

CoreStation Setup Manager

ユーザーガイド

バージョン 1.00
日本語

JA 102.00.CS40 V1.00A

目次

はじめに	3
デバイス初期設定.....	4
デバイス構成.....	6
スレーブデバイスの検出と登録.....	6
デバイスの再起動	7
デバイス設定と情報の変更.....	8
情報.....	8
ネットワーク.....	10
認証	11
ハイレベル設定	12
モニタリング	13
入力ポートの状態	13
出力ポートの状態	13
Wiegandポートの状態	14
デバイス設定.....	15
管理者アカウントの設定.....	15
管理者アカウントの追加.....	15
管理者アカウントの編集.....	17
管理者アカウントの削除.....	17
Webサーバーネットワーク	18
付録	19
免責事項	19
著作権の公示	19

はじめに

CoreStation Setup Managerは、CoreStationのネットワーク設定を管理したり、スレーブ装置、入力および出力ポート、Wiegandポートの接続状態を確認できるWebサーバーです。CoreStation Setup Managerを使用すると、CoreStationを利用したアクセスコントロールシステムを構成する際にBioStar 2サーバーの場所へ移動することなく、現場でのネットワークや配線の状態を確認することができます。

ヒント

- CoreStation Setup ManagerはCoreStationファームウェア1.3.1以降のバージョンでサポートされます。1.3.1より前のバージョンのファームウェアを使用する場合、BioStar 2に接続し、ファームウェアを最新バージョンにアップグレードしてください。
- CoreStationを接続してインストールする方法の詳細については、インストールガイドを参照してください。インストールガイドはSupremaホームページ (<https://www.supremainc.com>) からダウンロードできます。
- CoreStationとCoreStation Setup Managerについてのお問い合わせや技術サポートは、Suprema技術サポートチーム (<http://support.supremainc.com>) にお問い合わせください。

CoreStation Setup Managerでは、次のような機能を使用することができます。

- ・ IPアドレス設定
- ・ CoreStationデバイス情報の確認
- ・ 管理者レベルの設定
- ・ スレーブデバイス接続状態の確認
- ・ 入力と出力、Wiegandポートの状態をモニタリング
- ・ デバイスの初期化、ネットワーク設定を除く設定の初期化
- ・ 工場出荷時の設定に初期化

デバイス初期設定

CoreStation Setup Managerは、Webベースのサービスを提供しています。したがって、CoreStationを利用して中央集中型アクセスコントロールシステムを構築する際、配線を完了した後、どこからでも、Webブラウザを介してCoreStation Setup Managerに接続しCoreStationの接続状態を確認することができます。

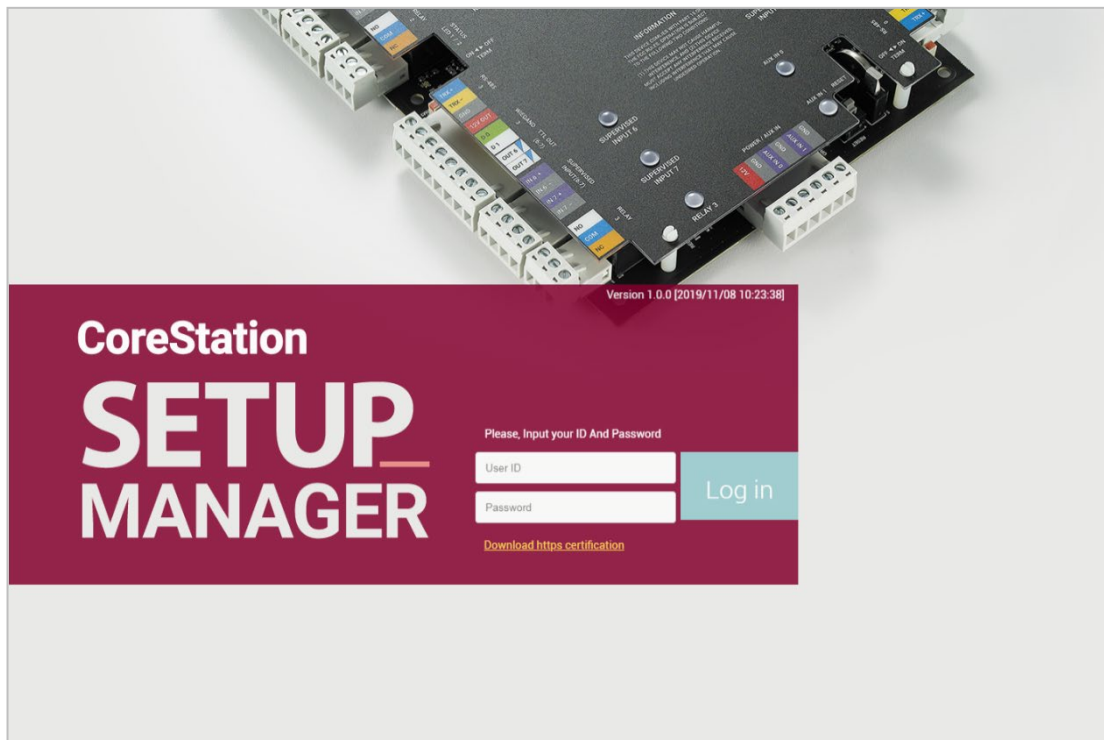
CoreStation Setup Managerを初めて使用する場合は、CoreStationを接続して、初期設定を行います。

- 1 CoreStationにケーブル接続を完了してください。
- 2 Webブラウザを起動してください。

ヒント

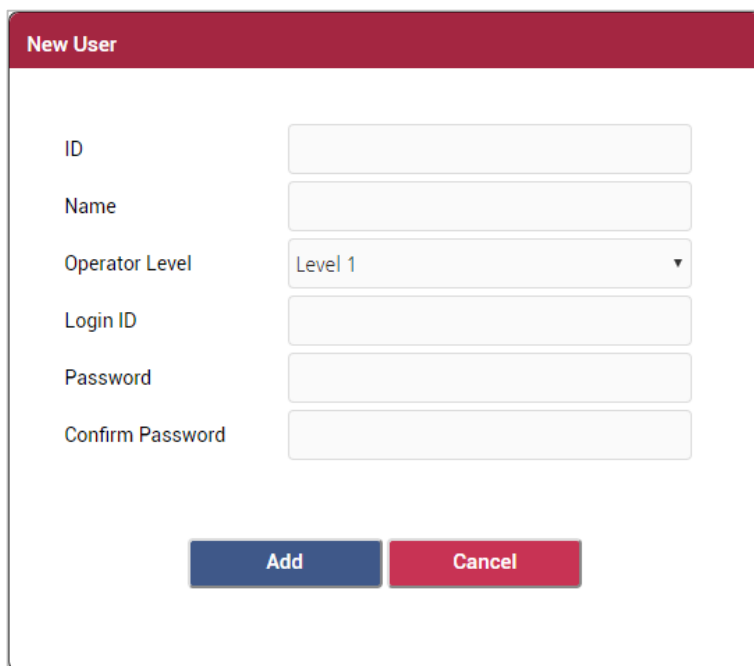
- Chrome75バージョン以上のWebブラウザを使用してください。

- 3 Webブラウザのアドレス入力フィールドに、基本IPアドレス (<https://169.254.0.1:3001>) を入力してください。
- 4 ログイン画面で、[Download https certification]をクリックしてください。CoreStation Setup Managerに初めて接続する場合、HTTPSを正しく使用するために認証書をインストールする必要があります。



- 5 cs40_client.crtファイルを実行してください。
- 6 Open File-Security Warningウィンドウが表示されたら[Open]をクリックしてください。

- 7 **Certificate details**ウィンドウで[**Install Certificate...**]をクリックしてください。 **Certificate Import Wizard** が起動します。
- 8 続けるには、 [**Next**]をクリックしてください。
- 9 認証書の保存場所を選択してから、 [**Next**] > [**Finish**] > [**OK**]をクリックしてください。
- 10 ユーザーIDとログインパスワードを入力してください。最初の接続時のユーザーIDとログインパスワードは、すべて「**admin**」です。
- 11 **管理者アカウントの追加**を参考にしてLevel 1の管理者を設定した後、 [**Add**]をクリックします。



The screenshot shows a dialog box titled "New User". It has a red header bar. Below the header, there are several input fields: "ID", "Name", "Operator Level" (a dropdown menu currently showing "Level 1"), "Login ID", "Password", and "Confirm Password". At the bottom of the dialog, there are two buttons: a blue "Add" button and a red "Cancel" button.

ヒント

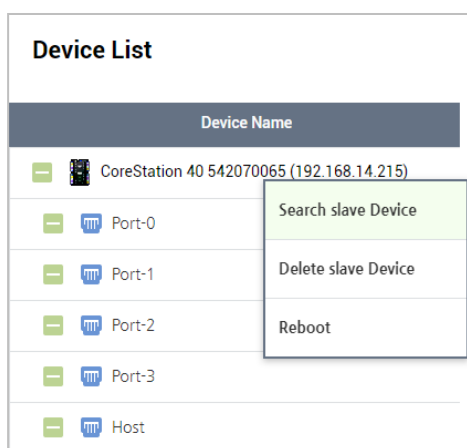
- Level 1の管理者を追加した後は、最初の接続時に入力した基本ユーザーIDとログインパスワードは使用できません。

デバイス構成

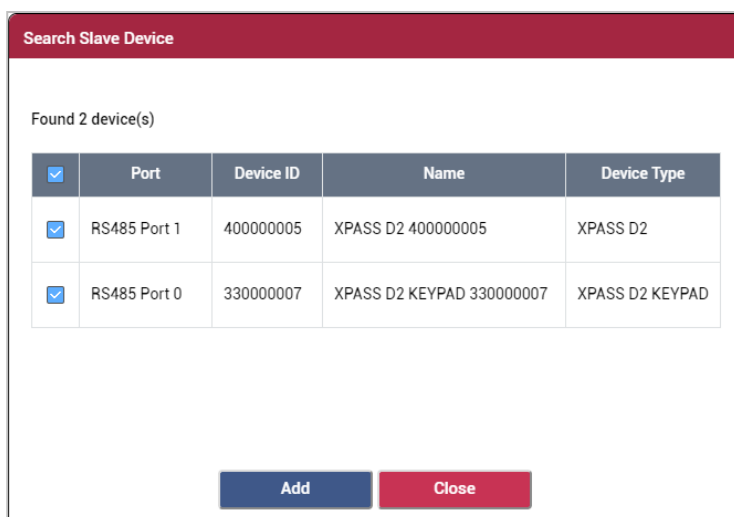
スレーブデバイスの検出と登録

CoreStationにスレーブデバイスを追加し、簡単にアクセスコントロールシステムのネットワークを拡張することができます。CoreStation（マスターデバイス）とスレーブデバイスは、RS-485に接続することができ、デバイスだけでなく、Secure I/Oなどの付加デバイスも接続して使用することができます。

- 1 [CONFIGURE]をクリックしてください。
- 2 Device ListのCoreStationをマウスの右ボタンでクリックした後、[Search slave Device]をクリックしてください。CoreStationに接続されたスレーブデバイスの一覧が表示されます。



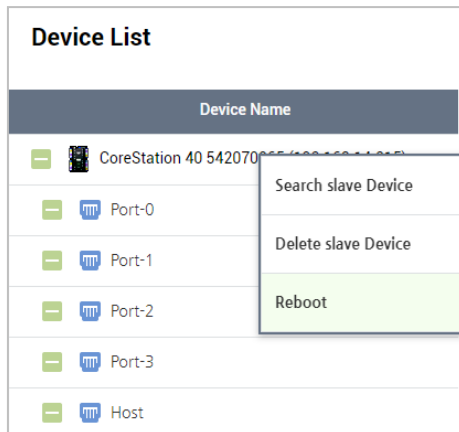
- 3 スレーブに登録するデバイスを選択した後、[Add]をクリックします。または個別のポートを選択して、スレーブデバイスを追加することもできます。



デバイスの再起動

デバイスを再起動することができます。

- 1 [CONFIGURE]をクリックしてください。
- 2 Device ListのCoreStationをマウスの右ボタンでクリックした後、[Reboot]をクリックしてください。



デバイス設定と情報の変更

CoreStationの詳細情報を設定することができます。

- 1 [CONFIGURE]をクリックしてください。
- 2 各項目を設定してください。

情報

No.	Item	Description
1	Name	デバイス名を確認することができます。
2	Device ID	デバイスIDを確認することができます。
3	Device Type	デバイスの種類を確認することができます。
4	Firmware Version	[Firmware Upgrade]をクリックすると、新しいファームウェアのバージョンをインストールすることができます。
5	Kernel Version	カーネルのバージョンを確認することができます。
6	Hardware Version	ハードウェアのバージョンを確認することができます。

7	Factory Default	デバイスに保存されたすべての情報とルート認証書を削除し、設定を初期化することができます。
8	Restore to Default	<p>デバイスの設定を初期化することができます。</p> <ul style="list-style-type: none"> • [ALL]：すべての設定を初期化します。 • [without Network]：ネットワーク設定を除くすべての設定を初期化します。
9	Locked	トリガ & 動作によりデバイスがロックされた場合、 [Unlock] ボタンを使用することができます。
10	Time Zone	デバイスのタイムゾーンを設定することができます。
11	Display Date	<p>日付と時刻を手動で設定することができます。</p> <ul style="list-style-type: none"> • [Get time]：デバイスに設定された時間を読み込む際に、クリックしてください。 • [Set time]：CoreStation Setup Managerに設定された時間をデバイスに適用する際に、クリックしてください。

ヒント

- **[Factory Default]**、**[All]** (Restore to Default)、**[Unlock]**はLevel 1の管理者アカウントでログインしている場合にのみ有効になります。

ネットワーク

The screenshot shows a 'Network' configuration window. It is divided into two main sections: 'TCP / IP' and 'Serial'.
 In the 'TCP / IP' section:
 - 'Use DHCP' is checked (indicated by '1').
 - 'IP Address' is set to 192.168.14.215 (indicated by '2').
 - 'Gateway' is set to 192.168.14.1 (indicated by '3').
 - 'DNS Server Address' is empty (indicated by '4').
 - 'Subnet Mask' is set to 255.255.255.0 (indicated by '5').
 - 'Device Port' is set to 51211 (indicated by '6').
 In the 'Serial' section:
 - 'RS485' is set to 'Master' (indicated by '7').
 - 'Baud Rate' is a table with two columns: 'Port' and 'Baud Rate'. The table has five rows: 0, 1, 2, 3, and Host, all with a Baud Rate of 115200 (indicated by '8').

No.	Item	Description
1	Use DHCP	デバイスが流動IP アドレスを使用するように設定する際に、選択してください。この項目を選択すると固定IPアドレスを割り当てることはできません。
2	IP Address	デバイスのIPアドレスを確認することができます。
3	Gateway	デバイスのゲートウェイを確認することができます。
4	DNS Server Address	装置のDSNサーバーアドレスを確認することができます。
5	Subnet Mask	デバイスのサブネットマスクを確認することができます。
6	Device Port	デバイスが使用するポートを入力してください。
7	RS485	[Master]モードのみ使用することができます。
8	Baud Rate	各RS-485ポートの転送速度を設定することができます。

認証

The screenshot shows the 'Authentication' settings page. Under the 'Fingerprint' section, there are three dropdown menus:

- 1: 1:N Security Level (set to Normal)
- 2: 1:N Fast Mode (set to Auto)
- 3: Template Format (set to Suprema)

No.	Item	Description
1	1:N Security Level	指紋を認証する際に使用するセキュリティレベルを設定することができます。セキュリティレベルが高いほど、本人拒否率（FRR）が高くなりますが、他人受諾率（FAR）は低くなります。
2	1:N Fast Mode	指紋認証の速度を設定することができます。[Auto]を選択すると、デバイスに登録された全指紋テンプレートの数に応じて、認証速度が設定されます。
3	Template Format	設定された指紋テンプレート形式を確認することができます。

ハイレベル設定

The screenshot shows the 'Advanced' configuration page with the following settings:

- 1 Tamper:** Set to 'None' (dropdown), Switch type checked 'N/O'.
- 2 AC Fail:** Set to 'None' (dropdown), Switch type checked 'N/O'.
- 3 Supervised Input Configuration:** A table with 8 rows (Index 0-7). Each row has a 'Supervised' checkbox (unchecked) and a 'Supervised Input register' dropdown (set to '2.2K').
- 4 Secure Tamper:** A checkbox (unchecked).

No.	Item	Description
1	Tamper	タンパーが接続されたAUXポートを設定することができます。
2	AC Fail	電源入力信号をモニタリングするAUXポートを設定することができます。
3	Configuration	CoreStationのSupervised InputポートをTTL Inputポートとして使用するよう設定することができ、Supervised Inputに使用する抵抗値を設定することができます。抵抗値は1kΩ、2.2kΩ、4.7kΩ、10kΩを設定することができます。
4	Secure Tamper	デバイスからタンパーイベントが発生した場合、デバイスに保存された全てのユーザー情報、全てのログ、セキュリティキーが削除されるように設定することができます。

3 設定を保存するには、[Apply]をクリックしてください。

モニタリング

配線が完了した後、CoreStationの入力および出力の状態をリアルタイムで確認することができます。また、接続されたWiegandリーダーでスキャンしたカードIDを確認することもできます。

入力ポートの状態

入力0～7、Aux入力0～1ポートの接続状態が表示されます。配線が完了した後、現場ですぐに入力ポートの接続状態を確認することができます。

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
Input Port 6	Off
Input Port 7	Off
Aux Input Port 0	Off
Aux Input Port 1	Off

出力ポートの状態

リレー0～3、出力0～7ポートの接続状態が表示されます。目的の項目を選択して、スイッチをクリックし、リレーと出力ポートを制御することもできます。

Output Status <input type="checkbox"/>	
<input checked="" type="checkbox"/> Port	Connect Status
<input checked="" type="checkbox"/> Relay 0	Off
<input checked="" type="checkbox"/> Relay 1	Off
<input checked="" type="checkbox"/> Relay 2	Off
<input checked="" type="checkbox"/> Relay 3	Off
<input checked="" type="checkbox"/> Output Port 0	Off
<input checked="" type="checkbox"/> Output Port 1	Off
<input checked="" type="checkbox"/> Output Port 2	Off
<input checked="" type="checkbox"/> Output Port 3	Off
<input checked="" type="checkbox"/> Output Port 4	Off
<input checked="" type="checkbox"/> Output Port 5	Off
<input checked="" type="checkbox"/> Output Port 6	Off
<input checked="" type="checkbox"/> Output Port 7	Off

Wiegandポートの状態

Wiegand0～3ポートに接続されたWiegandリーダーにカードをスキャンすると、そのカードIDが[Status]列に表示されます。

Port	Status
Wiegand Port 0	
Wiegand Port 1	
Wiegand Port 2	
Wiegand Port 3	

デバイス設定

管理者アカウントの設定

管理者アカウントの追加

CoreStation Setup Managerの管理者を指定し、管理することができます。

ヒント

- 管理者は、最大10人まで指定して管理することができます。


- 1 [SETTINGS]をクリックしてください。
- 2 [+ New User]をクリックしてください。
- 3 各項目を設定してください。

No.	Item	Description
1	ID	<p>管理者に付与する固有IDを入力してください。</p> <ul style="list-style-type: none"> • IDは、0～9の数字で入力することができます。
2	Name	<p>管理者の名前を入力してください。</p> <ul style="list-style-type: none"> • 名前は最大48文字まで入力することができます。

3	Operator Level	<p>管理者レベルを設定してください。</p> <ul style="list-style-type: none"> • 各管理者のレベルは下記のような権限を持ちます。 <ul style="list-style-type: none"> - Level 1：工場出荷時設定への初期化を含めて、全ての設定を確認したり、編集することができます。また、すべてのレベルの管理者情報を変更することができます、Level 2、3管理者アカウントを削除することもできます。 - Level 2：Factory Default、All (Restore to Default)、Unlockを除く全ての設定を確認したり、編集することができ、自分のアカウント情報を変更することができます。 - Level 3：設定を確認することができ、変更や管理することはできません。 • Level 1の管理者は、CoreStation Setup Managerに最初に接続する際にのみ設定することができます、1人のユーザーだけを指定することができます。 • Level 1の管理者は削除できません。
4	Login ID	<p>ログインIDを入力してください。</p> <ul style="list-style-type: none"> • ログインIDは、最大32文字まで入力することができます。
5	Password	<p>ログインパスワードを入力してください。</p> <ul style="list-style-type: none"> • ログインパスワードは、7～32文字の英数字と記号の組み合わせで入力してください。
6	Confirm Password	<p>確認のため、ログインパスワードを再入力してください。</p>

4 設定を保存するには、[Apply]をクリックしてください。

管理者アカウントの編集

- 1 [SETTINGS]をクリックしてください。
- 2 編集する管理者で **Edit**をクリックしてください。
- 3 **管理者アカウントの追加**を参考にして、各項目を編集した後、**[OK]**をクリックします。
- 4 設定を保存するには、**[Apply]**をクリックしてください。

管理者アカウントの削除

- 1 [SETTINGS]をクリックしてください。
- 2 削除する管理者で **Del**をクリックしてください。
- 3 **[Delete]**をクリックしてください。
- 4 設定を保存するには、**[Apply]**をクリックしてください。

Webサーバーネットワーク

CoreStation Setup Managerのネットワーク情報を変更することができます。

- 1 [SETTINGS]をクリックしてください。
- 2 各項目を設定してください。

The screenshot shows a configuration window titled "Web Server Network". It contains three input fields with the following values:

- 1 IP Address: 169.254.0.1
- 2 Gateway: 169.254.0.1
- 3 Subnet Mask: 0.0.0.0

No.	Item	Description
1	IP Address	CoreStation Setup ManagerのIP アドレスを編集してください。 <ul style="list-style-type: none"> 固定IPのみを使用することができます。DHCPはサポートされていません。
2	Gateway	CoreStation Setup Managerのゲートウェイを編集してください。
3	Subnet Mask	CoreStation Setup Managerのサブネットマスクを編集してください。

- 3 設定を保存するには、[Apply]をクリックしてください。デバイスが再起動されます。

付録

免責事項

- ・ この説明書にある情報はSuprema製品に関連して提供するものです。
- ・ Supremaが保証する販売合意事項と条件に含まれている製品に限り、使用する権利が認められます。この説明書で扱っているもの以外の知的財産権のライセンス権利は認められていません。
- ・ Supremaは、Suprema製品の販売や使用に関連して、特定の目的のための製品の適合性や商品性、そして特許、著作権、その他の知的財産権の侵害については、いかなる保証も責任を負いません。
- ・ 医療、人命救助、生命維持に関連する状況や、製品の誤作動によって人がケガをしたり命を失ったりする可能性のある状況では、Supremaの製品を使用しないでください。もし購入者が前例に挙げた状況で製品を使用している途中で、事故が発生した場合、たとえ製品の設計や製造の過程で不足している点が発見され、これを重要な過失であると主張しても、Supremaの職員、子会社、支店、提携会社、配布会社は責任を負わず、弁護士を選任費を含む、これと関連した全ての直接・間接的な費用や支出についても返済しません。
- ・ Supremaは、製品の安全性、機能、デザインを改良するために、適切な通知なしに、いつでも製品の規格と仕様を変更することもできます。設計者は、「実装される予定」や「定義されていない」と表示された機能や説明は、常に変動することがあることを念頭に置く必要があります。Supremaは近い将来、これらのことを実装したり、定義するというものであり、互換性の問題を含めて、これにより発生する可能性のある、いかなる問題についても責任を負いません。
- ・ 製品を注文する前に、最新の規格書を手に入れたい場合は、Suprema、Supremaの販売代理店、地域の配布会社にお問い合わせください。

著作権の公示

この文書の著作権はSupremaにあります。他の製品名、商標、登録された商標についての権利は、それぞれそれを所有した個人や団体にあります。

suprema
BIOMETRICS & SECURITY

シュプリマ株式会社

〒105-0004 東京都港区新橋4-21-3新橋東急ビル3階 オフィス#337

電話: 03-6895-7527 | Eメール: sales_jp@supremainc.com

©2019 Suprema, Inc. 本書に記載されている Suprema および Suprema 社の製品名および番号は、Suprema, Inc. の登録商標です。Suprema 社以外のすべてのブランドおよび製品名は、それぞれの企業の商標または登録商標です。製品の外観、ビルドステータスおよび/または仕様は、予告なく変更されることがあります。