

CoreStation Setup Manager

USER GUIDE

Version 1.01
English
EN 102.00.CSM

CONTENTS

Getting Started 2

Introduction 2

Minimum Requirements 2

Initial Setup 3

Configuration 5

Slave Device Search and Registration 5

Rebooting the Device 6

Editing Device Settings and Informaion 7

Information 7

Network 8

Authentication 9

Advanced 10

Monitoring 11

Input Port Status 11

Output Port Status 12

Wiegand Port Status 12

Settings 13

Editing Admin Accounts 13

Web Server Network 14

Appendices 15

Disclaimers 15

Copyright Notice 15

Getting Started

Introduction

The CoreStation Setup Manager is a web server that allows users to view or manage the network settings of CoreStation and monitor the status of slave devices, input and output ports, and Wiegand ports. The CoreStation Setup Manager allows users to check the status of the network and wiring in the field without going to the location of the BioStar 2 server when configuring the access control system using CoreStation.

CoreStation Setup Manager allows the users to:

- Configure the IP address.
- View CoreStation informations.
- Administrator Settings.
- Check the connection status of the slave devices.
- Monitor the status of Input, Output, and Wiegand ports.
- Restore all settings or settings without network.
- Factory Default

Minimum Requirements

Check the compatible devices and firmware versions.

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



- CoreStation Setup Manager is supported on CoreStation firmware version 1.3.1 or later and CoreStation 20 firmware version 1.0.0 or later. If you are using an older firmware version, access BioStar 2 to upgrade the firmware to the latest version.
- For more information on how to install and connect the CoreStation, refer to the installation guide. To download the installation guide, visit the Suprema Download Center (<https://download.supremainc.com>).
- For any inquiries or technical support concerning CoreStation and CoreStation Setup Manager, please contact the Suprema Technical Support Team (<http://support.supremainc.com>).

Initial Setup

The CoreStation Setup Manager provides web-based services. Therefore, when configuring the centralized access control system using the CoreStation, you can access the CoreStation Setup Manager through a web browser and check the connection status of the CoreStation from anywhere after the wiring is completed.

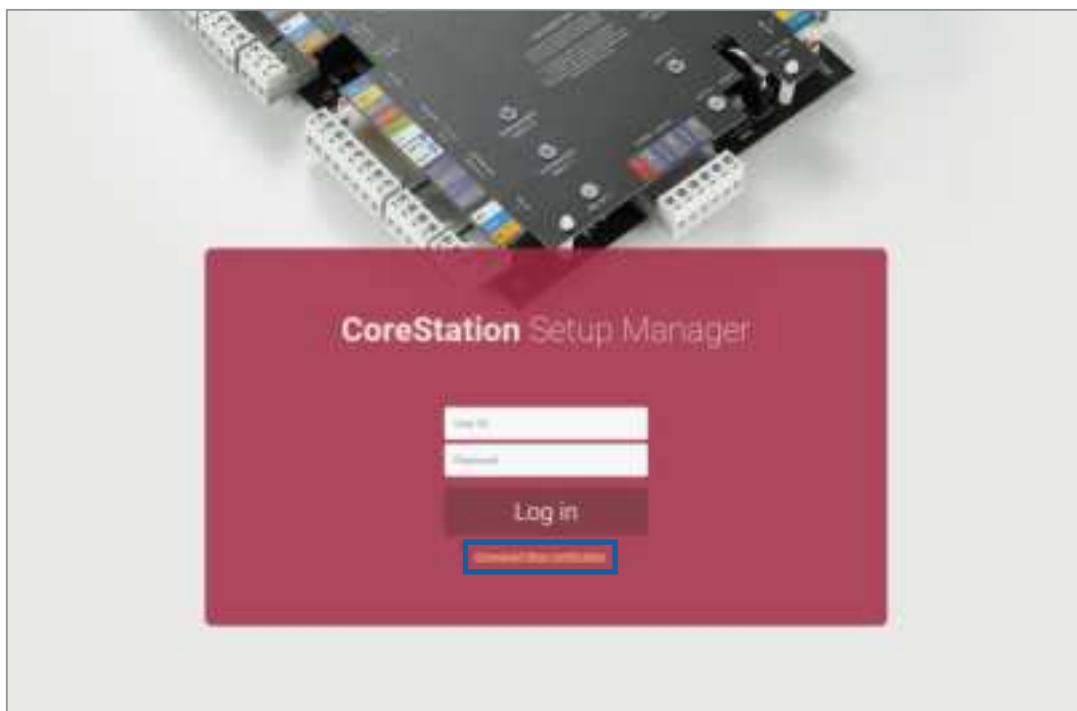
If you are using the CoreStation Setup Manager for the first time, connect the CoreStation and proceed with the initial setup.

- 1 Complete the CoreStation wiring.
- 2 Run your web browser.



We recommend that you use Google Chrome 75 or later.

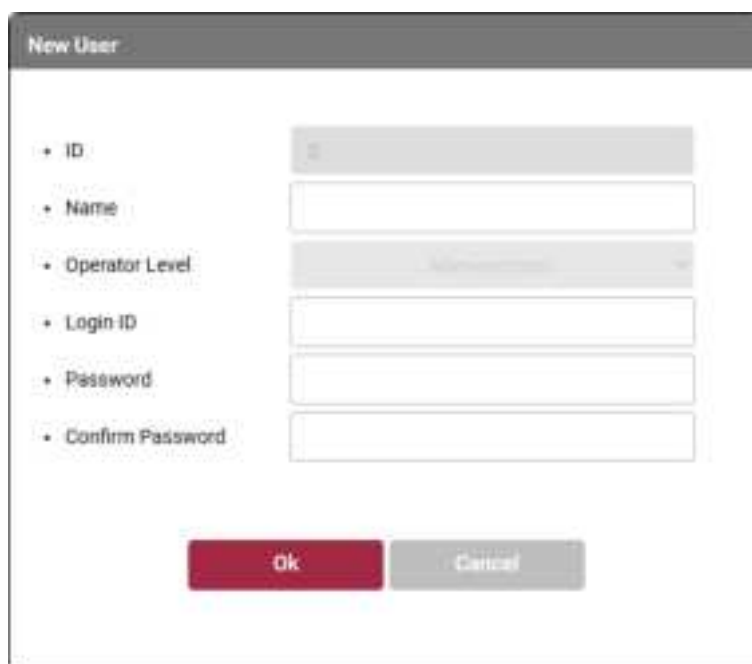
- 3 Enter the default IP address (<https://169.254.0.1:3001>) in the address input field of the web browser.
- 4 Click **Download https certification** on the login screen. The first time you log in to the CoreStation Setup Manager, you must install the certificate to use HTTPS properly.



- 5 Run `cs_client.crt` file.
- 6 When the **Open File - Security Warning** window appears, click **Open**.
- 7 Click **Install Certificate...** in the **Certificate details** window. The **Certificate Import Wizard** will appear.
- 8 Click **Next** to continue.
- 9 Select the certificate store and click **Next** → **Finish** → **OK**.

10 Enter your User ID and Password. The user ID and password are both 'admin' when first connected.

11 To register an administrator account, set each item and click **OK**.



The 'New User' dialog box contains the following fields and controls:

- ID:** A text field with the value '0' pre-filled.
- Name:** An empty text field.
- Operator Level:** A dropdown menu with 'Administrator' selected.
- Login ID:** An empty text field.
- Password:** An empty text field.
- Confirm Password:** An empty text field.
- Buttons:** 'Ok' (highlighted in red) and 'Cancel'.

Item	Description
ID	The ID is automatically set to '0' and cannot be changed.
Name	Enter the administrator's name. <ul style="list-style-type: none"> Up to 48 characters may be entered for a name.
Operator Level	The Operator Level is automatically set to 'Administrator' and cannot be changed.
Login ID	Enter the login ID. <ul style="list-style-type: none"> Up to 32 characters may be entered for a login ID.
Password	Enter the login password. <ul style="list-style-type: none"> A combination of characters, numbers, and symbols from 7 to 32 characters can be entered for the password.
Confirm Password	Enter the login password again to confirm.

12 The login screen will be displayed. Log in with the registered administrator account.



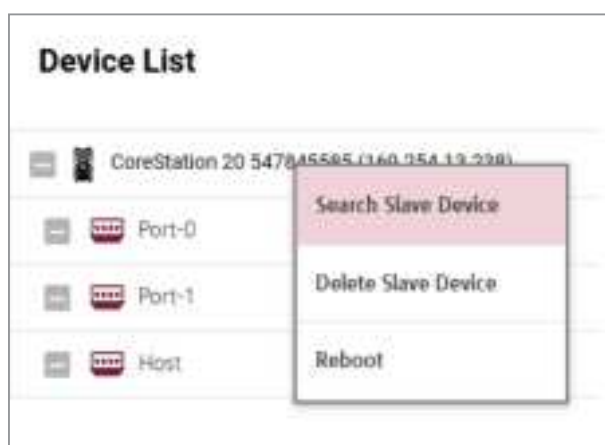
- The administrator account can only be set when first accessing the CoreStation Setup Manager, and only one user can be designated. Once registered, the default user ID and login password used during the initial access can no longer be used. Additionally, the administrator account can view and edit all settings, including performing a Factory Default.
- In CoreStation Setup Manager v1.01, the Level 1 administrator rank has been renamed to Administrator, and Level 2 ~ Level 3 administrator accounts are no longer supported.

Configuration

Slave Device Search and Registration

You can easily expand your access control system network by adding slave devices to the CoreStation. CoreStation (master device) and slave devices can be connected together via RS-485. Besides regular devices, additional devices such as Secure I/O can be connected.

- 1 Click **CONFIGURE**.
- 2 Right-click CoreStation in the Device List and click **Search Slave Device**. The list of slave devices connected to the CoreStation is shown.



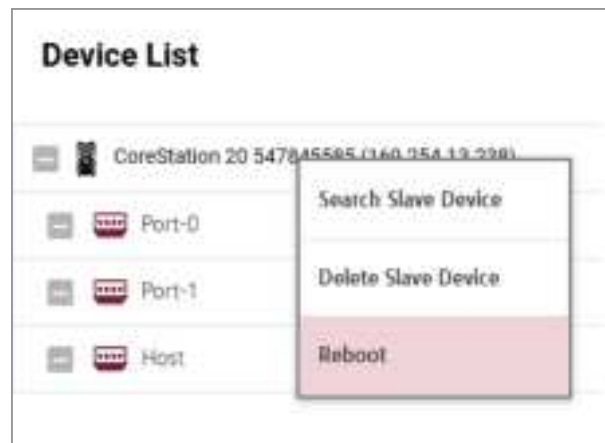
- 3 Select the device to register as a slave and click **Add**. Otherwise, you can add slave devices by selecting each port.



Rebooting the Device

You can reboot the device.

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



Editing Device Settings and Informaion

You can edit detailed settings of CoreStation.

- 1 Click **CONFIGURE**.
- 2 Edit the necessary items.

Information

The screenshot shows the 'Information' configuration page. It contains the following fields and buttons:

- Name:** A text input field.
- Device ID:** A text input field.
- Service Type:** A dropdown menu.
- Firmware Version:** A text input field and a **Firmware Upgrade** button.
- Kernel Version:** A text input field.
- Hardware Version:** A text input field.
- Factory Default:** A button.
- Restore to Default:** Two buttons: **ALL** and **without Network**.
- Locked:** A button labeled **unlock**.
- Time Zone:** A dropdown menu showing **UTC**.
- Display Date:** Two buttons: **Get Time** and **Set Time**.

Item	Description
Name	View the device name.
Device ID	View the device ID.
Device Type	View the device type.
Firmware Version	Click Firmware Upgrade , then select the firmware file to upgrade and install the new firmware version.
Kernel Version	View the kernel version.
Hardware Version	View the hardware version.
Factory Default	Delete all the information saved in the device and the root certificate and restore default settings.
Restore to Default	Reset the settings of the device. <ul style="list-style-type: none"> ALL: Reset all settings. without Network: Reset all settings excluding the network settings.
Locked	Unlock button will be available when the device is disabled via Trigger & Action.
Time Zone	Set the time zone of device.
Display Date	Set the date and time manually. <ul style="list-style-type: none"> Get Time: Click the button to fetch the time set in the device. Set Time: Click the button to apply the time in CoreStation Setup Manager to the device.



Factory Default menu can be used when the root certificate is saved in the device. When a Factory Default is performed, the administrator account is deleted.

Network

Network

TCP / IP

☒ Use DHCP

IP Address:

Gateway:

DNS Server Address:

Subnet Mask:

Device Port:

Server

☐ Device to Server Connection

Server Address:

Server Port:

Serial

RS485:

Baud Rate:

Port	Baud Rate
0	115200
1	115200
Host	115200

Item	Description
Use DHCP	Select this option to allow the device to use a dynamic IP address. If this option is selected, network settings cannot be entered.
IP Address	View the IP address of the device.
Gateway	View the gateway of the device.
DNS Server Address	Set the DSN server address.
Subnet Mask	View the subnet mask of the device.
Device Port	Enter a port to be used by the device.
Device to Server Connection	Selecting this option allows entering BioStar 2 server information to connect the device to the server.
Server Address	Enter the IP address or domain name of the BioStar 2 server.
Server Port	Enter the port number of the BioStar 2 server.
RS485	You can only use Master.
Baud Rate	Set a baud rate of the RS-485 connection.

Authentication

Authentication

1:N Security Level

1:N Fast Mode

Template Format

1:N

Auto

1:N

Item	Description
1:N Security Level	You can set a security level to use for fingerprint. The higher the security level is set, the false rejection rate (FRR) gets higher, but the false acceptance rate (FAR) gets lower.
1:N Fast Mode	You can set the fingerprint authentication speed. Select Auto to have the authentication speed configured according to the total amount of fingerprint templates registered within the device.
Template Format	You can view the fingerprint template format.



Biometric authentication is only supported on CoreStation.

Advanced

Advanced

AC Fail

☐ Use Port

Switch type

☒ NFO

Tamper

☐ Use Port

Switch type

☒ NFO

Fire

☐ Use Port

Switch type

☒ NFO

Supervised Input

Configuration

Index	Supervised	Supervised Input register	
0	<input type="checkbox"/>	1E	▼
1	<input type="checkbox"/>	1E	▼
2	<input type="checkbox"/>	1E	▼
3	<input type="checkbox"/>	1E	▼
4	<input type="checkbox"/>	1E	▼
5	<input type="checkbox"/>	1E	▼

Secure Tamper

☐

Item	Description
AC Fail	You can set the AUX port that monitors the power input signal.
Tamper	You can set the AUX port where the tamper is connected.
Fire	You can set the AUX port that monitors the fire detection signal.
Configuration	You can set the supervised input port of CoreStation to be used as TTL input port and set a resistance value to be used for supervised input. 1 kΩ, 2.2 kΩ, 4.7 kΩ and 10 kΩ can be set for the resistance value.
Secure Tamper	You can set the secure tamper to delete the entire user information, the entire log, and the security key stored on the device when a tamper event occurs on the device.

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

Monitoring

After completing the wiring, you can check the status of the Input and Output in the CoreStation in real time. You can also view the card ID read by the connected Wiegand reader.

Input Port Status

The connection status of the Input, Aux Input ports is displayed. After completing the wiring, you can check the connection status of the Input port directly in the field.

Input Status	
Port	Connect Status
Input Port 0	Off
Input Port 1	Off
Input Port 2	Off
Input Port 3	Off
Input Port 4	Off
Input Port 5	Off
Aux Input Port 0	Off
Aux Input Port 1	Off
Aux Input Port 2	Off



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

Output Port Status

The connection status of the Relay, Output ports is displayed. You can also select the item and click the switch to control the relay and output ports.

Output Status		Connect Status Control <input type="checkbox"/>
<input checked="" type="checkbox"/>	Port	Connect Status
<input checked="" type="checkbox"/>	Relay 0	
<input checked="" type="checkbox"/>	Relay 1	
<input checked="" type="checkbox"/>	Relay 2	
<input checked="" type="checkbox"/>	Relay 3	
<input checked="" type="checkbox"/>	Output Port 0	
<input checked="" type="checkbox"/>	Output Port 1	
<input checked="" type="checkbox"/>	Output Port 2	
<input checked="" type="checkbox"/>	Output Port 3	
<input checked="" type="checkbox"/>	Output Port 4	
<input checked="" type="checkbox"/>	Output Port 5	



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

Wiegand Port Status

When you scan a card on the Wiegand reader connected to a Wiegand port, the card ID is displayed in the **Status** column.

Port	Status
Wiegand Port 0	
Wiegand Port 1	




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

Settings

Editing Admin Accounts

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

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

Admin Accounts			
Admin Account			
ID	Level	User Name	
0	Administrator	admin	 Edit

- 3 Edit the necessary items by referring to the **Initial Setup**, and click **OK**.

Edit User

• ID

• Name

• Operator Level

• Login ID

• Password

• Confirm Password

Ok

Cancel

- 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 information.

A screenshot of the 'Web Server Network' configuration window. It has a title bar 'Web Server Network' and a close button. Below the title bar, there are three labels: 'IP Address', 'Gateway', and 'Subnet Mask'. Each label is followed by a text input field. The 'IP Address' field contains '192.168.1.1', the 'Gateway' field contains '192.168.1.1', and the 'Subnet Mask' field contains '255.255.255.0'.

Item	Description
IP Address	Edit the IP address of the CoreStation Setup Manager. <ul style="list-style-type: none">• Only static IP is available. 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 be restarted.

Appendices

Disclaimers

- Information in this document 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 document.
- 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 of this document is vested in Suprema. The rights of other product names, trademarks and registered trademarks are vested in each individual or organization that owns such rights.



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>

© 2025 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.