CoreStation Setup Manager

USER GUIDE

Version 1.02

English
EN 102.00.CSM

suprema
SECURITY & BIOMETRICS

CONTENTS

Getting Started 3

Minimum requirements 3

Initial Setup of the Device 4

Device Settings 7

Search and register slave device 7

Restart device 8

Modify device settings and information 8

Monitoring 15

Input port status 15

Output port status 16

Wiegand port status 16

Settings 17

Edit admin account 17

Web server network 18

Appendices 19

Disclaimers 19

Copyright Notice 19

Getting Started

CoreStation Setup Manager is a web server that manages the network settings of CoreStation or checks the connection status of slave devices, input and output ports, and Wiegand ports. With CoreStation Setup Manager, you can check the status of the network and wiring on-site without having to go to the BioStar X server location while configuring the access control system using CoreStation.

The following features are available in CoreStation Setup Manager.

- IP address setting
- Check CoreStation device information
- CoreStation Settings Backup and Restore
- Admin settings
- Check the connection status of slave devices
- Monitor input and output, Wiegand port status
- Initialize device, excluding network settings
- Factory reset

Minimum requirements

Check compatible devices and firmware versions.

- CoreStation firmware version 1.3.1 or higher
- CoreStation 20 firmware version 1.0.0 or higher

Info

- CoreStation Setup Manager is supported on CoreStation firmware version 1.3.1 or higher, and CoreStation 20 firmware version 1.0.0 or higher. If using a lower version of firmware, connect to BioStar X to upgrade the firmware to the latest version.
- For more details on how to connect and install each device, refer to the guide for the respective product.
  - CoreStation
  - CoreStation 20
- For more information on CoreStation and CoreStation Setup Manager, contact Suprema Technical Support Team.

Initial Setup of the Device

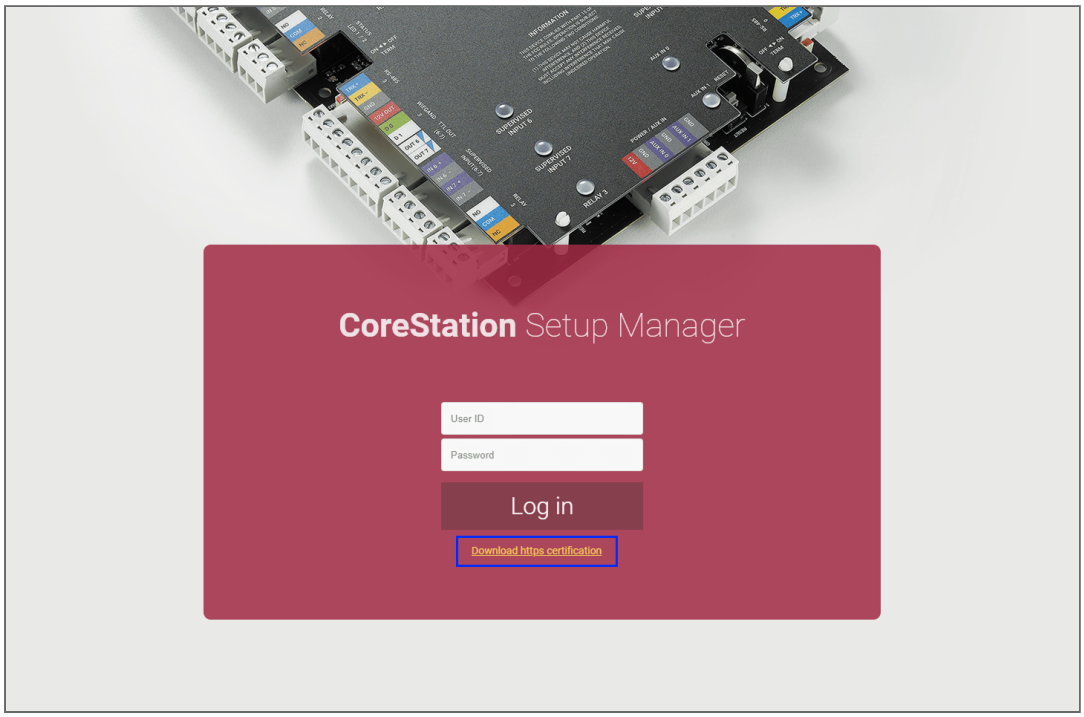
CoreStation Setup Manager provides a web-based service. Therefore, after completing the wiring to build a centralized access control system using CoreStation, you can access CoreStation Setup Manager from any location via a web browser and check the connection status of CoreStation.

If you are using CoreStation Setup Manager for the first time, connect CoreStation and proceed with the initial setup.

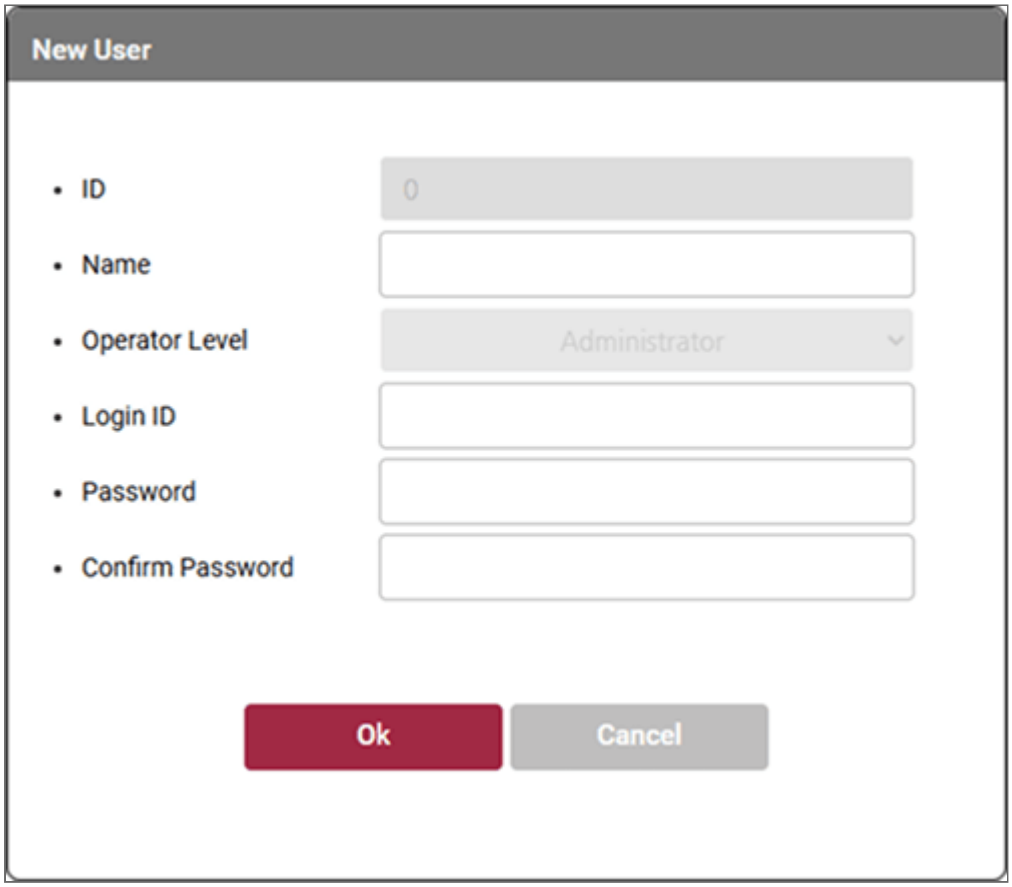
1. Complete the cable connection to CoreStation.
2. Please launch the web browser.

> **Info**
> Use a web browser version 75 or higher of Chrome.

3. Enter the default IP address `https://169.254.0.1:3001` in the address input field of the web browser.
4. Click **Download https certification** on the login screen. When accessing CoreStation Setup Manager for the first time, you need to install the certificate to use HTTPS correctly.



5. Run the **cs_client.crt** file.
6. When the **Open File - Security Warning** window appears, click **Open**.
7. In the **Certificate details** window, click **Install Certificate...**. The **Certificate Import Wizard** will be launched.
8. Click **Next** to continue.
9. Select the certificate store and then click **Next** → **Finish** → **OK**.
10. Enter your user ID and login password. The user ID and login password for the first access are both 'admin'.
11. To register the administrator account, configure each item and click **OK**.



Name	Feature description
ID	The ID is automatically set to **0** and cannot be changed.
Name	Enter the administrator's name. - A name of up to 48 characters can be entered.
Operator Level	The Operator Level is automatically set to **Administrator** and cannot be changed.
Login ID	Enter the login ID. - The login ID can be up to 32 characters long.
Password	Enter the login password. - The login password should be a combination of alphanumeric characters and symbols, with a length of 7 to 32 characters.
Confirm Password	Re-enter the login password for confirmation.

12. You will be redirected to the login screen. Log in with the registered administrator account.

Info

- The administrator account can only be set up when accessing CoreStation Setup Manager for the first time, and only one user can be designated. Once registration is complete, the default user ID and login password used during the first access can no longer be used. Additionally, the administrator account can review and edit all settings, including factory initialization.
- Starting from CoreStation Setup Manager version 1.01, the name of the **Level 1** administrator grade has been changed to **Administrator**, and **Level 2** to **Level 3** administrator accounts are no longer supported.

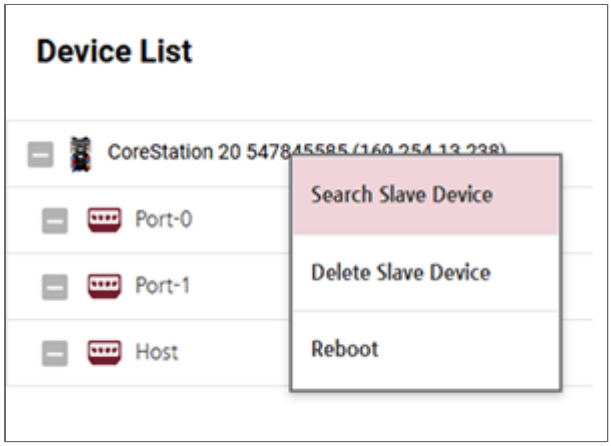
Device Settings

Guide for device settings and management.

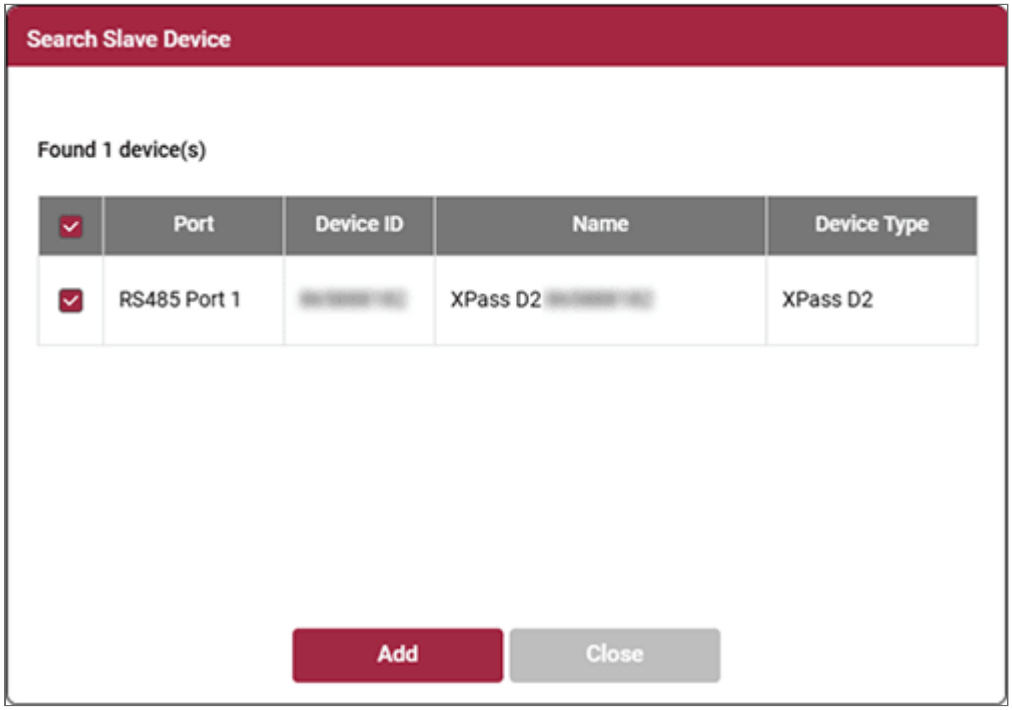
Search and register slave device

You can easily expand the access control system's network by adding slave devices to CoreStation. CoreStation (master) and slave devices can be connected via RS-485, and additional devices such as Secure I/O can also be connected for use.

1. Click **CONFIGURE**.
2. Right-click on CoreStation in the Device List and click **Search Slave Device**. A list of slave devices connected to CoreStation will appear.



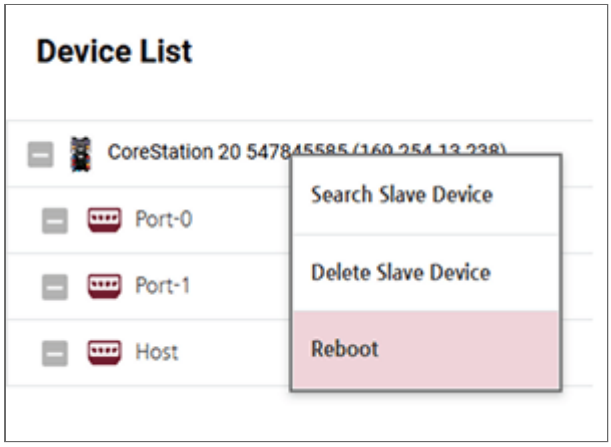
3. Select the device to register as a slave and click **Add**. Alternatively, you can select individual ports to add slave devices.



Restart device

The user can restart the device.

1. Click **CONFIGURE**.
2. Right-click on CoreStation in the Device List and click **Reboot**.

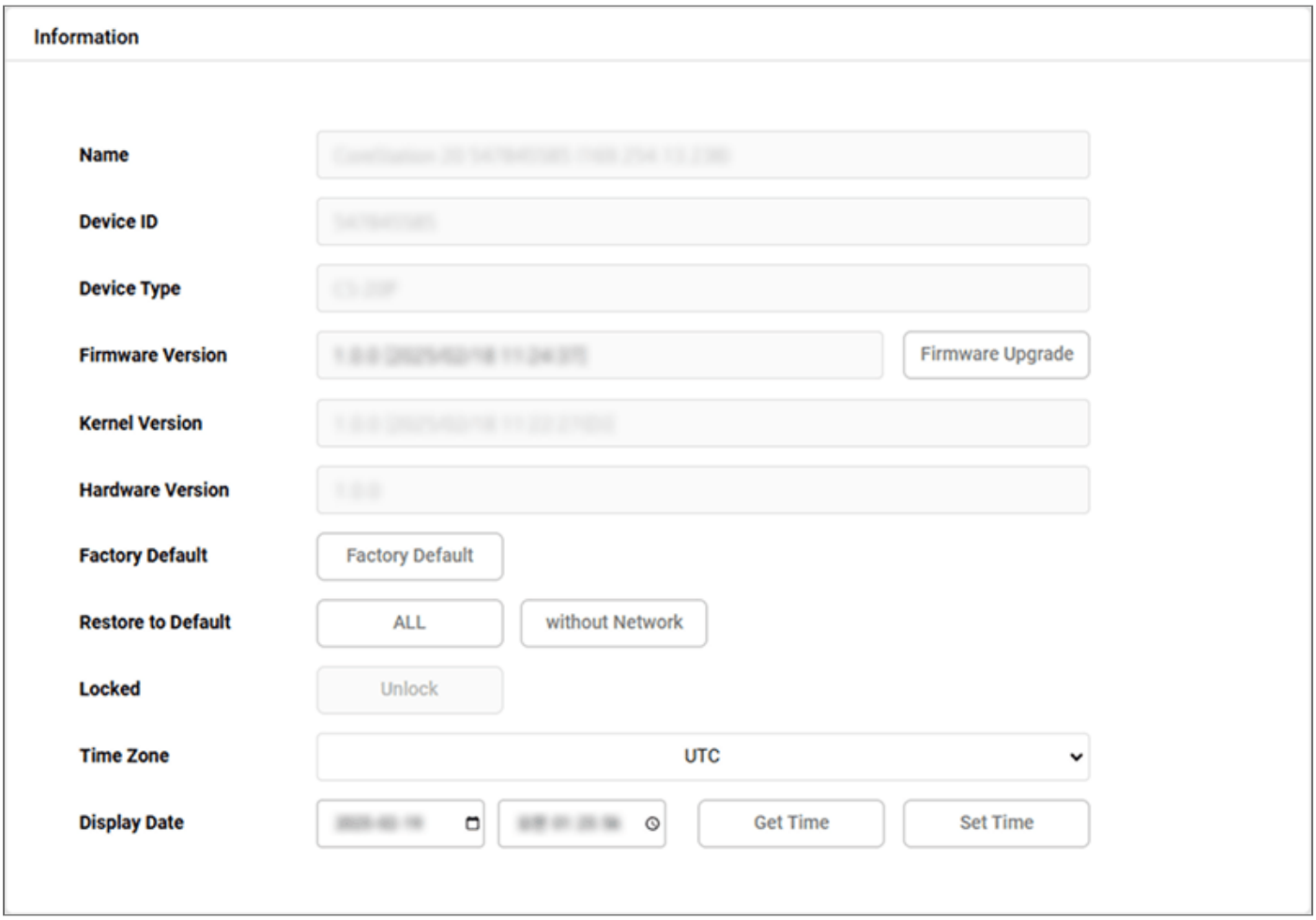


Modify device settings and information

You can configure details for CoreStation.

1. Click **CONFIGURE**.
2. Edit the necessary fields.
3. To complete all settings and save changes, click **Apply**.

Information



Name	Feature description
Name	You can check the device name.
Device ID	You can check the device ID.
Device Type	You can check the device type.
Firmware Version	You can install a new version of the firmware by clicking **Firmware Upgrade** and selecting the firmware file to upgrade.
Kernel Version	You can check the kernel version.
Hardware Version	You can check the hardware version.
Factory Default	You can delete all information stored on the device and reset the settings.
Restore to Default	You can initialize the device settings. - **ALL**: Initializes all settings. - **without Network**: Initializes all settings except network settings.

Name	Feature description
Locked	When the device is locked due to operating conditions, you can use the **Unlock** button.
Time Zone	You can set the device's time zone.
Display Date	You can manually set the date and time. - **Get Time**: Click to retrieve the time set on the device. - **Set Time**: Click to apply the time set in the CoreStation Setup Manager to the device.

Info

The **Factory Default** menu can be used when a root certificate is stored on the device. Executing a factory reset will delete the administrator account.

Backup and Restore

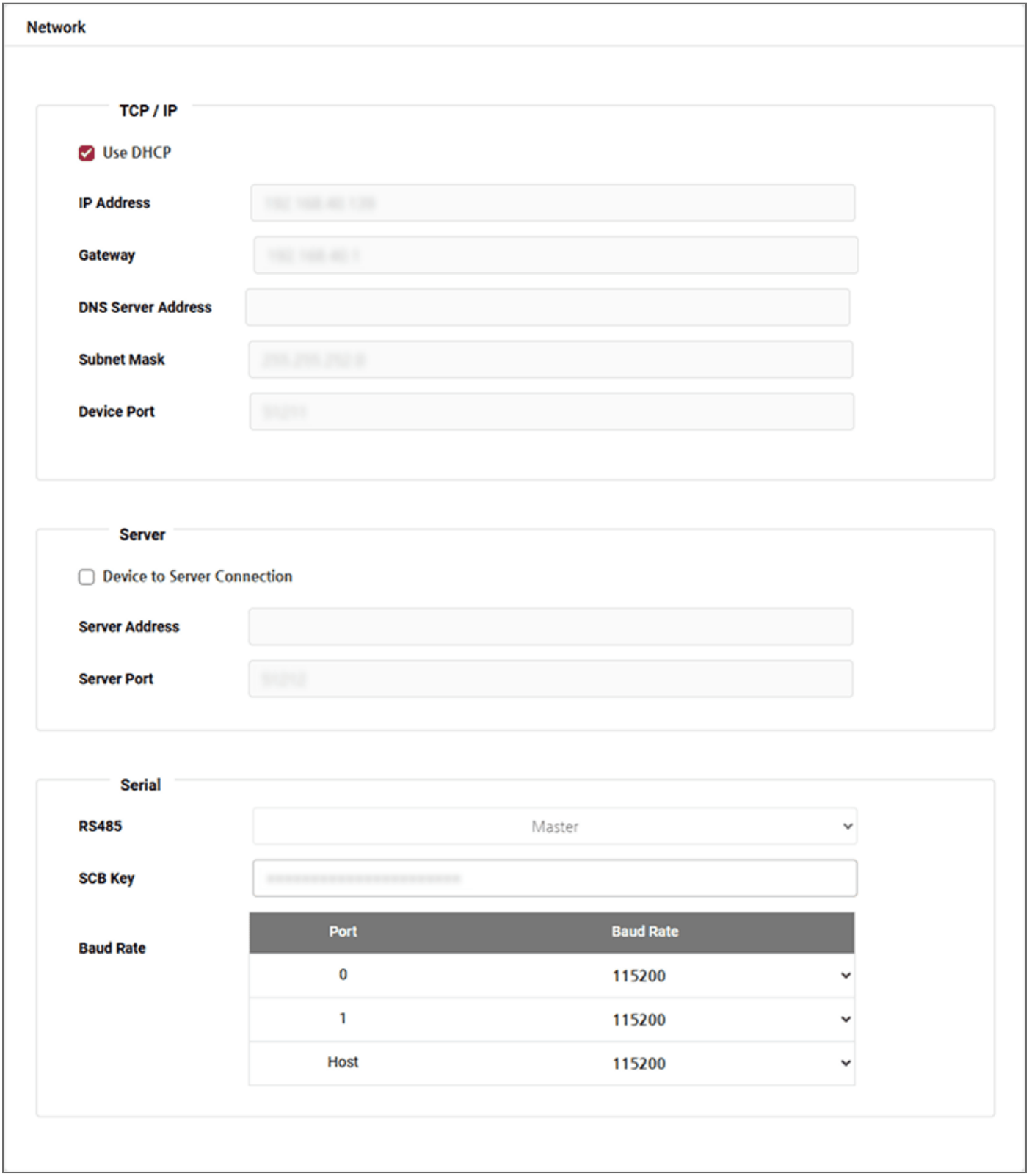


Name	Feature description
Device Backup	Click **Export Backup Data** to back up CoreStation setting information to a file. The backup file is compressed, encrypted, and saved to the download location set in the browser.
Restore Device	Click **Import Backup Data** to restore CoreStation setting information from a backed-up file.

Info

- The backup file includes the Device ID, Network (IP, DNS, Server, Gateway), RS485 Baud Rate (per channel), SCB Key, and root certificate. The MAC address is not included in the backup file. When you replace a device, the MAC address changes, so the IP address may change in a DHCP environment. Use a static IP for backup and restore.
- Restore is available only between the same device types as the one used to create the backup file.
- If slave devices are connected to CoreStation, SCB Key restore is not supported. You cannot restore a CoreStation that already uses the SCB Key to connect slave devices.

Network

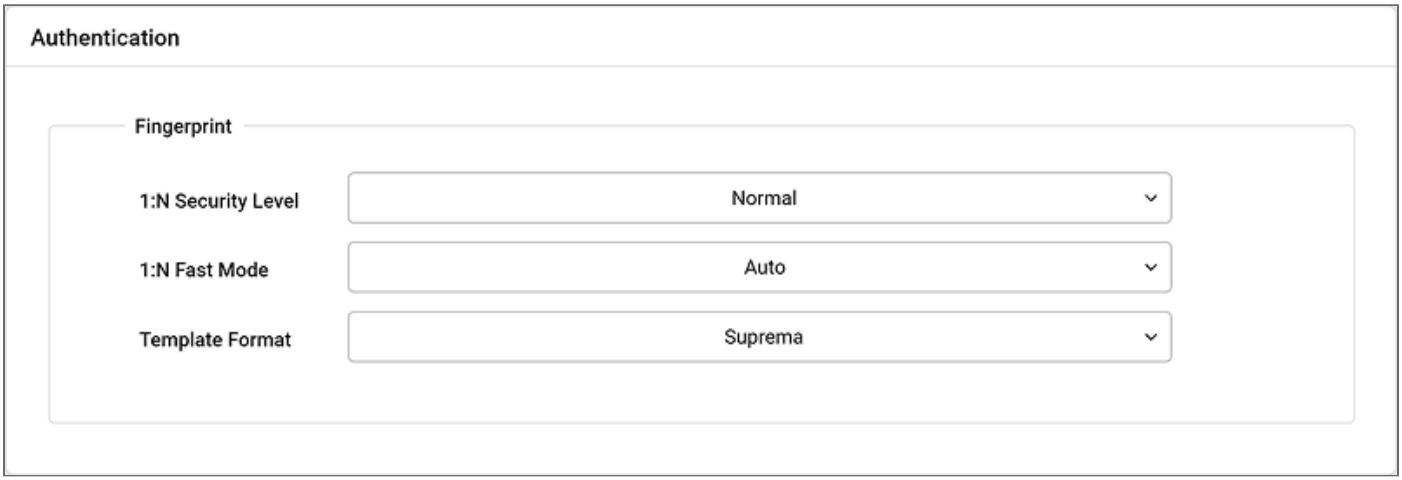


Name	Feature description
Use DHCP	Select this option to set the device to use a dynamic IP address. If you select this item, a fixed IP address cannot be assigned.

Name	Feature description
IP Address	You can check the device's IP address.
Gateway	You can check the device's gateway.
DNS Server Address	You can check the device's DNS server address.
Subnet Mask	You can check the device's subnet mask.
Device Port	Enter the port the device will use.
Device to Server Connection	Selecting this option allows you to enter BioStar X server information to connect the device to the server.
Server Address	Enter the IP address or domain address of the BioStar X server.
Server Port	Enter the port of the BioStar X server.
RS485	Only master mode is available.
SCB Key	Enter the security key to apply to CoreStation directly.
Baud Rate	You can set the transmission speed for each RS-485 port.

Info
If slave devices are connected to CoreStation, you cannot set the SCB Key.

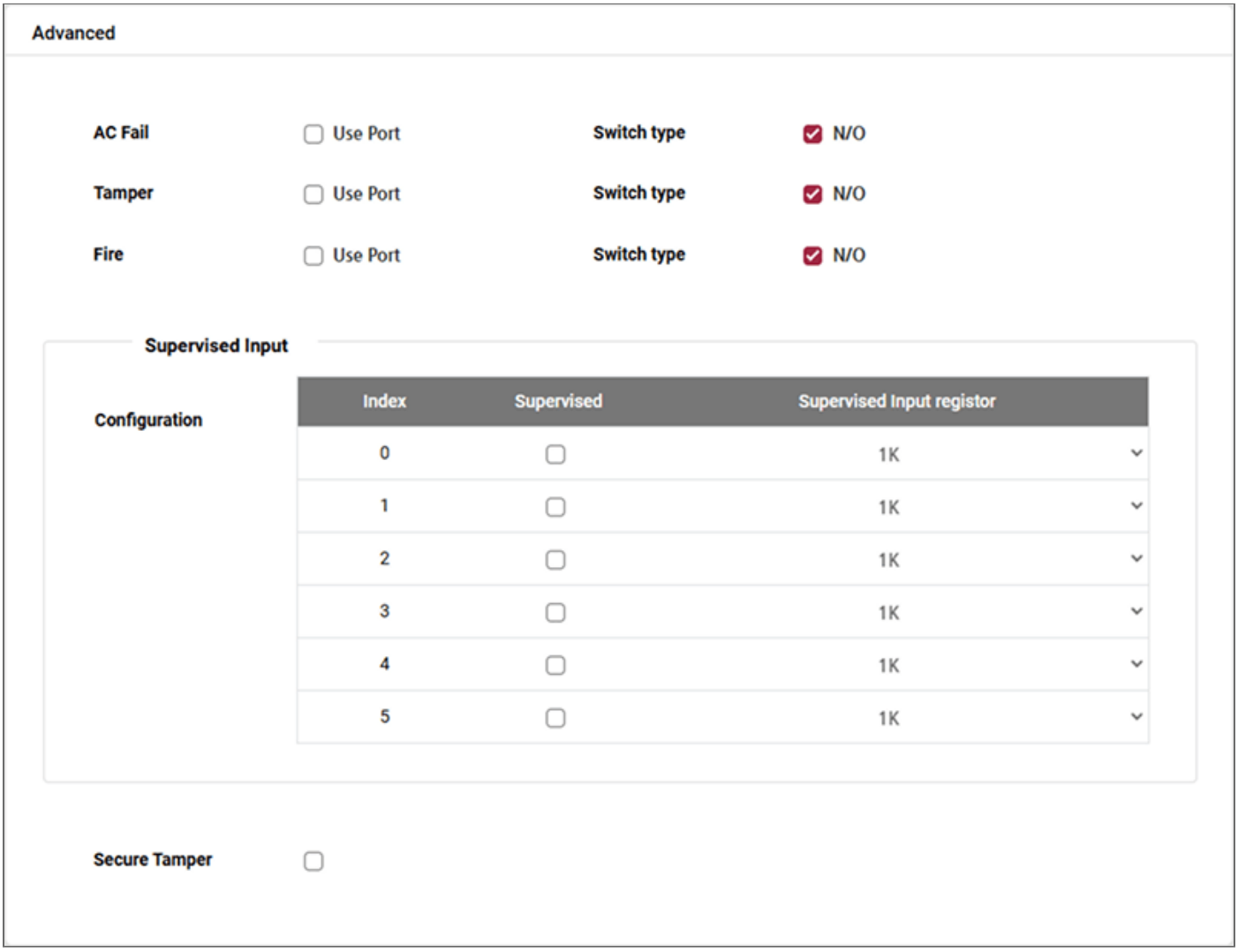
Authentication



Name	Feature description
1:N Security Level	You can set the security level used to authenticate fingerprints. As the security level increases, the false rejection rate (FRR) increases, while the false acceptance rate (FAR) decreases.
1:N Fast Mode	You can set the speed of fingerprint authentication. Selecting **Auto** sets the authentication speed according to the total number of fingerprint templates enrolled on the device.
Template Format	You can check the configured fingerprint template format.

Info
Biometric authentication is supported only on CoreStation.

Advanced Settings



Name	Feature description
AC Fail	You can set an AUX port to monitor power input signals.

Name	Feature description
Tamper	You can set an AUX port for tamper notifications.
Fire	You can set an AUX port to monitor fire detection signals.
Configuration	You can set CoreStation's Supervised Input port as an Input port and configure the resistor value to be used for Supervised Input. Resistor values can be set to 1 kΩ, 2.2 kΩ, 4.7 kΩ, or 10 kΩ.
Secure Tamper	In the event of tampering with the device, you can set it to delete all user information, logs, and security keys stored on the device.

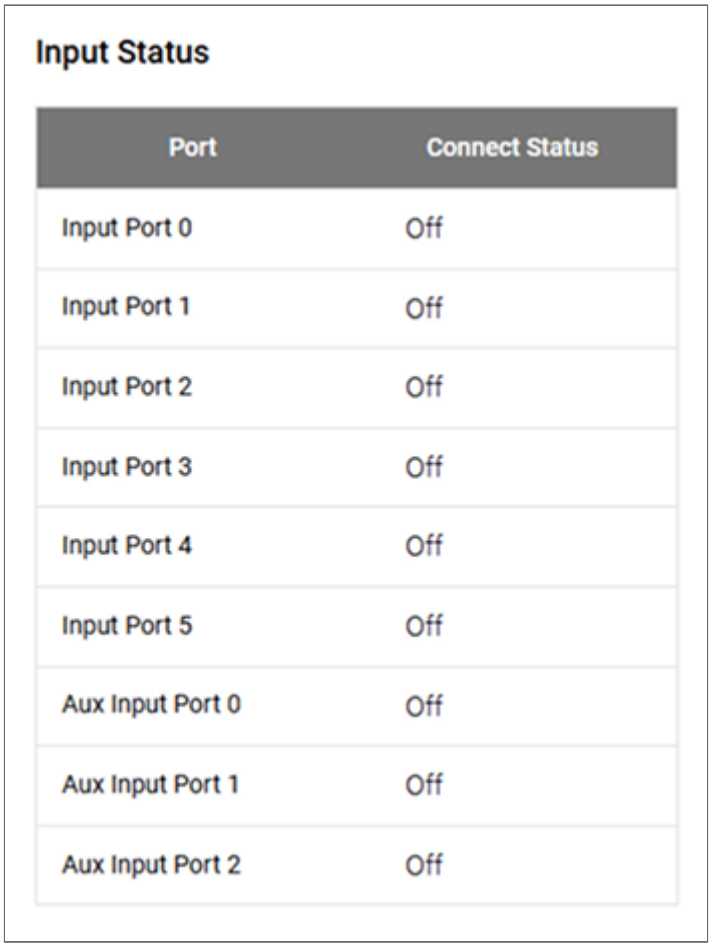
Monitoring

You can check the real-time status of the input and output of the CoreStation after completing the wiring. You can also check the scanned card ID from the connected Wiegand reader.

> **Info**
> The number of ports that can be connected may vary depending on the CoreStation model.

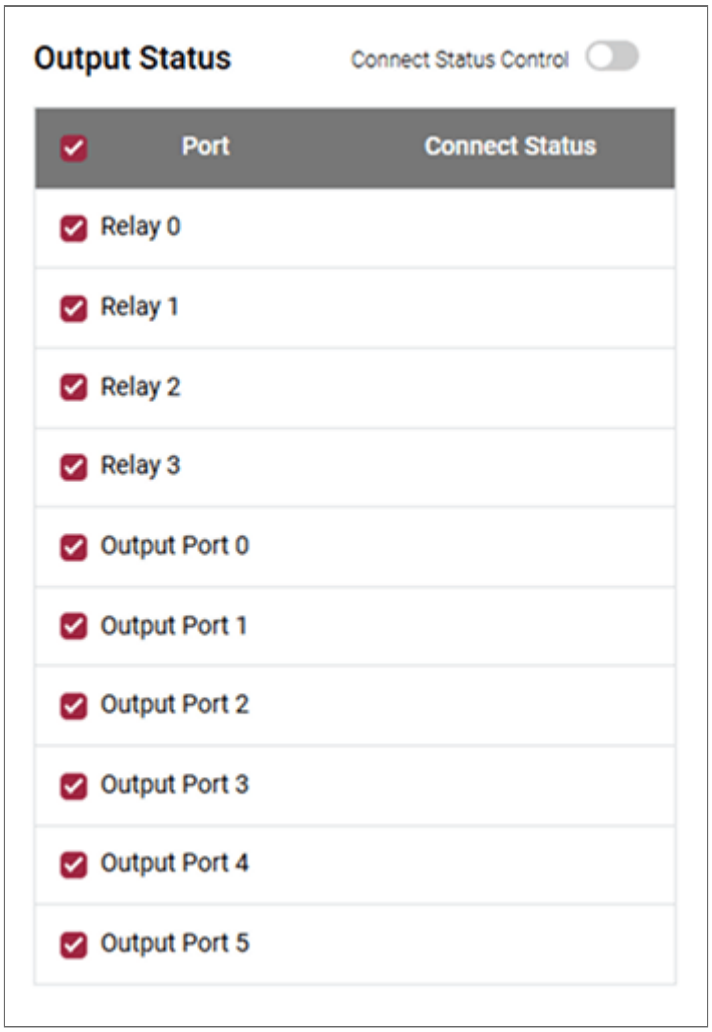
Input port status

The connection status of the input and Aux input ports is displayed. You can check the connection status of the input port on-site right after completing the wiring.



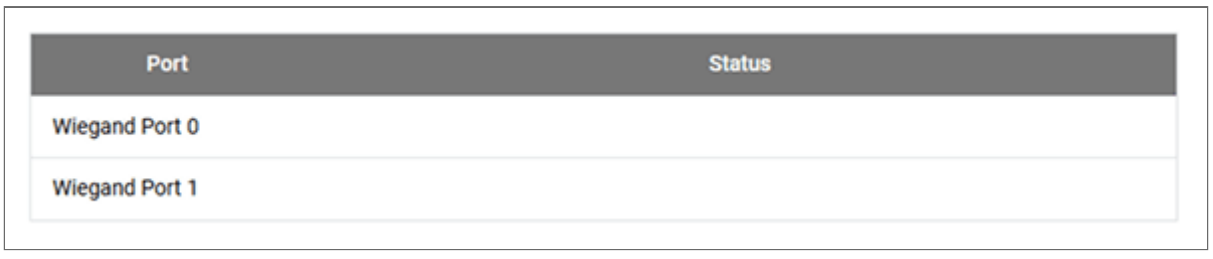
Output port status

The connection status of the relay and output ports is displayed. Select the desired item and click the switch to control the relay and output ports.



Wiegand port status

When a card is scanned at the Wiegand reader connected to the Wiegand port, the corresponding card ID will appear in the **Status** column.



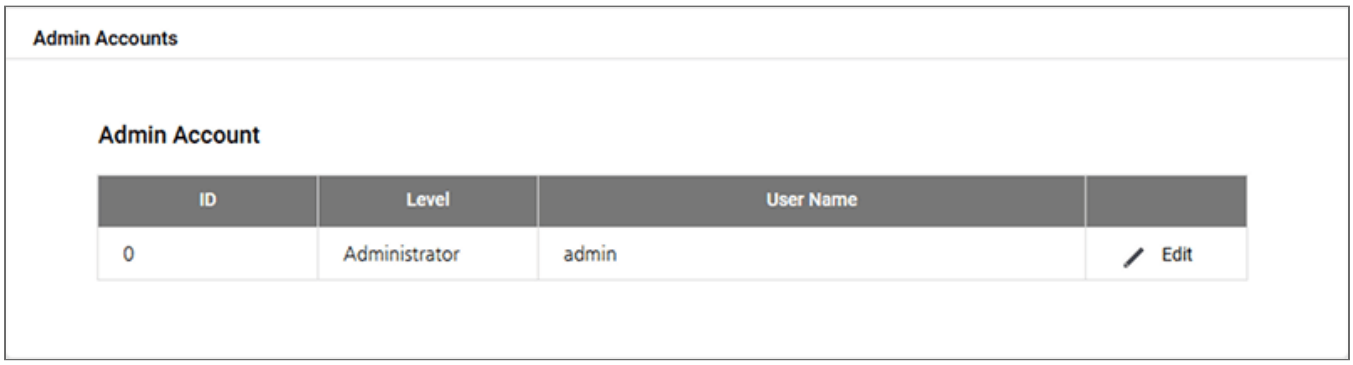
Settings

Guidance on how to set up the admin account and web server network settings.

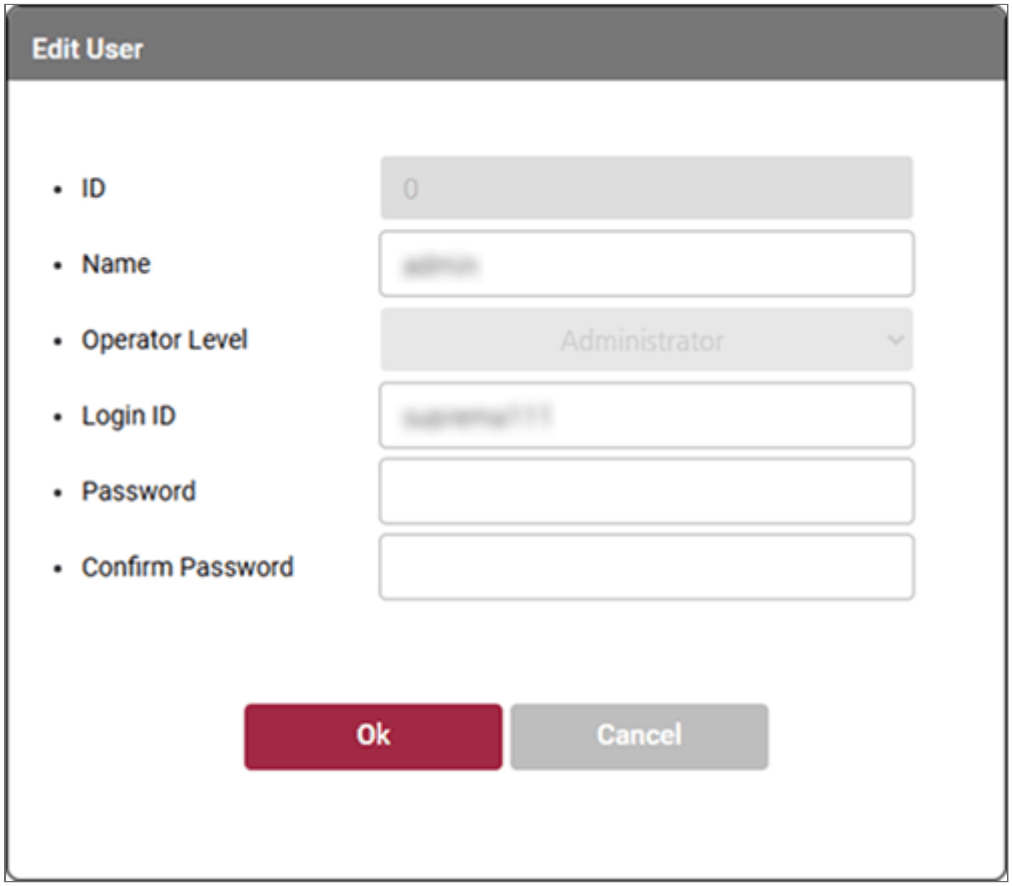
Edit admin account

You can edit the admin account of the CoreStation Setup Manager.

1. Click **SETTINGS**.
2. Click **Admin Account** → **Edit**.



3. Refer to Initial Setup of the Device, edit each item, and then click **OK**.

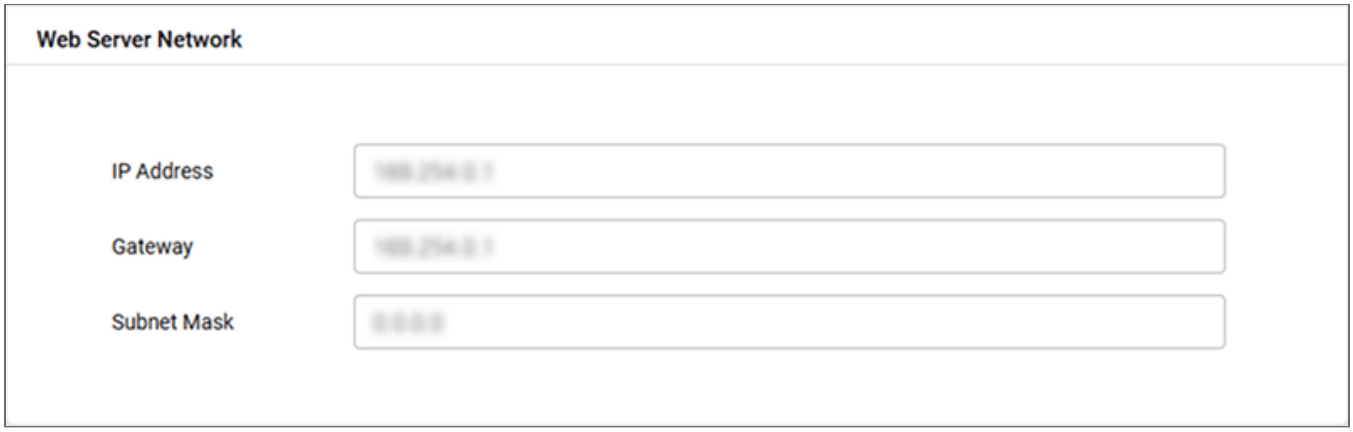


4. Click **Apply** to save the settings.

Web server network

You can change the network information of the CoreStation Setup Manager.

1. Click **SETTINGS**.
2. Edit the necessary fields.



Name	Feature description
IP Address	Edit the IP address of the CoreStation Setup Manager. - Only static IP can be used. DHCP is not supported.
Gateway	Edit the gateway of the CoreStation Setup Manager.
Subnet Mask	Edit the subnet mask of the CoreStation Setup Manager.

3. Click **Apply** to save the settings. The device will restart.

Appendices

Includes legal notices contained in the product.

Disclaimers

- Information in this web site is provided in connection with Suprema products.
- The right to use is acknowledged only for Suprema products included in the terms and conditions of use or sale for such products guaranteed by Suprema. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this web site.
- Except as expressly stated in an agreement between you and Suprema, Suprema assumes no liability whatsoever, and Suprema disclaims all warranties, express or implied including, without limitation, relating to fitness for a particular purpose, merchantability, or noninfringement.
- All warranties are VOID if Suprema products have been: 1) improperly installed or where the serial numbers, warranty date or quality assurance decals on the hardware are altered or removed; 2) used in a manner other than as authorized by Suprema; 3) modified, altered or repaired by a party other than Suprema or a party authorized by Suprema; or 4) operated or maintained in unsuitable environmental conditions.
- Suprema products are not intended for use in medical, lifesaving, life-sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should you purchase or use Suprema products for any such unintended or unauthorized application, you shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.
- Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design.
- Personal information, in the form of authentication messages and other relative information, may be stored within Suprema products during usage. Suprema does not take responsibility for any information, including personal information, stored within Suprema’s products that are not within Suprema’s direct control or as stated by the relevant terms and conditions. When any stored information, including personal information, is used, it is the responsibility of the product users to comply with national legislation (such as GDPR) and to ensure proper handling and processing.
- You must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.
- Except as expressly set forth herein, to the maximum extent permitted by law, the Suprema products are sold "as is".
- Contact your local Suprema sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright Notice

The copyright for this website is owned by Suprema. Rights to other product names, trademarks, and registered trademarks belong to the respective individuals or organizations that own them.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.