use this login data to log into Climatix IC. In the background and not visible to the user, the third-party providers are also forwarded through the Azure AD B2C procedure. See section "Register via e-mail invitation [➜ 25]".

NOTICE
!	**Reliably delete persistent external login data from the browser** External login procedures store information in the browser to increase user comfort. We recommend **private or incognito mode** for personal PCs, especially for public PCs. These browser modes reliably delete information when exiting the browser.

Frequently asked questions on logins

The following are answers to FAQs on logins.

How does login work with a social provider as the external login provider?

- You still need the Climatix IC user account as the starting point.
- The procedure as described in the following sections automatically connects an external login account at a social provider (e.g. from Microsoft, Google, or Siemens ID) to your Climatix IC account.
- After linking, you can click the logo of one of the listed social providers to login. The provider queries your login data.
- Simply click "Log-in" > "Logo of the social provider", to return to Climatix IC as long as the login data of the last login is stored in a browser session.
- The Climatix IC user e-mail address and the e-mail at the social provider must match.

When is a login not recommended or what should I look out for?

- Unprotected PCs without a windows login (e.g. private PC or Internet café) are not suitable, since the login data can remain in the browser.
- We recommend the incognito mode for your browser.
- Delete the browser data beforehand if you intend to switch the login role and use various external logins for both roles (check the browser's online help on how to do this).

What is the bill of quantity for IC user accounts and accounts at social providers?

- 1 account at a single social provider for 1 Climatix IC account and vice versa.

What is considered a secured login and logout?

- The terms and conditions of the login provider apply

5.3 Register

You must register as a new user in Climatix IC prior to logging into Climatix IC. You can register in one of two ways:

- A Tenant Administrator invites the new user (see section 'User').
    - The new user receives an e-mail with an invitation link and follows the workflow at the link (see section 'Register via e-mail invitation [➔ 25]').
- The new user has a plant with an activation key or tenant key.
    - The user can independently log in to Climatix IC using the activation key.
    - Using the workflow in section 'Self-registration as plant owner using an activation key [➔ 28]'.

The user can independently log into Climatix IC using the account after registering.

- For information on logging in, see section 'Registration and login [➔ 29]'.

5.3.1 Register via e-mail invitation

▷ A Tenant Administrator or a user with access to menu 'User' sets up a new user account with the e-mail address of the new user.

▷ Climatix IC sent an invitation e-mail with a link to Climatix IC. The user received the e-mail.

1. Click the link in the invitation e-mail from Climatix IC.

⇨ The Climatix IC start mask opens in the default browser with the e-mail address (1) of the invited user in the entry field.

⇨ A supplemental window opens with cookie preferences:

We value your privacy

By clicking "Accept All Cookies", you agree to the storing of cookies on your device and to the associated processing of data to enhance site navigation, analyze site usage, and assist in our marketing and performance efforts. You may withdraw your consent at any time via the "Manage Preferences" button in our Cookie Notice.

Cookie Notice   Manage Preferences
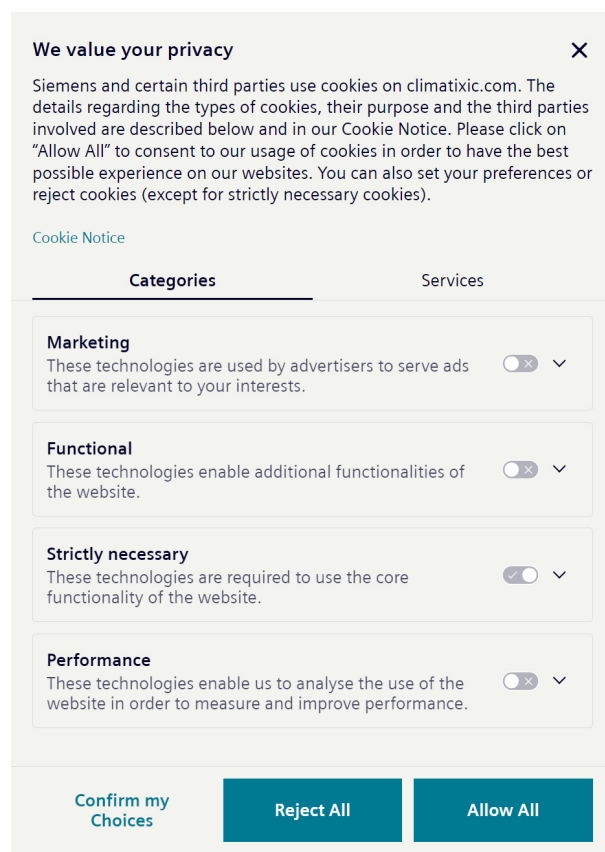
Reject Cookies   **Accept All Cookies**

2. Set and confirm cookie preferences:

We value your privacy   ✕

Siemens and certain third parties use cookies on climatixic.com. The details regarding the types of cookies, their purpose and the third parties involved are described below and in our Cookie Notice. Please click on "Allow All" to consent to our usage of cookies in order to have the best possible experience on our websites. You can also set your preferences or reject cookies (except for strictly necessary cookies).

Cookie Notice

Categories   **Services**

Marketing
These technologies are used by advertisers to serve ads that are relevant to your interests.

Functional
These technologies enable additional functionalities of the website.

Strictly necessary
These technologies are required to use the core functionality of the website.

Performance
These technologies enable us to analyse the use of the website in order to measure and improve performance.

Confirm my Choices   **Reject All**   **Allow All**

⇨ The cookie window closes.

3. Enter the first name (2) and last name (3) of the new user in the corresponding fields.

4. Enter a password for the new user access (4).

    –   Comply with password security requirements (see info below).
    ⇨   Entering a weak password triggers a note and the registration procedure is blocked until the password meets the minimum security requirements.

5. Repeat the password to confirm (5).

    ⇨   A note displays if the two passwords do not match, and the registration procedure is blocked until both passwords match.

6. Select 'Signup' (6).

⇨   You are registered.

⇨   The Climatix IC landing page opens for registration and login. See 'Set up multi-factor authentication and first-time login [➜ 30]'.

NOTICE
ⓘ	**The Climatix IC password must include:** At least 8 characters and includes at least one of the 4 character groups: ● Latin capital letters (A…Z) ● Latin low-case letters (a…z) ● Digits (0…9) ● Non-alphabetic characters (e.g. !, $, +,?)

NOTICE
ⓘ	**Protect passwords** ● Do not pass on your user name and password for Climatix IC to a third party. ● Encrypt e-mails that include the user name and password.

NOTICE	
ℹ	**Automatic password reset** The existing password is reset after 180 days. A new password must be entered thereafter: ● Password requirement (see note prior). ● Do not reuse a previous password: Climatix IC saves the last 5 passwords and blocks reuse. A warning displays when attempting to enter a previous password.

5.3.2 Self-registration as plant owner using an activation key

The user can independently register as the plant owner in Climatix IC. The Tenant-User must already be set up in tenant. The Tenant-User is then entitled to start the plant sign-up procedure. The plant does not have a default user in this case. An administrator adds a Default-User to the plant at a later date.

Procedure:

▷ The activation key is available.

▷ A tenant key is available as an alternative.

1. Go to the Climatix IC landing page: www.climatixic.com.

2. Click 'Register'.

    ⇨ A new log-in mask opens:

3. Enter your e-mail address (1).

4. Complete field 'Activation key' (2) or 'Tenant key' (3).

5. Click 'Register' (4).

⇨ You are registered.

⇨ The Climatix IC landing page opens for registration and login. See 'Set up multi-factor authentication and first-time login [➜ 30]'.

⇨ The plant↑ is activated but there is no plant owner.

⇨ But the Tenant-User can directly access the plant.

Self-registration is a multi-step procedure:

- First-time login of a user, without an invitation by another Climatix IC user with the appropriate privileges.
- Plant activation↑ using a valid activation key
- The new user is added to the plant↑ with the role↑ 'Owner'
- Optional: Direct move the plant to a Sub-Tenant↑ area

5.4 Registration and login

Access to Climatix IC is a two-step procedure:

1. First-time access to the login procedure for Climatix IC determines the login workflow.
2. The following logins to Climatix IC provide fast, simple, and secure access to Climatix IC using the previously determined login procedure.

---

i   You must register to log into Climatix IC. See section 'Register [→ 24]'

The login authentication for Climatix IC is performed by the authentication service of the identity provider and not by Climatix IC.

The Microsoft service Azure AD B2C creates an account for the default login (as a replacement for the former Climatix IC login). The user logs in as usual with the user name and password.

Climatix IC supports the following external login providers:

- Microsoft Private Accounts
- Google Private Accounts
- Siemens ID (not for Siemens employees using other Siemens apps)
- Siemens employee (Siemens employees only, via Microsoft Entra ID)

---

i   Multi-factor authentication MFA↑ must be set up and enabled at the appropriate login provider as needed. Consult the documentation from the applicable login provider on how to set up MFA.

Access control to Climatix IC via Microsoft Azure AD B2C

The external login providers listed above bundle the access information to Climatix IC in one authentication service: Microsoft Azure AD B2C. The authentication service saves and manages access data to Climatix IC.

Important note:

- The Climatix IC account and external provider login are in a 1:n relationship.
- The user can select and automatically link to an identity provider at any time.
- Users of API accounts or third-party apps, created based on Climatix IC APIs, must use the default login. MFA↑ is not required in this case.
- The e-mail address used for the external login provider and the Climatix IC account must be the same.
  - You cannot use one e-mail address for an external login provider, such as Microsoft, and then use the service to log in to an account under a different e-mail address on Climatix IC.

---

i   New as of D25: Access data is no longer managed internally in Climatix IC as of the introduction of Azure AD B2C. Existing menus to manage and edit access information, such as linking a Climatix IC account to an external login provider, have been switched off.

Existing accounts are automatically switched to the new login procedure during first-time login.

## 5.4.1 Set up multi-factor authentication and first-time login

ℹ The "Registration" described here applies to first-time login only.

Requirements for login: A user account is setup and an e-mail invitation is sent. Or self-registration using an Activation key or Tenant key was performed (See 'Register [➜ 24]'.

The following description of the login procedure includes configuring the external login for future logins (First-time login via a social provider [➜ 34]).

Login
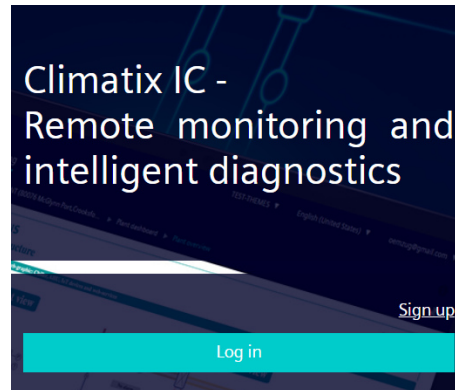
▷ An e-mail with the invitation link was received.

▷ The registration process was completed (See 'Register [➜ 24]').

1. Go to the Climatix IC landing page: www.climatixic.com.

2. Set the cookies (See 'Register via e-mail invitation [➜ 25]').

3. Click "Login".

4. Enter the e-mail address registered with the Climatix IC account and click "Login".
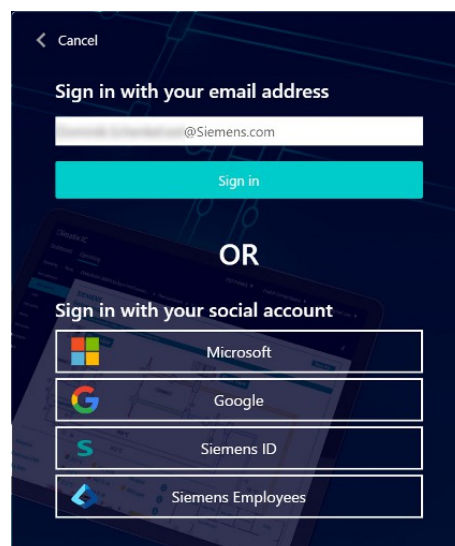
⇨ A new mask requests you install an authentication service app on an external device (cell phone or tablet).
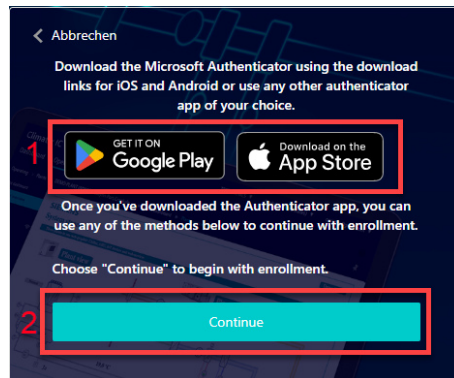
5. Install the recommended authentication services (1) or other authentication service (See 'Example for setting up an authentication service [➜ 33]').

6. Click "Continue" (2).

⇨ A QR code displays.
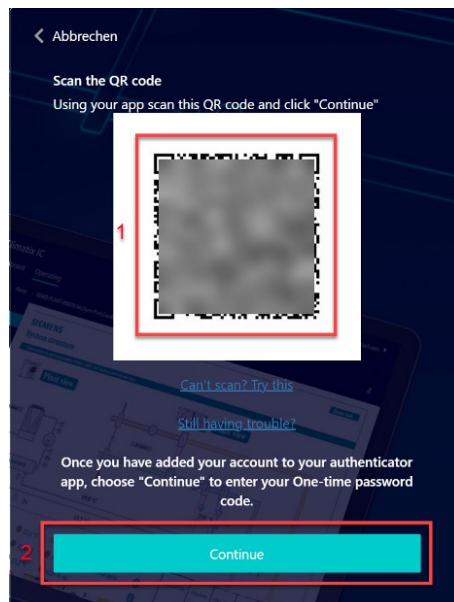
7. Scan the QR code (1) with the authentication service and save Climatix IC as a new password generator (See 'Example for setting up an authentication service [➜ 33]').

8. Click "Continue" (2).

⇨ A new mask requests that you enter the code.
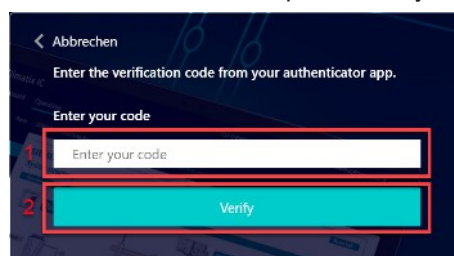
9. Enter the one-time password from the Climatix IC password generator (1) and click "Check" (2).

⇨ The login is successful and the Climatix IC landing with dashboard opens.

Secure login and out

Note the following functions for login/out:

- **30 minute session timeout**: The connection automatically ends after 30 minutes of inactivity. The web page returns to the Login screen.
  NOTICE! **Only the activity on the first tab is registered when working in multiple browser tabs.**
- The user account is locked for 60 seconds after 10 attempts with the wrong password.
  - Additional attempts only extend the lockout.
  - Microsoft 'Smart Lockout' is used here.
- For security reasons, a new login is required after 24 hours of uninterrupted user activity.

| *NOTICE*	
ℹ	**Protect passwords** ● Do not pass on your user name and password for Climatix IC to a third party. ● Encrypt e-mails that include the user name and password.

ℹ	For log-out, see also "Account details and log out".

### 5.4.1.1 Example for setting up an authentication service

'Microsoft Authenticator': An example of how to set up an authentication service on an external device (cell phone or tablet).
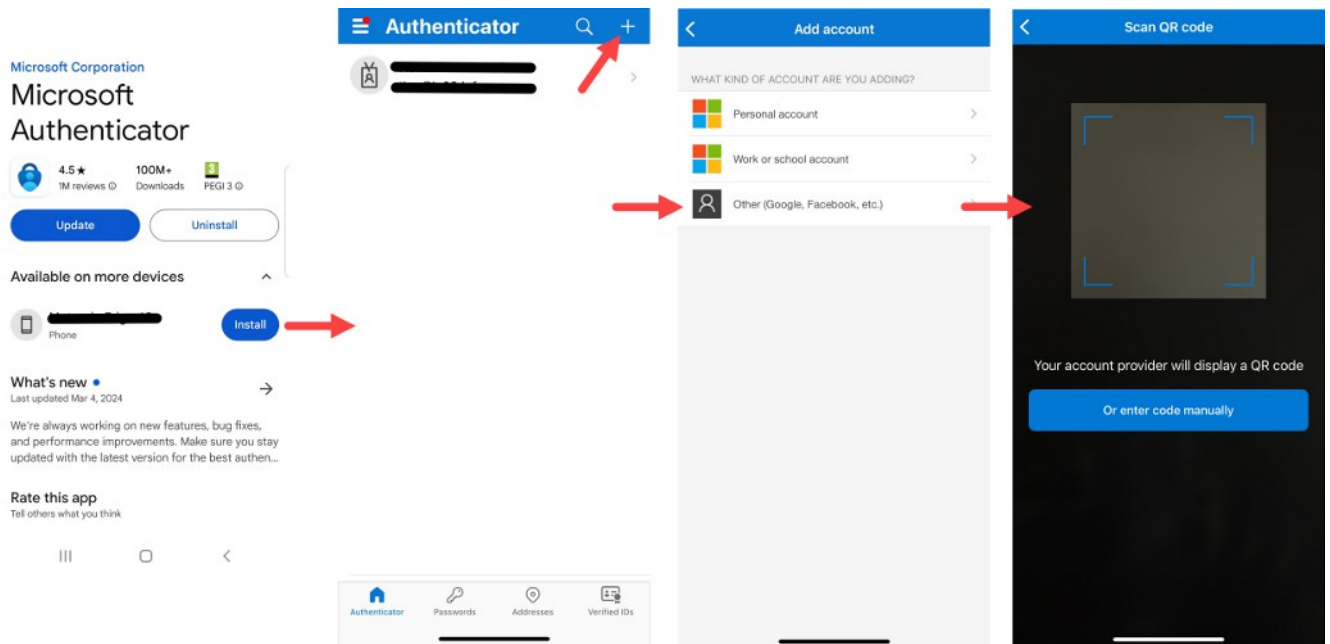
▷ An external device (cell phone or tablet) is available.

▷ The external device has Internet access.

▷ You have administrator rights to install the software.

1. Go to the app store for the external device.

2. Select an authentication service from the app store and install on the external device.

   – For example, 'Microsoft Authenticator', 'Google Authenticator' or similar apps.

3. On the installed authentication service, create an account using the '+' icon.

   – Select the type of new account: 'Other (Google, Facebook, etc.)'.

4. Use the new account to scan the QR code provided by Climatix IC.

⇨ The authentication service is installed.

⇨ A new account is setup in the authentication service.

⇨ The account on the external device is linked to the Climatix IC account.

5.4.2   First-time login via a social provider

**Login using an external authentication service**
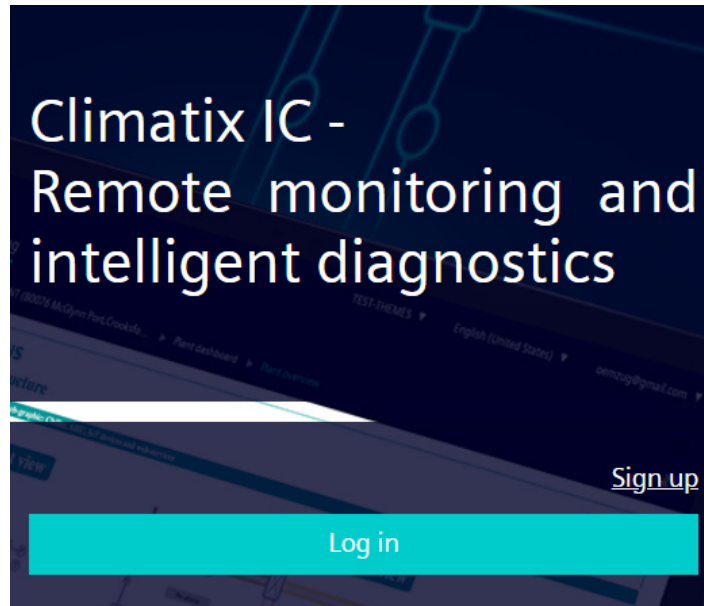
In the login dialog, select the button with your external identity provider under "Log in with social network account" and follow the login procedures of the external provider.

i	For log-out, see also "Account details and log out".

5.4.3 Fast login with existing account

The workflow to log into Climatix IC is as following once the account is setup:
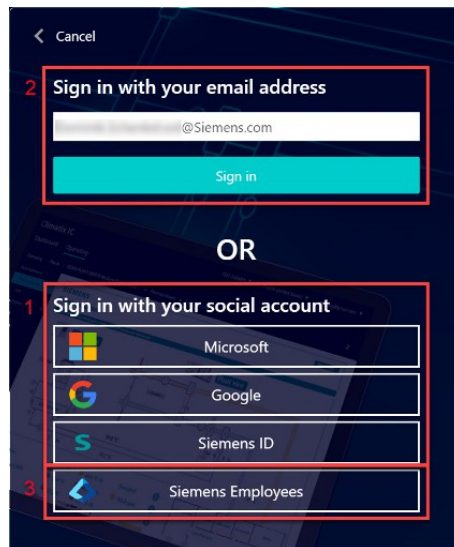
Log in via social provider

1. Go to the Climatix IC landing page: www.climatixic.com.

2. Set the cookies (See 'Register via e-mail invitation [➜ 25]').

3. Click "Register".

   ⇨ A mask opens to select the social providers.

4. Click your social provider (1):

   ⇨ Microsoft (private account)
   ⇨ Google (private account)
   ⇨ SiemensID (not for Siemens users)

5. Log in at an external identity provider.

6. Enter local Climatix IC password once for verification and linking to the account.

⇨ Complete login.

⇨ The login is successful and the Climatix IC landing with dashboard opens.

Log in as Siemens employee

1. Go to the Climatix IC landing page: www.climatixic.com.

2. Set the cookies (See 'Register via e-mail invitation [➙ 25]').

3. Click "Register".

4. **Option 1**: Enter e-mail address and click login (2).

   ⇨ You are automatically forwarded to the Siemens Entra ID login.

5. **Option 2**: Click "Siemens employees" (3).

   ⇨ Login is automatic via Siemens Entra ID.

⇨ The Climatix IC with dashboard opens.

Secure login and out

Note the following functions for login/out:

- **30 minute session timeout**: The connection automatically ends after 30 minutes of inactivity. The web page returns to the Login screen.
  NOTICE! **Only the activity on the first tab is registered when working in multiple browser tabs.**

- The user account is locked for 60 seconds after 6 attempts with the wrong password.
  – Additional attempts only extend the lockout.
  – Microsoft 'Smart Lockout' is used here.

- For security reasons, a new login is required after 24 hours of uninterrupted user activity.

5.4.4 Multi-Factor Authentication

An existing Multi-Factor Authentication (MFA) can be reset in Climatix IC. This is required when an external device used for MFA is replaced.

- Note: Multi-Factor Authentication using an external service (i.e. non-Climatic IC device), for example, Google, internal Siemens or similar must be reset using that service.

Independent reset of Multi-Factor Authentication

When changing to a new external device, the account owner must change the MFA to the new device in Climatix IC to continue to access the account.

How to proceed as the account owner:

▷ A Climatix IC account with access to a Tenant is available (See 'Register [➜ 24]').

▷ A Multi-Factor Authentication via Climatix IC is set up (see 'Set up multi-factor authentication and first-time login [➜ 30]').

▷ The external device originally used to authenticate is available.

1. Go to Account details (1).

2. Select 'Reset MFA' (2).

   ⇨ The existing MFA is reset.

3. Log out of Climatix IC.

4. Log in to Climatix IC using the existing log-in data.

5. Follow the instructions on how to set up a new MFA (See 'Set up multi-factor authentication and first-time login [➜ 30]').

   – Use the new external device.

⇨ The MFA is renewed.

⇨ The new external device is not integrated for future authentication.

⇨ The device used to date can no longer be used for authentication.
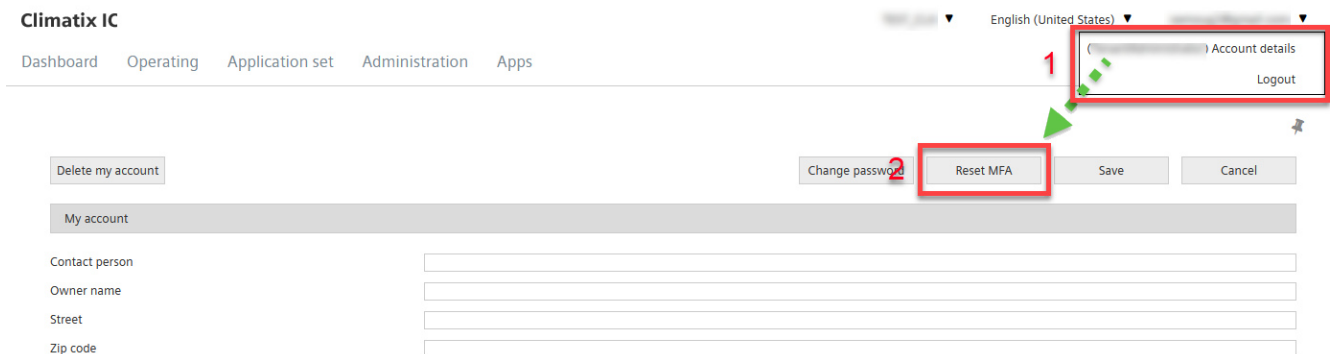
Have the Tenant Administrator reset the MFA.

The user can no longer access the account if the external device is lost or damaged. The Tenant Administrator can reset the account MFA in this case:

- Main-Tenant admins can reset multi-factor authentication for all Tenant Users.
- Sub-Tenant admins can only reset multi-factor authentication for Tenant Users of their Tenants.

Procedure as the Tenant Administrator:

▷ A Climatix IC account with access to the Tenant is available (See 'Set up multi-factor authentication and first-time login [➜ 30]').

▷ MFA was set up via Climatix IC.

▷ The device originally used for authentication is no longer available (for example, due to damage or loss) and a new device must be integrated for authentication.

1. Go to "Administration > User > 'Account for reset'".

2. Select 'Reset MFA' (1).

⇨ The existing MFA is reset.

3. The account owner is notified that the MFA was reset.
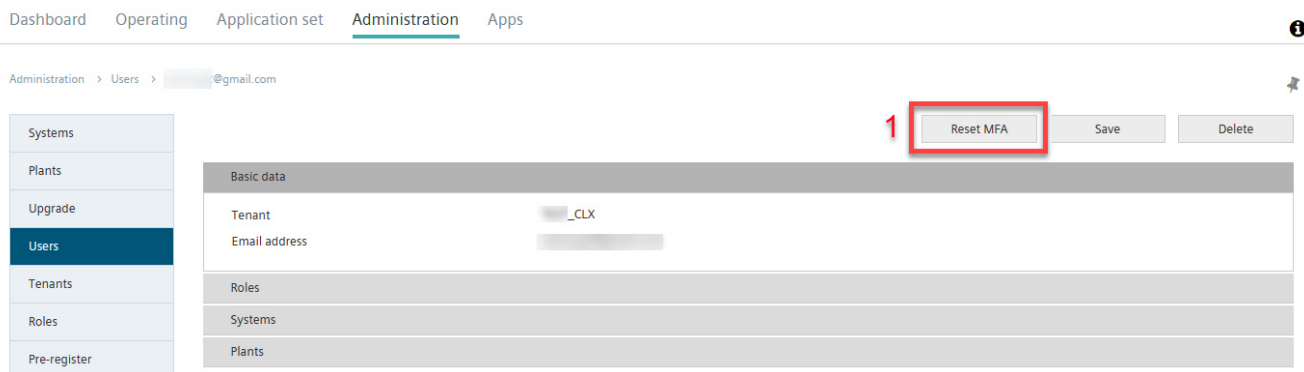
Additional steps as the account owner:

▷ The Tenant Administrator resets the MFA stored for the account.

1. If the user is logged in to Climatix IC: Log out.

2. Log in to Climatix IC using the existing log-in data.

3. Follow the instructions on how to set up a new MFA (See 'Set up multi-factor authentication and first-time login [➜ 30]').

   – Use the new external device.

⇨ The MFA is renewed.

⇨ The new external device is not integrated for future authentication.
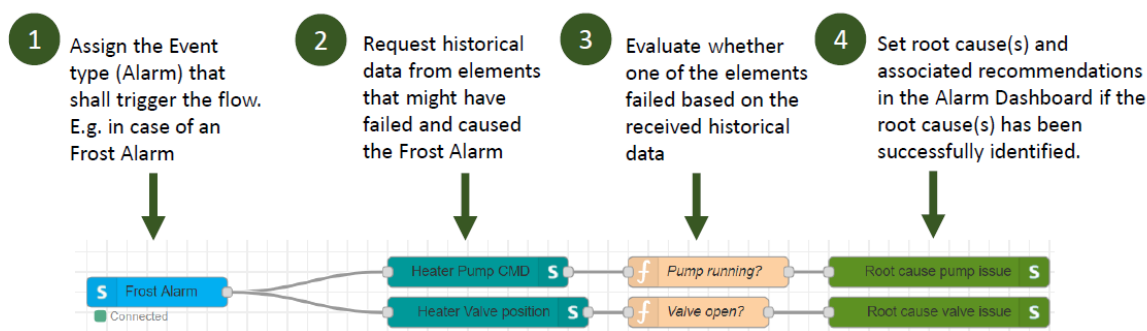
6 Menu Rule Editor
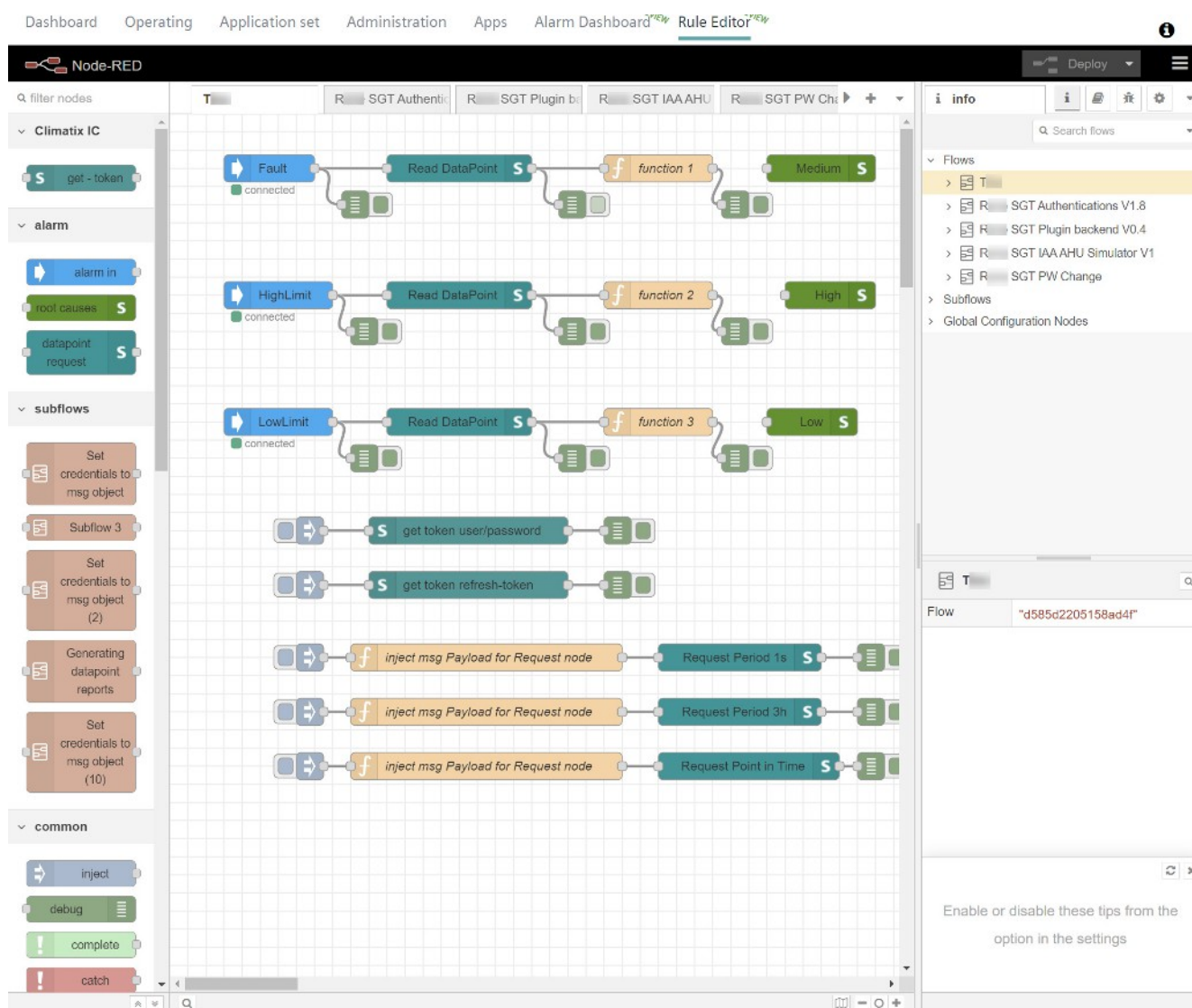
Configuration workflow at a glance

The Alarm Dashboard (see 'Alarm Dashboard menu') and Rule Editor work together to perform the workflow.

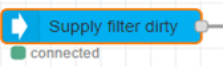The following conditions must be met:
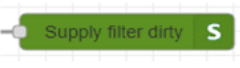
- An alarm type is defined;
- a root cause is defined;
- the rule is defined.

The following image show the workflow at a glance:

1. Assign the Event type (Alarm) that shall trigger the flow. E.g. in case of an Frost Alarm

2. Request historical data from elements that might have failed and caused the Frost Alarm

3. Evaluate whether one of the elements failed based on the received historical data

4. Set root cause(s) and associated recommendations in the Alarm Dashboard if the root cause(s) has been successfully identified.

The internal attribute links as follows:

Overview and interconnections of attributes accross the various menus/tools

ClimatixIC	Alarm string	Alarm ID				
Example	Supply filter	1234567891				

AlarmType		Alarm ID	Description	Label		
Example/Remark		1234567891	free text	(free text) Supply filter dirty		

Root Cause				Description of root cause	Root cause label	
Example/Remark				free text	(free text) Supply filter dirty xyz	
			Supply filter dirty connected			Supply filter dirty **S**

Rule Editor	Name	Alarm type	Name	Root causes
Example/Remark	free text	(Selection) Supply filter dirty	free text	(Multiselect) Supply filter dirty xyz (v-1)

---

i   For detailed information on Rule Editor: See document A6V12441321, in 'Additional information'.

---

7 Climatix IC portal security

7.1 Climatix IC

The portal provides thorough security, e.g. data security, security data storage, and reliable data transportation.

● All connections are encrypted (HTTPS) to prevent tapping into the line and man-in-the-middle attacks.

● Data security as per EU Data Privacy Chapter 5

● Geo-redundant data storage from northern Europe (primary) to western Europe (secondary).

Virus scan during upload

Uploaded files are scanned for viruses.
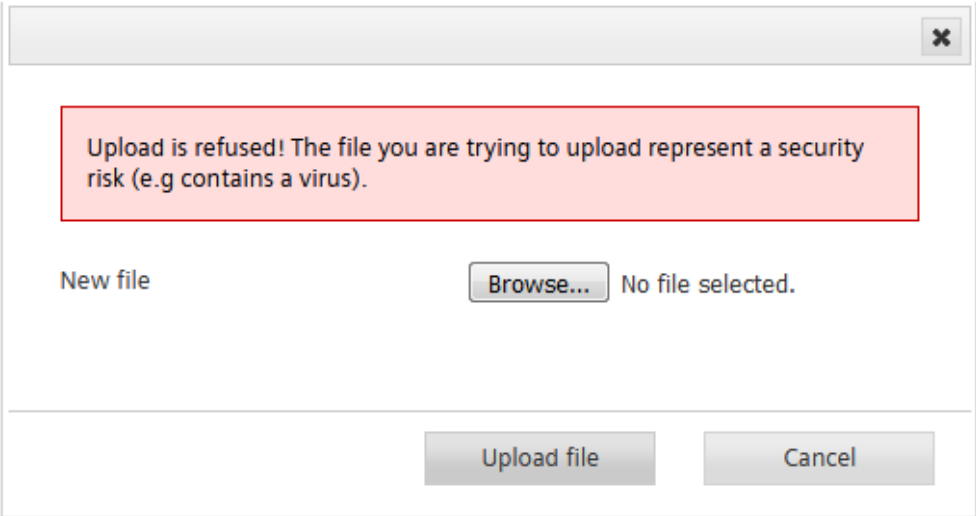
Virus scan during download

A residual risk remains to the portal of loading and saving infected files to the system despite performing a virus scan during upload files.

⚠ CAUTION	
!	**Damage to the client caused by downloading infected files**
	Perform a virus scan of the files downloaded from the system to prevent infections to the clients from the files.

7.2 Climatix controller

The Climatix controller is not suitable for connecting directly to the Internet; it must be connected via a firewall↑. This type of router typically has a firewall↑.

The firewall↑ must be configured to permit only outgoing connections. Incoming connections must be suppressed.

8 Support

Extranet registration

Register for the OEM extranet and access exclusive information and resources:
http://www.siemens.com/buildingtechnologies-oem.

Support on technical problems

Please adhere to the following sequence on support issues:

1. Contact the supplier of the device or plant.
2. If unknown, Siemens provides the following tools:

- Research info via Smart Information Delivery Portal (SID):
  https://sid.siemens.com.
- Research information via the Service and Support Portal:
  https://support.industry.siemens.com.
- Submit a support request:
  https://support.industry.siemens.com/cs/ww/en/my.

Climatix IC status page

Neutral and objectively reported online state of Climatix IC:
https://status.climatixic.com.