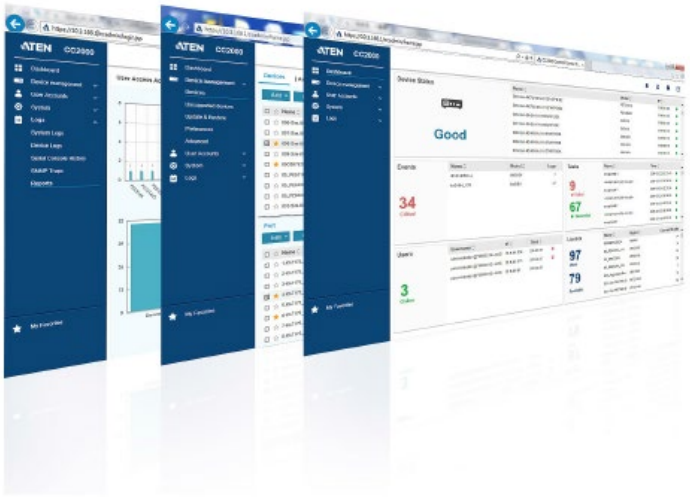
CC2000 4.0

日本語版ユーザーマニュアル



本ドキュメントについて

本書は ATEN ジャパン株式会社において、CC2000 取り扱いの便宜を図るため、英語版ユーザーマニュアルをローカライズしたドキュメントです。

製品情報、仕様はソフトウェア・ハードウェアを含め、予告なく改変されることがあり、本日本語版ユーザーマニュアルの内容は、必ずしも最新の内容でない場合があります。また製品の不要輻射仕様、各種安全規格、含有物質についての表示も便宜的に翻訳して記載していますが、本書はその内容について保証するものではありません。

製品をお使いになるときは、英語版ユーザーマニュアルにも目を通し、その取扱方法に従い、正しく運用を行ってください。詳細な製品仕様については英語版ユーザーマニュアルの他、製品をお買い上げになった販売店または弊社テクニカルサポート窓口までお問い合わせください。

ATEN ジャパン株式会社
技術部
TEL :03-5615-5811
MAIL :support@atenjapan.jp

2023 年 9 月 8 日

ユーザーの皆様へ

本マニュアルに記載された全ての情報、ドキュメンテーション、および製品仕様は、製造元である ATEN International により、予告なく改変されることがあります。製造元 ATEN International は、製品および本ドキュメントに関して、品質・機能・商品性および特定の目的に対する適合性について、法定上の、明示的または黙示的であるかを問わず、いかなる保証もいたしません。

弊社製品は一般的なコンピューターのメインフレームおよびインターフェースの操作・運用・管理を目的として設計・製造されております。高度な動作信頼性と安全性が求められる用途、例えば軍事使用、大規模輸送システムや交通インフラの制御、原子力発電所、セキュリティーシステム、放送システム、医療システムなどにおける可用性への要求を必ずしも満たすものではございません。

キーボード、マウス、モニター、コンピューターなど、弊社製品に接続されるクライアントデバイスは、それぞれベンダーの独自技術によって開発・ 製造されております。そのため、これらの異なるデバイスを接続した結果、予期できない機器同士の相性問題が発生する可能性があります。 また、機器の併用により、それぞれオリジナルで持つ機能を全て発揮できない可能性があります。異なる環境・異なる機器の組み合わせにより、機能面での使用制限が必要になる可能性があります。

本製品および付属のソフトウェア、ドキュメントの使用によって発生した装置の破損・データの損失などの損害に関して、直接的・間接的・特殊な事例・付帯的または必然的であるかを問わず、弊社の損害賠償責任は本製品の代金相当額を超えないものとします。

製品をお使いになる際には、製品仕様に沿った適切な環境、特に電源仕様についてはご注意の上、正しくお使いください。

ATEN ジャパン製品保証規定

弊社の規定する標準製品保証は、定められた期間内に発生した製品の不具合に対して、全てを無条件で保証するものではありません。製品保証を受けるためには、この『製品保証規定』およびユーザーマニュアルをお読みになり、記載された使用法および使用上の各種注意をお守りください。

また製品保証期間内であっても、次に挙げる例に該当する場合は製品保証の適用外となり、有償による修理対応といたしますのでご留意ください。

◆使用上の誤りによるもの
◆ 製品ご購入後の輸送中に発生した事故などによるもの
◆ ユーザーの手による修理または故意の改造が加えられたもの
◆ 購入日の証明ができず、製品に貼付されている銘板のシリアルナンバーも確認できないもの
◆ 車両、船舶、鉄道、航空機などに搭載されたもの
◆ 火災、地震、水害、落雷、その他天変地異、公害、戦争、テロリズムなどの予期しない災害によって故障、破損したもの
◆ 日本国外で使用されたもの
◆ 日本国外で購入されたもの

【製品保証手順】

弊社の製品保証規定に従いユーザーが保証を申請する場合は、大変お手数ですが、以下の手順に従って弊社宛に連絡を行ってください。

(1)不具合の確認

製品に不具合の疑いが発見された場合は、購入した販売店または弊社サポート窓口に連絡の上、製品の状態を確認してください。 この際、不具合の確認のため動作検証のご協力をお願いすることがあります。

(2)本規定に基づく製品保証のご依頼

(1)に従い確認した結果、製品に不具合が認められた場合は、本規定に基づき製品保証対応を行います。製品保証対応のご依頼をされる場合は、RMA 申請フォームの必要項目にご記入の上、『お客様の製品購入日が証明できる書類』を用意して、購入した販売店までご連絡ください。販売店が不明な場合は、弊社までお問い合わせください。

(3)製品の発送

不具合製品の発送は宅配便などの送付状の控えが残る方法で送付してください。

【製品保証期間】

製品保証期間は通常製品/液晶ディスプレイ搭載製品で異なります。詳細は下記をご覧ください。

①通常製品	製品納品日～30 日	初期不良、新品交換※1
	31 日～3 年間	無償修理
	3 年以上	有償修理※2
②型番 CL からはじまる LCD 搭載製品のみ	製品納品日～30 日	初期不良、新品交換※1
	31 日～2 年間	無償修理
	3 年目以降	有償修理※2

※1…製品購入日から 30 日以内に確認された不具合は初期不良とし、新品交換を行います。初期不良の場合の送料は往復弊社にて負担いたします。

※2…有償修理の金額は別途製品を購入された販売店までお問い合わせください。

※ケーブル類、その他レールキットなどのアクセサリー類は初期不良の際の新品交換のみ、承ります。

※EOL (生産終了)が確定した製品については、初期不良であっても無償修理対応とさせていただきます。また EOL 製品の修理に関して、上記無償修理期間中であっても、部材調達の都合などにより修理不可になる可能性がございます。そのような場合には、機能同等品による良品交換のご対応となる可能性がございます。また、EOL 製品の型番や、修理可否、後継機種については、随時情報更新を行っておりますので、弊社ウェブページにて最新情報をご確認ください。

※製品保証期間の延長や故障時の代替品などの保証オプションについては、弊社ウェブページをご確認ください。

【補足】

・本規定は ATEN 製品に限り適用します。

・ケーブル類は初期不良対応に準じます。

・初期不良による新品交換の場合は、ATEN より発送した代替品の到着後、5 営業日以内に不具合品を弊社宛に返却してください。返却の予定期日が守られない場合は弊社から督促を行いますが、それにもかかわらず不具合品が返却されない場合は、代替機相当代金を販売代理店経由でご請求いたします。

・ラベルの汚損や剥がれなどにより製品のシリアルナンバーが確認できない場合は、全て有償修理とさせていただきます。

【免責事項】

1. 弊社製品は映像関連システムやコンピューターのメインフレームおよびインターフェースの操作・運用・管理を目的として設計・製造されております。しかし、使用環境などによってはその機能が制限されることがあります。弊社では、ご購入前に弊社製品をお試しいただける「評価機貸出サービス」を、無償でご提供しております。評価機貸出サービスに関するお問い合わせは、弊社代理店または弊社ウェブサイト（https://www.aten.com/jp/ja/）内の「お問い合わせ」フォームをご利用ください。

2. キーボード、マウス、モニター、コンピューターなど、弊社製品に接続されるクライアントデバイスは、それぞれベンダーの独自技術によって開発・製造されております。そのため、これらの異なるデバイスを接続した結果、予期できない機器同士の相性問題が発生する可能性があります。また、機器の併用により、それぞれオリジナルで持つ機能を全て発揮できない可能性があります。異なる環境・異なる機器の組み合わせにより、機能面での使用制限が必要になる可能性があります。

3. 他社製品のKVMスイッチ、キーボード・マウスコンバーター、キーボード・マウスエミュレーター、KVM エクステンダーなどとの組み合わせはサポート対象外となりますが、お客様で自己検証の上であれば、使用を制限するものではありません。

4. 製品に対しての保証は、日本国内で使用されている場合のみ対象とさせていただきます。

5. 製品やサービスについてご不明な点がある場合は、弊社技術部門までお問い合わせください。

製品についてのお問い合わせ

製品の仕様や使い方についてのお問い合わせは、下記窓口または製品をお買い上げになった販売店までご連絡ください。

購入前のお問い合わせ	ATEN ジャパン株式会社　営業部 TEL：03-5615-5810 MAIL:sales@atenjapan.jp
購入後のお問い合わせ	ATEN ジャパン株式会社　技術部 TEL　：03-5615-5811 MAIL :support@atenjapan.jp

目次

同梱品

CC2000 製品パッケージには下記のアイテムが同梱されています。(※ソフトウェアライセンス購入時には USB ライセンスキーはございません)

◆ CC2000 USB ライセンスキー ×1

上記のアイテムがそろっているかご確認ください。万が一、欠品または破損品があった場合はお買い上げになった販売店までご連絡ください。

本ユーザーマニュアルをよくお読みいただき、正しい使用法により、本製品および接続する機器を安全にお使いください。

ソフトウェアバージョンに関する重要な注意事項

CC2000 v2.8.xxx からデータベースに変更が加えられているため、CC2000 v3.x.xxx および、これ以降のバージョンは v2.8.xxx と互換性がありません。したがって、同じサーバーに別のアプリケーションとしてインストールされたとしても動作しないため、ご注意ください。

CC2000 を v2.8 以前から v.3.0 以降にアップグレードする場合の詳細は、p.21 を参照してください。

本マニュアルについて

このユーザーマニュアルは、CC2000 に関する情報や使用法について説明しており、ソフトウェアのインストール・セットアップ・操作の各方法に関する、全ての情報を提供します。

本書の記載内容の概要は次の通りです。

概要

第1章　はじめに：CC2000 を紹介します。特長、機能概要および製品各部名称について説明しています。

第2章　サーバーのセットアップとユーティリティー：Windows および Linux の各システムにおける CC2000 のセットアップ方法について説明します。

第3章　ウェブブラウザーを使った操作：ウェブブラウザーを使った CC2000 へのログイン方法、および CC2000 のブラウザーインターフェースの操作方法について説明します。

第4章　ダッシュボードと基本操作：CC2000 サーバーのダッシュボード、およびインターフェースを使用する際の基本操作について説明します。

第5章　デバイス管理：CC2000 のネットワークで管理するデバイスへのアクセス・操作・追加・設定・構成の各方法について説明します。

第6章　ユーザー管理：ユーザーアカウントの追加・変更・削除、ユーザーグループの作成とグループへのユーザー登録、ユーザーやグループへのアクセス権限の設定、ユーザー認証の各方法について説明します。

第7章　システム：CC2000 の構成概念を紹介し、実際の環境における CC2000 プライマリーサーバーとセカンダリーサーバーのデプロイ・設定・管理の各方法について説明します。

第8章　ログ：CC2000 のログ機能の詳細、および記録されたログへのアクセス方法やログのフィルタリング・検索方法について説明します

付録A　技術情報：製品の技術情報およびトラブルシューティングの方法を提供します。

付録B　CC2000 ユーティリティー: CC2000 が稼働しているコンピューターのデスクトップから、ウェブブラウザーを使わずに CC2000 のパラメーターを設定する方法について説明します。

付録C　認証キーユーティリティー: CC2000 認証キー内のデータへのアクセス方法、および認証キーのアップグレード方法について説明します。

付録D　外部認証サービス: サードパーティーの外部認証サービスを使った CC2000 認証方法について説明します。また、OpenLDAP での CC2000 への認証の設定や、RADIUS を使った Linux 環境での CC2000 の認証方法を、例を挙げながら説明します。

付録E　シングルサインオン HTML サンプルコード: シングルサインオン機能のサンプルコードを掲載しています。

注意:

- ◆ 本書をよくお読みになった上で設置・操作の手順に従うことで、本機や接続機器の破損を防止してください。
- ◆ ATEN では新規仕様を反映させたファームウェアや関連ドキュメントを定期的にウェブサイトに公開しています。最新の CC2000 ドキュメントについては、以下のサイトにアクセスして、ご確認ください。
  http://www.aten.com/global/en/

マニュアル表記について

[　　]	入力するキーを示します。例えば[Enter]は**エンター**キーを押します。複数のキーを同時に押す場合は、[Ctrl + Alt]のように表記してあります。
1.	番号が付けられている場合は、番号に従って操作を行ってください。
◆	◆印は情報を示しますが、作業の手順を意味するものではありません。
→	矢印は操作の手順を示します。例えば Start → Run はスタートメニューを開き、Run を選択することを意味します。
	重要な情報を示しています。

※本マニュアルに記載されている商品名・会社名などは、各社の商標ならびに登録商標です。

第 1 章
はじめに

製品概要

CC2000 4.0 は、あらゆる業界の IT 部門が、ローカルであっても、あるいは国境を越えても、IT インフラをシングルポータルで簡単に一元管理することができる統合管理ソフトウェアです。本ソフトウェアを使うと、ATEN 製の IP-KVM スイッチ、シリアルコンソールサーバー、PDU、および他社製のブレードサーバーや物理/仮想サーバーを、インバンドおよびアウトオブバンドの方式で集約して管理することができます。CC2000 4.0 では、わかりやすいインターフェースによって、システム管理業務をより効率的に、そして、より生産的に行える環境を提供します。

簡潔で直感的に操作できる HTML 5 のウェブインターフェースを特長とする CC2000 4.0 では、ユーザー体験と操作性の面が向上しました。データの集約、タスク単位の操作、そしてメニューの簡素化によって、管理者は自身が担当する IT 機器へのアクセス・設定・管理といった操作を簡単に行うことができます。

CC2000 4.0 は、IT 担当者が重要な情報を迅速に把握し、最小限の労力と時間でタスクの監視を遂行するのに役立つ「ダッシュボード」と呼ばれる総合ポータルが特長です。このダッシュボードには、デバイスの状態、デバイスのイベント、タスクの結果、オンライン・ユーザー、ライセンス済みノードの使用状況が一目でわかるように表示されます。「デバイスの状態」および「デバイスのイベント」の各セクションにおいて、管理者は接続デバイスの状態を即座に把握できると同時に、重要なログを速やかに受信することができます。そして、「タスクの結果」セクションでは、操作成功や操作エラーに関する重要メッセージが配信されます。また、管理者はログイン中のユーザーの詳細を参照したり、不審なユーザーセッションを終了したりすることもできます。ダッシュボードの強化された通知機能は、ユーザーが問題を適切に処理して、効率的にトラブルシューティングするのをサポートします。

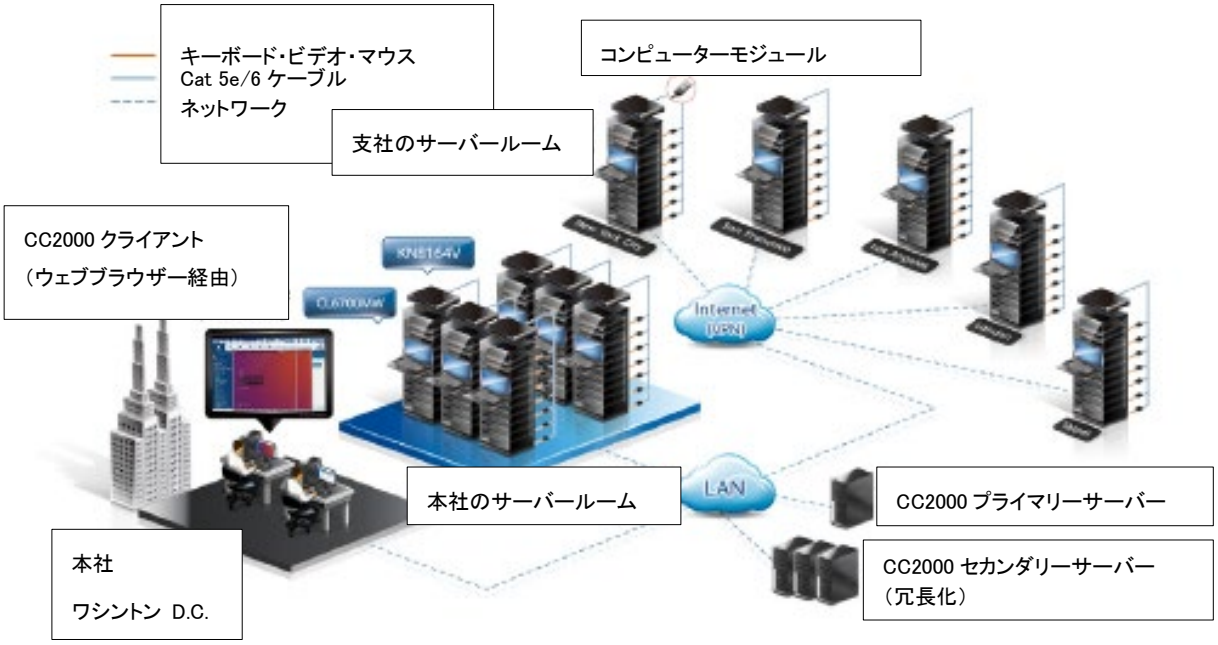
ATEN PDU シリーズおよびエネルギーボックスを CC2000 と併用することで、環境と電力の監視をリアルタイムで行うことができます。これにより、ユーザーはラック内の潜在的なホットスポットを認識し、IP デバイスの可用性を 24 時間 365 日確保し、接続された PDU の電源ステータスを監視し、CC2000 ダッシュボードを通じて他の重要な情報を調査することができます。

監視対象の数値がユーザー定義のしきい値を超えると、ユーザーはダッシュボード、メッセージセンター、電子メール、SNMP トラップ、および Syslog を介してリアルタイム警告を取得します。IT 管理者は、トレンドチャートからサーバールームの温度・湿度・気圧・電圧・電流・消費電力に関する本質を認識することができます。CC2000 4.0 のパネルダイナアレイモード（特許取得済み）は、管理者が一画面に分割出力された複数ポートのコンソールを参照するのに便利な機能です。パネル設定は、別々の IP-KVM スイッチのポートを組み合わせられるため、管理者は監視対象となるデバイスや、画面内にポートを表示させる方法を自由に選択することができます。また、表示されているパネルをクリックすると、そのポートにアクセスして操作できます。

そして、CC2000 4.0 はサービスを二重化するために、プライマリー・セカンダリーのサーバー・アーキテクチャーを採用しています。万が一、CC2000 4.0 のプライマリーサーバーがダウンした場合でも、プライマリーサーバーがオンラインに復旧するまでの間、セカンダリーサーバーが必要な管理サービスを提供し、CC2000 4.0 としての機能が常に維持されるため、いつでもデバイスにアクセスできる環境が保たれます。

CC2000 4.0 があれば、ユーザーは問題を適切に処理し、効率的にトラブルシューティングを行うことができます。CC2000 4.0 はセキュアな統合システム管理ソリューションとして、データセンターやサーバールーム、あるいは支社の場所を意識することなく管理できる環境を提供しますので、統合管理や手軽な監視といった面で IT 管理者が抱えるニーズに応えられる製品です。

適用例



特長

- ◆ 環境と電力のモニタリング – サーバールームやデータセンターの温度・湿度・気圧・電圧・電流・電力損失・水漏れ・ドア侵入を監視
- ◆ リアルタイム通知 – 重要警告の可用性を常時確保できるよう、CC2000 は監視データのしきい値超過時にユーザー通知
- ◆ トレンドチャートと監査の活用でユーザーは現状を正確に把握し、結果を分析した上で、戦略的アクションを実行可能
- ◆ エンタープライズシステムをシングルサインオンで一括管理 – 対象製品:ATEN 製 IP-KVM スイッチ、シリアルコンソールサーバー、インテリジェント PDU、およびサードパーティー製品（組込式サービスプロセッサー、物理サーバー、仮想サーバーなど）
- ◆ HTML5 で実装された直感的なユーザーインターフェースでユーザーフレンドリーな操作性を提供
- ◆ わかりやすいダッシュボード・ポータル – デバイスの状態、デバイスのイベント、タスクの結果、オンライン・ユーザー、ライセンス済みノードの使用状況を表示
- ◆ 各種サービスプロセッサーおよび IP ツール経由で柔軟にリモートアクセスを実現 – Redfish（iDRAC8/iLO5）、Dell iDRAC 5/6/8、IBM RSA II、HP iLO 2/3/5、Dell CMC、IBM AMM、HP OA、IPMI、IMM、RDP、VNC、SSH、Telnet に対応
- ◆ 仮想化環境のアクセスや操作が可能 – VMware vSphere 5.5/6.0/6.5/6.7、 Windows Server 2008、2012 & 2016、または Citrix XenServer 6.5 に対応
- ◆ APC PDU（AP79xx、AP89xx、AP86xx）対応
- ◆ 外部認証は LDAP、AD、Kerberos、RADIUS、TACACS+対応。ユーザーアクセスの権限管理はロールベースのポリシーを適用
- ◆ 軍事レベルの暗号化通信（AES 256-bit）でノード間アクセスの安全性を確保
- ◆ IP アドレスや MAC アドレスで権限の付与や制限を行うアクセスコントロール。また、ログイン再試行可能回数とユーザーID ロックアウトのパラメーターは SAS 70 準拠
- ◆ サードパーティー認証局（CA）署名済み証明書に対応
- ◆ TLS 1.2 暗号化によるデータ通信および RSA 2048-bit 認証によりブラウザーからのセキュアなユーザーログインが可能
- ◆ 強固なユーザーパスワードポリシーでユーザーアカウントのセキュリティーを強化
- ◆ ATEN 製 IP-KVM スイッチ・シリアルコンソールサーバー・その他のデバイスから出力されたログを、syslog プロトコル経由で統合し監査に活用可能
- ◆ ユニバーサルなバーチャルメディアに対応するソフトウェアの配置が容易（ISO イメージのマウント、ブート、またはデバイスのリモートアップグレード）

- メール、SNMP（v1、v2c、v3）、Syslog 経由でのイベント通知に対応
- タスクスケジューリング機能 – CC2000 のデータベースと設定のバックアップ、ログのエクスポート、PDU デバイスの電源オン・オフ制御
- メッセージボックス – 内部システムメッセージや重要なログをクリックひとつで簡単に詳細表示
- パネルアレイモード – 一画面を分割し、複数のサーバーのビデオ出力の監視が可能
- マウスダイナシンク – ローカルとリモートのマウスカーソルの動きを自動同期
- サーバーの冗長化 – サービスの可用性を考慮し、プライマリー・セカンダリーのサーバー・アーキテクチャーを採用
- デバイスへのクイックアクセスと管理 – 最近アクセスしたデバイスのリストは「**最近**」から、ブックマークされたデバイスのリストは「**お気に入り**」から、それぞれ簡単にアクセス可能
- ユーザー間での情報共有や連携が容易に行えるオンラインチャット機能
  （用途例：問題に対する迅速なトラブルシューティングなど）
- MOTP（モバイルワンタイムパスワード）認証をサポート

システム要件

サーバー側システム 最小要件

CC2000 サーバーをインストールするシステムには、以下の動作環境が必要です。この要件はいかなる環境でも動作を保証するサーバー自体のスペックではなく、CC2000 がプログラム単体で使用する最少の負荷の目安としてご参照ください。使用規模や想定稼働期間が長くなるほど負荷が大きくなるため十分に余裕を持ったスペックを持つサーバーをご用意ください。

◆ ハードウェア環境

	小規模システム （デバイス 100 台未満）	中～大規模システム （デバイス 100 台以上）
CPU	Intel Core i3 2GHz 以上	Intel Core i5 3GHz 以上
メモリー （OS とは別、プログラム単体での割り当て必須サイズ）	4GB 以上	8GB 以上
ハードディスクドライブ	20GB 以上	40GB 以上
イーサネット	1 カ所以上のイーサネットアダプター以上 （100Mbps 以降） – ギガビット LAN 推奨	

◆ OS 環境

JRE 8	OpenJDK 8
Windows: ◆ Server 2019 ◆ Server 2016 ◆ Server 2012 ◆ Server 2008 ◆ 10 ◆ 8	Windows: ◆ Server 2019 x64 ◆ Server 2016 x64 ◆ 10 x32/x64
Linux ◆ Red Hat Enterprise Linux V. 4 ◆ Novell SUSE Enterprise Server 9 / 10 ◆ Ubuntu 15.10 x64 ◆ Ubuntu 15.10 x86	Linux ◆ Ubuntu 16.04 x64 ◆ Ubuntu 20.04 x64 ◆ Fedora 32 x64 ◆ Redhat Enterprise 8.1 x64

◆ Debian 8.2 x64 ◆ Fedora 23 x64 ◆ Fedora 23 x86 ◆ OpenSUSE 13.1 x64 ◆ CentOS 7 x64	◆ CentOS 8.1 x64

クライアント側システム 最低動作環境

ハードウェア環境

- ◆ CPU および解像度 ： Intel® Pentium™ 4 2GHz 以上のプロセッサーを搭載し、解像度が 1024×768 に設定されているコンピューター推奨
- ◆ メモリー ： 512MB 以上（1GB 以上推奨）
- ◆ ネットワーク ： 10Mbps 以上のネットワーク転送速度に対応した Ethernet アダプター搭載（100Mbps 以上推奨）
- ◆ ウェブブラウザー ： 128-bit SSL 暗号化通信対応のこと
- ◆ ウェブブラウザーで Java Web Start（JNLP）ビューワーを使用する環境では、Oracle Java Runtime Environment（JRE）8 または Zulu OpenJDK 8 の最新のバージョンおよび IcedTea-Web がインストールされていることをご確認ください。IcedTea-Web は、次の URL からダウンロードしてください。 https://azul.com
- ◆ ウェブブラウザーからログインした後で、最初にビューワーへとアクセスするのに 205MB 以上の空きメモリーがあることを確認してください。また、ビューワーを複数立ち上げる場合は、1 回の起動ごとに 100MB 以上の空きメモリーがあることをご確認ください。

OS

◆ CC2000 に接続するクライアントワークステーションとして使用するコンピューターの対応 OS は以下の通りです。

OS		バージョン
Windows		8.1 以降
Linux	Red Hat	7.1 以降
	Fedora	Core2 以降
	SuSE	9.0 以降
	Mandriva (Mandrake)	9.0 以降
UNIX	AIX	4.3 以降
	FreeBSD	4.2 以降
	Sun	Solaris 8 以降

◆ CC2000 にログインするコンピューターには、OS が Windows2000 以降で、なおかつ、OpenJDK 8 または Oracle Java Runtime Environment (JRE) 8 が動作できる環境であることをご確認ください。

注意: Windows2000 クライアントは Windows クライアントビューワーに対応していません。

ウェブブラウザー

CC2000 へのログインに対応したウェブブラウザーは下表の通りです。

ウェブブラウザー		バージョン
Internet Explorer		11 以降
Edge		42 以降
Chrome		56 以降*
Firefox	Windows	60 以降
	Linux	60 以降
	Sun	52 以降
Safari	Mac	10 以降
Opera		57 以降

デバイス側システム要件

CC2000 で統合する ATEN 製品には、CC2000 に対応したバージョンのファームウェアがインストールされており、このデバイス側で CC2000 による管理が有効になっていることをご確認ください。また、必要であれば、関連デバイスにも最新版のファームウェアをインストールしてください。ファームウェアのアップグレードに関する詳細は p.166「アップデートとリストア」をご参照ください。

注意:

1. 通信ポートの設定は、デバイス側と CC2000 側で同じになるように設定してください(p.25 参照)。
2. CC2000 対応デバイスの型番については弊社ウェブサイトをご参照ください。

ライセンス

CC2000 のライセンスは、CC2000 サーバーで許可されたセカンダリーサーバー用のライセンス数と対応デバイスのノードの数によって構成されています。ライセンス情報は CC2000 パッケージに同梱されている USB ライセンスキーまたはソフトウェアライセンスに保存されています。

ライセンスポリシー

- CC2000 サーバーソフトウェアのインストールが完了すると、デフォルトのライセンス(1 プライマリー、セカンダリーサーバーライセンスなし、16 ノード)が自動的に付与されます。
- セカンダリーサーバーやノードを追加するには、有償のライセンスのアップグレードが必要です。詳細については p.229「ライセンス」を参照してください。
- システムを v3.3 から v4.0 にアップグレードするには、保守ライセンスが必要です。ライセンスの期限が切れてしまった場合でも CC2000 は正常に動作しますが、アップデートはマイナーな修正に限定されます(例:v4.0.109 から v4.0.201)。

注意:
- 期限切れの保守ライセンスを更新した場合、期限切れ後から更新までに経過した期間もライセンスの期間にカウントされます。
- 保守ライセンスの購入または更新に関する詳細は、担当営業までお問い合わせください。
- 保守ライセンス(例:最大 512 ノードをサポートする CCMA512)を 2 つ購入された場合は、2 年保証と同等の扱いになります。
- 更新済みの保守ライセンスを CC2000 システムに適用する方法の詳細については p.229「ライセンス」を参照してください。

ノード

- ノードはアグリゲートデバイスまたは物理ポートのどちらにもなりえます(例:KVM デバイスの KVM ポート、シリアルコンソールサーバーのシリアルポート、PDU のセンサー/アウトレットポート)。各ノードにはそれぞれライセンスが必要です。

  - アグリゲートデバイスは、CC2000 で管理するデバイス(ルーター、サーバー、スイッチングハブなど)に対して ATEN 製 Over IP 対応デバイスの複数のポート*からアクセスするような場合に作成することができます。これらのポートを 1 つのアグリゲートデバイスとして集約すると、このアグリゲートデバイスはシングルノードとして扱われますので、必要となるライセンスは 1 つだけとなります。

注意： 最大で、KVM は 2 ポート、シリアルは 4 ポート、アウトレットは 8 ポートです。

- ATEN 製の Over IP 対応デバイスのポートがアグリゲートデバイスの一部でない場合は、使用する際にロックの解除（p.141「デバイスのロックとロック解除」参照）が必要です。ロックが解除されたポートはそれぞれ 1 ノードとしてカウントされます。

◆ ジェネリックデバイス（ルーター、スイッチなど）はノードとしてカウントされません。

◆ ダイレクトウェブアクセスデバイスはノードとしてカウントされません。

◆ グループデバイスはノードとしてカウントされません。これらはロックされていない物理ポートのグループで構成されています。1 つ以上のグループデバイスに対して同一の物理ポートを追加することが可能ですが、追加されるグループデバイスの数にかかわらず、必要となるノードライセンスは 1 つだけとなります。

◆ ブレードサーバーおよびホスト VM ： *N* + 1 ノードのライセンスを消費します（*N* = ブレードと VM の数）。

注意： 各デバイスカテゴリーに関する詳細は、p.70「デバイス別 – 操作全般」をご参照ください。

セカンダリー

ライセンスには CC2000 プライマリーに登録できるセカンダリーの数が記録されています。プライマリーでセカンダリーを登録する方法の詳細については、p.36 をご参照ください。

第 2 章
サーバーのセットアップと
ユーティリティー

概要

サーバーにはLinuxマシンを採用するユーザーも多いことから、CC2000はWindowsに加えLinuxにも対応しています。本章では、Windows および Linux 環境における CC2000 サーバーのインストール方法について説明します。

Windows 版のインストール

インストールを始める前に

インストール作業を始める前に、CC2000 Windows 版をインストールするサーバーに OpenJDK 8 または Oracle Java Runtime Environment (JRE) 8 がインストールされていることをご確認ください。環境が整っていない場合は、ダウンロードしてインストールしてください。

JRE の最新版は次の URL に公開されています。
https://java.com/ja/

OpenJDK の最新版は次の URL に公開されています。
http://www.azul.com

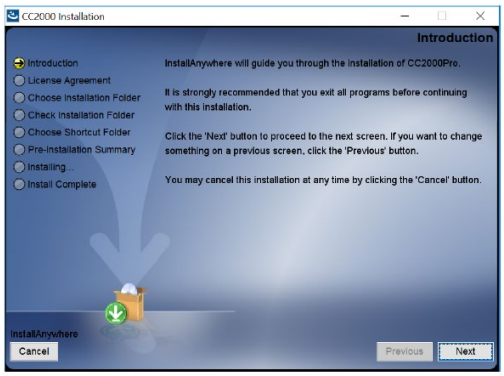
OpenJDK または JRE のインストールが完了すると、CC2000 をインストールすることができます。

インストール

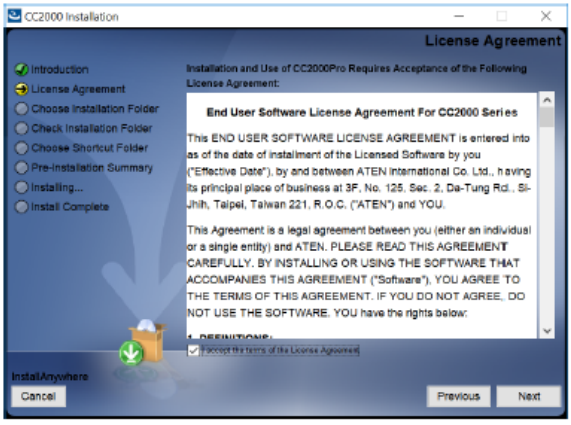
Windows に CC2000 をインストールする場合は、以下の手順で操作してください。

1. CC2000 のインストーラーを用意してください。インストーラーは CC2000 の製品ページからダウンロードできます。

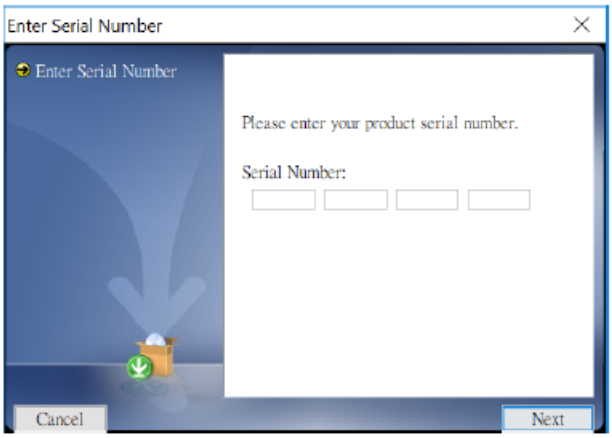
2. ファイル「CC2000_Setup_V4.0.0_ForWindows.exe」が置かれているフォルダーに移動して、このファイルを実行してください。インストーラーを起動すると、下図のような画面が表示されますので、「Next」(次へ)ボタンをクリックしてください。



3. インストーラーに使用許諾契約が表示されます。この内容を確認し、受け入れるのであれば、「I accept the terms of the License Agreement」(この使用許諾契約の内容に同意する)のチェックボックスをクリックしてください。そうしたら、「Next」(次へ)ボタンを押して、次の画面に進んでください。

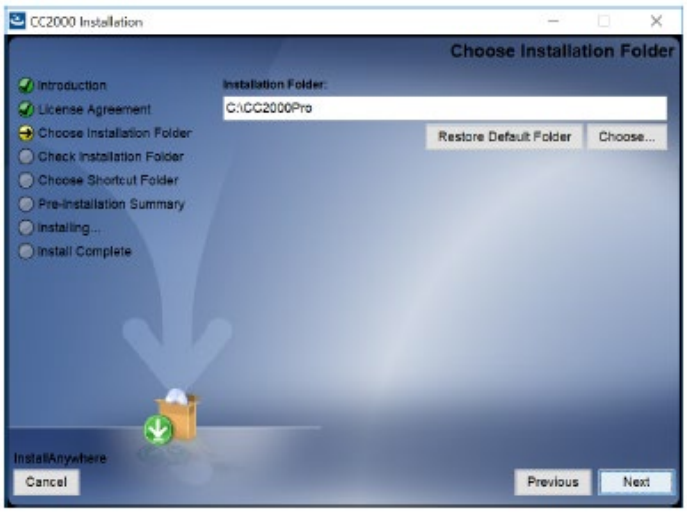


4. インストーラーからシリアルナンバーの入力を促されたら、CC2000 ソフトウェアのシリアルナンバーを入力し、「Next」(次へ)ボタンをクリックして、操作を続けてください。

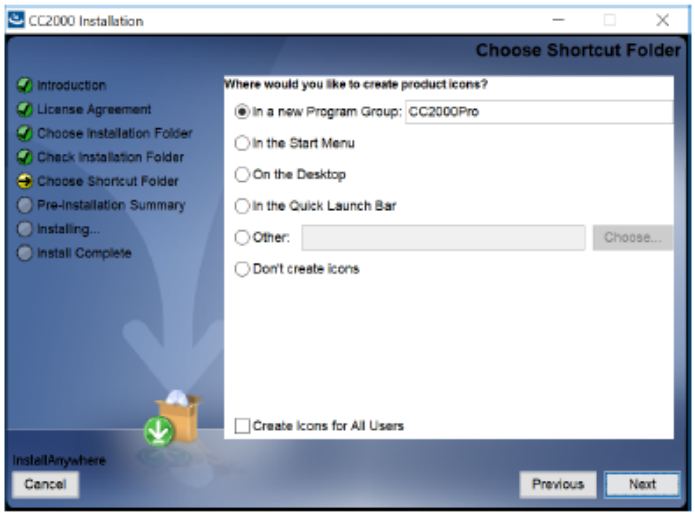


注意：	このシリアルナンバーは CC2000 の再インストール時にも必要になりますので、必ず記録しておいてください。

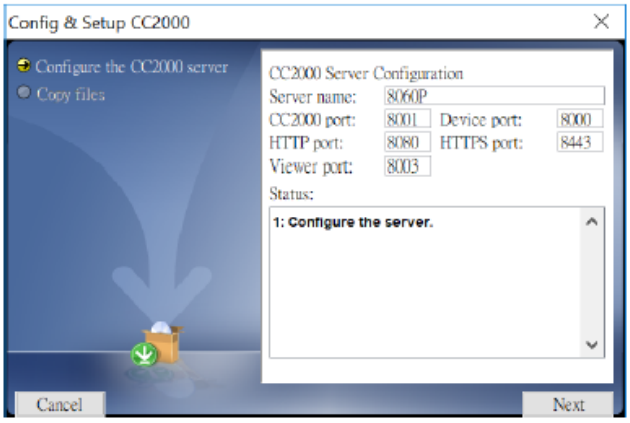
5. インストーラーは「Choose Installation Folder」(インストールフォルダーの選択)画面に切り替わり、CC2000 をインストールするフォルダーの指定が求められます。デフォルトのフォルダーを使用しない場合は、「**Choose…**」(選択…)ボタンをクリックし、「フォルダーの選択」ダイアログから CC2000 をインストールするフォルダーを選択してください。フォルダーを選択したら、「**Next**」(次へ)ボタンを押して次の画面に進んでください。



6. 「Choose Shortcut Folder」(ショートカットフォルダーの選択)ダイアログで、CC2000 のショートカットアイコンを作成する場所をラジオボタンで選択したら、「**Next**」ボタンをクリックして次の画面に進んでください。



7. 「Config & Setup CC2000」(CC2000 の設定&セットアップ)の画面が表示されたら、必要項目をそれぞれ入力してください。各項目の詳細は下表の通りです。



項目	説明
Server name (サーバー名)	この欄には Windows で設定されているコンピューター名がデフォルトで表示されますが、必要であれば別の名前に変更することも可能です。名前は 2～32 バイトで入力してください。(対応言語であれば、どの言語を使って入力しても構いません。) **注意:** 1. 以下の文字は使用できません。: “ ‘ ＼ 2. このサーバー名は CC2000 サーバー上で使用する名前ですので、お使いのサーバーの Windows 上でのコンピューター名には影響しません。

(表は次のページに続きます)

項目	説明
CC 2000 port （CC2000 ポート）	この CC2000 サーバーが他の CC2000 サーバーと通信する際に使用するポートを設定します。**デフォルトでは 8001** に設定されています。 **注意：** 1. この項目は、「Redundant Servers」（冗長サーバー）画面における **CC2000 ポート**と同じものです（p.280「冗長サーバー」参照）。 2. CC2000 サーバーはそれぞれ使用するポートを自由に設定できますが、管理をしやすくするために、お使いの環境では全て同じポートに設定されることを推奨します。
Device Port （デバイスポート）	CC2000 サーバーが、接続済みの ATEN の Over IP 製品との通信に使用するポートを設定します。**デフォルトでは 8000** に設定されています。 各 CC2000 はそれぞれ異なるデバイスポートナンバーを設定できますが、同じネットワークセグメント上にあるデバイスと通信できるようにするためには、これらのデバイス上でもここで設定されたポートを使用するように設定する必要があります。
HTTP port （HTTP ポート）	CC2000 がウェブ通信(HTTP)に使用するポートを設定します。**デフォルトでは 8080** に設定されています。これ以外のポートに設定した場合、ユーザーはウェブブラウザーでアクセスする際にこのポートをアドレスバーで指定する必要があります。
HTTPS port （HTTPS ポート）	CC2000 がウェブ通信(HTTPS)に使用するポートを設定します。**デフォルトでは 8443** に設定されています。これ以外のポートに設定した場合、ユーザーはウェブブラウザーでアクセスする際にこのポートをアドレスバーで指定する必要があります。
Viewer Port （ビューワーポート）	**デフォルトでは 8003** に設定されています。

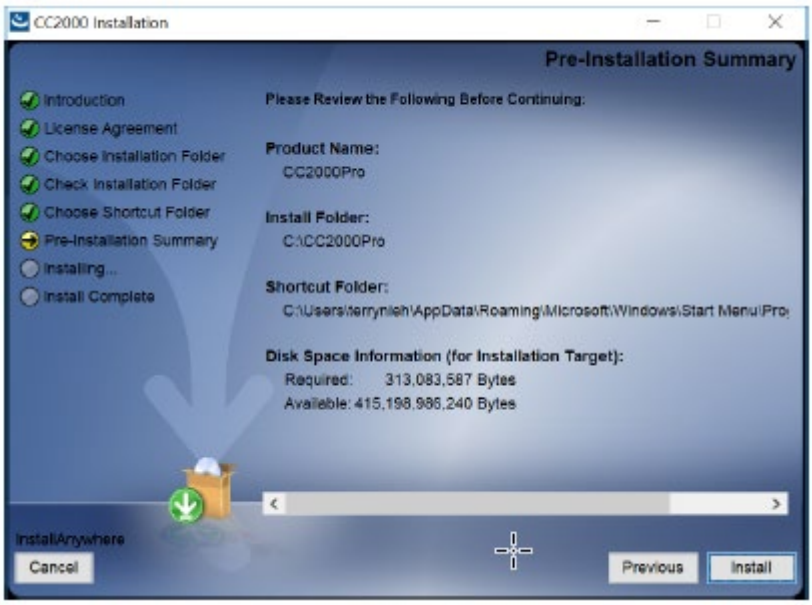
8. 必要項目を全て入力したら、「**Next**」（次へ）ボタンをクリックして次の画面に進んでください。

注意： ここで設定された項目は、全てインストール後に変更することができます。詳細については p.229「システム情報」をご参照ください。

9. インストールフォルダーにファイルをコピー中であることを示すダイアログが表示されます。ファ

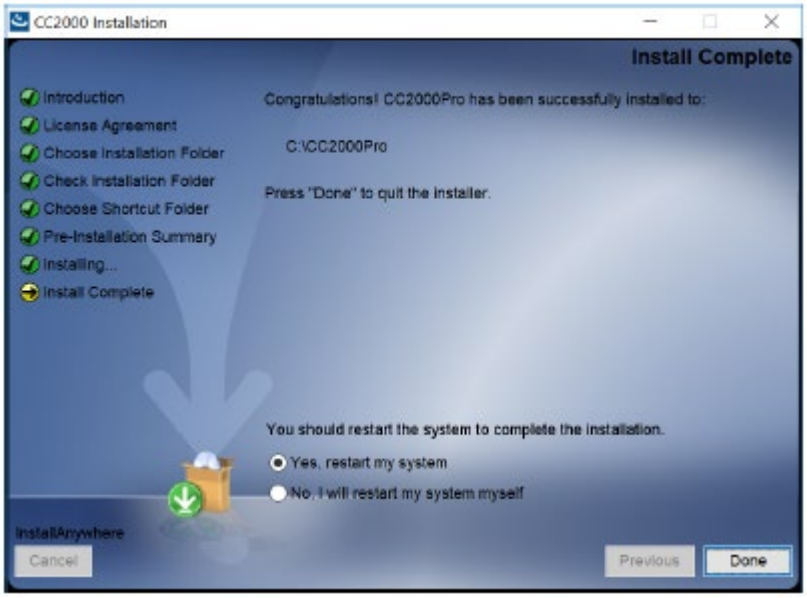
イルのコピーが完了したら、「Continue」（続行）ボタンをクリックし、次の画面に進んでください。

10. 下図のような「Pre-Installation Summary」（インストール前の確認）画面が表示されます。

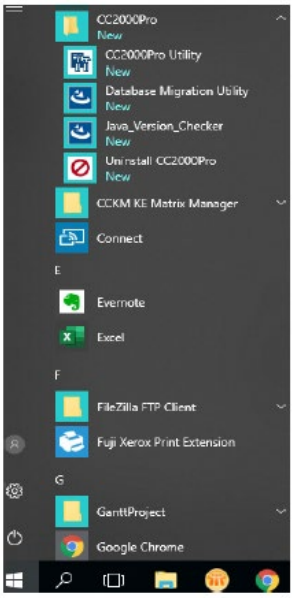


変更したい内容がある場合は「Previous」（前へ）ボタンを押して前の画面に戻ってください。この情報に間違いがない場合は「Install」（インストール）ボタンをクリックしてください。

11. インストールが完了すると、インストール処理を完全に終了させるためにシステムの再起動を行うかどうかの選択が求められます。インストーラーを終了してシステムを再起動する場合は、「Done」（完了）ボタンをクリックしてください。再起動を行わない場合は、「No, I will restart my system later」（後で再起動する）を選択してください。



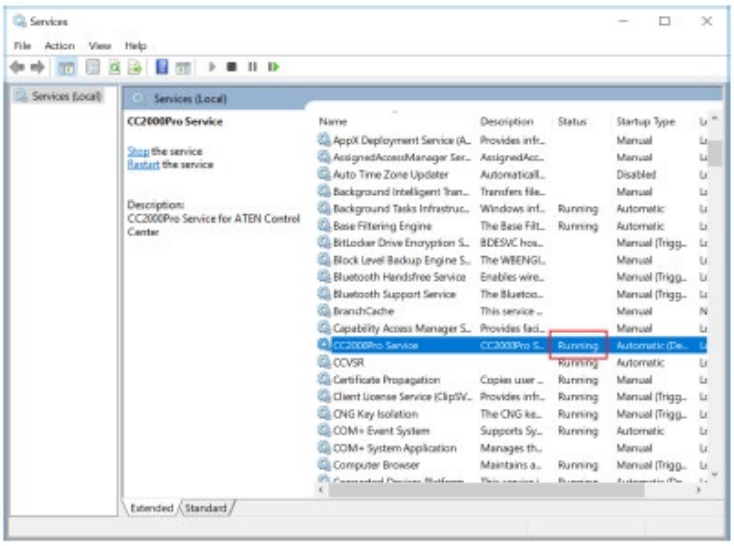
12. Windows のスタートメニューに CC2000Pro のエントリーが作成されます。



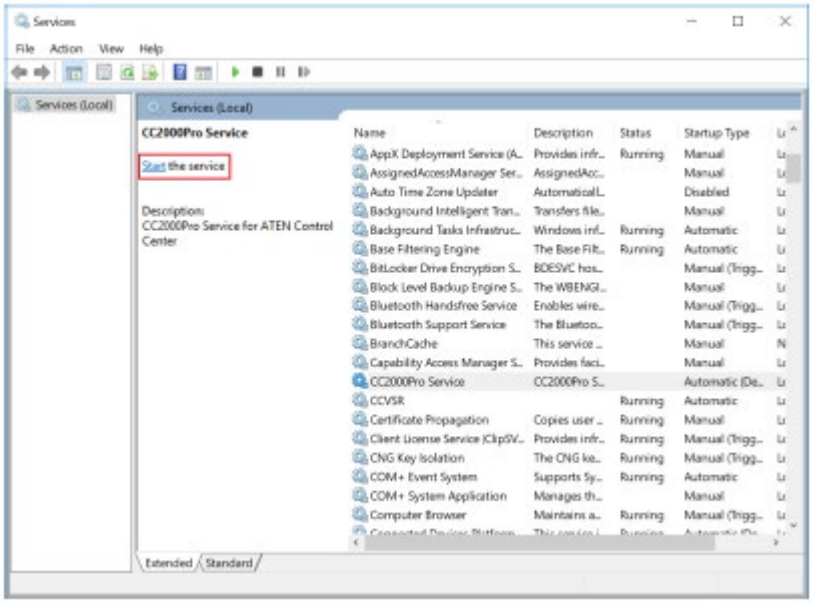
インストール後の確認

インストールが完了すると、CC2000 のサービスが自動的に立ち上がり、Windows の起動時にはこのサービスが必ず起動するようになります。

CC2000 が起動したかどうかを確認する場合は、デスクトップアプリの「サービス」に進み、「状態」列が「実行中」になっていることを確認してください。



「実行中」と表示されていない場合は、「起動」をクリックしてサービスを起動してください。



Linux 版のインストール

インストールを始める前に

Linux への CC2000 のインストールは、Windows 版のインストール手順とほぼ同様ですが、Java に関しては操作を始める前に以下の点に注意が必要です。

◆ CC2000 をセットアップするサーバーに Java がインストールされていない場合は、Oracle Java のウェブサイト(http://java.com)からダウンロードしてください。Java のインストール方法の詳細については、Java のダウンロードウェブページをご参照ください。

◆ CC2000 プログラムは、OpenJDK 8 または JRE 8 が実行できるシステムが必要です。一部の Linux ディストリビューションには、JRE 8 以外のバージョンの Java がインストールされている場合があります。お使いの Java のバージョンを確認する場合は、プロンプトから以下のコマンドを実行してください。

```
java -version
```

重要:	OpenJDK と CC2000 は、いずれも Linux の root ユーザーでインストールしてください。これ以外のユーザーでインストールすると、一部の機能が正しく動作しないおそれがあります。

このコマンドの実行結果がシステム要件を満たしていない場合は、OpenJDK 8 または JRE 8 をインストールする必要があります(上述の Java のダウンロードとインストール方法を参照)。

◆ お使いのサーバーの /root/.bash_profile というファイルに設定されている Java の環境変数「PATH」および「JAVA_HOME」の値が、CC2000 で使用する Java のインストールディレクトリーを参照していることを確認してください。以下は、Java を「/usr/java/jre1.6.0_0-b11」というディレクトリーにセットアップした場合における/root/.bash_profile の例です。

```
JAVA_HOME=/usr/java/jre1.6.0_0-b11
PATH=$JAVA_HOME/bin:$PATH:./
BASH_ENV= $HOME/.bashrc
USERNAME= "root"
export JAVA_HOME PATH BASH_ENV USERNAME
```

◆ インストール Java のバージョンに問題がなく、環境変数「PATH」および「JAVA_HOME」の値も新しくインストールした Java のディレクトリーを参照しているにもかかわらず、Linux 側ではその新しいバージョンを認識せず、古い Java のバージョンを使用し続ける場合があります。この問題が発生した場合は、以下の手順で、設定をやり直してください。

1. ダウンロードした「CC2000Setup_Linux.bin」というファイルを、お使いのサーバーの適当なディレクトリーにコピーしてください。
2. ターミナルを開き、手順 1 でファイルをコピーしたディレクトリーに移動してください。
3. 以下のコマンドを実行してください。

   export LAX_DEBUG=1

   sh CC2000-Setup-ForLinux.bin

注意：	インストーラーが起動した場合は、処理をキャンセルしてください。

4. 画面出力で、「Using VM.....」という文字列で始まっている行（太字で表示）を探し、お使いのディストリビューションのデフォルトの Java のバージョンを確認してください。

5. 手順 4 で確認した部分で、古い方の Java がインストールされていたディレクトリーにある「java」というファイルのパスが表示されている場合は、そのディレクトリーに移動して「java」ファイルを削除するか、このファイルを別の名前に変更してください。

6. ログアウト後、もう一度ログインしてください。

インストール

インストールされている OpenJDK または JRE のバージョンが正しいことを確認したら、以下の手順で CC2000 をインストールしてください。

1. CC2000 のインストーラーを用意してください。インストーラーは CC2000 の製品ページからダウンロードできます。

2. 「CC2000_Setup_V4.0.0_ForLinux.exe」があるディレクトリーに移動し、このインストーラーを実行してください。

重要:	OpenJDK と CC2000 は、いずれも Linux の root ユーザーでインストールしてください。これ以外のユーザーでインストールすると、一部の機能が正しく動作しないおそれがあります。

注意:	1. このインストーラーのファイルに実行権限があることを確認してください。 2. 一部のバージョンの Linux では、このインストーラーをターミナルから実行する必要があります。

インストーラーを実行すると、下図のような画面が表示されます。

「**Next**」(次へ)ボタンをクリックして、次の画面に進んでください。

3. これ以降のインストール手順は、Windows 版と同様です。インストール方法の詳細は p.21 をご参照ください。

インストール後の確認

◆ インストールに成功すると、CC2000 のサービスが自動的に立ち上がり、コンピューターの起動時にはこのサービスが必ず起動するようになります。
CC2000 が起動していることを確認したら、root ユーザーでログインし、ターミナルコンソールから以下のコマンドを使ってサービスの起動、停止、再起動を行ってください。

- サービスの起動　/etc/init.d/cc2000service start
- サービスの停止　/etc/init.d/cc2000service stop
- サービスの再起動 /etc/init.d/cc2000service restart
- サービスの状態確認　/etc/init.d/cc2000service status

◆ お使いのシステムで使用されている Java のバージョンを確認する場合は、以下の手順に従って操作してください。

1. [スタート]メニューを開いてください。
2. CC2000 エントリー([プログラム]→[CC2000])に移動し、[Java Version Checker]を選択してください。

インストール後に必要となるセットアップ

CC2000 ソフトウェアには、プライマリーサーバーとしてセットアップできるデフォルトのデモ用ライセンスが付属しています(セカンダリーなし、16 ノード:ノードは全て同一ネットワークセグメント上でのセットアップが必要)。お使いになる構成がこの規模を超える場合は、セカンダリーサーバーやノードを追加するライセンスキーの購入が必要です。

製品のインストールが完了したら、サーバーをプライマリーとセカンダリーのどちらとして使用するかを設定する必要があります。

◆ サーバーをプライマリーとして使用する場合、CC2000 の USB ライセンスキーをサーバーの USB ポートに接続し、サーバーにログイン(p.41 参照)した後、「License」(ライセンス)メニューにアクセスして「Upgrade」(アップグレード)ボタンをクリックしてください(p.257 参照)。許可されるセカンダリーとノードの数は購入したライセンスキーに格納されています。詳細については代理店までお問い合わせください。(ソフトウェアライセンスも同様に Licence メニューからライセンスファイルをアップロードすると登録ライセンスをアップグレードできます)

注意:	ライセンスをアップグレードしたら、キーを USB ポートから抜いて安全な場所に保管しておいてください。この USB ライセンスキーはライセンス更新の際に必要となります。

◆ サーバーをセカンダリーとして使用する場合、新規のライセンスキーを別途用意する必要はありません。プライマリーサーバー側で使用しているライセンスキーにあるセカンダリーサーバーライセンスノードを使用してセカンダリーサーバーとして登録してください。詳細は p.281「プロパティーの参照」をご参照ください。

CC2000 のアンインストール

Windows 版のアンインストール

Windows 版 CC2000 をアンインストールする場合は、以下の手順で操作してください。

1. 「スタート」ボタンをクリックしてください。
2. CC2000Pro のエントリー（[プログラム] → [CC2000Pro]）に進んだら、[Uninstall CC2000Pro]（CC2000Pro のアンインストール）を選択してください。

注意：	一部の CC2000 のファイルおよびフォルダーは、このアンインストーラーでは削除されません。これらのファイルやフォルダーを完全に削除したい場合は、CC2000 のインストールフォルダー(デフォルトでは C:¥CC2000Pro)を手作業で削除してください。(CC2000 を再インストールする場合は、これらのファイルやフォルダーを完全に削除しておく必要があります。)

Linux 版のアンインストール

Linux で CC2000 をアンインストールする場合は、root ユーザーでログインし、以下のコマンドを実行してください。

/install-path/Uninstall_CC2000Pro/Uninstall_CC2000Pro

上記の「/install-path」の部分には、CC2000 のインストールディレクトリーを適宜指定してください。

注意：	一部の CC2000 のファイルおよびディレクトリーは、このアンインストーラーでは削除されません。これらのファイルやディレクトリーを完全に削除したい場合は、CC2000 のインストールフォルダー(デフォルトでは/home/CC2000Pro)を手作業で削除してください。(CC2000 を再インストールする場合は、これらのファイルやフォルダーを完全に削除しておく必要があります。)

CC2000 のアップグレード

CC2000 を v3.0 から v4.0 以降にアップデートする場合は、次の手順に従って操作を行ってください。

1. 保守ライセンスを購入し、USB キーをアップグレードしてください。
   詳細は p.349「キーライセンスのアップグレード」を参照してください。

2. 次のいずれかの方法で、ライセンスを CC2000 v3.x に適用してください。
   - ◆ USB キーを使用したライセンスのアップグレード（p.257 参照）
   - ◆ ライセンスファイルを使用したライセンスのアップグレード（p.257 参照）

3. CC2000 アップグレードプログラムを使って CC2000 v3.x を v4.0 にアップデートしてください。
   - ◆ CC2000Upgrade_Win.exe (Windows の場合)
   - ◆ CC2000Upgrade_Linux.bin (Linux の場合)

注意：	アップグレードの際には、プライマリーと各セカンダリーサーバーをそれぞれアップグレードする必要があります。

このアップグレードプログラムは、新しいバージョンがリリースされると弊社ウェブサイト（https://www.aten.com/jp/ja/）からダウンロードできるようになります。このウェブサイトを定期的にチェックし、最新版のアップグレードプログラムがリリースされていないか確認してください。ダウンロードは、画面上部にある検索マーク（虫眼鏡のアイコン）をクリックして型番を入力し、製品ページにアクセスした後、「サポートとダウンロード」メニューをクリックすると、使用可能なパッケージのリストが表示されます。

事前準備

以下の作業は、CC2000 サーバーのインストールデータベースが全て最新のバージョンになっているかを確認するためのものです。CC2000 のアップグレード後に問題が発生した場合は、以下の手順で作成したバックアップを使ってデータベースを最新の動作レベルに回復してください。

CC2000 のアップグレードを始める前に、以下の方法でバックアップを作成することを推奨します。

1. スケジュールの設定で各セカンダリーのデータベースの複製を作成し、「すぐに実行する」ボタンを使ってタスクを実行してください（p.278 参照）。

2. 複製を作成したら、前の画面に戻り、アップグレードを行う時間を避けてスケジュールの時間を設定してください(来週、来月など)。
3. プライマリーユニットで、データベースバックアップを実行してください。

上記の事前準備が完了したら、プライマリーおよび各セカンダリーをアップグレードすることができます。アップグレードプログラムを実行する際は、インストールウィザードの画面内の指示に従って操作してください。

CC2000 セカンダリーサーバー

CC2000 を最大構成でセットアップした場合、ネットワークにアクセスできる場所であれば設置場所を問わず、1 台のプライマリーと最大 31 台のセカンダリーを利用することができます。お使いの CC2000 ソフトウェアのライセンスのアップグレードを行ったサーバーは、自動的にプライマリーサーバーへと指定されます。詳細については p.19 をご参照ください。

プライマリーサーバーが設定されると、登録機能を使って他の CC2000 サーバーをセカンダリーとして設定することができます。詳細については p.281「プロパティーの参照」をご参照ください。

CC2000 冗長セカンダリーサーバー

CC2000 サーバーを冗長化する場合、CC2000 冗長セカンダリーサーバーを少なくとも 1 台セットアップする必要があります。

ネットワークエラーや CC2000 自体のエラーが原因でプライマリー(優先)サーバーに障害が発生すると、セカンダリー(代替)サーバーが自動的に処理を引き継ぐため、接続デバイスの状態と通常操作は維持されます。ただし、アドミニストレーターは、プライマリーサーバーが正常に戻る(エラーがなくなるか、新規に割り当てられるか)まで、設定を変更することができません。

任意のセカンダリーサーバーを冗長サーバーとして割り当てる方法については、p.280「冗長サーバー」を参照してください。

データベース移行ツール

データベース移行ツールは、CC2000 v2.8 のデータベースを CC2000 v3.2 以降のバージョンに移行するのをサポートするユーティリティーです。

このツールは、Java ベースのプログラムであるため、Windows と Linux で使用することができます。

また、CC2000 v2.8 の最新データベースを、CC2000 v3.2 以降のバージョンと互換性のあるバックアップファイルとしてエクスポートします。

事前準備

移行元となる CC2000 サーバーのバージョンが v3.2 系以降への移設に対応している v2.8.271 以降であることを確認してください。これより古いバージョンを稼働させている場合は、弊社ウェブサイトにおける CC2000 の製品ページから、v2.8.271 の v2.x 系の最終バージョンのアップグレードファイルをダウンロードし、アップグレードしてください。

また、移行先となる CC2000 サーバーのバージョンが 3.2.312 以降であることを確認してください。これより古い場合は、弊社ウェブサイトにおける CC2000 4.0 の製品ページから、アップグレードファイルをダウンロードし、インストールしてください。

データベースの移行

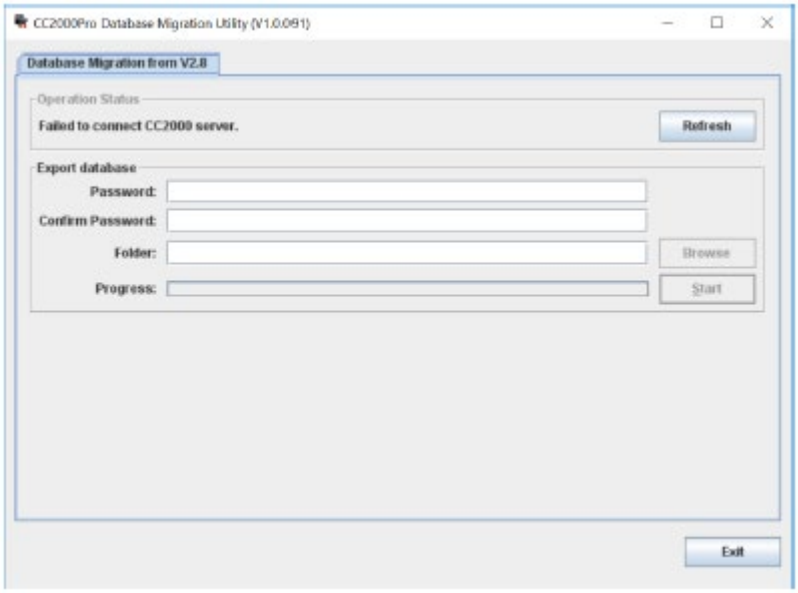
データベースの移行を行うには、次の手順に従って操作を行ってください。

1. CC2000 v2.8 が実行されているコンピューターで、データベース移行ツールのインストーラーをダウンロードしてください。このツールは、弊社ウェブサイトにおける CC2000 3.0 の製品ページから入手することができます。

2. インストーラーを起動し、画面内の指示に従って操作を行ってください。

3. データベース移行ツールを起動してください。

注意:	CC2000 v2.8 が実行中で、**動作の状態**が「接続中」として表示されていることを確認してください。状態を更新するには、「Refresh」(再読込)をクリックしてください。



4. 「Password」(パスワード)と「Confirm Password」(確認用パスワード)の各欄にパスワードを入力したら、「**参照…**」をクリックして、移行先となるフォルダーを選択してください。

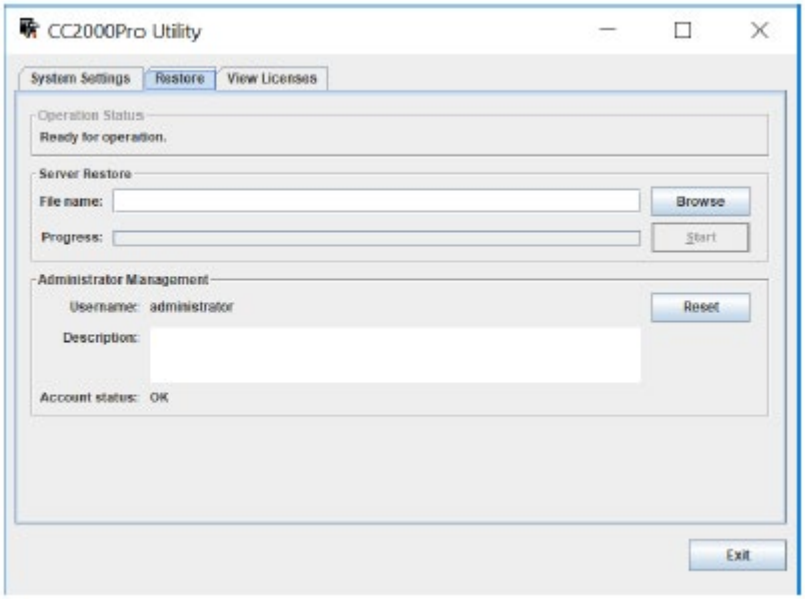
5. 「Start」(開始)をクリックして、エクスポートの処理を開始してください。処理が完了すると、データベースのバックアップファイル(*.cbk)とログファイル(*.log)が移行先のフォルダーに作成されます。

6. エクスポート処理が完了したら、CC2000 v2.8 サーバーを停止してください。

7. 拡張子が「*.cbk」のファイルを、CC2000 v3.2 が稼働しているコンピューターにコピーしてください。このとき、サーバーが実行中であることを確認してください。

注意:	CC2000 v3.2 サーバーは、プライマリーサーバーとして実行されている必要があります。

8. CC2000Pro ユーティリティーを起動し、「**Restore**」(リストア)タブを開いてください。



9. 「**参照…**」をクリックして、拡張子が「*.cbk」のファイルを選択してください。

10. ツールから、パスワードの入力を求められたら、パスワードを入力して「**Start**」(開始)をクリックし、インポート(リストア)処理を開始してください。

11. インポート処理が完了したら、次の操作を行ってください。
    - ◆ CC2000 v3.2 サーバーにログインし、下記の点を確認してください。
      - ➢ ログのエクスポートファイルに関連項目(認証サーバー、ユーザータイプ、ユーザーアカウント、通知)が含まれているか。
      - ➢ デバイス接続設定(CC 管理設定、サーバーIP、デバイスポートなど)が含まれているか。
    - ◆ 元々、CC2000 v2.8 サーバーにあった CC2000 セカンダリーサーバーを検索し、これらを CC2000 v3.2 プライマリーサーバーに再登録してください。

移行に関する注意事項

- ユーザータイプ：一部のユーザーに対しては再設定が行われて、ユーザー定義のユーザータイプは「権限なし」に変更されます。こちらも、必要に応じて、バックアップデータをインポートした後に再確認と再設定を行ってください。
- フォルダー：CC2000 v3.2 において、フォルダーはサポートされません。フォルダーは全て削除され、これらのフォルダーに置かれていたデバイスはデバイスのルートに移動されます。
- イベント：一部のイベントは、CC2000 v3.2 で変更されます。削除したものは削除されたままですが、対応ログは保存され、表示することができます。
- 通知：削除されたイベントと、これに関連する通知は、いずれも削除されます。
- 割り当てられたデバイス：この機能は CC2000 v3.2 ではサポートされないため、削除されます。
- メンテナンス関連の設定：設定の範囲が変更されたことで、一部のメンテナンス設定（ログ、デバイスログイン、シリアルコンソール履歴、SNMP トラップの各オプション）も変更されます。アップデートされる範囲については、それぞれの項目に関連するセクションを参照してください。

第 3 章
ウェブブラウザーを使った操作

CC2000 はマルチプラットフォーム環境に対応し、大半の標準ウェブブラウザーからアクセスすることができます。ユーザーのログイン認証が完了すると、CC2000 のウェブブラウザーGUI メニューが表示されます。本章では、製品へのログイン方法や、CC2000 のウェブブラウザーGUI メニューの機能について説明します。

ログイン

CC2000 には以下の手順でログインしてください。

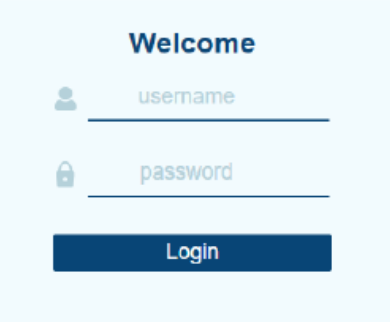
1. ウェブブラウザーを起動し、URL バーに CC2000 の IP アドレスを入力してアクセスしてください。
   デスクトップにショートカットを作成している場合は、これをダブルクリックすることで、デフォルトのブラウザーから CC2000 の URL にアクセスします。

   注意: HTTP ポートや HTTPS ポートの設定が管理者によって CC2000 のデフォルト(HTTP ポートは 8080、HTTPS ポートは 8443)以外の値に設定されている場合、IP アドレスの前に「**http://**」(非暗号化通信の場合)、または「**https://**」(暗号化通信の場合)を入力し、IP アドレスの後ろにポート番号を指定する必要があります。以下は、CC2000 サーバーの IP アドレスが「192.168.1.20」に設定されており、HTTPS 通信で「8443」番のポートを使ってアクセスする場合の URL の指定例です。

   https://192.168.1.20:8443

   IP アドレスとポート番号の間にはコロン(:)を入力してください。

2. 本製品の証明書は安全なものですので、セキュリティーの警告に関するダイアログが表示された場合はこれを許可してください。この場合の操作方法の詳細については p.325 をご参照ください。しばらくすると、下図のようなログイン画面が表示されます。

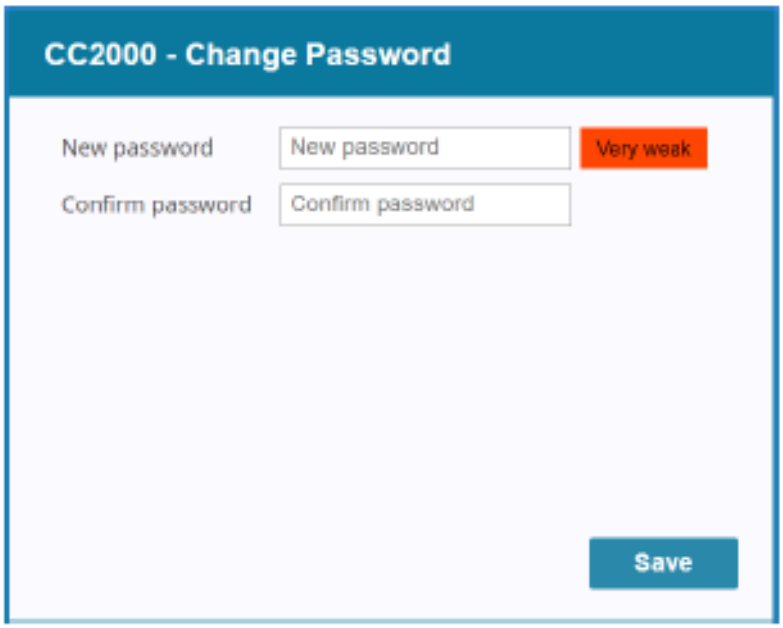


注意：	MOTP 認証または二要素認証を使用している場合は、p.43「MOTP または二要素認証を使ったログイン方法」を参照してください。

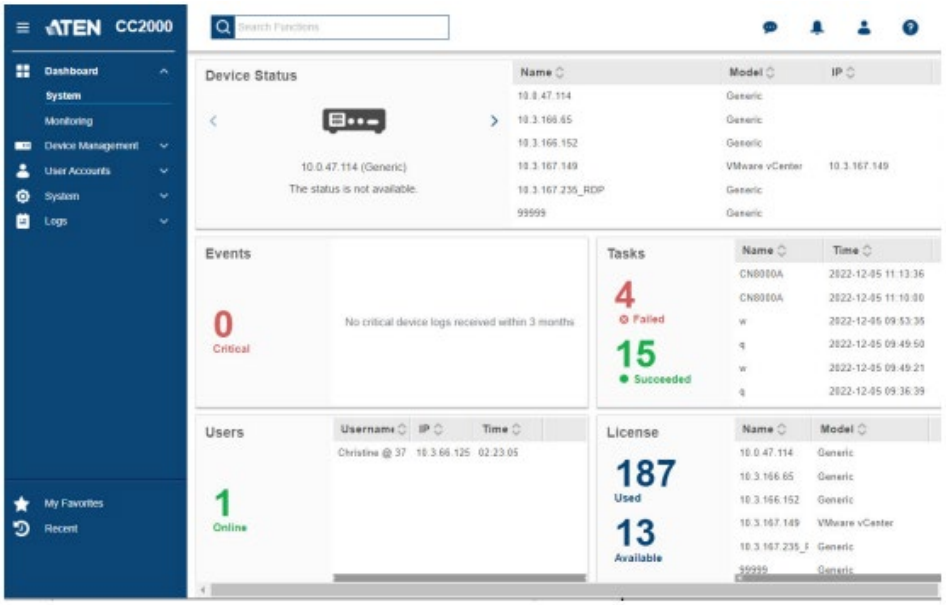
3. この画面にユーザーネームとパスワードを入力し、「**Login**」（ログイン）ボタンをクリックしてください。

注意：	CC2000 であらかじめ用意されているデフォルトユーザーのユーザーネームは「administrator」、パスワードは「password」です。

下図のような画面が表示され、システム側からログインパスワードの変更が求められます。



4. そうしたら、上から新規パスワード、確認用パスワードの順に入力を行い、「**Save**」（保存）ボタンをクリックしてください。いずれの項目も、半角英数字を使って最大 32 文字で設定することができます。
そうすると、システムはダッシュボードを表示します。



MOTP または二要素認証を使ったログイン方法

MOTP 認証

MOTP 認証を使用するように選択した場合、ログイン画面で要求されるのはユーザーネームの入力のみです。ユーザーネームを入力する際に、MOTP 認証ダイアログのウィンドウ画面が表示されます。そうしたら、画面内の指示に従い、MOTP 経由で認証を行ってください。

MOTP 認証の各種類に関する詳細は、p.224「二要素」を参照してください。

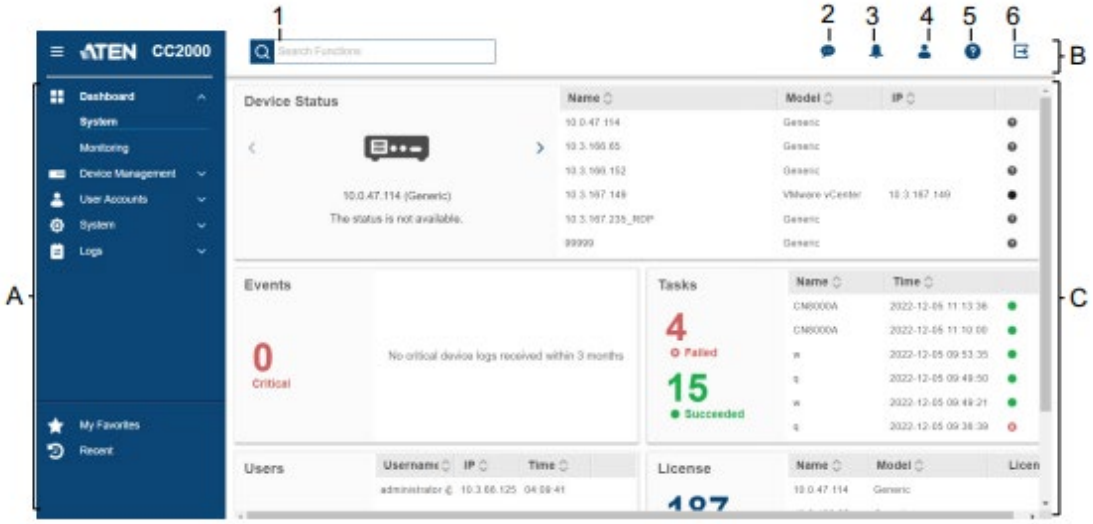
二要素認証

二要素認証を使用するように選択した場合、CC2000 ユーザーのユーザーネームとパスワードを入力する必要があります。この手順に続いて、MOTP 認証が行われます。

MOTP 認証または二要素認証に関する詳細は、p.214「認証サービス」にある「MOTP または二要素認証」のセクションを参照してください。

インターフェース

CC2000 の基本インターフェースと各部名称（セクションとアイテム）は、次の通りです。

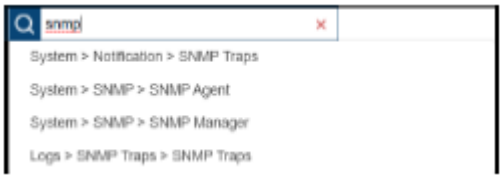


画面構成

CC2000 の画面構成は下表の通りです。

No.	項目	説明
A	サイドバーメニュー セクション	主にメニュー選択を行う部分です。参照や設定を行いたいメニューがある場合は、その項目をクリックして選択してください。また、さらに設定が行えるサブメニューがある場合は、このメニューを展開してください。
B	タスクバー セクション	ここには、検索、通知、個人設定（言語およびパスワード）、ヘルプ、ログアウトの各機能が提供されています。
C	相互表示パネル セクション	メインの作業エリアです。ここには、選択されたメニューバーやサイドバーで選択された項目に関連する内容が表示されます。このパネルの使用方法については、本章の後半で説明します。

（表は次のページに続きます）

No.	項目	説明
1	機能検索	CC2000 の機能検索を行います。 例えば、「SNMP」で検索を行いたい場合、検索バーにこの文字列を入力します。そうすると、SNMP に関連した機能が全て表示されます（下図参照）。目的の検索結果をクリックすると、その機能の設定画面に遷移します。 
2	オンラインチャット	このアイコンをクリックすると、チャットウィンドウが表示されます。詳細については p.53「チャット」を参照してください。
3	通知	通知がある場合は、ベル型のアイコンに通知件数が表示されます。 ここで表示される情報は、ユーザー権限によって異なります。 このアイコンをクリックすると、直近 50 件の通知が表示されます。内容は、重要ログ、警告ログ、システムメッセージで、最も新しいものから順に表示されます。 「Clean All」（全て消去）をクリックすると、通知を全て削除します。 「View Logs」（ログの参照）をクリックすると、システムログの画面に遷移します（p.289「システムログ」参照）。 「View message box」（メッセージボックスの参照）をクリックすると、メッセージボックスのウィンドウを表示します。メッセージボックスの使用方法については、p.50「メッセージボックス」を参照してください。

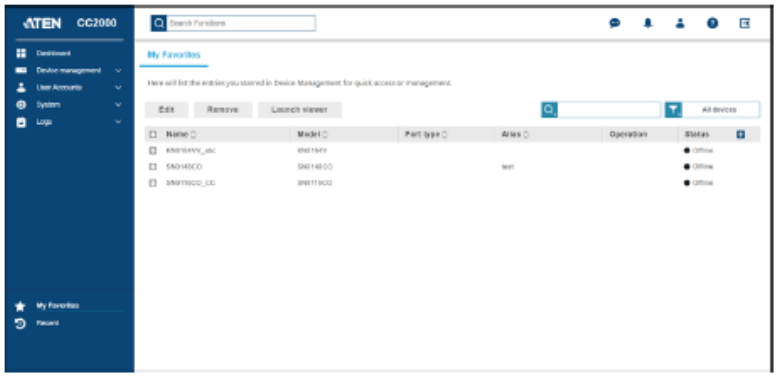
（表は次のページに続きます）

No.	項目	説明
4	個人情報	このアイコンをクリックすると、このセッションのユーザーネーム、最終ログイン日時、ユーザー設定オプション、およびパスワード変更オプションが表示されます。 「Preferences」（環境設定）をクリックすると、インターフェースの言語を変更したり、ログイン時に前回のログアウト状態で CC2000 を再開するかどうかを選択したりすることができます。 また、「Change Password」（パスワードの変更）をクリックすると、このユーザーのパスワードを変更します。
5	CC2000 について	このアイコンをクリックすると、CC2000 に関する情報を参照することができます。 「Help」（ヘルプ）をクリックすると、CC2000 のユーザーマニュアルにアクセスします。 「About」（CC2000 について）をクリックすると、お使いの CC2000 に関する情報が表示されます。
6	ログアウト	このアイコンをクリックすると、CC2000 のセッションからログアウトします。

お気に入り

「My Favorites」(お気に入り)画面は、ブックマークのような機能を提供します。頻繁にアクセスするデバイスやポートを、ここで選択したお気に入りの中に保存しておけば、この画面を開くことで、ポートをツリーから探すことなく、簡単にポートを選択することができます。これは特に、大規模システムに便利な機能です。

「**My Favorites**」(お気に入り)をクリックすると、下図のような画面が表示されます。

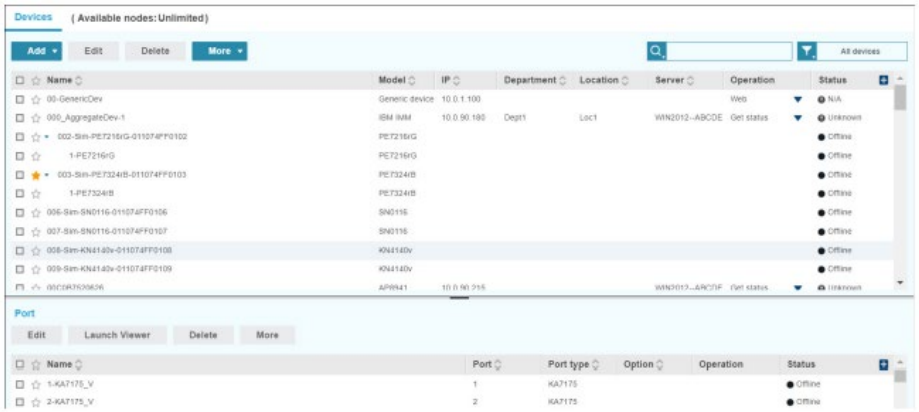


注意:	変更や操作の方法は、「Devices」(デバイス)サブメニューと同様です。詳細は p.70 「デバイス別 - 操作全般」を参照してください。

お気に入りの追加

お気に入りを作成するには、次の手順に従って操作を行ってください。

1. 「Devices」(デバイス)サブメニューを開いてください(「**Device Management**」(デバイス管理)→「**Devices**」(デバイス))。



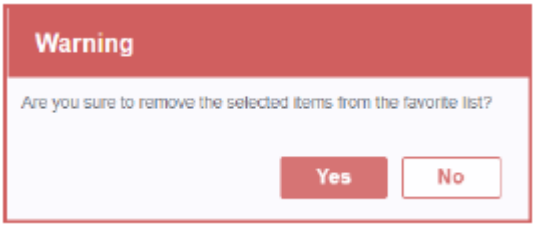
2. 「My Favorites」(お気に入り)に追加したいデバイスやポートを、デバイスリストやポートリストで探してください。

3. デバイスやポートの名前の左側に表示されている星型のアイコン(☆)をクリックしてください。

4. デバイスやポートがお気に入りへと正常に追加されると、星形のアイコンがオレンジ色に変わります(★)。

お気に入りの削除

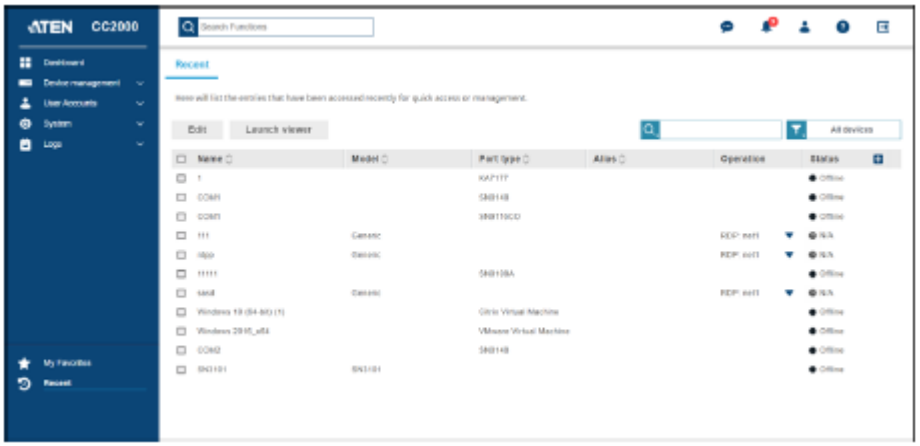
お気に入りからデバイスやポートを削除するには、対象となるデバイスやポートについているチェックボックスにチェックを入れて、「Remove」(削除)をクリックしてください。そうすると、システム側から、デバイスやポートを削除するかどうかが確認されます。削除を続行する場合は、「Yes」(はい)をクリックしてください。



最近使った項目

「Recent」(最近使った項目)画面は、履歴のような機能を提供します。ここには、過去にアクセスしたデバイスやポート(直近でアクセスした最大 100 のデバイスまたはポート)が一覧表示されるため、デバイスやポートを「Devices」(デバイス)サブメニューから探すことなく、簡単に選択することができます。これは特に、大規模で密なシステムに便利な機能です。

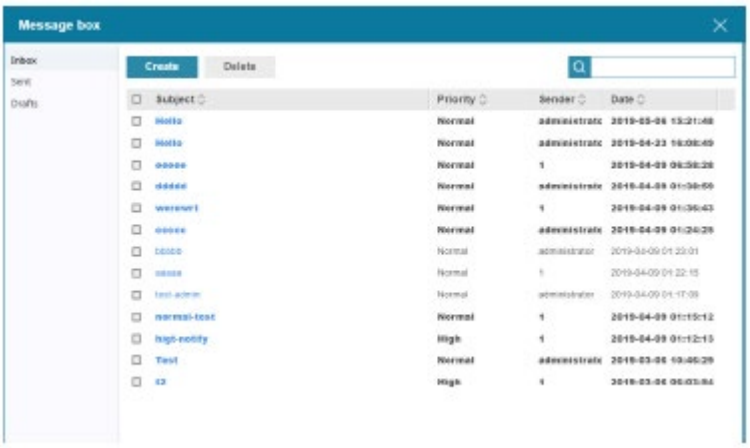
「Recent」(最近使った項目)をクリックすると、下図のような画面が表示されます。



注意： 変更や操作の方法は、「Devices」（デバイス）サブメニューと同様です。詳細は p.70 「デバイス別 - 操作全般」を参照してください。

メッセージボックス

「View Message Box」(メッセージボックスの参照)の後にある通知アイコンをクリックすると、メッセージボックス画面が表示されます。



注意:	「Sent」(送信済み)と「Draft」(下書き)の各オプションは、アドミニストレーターに操作が限定されています。

「Inbox」(受信トレイ)フォルダーでは受信メッセージを、「Sent」(送信済みトレイ)フォルダーは送信したメッセージを、また、「Draft」(下書き)フォルダーでは未送信のメッセージを、それぞれ確認することができます。

画面右上にある検索オプションを使うと、メッセージの絞り込み検索を行うことができます。

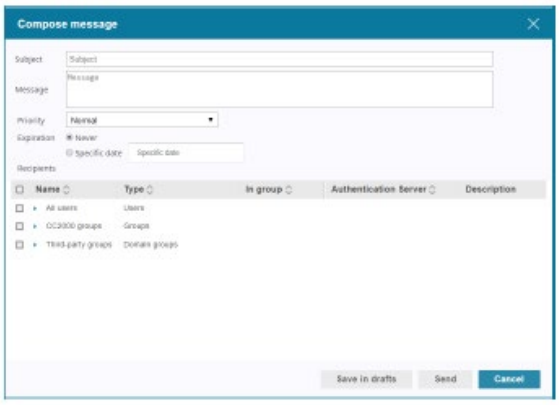
また、リストの列名をクリックすると、その項目順に並び替えて表示します。

受信トレイ

■通知の作成

通知を作成するには、次の手順に従って操作を行ってください。

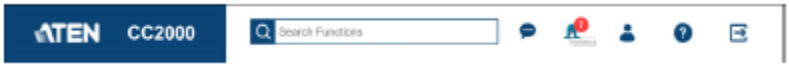
1. 「Create」(作成)をクリックしてください。そうすると、下図のような画面が表示されます。



2. 「**Subject**」(件名)と「**Message**」(メッセージ)の各欄に、メッセージの件名と本文をそれぞれ入力してください。
3. 「**Priority**」(優先度)ドロップダウンメニューを使って、優先度を選択してください。
4. 「**Expiration**」(期限)オプションを、「None」(なし)または「Specific date」(日付を指定)から選択してください。後者を選択した場合は、システムメッセージの期限となる日付を設定してください。
5. チェックボックスで「**Recepients**」(宛先)を選択してください(複数選択可)。宛先は、個々のユーザーを選択する矢印をクリックすることで、「Name」(名前)列を展開することができます。
6. 「**Save in drafts**」(下書きに保存)または「**Send**」(送信)をクリックしてください。
そうすると、メッセージがサイドバーの下書き、または送信済みトレイにコピーされます。

注意: 1. 優先度が高いメッセージは、ログイン時の最初の画面に表示されます(下図参照)。

2. 優先度が通常のメッセージは、通知アイコンで示されます(下図参照)。



■通知の削除

通知を削除するには、対象となる通知をチェックボックスで選択してから、「Delete」(削除)をクリックしてください(複数選択可)。そうすると、確認メッセージが表示されます。削除を続行する場合は「Yes」(はい)をクリックしてください。

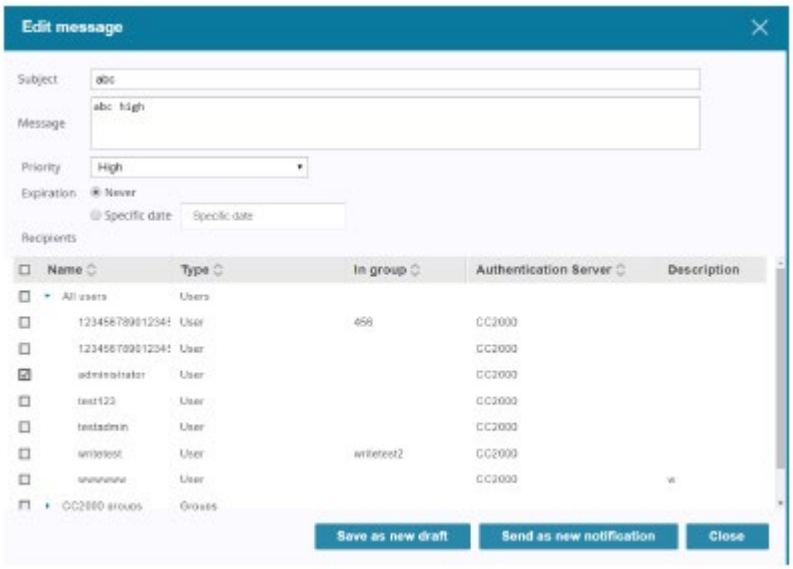
送信済みトレイ

「Sent」(送信済みトレイ)フォルダーをクリックすると、送信済みの通知を編集したり削除したりすることができます。

■送信済み通知の編集

通知を編集するには、次の手順に従って操作を行ってください。

1. 対象となる通知のチェックボックスにチェックを入れたら、「Edit」(編集)をクリックしてください。



2. 変更を加えたら、必要に応じて、「Save as new draft」(新規原稿として保存)または「Send as new notification」(新規通知として送信)のどちらかをクリックしてください。

■送信済み通知の削除

送信済みの通知を削除するには、対象となる通知をチェックボックスで選択してから、「Delete」(削除)をクリックしてください(複数選択可)。そうすると、確認メッセージが表示されます。削除を続行する場合は「Yes」(はい)をクリックしてください。

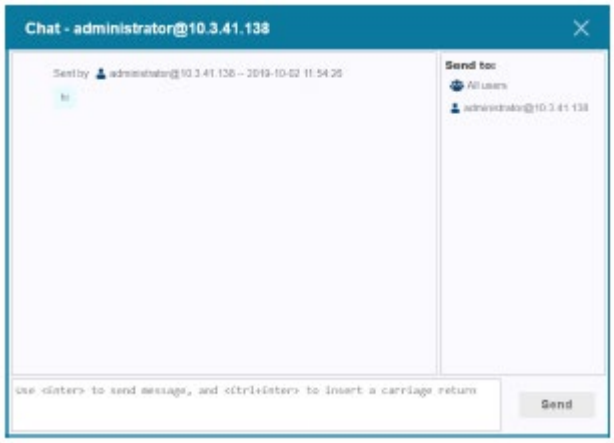
下書き

「Drafts」(下書き)フォルダーをクリックすると、未送信の通知を編集したり削除したりすることができます。

注意:	編集と削除の各オプションは、送信済みトレイで説明した内容と同じです。必要に応じて、p.52 を参照してください。

チャット

チャットアイコン( )をクリックすると、チャットパネルを表示します。下図は画面の一例です。



「Send to」(宛先)セクションには、現在オンライン状態のユーザーが一覧表示されます。チャットの相手となるユーザーをクリックして選択してください。ユーザーは、複数名を選択することができます。あるいは、「All users」(全てのユーザー)をクリックすると、全員宛にチャットメッセージを送信します。選択されたユーザーは強調表示されます(複数選択可)。

パネル右上にある「×」アイコンをクリックすると、チャット機能を終了します。

第 4 章
ダッシュボードと基本操作

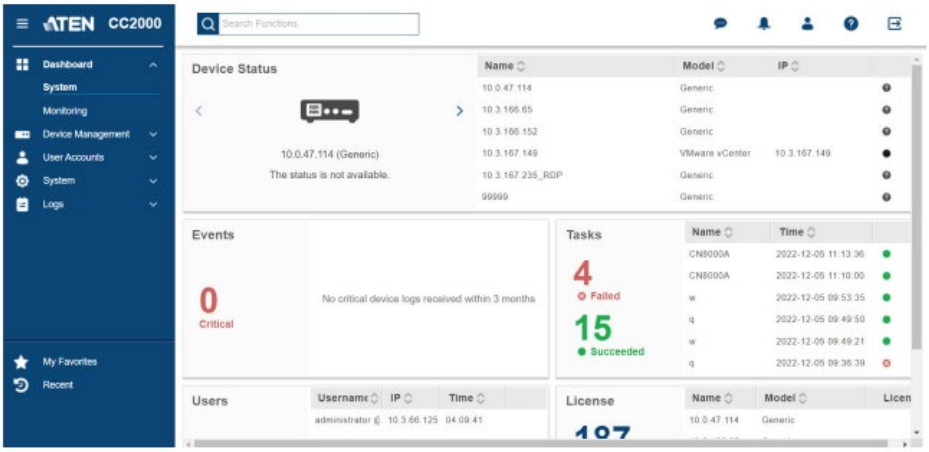
概要

ダッシュボードは、システムおよび監視対象となるポートや機器を視覚的に要約した情報を提供します。ここでは、現在のシステムの状態の概要を表示し、対処が必要となるクリティカルなイベントを強調表示します。詳しくは、次のセクションを参照してください。

- ◆ システムダッシュボード（次のセクション参照）
- ◆ ダッシュボードの監視（p.60 参照）

システムダッシュボード

次の情報パネルに分かれています。
「Device Status」（デバイスの状態）、「Events」（イベント）、「Users」（ユーザー）、「Tasks」（タスク）、「License」（ライセンス）



注意：	ダッシュボード画面へのアクセスは、スーパーアドミニストレーターとシステムアドミニストレーターに操作が限定されています。

デバイスの状態

システムに初めてログインすると、「Device Status」（デバイスの状態）パネルから、「Device Management」（デバイス管理）サイドメニューでデバイスを追加するよう促されます。

システムにデバイスが追加されると、このパネルに全てのデバイスの状態が一覧形式で表示されます。パネルの右側には先に述べた一覧が、また、左側にはデバイスの状態の詳細が、それぞれ表示されます。下図はその例です。

デバイスがオフライン状態であったり、ここで重要なイベントが発生したりすると*、このデバイスは左側に表示され、下にその状態が示されます。デバイスが複数ある場合は、デバイスの左または右に表示されている矢印をクリックすることで、表示するデバイスを切り替えることができます。

注意：	環境に関する情報が KN シリーズや SN シリーズのデバイスに切り替わると、ここに温度やファンのエラーも表示されます。

リストの列名をクリックすると、その項目順に並び替えて表示します。

また、リストの右端にある項目は、デバイスの状態を視覚的に表したものです。

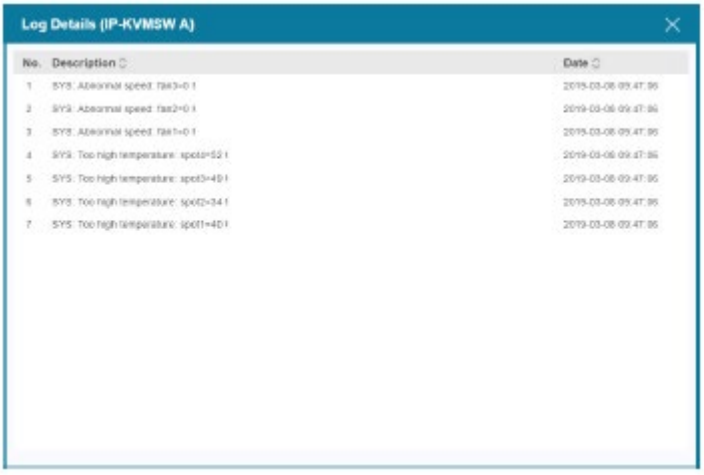
- オンライン状態
- オフライン状態
- エラー
- 不明

イベント

このパネルでは、システムが過去 3 か月の間に収集した重要なデバイスログを全て確認することができます。

左側の数字は、記録した重要なログの合計を表します。

特定のデバイスにおけるログを確認したい場合は、最後の列にある数字をクリックしてください。そうすると、詳細ログのウィンドウがポップアップ表示されます。下図はその例です。



タスク

このパネルには、過去3か月の間にスケジューリングされたタスクと、そのタスクの状態が表示されます。

赤色の数字は、スケジューリングされたタスクのうち、エラーになった件数を表します。

緑色の数字は、スケジューリングされたタスクのうち、成功した件数を表します。

ユーザー

このパネルには、現在オンライン状態であるユーザーが表示されます。下図はその例です。

左側の数字は、オンライン状態のユーザー数を表します。

この一覧では、オンライン状態のユーザーの詳細を確認することができます。

2 列目から最後の列には、セッション終了アイコン( )が表示されています。このアイコンをクリックすると、選択したユーザーをログアウトさせることができます。

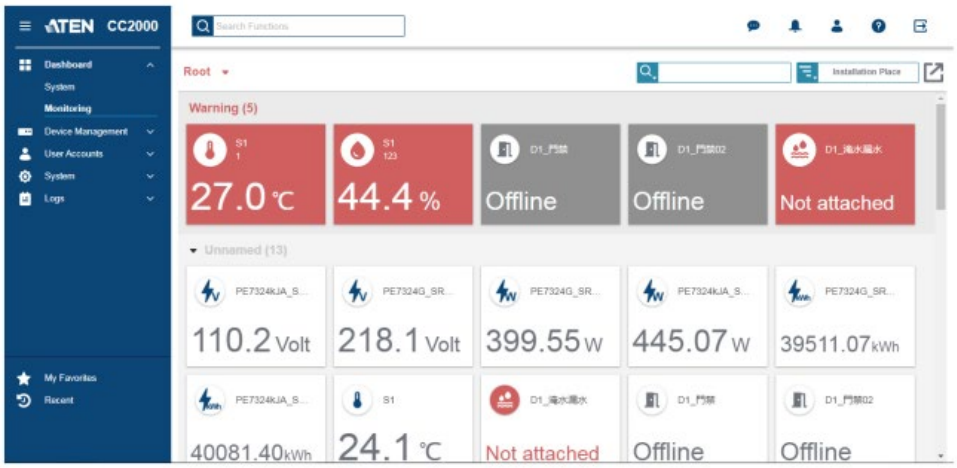
最後の列には、ユーザーアカウント無効アイコン( )が表示されます。このアイコンをクリックすると、選択したユーザーアカウントを無効にします。ユーザーアカウントを再度有効にする方法については、p.203「無効ユーザーの再有効化」を参照してください。

ライセンス

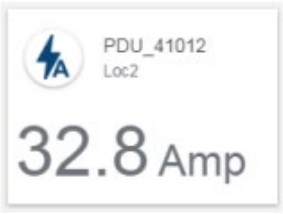
「License」(ライセンス)パネルには、使用済みノードと利用可能なノードの数が表示されます。下図はその例です。

ダッシュボードの監視

「監視」ダッシュボードは、監視対象となるポートおよび機器に関する情報を視覚的に要約して提供します（p.181「モニターアイテムの作成」参照）。

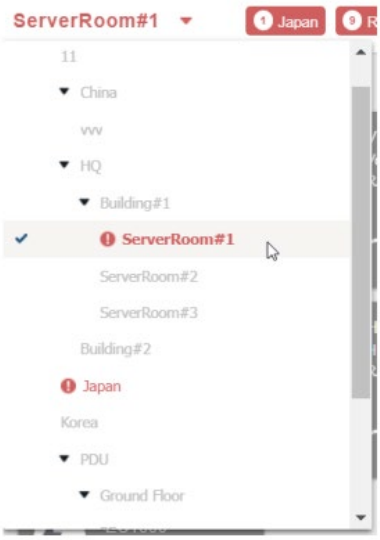


監視対象となるポート/機器それぞれに関する状態と値は、右の図のようにカードタイプのインターフェースで表示されます。



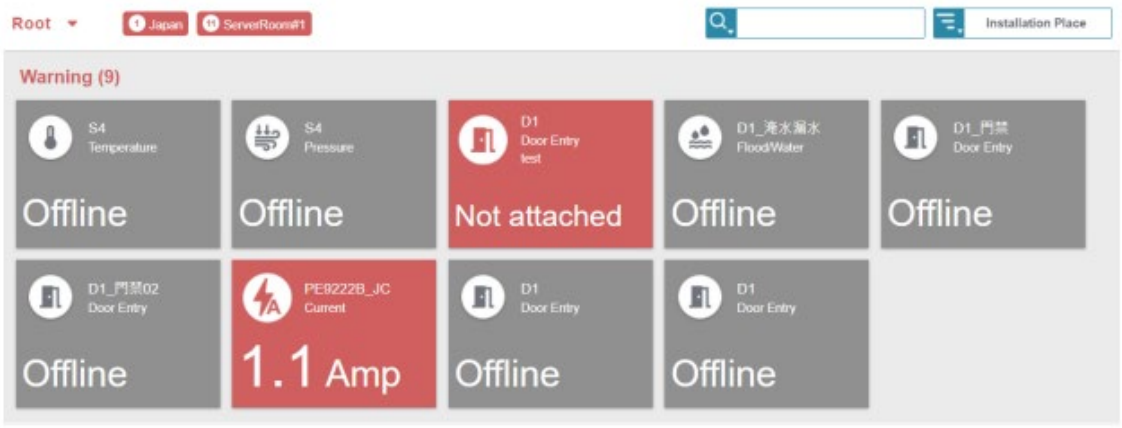
ダッシュボードを監視する階層やフォルダー間を移動する場合は、ドロップダウンメニューを操作してください。

表示された階層とフォルダーは「監視設定」画面で追加されたフォルダーの組織に基づいています。組織の設定については、p.182「フォルダーの追加」を参照してください。

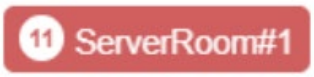


警告イベント

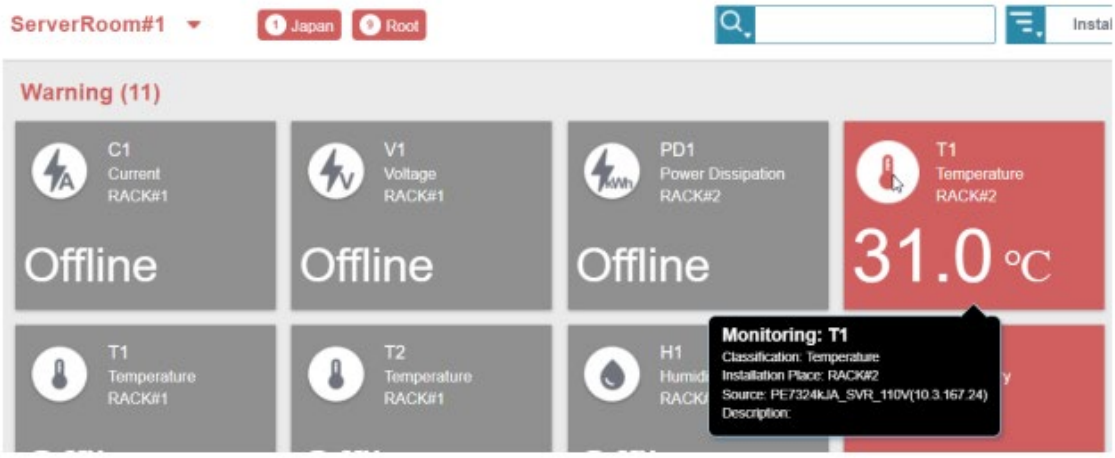
監視対象となるポートや機器において、しきい値の超過や警告状態（例:ドアの施錠解除）が検出されると、システムはこれを警告イベントであると認識して、ダッシュボードの上部バナーに警告を出したり、カードを赤色に変更させたりします。下図はその例です。



バナーには、警告イベントの総数と、これらのイベントを含むフォルダーの名前が表示されます。例えば、下図のバナーは「ServerRoom#1」の警告イベントが 11 件あることを表しています。

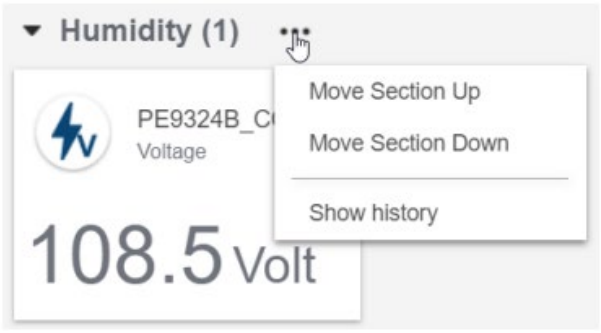


警告イベントの現在の状態を調べるには、バナーをクリックして該当する機器やポートのダッシュボードを開いてください。カードの上にマウスカーソルを移動させると、情報の詳細が表示されます。



カードの再配置

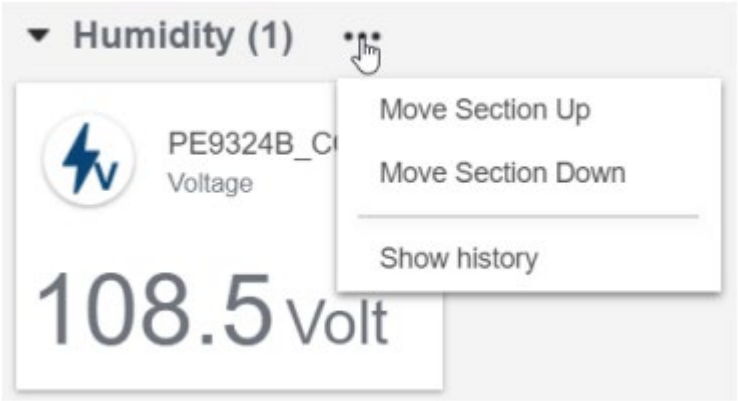
カードのセクションを再配置するには、「…」アイコンをクリックして「**セクションを上に移動**」または「**セクションを下に移動**」を選択してください。



セクション内にカードを再配置するには、カードをクリックしてドラッグし、移動先となる場所に動かしてドロップしてください。

分析チャートの確認

監視対象となるポートや機器のグループのトレンドチャートを確認するには、「…」アイコンをクリックして「**履歴の表示**」を選択してください。そうすると、トレンドチャートが表示されます。トレンドチャートに関する詳細は、p.185「監視機器のチャートを参照するには」を参照してください。

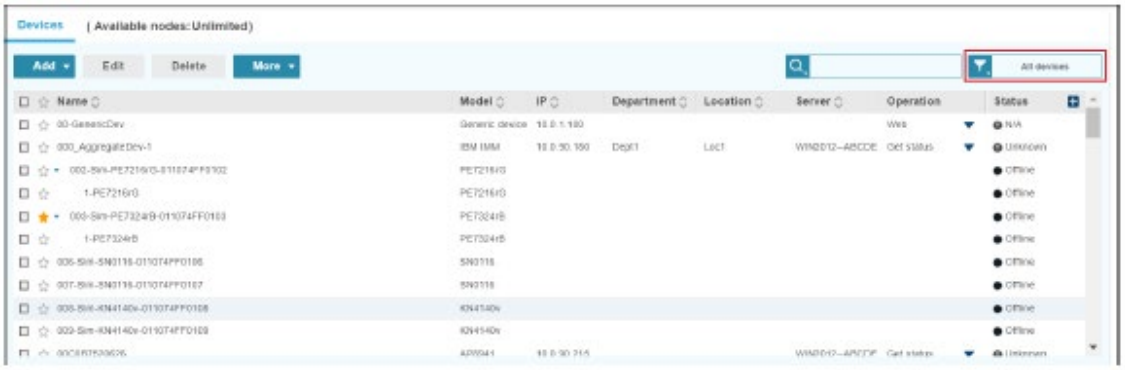


基本操作

基本操作の多くは CC2000 のインターフェース全体を通して確認することができます。方法については、この後のセクションでも説明していきます。

■フィルター

フィルター機能を使うと、表示するアイテムの数や種類を絞り込むことができます。この機能は、一覧の右上の端に提供されています。

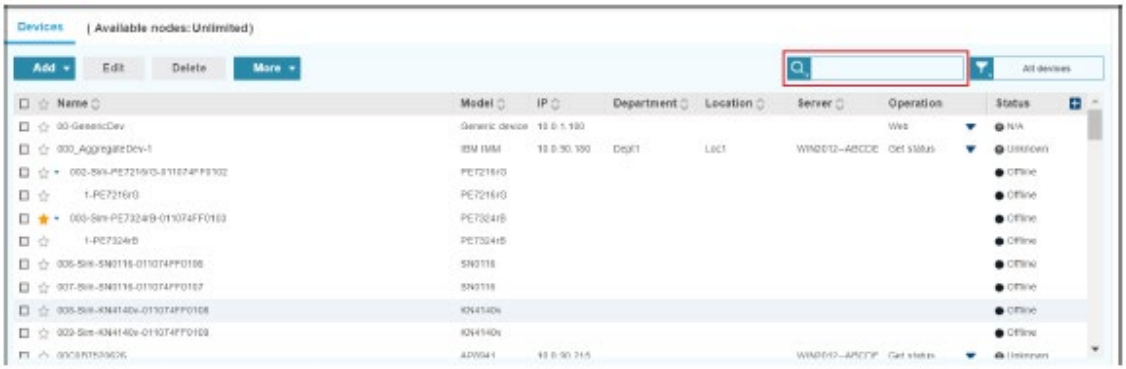


ドロップダウンメニューのフィルターバーをクリックすると、フィルターの各種オプションを確認することができます。下図はその例です。

表示したいアイテムに応じて、フィルターのオプションをクリックして選択してください。そうすると、選択されたフィルターの条件で、一覧を更新します。

■検索

この機能を使うと、検索オプションに関連したキーワードを使ってアイテムを検索することができます。この機能は、一覧の右上のフィルターの隣に提供されています。

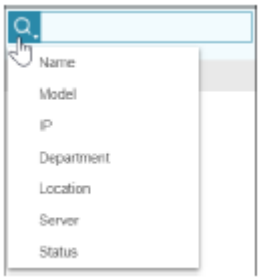


空欄のボックスに検索キーワードを入力し、[Enter]キーを押してください。

そうすると、指定されたキーワードの条件で検索し、一覧を更新します。下図はその例です。

中止アイコン( )をクリックすると、検索をキャンセルすることができます。一覧もこの操作に応じて更新されます。

検索結果を絞り込む場合は、虫眼鏡マークをクリックし、検索オプション一覧を表示させてください。



検索オプション(複数選択可)をクリックすると、検索対象となるカテゴリーを確認することができます。例えば、この図の場合、「Model」(型番)と「Location」(場所)にチェックを入れ、テキストボックス

に文字列を入力すると、この検索文字列に関連したアイテムを「Model」（型番）と「Location」（場所）のカテゴリーから検索します。

■一覧の列名

一覧の列名をクリックすると、その項目順に並び替えて表示します。

注意：	一覧の上にある見出しは、各表で全て表示されるわけではありません。参照したい列を追加する場合は「+」アイコンをクリックして、項目を選択してください。

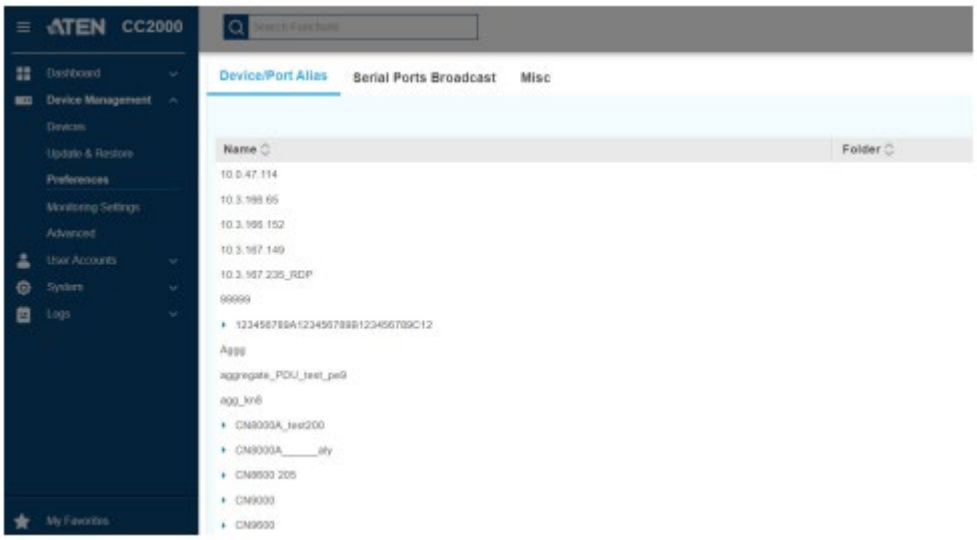
■編集/詳細オプション

「Edit」（編集）または「More」（詳細）の各オプションを使う代わりに、項目の上にカーソルを動かすと、鉛筆のアイコンやオプションのアイコンが表示されます。下図はその例です。

アイコンをクリックすると、ドロップダウンメニューが表示されます。設定を編集したい項目は、ここから選択してください。これらのオプションに関する詳細は、p.127「デバイスの編集」または p.137「詳細」を参照してください。

■相互表示パネルの編集

相互表示パネルで画面を編集すると、背景がグレーに変わる部分があります（下図参照）。これは、編集内容が保存されていないことをユーザーに知らせるものです。

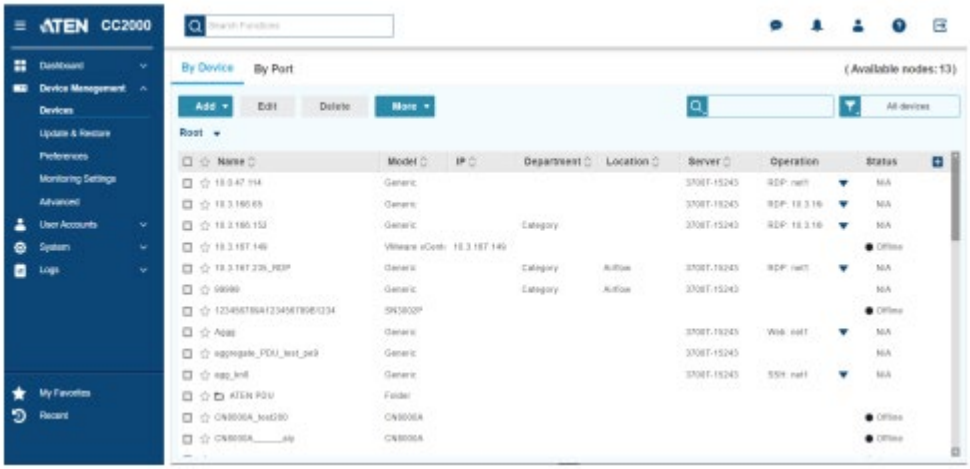


第 5 章
デバイス管理

概要

「Device Management」(デバイス管理)メニューでは、CC2000 配下で管理するデバイスの追加・設定・編成が可能です。

このメニューをクリックすると、下図のような「Devices」(デバイス)サブメニューのメインパネルが表示されます。



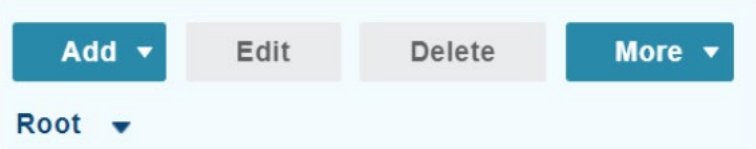
注意: 本章で説明する「Device Management」(デバイス管理)画面は、スーパーアドミニストレーター、システム管理者、ユーザー管理者、監査ユーザー向けの機能です。監査ユーザーは、このメニューのアイテムを参照することしかできません。また、デバイスへのアクセス権限が与えられているユーザーも、この画面にアクセスすることができます。

デバイスの相互表示パネルは、上下の画面に分かれています。

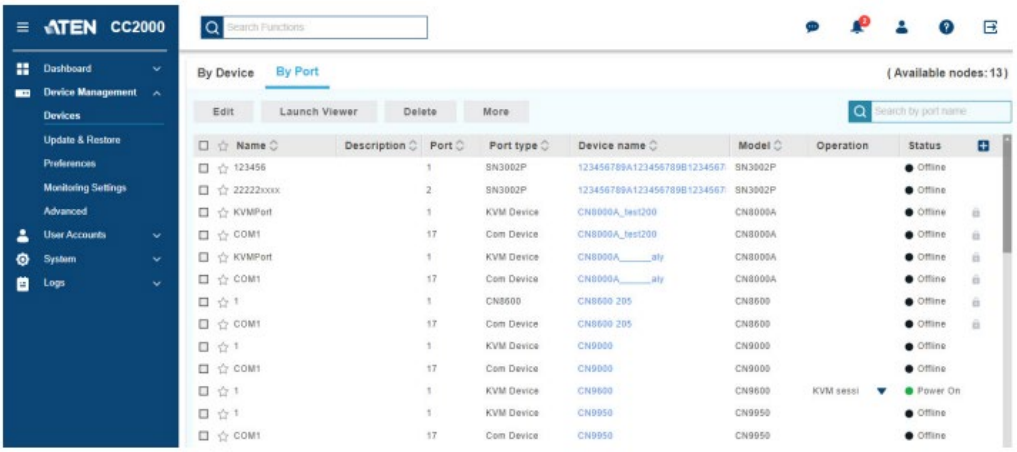
上部画面では、「**By Device**」(デバイス別)と「**By Port**」(ポート別)という 2 つのタブが利用可能です。

CC2000 サーバーで使用するように設定されているデバイス、およびデータベースに追加されているデバイスは全て、上部画面の「By Device」(デバイス別)タブに一覧表示されます。上図はその例です。

また、画面左上にあるボタンは、「By Device」(デバイス別)タブの操作全般に使用します。詳細については、p.70「デバイス別 - 操作全般」を参照してください。



追加されたデバイスのポートやアウトレットは全て、「By Port」(ポート別)タブに一覧表示されます。下図はその例です。



下の画面にも、選択されたデバイスのポートやアウトレットが一覧表示されます。上の画面でデバイスをクリックして強調表示すると、そのデバイスのポートやアウトレットが下の画面に表示されます。

「By Port」(ポート別)タブと下の画面の基本操作は下図の通りです。

詳細は p.160「ポート」を参照してください。

事前準備

デバイスの管理を始める前に、まず、これらをシステムに登録する必要があります。この操作は、4つの基本ステップで行われます。

1. 使用するデバイスをCC2000と同一のネットワークセグメント上にセットアップしてください。この手順は、プライマリーと各セカンダリーに対してそれぞれ行ってください。

2. デバイスが CC2000 と同一のネットワークセグメントに接続されると、そのセグメントを管理しているCC2000側で認識されます。CC2000側での認識は、そのデバイスにおける「ANMS」画面の「CC Management」機能(p.317「デバイスの ANMS 設定」参照)を有効にするか、「System Broadcast」(システムのブロードキャスト)の「Initialize devices IP/Port」(デバイス IP/ポートのイニシャライズ)機能(p.191「システムのブロードキャスト」参照)を使うことで可能になります。この機能を使うと、各セカンダリーはそれぞれ接続されているデバイスのプライマリーを認識します。

   注意:
   1. プライマリーの「Devices」(デバイス)画面において、「**Add**」(追加)→「**Auto Discovery**」(自動検出)をクリックすると、セカンダリーに接続されているものを含む全ての利用可能なデバイスが一覧表示されます。
   2. CC2000 に既に追加されているデバイスは、利用可能なデバイスの一覧には表示されません。

3. プライマリーの CC2000 ユニットから、手順 2 で認識されたデバイスを CC2000 に追加する必要があります(詳細は p.78 参照)。

4. 最後に、実在の物理ポートデバイスのポートを解除するか、複数のポートを組み合わせて論理デバイスの構成(アグリゲートデバイス、デバイス、グループデバイスなど)にすることで、デバイスを作成することができます。詳細については、p.95「デバイスの作成」をご参照ください。

VPN を使用する場合

CC2000 の管理機能を VPN(virtual private network)で使用する場合、プライマリーユニットが直接デバイスを認識しますので、そのネットワークセグメントを管理している CC2000 で認識させる必要はありません。CC 管理機能(デバイスの「ANMS」画面。p.317 参照)を有効にし、デバイスを認識させる CC2000 プライマリーの IP アドレスを入力することで、VPN の環境でも CC2000 を利用することができます。詳細については、p.318 をご参照ください。

デバイス別 – 操作全般

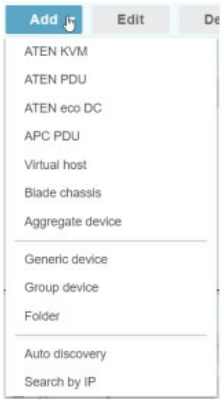
はじめに

デバイス一覧の列名

一覧の各列に関する説明は下表の通りです。

列名	説明
Name （名前）	CC2000 システムへの追加時に、このポートに設定された名前です。
Model （型番）	このデバイスの型番です。
IP Address （IP アドレス）	物理デバイスの場合、デバイスの IP アドレスが表示されます。
MAC Address （MAC アドレス）	物理デバイスの場合、デバイスの MAC アドレスが表示されます。
Alias （エイリアス）	ポートにエイリアス（別名）が付けられている場合は、その名前がここに表示されます。
Department（部署）	このデバイスが属している部署です。
Location （場所）	このデバイスが置かれている場所です。
Server（サーバー）	このデバイスが接続しているサーバーです。
Operation （操作）	このデバイスにアクセスする際のデフォルトの動作が、この欄に表示されます。 ◆ 一覧の枠の右にある矢印をクリックすると、他に利用可能なアクションを確認することができます。 ◆ このデバイスに対してセッションを開く方法をクリックして選択してください。デバイス操作の各種方法については、p.143「操作方法」で説明されています。
Type （種類）	このデバイスの種類です。
Status （状態）	◆ KVM デバイスやシリアルデバイスの場合は、ポートの状態（オンラインまたはオフライン）が表示されます。 ◆ PDU の場合は、アウトレットポートの電源ソケットの状態（オンまたはオフ）が表示されます。 ◆ ブレードシャーシの場合は、ポートの状態（オンライン、オフライン、不明のいずれか）が表示されます。

追加や設定が可能なデバイスタイプは、メインパネル上部にある「Add」(追加)ドロップダウンメニューで確認することができます。



各デバイスタイプとその使用目的に関する詳細は下表をご参照ください。

タイプ	目的
ATEN KVM	ATEN の Over IP 対応デバイスを CC2000 に追加する場合はこの種類を選択します。CC2000 では、ATEN の CN、CS、KH、KL、KN、PN、SN、PE の各シリーズのデバイスに対応しています。ここで言う「PE シリーズ」とは、ARM ベースの製品を指しています。 ARM ベースではない PE シリーズの製品を追加したい場合は、p.85「ATEN PDU の追加」にて詳細をご参照ください。 **注意:** デバイスが追加されると、追加されたポートはデフォルトではロックされていますので、これを解除する必要があります。詳細は、p.137「設定の移行」をご参照ください。デバイスを追加することによってポート数がライセンスで許可された数を超えてしまう場合でも、使用しないポートをこの機能でロックを解除し、空いたライセンスを新しく追加するポートに割り当てれば、ライセンスを新たに追加することなく運用を続けることができます。
ATEN PDU	CC2000 管理システムに PE シリーズのインテリジェント PDU を追加する場合は、これを選択してください。ここで言う「PE シリーズ」とは、ARM ベースの PE シリーズの製品を除きます。 ARM ベースの PE シリーズ製品を追加したい場合は、p.80「ATEN KVM の追加」にて詳細をご確認ください。

(表は次のページに続きます)

タイプ	目的
ATEN eco DC	CC2000 管理システムに eco DC を追加するには、これを選択してください。eco DC 自体は、ユーザーがウェブブラウザーから PDU の管理や操作を行うことができるウェブベースの GUI です。 ATEN eco DC の追加方法については、p.89「ATEN eco DC の追加」を参照してください。
APC PDU	CC2000 管理システムに APC PDU を追加するには、これを選択してください。CC2000 は単純なデバイス設定、Web SSO（シングルサインオン）および電源管理デバイス（AP79*xx*、AP89*xx*、AP86*xx* シリーズ）に対応しています。詳細はp.95「APC PDU の追加」を参照してください。
Aggregate Device（アグリゲートデバイス）	この種類を選択すると、CC2000 に追加された ATEN Over IP 対応デバイスや一部の SPM（例：IPMI、HP iLO2/3/5、IBM RSA II、Dell DRAC 5/6/8、Redfish が有効になっているデバイス）から選択されたポートで構成される論理デバイスを作成することができます。 このタイプのデバイスは、複数の接続方法で管理しているデバイス（例：KVM スイッチ、電源、シリアルポート）を 1 カ所にまとめて管理するものであるため、各々に対して個別に接続する必要がなくなります。各アグリゲートデバイスは構成されているポートの数にかかわらず 1 ノードとしてカウントされるため、このデバイスを作成しポートをこのデバイスに割り当てると、物理ライセンスの制限数を超える数のポートを管理することができます。詳細については p.110「アグリゲートデバイスの追加」をご参照ください。 **注意：** 1. アグリゲートデバイスに割り当てられているポートは、そのデバイス以外で使用することはできません。他のデバイスで使用する場合は、アグリゲートデバイスから削除する必要があります。 2. ポートがアグリゲートデバイスに割り当てられると、個別のポートとしては扱われなくなり、手動でロックしたりそれを解除したりすることもできなくなります。このポートを物理ポートとして扱いたい、また、このポートをグループに追加したい場合は、あらかじめこのアグリゲートデバイスから削除しておく必要があります。

（表は次のページに続きます）

タイプ	目的
Blade Chassis （ブレードシャーシ）	ブレードシャーシを追加する場合は、この項目を選択してください。
Virtual host （仮想ホスト）	VMware や Hyper-V や Citrix の仮想ホストを追加する場合は、この項目を選択してください。
Generic Device （ジェネリックデバイス）	Ethernet インターフェースを搭載し、URL や IP アドレスを指定して HTTP/HTTPS または Telnet/SSH 経由でアクセスできるデバイスであれば、ジェネリックデバイス(ルーターやスイッチなど)はサードパーティーのデバイスとして CC2000 からそのデバイスのメニューを呼び出すことができます。 ただし、これらのデバイスは CC2000 との併用を想定して設計されているわけではありませんので、CC2000 を使って認証を行ったり、CC2000 によるシングルサインオンの設定をしたりすることはできません。また、ジェネリックデバイスはデバイスノードライセンスの適用対象外となり、これらのデバイスに対する CC2000 のプロキシ機能もサポート対象外となります（p.320 参照）。 このタイプのデバイスを選択すると、CC2000 はこのデバイス自身にリダイレクトしますので、そのデバイスの認証手順に従ってログインしてください。 **注意：**ジェネリックデバイスがライセンスノード数に影響を与えることはありません。

（表は次のページに続きます）

タイプ	目的
Group Device (グループデバイス)	グループデバイスには、最大 64 のポートを追加することができます。グループデバイスも、実在する ATEN Over IP 対応デバイスに存在するポートをグループ化したものですが、アグリゲートデバイスとは以下の点において異なります。 物理ポートがアグリゲートデバイスに追加されると、そのポートは他のアグリゲートデバイスでは使用できないのに対し、グループデバイスには物理ポートをいくつでも追加することができます。 **注意:** 1. グループデバイスがライセンスノード数に影響を与えることはありません。 2. 複数のグループデバイスに追加された物理ポートは、所属しているグループデバイスの数にかかわらず 1 ライセンスとしてカウントされます。 3. グループデバイスと追加されたポートは、パネルアレイ表示で関連付けられます。詳細は、p.155「パネルアレイモード」を参照してください。

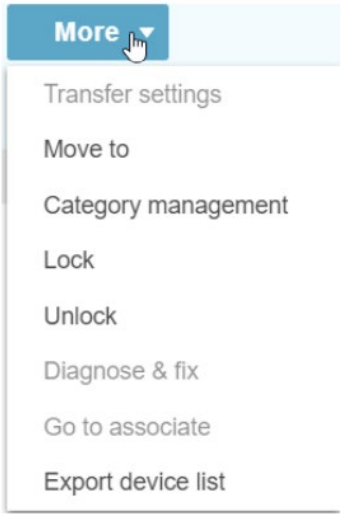
デバイスの追加方法については、p.78「デバイスの追加」を参照してください。

デバイスの編集を行う場合は、対象となるデバイスのチェックボックスにチェックを入れ、「**Edit**」(編集)をクリックしてドロップダウンメニューを展開してください。

デバイスの編集方法については、p.127「デバイスの編集」を参照してください。

デバイスの削除を行う場合は、対象となるデバイスのチェックボックスにチェックを入れ(複数選択可)、「**Delete**」(削除)をクリックしてください。

他にも利用可能な設定オプションがある場合は、ここで確認することができます。「More」（さらに表示）をクリックしてドロップダウンメニューを展開すると、下図のようなオプションが表示されます。



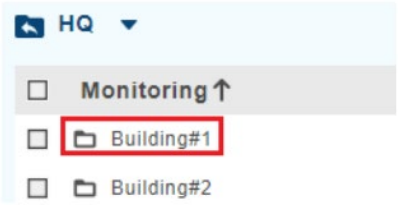
「More」（詳細）におけるオプションについては、p.137「詳細」を参照してください。

デバイスリストの操作

デバイスやフォルダーが、フォルダーやサブフォルダーを使って複数の階層で整理されている場合は、設定を行う際にデバイスリストを階層やレベル間で移動する必要が出てくるかもしれません。CC2000 では、デバイスリストで特定の階層やフォルダーに移動する方法をいくつか提供しています。

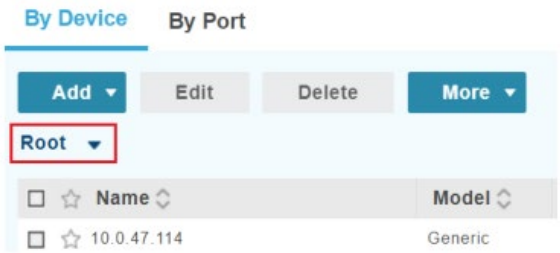
■特定の階層やフォルダーに移動するには

◆ デバイスリストで、対象となるフォルダーを直接ダブルクリックしてください。



◆ 対象となるフォルダーや階層を、デバイスツリーのドロップダウンメニューから選択してください。

1. 「**デバイス別**」タブで表示されるボタンをクリックして、デバイスツリーを開いてください。

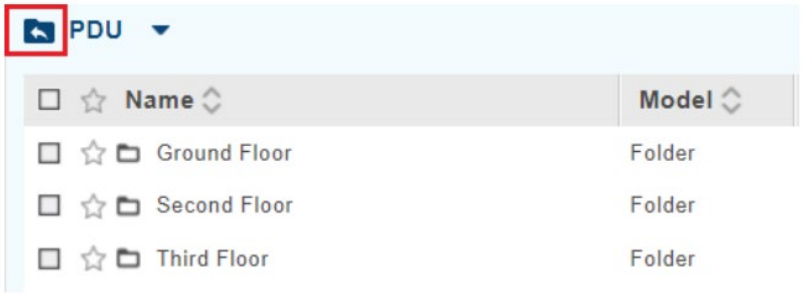


2. ポップアップメニューで、階層をクリックして選択してください。下図はその一例です。

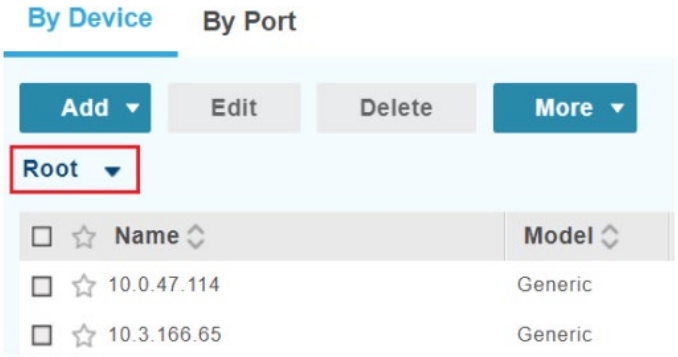
3. そうすると、選択されたフォルダーの表示に切り替わります。

■上の階層に戻るには

◆ 「戻る」アイコンをクリックしてください。



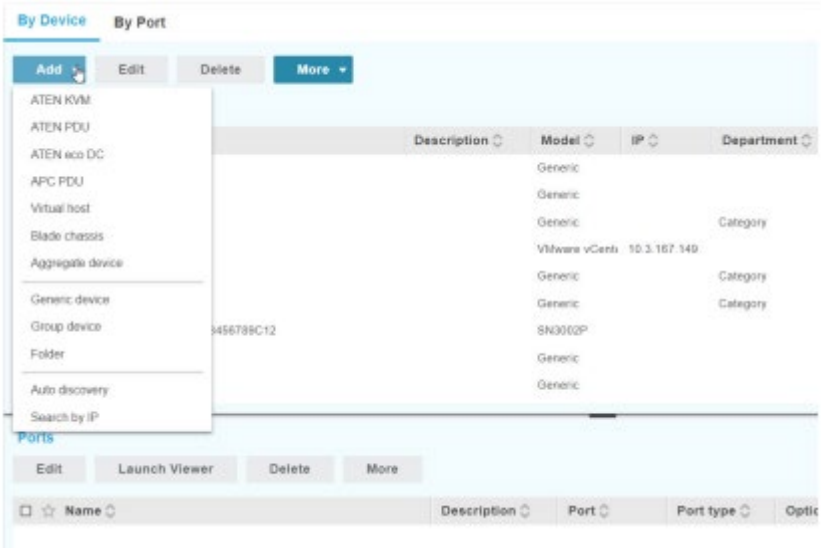
◆ デバイスツリーのドロップダウンメニューをクリックして、階層やフォルダーを選択してください。



デバイスの追加

デバイスを追加するには、次の手順に従って操作を行ってください。デバイスを追加する前に、フォルダーを作成しておくこともできます。詳しい方法については、p.79「フォルダーの追加」を参照してください。

1. 「Add」(追加)をクリックして、ドロップダウンメニューを展開してください。



2. 追加するデバイスタイプをリストから選択してください。そうすると、ウィンドウがポップアップ表示されます。表示インターフェースは、選択された項目に応じて異なります。各デバイスタイプの追加に関する詳しい情報は、次のセクションを参照してください。
   - p.80 「ATEN KVM の追加」
   - p.85 「ATEN PDU の追加」
   - p.89 「ATEN eco DC の追加」
   - p.95 「APC PDU の追加」
   - p.99 「仮想ホストの追加」
   - p.104 「ブレードシャーシの追加」
   - p.110 「アグリゲートデバイスの追加」
   - p.118 「ジェネリックデバイスの追加」

フォルダーの追加

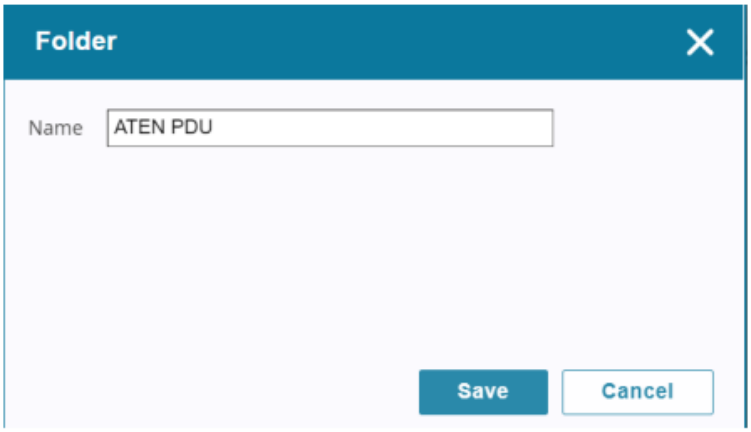
追加されたデバイスを、必要に応じて、タイプや場所、製品別に整理するために、フォルダーやサブフォルダーを作成することができます。フォルダーを追加するには、次のいずれかの方法で操作を行ってください。

■追加ボタン( )を使う方法

1. デバイスリスト画面で、対象フォルダーの上にマウスカーソルを移動させてください。
2. をクリックして、選択メニューを表示したら、「**フォルダー**」を選択してください。

■ナビゲーションメニューを使う方法

1. デバイスリスト画面で、フォルダーを追加したい階層またはフォルダーに移動してください。
2. Add をクリックしてください。
3. ポップアップメニューで「Folder」(フォルダー)をクリックしてください。そうすると、次の画面が表示されます。



4. フォルダーに名前を設定したら、「Save」(保存)をクリックしてください。

フォルダーの名前を編集するには、対象となるデバイスの上にマウスカーソルを移動させ、 をクリックして「Properties」(プロパティー)を選択してください。

ATEN KVM の追加

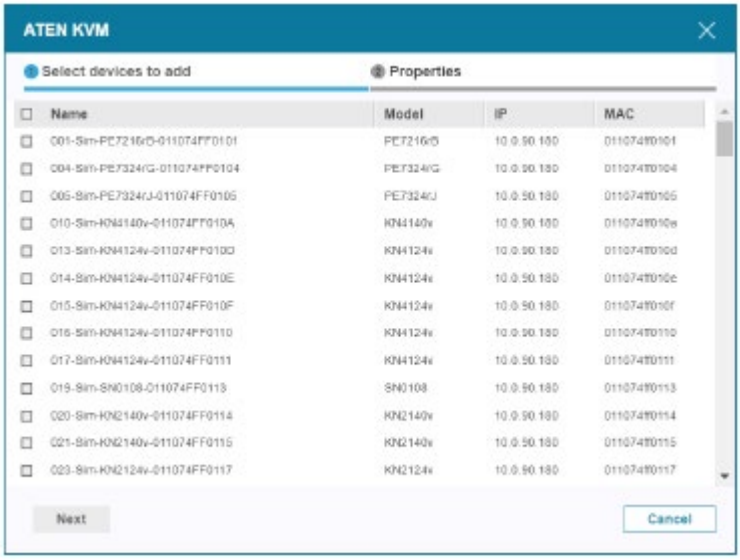
「Add」(追加)リストから「ATEN KVM」を選択すると、ATEN Over IP 対応デバイスを CC2000 に追加します。CC2000 では、ATEN の CN、CS、KH、KL、KN、PN、SN、PE(AEM ベースの製品)の各シリーズのデバイスに対応しています。

ARM ベースではない PE シリーズの製品を追加したい場合は、p.85「ATEN PDU の追加」で詳細をご参照ください。

注意:	ATEN Over IP 製品を CC2000 サーバーに追加する前に、そのデバイスが認識されていることを確認してください。詳細については p.69「事前準備」の内容をご参照ください。

ATEN KVM を追加する場合は、以下の手順で操作してください。

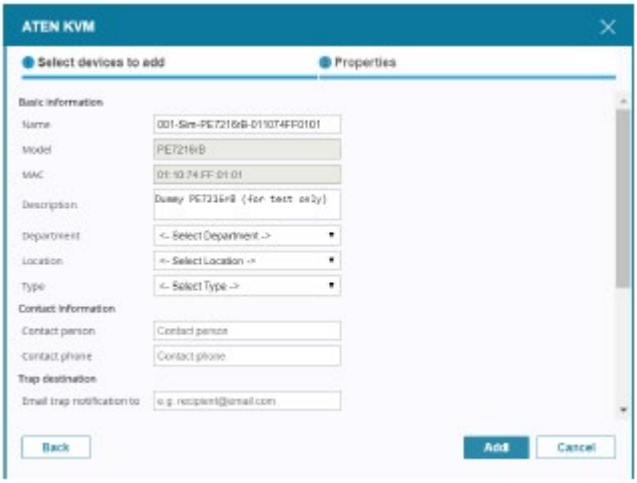
1. ドロップダウンメニューから「ATEN KVM」を選択してください。そうすると、追加可能なオンライン状態のデバイスが全て一覧表示されます。



制限については p.82 を、**CC2000 オプション**については p.83 を、それぞれ参照してください。

2. 追加するデバイスの隣にあるチェックボックスをクリックし、チェックを入れてください、

3. 「**Next**」(次へ)ボタンをクリックして、「Properties」(プロパティー)画面に遷移してください。



4. 下表の内容を参考にしながら、各項目を設定してください。

項目	説明
Basic Information （基本情報）	**Name（名前）**:デバイスの識別に使用する名前を設定してください。デフォルトでは、その製品にすでに与えられている名前が設定されます。ここで変更された名前は、CC2000 のデータベースには反映されますが、その製品自身の名前は変更されません。 **Model（モデル）**:デバイスタイプは CC2000 側で認識するため、この欄は自動的に設定されます。この欄は変更できません。デバイスが Cat 5e タイプの KVM スイッチである場合、コンピューターモジュールのモデルがこの欄に表示されます。 **MAC Address（MAC アドレス）**:CC2000 によって自動的に設定されるため、変更することはできません。 **Department（部署）**:企業内のシステムで使用する場合は部署別カテゴリー（例:R&D)を作成し、これにデバイスを割り当てることができます。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリスト（p.139「カテゴリーの管理」参照）を展開し、そのデバイスが所属するものをクリックしてください。

（表は次のページに続きます）

項目	説明
Basic Information （基本情報） (続き)	**Location（場所）**:企業内のシステムで使用する場合は地域別カテゴリー（例：西海岸)を作成し、これにデバイスを割り当てることができます。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリスト（p.139「カテゴリーの管理」参照）を展開し、そのデバイスが所属するものをクリックしてください。 **Type（タイプ）:**企業内のシステムで使用する場合はデバイスのタイプを作成し、これにデバイスを割り当てることができます。このデバイスをタイプに割り当てる場合は、あらかじめ作成しておいたタイプのリスト（p.139「カテゴリーの管理」参照）を展開し、そのデバイスが所属するものをクリックしてください。 **Description（説明）**:デバイスの詳細説明を設定する場合は、その内容をここに入力してください。この欄の設定はオプションです。
Contact Information （コンタクト情報）	このデバイスを管理するユーザーの名前および電話番号です。この欄の設定はオプションです。
Trap Destination （トラップ通知先）	トラップ通知の宛先となるユーザーのメールアドレスです。この欄の設定はオプションです。
Restrictions （制限）	**Hide IP Address from general users（一般ユーザーに対して IP アドレスを隠す）**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの IP アドレスをデバイス一覧に表示しなくなります。 **Hide MAC Address from general users（一般ユーザーに対して MAC アドレスを隠す）**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの MAC アドレスをデバイス一覧に表示しなくなります。

（表は次のページに続きます）

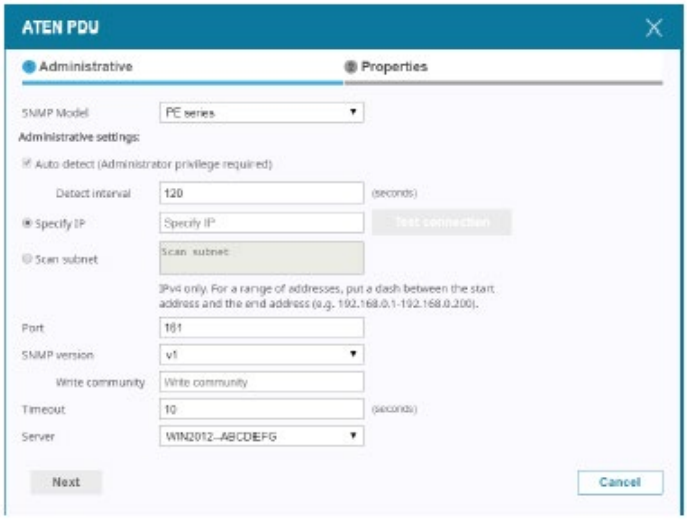
項目	説明
CC2000 Options （CC2000 オプション）	**Allow users to access the device through viewer or its web login page（ユーザーにビューワーまたはウェブログイン画面経由でのアクセスを許可する）**:セキュリティー対策として、この機能を無効にすると、デバイスは CC2000 経由でのログイン以外は受け付けなくなります。デバイスが CC2000 に接続されると、ユーザーはデバイス自身の認証システムにログインできなくなり、デバイスの管理も CC2000 のインターフェースを介して行われます。 **注意：** 1. このデバイスが CC2000 から切断されると、ユーザーはそのデバイスで提供されている認証システムを使ってログインできるようになります。 2. このチェックボックスにチェックを入れると、他の認証が有効になり、ユーザーはそのデバイスの認証システムを使ってログインできるようになります。 **Enable device logs to be sent to CC2000（CC2000 に対するデバイスログの送信を有効にする）**:この機能を有効にすると、CC2000 はデバイスのログサーバーとして機能し、受信したデバイスのイベント情報を記録して、このデータを検索できるようになります。 **Disable PDU local schedule（PDU ローカルスケジュールを無効にする）**:この機能を有効にすると、PDU のローカルスケジュールが無効になります。 **Device session timeout（デバイスセッションタイムアウト）**:セッションが何も入力を受信しないまま、ここで設定された時間が経過すると、このデバイスに対するウェブアクセスのセッションがタイムアウトとなります。この欄には、タイムアウトまでの時間を 2～99 秒で設定してください。0 で設定すると、セッションはタイムアウトしなくなります。

5.　項目を入力したら、「Add」（追加）ボタンをクリックして操作を完了してください。

注意：
- ◆ Cat 5 KVM スイッチの場合、コンピューターモジュールが接続されていて、かつ、オンライン状態のポートだけが認識されて、デバイスリストに追加されます。これは、それぞれのコンピューターモジュールが独自の ID を持っており、オフライン状態ではこれを認識することができないからです。ポートが追加された後は、オフライン状態でも一覧に表示されるようになります。
- ◆ ARM ベースの PE シリーズ PDU の追加がうまくいかない場合は、p.326「ARM ベースの PE シリーズ PDU の追加」にて詳しい内容を確認してください。

ATEN PDU の追加

「Add」(追加)リストから「ATEN PDU」を選択すると、ATEN PDU を CC2000 統合管理システムに追加します(複数追加可)。



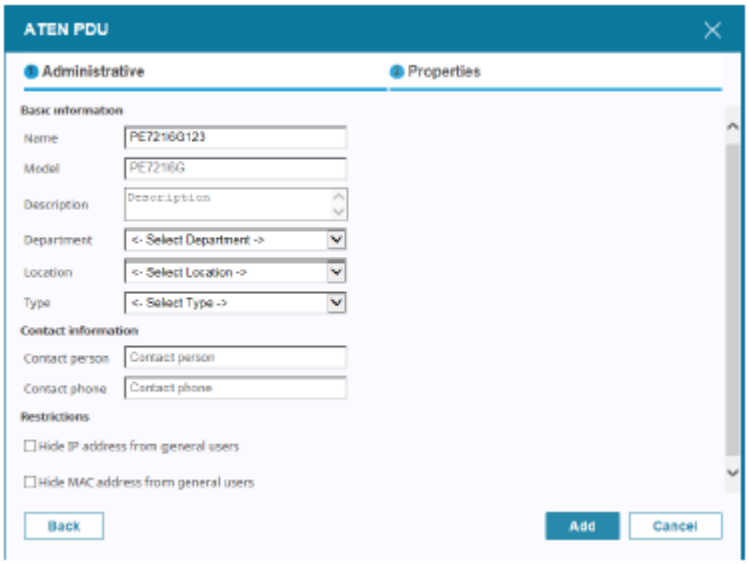
1. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
SNMP Model (SNMP モデル)	ここで言う「PE シリーズ」とは、ARM ベースではない製品を指しています。 **注意:** ARM ベースの PE シリーズの製品を追加したい場合は、p.80「ATEN KVM の追加」にて詳細をご参照ください。
Auto Detect (自動検出)	この機能を有効にすると、システムはデバイスがオンライン状態であるかどうかを自動的に確認します。 この機能は、管理権限を有するユーザーに操作が限定されています。 **注意:** ATEN PDU では、自動検出機能が常に有効になっています。
Detect Interval (検索インターバル)	検索を行うインターバルの秒数を30～300秒の範囲で設定してください。これは、システムがどのくらいの頻度でデバイスのオンライン状態を自動的に確認するかを定義します。
Specify IP (IP を指定)	デバイスの IP アドレスを入力してください。また、「**Test connection**」(接続のテスト)をクリックすると、IP が正しく検出されているかを確認することができます。

(表は次のページに続きます)

項目	説明
Scan subnet （サブネットのスキャン）	デバイスの検索条件として使用するサブネット IP アドレスの範囲を入力してください。
Port （ポート）	デバイスへのアクセスに使用するポート番号を入力してください。デフォルトのポート番号は、161 に設定されています。
SNMP version （SNMP バージョン）	SNMP バージョン（v1、v2c、v3 のいずれか）を選択してください。
Write community （書き込みコミュニティー）	SNMP バージョンによって必要になる場合は、コミュニティーの値を入力してください。
Timeout （タイムアウト）	サーバータイムアウトの値を入力してください。入力可能な値の範囲は 10～120 です。
Server （サーバー）	使用するサーバーを選択してください。

2. 画面への入力が完了したら、「**Next**」（次へ）をクリックしてください。そうすると、「Properties」（プロパティー）画面が表示されます。



3. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Device Information （デバイス情報）	**Name（名前）:**デバイスの識別に使用する名前を設定してください。 **Model（型番）:** CC2000 が認識している型番です。この項目は自動的に入力され、編集することができません。 **Description（説明）**:デバイスの詳細説明を設定する場合は、その内容をここに入力してください。この欄の設定はオプションです。 **Department（部署）**:企業内のシステムで使用する場合は部署別カテゴリー（例:R&D)を作成し、これにデバイスを割り当てることができます（p.139「カテゴリーの管理」参照）。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Location（場所）**:企業内のシステムで使用する場合は地域別カテゴリー（例:西海岸)を作成し、これにデバイスを割り当てることができます（p.139「カテゴリーの管理」参照）。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Type（タイプ）:**このデバイスのデバイスタイプをドロップダウンメニューから選択してください。
Contact Information （コンタクト情報）	デバイス管理者の名前および電話番号です。この欄の設定はオプションです。

（表は次のページに続きます）

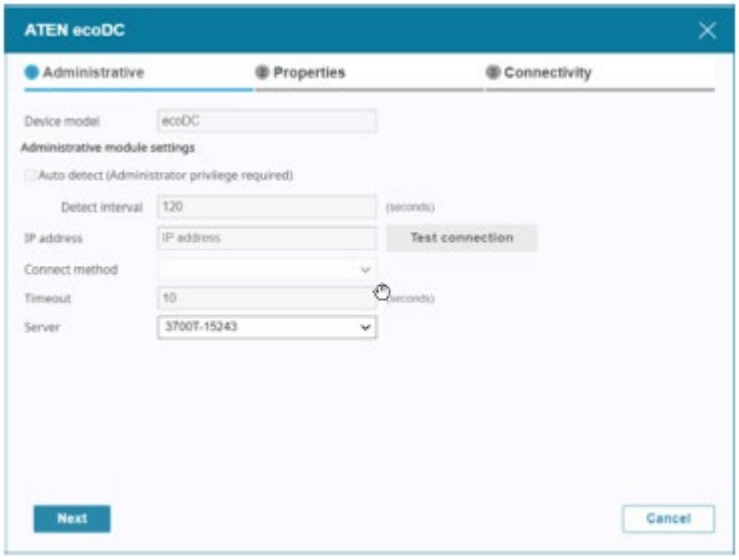
項目	説明
Restrictions （制限）	**Hide IP Address from general users（一般ユーザーに対して IP アドレスを隠す）**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの IP アドレスがデバイス一覧に表示されなくなります。 **Hide MAC Address from general users（一般ユーザーに対して MAC アドレスを隠す）**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの MAC アドレスがデバイス一覧に表示されなくなります。

4. 項目を入力したら、「**Add**」（追加）ボタンをクリックして操作を完了してください。

注意: デバイスが追加されたポートにはロックがかかります。詳細については p.141「デバイスのロックとロック解除」をご参照ください。

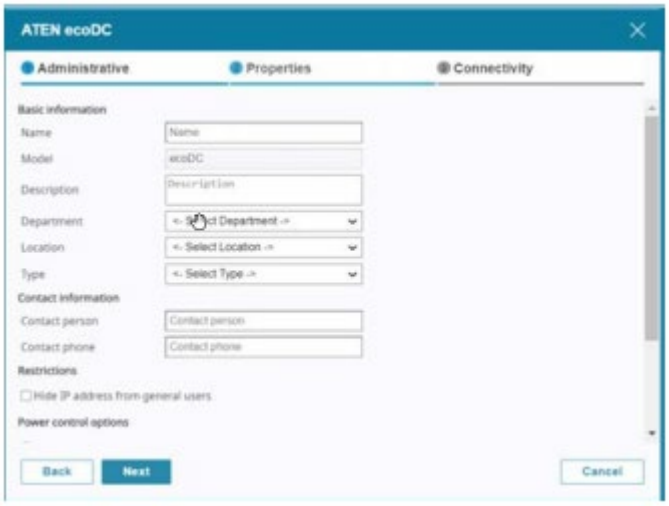
ATEN eco DC の追加

この画面を使うと、ATEN eco DC を CC2000 統合管理システムに追加します。



ATEN eco DC を追加するには、次の手順に従って操作を行ってください。

1. ドロップダウンメニューを使ってサーバーを選択したら、「**Next**」(次へ)をクリックしてください。そうすると、「Properties」(プロパティー)画面が表示されます。



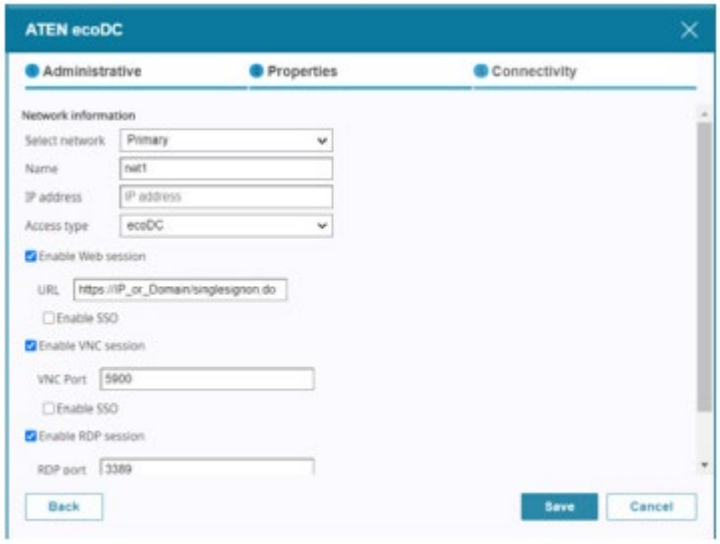
2. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Basic Information （基本情報）	**Name（名前）**: eco DC の識別に使用する名前を設定してください。 **Model（モデル）**:CC2000 側でサーバーを認識し、自動的に設定を行います。このため、この欄は変更できません。 **Description（説明）**:サーバーの詳細説明を設定する場合は、その内容をここに入力してください。この欄の設定はオプションです。 **Department（部署）**:企業内のシステムで使用する場合は部署別カテゴリー（例:R&D)を作成し、これにデバイスやサーバーを割り当てることができます。このサーバーを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリスト（p.139「カテゴリーの管理」参照）を展開し、そのサーバーが所属するものをクリックしてください。 **Location（場所）**:企業内のシステムで使用する場合は地域別カテゴリー（例:西海岸)を作成し、これにデバイスやサーバーを割り当てることができます。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリスト（p.139「カテゴリーの管理」参照）を展開し、そのサーバーが所属するものをクリックしてください。 **Type（タイプ）**:ドロップダウンメニューを使って、デバイスの種類を選択してください。
Contact Information （コンタクト情報）	このサーバーを管理するユーザーの名前および電話番号です。この欄の設定はオプションです。

（表は次のページに続きます）

項目	説明
Restrictions （制限）	**Hide IP Address from general users（一般ユーザーに対して IP アドレスを隠す）**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの IP アドレスをデバイス一覧に表示しなくなります。
Power Control Options （電源管理オプション）	次の説明に従って電源管理オプションを設定してください。 ◆ ボックスをクリックすると、電源操作の確認を有効にします。 ◆ ボックスをクリックすると、電源操作の遅延を有効にします。この場合は、「Power ON Delay」（電源 ON 遅延）、「Power OFF Delay」（電源 OFF 遅延）、「Power restart Delay」（電源再投入遅延）の各欄に、遅延する秒数を入力してください。

3. 画面への入力が完了したら、「**Next**」（次へ）をクリックしてください。そうすると、「Connectivity」（接続）画面が表示されます。



4. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Network Information （ネットワーク情報）	**Select network（ネットワークの選択）：**eco DC にネットワークインターフェースが 1 カ所しかない場合、「**Primary**」（プライマリー）を選択してください。ネットワークインターフェースが複数箇所ある場合は、「Primary」（プライマリー）の設定が完了した後、他のインターフェースの設定も順次行ってください。 **Name（名前）：**識別しやすくなるように、ネットワークインターフェースに対してそれぞれ名前を設定することができます。 **IP Address（IP アドレス）**：eco DC の IP アドレスをここに入力してください。 **Access Type（アクセスタイプ）：**ドロップダウンメニューからアクセスタイプを選択してください。

（表は次のページに続きます）

項目	説明
Web Session (ウェブセッション)	この項目にチェックを入れると、ウェブ操作を有効にします。 **URL:**ウェブ経由で eco DC にアクセスできるよう、管理画面にアクセスするための URL を入力してください。 **Enable SSO(シングルサインオンを有効にする):**SSO(シングルサインオン)機能を有効にするには、このボックスにチェックを入れてから、どの認証情報を使用するかを選択してください。 ◆ CC2000 のユーザーアカウントと同じアカウントのユーザーネームとパスワードを使用するには、「Use login user credentials」(ログインユーザー認証情報を使用する)を選択してください。 ◆ 新規に認証情報を作成するには、「Use following credentials」(以下の認証情報を使用する)を選択して、該当欄に認証情報を入力してください。 ◆ **Login name、Password(ログインネーム、パスワード):**これらの項目は、eco DC サーバーの認証や権限設定に基づいて設定を行ってください。
VNC Session (VNC セッション)	この項目にチェックを入れると VNC セッションを有効にします。 **VNC Port(VNC ポート):**VNC セッション用のポート番号を入力してください。 **Enable SSO(シングルサインオンを有効にする):**SSO(シングルサインオン)機能を有効にするにはこのボックスにチェックを入れてから、「View only」(参照のみ)および「Full control」(フル操作)の各パスワードを入力してください。

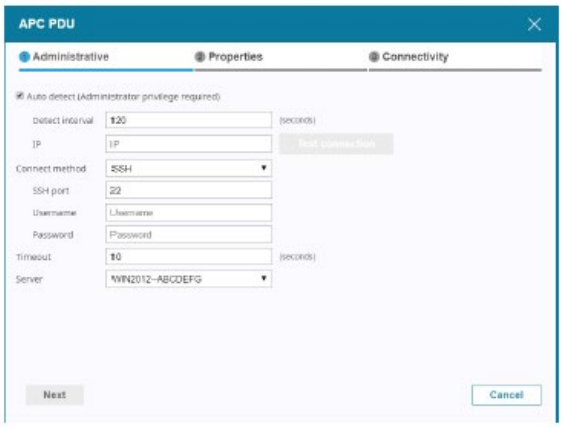
(表は次のページに続きます)

項目	説明
RDP Session (RDP セッション)	この項目にチェックを入れると RDP セッションを有効にします。 **RDP Port (RDP ポート) :** RDP セッション用のポート番号を入力してください。 **Always use local RDP client on Windows platform (Windows プラットフォームでは常にローカル RDP クライアントを使用する) :** この機能を有効にする場合は、チェックを入れてください。 **注意 :** この項目にチェックを入れると、SSO が無効になります。 **Enable SSO (シングルサインオンを有効にする) :** SSO (シングルサインオン) 機能を有効にするには、このボックスにチェックを入れてから、どの認証情報を使用するかを選択してください。 ◆ CC2000 のユーザーアカウントと同じアカウントのユーザーネームとパスワードを使用するには、「Use login user credentials」(ログインユーザー認証情報を使用する) を選択してください。 ◆ 新規に認証情報を作成するには、「Use following credentials」(以下の認証情報を使用する) を選択して、該当欄に認証情報を入力してください。

5. この画面での入力が完了したら、「**Save**」(保存) ボタンをクリックしてください。そうすると、システムは、ユーザーが ATEN eco DC に追加するデバイスを選択できる一覧を表示します。ATEN eco DC に関連付けたいデバイスやポートにチェックを入れて選択してください (複数選択可)。

APC PDU の追加

「Add」(追加)リストから「APC PDU」を選択すると、APC PDU を CC2000 統合管理システムに追加します。



APC PDU を追加するには、以下の手順で操作してください。

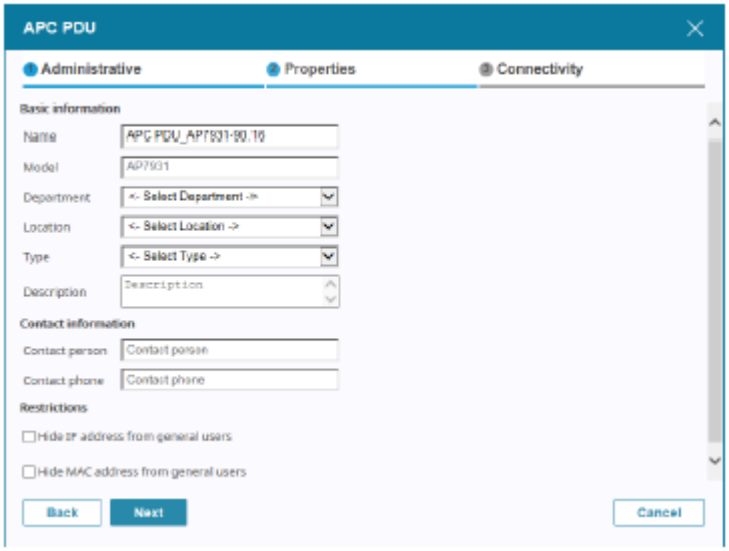
1. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Auto Detect (自動検出)	この機能を有効にすると、システムはデバイスがオンライン状態であるかどうかを自動的に確認します。 この機能は、管理権限を有するユーザーに操作が限定されています。
Detect Interval (検索インターバル)	検索を行うインターバルの秒数を設定してください。これは、システムが APC PDU のオンライン状況を自動的に確認する頻度を設定するパラメーターです。
IP	APC PDU の IP アドレスを入力してください。「**Test connection**」(接続のテスト)をクリックすると、IP が正しく検出されているかを確認することができます。
Connect Method (接続方法)	ドロップダウンメニューから SSH または Telnet のどちらかを選択してください。
SSH Port (SSH ポート)	(ブラウザー経由での)接続に使用するアクセスポート番号を入力してください。デフォルトのポート番号は、SSH ポートでは 22 に、また、Telnet では 23 に、それぞれ設定されています。

(表は次のページに続きます)

項目	説明
Username/Password (ユーザーネーム/パスワード)	APC PDU にアクセスするのに必要なユーザーネームとパスワードを入力してください(Telnet 経由のみ)。
Timeout (タイムアウト)	キャンセル前に接続リクエストが完了するのを待機する秒数です。
Server (サーバー)	APC PDU サーバーを接続している CC2000 を選択してください。

2. 画面の入力が完了したら、「**Next**」(次へ)をクリックしてください。そうすると、「Properties」(プロパティー)画面が表示されます。



3. 下表を参考にしながら、各欄に必要事項を入力してください。

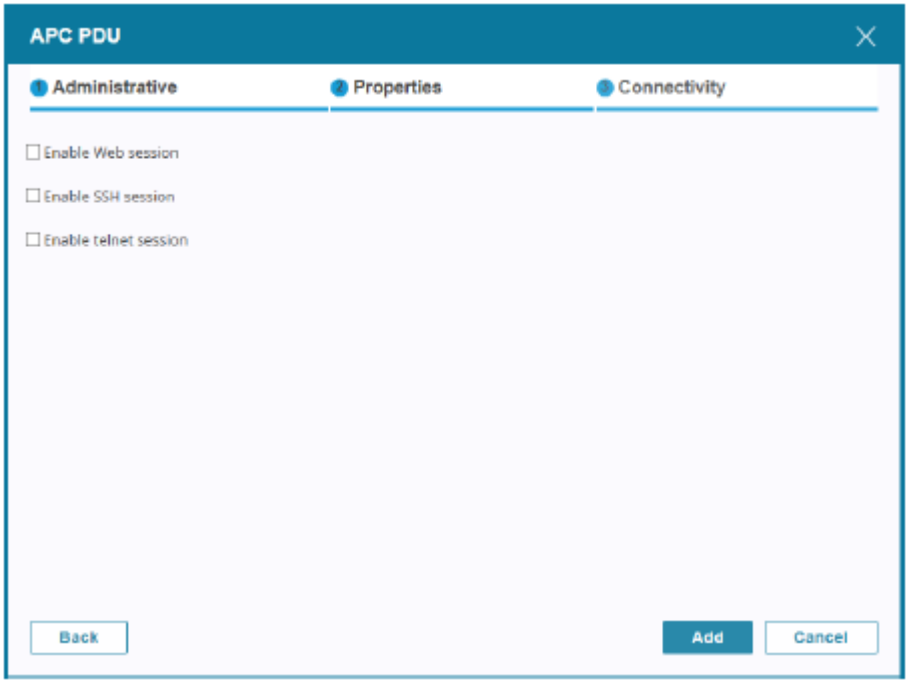
項目	説明
Device Information (デバイス情報)	**Name(名前)**:デバイスの識別に使用する名前を設定してください。 **Model(型番)**:CC2000 が認識している型番です。この項目は自動的に入力され、編集することができません。

(表は次のページに続きます)

項目	説明
Device Information （デバイス情報） （続き）	**Department（部署）**：企業内のシステムで使用する場合は部署別カテゴリー（例：R&D)を作成し、これにデバイスを割り当てることができます（p.139「カテゴリーの管理」参照）。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Location（場所）**：企業内のシステムで使用する場合は地域別カテゴリー（例：西海岸)を作成し、これにデバイスを割り当てることができます（p.139「カテゴリーの管理」参照）。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Type（タイプ）**：このデバイスのデバイスタイプをドロップダウンメニューから選択してください。 **Description（説明）**：デバイスの詳細説明を設定する場合は、その内容をここに入力してください。この欄の設定はオプションです。
Contact Information （コンタクト情報）	デバイス管理者の名前および電話番号です。この欄の設定はオプションです。
Restrictions （制限）	**Hide IP Address from general users（一般ユーザーに対して IP アドレスを隠す）**：セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの IP アドレスがデバイス一覧に表示されなくなります。 **Hide MAC Address from general users（一般ユーザーに対して MAC アドレスを隠す）**：セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの MAC アドレスがデバイス一覧に表示されなくなります。

4. 画面への入力が完了したら、「**Next**」（次へ）をクリックしてください。「Connectivity」（接続）画

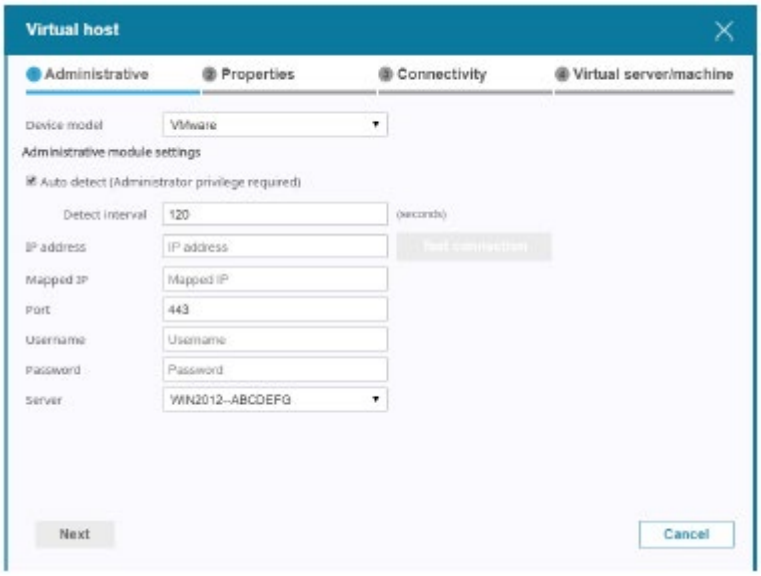
面が表示されたら、「Enable Web session」(ウェブセッションを有効にする)、「Enable SSH session」(SSH セッションを有効にする)、「Enable telnet session」(Telnet セッションを有効にする)の項目のうち、有効にしたいものにチェックを入れてください。



5. 項目を入力したら、「Add」(追加)ボタンをクリックして操作を完了してください。

仮想ホストの追加

「Add」(追加)リストから「Virtual host」(仮想ホスト)を選択すると、仮想ホストを CC2000 統合管理システムに追加します。



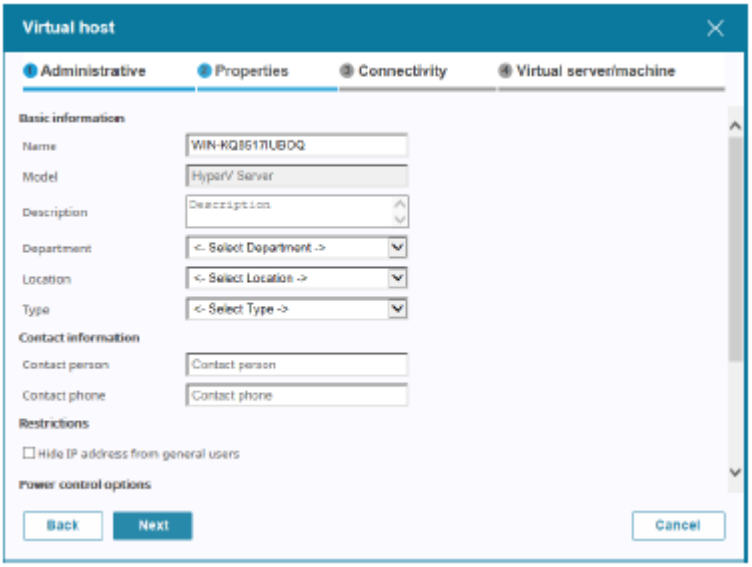
1. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Device Model (デバイスモデル)	ドロップダウンメニューから、VMware、Citrix、Hyper-V のいずれかを選択してください。
Auto Detect (自動検出)	この機能を有効にすると、CC2000 はこの仮想マシンがオンラインかどうかを自動的に確認します。 この機能は、管理権限を有するユーザーに操作が限定されています。
Detect Interval (検索インターバル)	検索を行うインターバルの秒数を設定してください。これは、システムが仮想マシンのオンライン状況を自動的に確認する頻度を設定するパラメーターです。
IP Address/Port (IP アドレス/ポート)	ブラウザー経由での接続に使用される仮想マシンの IP アドレスとアクセスポートを入力してください。デフォルトのポートは 443 に設定されています。「Test connection」(接続のテスト)をクリックすると、IP やポートが正しく検出されているかを確認することができます。

(表は次のページに続きます)

項目	説明
Mapped IP (割り当てられた IP)	この機能は、VMware のリモートコンソール対応のためのものです(ルーターやファイアウォール経由での VMRC)。 この機能を有効にするには、この欄に仮想ホストの外部 IP アドレスを入力してください。
Username/Password (ユーザーネーム/ パスワード)	仮想マシンに(ウェブブラウザー経由で)アクセスするのに必要となるユーザーネームとパスワードを入力してください。
Server (サーバー)	仮想ホストのサーバーを接続している CC2000 を選択してください。

2. 画面の入力が完了したら、「**Next**」(次へ)をクリックしてください。そうすると、「Properties」(プロパティー)画面が表示されます。



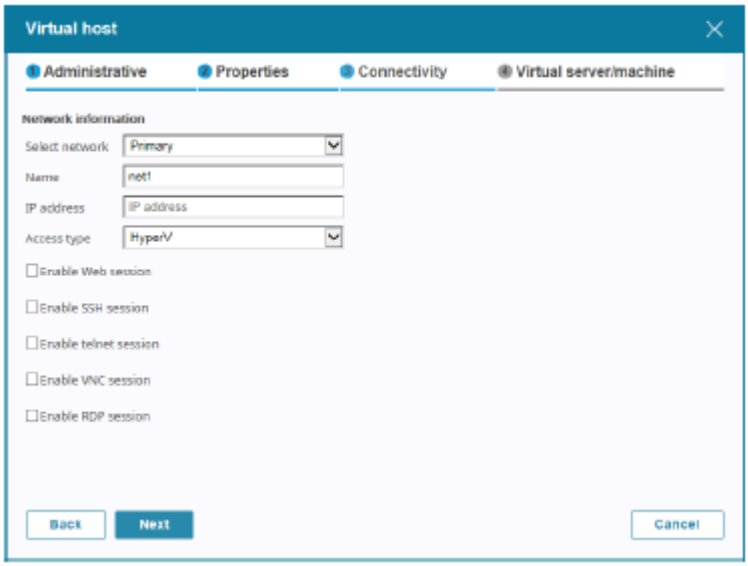
3. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Device Information (デバイス情報)	**Name(名前)**:デバイスの識別に使用する名前を設定してください。 **Model(型番)**:CC2000 が認識している型番です。この項目は自動的に入力され、編集することができません。

(表は次のページに続きます)

項目	説明
Device Information (デバイス情報) (続き)	**Department (部署)**:企業内のシステムで使用する場合は部署別カテゴリー (例:R&D)を作成し、これにデバイスを割り当てることができます(p.139「カテゴリーの管理」参照)。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Location (場所)**:企業内のシステムで使用する場合は地域別カテゴリー (例:西海岸)を作成し、これにデバイスを割り当てることができます(p.139「カテゴリーの管理」参照)。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Type (タイプ)**:このデバイスのデバイスタイプをドロップダウンメニューから選択してください。
Contact Information (コンタクト情報)	デバイス管理者の名前および電話番号です。この欄の設定はオプションです。
Restrictions (制限)	**Hide IP Address from general users (一般ユーザーに対して IP アドレスを隠す)**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの IP アドレスがデバイス一覧に表示されなくなります。 **Hide MAC Address from general users (一般ユーザーに対して MAC アドレスを隠す)**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの MAC アドレスがデバイス一覧に表示されなくなります。

4. 画面への入力が完了したら、「**Next**」(次へ)をクリックしてください。そうすると、「Connectivity」(接続)画面が表示されます。



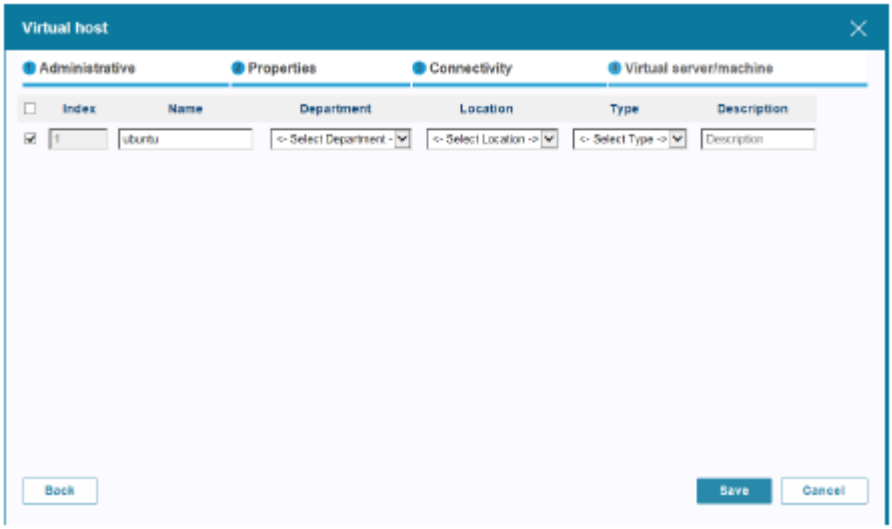
5. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Network Information (ネットワーク情報)	**Select network (ネットワークの選択) :** 仮想ホストのサーバーにネットワークインターフェースが 1 カ所しかない場合、「**Primary**」(プライマリー)を選択してください。ネットワークインターフェースが複数箇所ある場合は、「Primary」(プライマリー)の設定が完了した後、他のインターフェースの設定も順次行ってください。 **Name (名前) :** 識別しやすくなるように、ネットワークインターフェースに対してそれぞれ名前を設定することができます。 **IP Address (IP アドレス)** : 仮想ホストの IP アドレスをここに入力してください。 **Access Type (アクセスタイプ) :** ドロップダウンメニューからアクセスタイプを選択してください。

(表は次のページに続きます)

項目	説明
Enable Web session （ウェブセッションを有効にする） Enable SSH session （SSH セッションを有効にする） Enable telnet session （Telnet セッションを有効にする） Enable VNC session （VNC セッションを有効にする） Enable RDP session （RDP セッションを有効にする）	有効にしたいセッションがあれば、該当項目にチェックを入れてください。

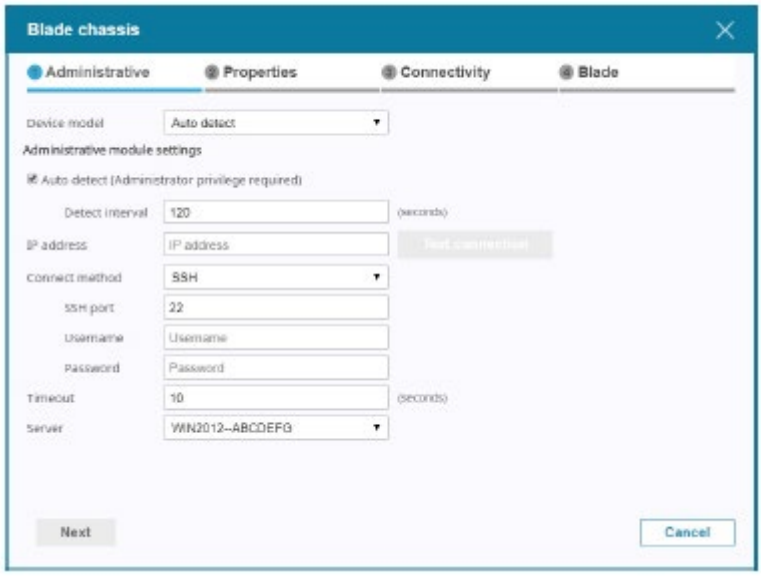
6. 画面への入力が完了したら、「**Next**」（次へ）をクリックしてください。そうすると、「Virtual server/machine」（仮想サーバー/マシン）画面に遷移します。



7. 項目にチェックを入れたら、「**Save**」（保存）ボタンをクリックして操作を完了してください。

ブレードシャーシの追加

「Add」(追加)リストから「Blade chassis」(ブレードシャーシ)を選択すると、ブレードシャーシをCC2000 統合管理システムに追加します。



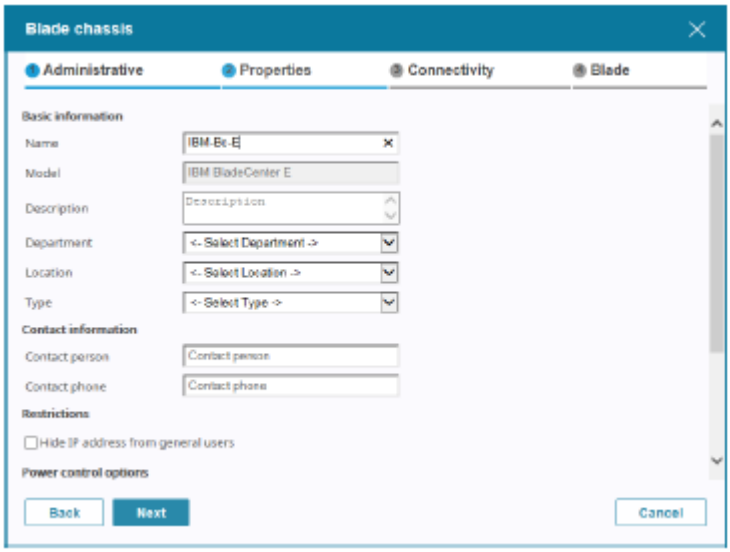
1. 下表を参考にしながら、各項目に値を設定してください。

項目	説明
Device Model (デバイスモデル)	追加するモデルをドロップダウンメニューから選択してください。
Auto detect (自動検出)	この機能を有効にすると、システムはデバイスがオンライン状態であるかどうかを自動的に確認します。 この機能は、管理権限を有するユーザーに操作が限定されています。
Detect Interval (検索インターバル)	検索を行うインターバルの秒数を設定してください。これは、システムがどのくらいの頻度でブレードサーバーがオンラインであるかを自動的に確認するものです。

(表は次のページに続きます)

項目	説明
IP Address/ Connect method/SSH Port (IP アドレス/ 接続方法/SSH ポート)	自動検出機能を使用しない場合は、ブレードサーバーの IP アドレス、および接続に使用するアクセスポート(Telnet または SSH)を入力し、接続方法を選択してください。デフォルトポートは 22(SSH)です。「**Test connection**」(接続のテスト)をクリックすると、IP やポートが正しく検出されているかを確認することができます。
Username/Password (ユーザーネーム/パスワード)	ブレードサーバーへのアクセス(Telnet または SSH 経由)に必要となるユーザーネームとパスワードを入力してください。 **注意:** 必要な情報を得るためには、管理者権限が与えられているアカウントを使ってください。
Timeout (タイムアウト)	キャンセル前に接続リクエストが完了するのを待機する秒数です。
Server (サーバー)	ブレードサーバーが接続している CC2000 を選択してください。

2. 画面の入力が完了したら、「**Next**」(次へ)をクリックしてください。そうすると、「Properties」(プロパティー)画面が表示されます。



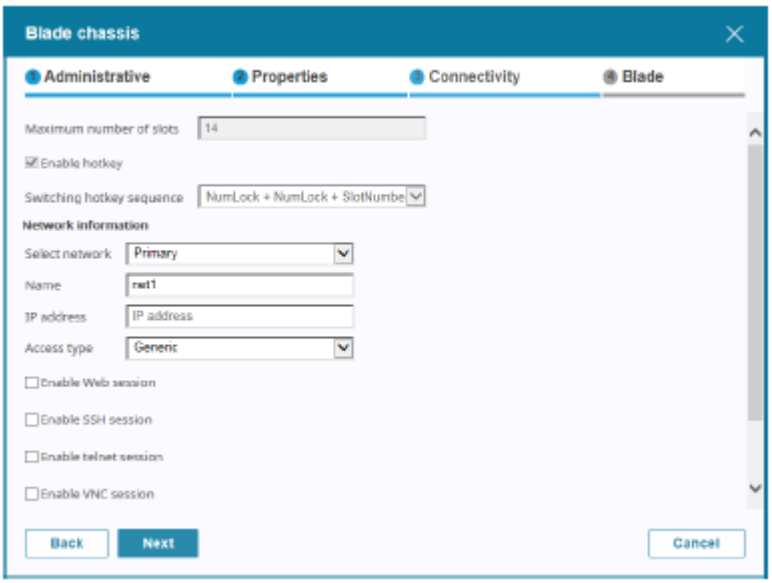
3. 下表を参考にしながら、各項目に値を設定してください。

項目	説明
Device Information （デバイス情報）	**Name（名前）：**デバイスの識別に使用する名前を設定してください。 **Model（型番）：**CC2000 が認識している型番です。この項目は自動的に入力され、編集することができません。 **Description（説明）**：デバイスに補足説明を設定する場合は、この欄に入力してください。この項目への設定はオプションです。 **Department（部署）**：企業内のシステムで使用する場合は部署別カテゴリー（例：R&D)を作成し、これにデバイスを割り当てることができます（p.139「カテゴリーの管理」参照）。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Location（場所）**：企業内のシステムで使用する場合は地域別カテゴリー（例：西海岸)を作成し、これにデバイスを割り当てることができます（p.139「カテゴリーの管理」参照）。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Type（タイプ）：**このデバイスのデバイスタイプをドロップダウンメニューから選択してください。
Contact Information （コンタクト情報）	デバイス管理者の名前および電話番号です。この欄の設定はオプションです。

（表は次のページに続きます）

項目	説明
Restrictions （制限）	**Hide IP Address from general users（一般ユーザーに対して IP アドレスを隠す）**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの IP アドレスがデバイス一覧に表示されなくなります。 **Hide MAC Address from general users（一般ユーザーに対して MAC アドレスを隠す）**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの MAC アドレスがデバイス一覧に表示されなくなります。
Power Control Options （電源管理オプション）	次の説明に従って電源管理オプションを設定してください。 ◆ ボックスをクリックすると、電源操作の確認を有効にします。 ◆ ボックスをクリックすると、電源操作の遅延を有効にします。この場合は、「Power ON Delay」（電源オン遅延）と「Power OFF Delay」（電源オフ遅延）の各欄に秒数を入力してください。

4. 画面への入力が完了したら、「**Next**」（次へ）をクリックしてください。そうすると、「Connectivity」（接続）画面が表示されます。

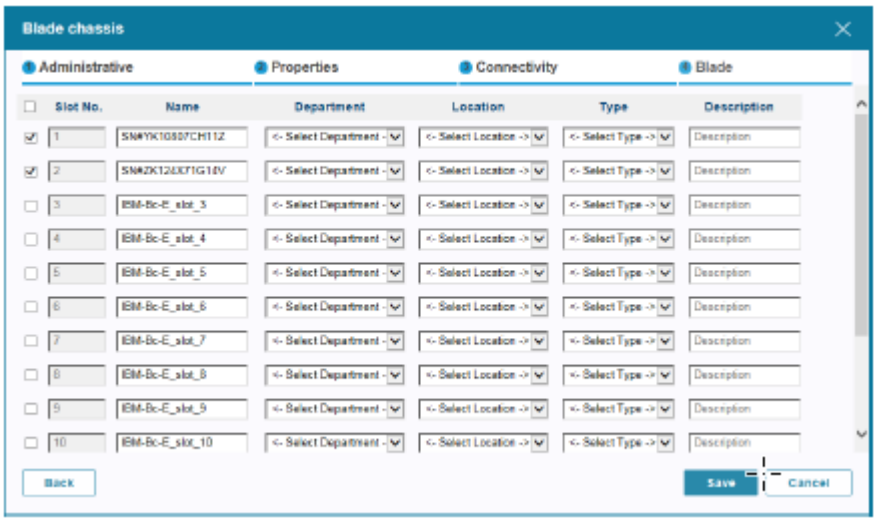


5. 下表を参考にしながら、各欄に必要事項を入力してください。

- 「Maximum number of slots」(スロット数の上限)の項目は読取専用欄で、対応シャーシでは設定することができません。この項目はジェネリックシャーシでのみ設定が可能です。
- 「Blade switching hotkey」(ブレード切替ホットキー)の情報は、割り当てられたモデルの詳細情報から自動的に入力されます。

項目	説明
Network Information (ネットワーク情報)	**Select network(ネットワークの選択):**ブレードシャーシのサーバーにネットワークインターフェースが 1 カ所しかない場合、「**Primary**」(プライマリー)を選択してください。ネットワークインターフェースが複数箇所ある場合は、「Primary」(プライマリー)の設定が完了した後、他のインターフェースの設定も順次行ってください。 **Name(名前):**識別しやすくなるように、ネットワークインターフェースに対してそれぞれ名前を設定することができます。 **IP Address(IP アドレス)**:ブレードシャーシの IP アドレスをここに入力してください。 **Access Type(アクセスタイプ):**ドロップダウンメニューからアクセスタイプを選択してください。
Enable Web session (ウェブセッションを有効にする) Enable SSH session (SSH セッションを有効にする) Enable telnet session (Telnet セッションを有効にする) Enable VNC session (VNC セッションを有効にする)	有効にしたいセッションがあれば、該当項目にチェックを入れてください。

6. 画面への入力が完了したら、「**Next**」（次へ）をクリックしてください。そうすると、「Blade」（ブレード）画面に遷移します。

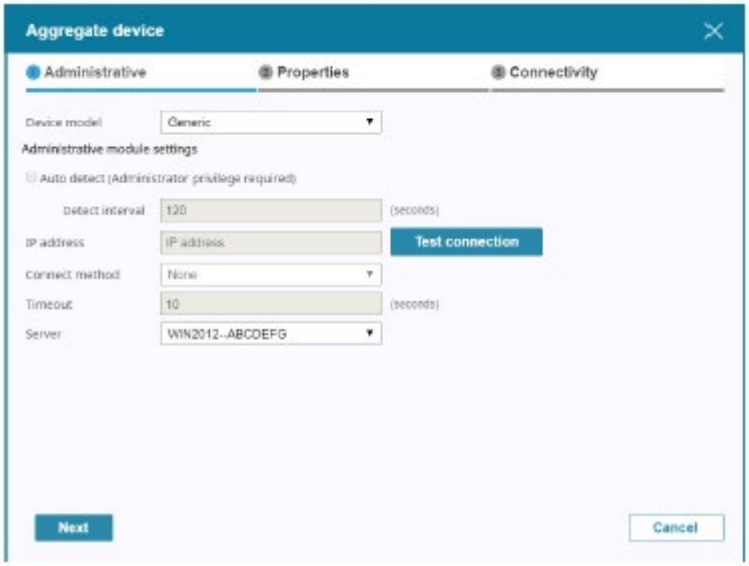


7. 各ブレードに対し、「Department」（部署）、「Location」（場所）、「Type」(タイプ)、「Description」（説明）をそれぞれ設定してください。

8. ブレードシャーシが接続するポートにチェックを入れたら、「**Save**」（保存）ボタンをクリックして操作を完了してください。

アグリゲートデバイスの追加

「Add」(追加)リストから「Aggregate device」(アグリゲートデバイス)を選択すると、アグリゲートデバイスを CC2000 統合管理システムに追加します。



注意: アグリゲートデバイスの詳細については p.72 をご参照ください。

アグリゲートデバイスを追加するには、以下の手順で操作してください。

1. 管理画面で、ドロップダウンメニューから「Device Model」(デバイスモデル)を選択し、下表を参考にしながら、各欄に必要事項を入力してください。

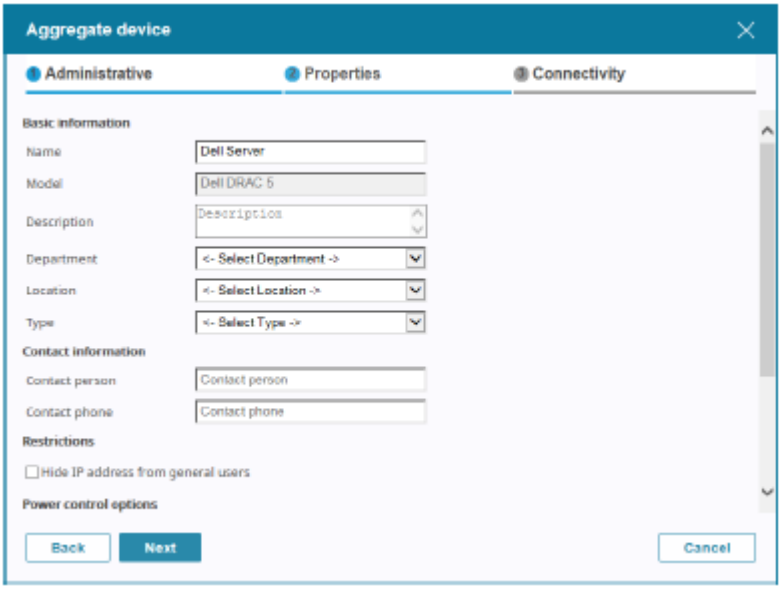
   注意:
   - ◆ 利用可能な項目は、選択されたデバイスモデルによって異なります。
   - ◆ Redfish が有効になっている HP iLO 5 および Dell iDRAC 8 は、デバイスモデルとして「Redfish-enabled Device」(Redfish が有効なデバイス)が選択されている場合にサポートされます。

項目	説明
Auto Detect (自動検出)	この機能を有効にすると、システムはデバイスがオンライン状態であるかどうかを自動的に確認します。 この機能は、管理権限を有するユーザーに操作が限定されています。

(表は次のページに続きます)

項目	説明
Detect Interval （検索インターバル）	検索を行うインターバルの秒数を設定してください。これは、システムがどのくらいの頻度でアグリゲートデバイスがオンラインであるかを自動的に確認するものです。
IP Address （IP アドレス）	アグリゲートデバイスの IP アドレスを入力してください。また、「Test connection」（接続のテスト）をクリックすると、IP が正しく検出されているかを確認することができます。
Connect Method （接続方法）	IPMI デバイスの場合、接続方法は IPMI のみです。 また、Redfish が有効なデバイスの場合、接続方法は HTTPS のみです。 上記以外の場合は、ドロップダウンメニューから SSH または Telnet から選択してください。
Port （ポート）	接続に使用するアクセスポート番号を入力してください。 デフォルトの SSH ポート：22 デフォルトの Telnet ポート：23 デフォルトの IPMI ポート：623 デフォルトの HTTPS ポート：443
Username/Password （ユーザーネーム/ パスワード）	アグリゲートデバイスにアクセスするのに必要なユーザーネームとパスワードを入力してください。
Timeout （タイムアウト）	リクエストをキャンセルするまでに接続リクエストが完了するのを待機する秒数です。
Server （サーバー）	アグリゲートデバイスサーバーが接続している CC2000 を選択してください。

2. 画面の入力が完了したら、「**Next**」(次へ)をクリックしてください。そうすると、「Properties」(プロパティー)画面が表示されます。



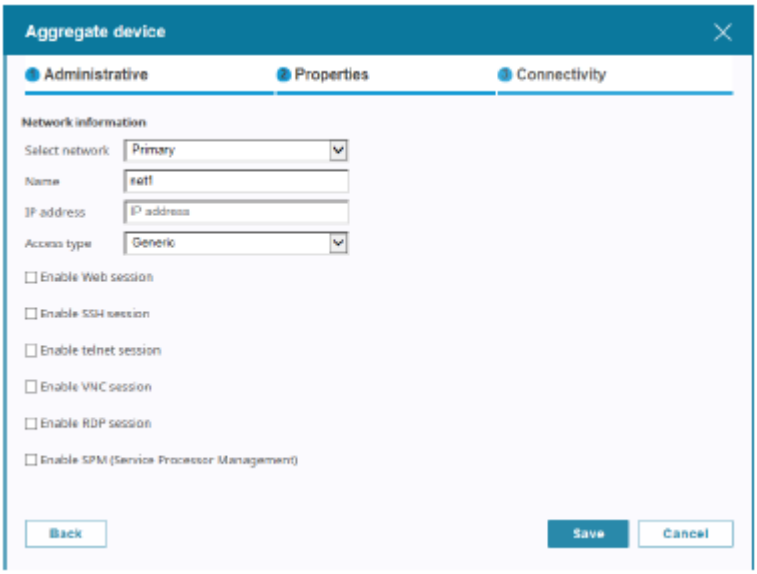
3. 下表を参考にしながら、各項目に値を設定してください。

項目	説明
Device Information (デバイス情報)	**Name(名前)**:デバイスの識別に使用する名前を設定してください。 **Model(型番)**:CC2000 が認識している型番です。この項目は自動的に入力され、編集することができません。 **Description(説明)**:デバイスに補足説明を設定する場合は、この欄に入力してください。この項目への設定はオプションです。 **Department(部署)**:企業内のシステムで使用する場合は部署別カテゴリー (例:R&D)を作成し、これにデバイスを割り当てることができます(p.139「カテゴリーの管理」参照)。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリストを展開し、そのデバイスが所属するものをクリックしてください。

(表は次のページに続きます)

項目	説明
Device Information (デバイス情報)	**Location(場所)**:企業内のシステムで使用する場合は地域別カテゴリー (例:西海岸)を作成し、これにデバイスを割り当てることができます(p.139「カテゴリーの管理」参照)。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリストを展開し、そのデバイスが所属するものをクリックしてください。 **Type(タイプ)**:このデバイスのデバイスタイプをドロップダウンメニューから選択してください。
Contact Information (コンタクト情報)	デバイス管理者の名前および電話番号です。この欄の設定はオプションです。
Restrictions (制限)	**Hide IP Address from general users(一般ユーザーに対して IP アドレスを隠す)**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの IP アドレスがデバイス一覧に表示されなくなります。 **Hide MAC Address from general users(一般ユーザーに対して MAC アドレスを隠す)**:セキュリティー対策として、この機能を有効にすると、ユーザーがウェブブラウザーでログインした際にデバイスの MAC アドレスがデバイス一覧に表示されなくなります。
Power Control Options (電源管理オプション)	次の説明に従って電源管理オプションを設定してください。 ◆ ボックスをクリックすると、電源操作の確認を有効にします。 ◆ ボックスをクリックすると、電源操作の遅延を有効にします。この場合は、「Power ON Delay」(電源オン遅延)と「Power OFF Delay」(電源オフ遅延)の各欄に秒数を入力してください。

4. 画面への入力が完了したら、「**Next**」(次へ)をクリックしてください。そうすると、「Connectivity」(接続)画面が表示されます。



5. 下表を参考にしながら、各欄に必要事項を入力してください。

項目	説明
Network Information (ネットワーク情報)	**Select network (ネットワークの選択) :** アグリゲートデバイスにネットワークインターフェースが 1 カ所しかない場合、「**Primary**」(プライマリー)を選択してください。ネットワークインターフェースが複数箇所ある場合は、「Primary」(プライマリー)の設定が完了した後、他のインターフェースの設定も順次行ってください。 **Name (名前) :** 識別しやすくなるように、ネットワークインターフェースに対してそれぞれ名前を設定することができます。 **IP Address (IP アドレス) :** アグリゲートデバイスの IP アドレスをここに入力してください。 **Access Type (アクセスタイプ) :** ドロップダウンメニューからアクセスタイプを選択してください。

(表は次のページに続きます)

項目	説明
Enable Web Session (ウェブセッションを有効にする)	この項目にチェックを入れると、ウェブ操作を有効にします。この設定は、デバイスリスト(画面上部)における「Operation」(操作)列のドロップダウンメニューに反映されます。 **URL:**ウェブ経由でアグリゲートデバイスにアクセスできるよう、管理画面にアクセスするための URL を入力してください。 **Enable SSO(シングルサインオンを有効にする):**SSO(シングルサインオン)機能を有効にするには、このボックスにチェックを入れてから、どの認証情報を使用するかを選択してください。 ◆ CC2000 のユーザーアカウントと同じアカウントのユーザーネームとパスワードを使用するには、「Use login user credentials」(ログインユーザー認証情報を使用する)を選択してください。 ◆ 新規に認証情報を作成するには、「Use following credentials」(以下の認証情報を使用する)を選択して、該当欄に認証情報を入力してください。 **Login name、Password(ログインネーム、パスワード):**これらの項目は、アグリゲートデバイスの認証や権限設定に基づいて設定を行ってください。
Enable SSH session (SSH セッションを有効にする) Enable telnet session (Telnet セッションを有効にする)	「Enable SSH Session」(SSH セッションを有効にする)にチェックを入れると SSH セッションを、また、「Enable telnet Session」(Telnet セッションを有効にする)にチェックを入れると Telnet セッションを、それぞれ有効にします。この設定は、デバイスリスト(画面上部)における「Operation」(操作)列のドロップダウンメニューに反映されます。 **IP address, Login name, Password, SSH / Telnet port(IP アドレス、ログインネーム、パスワード、SSH/Telnet ポート):**SSH/Telnet セッション経由でアグリゲートデバイスサーバーにアクセスする場合は、アグリゲートデバイスの認証や権限設定に基づいて、これらの項目の設定を行ってください。 **注意:**SSH セッションはログイン文字列情報を入力する必要があります。

(表は次のページに続きます)

項目	説明
Enable VNC Session （VNC セッションを有効にする）	この項目にチェックを入れるとVNC セッションを有効にします。この設定は、デバイスリスト（画面上部）における「Operation」（操作）列のドロップダウンメニューに反映されます。 **Port（ポート）：**VNC セッション用のポート番号を入力してください。 **Enable SSO（シングルサインオンを有効にする）：**SSO（シングルサインオン）機能を有効にするにはこのボックスにチェックを入れてから、「View only」（参照のみ）および「Full control」（フル操作）の各パスワードを入力してください。
Enable RDP Session （RDP セッションを有効にする）	この項目にチェックを入れると RDP セッションを有効にします。この設定は、デバイスリスト（画面上部）における「Operation」（操作）列のドロップダウンメニューに反映されます。 **RDP Port（RDP ポート）：**RDP セッション用のポート番号を入力してください。 **Enable SSO（シングルサインオンを有効にする）：**SSO（シングルサインオン）機能を有効にするにはこのボックスにチェックを入れてから、どの認証情報を使用するかを選択してください。 ◆ CC2000 のユーザーアカウントと同じアカウントのユーザーネームとパスワードを使用するには、「Use login user credentials」（ログインユーザー認証情報を使用する）を選択してください。 ◆ 新規に認証情報を作成するには、「Use following credentials」（以下の認証情報を使用する）を選択して、該当欄に認証情報を入力してください。

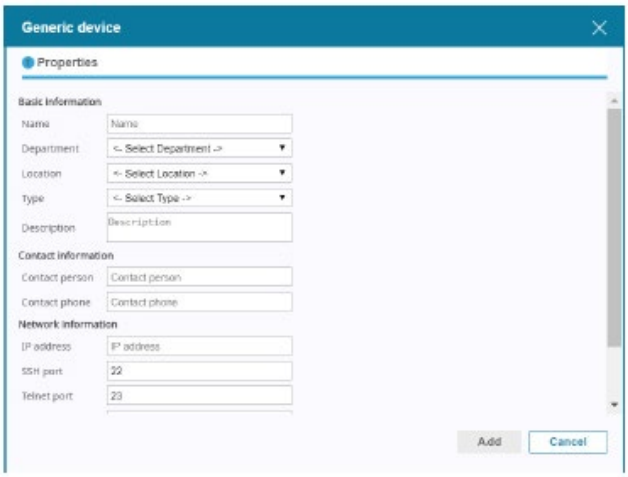
（表は次のページに続きます）

項目	説明
Enable SPM (Service Processor Management) (SPM(サービスプロセッサー管理)を有効にする)	この項目にチェックを入れると、SPM 操作を有効にします。この設定は、デバイスリスト(画面上部)における「Operation」(操作)列のドロップダウンメニューに反映されます。 **SPM Method(SPM 方法):**ドロップダウンメニューから該当する項目を選択してください。選択できる項目は、IPMI、HP iLO 2、HP iLO 3、HP iLO 5、IBM RSA II、IBM IMM、Dell DRAC 5、Dell iDRAC 6 Blade (modular)、Dell iDRAC 6 Standard (monolithic)、Dell iDRAC 8、Redfish 対応 Dell iDRAC 8、および Redfish 対応 HP iLO 5 です。 **Port(ポート):**SPM セッション用のポート番号を入力してください。 **Login name, Password(ログインネーム、パスワード):**SPM サーバーの認証や権限設定に基づいて、これらの項目の設定を行ってください。 **Timeout(タイムアウト):**接続要求がキャンセルされるまでに待機する時間を入力してください。

6. 入力し終わったら、「**Save**」(保存)ボタンをクリックして操作を完了してください。
「Operation」(操作)列におけるドロップダウンメニューの操作については、p.143「操作方法」を参照してください。

ジェネリックデバイスの追加

「Add」(追加)リストから「Generic device」(ジェネリックデバイス)を選択すると、ジェネリックデバイスを CC2000 統合管理システムに追加します。



注意: ジェネリックデバイスの詳細については p.73 をご参照ください。

1. 下表の内容を参考にしながら、各項目を設定してください。

項目	説明
Basic Information (基本情報)	**Name(名前)**:デバイスの識別に使用する名前を設定してください。 **Department(部署)**:企業内のシステムで使用する場合は部署別カテゴリー (例:R&D)を作成し、これにデバイスを割り当てることができます。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリスト(p.139「カテゴリーの管理」参照)を展開し、そのデバイスが所属するものをクリックしてください。 **Location(場所)**:企業内のシステムで使用する場合は地域別カテゴリー (例:西海岸)を作成し、これにデバイスを割り当てることができます。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリスト(p.139「カテゴリーの管理」参照)を展開し、そのデバイスが所属するものをクリックしてください。

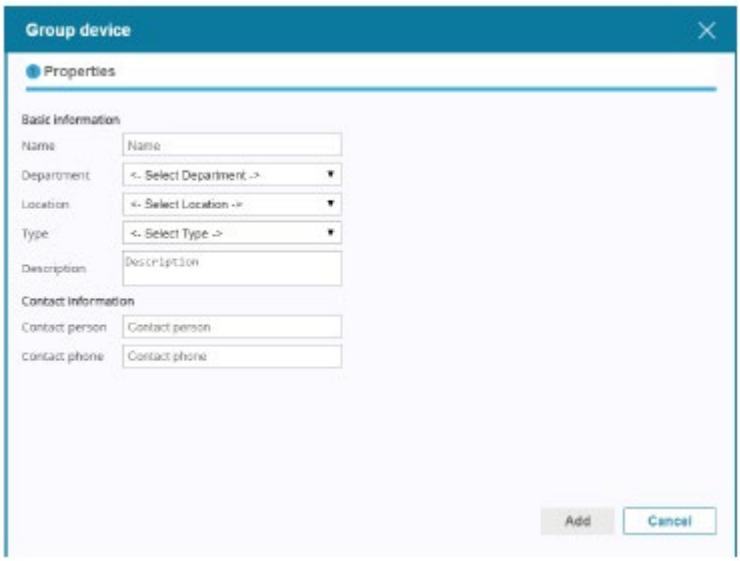
(表は次のページに続きます)

項目	説明
Basic Information (基本情報) (続き)	**Type(タイプ):**ドロップダウンメニューからデバイスのタイプを選択してください。 **Description(説明):**デバイスの詳細説明を設定する場合は、その内容をここに入力してください。この欄の設定はオプションです。
Contact Information (コンタクト情報)	このデバイスを管理するユーザーの名前および電話番号です。この欄の設定はオプションです。
Network Information (ネットワーク情報)	以下の例に従って残りの項目を入力してください。 ◆ ジェネリックデバイスにウェブブラウザーでアクセスする場合は、そのデバイスの URL または IP アドレスを「URL」欄に入力してください。 ◆ ジェネリックデバイスに Telnet または SSH でアクセスする場合は、「IP Address」(IP アドレス)欄に IP アドレスを、また、必要であれば Telnet または SSH ポートを該当欄にそれぞれ入力してください。 ◆ ジェネリックデバイスに対してこの 3 つの方法のどれでもアクセスができる場合は、項目を全て設定することも、また、必要となる項目だけを設定することもできます。
Restrictions (制限)	セキュリティー対策のため、「Hide IP Address from general users」(一般ユーザーに対して IP アドレスを隠す)の項目が有効になっていると、デバイスの IP アドレスはデバイスリストに表示されなくなります。この欄の設定はオプションです。

2. 入力し終わったら、「**Add**」(追加)ボタンをクリックして操作を完了してください。

グループデバイスの追加

「Add」(追加)リストから「Group device」(グループデバイス)を選択すると、グループデバイスをCC2000 統合管理システムに追加します。



1. 下表の内容を参考にしながら、各項目を設定してください。

項目	説明
Basic Information (基本情報)	**Name(名前)**:デバイスの識別に使用する名前を設定してください。 **Department(部署)**:企業内のシステムで使用する場合は部署別カテゴリー(例:R&D)を作成し、これにデバイスを割り当てることができます。このデバイスを部署別カテゴリーに割り当てる場合は、あらかじめ作成しておいた部署のリスト(p.139「カテゴリーの管理」参照)を展開し、そのデバイスが所属するものをクリックしてください。 **Location(場所)**:企業内のシステムで使用する場合は地域別カテゴリー(例:西海岸)を作成し、これにデバイスを割り当てることができます。このデバイスを地域別カテゴリーに割り当てる場合は、あらかじめ作成しておいた地域のリスト(p.139「カテゴリーの管理」参照)を展開し、そのデバイスが所属するものをクリックしてください。

(表は次のページに続きます)

項目	説明
Basic Information (基本情報) (続き)	**Type(タイプ):**ドロップダウンメニューからデバイスのタイプを選択してください。 **Description(説明):**デバイスの詳細説明を設定する場合は、その内容をここに入力してください。この欄の設定はオプションです。
Contact Information (コンタクト情報)	このデバイスを管理するユーザーの名前および電話番号です。この欄の設定はオプションです。

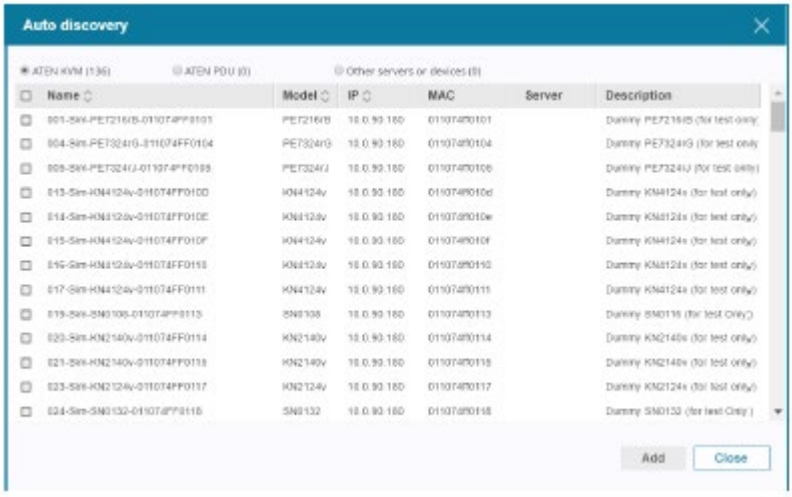
2. 入力し終わったら、「**Add**」(追加)ボタンをクリックして操作を完了してください。

注意:
1. アグリゲートデバイスとグループデバイスの違いについては、p.74「グループデバイス」をご参照ください。
2. ポートが所属できるグループデバイスの数には制限がありません。ポートがグループデバイスの一部である場合、そのグループデバイスは本来の物理ポートのロック状態を保持します。このポートをロックまたはロック解除すると、本来の物理ポートを含む全てのポートが新しいロック状態やロック解除状態に変わります。

自動検出

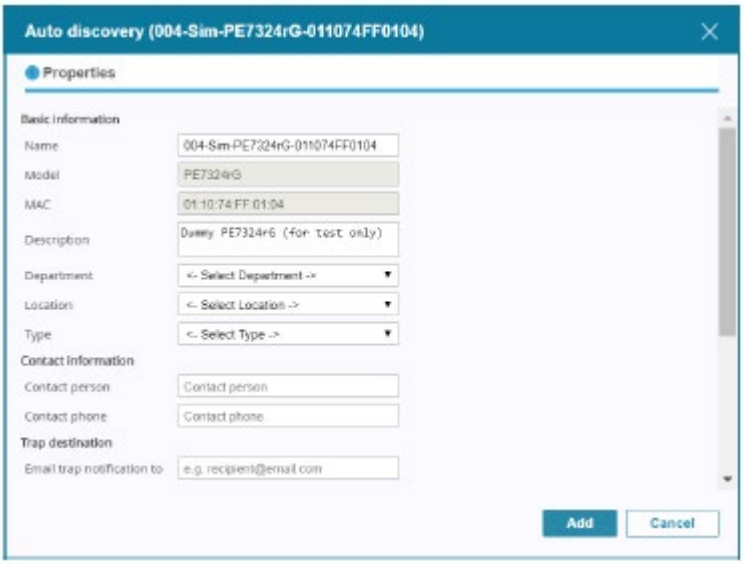
「Add」(追加)リストから「Auto Discovery」(自動検出)を選択すると、自動検出機能を使ってデバイスを CC2000 統合管理システムに追加します。

自動検出ウィンドウは下図のような画面です。



一覧に表示したいデバイスタイプ(ATEN デバイス、ATEN PDU、その他のサーバーまたはデバイス)は、ラジオボタンを使って選択してください。

そして、追加したいデバイスにチェックを入れて選択したら、「Add」(追加)ボタンをクリックしてください。



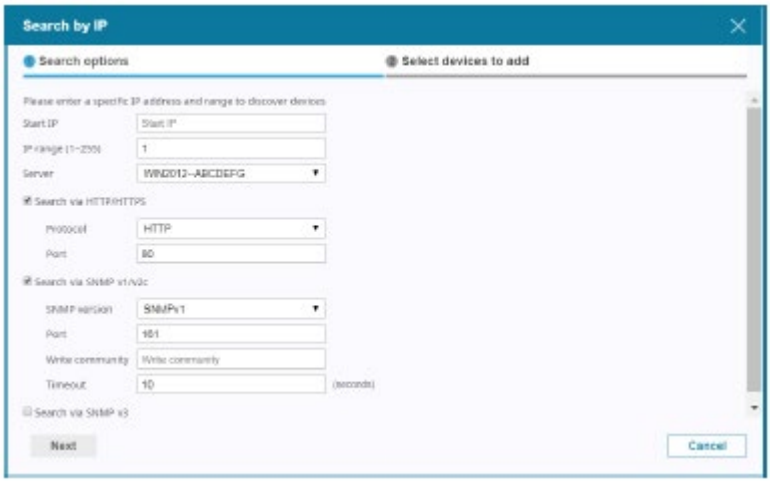
プロパティーの各欄への入力が完了したら、「Add」（追加）ボタンをクリックしてください。

入力内容の変更については、前のセクションを参考にしてください。

IP による検索

ここでは、IP 検索オプションを使ってデバイスを CC2000 統合管理システムに追加します。

IP 検索ウィンドウは下図のような画面です。



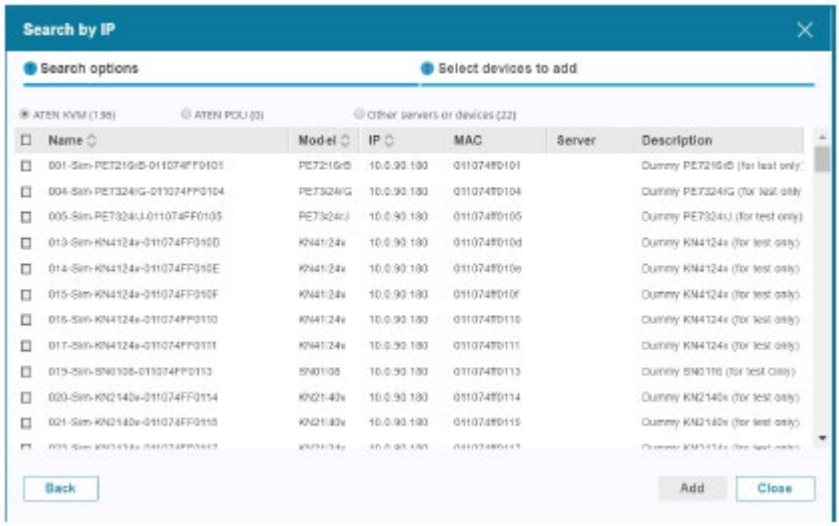
1. 下表の内容を参考にしながら、各項目を設定してください。

項目	説明
Start IP（開始 IP）	検索範囲の始点となる IP アドレスを入力してください。
IP Range（IP 範囲）	検索範囲の終点となる値（1～255）を入力してください。
Server（サーバー）	デバイスが接続している CC2000 サーバーを、ドロップダウンメニューから選択してください。
Search via HTTP/HTTPS（HTTP/HTTPS で検索）	この項目にチェックを入れた場合は、「Protocol」（プロトコル）ドロップダウンメニューからプロトコルを選択し、「Service port」（サービスポート）欄にポート番号を入力してください。そうすると、この HTTP または HTTPS 設定に合致したデバイスを検索します。
Search via SNMP v1/v2c（SNMP v1/v2c で検索）	この項目にチェックを入れた場合は、「SNMP version」（SNMP バージョン）ドロップダウンメニューから該当するもの選択し、「Port」（ポート）、「Write community」（書き込みコミュニティー）、「Timeout」（タイムアウト）の各欄に、関連情報を入力してください。そうすると、この SNMP v1/2c プロトコルを使用しているデバイスを検索します。

（表は次のページに続きます）

項目	説明
Search via SNMP v3 (SNMP v3 で検索)	この項目にチェックを入れた場合は、SNMP v3 プロトコルを使用しているデバイスを検索します。

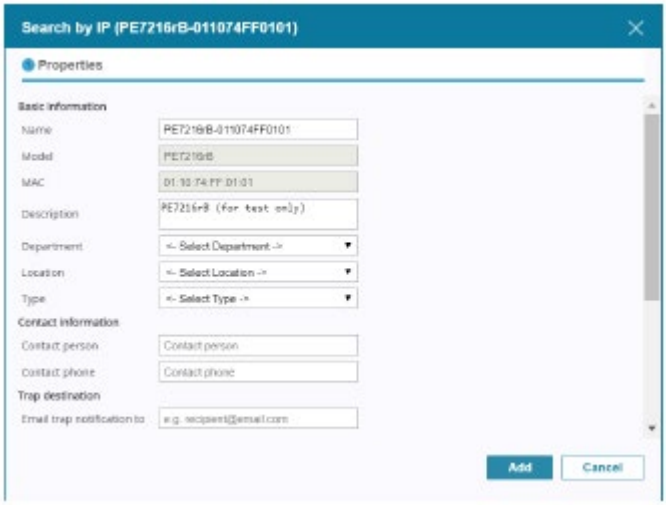
2. 「Next」(次へ)ボタンをクリックすると、検索結果が一覧形式で表示されます。ラジオボタンを使うと、一覧に表示するデバイスのタイプ(ATEN デバイス、ATEN PDU、その他のサーバーまたはデバイス)を選択することができます。



「Description」(説明)列には、次の結果のいずれかが表示されます。

結果	情報
空欄	そのようなデバイスやサーバーは見つかりませんでした。
IP が一致	同じ IP アドレスのデバイスまたはサーバーが CC2000 で見つかりましたが、タイプが異なります。
一致	IP とタイプの両方が一致するデバイスまたはサーバーが CC2000 で見つかりました。

3. 追加対象となるデバイスまたはサーバーにチェックを入れたら、「Add」(追加)ボタンをクリックしてください。



4. プロパティーの各欄に入力し終わったら、「Add」(追加)ボタンをクリックしてください。
   入力内容の変更については、前のセクションを参考にしてください。

5. 入力し終わったら、「Add」(追加)ボタンをクリックして操作を完了してください。

デバイスの編集

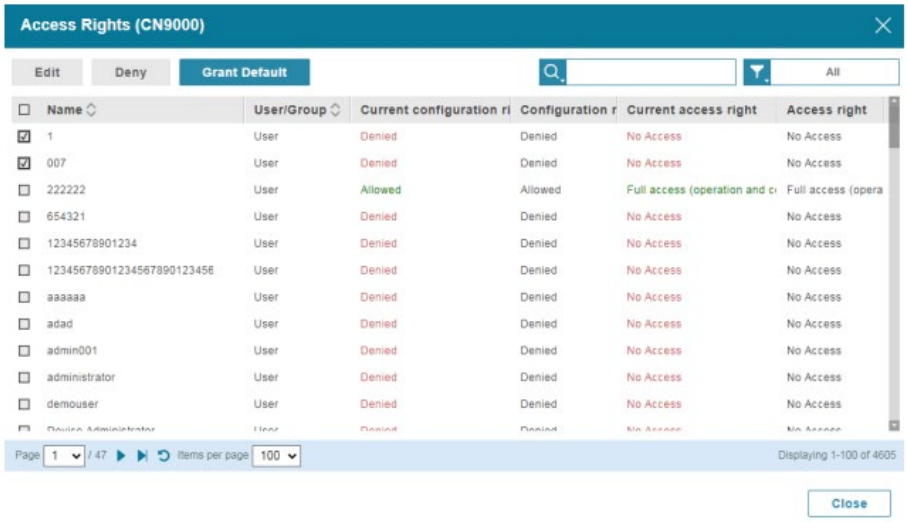
デバイスの編集を行うには、次の手順に従って操作を行ってください。

1. 編集対象となるデバイスにチェックを入れたら、「Edit」(編集)ドロップダウンメニューをクリックしてください。

2. 編集対象となるアイテムをクリックして選択したら、次のセクションを参考にしながら操作を進めてください。

アクセス権限

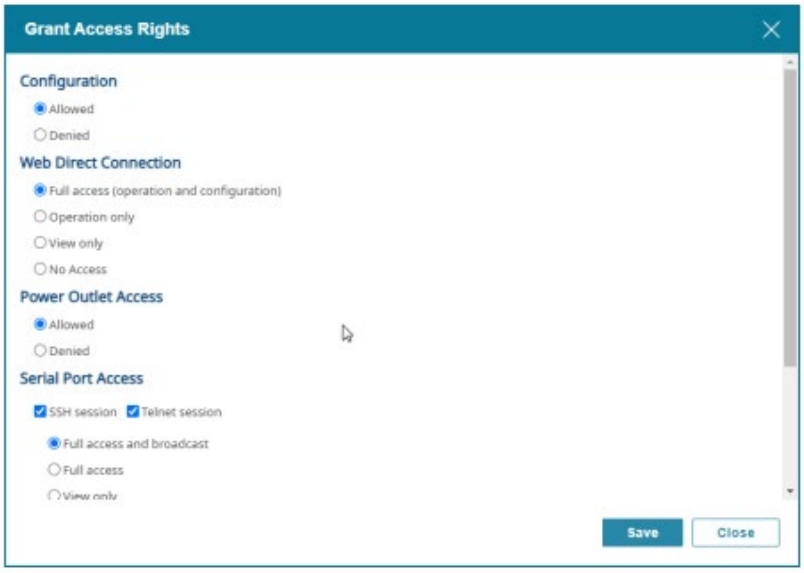
「Access rights」(アクセス権限)をクリックすると、下図のような画面が表示されます。



ユーザーのアクセス権限を編集するには、対象となるユーザーにチェックを入れて、「Edit」(編集)をクリックしてください。そうすると、別ウィンドウがポップアップ表示されます。アクセス権限のオプションは、デバイスタイプによって異なります。詳細は次のセクションを参照してください。

注意：

1. アクセス権限の編集には、ユーザーの行の上にカーソルを動かしたときに表示される鉛筆のアイコンを使うこともできます。
2. 複数のユーザーやユーザーグループに対して同一のアクセス権限や設定権限を同時に適用したい場合は、「**デフォルトを適用**」をクリックしてください。そうすると、次のような画面が表示されます。



適用可能なアクセス/設定権限に関する詳細は、次のセクションを参照してください。

■ATEN KVM

ATEN　KVM デバイスのオプションは下図の通りです。

ユーザーまたはグループに対して、設定権限を定義してください。

◆ **Allowed（許可）** – ユーザーまたはグループは、デバイスの設定を行うことができます。

◆ Denied(拒否) – ユーザーまたはグループは、デバイスの設定を行うことができません。

ユーザーまたはグループに対して、アクセス権限を定義してください。

◆ Full access (operation and configuration)(フルアクセス(操作および設定)) – ユーザーまたはグループは、全ての設定と操作を実行することができます。

◆ Operation only(操作のみ) – ユーザーまたはグループは、全ての操作を実行することができます。

◆ View only(参照のみ) – ユーザーまたはグループは、デバイスの参照のみを行うことができます。

◆ No Access(アクセス付加) – ユーザーまたはグループは、デバイスにアクセスすることができません。

■ATEN PDU

ATEN PDU のオプションは下図の通りです。

ユーザーまたはグループに対して、設定権限を定義してください。

◆ Allowed(許可) – ユーザーまたはグループは、デバイスの設定を行うことができます。

◆ Denied(拒否) – ユーザーまたはグループは、デバイスの設定を行うことができません。

ユーザーまたはグループに対して、アクセス権限を定義してください。

◆ Web – ユーザーまたはグループは、デバイスに対してウェブセッション経由でアクセスすることができます。

■APC PDU

APC PDU のオプションは下図の通りです。

ユーザーまたはグループに対して、設定権限を定義してください。

- Allowed（許可） – ユーザーまたはグループは、デバイスの設定を行うことができます。
- Denied（拒否） – ユーザーまたはグループは、デバイスの設定を行うことができません。

ユーザーまたはグループに対して、アクセス権限を定義してください。

- Web – ユーザーまたはグループは、デバイスに対してウェブセッション経由でアクセスすることができます。
- Telnet – ユーザーまたはグループは、デバイスに対して Telnet セッション経由でアクセスすることができます。
- SSH – ユーザーまたはグループは、デバイスに対して SSH セッション経由でアクセスすることができます。

■バーチャルホスト

バーチャルホストのオプションは下図の通りです。

ユーザーまたはグループに対して、アクセス権限を定義してください。

- **Primary NIC（プライマリーNIC）** – この NIC に対するネットワークプロトコルを指定してください。
- **Additional NIC1（追加 NIC1）** – この NIC に対するネットワークプロトコルを指定してください。
- **Additional NIC2（追加 NIC2）** – この NIC に対するネットワークプロトコルを指定してください。
- **Additional NIC3（追加 NIC3）** – この NIC に対するネットワークプロトコルを指定してください。
- **KVM settings（KVM 設定）** – アクセス権限を選択してください。詳細は下表の通りです。

権限	説明
Full access and VM (Read / Write)（フルアクセスおよび VM（読み込み/書き込み））	ユーザーはデバイス（またはデバイスにおける特定のポート）へのアクセス、画面の参照、キーボードやマウスを使った I/O 操作が可能です。また、バーチャルメディア機能を使った読み込み権限や書き込み権限も与えられます。
Full access and VM (Read Only)（フルアクセスおよび VM（読み込みのみ））	ユーザーはデバイス（またはデバイスにおける特定のポート）へのアクセス、画面の参照、キーボードやマウスを使った I/O 操作が可能です。また、バーチャルメディア機能の読み込み権限も与えられます。
Full access（フルアクセス）	ユーザーはデバイス（またはデバイスにおける特定のポート）へのアクセス、画面の参照、キーボードやマウスを使った I/O 操作が可能です。

（表は次のページに続きます）

権限	説明
View only (参照のみ)	ユーザーはデバイス(またはデバイスにおける特定のポート)へのアクセス、および画面の参照が可能ですが、操作を行うことはできません。
No access (アクセス不可)	ユーザーはデバイス(またはデバイスにおける特定のポート)へのアクセスを行うことができません。デバイス(および特定のポート)は、「Port Access」(ポートアクセス)画面のサイドバーや一覧にも表示されません。

- **Serial settings(シリアル設定)** – ネットワークプロトコル(複数選択可)とアクセス権限(フルアクセスおよびブロードキャスト、フルアクセス、参照のみのいずれか)を選択してください。
- **Power via PDU(PDU 経由の給電)** – 有効にする場合はチェックを入れ、無効にする場合はチェックを外してください。

■ブレードシャーシおよびアグリゲートデバイス

ブレードシャーシやアグリゲートデバイスのオプションは下図の通りです。

ユーザーまたはグループに対して、アクセス権限を定義してください。

- **Primary NIC(プライマリーNIC)** – この NIC に対するネットワークプロトコルを指定してください。
- **Additional NIC1(追加 NIC1)** – この NIC に対するネットワークプロトコルを指定してください。
- **Additional NIC2(追加 NIC2)** – この NIC に対するネットワークプロトコルを指定してください。
- **Additional NIC3(追加 NIC3)** – この NIC に対するネットワークプロトコルを指定してください。
- **KVM settings(KVM 設定)** – アクセス権限を選択してください。詳細は下表の通りです。

権限	説明
Full access and VM (Read / Write) (フルアクセスおよび VM (読み込み/書き込み))	ユーザーは、デバイス(またはデバイスにおける特定のポート)へのアクセス、画面の参照、キーボードやマウスを使った I/O 操作が可能です。また、バーチャルメディア機能を使った読み込み/書き込み権限も与えられます。
Full access and VM (Read Only) (フルアクセスおよび VM (読み込みのみ))	ユーザーはデバイス(またはデバイスにおける特定のポート)へのアクセス、画面の参照、キーボードやマウスを使った I/O 操作が可能です。また、バーチャルメディア機能の読み込み権限も与えられます。
Full access (フルアクセス)	ユーザーはデバイス(またはデバイスにおける特定のポート)へのアクセス、画面の参照、キーボードやマウスを使った I/O 操作が可能です。
View only (参照のみ)	ユーザーはデバイス(またはデバイスにおける特定のポート)へのアクセス、および画面の参照が可能ですが、操作を行うことはできません。
No access (アクセス不可)	ユーザーはデバイス(またはデバイスにおける特定のポート)へのアクセスを行うことができません。デバイス(および特定のポート)は、「Port Access」(ポートアクセス)画面のサイドバーや一覧にも表示されません。

- **Serial settings(シリアル設定)** – ネットワークプロトコル(複数選択可)とアクセス権限(フルアクセスおよびブロードキャスト、フルアクセス、参照のみのいずれか)を選択してください。
- **Power via PDU(PDU 経由の給電)** – 有効にする場合はチェックを入れ、無効にする場合はチェックを外してください。

■ジェネリックデバイス

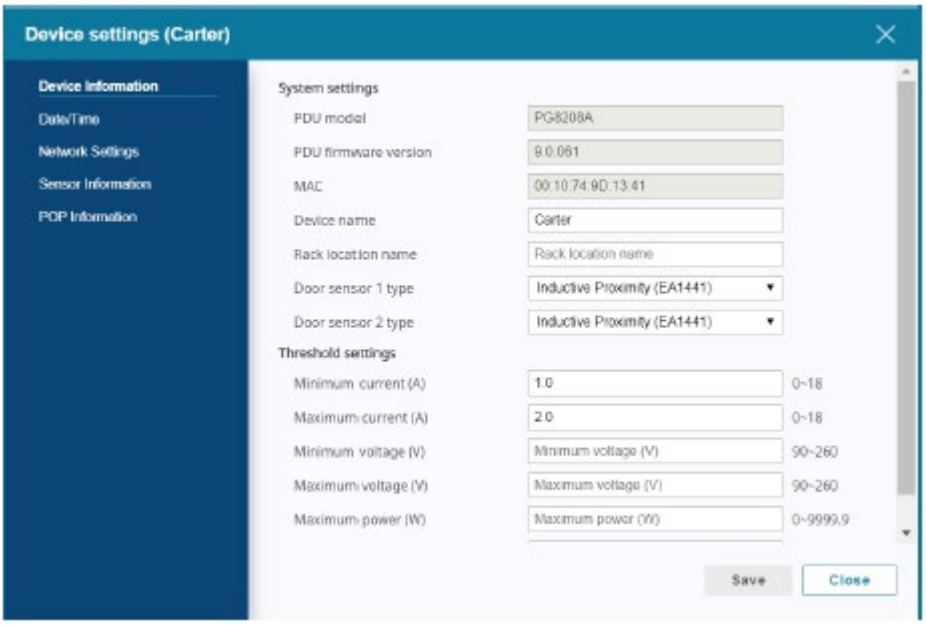
ジェネリックデバイスのオプションは下図の通りです。

ユーザーまたはグループに対して、アクセス権限を定義してください。

- Web – ユーザーまたはグループは、デバイスに対してウェブセッション経由でアクセスすることができます。
- Telnet – ユーザーまたはグループは、デバイスに対して Telnet セッション経由でアクセスすることができます。
- SSH – ユーザーまたはグループは、デバイスに対して SSH セッション経由でアクセスすることができます。

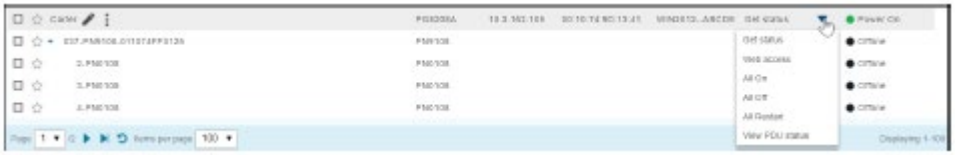
デバイス設定

デバイス設定を定義するには、そのデバイスのチェックボックスにチェックを入れて、「**Device settings**」（デバイス設定）を選択してください。そうすると、ウィンドウがポップアップ表示されます。下図はその例です。



サイドメニューを使って、設定可能なカテゴリーを選択したら、適切な項目を設定して「**Save**」（保存）をクリックしてください。設定可能な項目の詳細は、そのデバイスのマニュアルを参照してください。

デバイス設定を行うウェブ画面に遷移するには、「**Operation**」（操作）列のドロップダウンメニューをクリックして、「**Web access**」（ウェブアクセス）を選択してください。下図はその例です。



プロパティー

デバイスの**プロパティー**は、ここで編集することができます。各種デバイスで利用可能なオプションに関する情報は、p.78「デバイスの追加」で該当するデバイスタイプのセクションを参照してください。

全ノードのプロパティー

「All Nodes Properties」(全ノードのプロパティー)ボタンをクリックすると、そのデバイス配下にあるアイテムを全て一覧表示する画面に遷移します。この画面では、配下にあるアイテム(子アイテム)の部署、場所、タイプ、説明、トラップ宛先を設定(または再設定)することができます。

デバイスの削除

デバイスを削除するには、対象となるデバイスにチェックを入れて選択してから「**Delete**」(削除)をクリックしてください(複数選択可)。

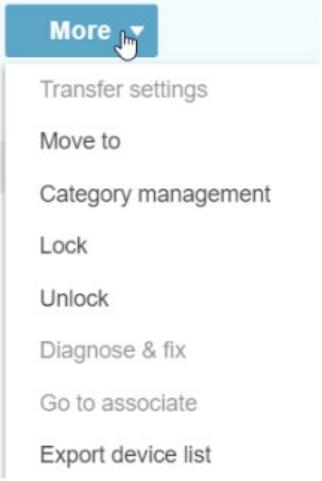
そうすると、確認メッセージがポップアップ表示されます。削除を続行する場合は「**Yes**」(はい)をクリックしてください。

注意:

1. 必要に応じて、複数のデバイスにチェックを入れて、同時に削除することができます。また、列の見出しにあるチェックボックスにチェックを入れて削除を行うと、全てのデバイスを一括削除することもできます。
2. アグリゲートデバイスを削除すると、そのポートは全て、ロックされた状態で元の物理デバイスへと戻ります。

詳細

ここでは「More」(詳細)設定オプションを利用することができます。「More」(詳細)ドロップダウンメニューをクリックすると、次のアイテムが表示されます。



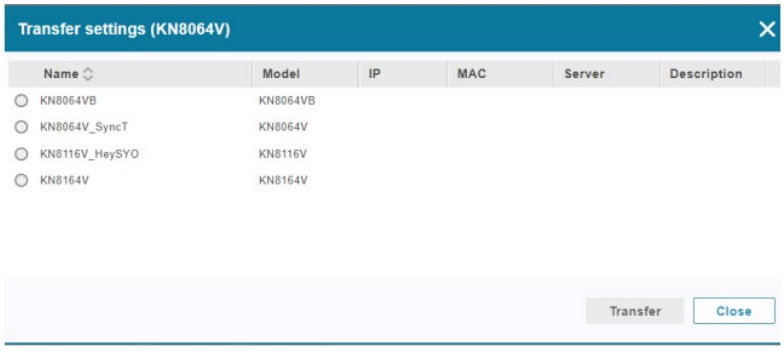
注意: 詳細設定へのアクセスには、ユーザーの行の上にカーソルを動かしたときに表示される詳細アイコン(⋮)を使うこともできます。

設定方法については、次のセクションで説明します。

設定の移行

この機能を使うと、デバイスの設定やアクセス権限を、ソースデバイスから選択されたデバイスへと移行することができます。

デバイスにチェックを入れて選択したら(例:デバイス A)、「Transfer」(移行)をクリックしてください。そうすると、下図のような画面がポップアップ表示されます。



ソースデバイス(例:デバイス B)を選択したら、画面右下にある「Transfer」(移行)ボタンをクリックしてください。そうすると、移行を確認するメッセージが表示されます。CC2000 は、ソースデバイス(デバイスB)における(デバイスID、モデル名、ポート番号を除く)デバイス設定、およびアクセス権限を全て、選択されたデバイス(デバイス A)へと移行します。なお、移行操作がソースデバイスに影響を与えることはありません。

フォルダーとデバイスの移動

「Move To」(次に移動)機能を使うと、追加したデバイスを移動したり整理したりすることができます。

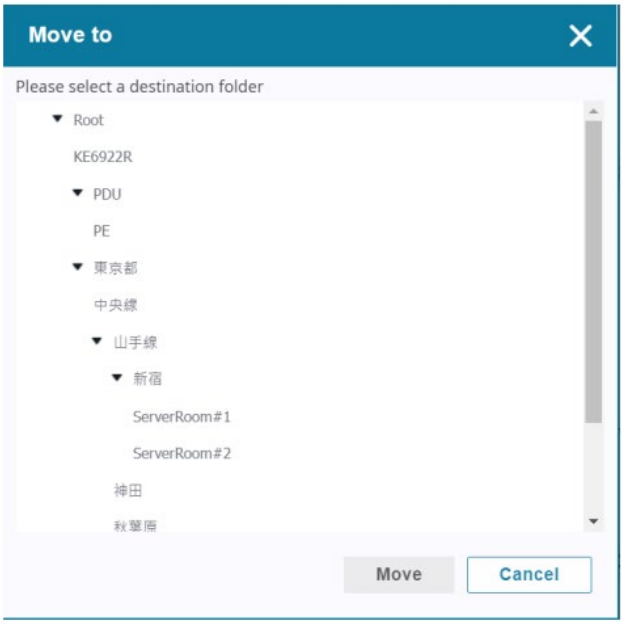
1 台または複数の追加デバイスを移動するには、次の手順に従って操作を行ってください。

1. デバイスリストで、対象となるデバイスまたはフォルダーの上にマウスカーソルを移動させ、「詳細」アイコン( )をクリックしてください。

注意: 複数のデバイスやフォルダーを移動させる場合は、対象となるアイテムをクリックして選択してから、 More ボタンをクリックしてください。

---

2. ポップアップメニューで、「Move to」(次へ移動)をクリックしてください。そうすると、構造図が表示されます。



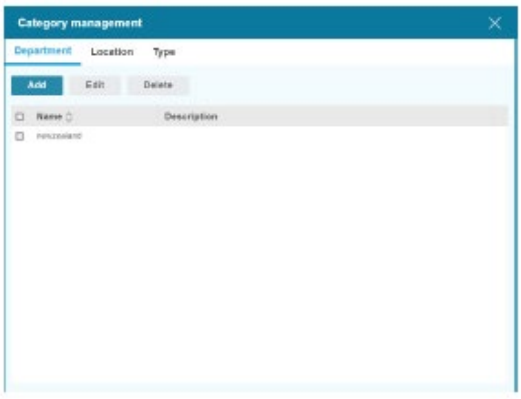
3. 場所をクリックして選択したら、「Move」(移動)をクリックして、設定を完了させてください。

カテゴリーの管理

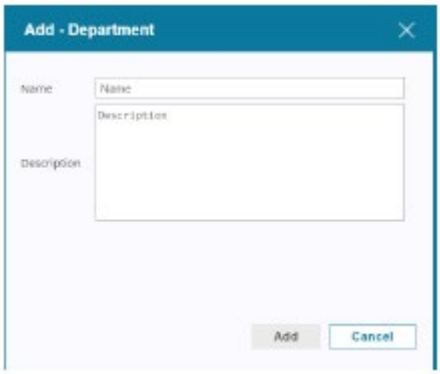
管理が簡単かつ便利に行えるよう、デバイスは部署、場所、タイプといったカテゴリーに分類することができます。この分類を使用するには、まず適切なカテゴリー（例：「部署」には「R&D」や「製造」、「場所」には「東海岸事業部」、「タイプ」には「電源」など）を作成し、（デバイスのプロパティー画面から）デバイスをこれらのカテゴリーに割り当てる必要があります。詳しくは、次のセクションで説明していきます。

部署、場所、またはタイプの分類を作成するには、次の手順に従って操作を行ってください。

1. 「**More**」（詳細）をクリックして、「**Category management**」（カテゴリー管理）を選択してください。そうすると、「Category management」（カテゴリー管理）画面がポップアップ表示されます。



2. 「**Add**」（追加）をクリックしてください。そうすると、部署（または場所、タイプのいずれか）の追加画面がポップアップ表示されます。



3. 「Name」（名前）および「Description」（説明）の各欄に入力したら、「**Add**」（追加）をクリックしてください。

部署、場所、またはタイプの分類を編集するには、対象となる項目にチェックを入れて、「**Edit**」（編集）をクリックしてください。そうしたら、「Name」（名前）や「Description」（説明）の欄を編集し、

「Save」（保存）をクリックしてください。

部署、場所、またはタイプの分類を削除するには、対象となる項目にチェックを入れて（複数選択可）、「Delete」（削除）をクリックしてください。そうすると、確認メッセージがポップアップ表示されます。削除を続行する場合は「Yes」（はい）をクリックしてください。

デバイスやポートを、部署、場所、またはタイプに割り当てるには、次の手順に従って操作を行ってください。

1. 「Device」（デバイス）画面で、デバイスやポートにチェックを入れて選択してください。
2. 「Edit」（編集）をクリックして、「Properties」（プロパティー）を選択してください。そうすると、下図のようなプロパティー画面がポップアップ表示されます。

3. 部署、場所、またはタイプを確認したら、対応するドロップダウンメニューをクリックして、デバイスやポートに割り当てるカテゴリーを選択してください。
4. 「Save」（保存）をクリックして、設定内容を保存してください。

デバイスのロックとロック解除

ポートを監視の対象外にするには、「More」(詳細)をクリックしてから「Lock」(ロック)をクリックしてください。そうすると、ポート一覧の最後の列に、ロックアイコン( )が表示されます。ロックされているポートは、使用中のノードとしてカウントされません。

デバイスのロックを解除するには、画面上部で対象となるデバイスにチェックを入れて選択し(複数選択可)、「More」(詳細)をクリックして、「Unlock」(ロック解除)をクリックしてください。

注意:
- ◆ 物理デバイスが CC2000 管理システムに追加されると、ポートはデフォルトでロックされます。
- ◆ ポートはアグリゲートデバイスに追加されると、自動的にロックが解除されますが、デバイスにおける物理ポートを 1～2 ポートだけ使用するのであれば、アグリゲートデバイスの作成を行う必要はありません。このような場合は、対象となるポートを選択し(複数選択可)、「Unlock」(ロック解除)をクリックしてください。

診断と修正

デバイスで問題が発生した場合(例:ドングルポートの変更)、「Diagnose & fix」(診断と修正)をクリックすることで、問題を解決することができます。この問題はログとして記録され、(画面上部における)デバイス一覧の最後の列に警告アイコンが表示されます。

デバイスの診断および問題修正が行われると、**診断＆修正**アイコン( )が上部画面(デバイス)の一覧の最後の列に表示されます。

関連付け

名前の後ろに「 」アイコンが付いているデバイスやポートは、関連付けられているデバイスやポートがあることを表します。

このオプションを選択するか、アイコンをクリックすると、関連付けデバイス一覧やポート一覧に遷移します。

関連付けは、ポートの管理がより簡単に行えるよう、異なるデバイス上の異なるポートを関連付けるアグリゲートデバイスで使用します。

デバイスリストのエクスポート

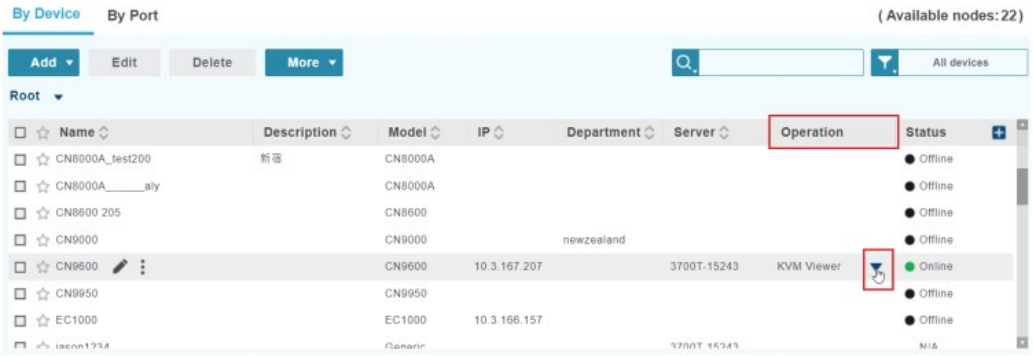
デバイスリストは、作成したりエクスポートしたりすることができます。このリストには、名前、説明、型番、IP アドレス、MAC アドレス、場所の情報が含まれ、CSV ファイルに保存することができます。デバイスリストをエクスポートするには、次のいずれかの方法で操作を行ってください。

- 

ボタンをクリックして、「Export device list」（デバイスリストのエクスポート）をクリックしてください。
- 追加デバイスで「」アイコンをクリックし、「Export device list」（デバイスリストのエクスポート）をクリックしてください。

操作方法

選択されたデバイスに応じてアクセスや操作ができるよう、各種ポート操作方法が提供されています。「Operation」（操作）列にあるドロップダウンメニューをクリックして、操作方法を選択してください。これらについては後続のセクションで説明します。



状態の取得

デバイスやサーバーの状態を更新するには、「Get Status」（状態の取得）をクリックして選択してください。

シャットダウン

デバイスやサーバーをシャットダウンするには、「Shutdown」（シャットダウン）をクリックして選択してください。

強制オフ

デバイスやサーバーを強制的にシャットダウンするには、「Force OFF」（強制オフ）をクリックして選択してください。

再起動

デバイスやサーバーを再起動するには、「Restart」（再起動）をクリックして選択してください。

強制再起動

デバイスやサーバーを強制的に再起動するには、「Force Restart」（強制再起動）をクリックして選択してください。

オン

デバイスやサーバーの電源をオンにするには、「ON」をクリックして選択してください。

Web クライアントビューワー

Web クライアントビューワーに対応している KVM デバイスの場合、ユーザーはドロップダウンメニューから KVM ビューワーをクリックすると、Windows または Java クライアントをセットアップすることなく、ブラウザーの新規タブで直接 KVM ビューワーセッションを起動するように選択することができます。詳細は p.178 を参照してください。

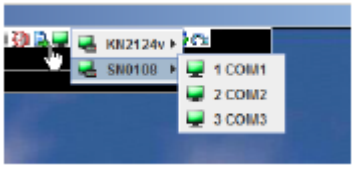
CC ビューワー/KVM ビューワー/SN ビューワー

ドロップダウンメニューから「CC/KVM/SNViewer」(CC/KVM/SN ビューワー)をクリックすると、選択されたデバイスのポートに対してビューワーセッションを直接開きます。このセッションは、お使いのデスクトップにウィンドウを開き、そのデバイスのポートを表示します。

ビューワーの操作方法は、KVM デバイスや SN デバイスから開いたビューワーの操作方法と同じです。

例えば、KVM スイッチ「KN2124v」とシリアルデバイス「SN0108」のポートから構成されているアグリゲートデバイスでは、CC ビューワーを開くと、そのアグリゲートデバイスにおける KN2124v の最初のポートが表示されます。

ビューワーでポートを切り替えるには、非表示になっているコントロールパネルを(ビューワーウィンドウの上部中央にマウスを移動させることで)開いて、「Port List」(ポート一覧)アイコンを選択してください。ポート一覧で選択できる項目には、そのデバイス配下にある全てのポートが含まれています。

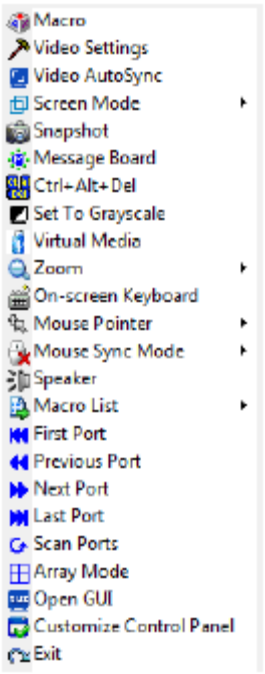


- 一覧で、ポートが属しているデバイスを選択して、アクセス対象となるポートをクリックしてください。
- デバイスまたはポートの名前は、CC ビューワーのタイトルバーに表示されます。
- 各ポートのビューワーウィンドウでは、コントロールパネルが非表示になっています。デバイスの別のポートに切り替える場合は、ポート一覧を起動して、目的のポートをクリックしてください。
- 対象となるデバイスが PDU と関連付けられている場合、CC ビューワーのコントロールパネルに電源操作が追加で表示されます。
- セッションを終了する場合は、コントロールパネルを開いて、「Exit」（終了）アイコンを選択してください。

■CC/KVM ビューワー

CC/KVM ビューワーのコントロールパネルは、画面上部または下部（通常は画面上部）の中央に隠れていますが、この部分にマウスカーソルを移動させると表示されます。パネルは、上部のアイコン行、中央と下部のテキスト行の合計 3 行から構成されています。

◆ テキスト行を右クリックすると、メニュー形式版のツールバーが起動します。



コントロールパネルの機能

コントロールパネルの各機能は下表の通りです。

アイコン	機能
	このアイコンをクリックすると、コントロールパネルを常に前面に表示します。もう一度このアイコンをクリックすると、通常の状態に戻します。
	マクロダイアログを起動します（詳細は KVM デバイスのマニュアルを参照）。
	ビデオオプションダイアログを起動します。右クリックすると、クイック自動同期を実行します（詳細は KVM デバイスのマニュアルを参照）。

（表は次のページに続きます）

アイコン	機能
	ビデオとマウスの自動同期を実行します。これは、「Video Options」(ビデオオプション)ダイアログの「Auto-sync」(自動同期)ボタンと同じ機能を提供します(詳細はKVM デバイスのマニュアルを参照)。
	画面表示をフルスクリーンモードまたはウィンドウモードに切り替えます。
	リモート画面のスナップショット(画面キャプチャー)を取得します(詳細は KVM デバイスのマニュアルを参照)。
	メッセージボードを起動します(詳細は KVM デバイスのマニュアルを参照)。
	[Ctrl] + [Alt] + [Delete]の信号をリモートコンピューターに送信します。
	リモート画面の表示をカラーまたはモノクロに切り替えます。
	「Virtual Media」(バーチャルメディア)ダイアログを起動します。アイコンの外観は、バーチャルメディア機能の状態に応じて変わります(詳細は KVM デバイスのマニュアルを参照)。
	リモート画面をズーム表示します。
	オンスクリーンキーボードを起動します(詳細は KVM デバイスのマニュアルを参照)。
	マウスポインターの種類を選択します。
	マウス同期を自動または手動で行います。 ◆ 「Automatic」(自動)を選択すると、アイコンに緑色のチェックマークが表示されます。 ◆ 「Manual」(手動)を選択すると、アイコンに赤色の×マークが表示されます。 (詳細は KVM デバイスのマニュアルを参照)
	リモートサーバー側の音声を、クライアントコンピューター側のスピーカーで出力するかどうかを切り替えます。スピーカーがオフになるとアイコンに禁止マーク(赤い円に斜線が入ったもの)が表示されます。

(表は次のページに続きます)

アイコン	機能
	接続された PDU の電源アウトレットの制御を、オン、オフ、再起動の間で切り替えます。 **注意:**この機能は、最低でも KVM ポートとアウトレットポートを 1 ポートずつ有するアグリゲートデバイスでのみ利用可能です。
	ユーザーマクロのドロップダウンリストを表示します。マクロへのアクセスやマクロの実行は、「Macro」(マクロ)ダイアログを使うよりもこの機能を使った方が簡単です(詳細は KVM デバイスのマニュアルを参照)。
	このアイコンは、拡張表示の設定で表示する際に使用するモニターを選択します(詳細は KVM デバイスのマニュアルを参照)。
	ポートにアクセスしている際にクリックすると、「Port Access」(ポートアクセス)タブを呼び出すことなく、現在の機器構成における、最初にアクセス可能なポートに移動します。
	ポートにアクセスしている際にクリックすると、「Port Access」(ポートアクセス)タブを呼び出すことなく、一つ前のアクセス可能なポートに移動します。
	ポートにアクセスしている際にクリックすると、「Port Access」(ポートアクセス)タブを呼び出すことなく、次のアクセス可能なポートに移動します。
	ポートにアクセスしている際にクリックすると、「Port Access」(ポートアクセス)タブを呼び出すことなく、現在の機器構成における、最後にアクセス可能なポートに移動します。
	ポートにアクセスしている際にクリックすると、オートスキャンモードを開始します。IP-KVM スイッチは、オートスキャンの対象となるポートをポート選択とフィルター機能の条件に従って自動的に切り替えます(詳細は KVM デバイスのマニュアルを参照)。これによって、コンピューターを手動で切り替えることなく、連続的にポートの状態をモニタリングすることができます。
	ポートにアクセスしている際にクリックすると、パネルアレイモードを起動します。
	ポートにアクセスしている際に GUI メニューを呼び出します。
	クリックするとコントロールパネル設定のダイアログボックスを表示します(詳細は KVM デバイスのマニュアルを参照)。
	クリックするとビューワーを終了します。

(表は次のページに続きます)

アイコン	機能
	これらのアイコンはリモートコンピューターの[Num Lock]、[Caps Lock] および[Scroll Lock]各キーの状態を表します。 ◆ キーが有効になっていると、そのキーのパネルが明るいグリーンに変化し、錠前が閉じたアイコンが表示されます。 ◆ キーが無効になっていると、そのキーのパネルは暗いグリーンに変化し、錠前が開いたアイコンが表示されます。 このアイコンをクリックすると状態は交互に切り替わります。 **注意:**このアイコンはローカルキーボードアイコンと同期しています。アイコンをクリックするとご使用のキーボードの LED がそれに応じます。同様にキーボードの[Lock]キーを押すとアイコンの色もそれに応じて変化します。

■SN ビューワー

SN ビューワーのコントロールパネルは、画面上部の中央に隠れていますが、この部分にマウスカーソルを移動させると表示されます。パネルは、上部のアイコン行、および中央と下部のテキスト行の合計 3 行から構成されています。

コントロールパネルの機能

コントロールパネルの各機能は、下表および後続のセクションで説明します。

アイコン	機能
	これはトグルボタンです。クリックすると、コントロールパネルを常に前面に表示します。言い換えれば、SN ビューワーの画面の上部に常に表示するということです。もう一度クリックすると、マウスカーソルと画面上部中央に移動させたときにのみ表示させるという自動非表示モードで表示します。
	画面上で選択されたテキストをコピーします。
	画面上に表示された全てのテキストをコピーします。
	コピーされたテキストをペースト(貼り付け)します。
	このアイコンをクリックすると、ログのオンとオフを交互に切り替えます。オンにすると、シリアル機器から SN ビューワーに送られたテキスト形式のログファイルを開始します。この機能を使うには、最初にテキストベースのログファイルを作成し、インポートしておく必要があります(詳細は SN デバイスのマニュアルを参照)。
	インポートするデータファイルを参照します(詳細は SN デバイスのマニュアルを参照)。
	画面のエンコーディング方法を変更します(詳細は SN デバイスのマニュアルを参照)。

(表は次のページに続きます)

アイコン	機能
	ブロードキャスト機能を有効にします。ブロードキャスト機能を使うと、一つのポートに対して行った変更を、全てのブロードキャストポートに対して同様に適用することができます。ブロードキャスト機能を使用する前に、「Broadcast Timeout」(ブロードキャストタイムアウト)と「Broadcast Ports」(ブロードキャストポート)を設定しておいてください(詳細は SN デバイスのマニュアルを参照)。 ブロードキャストを機能させるためには、あらかじめポートにブロードキャストポートとしてアクセスし、コントロールパネルにあるブロードキャストアイコンをクリックしておいてください。
	ブレークコマンドを送信します。
	ターミナルをリセットし、デフォルトの設定に戻します。
	メッセージボードを起動します(詳細は SN デバイスのマニュアルを参照)。
	ウィンドウを開いて、カスタムのテキストマクロ一覧を作成します(詳細は SN デバイスのマニュアルを参照)。
	フォント、色、その他 SN ビューワーの設定を変更します(詳細は SN デバイスのマニュアルを参照)。
	SN ビューワーのウィンドウ幅の調整を行います。
	ビューワーを終了します。

■Web クライアントビューワー

Web クライアントビューワーは、Windows または Java クライアントアプリをインストールすることなく、ブラウザーからデバイスのポートに対して直接アクセスできる手段を提供します。コントロールパネルは下図のような外観です。

注意： KVM ビューワーをクリックした際に Web クライアントビューワーを起動する方法については、p.178 を参照してください。

コントロールパネルの機能

アイコン	機能
	これはトグルボタンです。このアイコンをクリックすると、コントロールパネルを常に前面に表示します。もう一度このアイコンをクリックすると、通常の状態に戻します。
	クリックすると、ビデオオプションダイアログを起動します（詳細は、お使いの CC 製品や KVM 製品のユーザーマニュアルを参照）。
	クリックすると、ビデオの自動同期を実行します。
	クリックすると、スクリーンモードのドロップダウンメニューを表示します。このドロップダウンメニューからは、画面表示をフルスクリーンモードまたはウィンドウモードに切り替えることができます。
	クリックすると、リモート画面の表示をカラーまたはモノクロに切り替えます。
	ポートにアクセスしている際にクリックすると、パネルアレイモードを起動します（詳細は、お使いの CC 製品や KVM 製品のユーザーマニュアルを参照）。
	クリックすると、利用可能なオンラインポートのドロップダウンメニューを展開し、接続したいポートを選択することができます。
	クリックすると、[Ctrl] + [Alt] + [Delete]の信号をリモートシステムに送信します。
	クリックすると、オンスクリーンの英語キーボードを起動します（詳細は、お使いの CC 製品や KVM 製品のユーザーマニュアルを参照）。

（表は次のページに続きます）

アイコン	機能
	クリックすると、マウスポインターの種類を選択します。 **注意:**このアイコンは選択されたマウスポインターの種類に応じて変わります(詳細は、お使いの CC 製品や KVM 製品のユーザーマニュアルを参照)。
	クリックすると、マウス同期を自動または手動で行います(詳細は、お使いの CC 製品や KVM 製品のユーザーマニュアルを参照)。
	クリックすると、「Virtual Media」(バーチャルメディア)ダイアログを起動します。アイコンの外観は、バーチャルメディア機能の状態に応じて変わります(詳細は、お使いの CC 製品や KVM 製品のユーザーマニュアルを参照)。
	リモートサーバー側の音声を、クライアントコンピューター側のスピーカーで出力するかどうかを切り替えます。スピーカーがオフになるとアイコンに禁止マーク(赤い円に斜線が入ったもの)が表示されます。

ウェブアクセス

「Web Access」(ウェブクセス)をクリックすると、ブラウザーを開いて URL バーからログインしたときと同様に、お使いのデスクトップからデバイスに対してブラウザーセッションを開くことができます。

電源オン/オフ

- ◆ アグリゲートデバイスや電源デバイスの場合は、そのデバイスに属しているアウトレット全てに対して電源操作を行うことができます。「All ON」(全てオン)を選択すると、全ての電源をオンにし、「All OFF」(全てオフ)を選択すると、全ての電源をオフにします。
- ◆ 電源アウトレットの場合は、オンまたはオフを選択することができます。ポートの状態がオンの場合、選択できる項目はオフとなります。オフをクリックすると、そのアウトレットに対する電源をオフにします。

注意: 一覧の内容を変更する場合は、一度、別の画面に移動してから、その画面に戻って再表示してください。

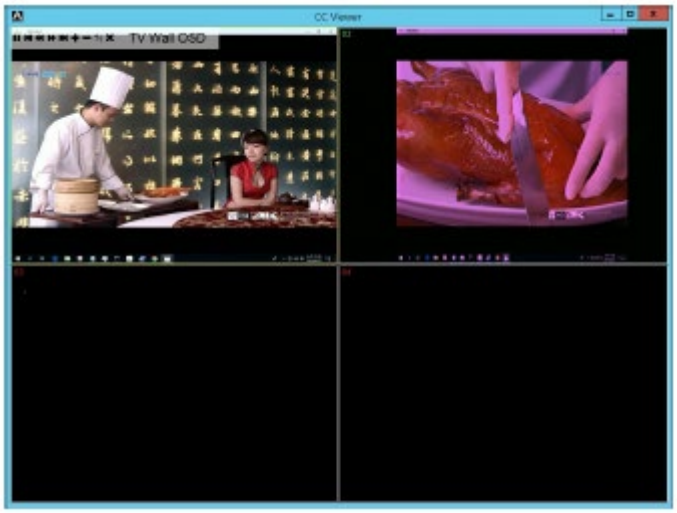
SSH/Telnet セッション

「SSH/Telnet Session」(SSH/Telnet セッション)を選択すると、指定されたポートに対して SSH または Telnet セッションを開きます。この項目を選択すると、ブラウザー経由でシリアルデバイス(例: SN0108)にログインし、メインのウェブ画面で「Telnet」を選択したときと同様に、SSH または Telnet ビューワーを開くことができます。

パネルアレイモード

グループデバイスが作成されていると、(「Operation」(操作)列にある)「CC Viewer」(CC ビューワー)ボタンをクリックすることで、そのデバイスのパネルアレイモードを起動することができます。また、パネルアレイモードは、コントロールパネルのパネルアレイ開始アイコンをクリックすることでも、起動することができます。

下図はアレイ表示の例です。



CC ビューワーの上にあるアイコンを使うと、パネルアレイの表示設定を調節することができます。

実際の操作は、次の URL にある短い動画にて確認することができます(英語版)。
https://www.youtube.com/watch?v=tbaQWK1vh60

SPM セッション

「Operation」(操作)列にあるドロップダウンメニューから「SPM」をクリックすると、「System Information」(システム情報)、「Monitoring Information」(モニタリング情報)、「Event Logs」(イベントログ)といった 3 つのタブが用意された画面が表示されます。

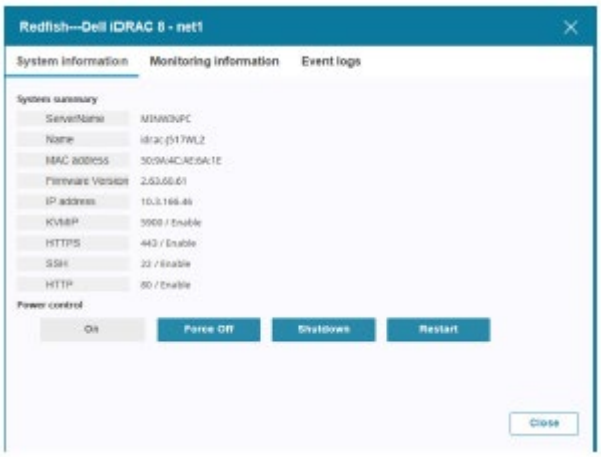
注意:	表示される情報やオプションは、サポートされる 2 種類の Redfish 対応デバイス(HP iLO 5 および Dell iDRAC 8)で異なります。

■システム情報

「System Information」(システム情報)タブでは、サーバーのシステム情報が表示されます。

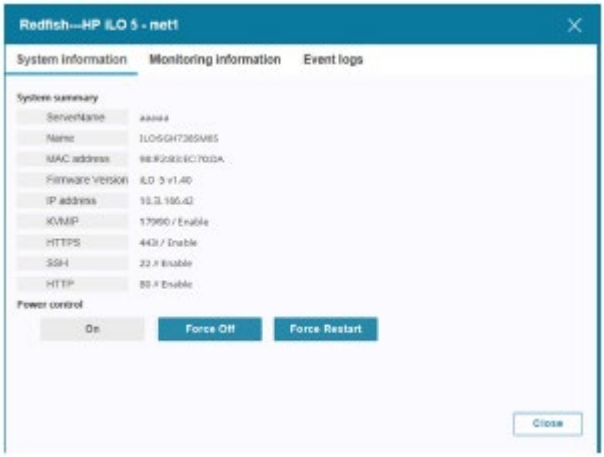
◆ Dell iDRAC 8 の例

ここでは、サーバーの電源**オン**、**シャットダウン**、**強制オフ**、**再起動**が行えます。



◆ HP iLO 5 の例

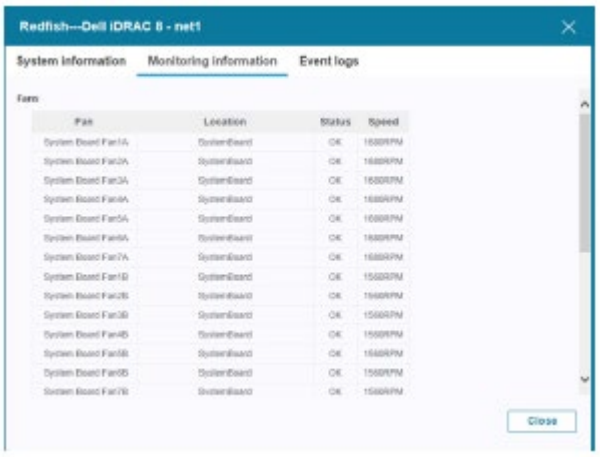
ここでは、サーバーの電源**オン**、**強制オフ**、**強制再起動**が行えます。



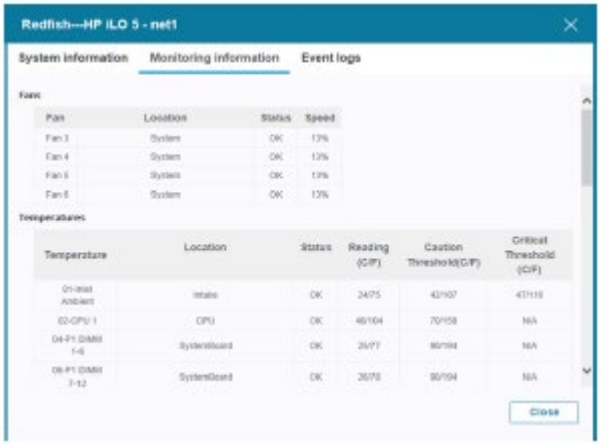
■モニタリング情報

表示される情報や詳細は、サポートされる 2 種類の Redfish 対応デバイスで異なります。

◆ Dell iDRAC 8 の例

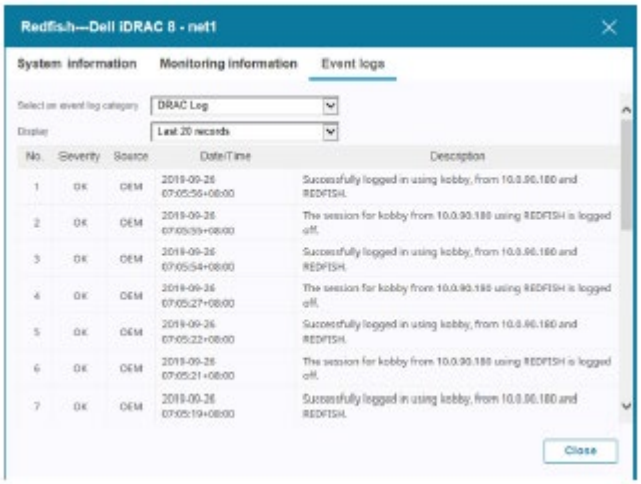


◆ HP iLO 5 の例

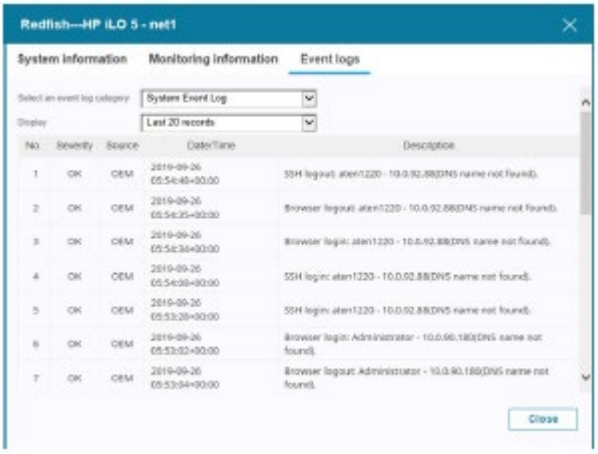


■イベントログ

◆ Dell iDRAC 8 の例



◆ HP iLO 5 の例



PDU の状態確認

「Operations」（操作）列のドロップダウンメニューにある「View PDU Status」（PDU の状態確認）をクリックすると、選択したデバイスに対して次の状態を検索します。

- デバイスの状態全般（電圧、電流、電力、消費電力）
- センサーの状態
  - 電流センサーの値（温度、湿度、気圧）
  - センサーの台数
  - センサーの状態（オープン、クローズ）
- バンクの状態（電圧、電流、電力、消費電力）
- アウトレットの状態（アウトレットの名前、オンやオフの状態、電圧、電流、電力、消費電力）

ポート

「**By Port**」(ポート別)を選択すると、システムにおける全てのポートが一覧表示されます。

「**By Device**」(デバイス別)でデバイスを選択すると、そのデバイスにおける全てのポートが、下の画面に一覧表示されます。

ポート列見出し

見出し	説明
Name (名前)	CC2000 システムへの追加時に、このポートに設定された名前です。
Alias (エイリアス)	ポートにエイリアス(別名)が付けられている場合は、その名前がここに表示されます。
Port (ポート)	デバイスにおけるポート番号です。
Port Type (ポートタイプ)	ポートが属するデバイスの種類を表します。
Status (状態)	◆ KVM デバイスやシリアルデバイスの場合は、ポートの状態(オンラインまたはオフライン)が表示されます。 ◆ 電源アウトレットの場合は、アウトレットポートの電源ソケットの状態(オンまたはオフ)が表示されます。 **注意:**このカテゴリーは、ブレードシャーシや個々のブレードには適用されません。このため、この欄は、ブレードシャーシでは「N/A」と、また、個々のブレードでは「Unknown」(不明)と、それぞれ表示されます。
Operation (操作)	このデバイスやポートにアクセスする際のデフォルトの動作が、この欄に表示されます。 ◆ 一覧の枠の右にある矢印をクリックすると、他に利用可能なアクションを確認することができます。 ◆ このポートのセッションを開く方法をクリックして選択してください。

操作全般は基本的にデバイス(p.70「デバイス別 - 操作全般」参照)と同じですが、設定がポートレベルにある点と、「**Launch Viewer**」(ビューワーの起動)オプションが含まれている点が異なります。

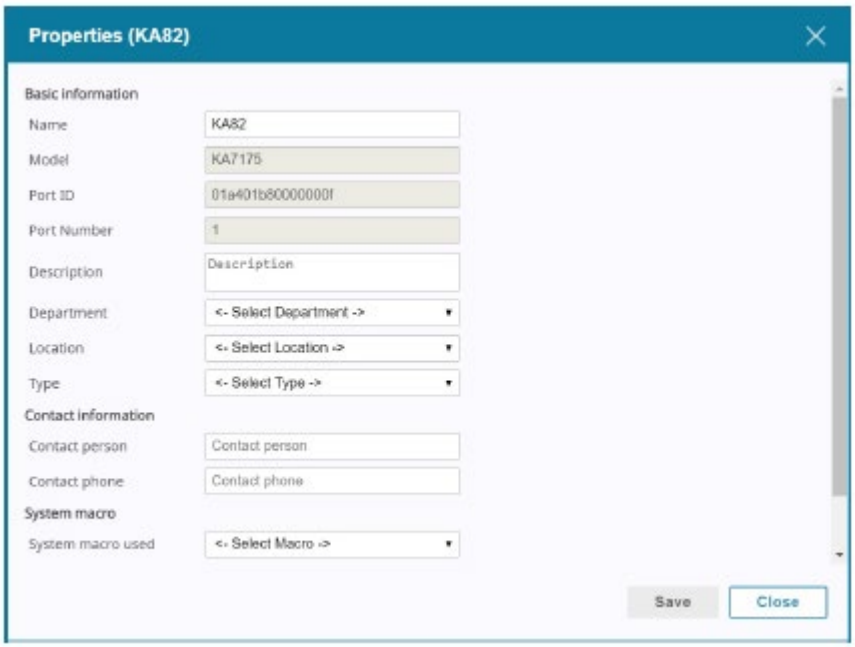
ビューワーの起動

ビューワーを起動してポートの画面を参照したい場合は、対象となるポートにチェックを入れて「Launch Viewer」(ビューワーの起動)をクリックしてください。そうすると、システム側でビューワー(Java または Win クライアント)が新規ウィンドウとして起動します。

詳細については、p.143「操作方法」を参照してください。

プロパティー – システムマクロ

プロパティーの編集画面(「Edit」(編集)→「Properties」(プロパティー)は、基本的にデバイスのプロパティー画面(p.135 参照)と同じですが、システムマクロの項目がある点が異なります。下図はその例です。

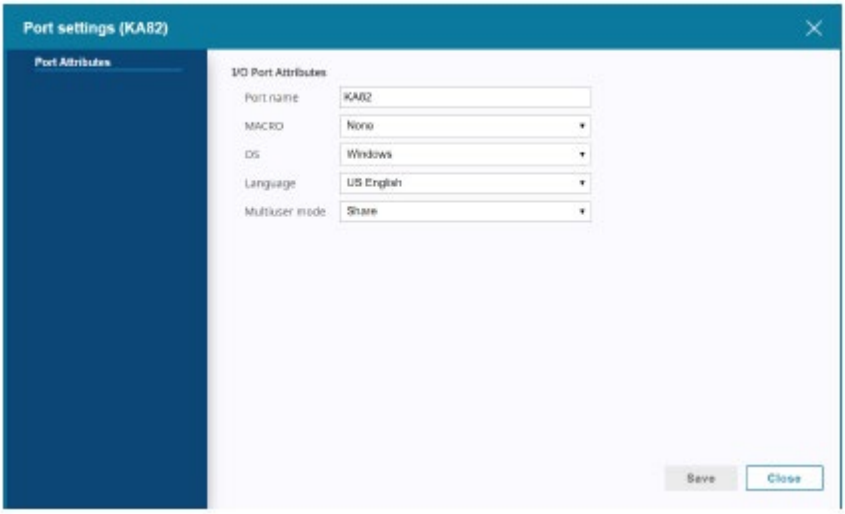


(CC ビューワーで)システムマクロが作成されている場合は、ドロップダウンメニューをクリックするとアイテムを選択することができます。

なお、この項目はサーバーが接続されているポートにしか表示されません。

ポート設定

「Edit」(編集)→「Port Settings」(ポート設定)をクリックすると、ポート属性を編集することができます。下図はその例です。



属性一覧における各列とその説明は、下表の通りです。

見出し	説明
Port Name (ポート名)	このポートに設定された名前です。
Macro (マクロ)	(デバイスビューワーにおいて)システムマクロを作成している場合(例:Win クライアント)は、実行したいマクロをリストから選択してください。変更内容を保存すると、マクロはこのポートに接続されているサーバーへと送信され、そのサーバーで実行されます。
OS	そのポートに接続されたコンピューターで使用している OS を設定します。
Language (言語)	そのポートに接続されたコンピューターで使用している OS 言語を設定します。

(表は次のページに続きます)

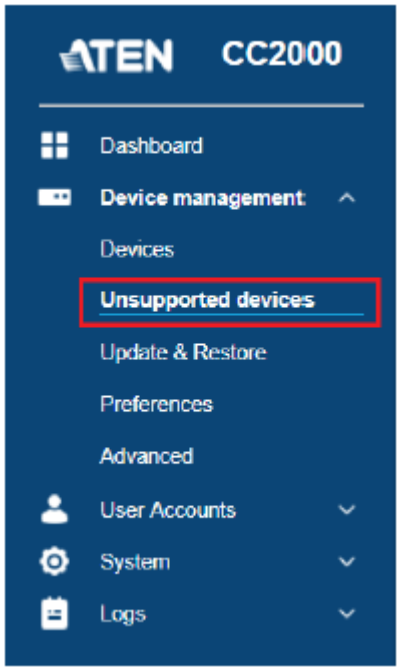
見出し	説明
Multiuser Mode（マルチユーザーモード）	これは、本来のデバイスのアクセスモードの設定(共有・占有・排他)に対応し、複数ユーザーがログインしている場合におけるポートへのアクセス方法を定義します。 ◆ **Exclusive（排他）:** このポートに最初に切り替えたユーザーは、ポートを排他的に操作することができます。他のユーザーはこのポートを参照することができません。タイムアウト機能はこの内容に設定されているポートには適用されません。 ◆ **Occupy（占有）:** このポートに最初に切り替えたユーザーは、ポートを操作することができますが、他のユーザーもそのポートの画面出力を参照することが可能です。ポートを操作しているユーザーが操作をしないまま「Timeout」（タイムアウト）で設定された時間が経過すると、ポートへの操作権限は次にマウスやキーボードの操作を行ったユーザーに移動します。 ◆ **Share（共有）:** ユーザーはポートの操作を同時に共有します。ユーザーからの入力はキューに格納され、順番に実行されます。

項目の設定に関する詳細は、お使いの製品のユーザーマニュアルをご参照ください。

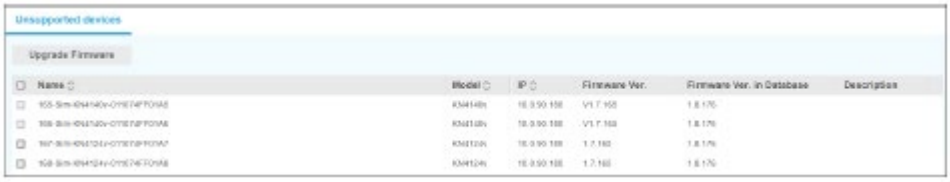
サポート外のデバイス

ATEN デバイスのファームウェアレベルが、CC2000 における現在のソフトウェアバージョンと互換性がない場合、そのデバイスはサポート対象外となります。

サポートされないデバイスがシステムに表示されている場合、下図のようにサブメニューがサイドバーメニューに表示されます。



サポートされないデバイスは、相互表示パネルに一覧表示されます。下図はその例です。



こういったデバイスを CC2000 で管理できるようにするには、ファームウェアを最新バージョンにアップグレードする必要があります。アップグレードを行うには、次の手順に従って操作を行ってください。

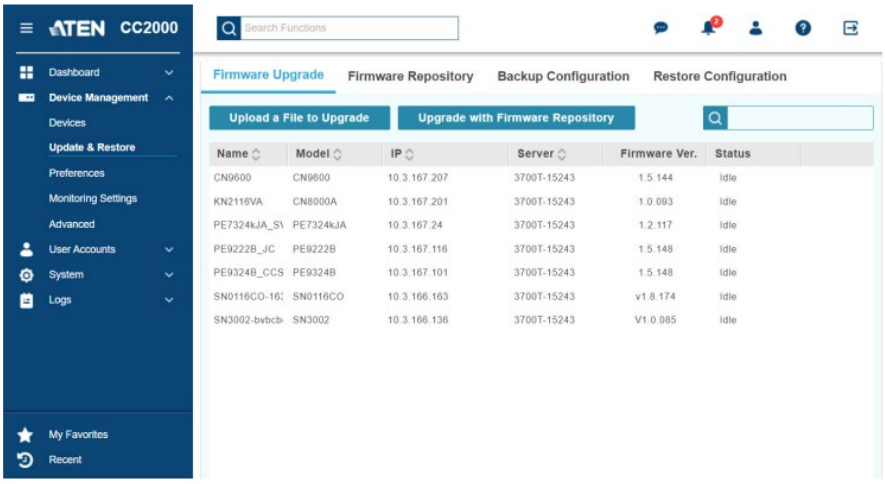
1. デバイスのファームウェアアップグレードファイルを CC2000 に追加してください。追加方法については、p.171「ファームウェアレポジトリー」を参照してください。

2. デバイスのファームウェアアップグレードファイルを CC2000 に保存すると、この画面にあるチェックボックスが有効になりますので、これにチェックを入れてください。
3. 「Firmware Upgrade」(ファームウェアアップグレード)をクリックしてください。
4. 確認メッセージがポップアップ表示されたら、「Yes」(はい)をクリックして、デバイスのファームウェアをアップグレードしてください。

ファームウェアアップグレードが完了すると、デバイスはサポート外のデバイスからは削除されて、「Devices」(デバイス)サブメニューの上部画面に表示されるようになります。

アップデートとリストア

サブメニューを使うと、ファームウェアやバックアップ用ファイルの管理を行うことができます。



この一覧には、最近ファームウェアがアップグレードされた ATEN デバイスと Redfish 対応デバイスが表示されています。

「Status」(状態)列には、デバイスのファームウェアアップグレードの状態が表示されます。

状態	説明
Idle (アイドル)	デバイスでファームウェアアップグレードのラインナップが存在しない場合に CC2000 を再起動すると、この状態が表示されます。
Waiting (待機中)	デバイスはファームウェアアップグレードを待機しています。
Uploading (アップロード中)	このデバイスに対して、ファームウェアアップグレードファイルをアップロードしています。
Upgrading (アップグレード中)	デバイスをアップグレードしています。
Succeeded (成功)	ファームウェアのアップグレードやアップロードは正常に終了しました。
Failed (失敗)	ファームウェアのアップグレードやアップロードに失敗しました。

ファームウェアアップグレード

「Firmware Upgrade」(ファームウェアアップグレード)タブでは、2 種類あるデバイスのアップグレードの方法から、いずれかを選択することができます。

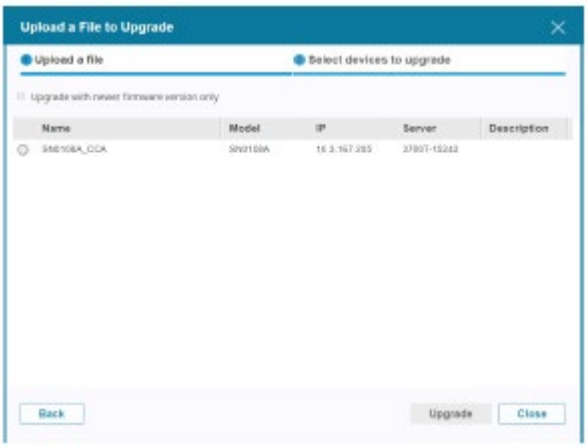
アップグレードファイルのアップロード

デバイスをアップグレードする 1 つ目の方法は、**アップグレードファイルのアップロード**です。この方法でアップグレードを行う場合は、次の手順に従って操作を行ってください。

1. アップグレード対象となるデバイスを指定し、弊社ウェブサイトからファームウェアファイルをダウンロードしてください。ダウンロードは、画面上部にある検索マーク(虫眼鏡のアイコン)をクリックして型番を入力し、製品ページにアクセスした後、「サポートとダウンロード」メニューをクリックすると、使用可能なパッケージのリストが表示されます。

2. 「**Upload a File to Upgrade**」(アップグレードファイルのアップロード)をクリックしてください。そうすると、ウィンドウがポップアップ表示されます。

3. 「**参照**」をクリックして、お使いのシステムにあるファームウェアファイルを指定したら、「Next」（次へ）をクリックしてください。



4. アップグレード対象となるデバイスを選択したら、「Upgrade」（アップグレード）をクリックしてください。

5. そうすると、確認メッセージが表示されます。ファームウェアアップグレードを続行する場合は「Yes」（はい）をクリックしてください。

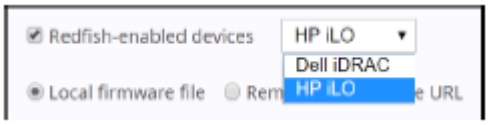
Redfish 対応デバイスのアップグレード

Redfish 対応デバイスをお使いの場合は、「**Upload a File to Upgrade**」(アップグレードファイルのアップロード)を使ってアップグレードを行ってください。

1. アップグレード対象となる Redfish 対応デバイスを指定し、弊社ウェブサイトからファームウェアファイルをダウンロードしてください。ダウンロードは、画面上部にある検索マーク(虫眼鏡のアイコン)をクリックして型番を入力し、製品ページにアクセスした後、「サポートとダウンロード」メニューをクリックすると、使用可能なパッケージのリストが表示されます。

2. 「**Upload a File to Upgrade**」(アップグレードファイルのアップロード)をクリックしてください。そうすると、ウィンドウがポップアップ表示されます。

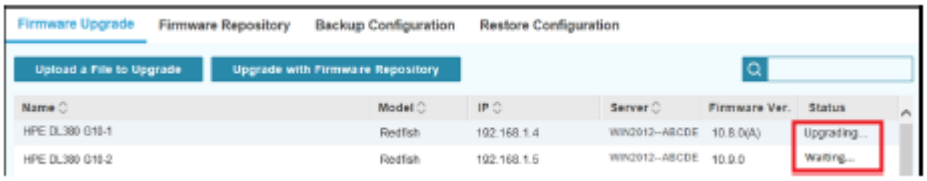
3. 「Redfish-enabled devices」(Redfish 対応デバイス)の項目にチェックを入れると、Redfish 対応デバイスの種類を選択できるドロップダウンメニューが表示されます。



4. Redfish 対応デバイスの種類を選択したら、「**参照**」をクリックして、お使いのシステムにあるファームウェアファイルを指定し、「**Next**」(次へ)をクリックしてください。

5. そうすると、この Redfish 対応デバイスの種類と同じデバイスが一覧表示されます。アップグレード対象となるデバイスにチェックを入れて選択したら(複数選択可)、「**Upgrade**」(アップグレード)をクリックしてください。
「Status」(状態)列は、アップグレード中のデバイスの場合は「Upgrading...」(アップグレード中

…)と、また、待機中のデバイスの場合は「Waiting…」(待機中…)と、それぞれ表示されます。

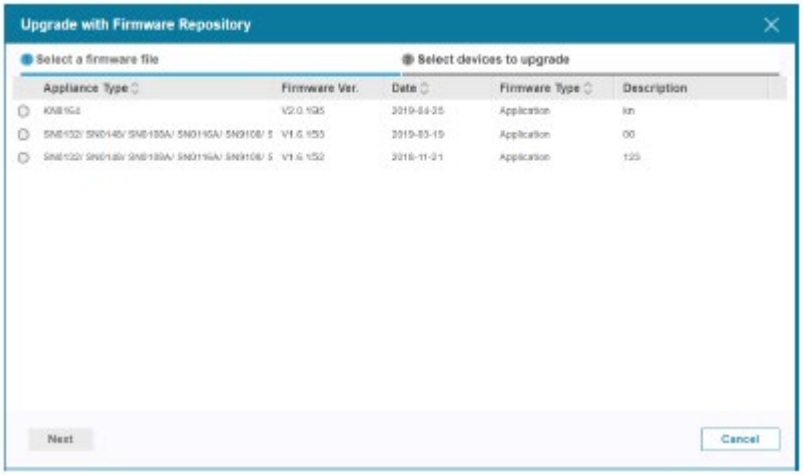


ファームウェアレポジトリーを使ったアップグレード

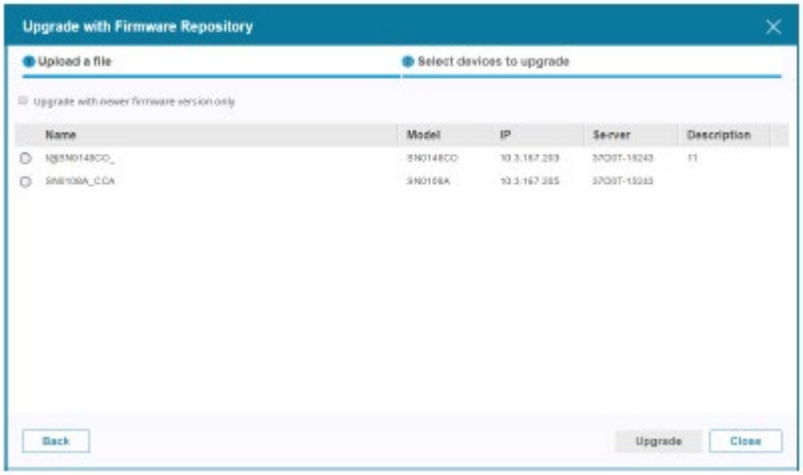
デバイスをアップグレードする 2 つ目の方法は、**ファームウェアレポジトリーを使ったアップロード**です。この方法でアップグレードを行う場合は、次の手順に従って操作を行ってください。

1. アップグレード対象となるデバイスを指定したら、アップグレードファイルがファームウェアレポジトリーにあることを確認してください。ファームウェアレポジトリーをファームウェアレポジトリーにアップロードする方法については、p.171「ファームウェアレポジトリー」を参照してください。

2. 「Upgrade with Firmware Repository」(ファームウェアレポジトリーを使ったアップグレード)をクリックしてください。そうすると、ウィンドウがポップアップ表示されます。



3. ファームウェアファイルを選択したら、「Next」（次へ）をクリックしてください。

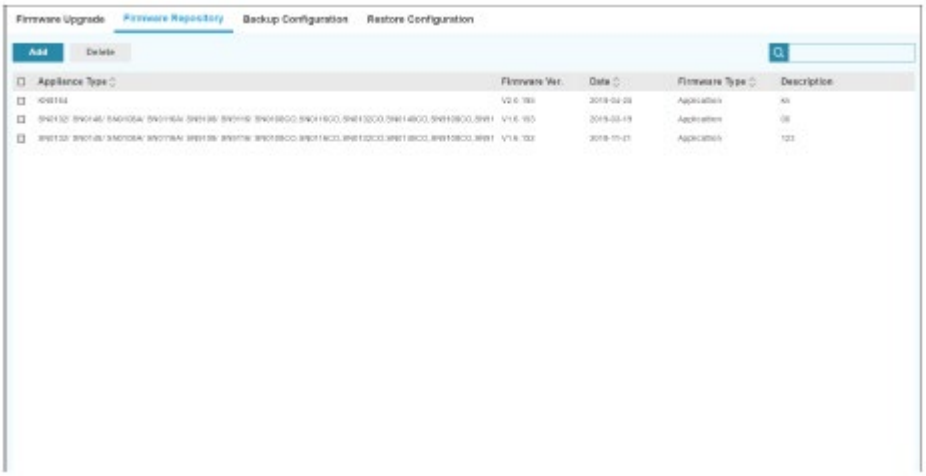


4. アップグレード対象となるデバイスを選択したら、「Upgrade」（アップグレード）をクリックしてください。

5. そうすると、確認メッセージが表示されます。ファームウェアアップグレードを続行する場合は「Yes」（はい）をクリックしてください。

ファームウェアレポジトリー

「Firmware Repository」（ファームウェアレポジトリー）タブは下図のような画面です。



この画面には、CC2000 に保存されているアップグレードファイル全てが一覧表示されるため、各ファイルの概要を一目で把握することができます。

この一か所から最新のファームウェアアップグレードファイルをディストリビューションとして利用できるようにすることで、CC2000 からアップグレードを簡単に実行して、システムにおける全てのデバイスを同時に運用し、最新のファームウェアレベルにすることができるようになります。

注意：
1. ファームウェアアップグレードは、「Task Manager」（タスクマネージャー）サブメニューからも実行可能です。詳細は p.261 を参照してください。
2. 新しいファームウェアアップグレードのパッケージは、利用可能になると弊社ウェブサイトに公開されます。このサイトへ定期的にアクセスし、パッケージや製品に関する情報をご確認ください。

ファームウェアファイルの追加

1. ファームウェアファイルを一覧に追加するには、「**Add**」（追加）をクリックしてください。そうすると、ウィンドウがポップアップ表示されます。

2. 「**参照**」をクリックして、ファームウェアファイルを選択してください。
3. 説明を入力し、「**Save**」（保存）をクリックしてください。

注意： CC2000 と互換性がないファームウェアファイルは、（スタンドアロンの設定では、そのデバイスと互換性があるものであっても）CC2000 で読み込むことができません。

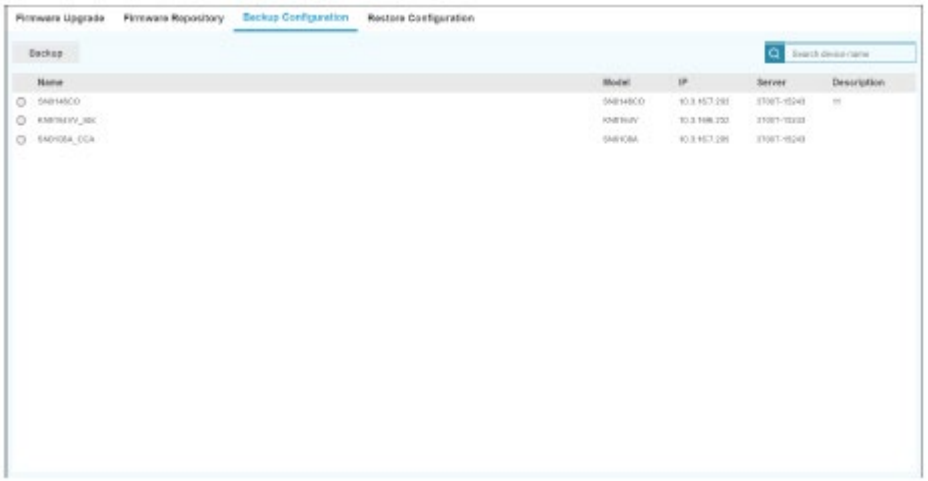
ファームウェアファイルの削除

一覧からファームウェアファイルを削除するには、ファイルにチェックを入れて選択し（複数選択可）、「**Delete**」（削除）をクリックしてください。

そうすると、確認メッセージが表示されます。削除を続行する場合は「**Yes**」（はい）をクリックしてください。

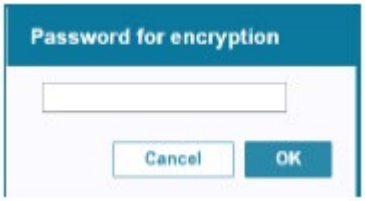
バックアップの設定

「Backup Configuration」(バックアップの設定)タブには、CC2000 に登録されているデバイスと、そのデバイスに関連する情報が一覧表示されます。



デバイス設定をバックアップするには、対象となるデバイスを選択して「Backup」(バックアップ)をクリックしてください。

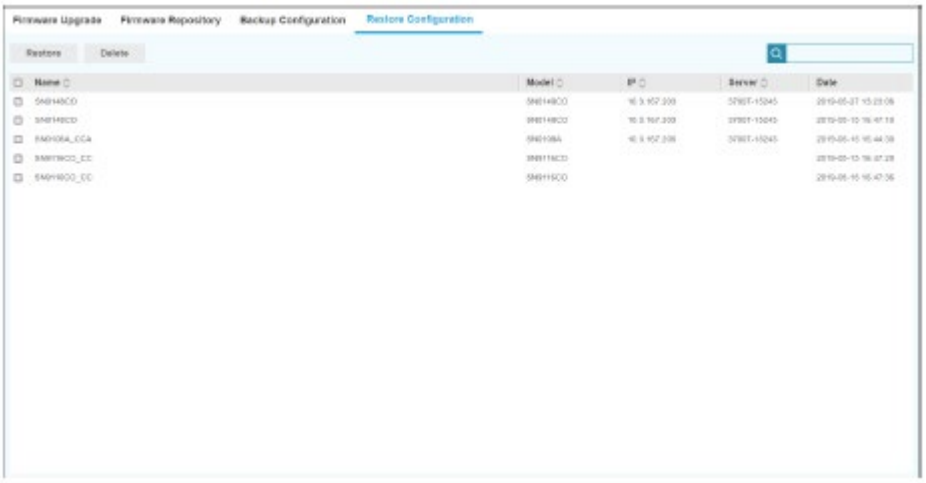
そうすると、システム側から暗号化用パスワードの入力が求められます。



「OK」をクリックして、設定のバックアップを作成してください。

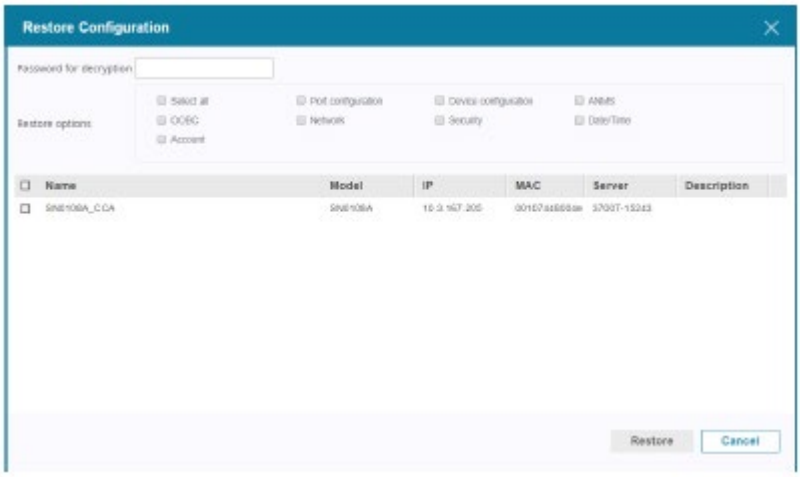
設定のリストア

「Restore Configuration」(設定のリストア)タブには、CC2000 における現在のデバイス設定が一覧表示されます。



リストア

1. 設定をリストアするには、一覧から設定ファイルをクリックして選択し、「**Restore**」(リストア)をクリックしてください。そうすると、ウィンドウがポップアップ表示されます。



2. 設定ファイルに掛けられている暗号化パスワードを「Password for encryption」(暗号化用パスワード)欄に入力してください。
3. リストアするオプションのチェックボックスにチェックを入れて選択してください(複数選択可)。
4. リストア対象となるデバイスのチェックボックスにチェックを入れて選択してください。
5. 「**Restore**」(リストア)をクリックしてください。そうすると、確認メッセージがポップアップ表示されます。リストアを続行する場合は「**Yes**」(はい)をクリックしてください。

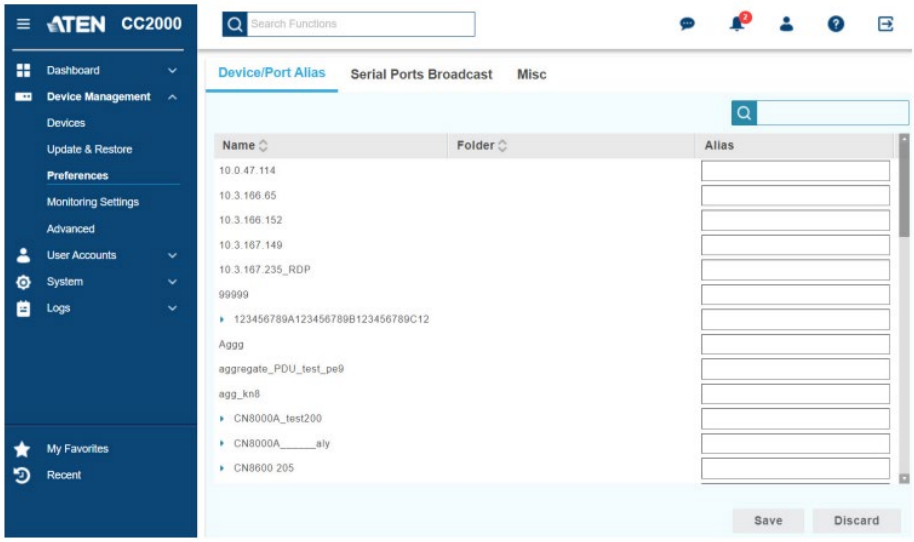
削除

一覧から設定ファイルを削除するには、ファイルにチェックを入れて選択し（複数選択可）、「Delete」（削除）をクリックしてください。

そうすると、確認メッセージが表示されます。削除を続行する場合は「Yes」（はい）をクリックしてください。

環境設定

「Preferences」(環境設定)サブメニューでは、複数のタブを使ってユーザーの環境設定を定義することができます。



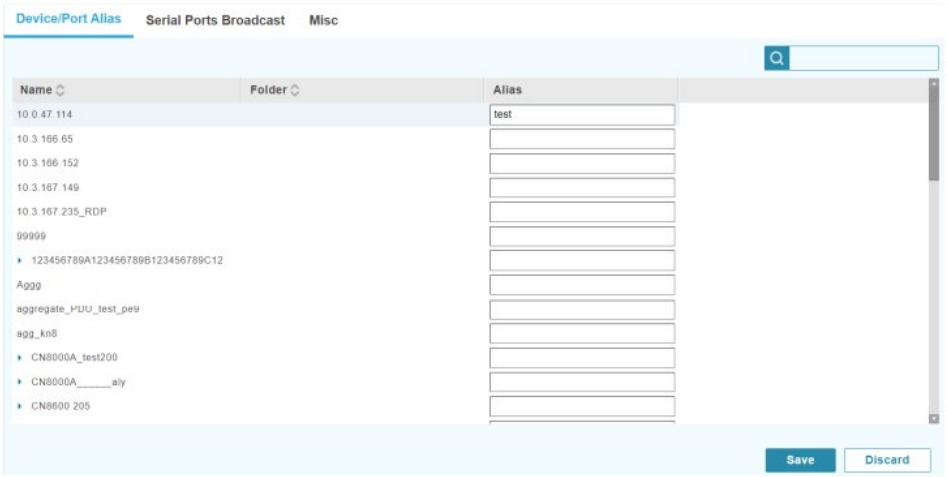
デバイスやポートのエイリアス

「Device/Port Alias」(デバイスやポートのエイリアス)タブでは、お使いのデバイス、ポート、およびアウトレットが識別しやすくなるよう、エイリアス(別名)を付けることができます。

◆ デフォルトでは、デバイスしか表示されません。ポートやアウトレットにエイリアスを付けるには、対象となるデバイスの前にある矢印マークをクリックして、配下にあるポートやアウトレットを表

示してください。

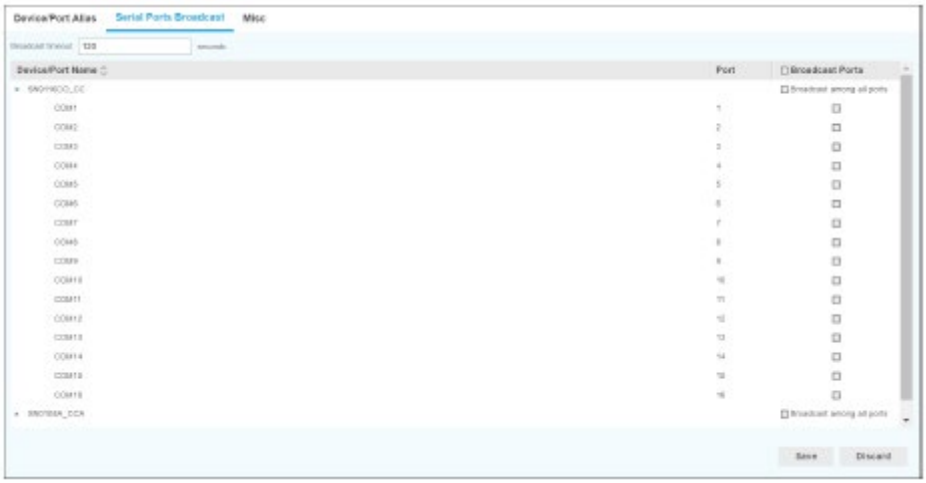
◆ そのデバイスやポートまたはアウトレットに対応した「Alias」(別名)欄に、エイリアスとして設定する文字列を入力したら、「Save」(保存)をクリックしてください。



注意: エイリアスは、そのエイリアスを作成した特定のユーザーにしか表示されません。その他のユーザーが見られるのは、元の名前(もしくは、そのユーザー自身が設定したエイリアス)だけです。

シリアルポートのブロードキャスト

「Serial Ports Broadcast」(シリアルポートのブロードキャスト)タブでは、コマンドを受信するシリアルデバイスのポートを選択することができます。複数のブロードキャストポートを選択すると、1 箇所のシリアルポートで行われた変更が、全てのブロードキャストポートに反映されるようになります。



ブロードキャスト機能を使うには、SN ビューワーを使ってブロードキャストポートにアクセスし、コントロールパネルからブロードキャスト機能を有効にする必要があります。詳細は、SN シリーズ製品のユーザーマニュアルにおける「コントロールパネル機能」のセクションを参照してください。

Broadcast timeout (ブロードキャストのタイムアウト) : ユーザーからの入力がないまま、ここで指定された時間が経過すると、(他のポートに対する) ブロードキャスト機能は自動的に終了します。タイムアウト時間は 0～240 秒の範囲で設定してください。0 を設定すると、この機能を無効にします。

一覧の右端にある「**Broadcast Ports**」(ブロードキャストポート) にチェックを入れると、表にある全てのシリアルポートのチェックボックスにチェックを入れます。

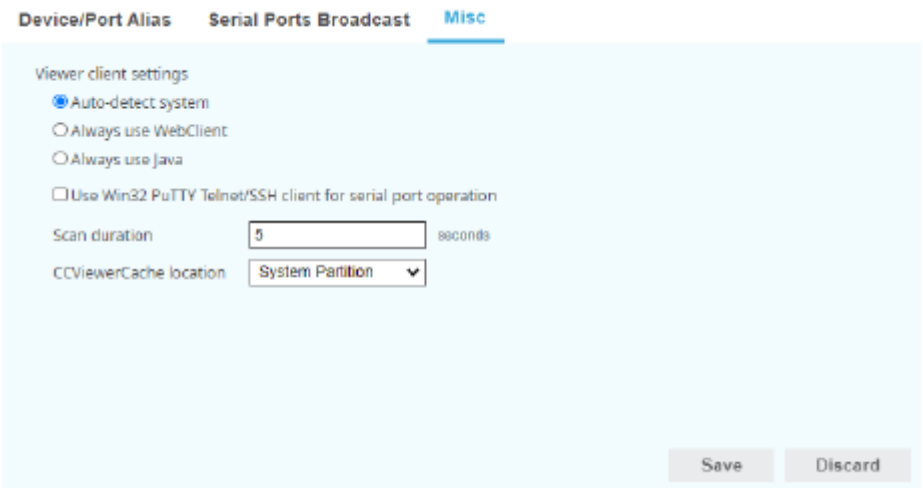
また、「**Broadcast among all ports**」(全てのポートにブロードキャストする) にチェックを入れると、特定のデバイスにおいて、全てのシリアルポートのチェックボックスにチェックを入れます。

デバイスの先頭にある矢印をクリックすると、シリアルデバイスを展開して、配下にあるシリアルポートを全て確認することができます。ここから、個々のポートにチェックを入れて、ブロードキャストの対象となるポートを選択することができます。

注意:	CC2000 は、ブロードキャストポートに対応したシリアルコンソールサーバーに接続されたシリアルデバイスだけを一覧表示します。

その他

「Misc」(その他) タブでは、ビューワークライアントの設定と、CC ビューワーのキャッシュを保存するパスの変更を行うことができます。



◆ 「Auto-detect system」(システムの自動検出)が選択されている場合、CC2000 はユーザーがログインに使用したブラウザ(IE またはその他のブラウザー)を判別します。ユーザーが IE でログインしている場合は、デバイスやポートにアクセスする際に Windows クライアントビューワーを起動します。これ以外のブラウザーを使用している場合は、Web クライアントビューワーがサポートされていれば、このビューワーを、それ以外の場合は Java クライアントビューワーを、それぞれ起動します。

◆ 「Always use WebClient」(常に Web クライアントを使用する)が選択されている場合、CC2000 は、Web クライアントビューワーがサポートされていれば、このビューワーを、それ以外の場合は Java クライアントビューワーを、それぞれ起動します。

注意: Web クライアントビューワーに対応している ATEN IP-KVM スイッチをお使いの場合は、各製品のウェブページにて詳細をご確認ください。

◆ 「Always use java」(常に Java を使用する)が選択されている場合、CC2000 はユーザーがログインしているブラウザーの種類にかかわらず、Java クライアントビューワーを起動します。

◆ 「Use Win32 PuTTY Telnet/SSH client for serial port operation」(シリアルポートの操作時に Win32 PuTTY Telnet/SSH クライアントを使用する)のオプションにチェックが入っていると、IE を使って CC2000 経由でシリアルデバイスに接続した際に PuTTY Telnet/SSH クライアントソフトウェアを起動します。

◆ 「Scan Duration」(スキャンインターバル)では、パネルアレイモードでポートを参照する際にポートをスキャンするインターバル時間を設定します。

◆ 「CCViewerCache location」(CC ビューワー・キャッシュの場所)では、CC ビューワーのキャッシュが保存されるドライブを指定します。クライアント PC のシステムドライブに保存されるよう、この場所はデフォルトではシステムパーティションに設定されています。

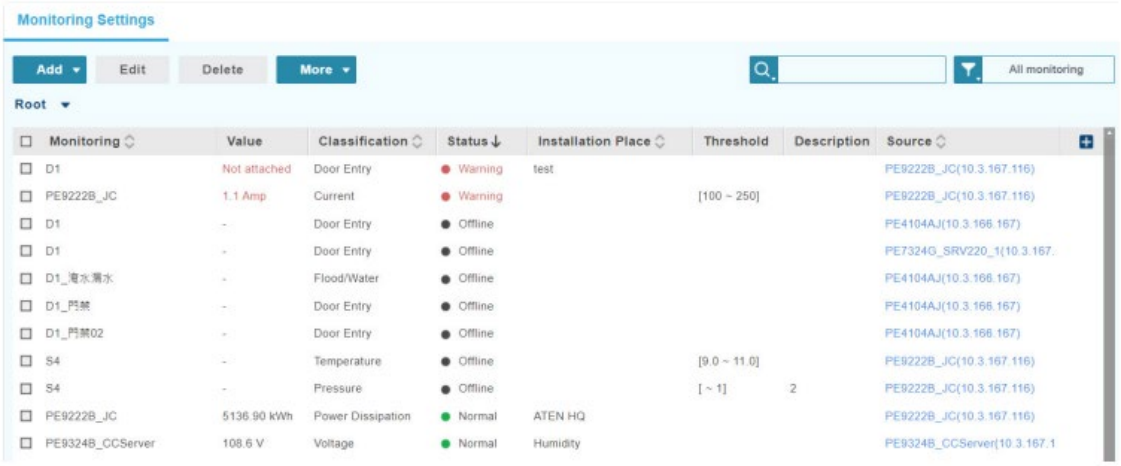
注意: 存在しないドライブを選択した場合、CC ビューワーのキャッシュは、クライアント PC のシステムドライブに保存されます。

監視設定

ユーザーは、ポートまたは機器の状態（例：気温、湿度、ドアの開閉、電圧、消費電力、電流）の監視や記録を行うために、モニターアイテムを作成することができます。また、E メールやメッセージによる重要なイベントの通知を受けることも可能です。

注意：
- ◆ 監視対象となる機器やポートの値を 1 回あたり取得するのに確保されるデータサイズは 8 バイトです。仮に、CC2000 が 15 秒おきに読み込みを更新するとなると、100 の監視アイテムに対して 1 日で約 4.5MB が必要となります（100×8×60/15×24×60）。
- ◆ システムは、セカンダリー冗長サーバーに対する監視データのバックアップをサポートしません。監視データをバックアップする場合は、別のサーバーに対してバックアップのタスクを作成してください。詳細は、p.263「プライマリーサーバーのデータベースバックアップ」を参照してください。

「Monitoring Settings」（監視設定）画面に移動するには、「**Device Management**」（デバイス管理）→「**Monitoring Settings**」（監視設定）へと進んでください。そうすると、下図のような画面が表示されます。



- ◆ 「Monitoring Settings」（監視設定）画面では、作成済みモニターの一覧を確認することができます。ここには次の情報（列）が提供されています。
  - ➢ **Value**（値）：監視対象機器の電流値または状態です。
  - ➢ **Classification**（分類）：監視対象機器の種類を表示します。
  - ➢ **Status**（状態）：監視対象機器の状態全般（正常、オフライン、ロック、警告）を表示します。

- Source（ソース）：ソースデバイスの型番および IP アドレスが表示されます。ソースの文字列（青色）をクリックすると、そのデバイスリストの画面にリダイレクトします。

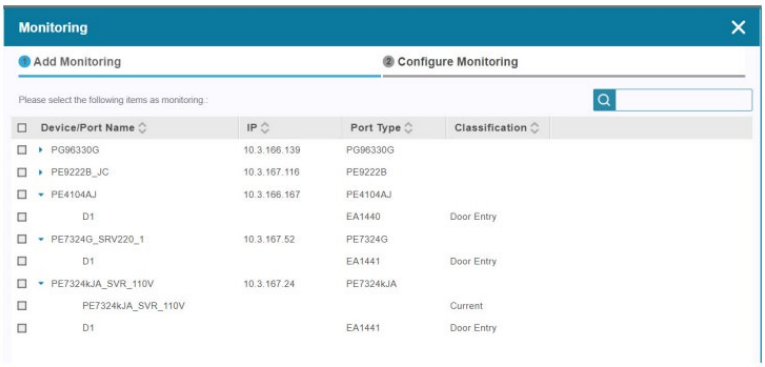
◆ 列の見出しに基づいてエントリーを再配置するには、各列の文字列の隣にあるマークをクリックしてください。

◆ 表示されている列を非表示にするには、  をクリックしてポップアップメニューから当該アイテムを選択してください。

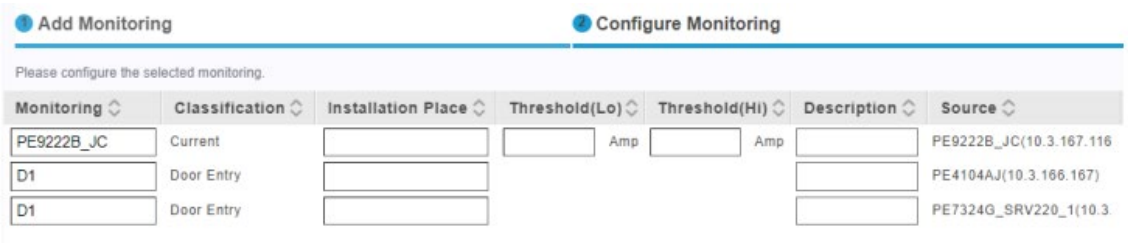
◆ システムでサポートされるモニターアイテムの数は、最大で 10000 です。

モニターアイテムの作成

1. 監視対象となるデバイスや機器がデバイスリストに追加されていることを確認してください（「Device Management」（デバイス管理） → 「Devices」（デバイス））。詳細は、p.78「デバイスの追加」を参照してください。
2. 「**Device Management**」（デバイス管理） → 「**Monitoring Settings**」（監視設定）に進んでください。
3.  をクリックして、「**Monitoring**」（監視）を選択してください。そうすると、利用可能なデバイスリストが表示されます。



4. モニターアイテムを作成するデバイスやポート（単体または複数）をクリックして選択したら、「**Next**」（次へ）をクリックしてください。そうすると、下図のような画面が表示されます。



5. 必要に応じて設定値や説明を入力または編集してください。

注意:	通知が設定されていると、CC2000 システムが、しきい値の超過や監視対象のドアの開錠を検知した場合にユーザー通知を行います。

6. 「Add」(追加)をクリックしてください。選択されたデバイスやポートが監視リストに表示されます。

注意:	センサーポートに対してモニターアイテムが作成されている場合は、このロックが解除されていることを確認してください。

モニターアイテムの編集

◆ モニターアイテムを 1 つだけ編集する場合は、  をクリックしてください。

◆ 複数のモニターアイテムを同時に編集する場合は、対象となるアイテムをクリックして選択し、  をクリックしてください。

フォルダーの追加

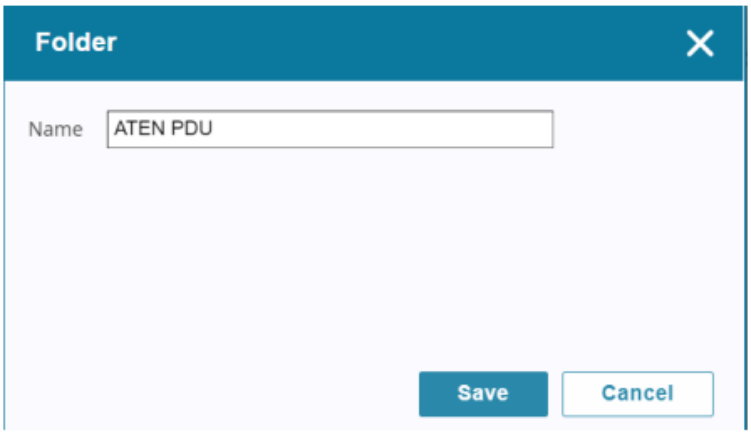
必要に応じて、追加されたモニターアイテムを場所や製品シリーズごとに整理できるよう、フォルダーやサブフォルダーを作成することができます。フォルダーを追加するには、次のいずれかの方法で操作を行ってください。

■追加ボタン()を使う方法

1. 「Monitoring Settings」(監視設定)画面で、対象フォルダーの上にマウスカーソルを移動させてください。
2.  をクリックして、選択メニューを表示したら、「Folder」(フォルダー)を選択してください。

■ナビゲーションメニューを使う方法

1. 「Monitoring Settings」(監視設定)画面で、フォルダーを追加したい階層またはフォルダーに移動してください。
2.  をクリックしてください。
3. ポップアップメニューで「Folder」(フォルダー)をクリックしてください。そうすると、次の画面が表示されます。



4. フォルダーに名前を設定したら、「Save」(保存)をクリックしてください。

フォルダーの名前を編集するには、対象となるデバイスの上にマウスカーソルを移動させ、  をクリックして「Properties」(プロパティー)を選択してください。

追加されたモニターアイテムの移動

「Move To」(次に移動)機能を使うと、追加したモニターアイテムの移動や整理が行えます。

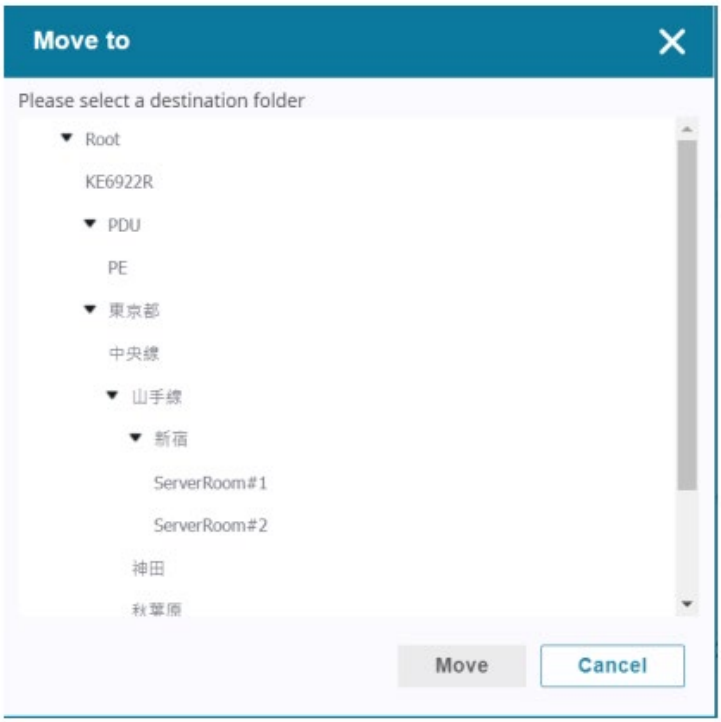
1 つまたは複数の追加モニターアイテムを移動するには、次の手順に従って操作を行ってください。

1. 「Monitoring Settings」(監視設定)画面で、対象となるモニターアイテムまたはフォルダーの上にマウスカーソルを移動させ、「**詳細**」アイコン( )をクリックしてください。

注意: 複数のモニターアイテムやフォルダーを移動させる場合は、「Monitoring Settings」(監視設定)画面で対象となるアイテムをクリックして選択してから、More ボタンをクリックしてください。

---

2. ポップアップメニューで、「**Move to**」(次へ移動)をクリックしてください。そうすると、構造図が表示されます。



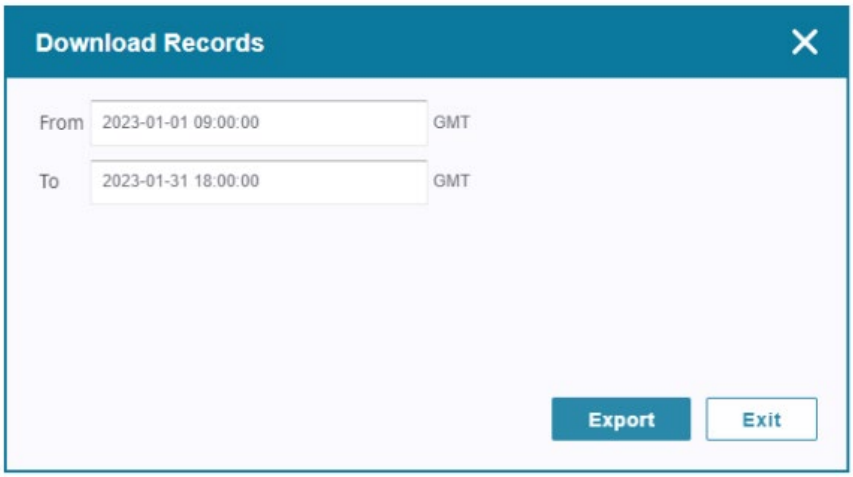
3. 場所をクリックして選択したら、「**Move**」(移動)をクリックして、設定を完了させてください。

監視記録のエクスポート

監視対象のポートおよびデバイスのデータを CSV ファイルにエクスポートするには、次の手順に従って操作を行ってください。

1. 「Monitoring Settings」(監視設定)画面で、モニターアイテムを選択してください(複数選択可)。
2. 

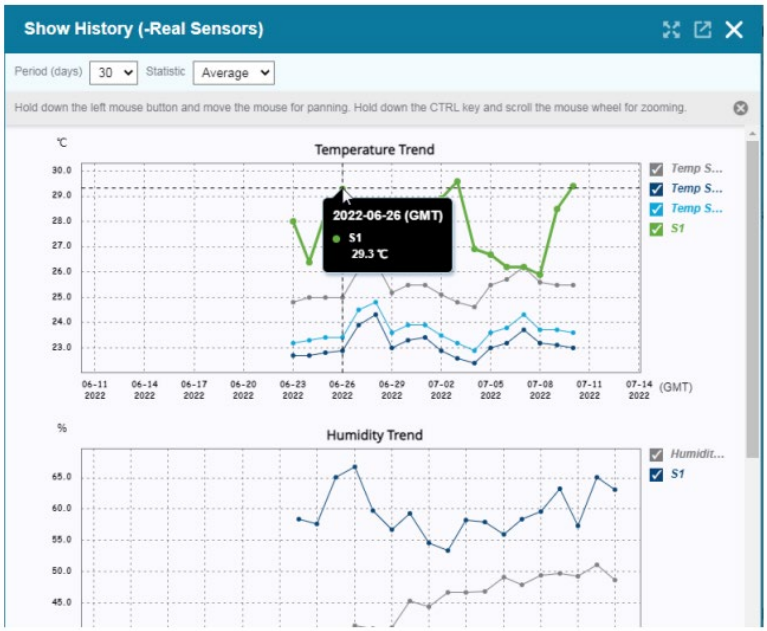
をクリックして「Download Records」(記録のダウンロード)を選択してください。下図のような画面が表示されます。



3. 期間をクリックして特定したら、「Export」(エクスポート)をクリックしてください。
そうすると、記録は CSV 形式でエクスポートされます。複数のモニターアイテムが選択されている場合は、各アイテムのデータが個別の CSV ファイルに出力され、ZIP 形式で圧縮されます。

監視機器のチャートを参照するには

履歴表示機能を使うと、監視対象となるポートおよび機器のトレンドチャート(下図参照)を生成し参照することができます。この機能を活用することで、管理者はシステムで起こっている変化を認識することができます。


Show History (-Real Sensors)
Period (days)
30
Statistic
Average
Hold down the left mouse button and move the mouse for panning. Hold down the CTRL key and scroll the mouse wheel for zooming.
℃
Temperature Trend
30.0
29.0
28.0
27.0
26.0
25.0
24.0
23.0
2022-06-26 (GMT)
S1
29.3 ℃
Temp S...
Temp S...
Temp S...
S1
06-11 2022
06-14 2022
06-17 2022
06-20 2022
06-23 2022
06-26 2022
06-29 2022
07-02 2022
07-05 2022
07-08 2022
07-11 2022
07-14 2022
(GMT)
%
Humidity Trend
65.0
60.0
55.0
50.0
45.0
Humidit...
S1

■トレンドチャートの作成

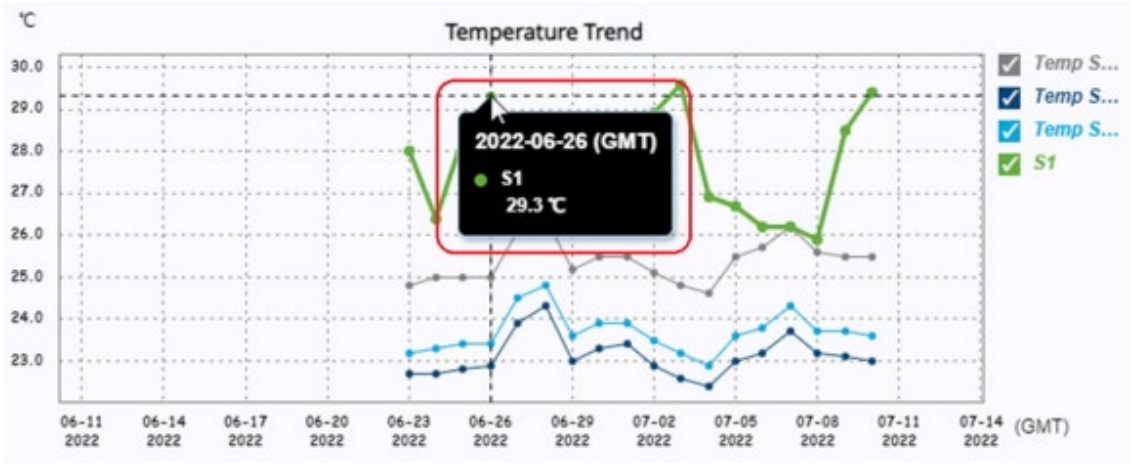
1. モニターアイテムを 1 つまたは複数選択したら、 

をクリックして、「Show History」(履歴の表示)を選択してください。
2. 表示期間を変更する場合は、「Period」(期間)ドロップダウンメニューをクリックして、期間を選択してください。デフォルトでは「30 days」(30 日間)に設定されています。
3. 分析を変更するには、「Statistic」(統計)ドロップダウンメニューをクリックし、オプションを選択してください。デフォルトでは「Average」(平均)に設定されています。
   トレンドチャートは、すぐに作成されます。同じタイプのポートや機器(例:別々の機器に取り付けられた温度センサー)は、1 つのチャートに表示されます。

■分析チャートの読み方

◆ 「Show History」(履歴の表示)画面を最大化するには、画面右上にある  をクリックしてください。

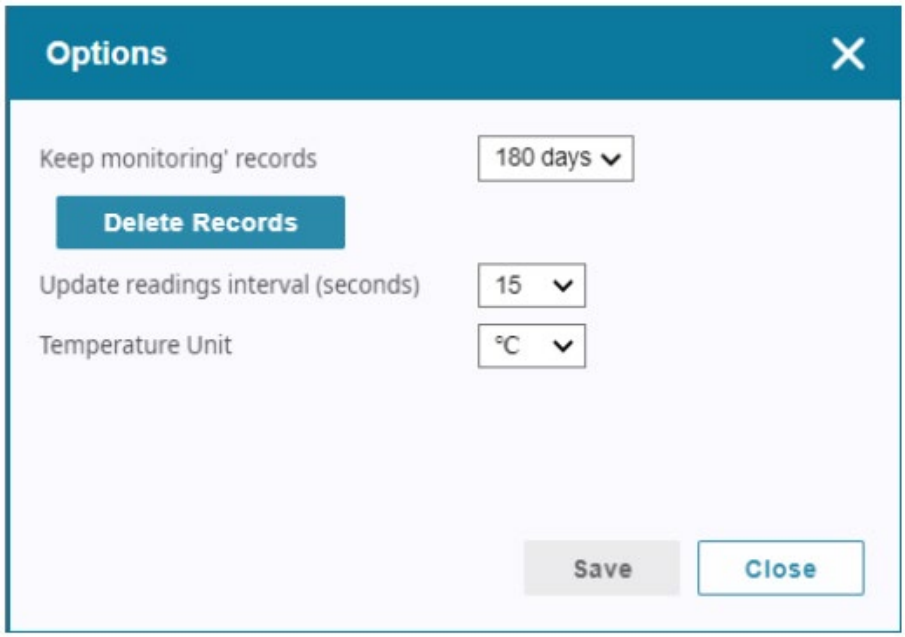
◆ 特定の日における値を表示するには、チャートのドットの上にマウスカーソルを重ねてください。



◆ 表示期間外の統計を確認する場合は、グラフをクリックしたまま左右にドラッグしてください。

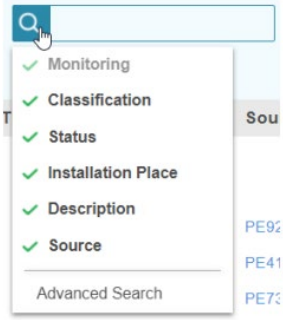
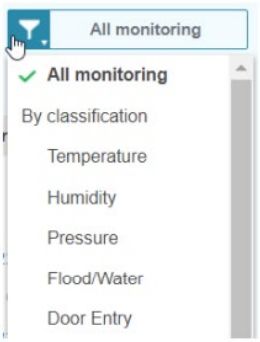
モニターアイテムの全般設定

（監視機器の値を取得するための）保存期間、気温単位、検出インターバルを変更したり、監視記録のデータを削除したりするには、More をクリックして「Options」（オプション）を選択してください。



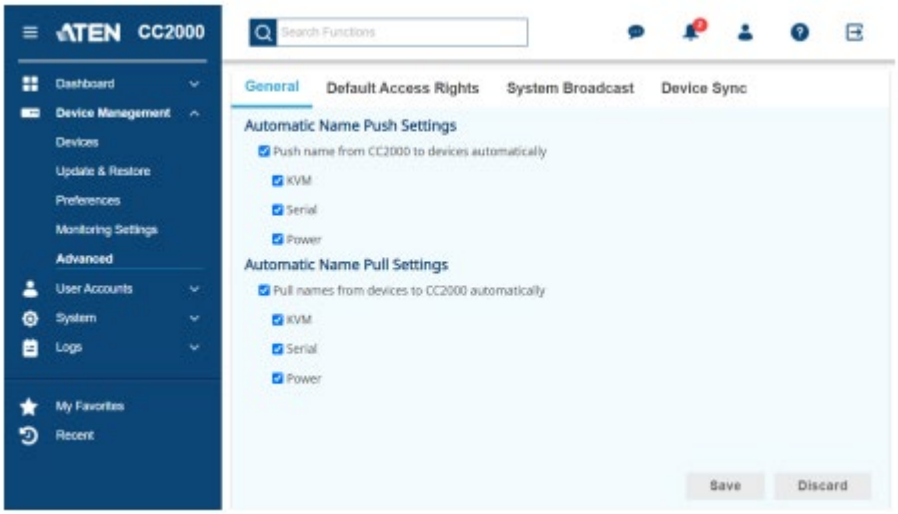
検索とフィルターによるモニターアイテムの配置

検索ボックスやフィルターを使うと、指定した条件に基づいてモニターアイテムを素早く配置することができます。この機能には、「Monitoring Settings」(監視設定)画面の右上からアクセスすることができます。検索ボックスとフィルターの機能については、次の表を参照してください。

コントロール	説明
	モニターアイテムを、検索ボックスに入力されたキーワードに基づいて検索します。
	検索アイコンをクリックすると、検索範囲を変更します。 
高度な検索	追加されたモニターアイテムの全項目(モニター名、説明、デバイス型番、IP アドレス、部署、サーバー、デバイスの状態)を条件として高度な検索を行います。この機能にアクセスするには、検索アイコンをクリックして「Advanced Search」(高度な検索)を選択してください。
	フィルターボックスを使うと、選択されたフィルターを使って検索結果をさらに絞り込みます。フィルターのマークがついた検索ボックスをクリックして、ポップアップメニューからフィルターを選択してください。 

詳細

「Advanced」（詳細）サブメニューには、詳細設定を行う各種タブが提供されています。



全般

「General」（全般）タブは下図のような画面です。

この画面では、CC2000 とセットアップデバイスの間における名前の自動同期の設定を行います。有効にしたい機能のチェックボックスにチェックを入れ、「Save」（保存）をクリックしてください。

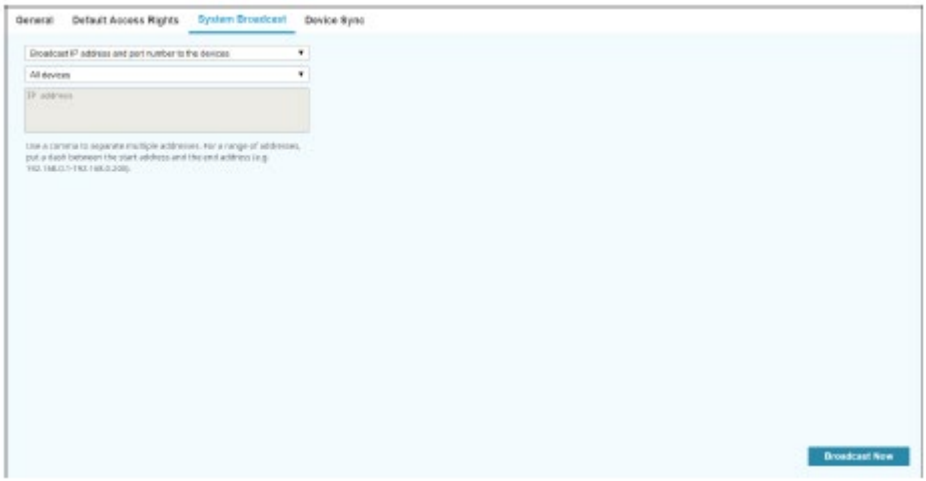
デフォルトのアクセス権限

「Default Access Rights」(デフォルトのアクセス権限)タブは下図のような画面です。

この画面では、CC2000 システムに追加された新規デバイス全てに対するデフォルトのアクセス権限の設定を行うことができます。

システムのブロードキャスト

「System Broadcast」(システムのブロードキャスト)タブは下図のような画面です。



デバイスに対する IP アドレスとポート番号のブロードキャスト

デバイスが CC2000 と通信できるようにするには、ANMS 設定で CC2000 の IP アドレスとデバイス管理のポート番号をあらかじめ定義しておく必要があります。

ドロップダウンメニューから「Broadcast IP address and port number to the devices」（デバイスに対する IP アドレスとポート番号のブロードキャスト）のオプションを選択すると、CC2000 は、同じネットワークに接続されているデバイスに対して、自身の IP アドレスとデバイス管理用のポート番号をブロードキャストします。このため、これらの情報は（手動で設定しなくても）デバイスに自動で設定されることになります。この処理は、CC2000 ネットワークにデバイスを初めて接続する場合、またはデバイスがデフォルト設定にリセットされた場合に実行されます。

注意：
1. この機能では、情報をブロードキャストするのにUDPを使用します。このため、デバイスは（VPN が正しく動作できるよう）CC2000 と同一セグメントにセットアップされている必要があります。UDP は 18768 番のポートを使用します。CC2000 がインストールされているコンピューターのネットワーク設定でこのポートが開いていることを確認してください。
2. セキュリティーを最大限に確保するために、ブロードキャスト機能が終了し、情報がデバイスに対して送信されると、デバイスは他の CC2000 からの UDP ブロードキャストを受け付けなくなります。
3. CC2000 を変更する場合は、ANMS 設定画面を使用して IP アドレスとポート番号を指定してください。

次のドロップダウンメニューから、「All Devices」（全てのデバイス）または「Specific IP Address」（特定の IP アドレス）を選択してください。後者を選択した場合は、次の欄に IP アドレスを入力してください。

「Broadcast Now」（今すぐブロードキャスト）をクリックすると、ブロードキャストを開始します。

変更済み IP アドレスとポート番号をデバイスにブロードキャスト

「Broadcast changed IP address and port number to the devices」（変更済み IP アドレスとポート番号をデバイスにブロードキャスト）の機能は、CC2000 の IP アドレスやデバイス管理ポートが変更された場合に使用します。

ドロップダウンメニューからこのオプションを選択すると、CC2000 は、同じネットワークに接続されているデバイスに対して、自身の新しい IP アドレスとデバイス管理用のポート番号をブロードキャストするため、これらの情報はデバイスの ANMS 設定へと自動的に反映されます。

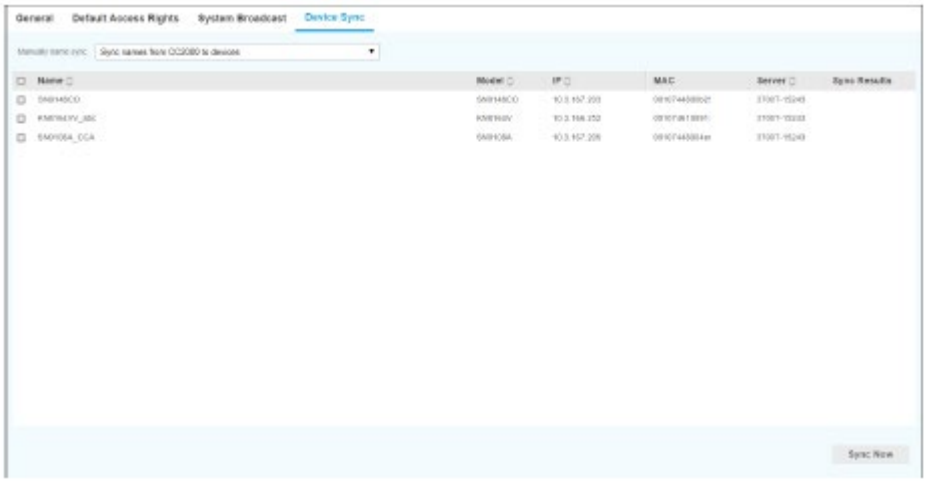
注意： 1. この機能では、情報をブロードキャストするのにUDPを使用します。このため、デバイスは（VPN が正しく動作できるよう）CC2000 と同一セグメントにセットアップされている必要があります。
2. セキュリティーを最大限に確保するために、受信側のデバイスは、初期化に使用されたCC2000 からブロードキャストされたUDP 以外を受け付けなくなります。

次のドロップダウンメニューから、「All Devices」（全てのデバイス）または「Specific IP Address」（特定の IP アドレス）を選択してください。後者を選択した場合は、次の欄に IP アドレスを入力してください。

「Broadcast Now」（今すぐブロードキャスト）をクリックすると、ブロードキャストを開始します。

デバイスの同期

「Device Sync」（デバイスの同期）タブは下図のような画面です。



デバイスの名前を変更するには、このタブを使ってデバイスと CC2000 の間において名前を手動で同期してください。

使用環境に応じて、「Sync names from CC2000 to devices」（CC2000 の名前をデバイスに同期する）、または「Sync names from devices to CC2000」（デバイスの名前を CC2000 に同期する）を選択してください。

同期の対象となるデバイスのチェックボックスにチェックを入れて選択してください（複数選択可）。

そうしたら、「Sync Now」（今すぐ同期）をクリックしてください。

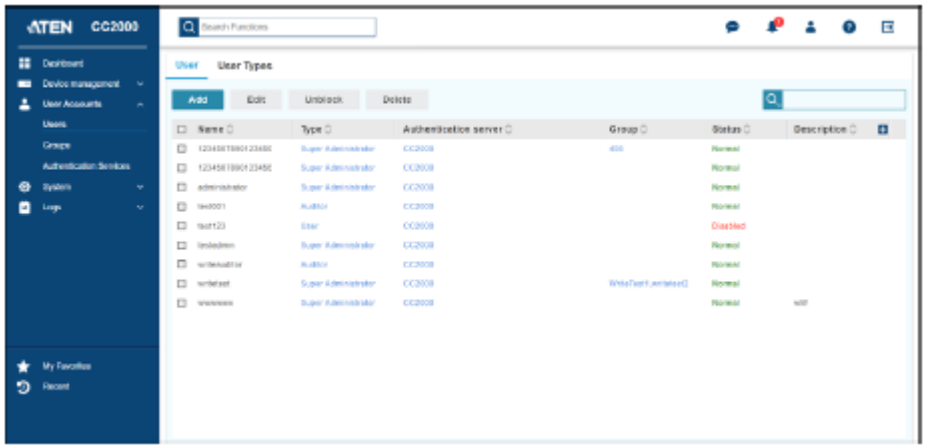
第 6 章
ユーザーアカウント

概要

「User Management」(ユーザー管理)画面では、以下の機能を提供しています。

- ユーザーアカウントの追加・変更・削除
- ユーザーグループの作成、およびユーザーグループへのユーザー登録
- ユーザーやグループに対する、システムデフォルトまたはカスタマイズされたユーザータイプに基づいたデバイスアクセス権限の設定
- ユーザー認証を行う方法の選択(CC2000 経由または外部認証サーバー経由のいずれかを選択)

「User Accounts」(ユーザーアカウント)を選択すると、下図のような画面が表示されます。

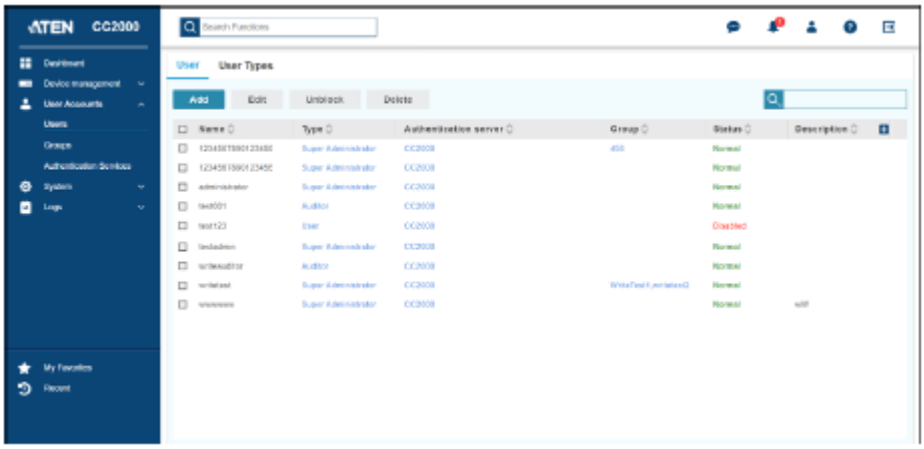


サブメニューには、「Users」(ユーザー)、「Groups」(グループ)、「Authentication Services」(認証サービス)が含まれます。

注意:
1. 「User Accounts」(ユーザーアカウント)画面は、スーパーアドミニストレーター、システム管理者、ユーザー管理者、監査ユーザー向けの機能です。監査ユーザーは、このメニューのアイテムを参照することしかできません。
2. 作成可能なユーザー数は 4096 で、グループ数は 512 です。

ユーザー

「Users」(ユーザー)サブメニューは、下図のように表示されます。

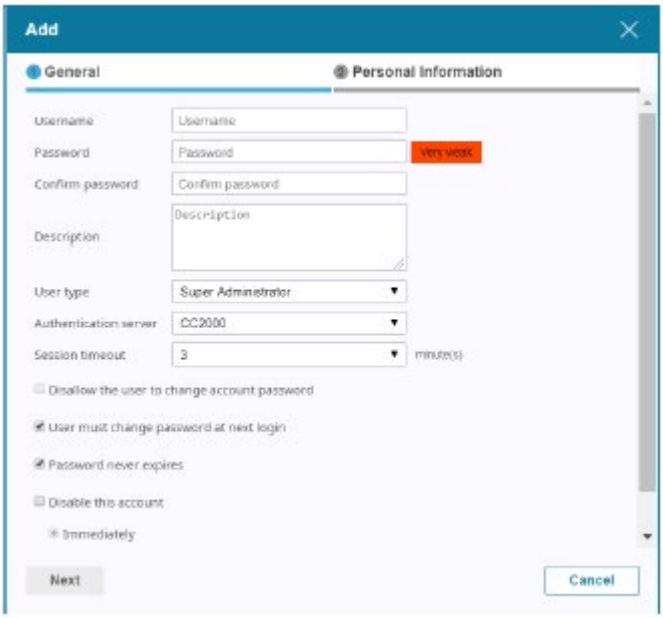


ユーザー

ユーザーの追加

ユーザーを追加する場合は、以下の手順で操作してください。

1. 下図の画面から「Add」(追加)をクリックしてください。



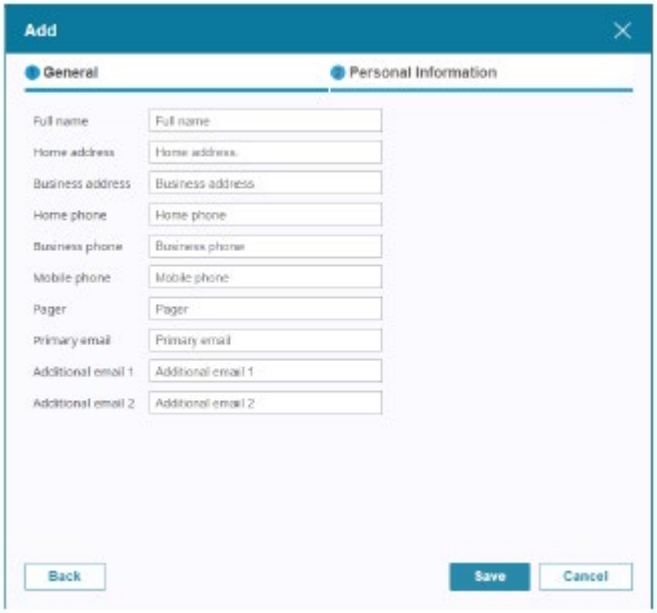
2. 画面内の項目に必要事項を入力してください。各項目の詳細は下表の通りです。

項目	説明
Username (ユーザーネーム)	**Internal (CC2000) Accounts(内部 (CC2000) アカウント)**: 半角英数字を使って最大 32 文字で入力してください。入力が必要な最小文字数は、CC2000 のアカウントポリシーの設定に基づいて定められています(p.323「CC2000 認証」参照)。 **External Authentication(外部認証)**:ログインネームは外部認証サーバー上に存在するものでなければなりません。 **注意:**これらの外部サーバーは認証サービスを提供するだけであって、ユーザーの権限設定は行いません。権限設定は CC2000 で行いますので、アクセス権限は CC2000 上で設定する必要があります。
Password / Confirm password (パスワード/確認用パスワード)	いずれの項目も、半角英数字を使って最大 32 文字で入力してください。
Description (説明)	ユーザーに関する追加情報です。最大 256 バイトで入力することが可能です。
User type (ユーザータイプ)	ドロップダウンメニューをクリックして、新規ユーザーに設定したいユーザータイプを選択してください。ユーザータイプに関する詳細は p.204 をご参照ください。
Authentication Server (認証サーバー)	CC2000 を使って認証を行う場合は、変更する必要はありません。外部認証サービスを使って認証を行う場合は、リストから該当するものを選択してください。 **注意:**ここで外部認証サービスを選択する前に、外部認証サーバーをあらかじめ登録しておく必要があります。詳細については、p.215「認証サービスの追加」をご参照ください。

(表は次のページに続きます)

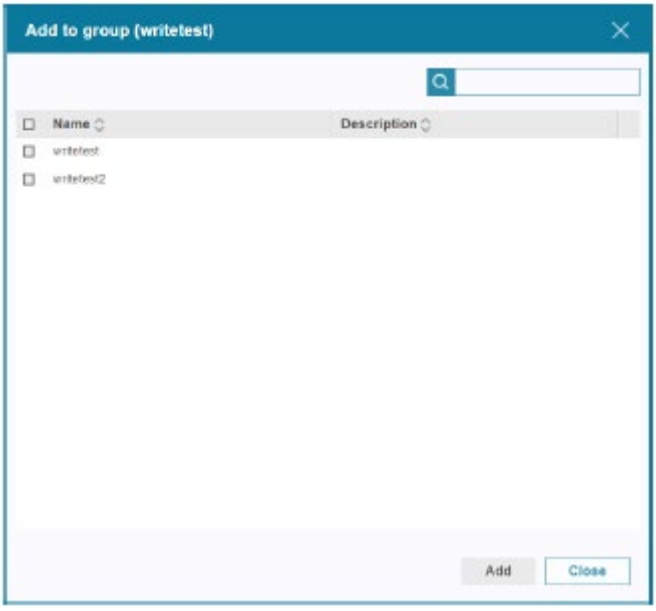
項目	説明
User base RDN （ユーザーのベース RDN）	認証サーバーが LDAP サーバーの場合は、この欄にユーザーのベース RDN を設定してください。
Session Timeout （セッションタイムアウト）	ユーザー操作のアイドル状態が一定の時間経過した場合におけるセッションタイムアウトを設定したい場合は、タイムアウトまでのアイドル時間をドロップダウンメニューから選択してください。デフォルトでは 3 分間に設定されています。 ユーザーの操作が一定の時間アイドル状態のままでもセッションタイムアウトの時間を設けない場合は、ドロップダウンメニューから「Never」（なし）を選択してください。 **注意：**この設定は、ユーザーの次のログインから適用されます。
Other Information （その他の情報）	このアカウントを管理する追加ポリシーがある場合は、該当する項目にチェックを入れてください。

3. 「Next」(次へ)ボタンをクリックして、「Personal Information」(個人情報)画面に遷移してください。



ここで入力される個人情報は、ユーザーの識別に使用する内容だけです。

4. 「Save」(保存)ボタンをクリックして、設定内容を保存してください。そうすると、「Add to Group」(グループへの追加)画面が表示され、ここでユーザーをグループに登録することができます。



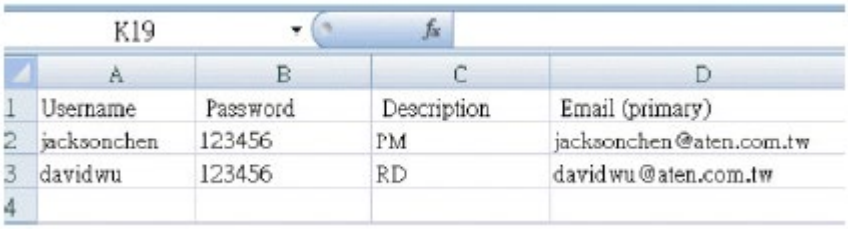
5. ユーザーの登録先となるグループにチェックを入れて選択したら、「Add」(追加)をクリックしてください。
6. 「Close」(閉じる)をクリックして、操作を終了してください。

ユーザーのインポート

追加対象となるユーザーアカウントが多数存在する場合は、ユーザーのインポート機能を使うことで作業を簡素化することができます。このボタンをクリックすると、CSV 形式で保存されたユーザーリストをインポートすることができます。

リストを作成するには、以下の手順で操作してください。

1. 次に定義されているフォーマットに合わせて、各ユーザーアカウントのデータをスプレッドシートに作成してください。



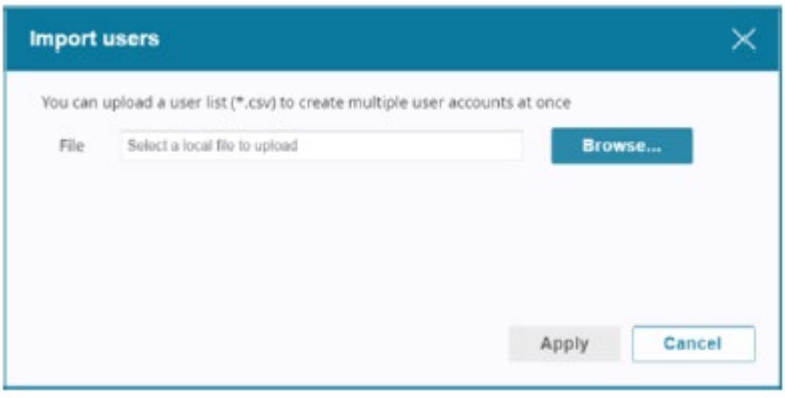
	A	B	C	D
1	Username	Password	Description	Email (primary)
2	jacksonchen	123456	PM	jacksonchen@aten.com.tw
3	davidwu	123456	RD	davidwu@aten.com.tw
4				

注意: 列名にある「Email」と「(primary)」の間には必ず半角スペースを 1 つ入れてください。

2. スプレッドシートを CSV 形式のファイル(*.csv)に保存してください。

リストをインポートするには、以下の手順で操作してください。

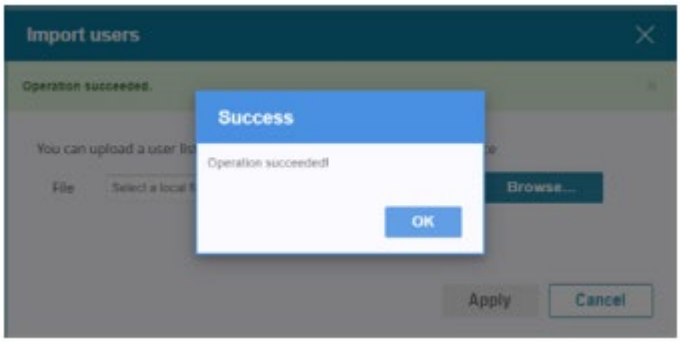
1. 次のダイアログウィンドウで、「**Import Users**」(ユーザーのインポート)をクリックしてください。



2. 「**参照…**」をクリックし、アップロード対象となるファイルを選択してください。
3. 「ファイルの選択」ウィンドウでリストを選択し、このファイルを開いてください(ダブルクリックする

か、選択後に「**開く**」をクリック)。

4. 「Apply」(適用)をクリックしてください。
5. 操作が完了すると、成功したことを表すメッセージが表示されます。



インポートが成功しなかった場合は、CSV ファイルのフォーマットを見直してみてください。

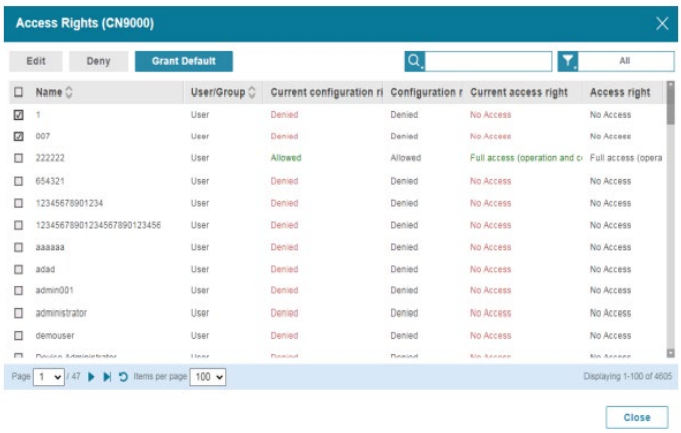
ユーザーの編集

ユーザーのアクセス権限とプロパティーを編集することができます。

■アクセス権限の編集

1. ユーザーを選択し、「Edit」(編集)をクリックしてください。
   もしくは、対象となるユーザーの上にマウスカーソルを動かして、鉛筆のアイコンをクリックしてください。

2. 「Access rights」(アクセス権限)をクリックしてください。そうすると、画面がポップアップ表示されます。下図はその例です。



3. デバイスまたはポートにチェックを入れたら、「Edit」(編集)をクリックしてください。
   もしくは、対象となるデバイスまたはポートの上にマウスカーソルを動かして、鉛筆のアイコンを

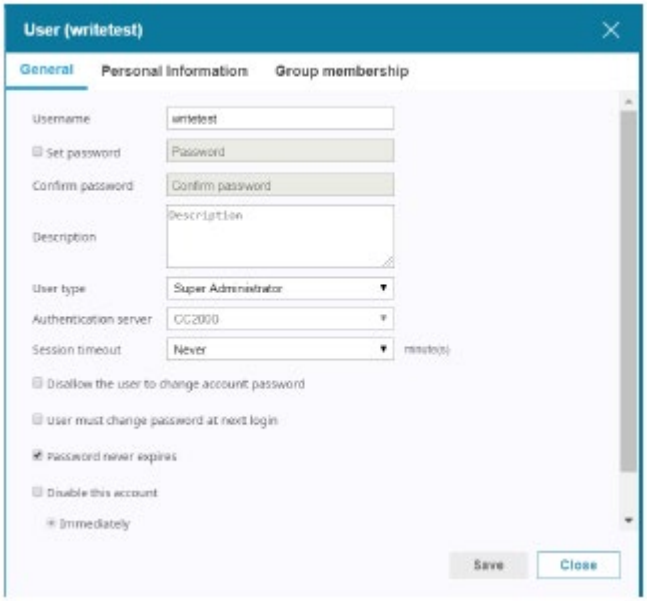
クリックしてください。
そうすると、ウィンドウがポップアップ表示されます。下図はその例です。

4. 権限の編集に関する詳細は p.127「アクセス権限」を参照してください。

■プロパティーの編集

1. ユーザーを選択し、「Edit」(編集)をクリックしてください。
もしくは、対象となるユーザーの上にマウスカーソルを動かして、鉛筆のアイコンをクリックしてください。

2. 「Properties」(プロパティー)をクリックしてください。そうすると、画面がポップアップ表示されます。下図はその例です。



3. このタブでオプションを編集してください。タブは、クリックすると切り替わります。

ここで表示される 3 つのタブに関する詳細は、p.196「ユーザー」を参照してください。

■ユーザーのブロック解除

ログイン再試行の回数が上限を超えると、ユーザーはブロックされます。

ユーザーのブロックを解除するには、対象となるユーザーを選択し（複数選択可）、「**Unblock**」（ブロック解除）をクリックしてください。

そうすると、確認メッセージが表示されます。ブロック解除を続行する場合は「**Yes**」（はい）をクリックしてください。

注意：

1. 必要に応じて、複数のユーザーにチェックを入れ、同時にブロックを解除することができます。また、列の見出しにあるチェックボックスにチェックを入れてブロック解除を行うと、全てのユーザーのブロックを一括解除することもできます。
2. システムアドミニストレーターを含む全ユーザーがブロックされた場合は、システムアドミニストレーターとして CC2000Pro ユーティリティーを使って、このアカウントの情報をリストアした上で、ロックされたユーザーを解除することができます。詳細は p.341「リストア」を参照してください。

■ユーザーの削除

ユーザーを削除するには、対象となるユーザーにチェックを入れて選択してから「**Delete**」（削除）をクリックしてください（複数選択可）。

そうすると、確認メッセージがポップアップ表示されます。削除を続行する場合は「**Yes**」（はい）をクリックしてください。

◆ **Reactivate Disabled Users**（無効ユーザーの再有効化）

無効化されたユーザーを再度有効にする場合は、プロパティー画面の下部に進んでください。下図のような画面が表示されます。

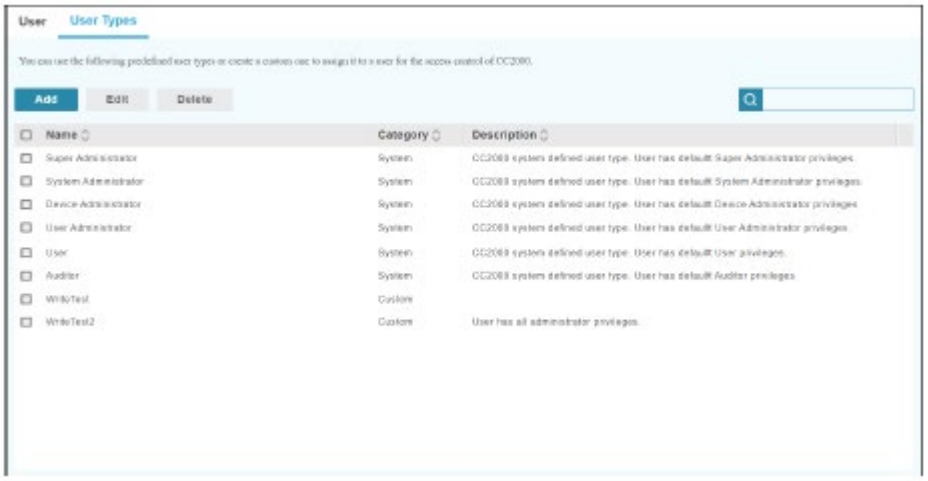
「Disable this account」（このアカウントを無効にする）の項目からチェックを外して、「**Save**」（保存）をクリックしてください。

そうすると、「Operation succeeded」（操作に成功しました）というメッセージが画面上部に表示

されます。

ユーザータイプ

「User Types」（ユーザータイプ）タブをクリックすると、ユーザータイプの一覧が表示されます。下図はその例です。



この画面では、ユーザータイプとして「System」（システム）と「Custom」（カスタム）があり、これは「Category」（カテゴリー）列で見分けることができます。

CC2000 では 6 種類のシステムユーザータイプがサポートされており、CC2000 にあらかじめ組み込まれています。これらのユーザータイプのメンバーに割り当てられたロールは固定で、変更することができません。

一方、「Custom」（カスタム）のユーザータイプは、使用環境の要件に合わせて、各種ロールを自由に組み合わせて割り当てることができます。

システムのユーザータイプ

サポートされる機能および特長は、各ユーザータイプで決まっています。概要は下表の通りです。

割り当てられたロール	Super Admin	System Admin	User Admin	Device Admin	User	Auditor
システム設定	✔	✔				◊
システムタスク	✔	✔				◊
認証サービス	✔	✔	✔			◊
ユーザーおよびグループの管理	✔	✔	✔			◊
ユーザーおよびグループのデバイスアクセス権限	✔	✔	✔			◊
デバイス管理	✔	✔		✔		◊
監視設定	✔	✔		✔		◊
ログ設定	✔	✔	✔	✔		◊
ログおよびレポートの参照	✔	✔	✔	✔		◊
ユーザー自身のパスワードの変更	✔	✔	✔	✔	✔	✔

注意:

1. スーパーアドミニストレーターとシステムアドミニストレーターの違いは以下の通りです。
   - ◆ スーパーアドミニストレーターには全ロールの権限が与えられ、全てのデバイス、ポート、およびアウトレットにアクセスすることができます。これらのロールは固定であり、変更することはできません。
2. 以下は、「Auditor」(監査ユーザー)タイプに関する補足事項です。
   - ◆ このタイプのユーザーは、全てのタブおよび画面にアクセスすることができますが、参照権限しか与えられていません。
   - ◆ 「Logs」(ログ)画面において、このタイプのユーザーはログの参照の他に、ログのエクスポートや印刷が可能ですが、設定の変更はできません。
   - ◆ 「Preferences」(設定)画面において、このタイプのユーザーはウェブオプションおよびパスワードの各設定を変更することができます。

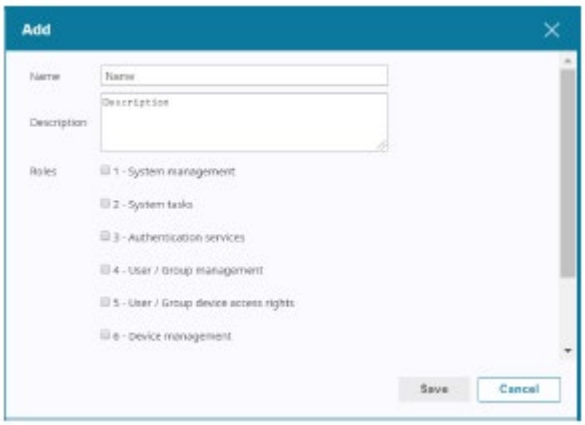
カスタムのユーザータイプ

CC2000 では、使用環境の要件に合わせて、各種ロールを自由に組み合わせて定義できる、「Custom」(カスタム)のユーザータイプを作成することができます。

■ユーザータイプの追加

カスタムのユーザータイプを作成するには、次の手順に従って操作を行ってください。

1. 「Add」(追加)をクリックしてください。そうすると、ウィンドウがポップアップ表示されます。



2. 新規ユーザータイプに与えたい「Name」(名前)と「Description」(説明)を各欄に入力してください。また、このユーザータイプのロールにチェックを入れて選択してください。

注意:	1. 「Name」(名前)欄には、半角英数字を使って 2～32 文字で入力してください。ただし、以下の文字を使用することはできません。 “ ‘ ¥ 2. 「Description」(説明)欄は 256 バイト以内で入力してください。

3. 設定が完了したら、「Save」(保存)をクリックしてください。

■ユーザータイプの編集

1. ユーザータイプを選択し、「Edit」(編集)をクリックしてください。
   もしくは、対象となるユーザータイプの上にマウスカーソルを動かして、鉛筆のアイコンをクリックしてください。

2. 新規ユーザータイプの名前、説明、ロールをそれぞれ設定してください。

3. 設定が完了したら、「Save」(保存)をクリックしてください。

ユーザータイプの削除

対象となるユーザータイプにチェックを入れて選択してから「Delete」（削除）をクリックしてください（複数選択可）。

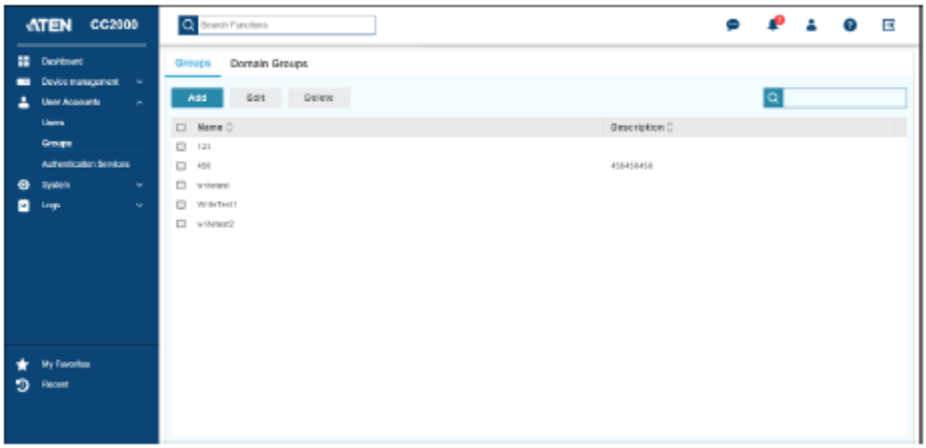
そうすると、確認メッセージがポップアップ表示されます。削除を続行する場合は「Yes」（はい）をクリックしてください。

注意：	カテゴリーが「System」（システム）のユーザータイプは削除することができません。

グループ

「Groups」(グループ)を使うと、管理者はユーザーやデバイスを簡単かつ効率的に管理することができます。グループに設定されたデバイスのアクセス権限はグループ内の全メンバーに適用されますので、管理者はグループにアクセス権限を設定しさえすれば、ユーザー一人一人に対してアクセス権限の設定をする必要がなくなります。この機能を使うと複数のグループを設定し、特定デバイスへのユーザーアクセスを許可したり、逆に制限をかけたりすることが可能です。

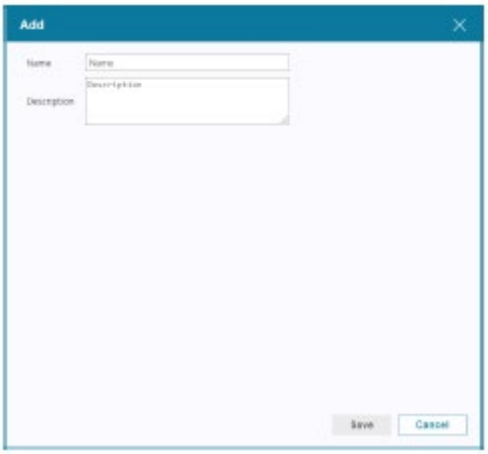
「Groups」(グループ)サブメニューは、下図のような画面が表示されます。



グループタブ

グループの追加

1. 「Add」(追加)をクリックしてください。そうすると、部署(または場所、タイプのいずれか)の追加画面がポップアップ表示されます。

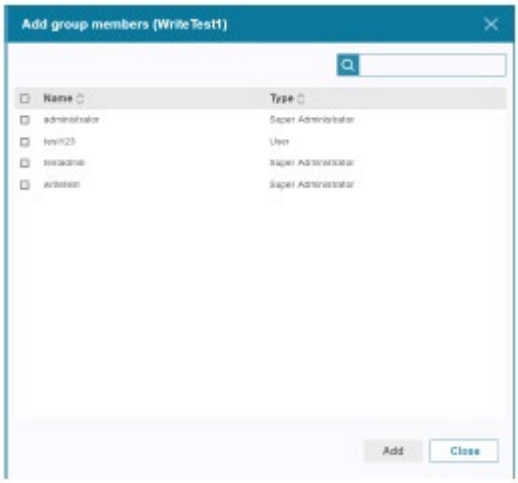


2. 「Name」(名前)と「Description」(説明)の各欄に入力してください。

注意: 1. 「Name」(名前)欄には、半角英数字を使って 2～32 文字で入力してください。ただし、以下の文字を使用することはできません。
/ ¥ [ ] : ; | = , + * ? < > @ ″ ’
2. 「Description」(説明)欄は 256 バイト以内で入力してください。

3. 「**Save**」(保存)をクリックしてください。

4. そうすると、メンバーをこのグループに追加するかどうかの選択を、システムから促されます。下図はその例です。



5. グループに追加したいユーザーにチェックを入れて選択したら、「**Add**」(追加)をクリックしてください。

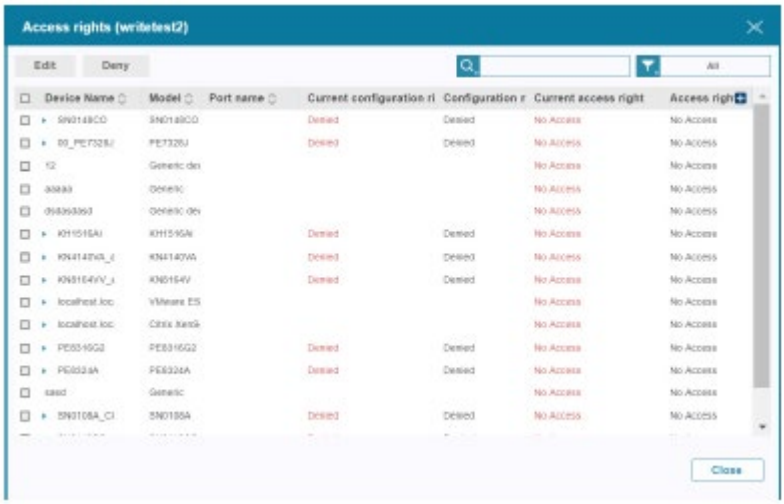
6. ユーザーの追加が完了したら、「**Close**」(閉じる)をクリックしてください。

グループの編集

■グループのアクセス権限の編集

グループのアクセス権限を編集するには、次の手順に従って操作を行ってください。

1. グループにチェックを入れて選択し、「**Edit**」(編集)をクリックしてください。
もしくは、対象となるグループの上にマウスカーソルを動かして、鉛筆のアイコンをクリックしてください。
2. 「**Access rights**」(アクセス権限)をクリックしてください。そうすると、下図のような画面が表示されます。



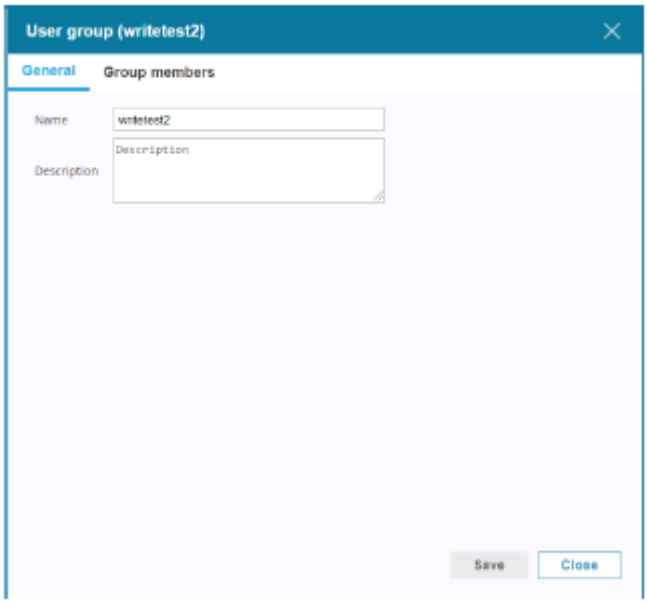
3. デバイスまたはポートにチェックを入れて選択したら、「Edit」(編集)をクリックしてください。
もしくは、対象となるデバイスまたはポートの上にマウスカーソルを動かして、鉛筆のアイコンをクリックしてください。
そうすると、画面がポップアップ表示されます。下図はその例です。

4. 権限の編集に関する詳細は p.127「アクセス権限」を参照してください。

■プロパティーの編集

1. グループを選択し、「Edit」(編集)をクリックしてください。
もしくは、対象となるグループの上にマウスカーソルを動かして、鉛筆のアイコンをクリックしてください。

2. 「Properties」(プロパティー)をクリックしてください。そうすると、画面がポップアップ表示されます。下図はその例です。



3. このタブでオプションを編集してください。タブは、クリックすると切り替わります。
ここで表示される 2 つのタブに関する詳細は、p.208「グループの追加」を参照してください。

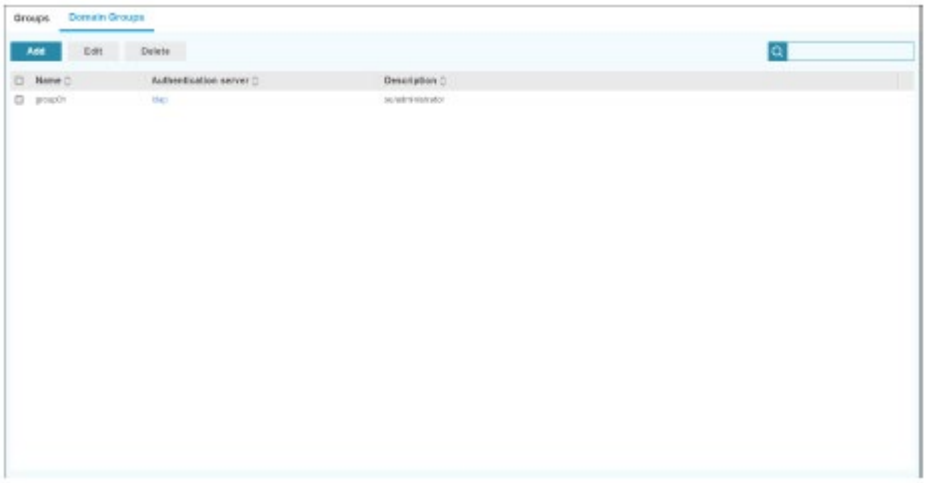
グループの削除

グループを削除するには、対象となるグループにチェックを入れて選択してから「Delete」(削除)をクリックしてください(複数選択可)。

そうすると、確認メッセージがポップアップ表示されます。削除を続行する場合は「Yes」(はい)をクリックしてください。

ドメイングループタブ

「Domain Groups」(ドメイングループ)タブは、下図のような画面です。



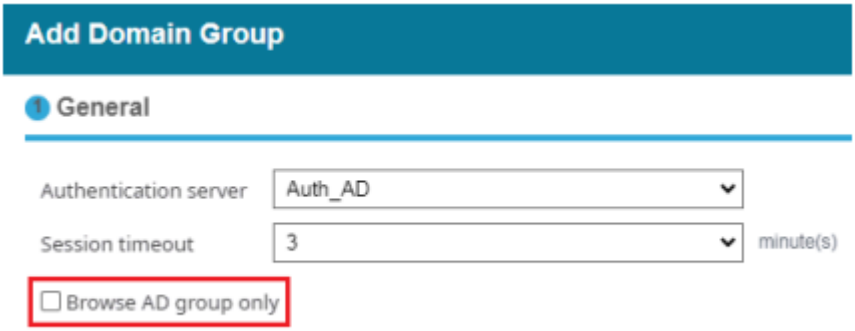
この画面で設定を行う前に、外部認証サービスを用意する必要があります。認証サービスの追加に関する詳細は、p.215「認証サービスの追加」を参照してください。

ドメイングループの追加

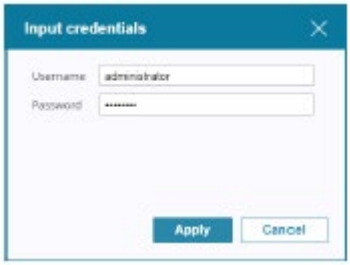
1. 「Add」(追加)をクリックしてください。そうすると、「Add domain group」(ドメイングループの追加)画面がポップアップ表示されます。

2. 「Authentication server」(認証サーバー)と「Session timeout」(セッションタイムアウト)の各項目に設定する内容を、それぞれドロップダウンメニューをクリックして選択してください。

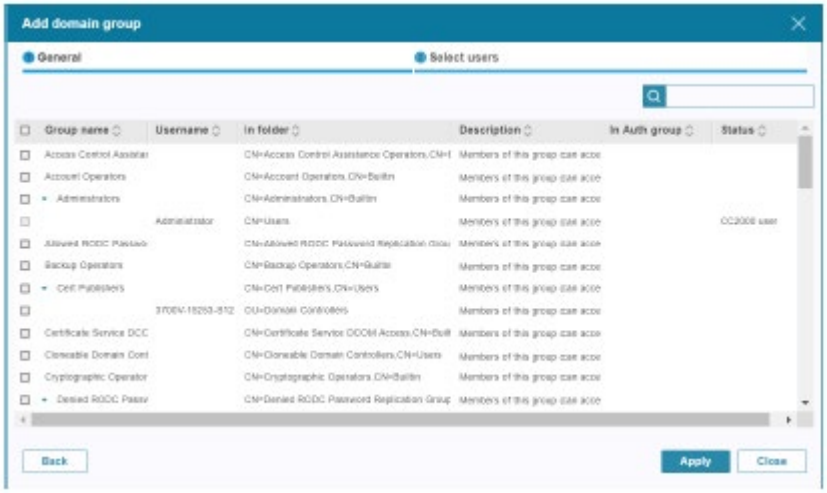
注意： 認証サーバーとしてADサーバーが選択されている場合は、オプションで「Browse AD group only」(ADグループのみを参照する)の項目にチェックを入れて、ADグループのみを参照し、個々のADユーザーを除外することができます。



3. 「Next」(次へ)をクリックしてください。必要に応じて、サーバー側から認証情報の入力が求められます。下図はその例です。



4. 認証情報を入力したら、「Apply」(適用)をクリックしてください。そうすると、「Select users」(ユーザーの選択)画面に遷移します。



5. 対象となるグループにチェックを入れて選択したら(複数選択可)、「Apply」(適用)をクリックしてください。

認証サービス

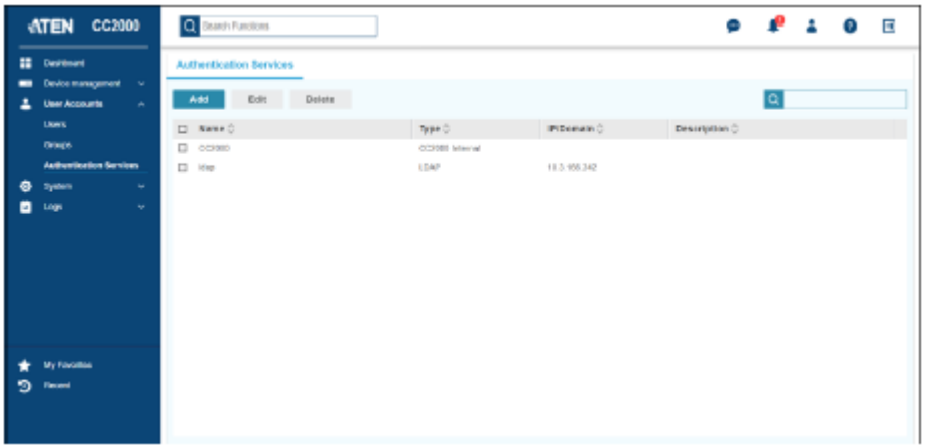
CC2000 単体でもユーザーネームとパスワードによる認証サービスを提供していますが、以下のサードパーティー外部認証サーバーにも対応しています。
Active Directory、Kerberos、LDAP、RADIUS、TACACS+、Windows NT Domain、MOTP*、二要素認証

注意:
1. 「authentication」(認証)は、ログインユーザーが正しいかどうかを判断することを指すのに対し、「authorization」(権限設定)は、デバイスの各機能の使用権限を割り当てることを指しています。
2. これらの外部サーバーからは認証サービスの機能のみを提供し、権限設定のサービスは提供しません。権限設定は CC2000 側で行います。
3. CC2000 は、モバイルワンタイムパスワード(MOTP)サーバーに対応しています。これは、セキュリティー向上のためにサードパーティーの認証サーバーとして使用することができるものです。詳細については、本マニュアルにおけるp.381「MOTP 設定」、または以下のウェブサイト(英語)をご確認ください。
http://www.aten.com/CC2000-OTP

外部認証サーバーを CC2000 に追加する(p.215 参照)ことによって、ユーザーアカウントを追加した際に、認証サーバーの一覧から外部認証サーバーを選択できるようになります。

注意: LDAP や Active Directory の場合は、ログインしようとしているユーザーが CC2000 上にアカウントを持たない認証方法もあります。この場合、CC2000 では、外部サーバーをチェックし、ログインしようとしているユーザーのユーザーネームとパスワードを持ったアカウントがあるかどうかを確認します。そのアカウントが存在する場合、CC2000 はそのユーザーが CC2000 のドメイングループに対応したグループに所属しているかどうかの確認を行います。グループに所属している場合、CC2000 はそのユーザーのログインを許可し、そのユーザーが所属しているグループのアクセス権限を割り当てます。詳細についてはp.212「ドメイングループタブ」をご参照ください。

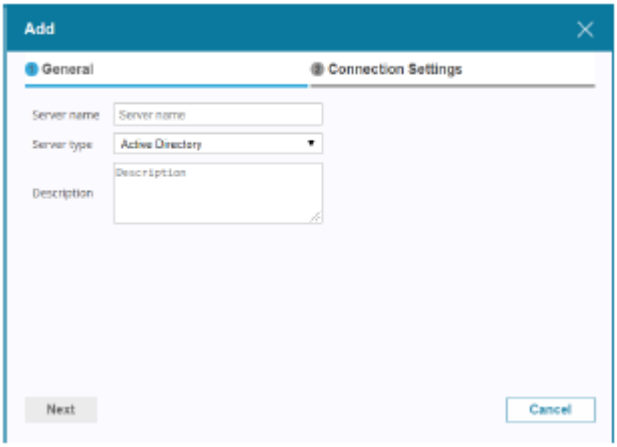
「Authentication Services」(認証サービス)サブメニューは下図のような画面です。



認証サービスの追加

認証サービスを追加するには、次の手順に従って操作を行ってください。

1. 「**Add**」(追加)をクリックしてください。そうすると、下図のような画面がポップアップ表示されます。

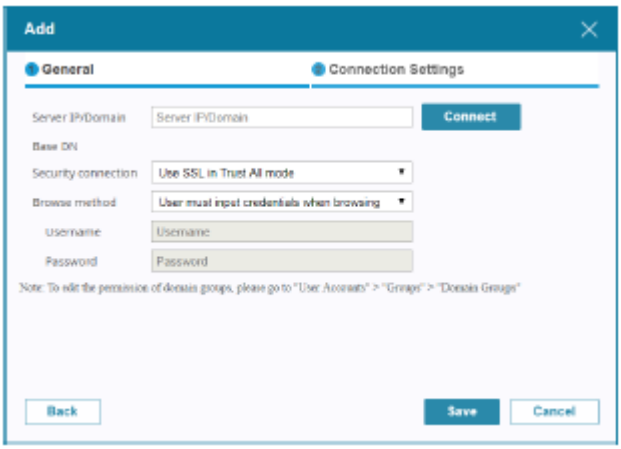


2. 「Server name」(サーバー名)と「Description」(説明)の各欄に入力してください。また、「Server type」(サーバーの種類)の項目はドロップダウンメニューから選択してください。

注意:
1. 「Name」(名前)欄には、半角英数字を使って 2～32 文字で入力してください。ただし、以下の文字を使用することはできません。 “ ‘ ¥
2. 「Description」(説明)欄は 256 バイト以内で入力してください。

3. 「**Next**」(次へ)をクリックしてください。そうすると、「Connection Settings」(接続設定)画面に遷

移します。この画面は、サーバータイプによって内容が異なります。



4. 画面内の項目に値を入力してください。各項目の詳細は p.217「サーバー情報」を参照してください。

5. サーバーIP またはドメインを入力したら、「Connect」(接続)をクリックして、接続のテストを行ってください。

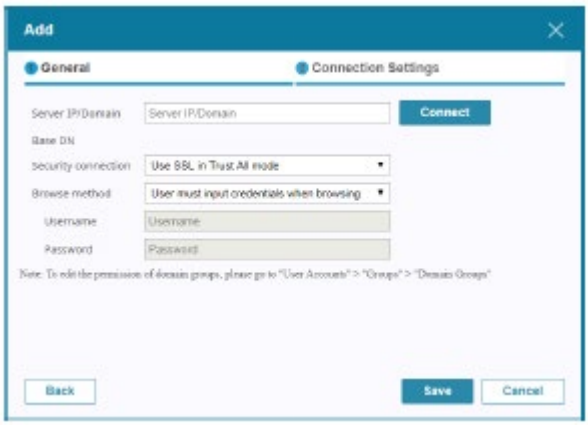
6. 「Security connection」(セキュリティー接続)と「Browse method」(閲覧方法)の各項目をドロップダウンメニューから選択したら、「Save」(保存)をクリックしてください。

サーバー情報

各サービスの設定に必要となる項目は下表をご参照ください。

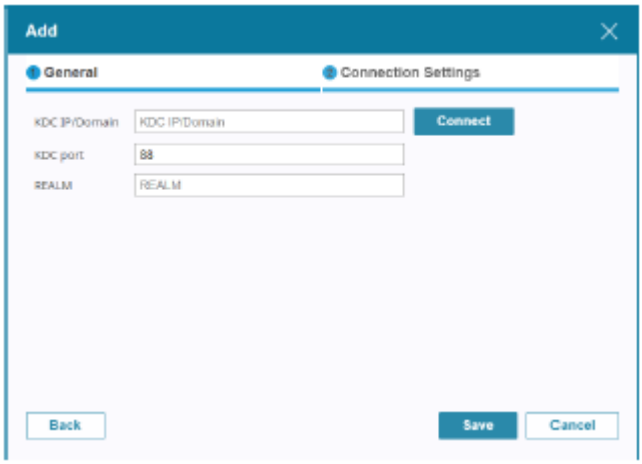
1. Active Directory

項目	内容
Server IP/Domain （サーバーIP/ドメイン）	詳細は Active Directory の管理者にご確認ください。 設定例は p.367「Active Directory 設定例」をご参照ください。
Security connection （セキュリティー設定）	「Trust All mode」（全信頼モード）で SSL を使用するかどうかをラジオボタンで選択してください。
Browse method （閲覧方法）	◆ ユーザーがそのサーバーで発行された証明書を使って LDAP や LDAPS を閲覧できるようにする場合は、「Browse with user credentials」（ユーザーの資格で閲覧する）を選択してください。この項目が選択されていると、ユーザーは閲覧時に毎回証明書を入力する必要がなくなります。 ◆ ユーザーが Active Directory で閲覧した際に毎回証明書を入力するようにする場合は、「User must input credentials when browsing」（ユーザーは閲覧時に認証情報を入力する）を選択してください。



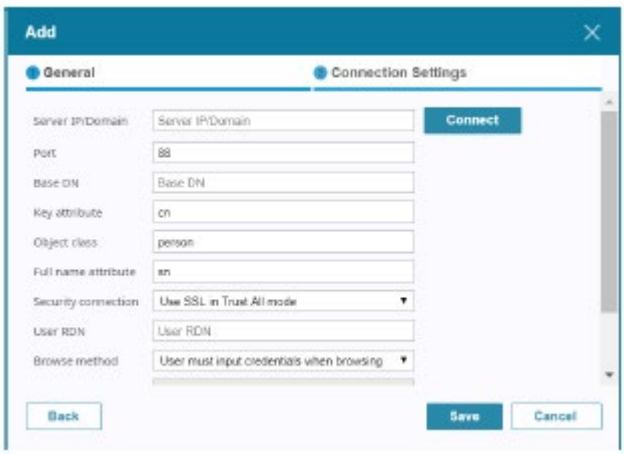
2. Kerberos

項目	内容
KDC IP/Domain （KDC IP/ドメイン）	詳細は Kerberos サーバーの管理者にご確認ください。
KDC port （KDC ポート）	詳細は Kerberos サーバーの管理者にご確認ください。
REALM （レルム）	これは、Kerberos 認証サーバーが、ユーザーやホストやサービスを認証する権限を持っているドメインです。 項目に関する詳細は Kerberos サーバーの管理者にご確認ください。



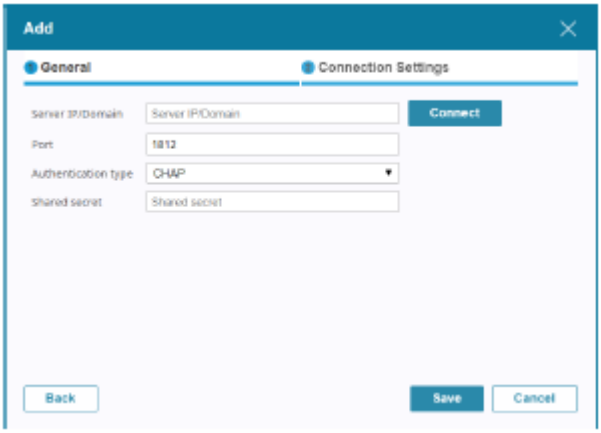
3. LDAP

項目	内容
Connection Settings （接続設定）	これらの項目に関する詳細は LDAP サーバーの管理者にご確認ください。ポートのデフォルトは636番ポートですが、変更されている可能性もありますので、詳しくはLDAP/LDAPS サーバーの管理者にお尋ねください。 設定例は p.364「LDAP/LDAPS - OpenLDAP 設定例」をご参照ください。
Security connection （セキュリティー接続）	全てを信頼するモードで SSL を使用するかどうかをラジオボタンで選択してください。
User RDN （ユーザーRDN）	詳細は LDAP サーバーの管理者にご確認ください。 設定例は p.364「LDAP/LDAPS - OpenLDAP 設定例」をご参照ください。
Browse method （閲覧方法）	◆ ユーザーがそのサーバーで発行された証明書を使って LDAP/LDAPS を閲覧できるようにする場合は、「Browse with user credentials」（ユーザーの認証情報で閲覧する）を選択してください。この項目が選択されていると、ユーザーは閲覧時に毎回証明書を入力する必要がなくなります。 ◆ ユーザーが LDAP/LDAPS で閲覧した際に毎回証明書を入力するようにする場合は、「User must input credentials when browsing」（ユーザーは閲覧時に認証情報を入力する）を選択してください。



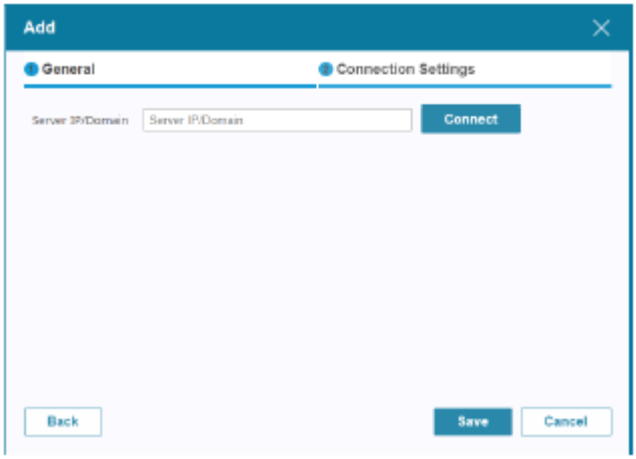
4. RADIUS および TACACS+

項目	内容
Connection Settings （接続設定）	これらの項目に関する詳細は管理者にご確認ください。デフォルト値は RADIUS では 1812 に、TACACS+では 49 にそれぞれ設定されていますが、変更されている可能性もありますので、詳しくは管理者にお尋ねください。 設定例は p.368「RADIUS 設定例」、p.370「TACACS+設定例」をご参照ください。
Authentication Settings （認証設定）	これらの項目に関する詳細は管理者にご確認ください。設定例は p.368「RADIUS 設定例」、p.370「TACACS+設定例」をご参照ください。 1. ドロップダウンメニューをクリックして、お使いの RADIUS サーバーで設定されている「Authentication type」（認証タイプ）を選択してください。 2. RADIUS サーバーとの認証に使用する文字列を「Shared Secret」（共有シークレット）欄に入力してください。 3. 共有シークレットの文字列を「Confirm Shared Secret」（確認用共有シークレット）欄にもう一度入力してください。

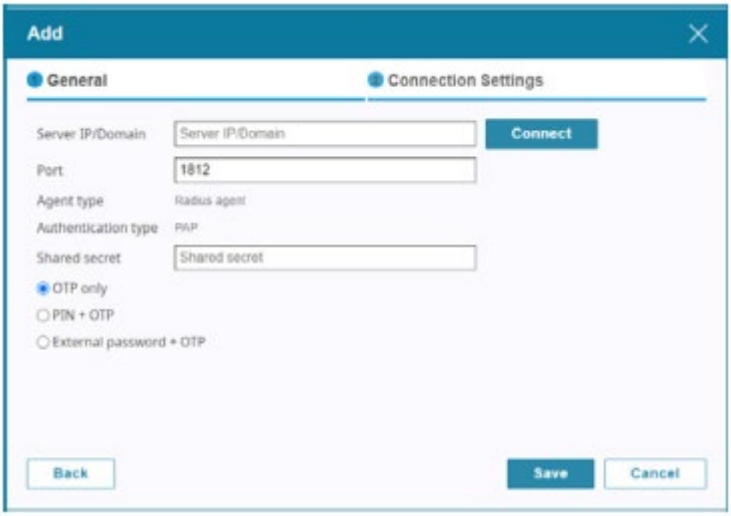


5. Windows NT Domain

「Domain Name」（ドメイン名）に関する詳細は管理者にご確認ください。また、設定例は p.372「NT Domain 設定例」をご参照ください。



6. MOTP(モバイルワンタイムパスワード)*



項目	内容
Server IP/Domain (サーバーIP/ドメイン)	IP やドメインに関する情報をサーバー管理者にご確認の上、入力を行ってください。「Connect」(接続)をクリックすると、接続のテストを行うことができます。
Port (ポート)	ポートに関する情報をサーバー管理者にご確認の上、入力を行ってください。デフォルトの MOTP ポートは 1812 です。
Agent type (エージェントタイプ)	RADIUS が自動的に選択されています。
Authentication Type (認証タイプ)	PAP が自動的に選択されています。

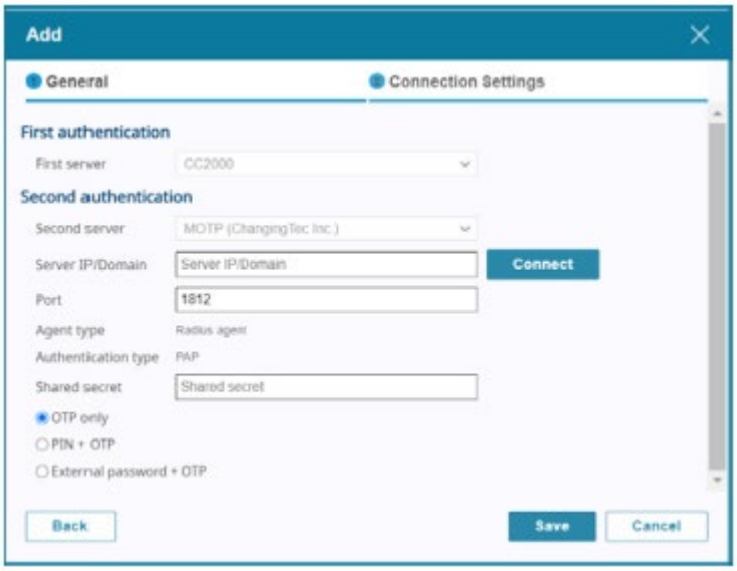
(表は次のページに続きます)

項目	内容
Shared secret （共有シークレット）	MOTP サーバーの認証で使用する文字列を入力してください。ご不明な場合は、サーバー管理者にご確認ください。
Two Factor （二要素）	この項目では、CC2000 へのログインに使用する MOTP 認証の方法を選択します。 1. 「OTP only」（OTP のみ）を選択している場合、CC2000 はユーザーに対してユーザーネームの入力を促します。このとき、システムは（デバイストークンの）OTP を入力する画面を表示します。このとき、パスワード欄の内容は無視されます。 2. 「PIN＋OTP」を選択している場合、CC2000 はユーザーに対してログインユーザーのユーザーネームの入力を促します。このとき、システムは（デバイストークンの）OTP および（MOTP サーバーで設定された）PIN を入力する画面を表示します。このとき、パスワード欄の内容は無視されます。 3. 「External password + OTP」（外部パスワード＋OTP）を選択している場合、CC2000 はユーザーに対してログインユーザーのユーザーネームの入力を促します。このとき、システムは（デバイストークンの）OTP、および（MOTP サーバーで設定された）サードパーティー認証サーバーの外部パスワードを入力する画面を表示します。このとき、パスワード欄の内容は無視されます。

注意：

- ◆ MOTP サーバーは、ワンタイムパスワード（OTP）トークンの認証だけに使用されます。OTP 機能を採用したい場合は、あらかじめ MOTP サーバーをセットアップする必要があります。
- ◆ MOTP サーバーを購入される場合は、CHANGING Information Technology Inc までお問い合わせください。
  （https://www.changingtec.com/EN/）

7. 二要素認証



二要素認証では、CC2000 サーバーにおけるユーザーのユーザーネームとパスワードを入力した後で、MOTP 認証を使ってログインする必要があります。

項目	内容
First authentication （最初の認証）	最初の認証方法は、CC2000 による認証となります。
Second authentication （2 つ目の認証）	2 つ目の認証方法は、MOTP による認証となります。
Server IP/Domain （サーバーIP/ドメイン）	IP やドメインに関する情報をサーバー管理者にご確認の上、入力を行ってください。「Connect」（接続）をクリックすると、接続のテストを行うことができます。
Port （ポート）	ポートに関する情報をサーバー管理者にご確認の上、入力を行ってください。デフォルトの MOTP ポートは 1812 です。
Agent type （エージェントタイプ）	RADIUS が自動的に選択されています。
Authentication Type （認証タイプ）	PAP が自動的に選択されています。
Shared secret （共有シークレット）	MOTP サーバーの認証で使用する文字列を入力してください。ご不明な場合は、サーバー管理者にご確認ください。

（表は次のページに続きます）

項目	内容
Two Factor （二要素）	この項目では、CC2000 へのログインに使用する MOTP 認証の方法を選択します。 1. 「OTP only」（OTP のみ）を選択している場合、CC2000 はユーザーに対してログインユーザーのユーザーネームの入力を促します。このとき、システムは（デバイストークンの）OTP を入力する画面を表示します。このとき、パスワード欄の内容は無視されます。 2. 「PIN＋OTP」を選択している場合、CC2000 はユーザーに対してログインユーザーのユーザーネームの入力を促します。このとき、システムは（デバイストークンの）OTP および（MOTP サーバーで設定された）PIN を入力する画面を表示します。このとき、パスワード欄の内容は無視されます。 3. 「External password + OTP」（外部パスワード＋OTP）を選択している場合、CC2000 はユーザーに対してログインユーザーのユーザーネームの入力を促します。このとき、システムは（デバイストークンの）OTP、および（MOTP サーバーで設定された）サードパーティー認証サーバーの外部パスワードを入力する画面を表示します。このとき、パスワード欄の内容は無視されます。

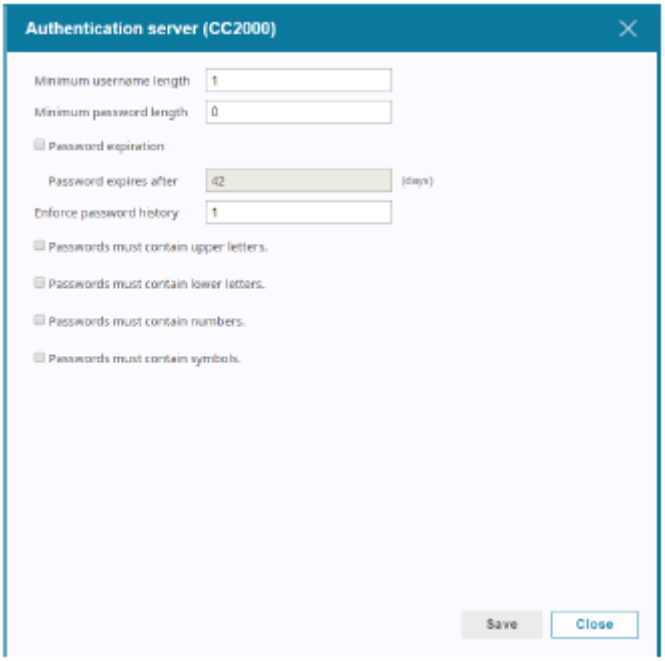
注意：

1. MOTP サーバーは、ワンタイムパスワード（OTP）トークンの認証だけに使用されます。OTP 機能を採用したい場合は、あらかじめ MOTP サーバーをセットアップする必要があります。
2. MOTP サーバーを購入される場合は、CHANGING Information Technology Inc までお問い合わせください。（https://www.changingtec.com/EN/）

CC2000 の認証

CC2000 の内部認証サービスに関して、パスワードポリシー機能にいくつかの設定を行うことができます。ここで設定を行うと、全てのユーザーアカウントはこのポリシーに従わなければなりません。CC2000 のパスワードポリシーを設定する場合は、以下の手順で操作してください。

1. サーバーを選択し、「Edit」(編集)をクリックしてください。
   もしくは、対象となるサーバーの上にマウスカーソルを動かして、鉛筆のアイコンをクリックしてください。



2. 下表を参照しながらパスワードポリシーを設定してください。

項目	説明
Minimum username length （最小ユーザーネーム文字数）	ユーザーネームは半角英数字を使って 1～32 文字で入力することができます。デフォルトでは 6 文字に設定されています。
Minimum password length （最小パスワード文字数）	ユーザーネームは半角英数字を使って 0～32 文字で入力することができます。デフォルトでは 6 文字に設定されています。0 を設定すると、パスワードの入力は不要になりますが、お使いのシステムのセキュリティーを低下させないために、0 以外の値の設定を推奨します。
Password expiration （パスワード期限切れ）	セキュリティーのため、定期的にパスワードの更新をユーザーに要求することができます。ユーザーに定期的なパスワードの変更を求める場合は、この項目にチェックを入れて、パスワードの有効日数を設定してください。パスワードの期限が切れると、新しいパスワードに変更しなければなりません。パスワードの有効日数は、アカウントが作成されたとき、またはパスワードが変更されたときからカウントが始まります。
Enforce Password History （パスワード履歴を実行する）	セキュリティー対策として、この機能を有効にして、古いパスワードを再度使用できるようにするまでに、固有のパスワードを設定しなければならない回数をテキストボックスに入力してください。
Passwords must contain upper case letters （パスワードに英字の大文字を含める）	セキュリティーのために、この設定を有効にし、ユーザーのパスワードに半角英字の大文字を含めるようにしてください。
Passwords must contain lower case letters （パスワードに英字の小文字を含める）	セキュリティーのために、この設定を有効にし、ユーザーのパスワードに半角英字の小文字を含めるようにしてください。
Passwords must contain numbers （パスワードに数字を含める）	セキュリティーのために、この設定を有効にし、ユーザーのパスワードに半角数字を含めるようにしてください。

（表は次のページに続きます）

項目	説明
Passwords must contain symbols (パスワードに記号を含める)	セキュリティーのために、この設定を有効にし、ユーザーのパスワードに半角記号を含めるようにしてください。

3. 設定が完了したら、「Save」(保存)ボタンをクリックしてください。

外部認証サーバーの削除

認証サーバーを削除するには、対象となるサーバーにチェックを入れて選択してから「Delete」(削除)をクリックしてください(複数選択可)。

そうすると、確認メッセージがポップアップ表示されます。削除を続行する場合は「Yes」(はい)をクリックしてください。

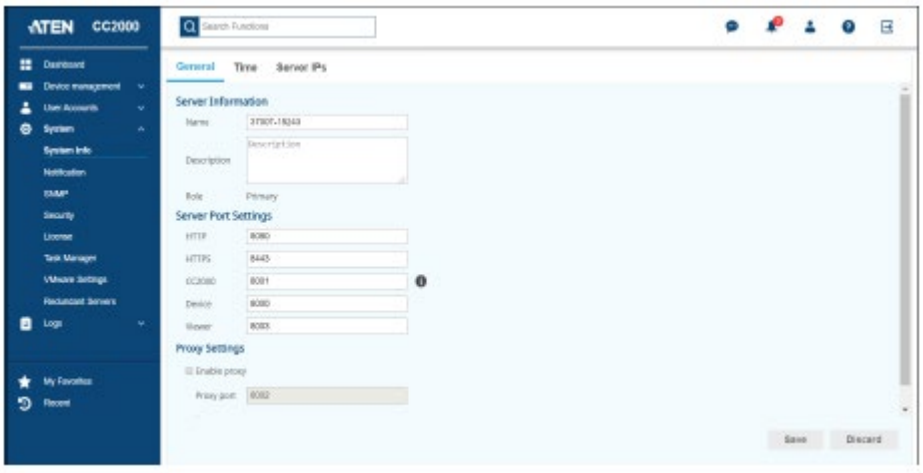
注意:
1. 列の見出しにあるチェックボックスにチェックを入れて削除を行うと、全てのデバイスを一括削除することができます。
2. 認証サーバーを使用しているユーザーアカウントが CC2000 に存在している場合、そのサーバーは削除することができません。

第 7 章
システム

概要

CC2000 のインストールには、CC2000 サーバーに接続する対応デバイスのセットアップが必要です。これらのデバイスはネットワーク経由で CC2000 に接続することができ、なおかつ、CC2000 サーバーと同一ネットワークセグメント上にセットアップされていなければなりません。本製品は個々の CC2000 サーバーのセグメントを IP アドレスで接続することで、世界各国に分散したシステムを統合しますので、インターネットに接続された環境であれば、いつでも、どこからでも、データセンターに設置されたデバイスに安全かつシングルサインオンで一元アクセスすることができます。

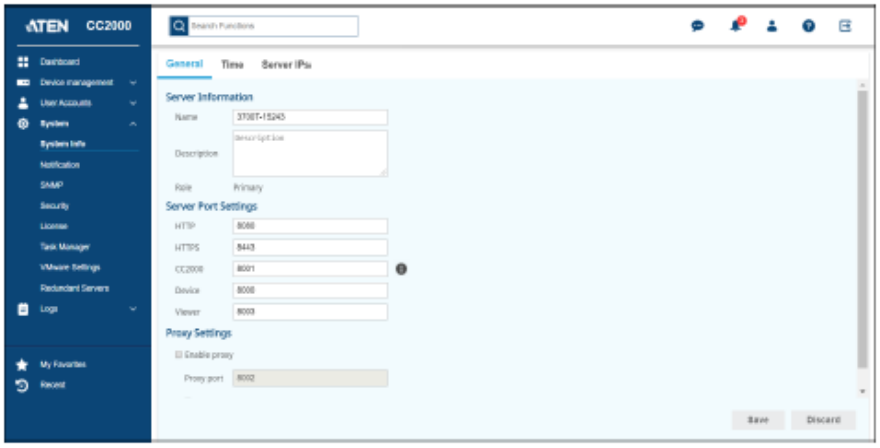
管理や配置上の目的に合わせて、CC2000 のサーバーのうち、1 台をプライマリーサーバーとして、また、残りをセカンダリーサーバーとしてそれぞれ使用します。「System」(システム)をクリックすると、下図のようなデフォルトの「System」(システム)画面が表示されます。



注意: 「System」(システム)画面は、スーパーアドミニストレーター、システム管理者、および監査ユーザー向けの機能です。監査ユーザーは、このメニューのアイテムを参照することしかできません。

システム情報

「System Info」(システム情報)サブメニューは、「General」(全般)、「Time」(時刻)、「Server IPs」(サーバーIP)といった 3 つのタブメニューから構成されています。「System Info」(システム情報)画面のデフォルトは「General」(全般)で、下図のような外観です。



全般

デフォルト画面は「General」(全般)で、上図のような外観です。

注意: システムにおけるその他のサーバーに対する変更は、そのサーバーに直接ログインしないと行うことができません。

この画面では、CC2000 サーバーの設定を定義することができます。

各項目とその説明は、下表の通りです。

項目	説明
Name* (名前)	この項目を編集すると、CC2000 サーバーの名前を変更することができます。
Description (説明)	この項目を編集すると、CC2000 サーバーの説明を変更することができます。この項目は、CC2000 でサポートされる言語を使って、2～32 バイトで設定してください。
Role (ロール)	このサーバーがプライマリーとセカンダリーのどちらであるかを示します。

(表は次のページに続きます)

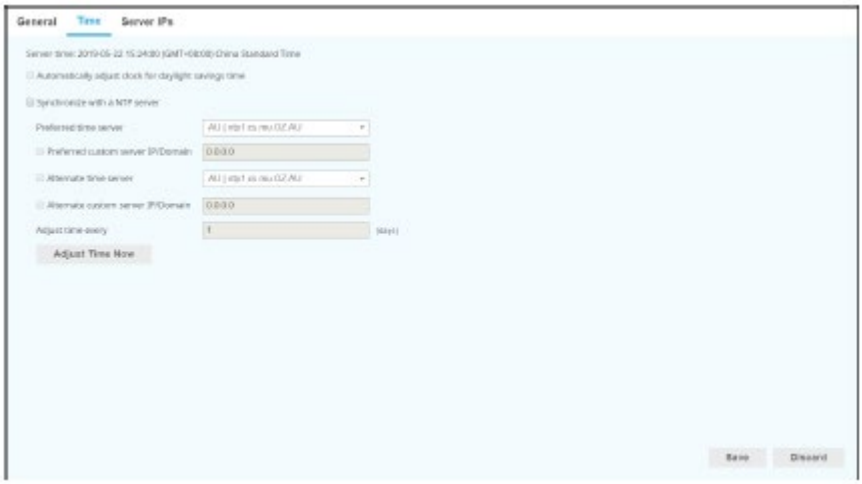
項目	説明
HTTP*	CC2000 がウェブブラウザーで非暗号化通信に使用するポートです。
HTTPS*	CC2000 がウェブブラウザーで暗号化通信に使用するポートです。
CC2000*	CC2000 が、システムにおける他の CC2000 サーバーとの通信に使用するポートです。
Device （デバイス）*	CC2000 がシステムにおいてデバイスとの通信に使用するポートです。
Viewer （ビューワー）	マルチビューワーが有効な場合に、CC2000 がビューワー通信に使用するポートです。詳細については p.161「ビューワーの起動」をご参照ください。
Enable proxy （プロキシを有効にする）	プロキシを使用する場合は、この項目にチェックを入れ、該当欄にプロキシポートを入力してください（p.320「CC2000 プロキシ機能」参照）。
Always use proxy （常にプロキシを使用する）	常にプロキシ機能を使用する場合は、この項目にチェックを入れてください。

＊　詳細については p.24 をご参照ください。

項目の設定が完了したら、「**Save**」（保存）ボタンをクリックしてください。

時刻

「Time」(時刻)画面では、CC2000 がインストールされているサーバーの時刻を、ネットワークタイムサーバーに自動同期します。



注意:	サマータイムが実施されていないタイムゾーンでお使いの場合は、「Automatically adjust clock for daylight savings time checkbox」(時刻をサマータイム時間に自動調整する)のチェックボックスが無効になります。

ネットワークタイムサーバーに自動同期させる場合は、下記の手順に従って操作してください。

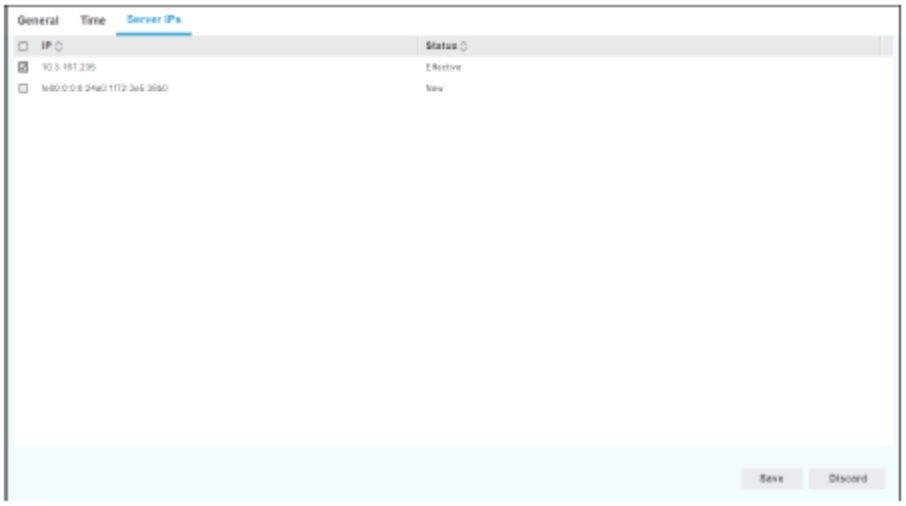
1. 「Synchronize with a NTP server」(NTP サーバーと同期する)のチェックボックスにチェックを入れてください。
2. 「Preferred time server」(優先タイムサーバー)のドロップダウンメニューから、優先タイムサーバーを選択してください。
   - または -
   「Preferred custom server IP/Domain」(優先カスタムサーバーIP/ドメイン)のチェックボックスにチェックを入れて、選択したタイムサーバーの IP アドレスを入力してください。
3. 代替タイムサーバーを設定したい場合は、「Alternate time server」(代替タイムサーバー)と「Alternate custom server IP/Domain」(代替カスタムサーバーIP/ドメイン)の項目にチェックを入れ、手順 2 と同様の方法で、このサーバーのエントリーに対しても設定を行ってください。
4. 「Adjust time every」(次の日数おきに調整する)の欄に、同期を実行する間隔の日数を入力してください。
5. すぐに同期する場合は、「Adjust Time Now」(すぐに時刻同期する)ボタンをクリックしてくださ

い。

6. 全ての設定が終わったら、「Save」(保存)ボタンをクリックしてください。

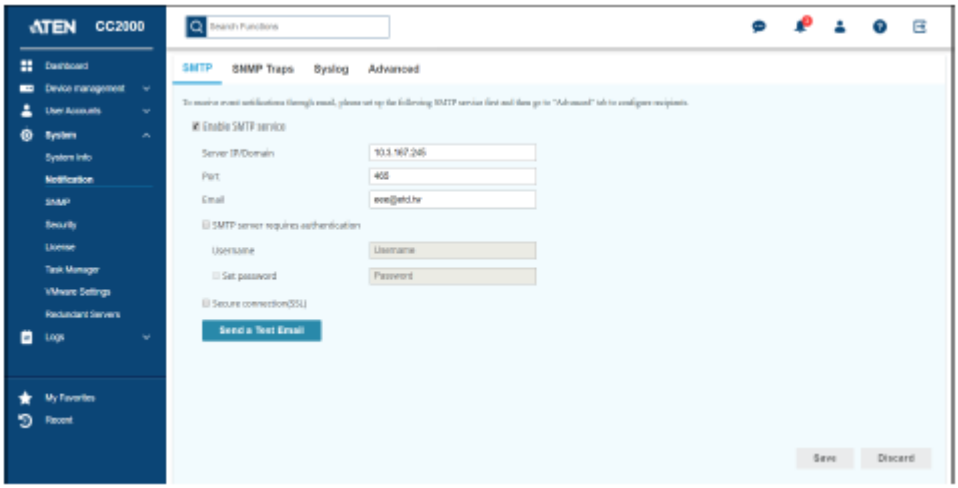
サーバーIP

「Server IP」(サーバーIP)画面には、CC2000 がセットアップされているサーバーで利用可能な IP アドレスが表示されます。サーバーを有効にするには、使用する IP アドレスのチェックボックスにチェックを入れてから(複数選択可)、「Save」(保存)をクリックしてください。



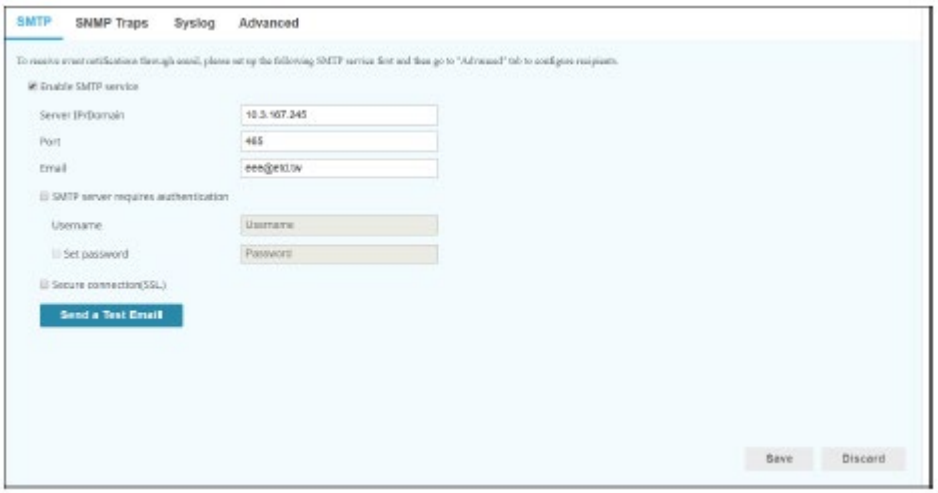
通知

「Notification」(通知)メニューは、「SMTP」、「SNMP Traps」(SNMP トラップ)、「Syslog」、「Advanced」(詳細)といった 4 つのタブメニューから構成されています。「Notification」(通知)画面のデフォルトは「SMTP」で、下図のような外観です。



SMTP

CC2000 では、システムにおけるイベントトラップの通知を、特定のユーザーに対してメールで送信することができます。



注意： 宛先となるユーザーを設定するには、SNTP の設定が完了してから、「Advanced」（詳細）画面に進むようにしてください。詳細は p.238 を参照してください。

SMTP サーバーの設定を有効にするには、次の手順に従って操作を行ってください。

1. 「**Enable SMTP service**」（SMTP サービスを有効にする）のチェックボックスにチェックを入れてください。

2. SMTP サーバーを稼働させているコンピューターの IP アドレスないしはドメイン名を「**Server IP/Domain**」（サーバーIP/ドメイン）欄に入力してください。

3. SMTP サーバーがリッスンするポート番号を、「**Port**」（ポート）欄に設定してください。

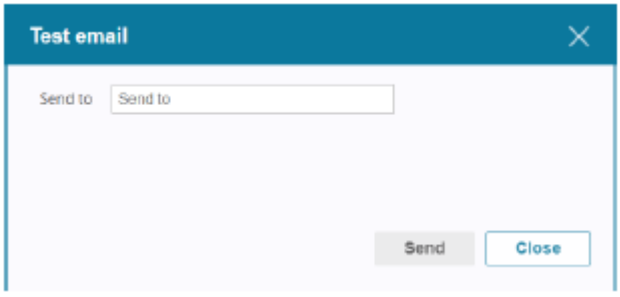
4. CC2000 の管理者のメールアドレスを、「**Email**」（E メール）欄に入力してください。

   注意： この欄は必ず設定してください。

5. SMTP サーバーで認証が必要な場合は、「**SMTP server requires authentication**」（SMTP サーバーは認証が必要）のチェックボックスにチェックを入れ、「Username」（ユーザーネーム）の欄に認証アカウント名を入力してください。また、「**Set password**」（パスワードの設定）の項目にチェックを入れて、入力欄にパスワードを設定してください。

6. SLL 経由で SMTP を保護する場合は、「**Secure connection (SSL)**」（セキュア接続（SSL））の項目にチェックを入れてください。

7. SMTP サーバーの設定が正しいかどうかを確認する場合は、「**Send a Test Email**」（テストメールを送信する）ボタンをクリックしてください。そうすると、下図のような画面が表示されます。



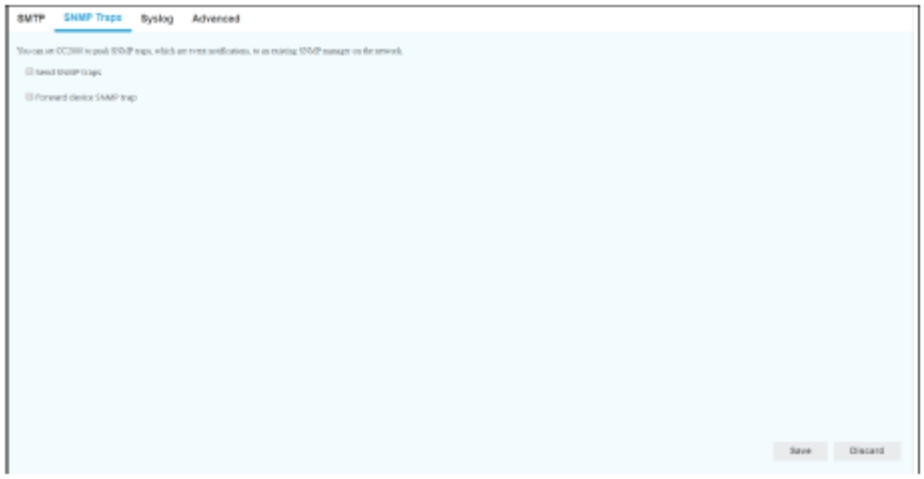
8. テストメールを受信するユーザーのメールアドレスを入力したら、「**Send**」(送信)ボタンをクリックしてください。設定に問題がない場合は、ここで指定されたメールアドレス宛にテストメールが送信されます。

注意:	宛先となるユーザーのメールアドレスは、半角英数字および記号を使用し、最大 128 文字以内になるように設定してください。

9. 「**保存**」ボタンをクリックして、設定内容を保存してください。

SNMP トラップ

「SNMP Traps」(SNMP トラップ)画面では、下記に説明するように、最大 4 つの SNMP マネジャーの情報を含むメイン SNMP トラップの設定を行うことができます。



SNMP トラップ通知を使用する場合は、下記の操作を行ってください。

1. 「**Send SNMP Traps**」(トラップを送信する)にチェックを入れてください。

2. トラップ情報をデバイスに転送する場合は、「**Forward device SNMP trap**」(デバイスの SNMP トラップを転送する)にチェックを入れてください。

3. チェックボックスにチェックを入れて、マネジャー設定を行ってください。

4. SNMPトラップイベント通知を受けるマネジャーコンピューターのIPアドレスとサービスポート番号を入力してください。IP アドレスは「**Destination IP/Domain**」(宛先 IP/ドメイン)欄に、また、ポート番号は「**Port**」(ポート)欄に、それぞれ入力します。有効なポート番号の範囲は 1～65535 で、デフォルトポート番号は 162 です。

注意:	ここで設定するポート番号がSNMP受信コンピューターで使用するポート番号と一致していることを確認してください。

5. 「**Version**」(バージョン)ドロップダウンメニューから、お使いの環境に適したオプションを選択してください。利用可能なオプションは、「SNMPv21」、「SNMPv2c」、「SNMPv3」です。

6. 手順 5 で設定した SNMP バージョンに対して、「**Community/Username**」(コミュニティー/ユーザーネーム)を入力してください。また、「**Security level**」(セキュリティーレベル)を選択してください。

7. 「**Authentication**」(認証)ドロップダウンメニューから、認証タイプを選択してください。また、各ステーションに該当する「**Authentication password**」(認証パスワード)欄に、認証パスワードを入力してください。

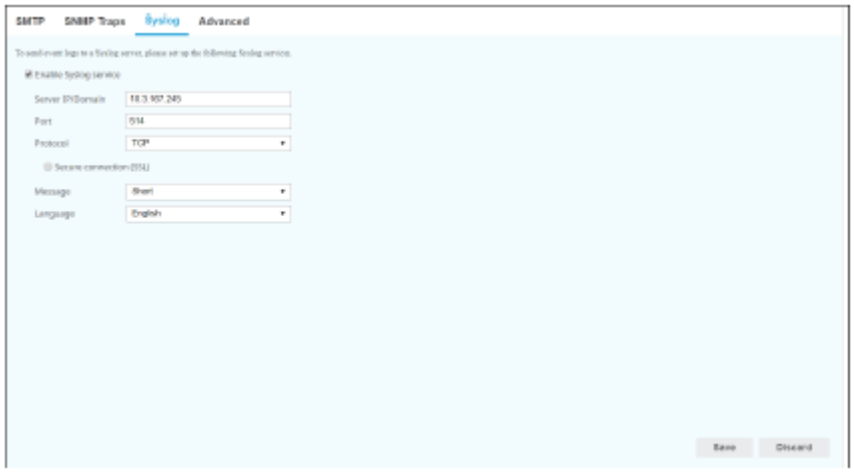
8. 「**Privacy**」(プライバシー)ドロップダウンメニューから、プライバシータイプを選択してください。また、各ステーションに該当する「**Privacy password**」(プライバシーパスワード)欄に、プライバシーパスワードを入力してください。

9. 残り 3 つの SNMP マネジャーに対して、手順 4～8 の操作を繰り返してください。

10. 設定が完了したら、「**Save**」(保存)をクリックしてください。

注意:	システムが設定内容を保存できるよう、これらの項目は、全て正確に入力してください。

Syslog

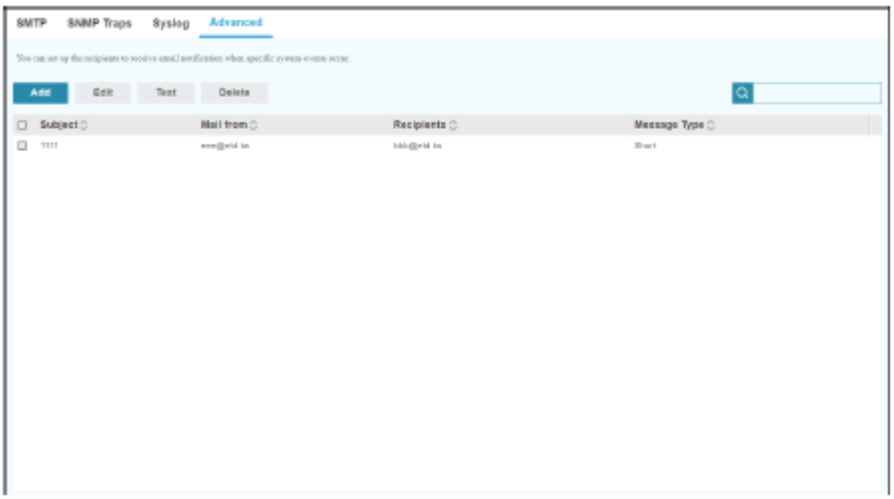


CC2000 で発生した全イベントを記録し、Syslog サーバーに書き込む場合は、次の手順に従って操作を行ってください。

1. 「Enable Syslog service」(Syslog サービスを有効にする)の項目にチェックを入れてください。
2. Syslog サーバーの IP アドレスを「Server IP/Domain」(サーバーIP/ドメイン)欄に、ポート番号を「Port」(ポート)欄に、それぞれ入力してください。有効な値の範囲は、1～65535 です。
3. 「Protocol」(プロトコル)ドロップダウンメニューから、プロトコルタイプを選択してください。選択できるオプションは、UDP と TCP です。
   TCP を選択した場合は、「Secure connection (SSL)」(セキュア通信(SSL))の項目にチェックを入れて、セキュア通信(SSL)を有効にすることができます。
4. 「Message」(メッセージ)ドロップダウンメニューから、ログをショートメッセージで記録するのか、フルメッセージで記録するのかを選択してください。
5. 「Language」(言語)ドロップダウンメニューから、送信メッセージで使用する言語を選択してください。
6. 全ての設定が終わったら、「Save」(保存)ボタンをクリックしてください。

詳細

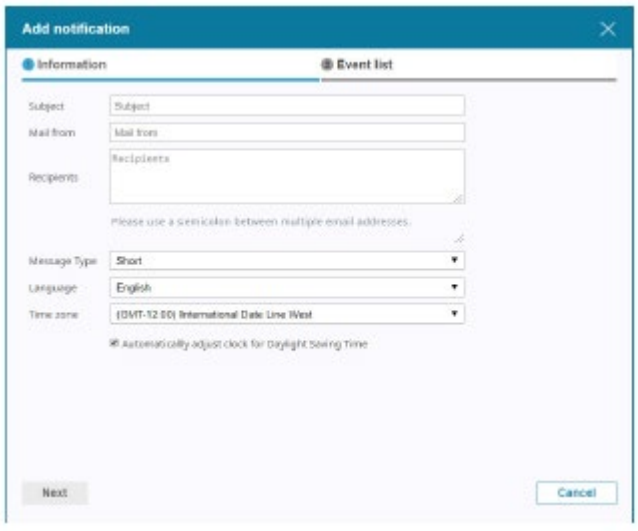
「Advanced」(詳細)画面は、CC2000 で発生した特定のイベントを、選択されたユーザー宛に通知するのに使用されます。このメニューを選択すると、下図のような画面が表示されます。



通知設定の追加

「Advanced」(詳細)画面には、「Add」(追加)、「Edit」(編集)、「Test」(テスト)、「Delete」(削除)といった 4 種類のボタンが提供されています。ユーザーを追加し、これらのユーザーが通知を受け取れるようにするには、次の手順に従って操作を行ってください。

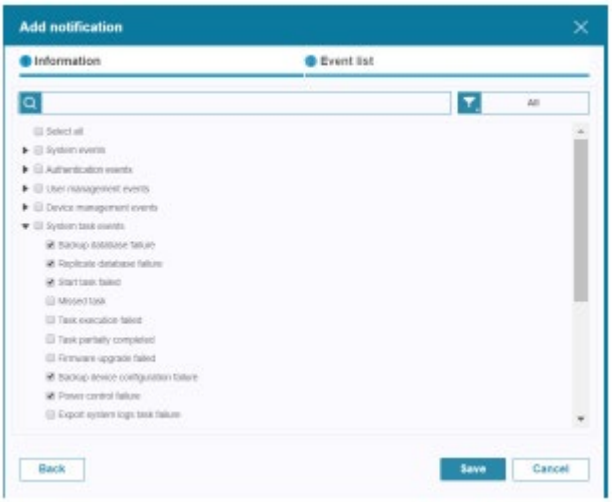
1. 「**Add**」(追加)をクリックして、「Add notification」(通知の追加)画面に遷移してください。



2. 通知メッセージのタイトルとなる文言を、「**Subject**」(件名)欄に入力してください。

3. 管理者のメールアドレスを、「Mail from」(差出人)欄に入力してください。
4. 通知メールの宛先となるユーザーのメールアドレスを、「Recipients」(宛先)欄に入力してください。複数のユーザー宛に通知を行う場合は、各メールアドレスをセミコロンで区切ってください。このとき、セミコロンの前後にスペースを入れないようにしてください。
5. メッセージタイプ(フルまたはショート)を、「Message Type」(メッセージタイプ)ドロップダウンメニューから選択してください。
6. 送信メッセージで使用する言語を「Language」(言語)ドロップダウンメニューから、また、ここで使用するタイムゾーンは「Time zone」(タイムゾーン)ドロップダウンメニューから、それぞれ選択してください。サマータイムが導入されている地域でお使いの場合は、「Automatically adjust clock for Daylight Saving Time」(サマータイムに合わせて時刻を自動調整する)の項目にチェックを入れてください。
7. 「Next」(次へ)をクリックして、メール通知の対象となるイベントを選択してください。選択済みの項目は、画面の右上にあるフィルターアイコン( )を使って確認することができます。

   選択済みのイベントを確認する場合は「Selected」(選択済み)を、全てのイベントを選択する場合は「All」(全て)を、それぞれ選択してください。



8. この画面でイベントを選択し終えたら、「Save」(保存)をクリックして、設定内容を保存してください。そうすると、「Advanced」(詳細)画面へと戻ります。

注意:	ユーザーがイベント通知のメールを受信できるようにするには、CC2000 の SMTP 設定画面で SMTP の設定を行う必要があります(詳細は p.238 参照)。

通知設定の編集

通知設定を変更するには、次の手順に従って操作を行ってください。

1. 変更対象となる通知のチェックボックスにチェックを入れたら、「Edit」（編集）をクリックしてください。
2. 「Event notification」（イベント通知）画面の情報とイベント一覧で変更を加えてください。
3. 設定を行ったら、パネルの右下にある「Save」（保存）をクリックしてください。

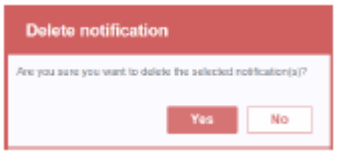
イベント通知のテスト

イベント通知のテストを行うには、次の手順に従って操作を行ってください。

1. テスト対象となる通知のチェックボックスにチェックを入れたら、「Test」（テスト）をクリックしてください。
2. システムが正常に動作している場合、宛先となるユーザーは、イベント通知のメールを受信します。失敗した場合は、エラーメッセージが表示されます。

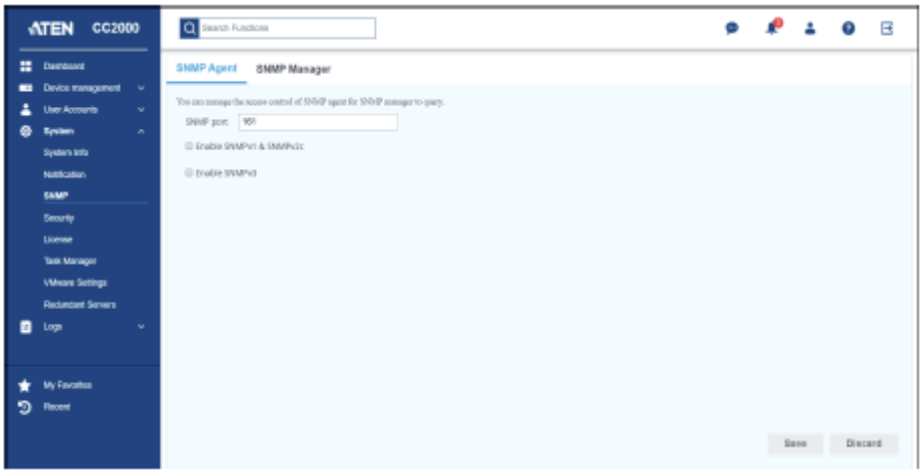
通知設定の削除

通知設置の削除を行うには、対象となる通知のチェックボックスにチェックを入れて、「Delete」（削除）をクリックしてください。そうすると、確認メッセージが表示されます。操作を続行する場合は、「Yes」（はい）をクリックしてください。



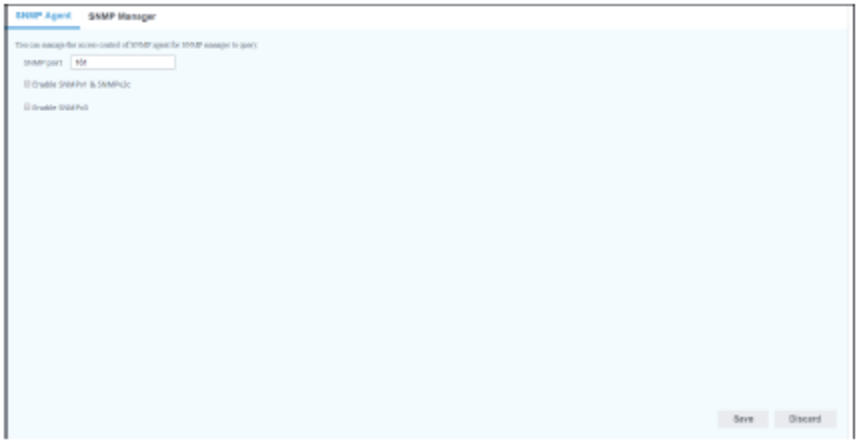
SNMP

「SNMP」メニューは、「**SNMP Agent**」(SNMP エージェント)と「**SNMP Manager**」(SNMP マネジャー)といった 2 つのタブメニューから構成されています。ここでは、SNMP マネジャーが問い合わせる SNMP エージェントのアクセス制御を管理することができます。「SNMP」画面のデフォルトは「**SNMP Agent**」(SNMP エージェント)で、下図のような外観です。



SNMP エージェント

「SNMP Agent」(SNMP エージェント)画面では、下図に示すように、CC2000 のエージェントを設定し、SNMP トラップイベントに対するアクセスを管理します。



SNMP エージェントを設定するには、下記の操作を行ってください。

1. トラップイベント情報を収集するエージェントコンピューターのポート番号を、「SNMP Port」（SNMP ポート）欄に入力してください。有効なポート番号の範囲は 1～65535 で、デフォルトポート番号は 161 です。

注意：	ここで設定するポート番号が SNMP マネジャーで使用するポート番号と一致していることを確認してください。

2. SNMP バージョン 1 と 2 をご使用の場合、「**Enable SNMPv1 and SNMPv2c Trap**」（SNMPv1 および SNMPv2c トラップを有効にする）にチェックを入れてください。そうすると、入力項目が表示されます。

3. コミュニティー名を「Community」（コミュニティー）欄に入力し、「**Access Type**」（アクセスタイプ）ドロップダウンメニューから適切な値（「Disable」（無効）、「Read」（読み込み）、「Write」（書き込み））を選択してください。「Read」（読み込み）または「Write」（書き込み）が選択されると、「Allowed NMS IP」（許可された NMS IP）の項目が有効になりますので、ここに NMS IP アドレスを入力してください。

4. SNMP v3 をご使用の場合、「**Enable SNMPv3**」（SNMPv3 を有効にする）をクリックしてください。

5. SNMP エージェントのチェックボックスにチェックを入れたら、ユーザーネームを「Username」（ユーザーネーム）欄に入力し、「**Security Level**」（セキュリティーレベル）ドロップダウンメニューから、適切な値（「None」（なし）、「Auth Protocol」（認証プロトコル）、「Authentication & Privacy」（認証＆プライバシー））を選択してください。

6. 「**Authentication**」(認証)ドロップダウンメニューから、適切な認証プロトコル(MD5 または SHA)を選択し、認証パスワードを「Authentication password」(認証パスワード)欄に入力してください。

7. 「**Privacy**」(プライバシー)ドロップダウンメニューから、適切なプロトコルを選択し、プライバシーパスワードを「Privacy password」(プライバシーパスワード)欄に入力してください。

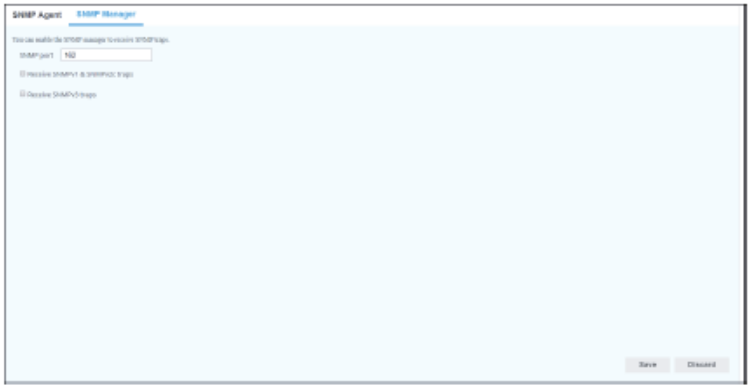
8. 各プロファイルに対応している許可された NMS IP アドレスを、「Allowed NMS IP」(許可された NMS IP)欄に入力してください。

9. 「**Save**」(保存)をクリックして、設定内容を保存してください。

注意:	システムが設定内容を保存できるよう、これらの項目は、全て正確に入力してください。

SNMP マネジャー

「SNMP Manager」(SNMP マネジャー)画面では、下記に説明するように、SNMP トラップイベント通知を受信する CC2000 の管理ステーションを設定することができます。



SNMP マネジャーを設定するには、下記の操作を行ってください。

1. 通知を受信するコンピューターのサービスポート番号を、「SNMP port」(SNMP ポート)欄に入力してください。有効なポート番号の範囲は 1～65535 で、デフォルトポート番号は 162 です。

注意:	ここで設定するポート番号が SNMP エージェントで使用するポート番号と一致していることを確認してください。

2. SNMPv1 と v2 をご使用の場合、「**Receive SNMPv1 & SNMPv2c traps**」(SNMPv1 および SNMPv2c トラップを受信する)にチェックを入れてください。そうすると、「Community」(コミュニティー)欄が表示されます。

3. SNMP バージョンのコミュニティーの値を「Community」(コミュニティー)欄に入力してください。

4. SNMP バージョン 3 をご使用の場合、「**Receive SNMPv3 traps**」(SNMPv3 トラップを受信する)をクリックして有効にしてください。そうすると、設定項目が表示されます。

5. SNMP マネジャーのチェックボックスにチェックを入れたら、ユーザーネームを「Username」(ユーザーネーム)欄に入力し、「**Security Level**」(セキュリティーレベル)ドロップダウンメニューから、適切な値(「None」(なし)、「Auth Protocol」(認証プロトコル)、「Authentication & Privacy」(認証&プライバシー))を選択してください。

6. 「**Authentication**」(認証)ドロップダウンメニューから、適切な認証プロトコル(MD5 または SHA)を選択し、認証パスワードを「Authentication password」(認証パスワード)欄に入力してください。

7. 「**Privacy**」(プライバシー)ドロップダウンメニューから、適切なプロトコルを選択し、プライバシーパスワードを「Privacy password」(プライバシーパスワード)欄に入力してください。

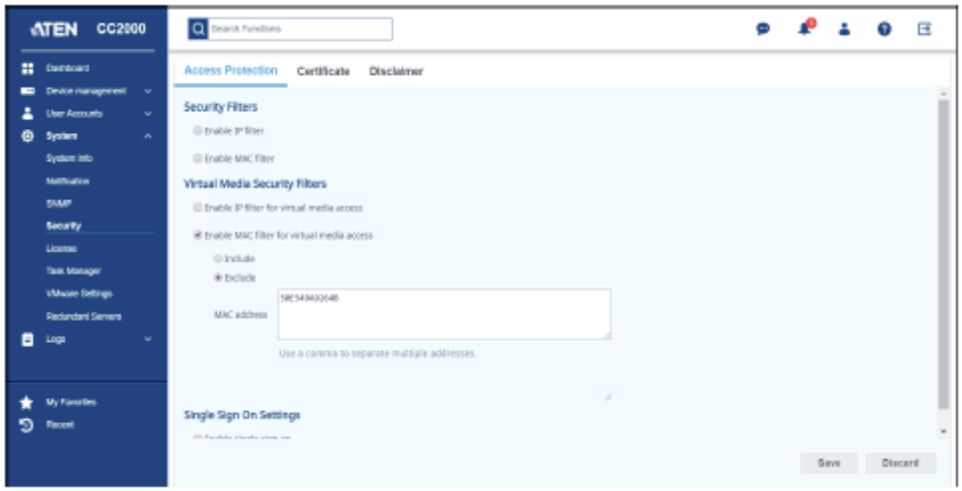
8. 「Save」(保存)をクリックして、設定内容を保存してください。

注意:

1. システムが設定内容を保存できるよう、これらの項目は、全て正確に入力してください。
2. ATEN PDU からの SNMMP v3 トラップを受信するには、「Authentication」(認証)ドロップダウンリストから「MD5」を選択し、「Privacy」(プライバシー)ドロップダウンリストから「AES-128」を選択してください。

セキュリティー

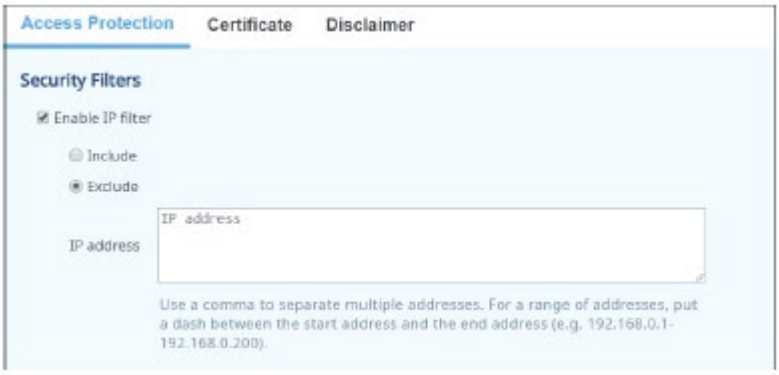
「Security」(セキュリティー)メニューは、「**Access Protection**」(アクセス保護)、「**Certificate**」(証明書)、「**Disclaimer**」(免責事項)といった 3 つのタブメニューから構成されています。この画面では、CC2000 へのアクセスを制御することで、セキュリティーレベルを設定することができます。「Security」(セキュリティー)画面のデフォルトは「**Access Protection**」(アクセス保護)で、下図のような外観です。



アクセス保護

IP フィルター

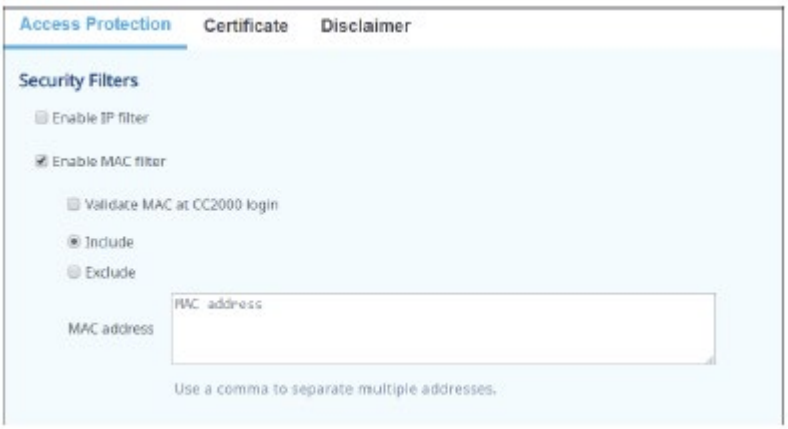
IP フィルター機能は、接続を試みるコンピューターの IP アドレスに基づいて CC2000 へのアクセスを制御します。



- IP フィルター機能を有効にするには、「**Enable IP filter**」(IP フィルターを有効にする)の項目にチェックを入れてください。
  - 「**Include**」(許可)のラジオボタンが選択されると、このアドレスリストで設定されている全てのアドレスからのアクセスが許可されます。このとき、これ以外のアドレスからのアクセスは拒否されます。
  - 「**Exclude**」(除外)のラジオボタンが選択されると、このアドレスリストで設定されている全てのアドレスからのアクセスが拒否されます。このとき、これ以外のアドレスからのアクセスは許可されます。
- IP フィルターは、IP アドレスを単独または範囲で指定することができます。IP アドレスは必要なだけ登録することができます。次の注意事項に従って、IP アドレスを「**IP address**」(IP アドレス)のテキスト入力ボックスに直接設定してください。
  - 単独の IP アドレスを複数設定する場合は、IP アドレスをコンマで区切ってください。コンマの前後にはスペースを入れないでください。
  - IP アドレスを範囲で設定する場合は、範囲の始点となる IP アドレスを入力した後にダッシュを続け、範囲の終点となる IP アドレスを入力してください。
- 設定内容を保存するには、「**Save**」(保存)をクリックしてください。
- フィルターを変更または削除する場合は、「**IP address**」(IP アドレス)のテキスト入力ボックスを直接編集してください。

MAC フィルター

MAC フィルター機能は、接続を試みるコンピューターの MAC アドレスに基づいて CC2000 へのアクセスを制御します。



- MAC フィルター機能を有効にするには、「**Enable MAC filter**」(MAC フィルターを有効にする)の項目にチェックを入れてください。
  - 「**Validate MAC at CC2000 login**」(CC2000 ログイン時に MAC アドレスをチェックする)が

有効になっていると、CC2000 はユーザーのログイン時に、そのユーザーが使っているクライアント PC の MAC アドレスを確認します。無効になっている場合は、ビューワーの起動時にのみ MAC アドレスを確認します。

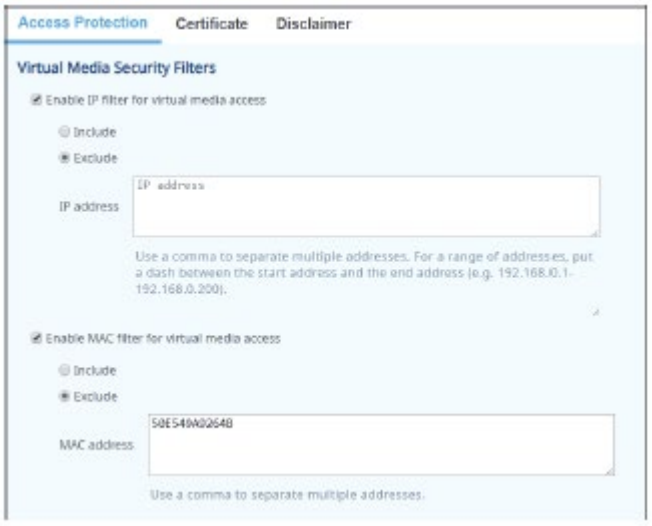
- 「Include」(許可)のラジオボタンが選択されると、このアドレスリストで設定されている全てのアドレスからのアクセスが許可されます。このとき、これ以外のアドレスからのアクセスは拒否されます。
- 「Exclude」(除外)のラジオボタンが選択されると、このアドレスリストで設定されている全てのアドレスからのアクセスが拒否されます。このとき、これ以外のアドレスからのアクセスは許可されます。

◆ MAC フィルターは、MAC アドレスを単独または範囲で指定することができます。MAC アドレスは必要なだけ登録することができます。MAC アドレスは、「MAC address」(MAC アドレス)のテキスト入力ボックスに直接入力してください。また、MAC アドレスを複数設定する場合は、MAC アドレスをコンマで区切ってください。この時、コンマの前後にはスペースを入れないでください。

◆ 設定内容を保存するには、「Save」(保存)をクリックしてください。

バーチャルメディアのセキュリティーフィルター

IP および MAC フィルターは、バーチャルメディアにアクセスしようとするコンピューターの IP アドレスと MAC アドレスに基づいて、バーチャルメディアへのアクセスを制御する場合にも使用することができます。



◆ バーチャルメディアのセキュリティーフィルターを有効にするには、「Enable IP filter for virtual media access」(バーチャルメディアのアクセスに対する IP フィルターを有効にする)または「Enable MAC filter for virtual media access」(バーチャルメディアのアクセスに対する MAC フ

ィルターを有効にする）にチェックを入れて、p.246「IP フィルター」および p.247「MAC フィルター」に記載の操作手順に従ってください。

◆ 設定内容を保存するには、「Save」（保存）をクリックしてください。

シングルサインオンの設定

シングルサインオンの設定が有効になっている場合、別のウェブサービスからアクセスしたユーザーは、フォームベース認証経由で CC2000 へと自動的にログインすることができます。ログインを統合するには、p.402「シングルサインオン HTML サンプルコード」を参照してください。

証明書

SSL による暗号化通信で CC2000 にログインする場合は、ユーザー自身が意図したウェブサイトにログインすることを証明するために、署名済み証明書が使用されます。この「Certificate」（証明書）画面では、証明書の作成や変更、また、証明書の取得をそれぞれ行うことができます。

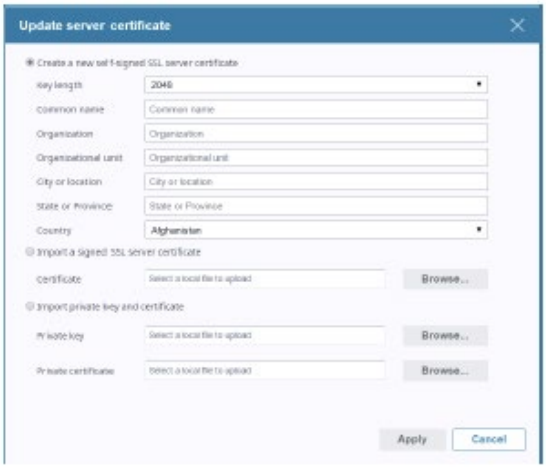
ウェブ接続（HTTPS）のようなセキュア SSL サービスを利用するために、サードパーティーの認証局から発行された署名済み証明書をインポートすることができます。

各 CC2000 は、セットアップの際に下図の画面の情報に基づいて独自の自己署名証明書を作成します。

自己署名証明書の変更

自己署名証明書を変更すると、セットアップ証明書では作成されていない付加情報を証明書に提供することができます。新しい証明書を作成することで自己署名済みの SSL 証明書を変更することができます。新しい自己署名証明書を作成する場合は、以下の手順で操作してください。

1. 画面左下にある「**Update**」(アップデート)ボタンをクリックしてください。そうすると、下図のような画面が表示されます。



2. 「**Create a new self-signed SSL server certificate**」(SSL の自己署名証明書を作成する)のラジオボタンを選択し、下表の内容を参考にしながら画面内の項目を入力してください。

項目	説明
Key length (鍵長)	証明書の鍵長(ビット数)をドロップダウンメニューから選択してください。オプションは、1024、2048、4096 です。
Common Name (共通の名前)	SSL 証明書を要求するサイトの完全修飾ドメイン名(FQDN)を入力してください。 例:www.yourdomainname.com
Organization (組織)	CC2000 が使用されている地域で、法律上認められた企業名、もしくは個人名を入力してください。
Organizational Unit (組織ユニット)	証明書の発行を要求している企業の部署名を入力してください。 例:会計部、マーケティング部
City or Location (地名または ロケーション)	都市または地域の正式名称を入力してください。 例:台北

(表は次のページに続きます)

項目	説明
State or Province （州または省）	州または省の正式名称を入力してください。
Country （国名）	証明書が登録された組織が属している国の国コード(2 桁)です。 **注意:** これらは一般的な略称と必ずしも一致する訳ではありません。この国コードが不明な場合は、「**SSL 国コード**」などのキーワードでオンライン検索して調べてください。

3. 項目の設定が完了したら、「**Apply**」（適用）ボタンをクリックしてください。

データベースの更新中には、処理を待機するよう促すメッセージが表示され、しばらくするとウェブ画面が終了しますので、ログイン手順の最初に戻り、セキュリティー証明書を受け入れてもう一度ログインを行ってください。

このとき、ログイン手順の最初に戻りますが、セキュリティー証明書の許可とログインを行う必要があります。

署名済み SSL サーバー証明書のインポート

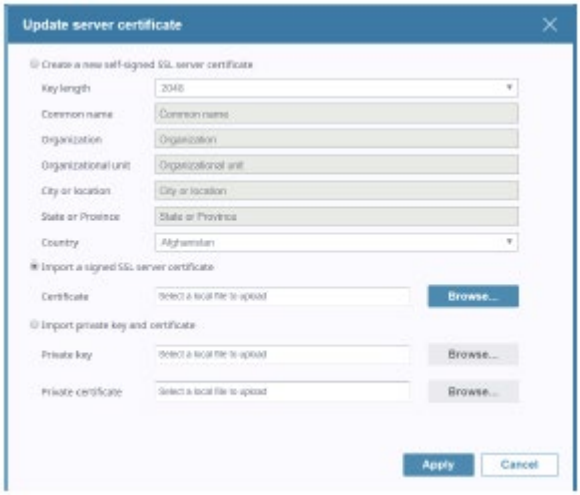
ログイン時に証明書の受け入れを促すメッセージを毎回表示しないようにするために、管理者はサードパーティーの認証局（CA)が署名した証明書を使用することが可能です。

サードパーティーによる署名済み証明書を使用する場合は、以下の手順で操作してください。

1. 自己署名証明書を作成した後、パネル右上の「**Get CSR**」（CSR を取得する）ボタンをクリックしてください。

2. 選択した CA のウェブサイトにアクセスし、手順 1 で生成された情報で SSL 証明書を申請してください。

3. CA から証明書が送られてきたら、「Certificate」（証明書）画面を開き、パネル左下にある「**Update**」（アップデート）ボタンをクリックしてください。



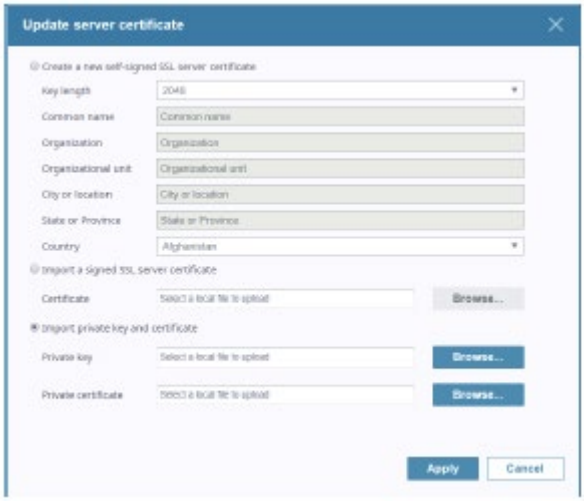
4. 「Import a signed SSL server certificate」(署名された SSL サーバーの証明書をインポートする)の項目を選択し、証明書ファイルが保存されている場所を選択してください。

5. 画面右下にある「Apply」(適用)ボタンをクリックしてください。

注意:	本セクションで挙げられた証明書は、いずれもセキュリティーのレベルに変わりはありません。変更された自己署名証明書のメリットは、セットアップ証明書に比べて、より多くの情報を提供できるという点にあります。これに対し、CA サードパーティーの証明書のメリットは、ユーザーのログイン時に証明書の受け入れを促すダイアログを毎回操作する必要がなく、その証明書が認可された機関によって有効だと証明されている点にあります。

プライベートキーと証明書のインポート

SSL による暗号化通信で CC2000 にログインする場合は、ユーザー自身が意図したウェブサイトにログインすることを証明するために、署名済み証明書が使用されます。デフォルトの ATEN 証明書を使うのではなく、このセクションで自分のプライベート暗号キーと署名済み証明書を使うように設定することで、セキュリティーを強化することができます。



プライベート証明書を発行するには、自己署名された証明書を作成する方法と、サードパーティーの証明局(CA)によって署名された証明書をインポートする方法の 2 つの方法があります。

自己署名済証明書の作成

自己署名済証明書は、「openssl.org.」で公開されている「Win32 OpenSSL」などで作成できます。OpenSSL を使って独自のプライベートキーと SSL 証明書を作成する方法の詳細については、p.337 「自己署名(プライベート)証明書」を参照してください。

CA 署名済 SSL サーバー証明書の取得

セキュリティーを強化するために、サードパーティーの認証局(CA)によって署名された証明書を使うことを推奨します。サードパーティーによって署名された証明書を取得する場合は、認証局のウェブサイトにアクセスし、SSL 証明書を申請してください。CA から証明書が送られてきたら、お使いのコンピューターのハードディスクドライブの適当なフォルダーに保存してください。

プライベート証明書のインポート

プライベート証明書をインポートする場合は、下記の手順に従って操作してください。

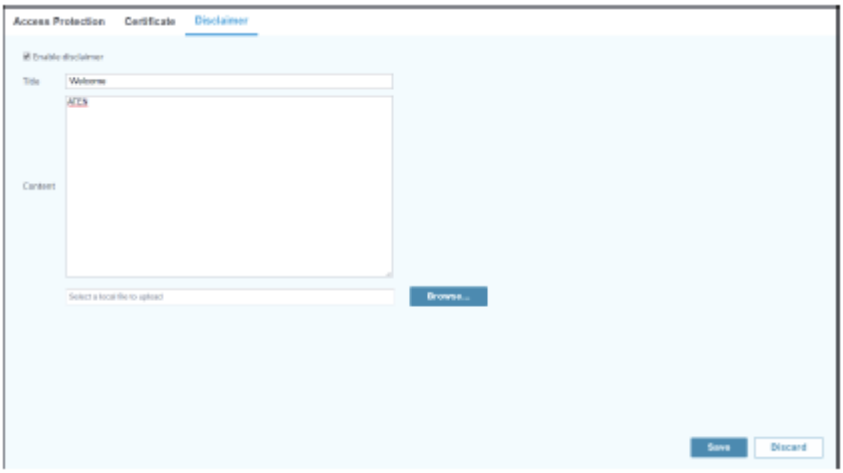
1. 「**Update**」(アップデート)をクリックしてください。
2. 「**Private Key**」(プライベートキー)の隣にある「**Browse**」(参照)ボタンをクリックして、プライベート暗号キーのファイルがあるフォルダーに移動し、このファイルを選択してください。
3. 「**Certificate**」(証明書)の隣にある「**Browse**」(参照)ボタンをクリックして、証明書のファイルがあるフォルダーに移動し、このファイルを選択してください。
4. パネル右下にある「**Apply**」(適用)ボタンをクリックしてください。

注意: プライベート暗号キーと署名済証明書は同時にインポートしてください。

免責事項

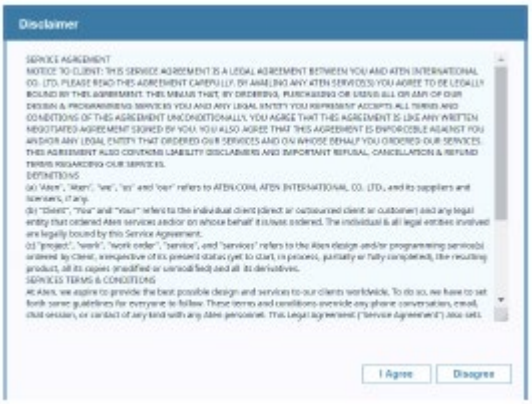
ユーザーが CC2000 にログインした際に免責事項が表示されるように設定することができます。

免責事項を設定するには、「Enable disclaimer」(免責事項を有効にする)の項目にチェックを入れ、免責事項のタイトルと内容を入力し、「Save」(保存)をクリックしてください。



免責事項の設定は、「Browse」(参照)をクリックして、保存済みの免責事項ファイルをアップロードすることでも行えます。

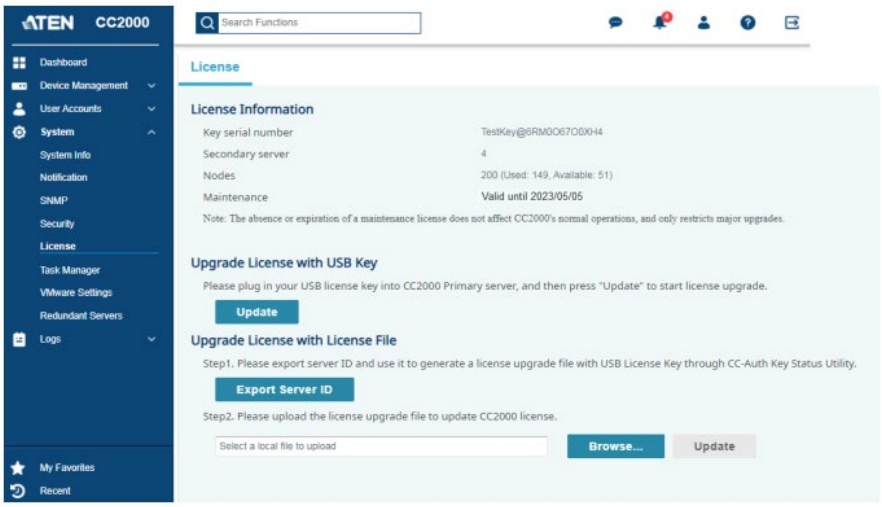
設定が行われると、ログイン時に免責事項が表示されるようになります。



ライセンス

CC2000 のライセンスは、CC2000 サーバーの構成で許可されたノード数を管理します。購入された CC2000 にデフォルトで付属しているライセンスは、16 ノード版の 1 プライマリー(セカンダリーなし)のデモ用ライセンスです。セカンダリーサーバーや追加ノードを増やす場合は、ライセンスの購入およびアップグレードが必要です。

「System」(システム)メニューから「**License**」(ライセンス)メニューを選択すると、下図のような画面が表示されます。



この画面における各項目の詳細は下表の通りです。

セクション	項目	説明
License Information (ライセンス情報)	Key serial number (キーシリアルナンバー)	ライセンスキーのシリアルナンバーです。 **注意:**これは CC2000 サーバーのインストール時に使用したソフトウェアのシリアルナンバーとは異なります。このシリアルナンバーは USB ライセンスキーの表面に記載されているものです。
	Secondary server (セカンダリーサーバー)	許可されたセカンダリーサーバーの合計数です(購入ライセンスに応じて最大 31 ユニットまで対応)。

(表は次のページに続きます)

セクション	項目	説明
License Information （ライセンス情報） （続き）	Nodes （ノード）	現在の機器構成において、購入済みライセンスに応じて許可されたノードの合計です。 **注意：**ライセンス可能なノード数は、購入ライセンスにもよりますが、数の制限はありません。
	Maintenance （メンテナンス）	CC2000 ソフトウェアのアップデートの有効期間を表示します。「N/A」と表示されている場合は、保守ライセンスがライセンスキーに適用されていないことを示します。 **注意：** ◆ ライセンスの期限が切れてしまった場合でも CC2000 は正常に動作しますが、アップデートはマイナーな修正に限定されます（例：v4.0.109 から v4.0.201）。 ◆ システムを v3.3 から v4.0 にアップグレードするには、保守ライセンスが必要です。保守ライセンスの購入または更新に関する詳細は、担当営業までお問い合わせください。
Upgrade License with USB Key （USB キーでライセンスをアップグレードする）	Update （アップデート）	クリックすると、CC2000 サーバーに挿入した USB ライセンスキーでライセンスのアップグレードを行います。
Upgrade License with License File （ライセンスファイルでライセンスをアップグレードする）		このセクションを使用すると、CC2000 サーバーに USB ライセンスキーを直接挿入することなくライセンスのアップグレードを行います。

ライセンスをアップグレードするには、希望するセカンダリーとノードの数に合わせてライセンスキーをご購入ください。購入した USB キーがお手元に届きましたら、次のいずれかの方法で CC2000 のライセンスをアップグレードすることができます。

◆ サーバーにライセンスキーを直接挿入することで、ライセンスをアップグレードする
◆ ライセンスキーを直接挿入せずに、ライセンスをアップグレードする

USB キーを使用したライセンスのアップグレード

1. お使いのプライマリーサーバーの USB ポートにライセンスキーを挿してください。
2. 「Upgrade License with USB key」(USB キーを使ってライセンスをアップグレードする)セクションにある「**Update**」(アップデート)ボタンをクリックしてください。

注意:

- ◆ アップデートが完了したら、USB ポートにキーを接続したままにする必要はありませんので、キーを取り外してください。このキーは、将来、アップグレードアプリを実行した時にライセンス認証するため必要になります。安全な場所に保管するようにしてください。
- ◆ USB ライセンスキーを紛失した場合は、弊社販売代理店にご連絡の上、新しいものを入手してください。紛失したキーのシリアルナンバーを提供すると、新しいキーにはそのキーに保存されていた情報と同じものが格納されます。
- ◆ CC2000 が Windows Hyper-V 仮想マシンにインストールされている場合、USB ライセンスキーを使用すると、ライセンスはアップデートに失敗します。これは、Hyper-V が USB の非ディスクデバイスを仮想マシンに対してパススルーできないことに起因します。このような場合には、USB Redirector などのサードパーティーのソフトウェアを使用することで、仮想マシンが USB ライセンスキーへとアクセスしてアップデートできるようにしてください。

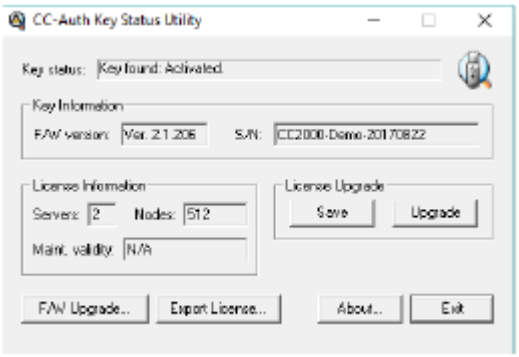
ライセンスファイルを使用したライセンスのアップグレード

この方法は、例えば、USB 接続が許可されない制限エリアのように、CC2000 プライマリーサーバーに対して USB ライセンスキーを直接挿入するのが難しい場合に有用です。

1. CC2000 のプライマリーサーバーで、「**Export Server ID**」(サーバーID をエクスポートする)をクリックして、サーバーID ファイル(*.sid)を生成してください。このファイルには、サーバーとシステムに関する詳しい情報が含まれています。このファイルは、エクスポートしたら、別の PC に保存してください。

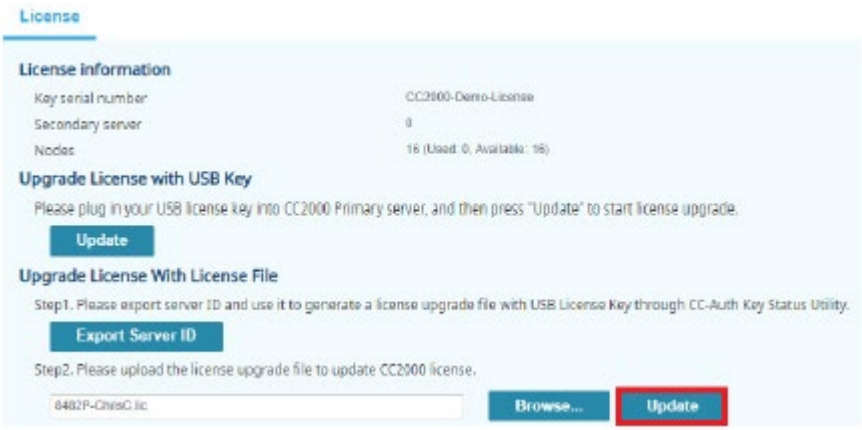
2. 手順 1 でファイルを保存した PC に、USB ライセンスキーを挿入してください。

3. 「CC-Auth Key Utility」(CC 認証キーユーティリティー)を起動すると、下図のような画面が表示されます。この画面で「**Export License**」(ライセンスのエクスポート)をクリックしてください。そうすると、手順 1 で生成したサーバーID ファイルのパスを指定するよう促されます。操作が完了すると、ライセンスアップグレードファイル(*.lic)が生成されます。



4. ライセンスアップグレードファイル(*.lic)をインポートし、CC プライマリーの PC に保存してください。そうしたら、「Upgrade License with License File」(ライセンスファイルを使ってライセンスをアップグレードする)セクションにある「**Browse**」(参照)ボタンをクリックして、ファイルを指定してください。

5. 「**Upgrade**」(アップグレード)をクリックして、ライセンスのアップグレードを開始してください。



注意:	ライセンスアップグレードファイルは、サーバーID ファイルが生成された CC2000 サーバーのライセンスのアップグレードにしか使用することができません。

ライセンスの共有

CC2000 のシステム構成において権限が与えられているデバイスのライセンス数は、ライセンスキーを通じてプライマリーサーバーに設定され、その構成における全ての CC2000 サーバーによって共有されます。ライセンス数に関する情報は、プライマリーサーバーで登録した際に各セカンダリー

に送られます（p.281「プロパティーの参照」参照）。

CC2000 に追加できるデバイスの数に制限はありませんが、実際にはライセンスと同じ数のノードが作成され管理されます（p.69 参照）。

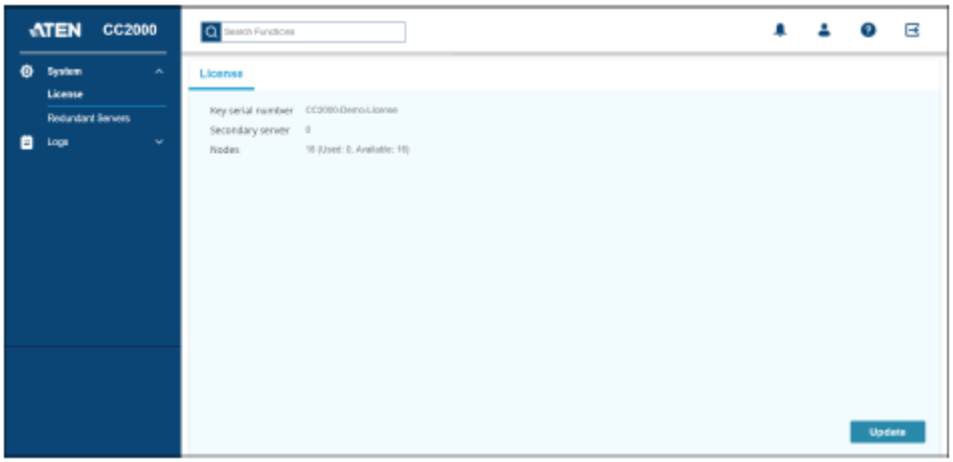
デバイスが CC2000 に追加されると、これらのデバイスはデフォルトではロックされるように設定されます。これらのデバイスの設定情報は CC2000 に格納されますが、管理することはできません。

ロックされたポートは、物理ポートを選択した後で「**Unlock**」（ロック解除）ボタンをクリックする（p.141「デバイスのロックとロック解除」参照）か、そのポートをアグリゲートデバイスの一部に設定する（p.110 参照）ことで解除することができます。

全ライセンスノードが使用中である場合、現在ロックされていないポートがロックされた後か、アグリゲートデバイスが削除されて、その結果、使用中のライセンスに空きができると、ロックされたポート(または新しいアグリゲートデバイス)はそのライセンスでロックを解除することができますので、CC2000 で管理できるようになります。

ライセンスの競合

同一ネットワークセグメント上にある 2 つのプライマリーサーバーが同じライセンスキーでアップグレードされると、ライセンスの競合が発生します。2 番目にアップグレードされた CC2000 サーバーのウェブブラウザーの GUI メニューは、下図のように表示されます。



競合の発生を確認する場合は、「**Logs**」（ログ）タブをクリックしてください。ライセンスの競合が発生している場合、ログファイルに以下のメッセージが表示されています。

A license violation has been detected at primary server. Remote CC server (IP:[*競合しているサーバーの IP アドレス*])

このような場合、競合を解消するにはいくつか方法があります。

1. 2 台のプライマリーサーバーのうち片方に対して、シャットダウンするか、サービスを停止するか、ネットワークから切り離すか、CC2000 を完全にアンインストールするかの、いずれかの方法を採ってください。
2. 競合が発生している方の CC2000 (2 台目のサーバー) を正常な方 (1 台目のサーバー)で登録してください。登録された方の CC2000 はセカンダリーサーバーになります。(このとき、セカンダリーライセンスが利用可能であることが前提です。)
3. 2 台の CC2000 サーバーを独立させて使用したい場合は、代理店に連絡して、2 台目の CC2000 のライセンスも別途購入してください。

タスクマネージャー

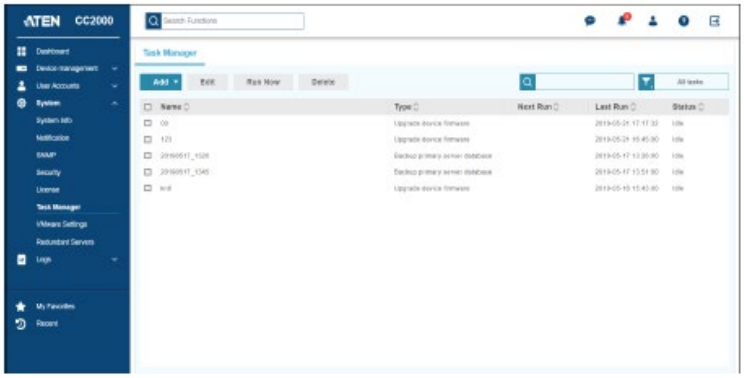
「Task manager」(タスクマネージャー)メニューには、「**Add**」(追加)、「**Edit**」(編集)、「**Run Now**」(今すぐ実行)、「**Delete**」(削除)といった 4 つの設定アクションが提供されています。システム管理権限のある管理者は、このメニューでシステムのメンテナンスタスクを実行することができます。実行できるタスクは、そのユーザーアカウントが作成された際に設定されたユーザータイプと権限オプションによって決定されます。CC2000 で実行可能なタスクは以下の通りです。

- プライマリーサーバーのデータベースバックアップ

注意:
1. このタスクは、CC2000 のプライマリーサーバーでのみ実行可能です。
2. データベースのリストアは、CC2000 ユーティリティーを使って行います。詳細については p.341「リストア」をご参照ください。

- デバイスの電源管理
- デバイスの最新ファームウェアへの自動アップグレード
- デバイス設定のバックアップ
- イベントログのエクスポート
- デバイスログのエクスポート
- シリアルコンソール履歴のエクスポート

「System」(システム)メニューから「**Task Manager**」(タスクマネージャー)を選択すると、下図のような画面が表示されます。



注意: 上図は、プライマリーサーバーの画面の表示例です。セカンダリーサーバー側でも基本的には上図と同じような画面が表示されますが、リストにデフォルトで「Replicate Database」(データベースの複製)という項目が表示されます。これは、接続しているプライマリーのデータベースを複製する機能です(p.278 参照)。

「Task Manager」(タスクマネージャー)一覧には、設定済みのタスクが全て表示されます。一覧の各項目の詳細は下表の通りです。

項目	説明
Name （名前）	タスクを作成した際に設定した名前です。
Type （タイプ）	設定されたタスクの種類です。
Next Run （次回の実行）	タスクが特定の時刻に実行されるようスケジューリングされている場合は、その実行予定時刻がここに表示されます。
Last Run （前回の実行）	タスクが最後に実行された時間が表示されます。
Status （ステータス）	タスクが実行中であるか、また待機中であるかが表示されます。

追加

タスクを追加する場合は、以下の手順で操作してください。

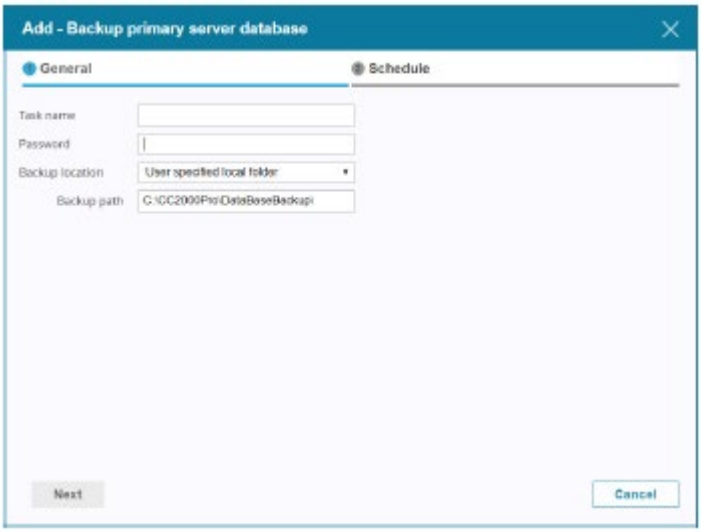
1. 「Add」(追加)をクリックしてください。そうすると、選択できるタスクの一覧が表示されます。

2. 追加するタスクをクリックして選択してください。そうすると、ウィンドウがポップアップ表示されます。内容は選択されたタスクによって異なります。

選択されたタスクに応じた画面が表示されます。これらのタスクは、種類はそれぞれ異なりますが、設定手順はほとんど同じです。本マニュアルでは、タスクの設定方法として次の例を挙げておきますので、参考にしてください。

プライマリーサーバーのデータベースバックアップ

リストから「**Backup primary server database**」(プライマリーサーバーのデータベースバックアップ)の項目を選択すると、下図のような画面が表示されます。



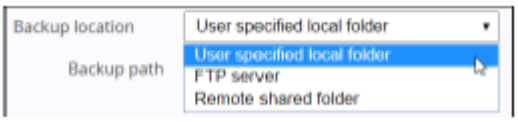
1. タスクの名前を「Task Name」(タスク名)欄に、パスワードを「Password」(パスワード)欄に、それぞれ入力してください。

注意:

1. このタスクは、CC2000 のプライマリーサーバーでのみ実行可能です。
2. 設定したパスワードは控えておき、人目に付かない場所に保管しておいてください。このパスワードはデータベースのリストアの際に必要になります(未設定の場合は、データベースのリストアの際にもパスワードは必要ありません)。データベースのリストアに関する詳細は、p.341「リストア」をご参照ください。
3. パスワードは、半角英数字を使って 32 文字以内で設定してください。
4. このバックアップファイルには「.cbk」という拡張子が付きます。

---

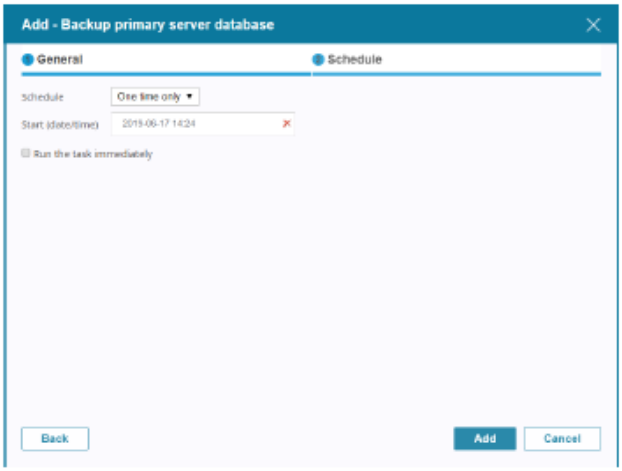
2. バックアップファイルを保存する場所を「**Backup location**」(バックアップ場所)ドロップダウンメニューから選択してください。選択できるオプションは、「**User specified local folder**」(ユーザーが指定するローカルフォルダー)、「**FTP server**」(FTP サーバー)、「**Remote shared folder**」(リモート共有フォルダー)の 3 種類です。



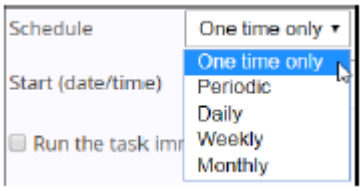
◆ デフォルトでは、このバックアップファイルは CC2000 のローカル・インストールディレクトリーに保存されます。例:C:¥CC2000Pro¥DataBaseBackup

◆ 「FTP server」(FTP サーバー)または「Remote shared folder」(リモート共有フォルダー)を選択した場合は、残りの項目も入力してください。

3. 画面内の項目の入力が完了したら、「**Next**」(次へ)ボタンをクリックしてください。このボタンをクリックすると、「Schedule」(スケジュール)画面が表示されます。



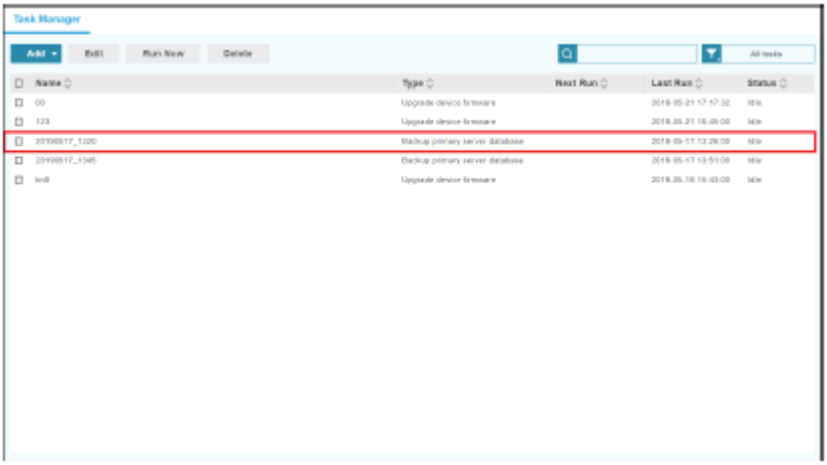
4. 「Schedule」(スケジュール)ドロップダウンメニューを使って、利用可能な値の一覧を確認してください。



「Schedule」(スケジュール)で選択された項目に応じて、スケジュールに必要な項目を入力する画面が表示されます。例えば、「One time only」(一度きり)を選択した場合は、「Start (date/time)」(開始(日時))の項目が表示されます。また、「Periodic」(定期)を選択した場合は、オプションの期間の項目が表示されます。

注意: 「Schedule」(スケジュール)でバックアップが実行される時間を設定していて(例:毎月)、今月から実行したい場合は、画面に表示されている日時よりも後になるように開始日時を設定し、「Run the task immediately」(タスクをすぐに実行する)の項目からチェックを外してください。この画面における時刻設定の項目には、画面にアクセスした際の時刻が表示されているため、変更せずに保存した場合、実行予定時刻は、変更を保存した時間の前になってしまいます。そうすると、CC2000 がタスクを実行するのは翌月となってしまいますので、ご注意ください。

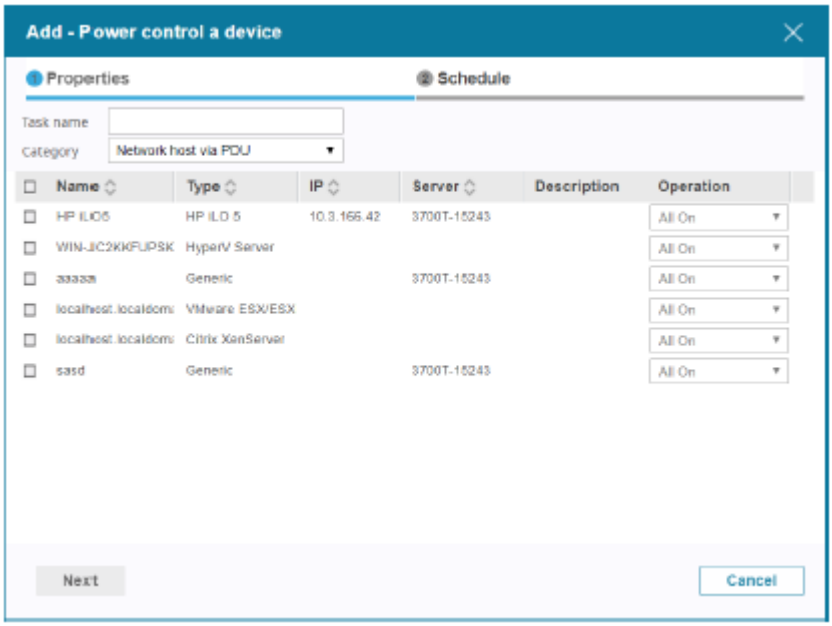
5. タスクのスケジュールを設定したら、「Add」(次へ)ボタンをクリックしてください。以上の操作でタスクはメイン画面のタスク一覧に追加されます。



注意: タスクをすぐに実行したい場合は、該当するタスクの名前の前にあるチェックボックスにチェックを入れ(複数指定可)、「Run Now」(すぐに実行)ボタンをクリックしてください。

デバイスの電源管理

リストから「Power Control a Device」(デバイスの電源管理)の項目を選択すると、ポートに対する電源のオンまたはオフ操作を自動的に実行するタスクのスケジューリングを設定することが可能です。



1. タスクに名前を設定してください。

2. 電源オンまたは電源オフの操作を、選択されたデバイス全体に対して行うのか、あるいはポート単位で行うのかを「Category」(カテゴリー)ドロップダウンメニューから選択してください。

3. 操作対象となるデバイスを選択してください。列の見出しにあるチェックボックスを使うと、デバイスを一括で選択または選択解除できます。各行にあるチェックボックスを使うと、個々のデバイスを選択または選択解除できます。

4. 各ポートの電源をオンにするかオフにするかを、「Operation」(操作)列で選択してください。

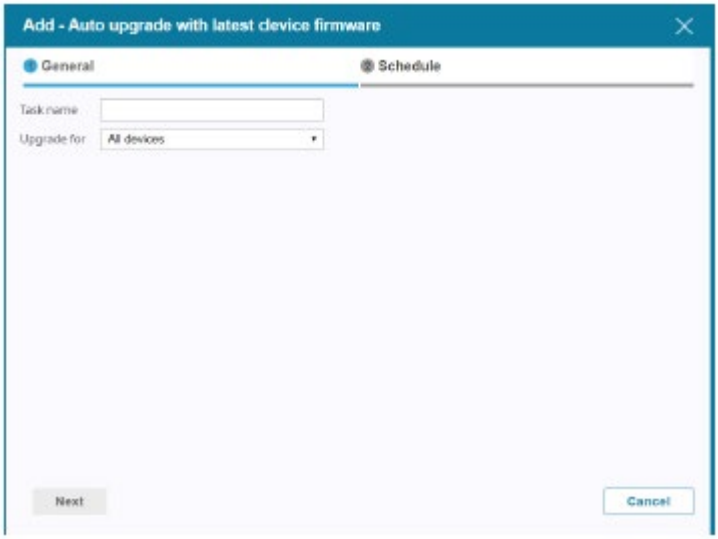
5. 「**Next**」(次へ)ボタンをクリックし、「Schedule」(スケジュール)画面でスケジュールの選択を行ってください。

注意:	スケジュールの設定手順については p.263「プライマリーサーバーのデータベースのバックアップ」を参照してください。

6. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

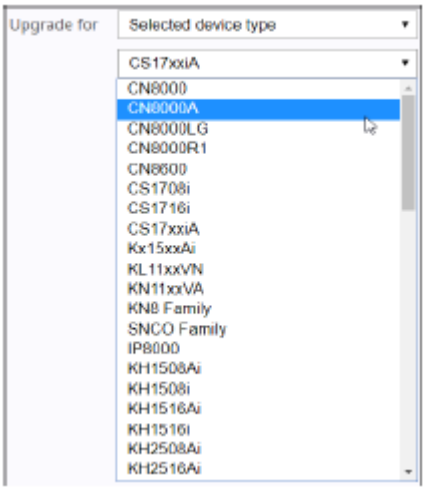
デバイスの最新ファームウェアへの自動アップグレード

リストから「**Auto upgrade with latest device firmware**」(デバイスの最新ファームウェアへの自動アップグレード)の項目を選択すると、指定された時間に、デバイスのファームウェアを自動で最新バージョンへとアップグレードすることができます。



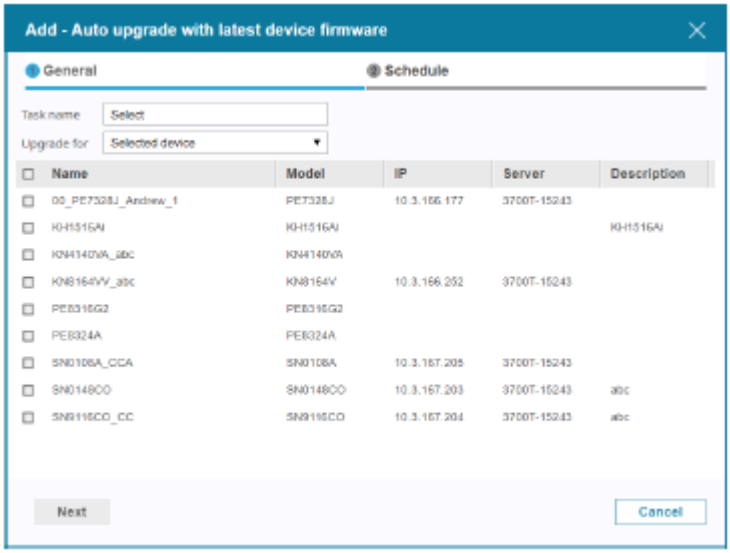
1. タスクに名前を設定してください。
2. 「**Upgrade for**」(アップグレード対象)ドロップダウンメニューを使って、指定されたオプションから自動アップグレードを受信するデバイスを選択してください。選択できるオプションは、「**All devices**」(全てのデバイス)、「**Selected device type**」(選択されたデバイスタイプ)、「**Selected device**」(選択されたデバイス)の 3 種類です。

3. 「All devices」(全てのデバイス)を選択した場合(推奨)、アップグレードは全デバイスが自動的に対象となります。
   「Selected device type」(選択されたデバイスタイプ)を選択した場合は、ドロップダウンメニューを使って、アップグレード対象となるデバイスタイプを選択してください。



「Selected device」(選択されたデバイス)を選択した場合は、アップグレード対象となるデバイスのチェックボックスにチェックを入れてください。一覧に表示されている全てのデバイスが対象となる場合は、列の見出しにあるチェックボックスを使って、一括選択または一括選択解除を行ってください。

注意:	デバイス一覧は、名前、タイプ、IP の各項目で並び替えることができます。



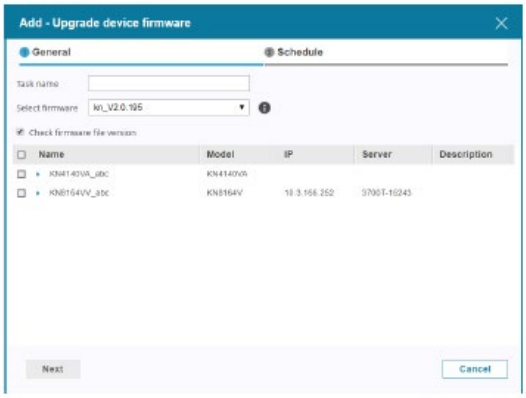
4. 設定が完了したら、「**Next**」(次へ)ボタンをクリックし、「Schedule」(スケジュール)画面でスケジュールの選択を行ってください。

注意:	スケジュールの設定手順については p.263「プライマリーサーバーのデータベースのバックアップ」を参照してください。

5. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

デバイスファームウェアのアップグレード

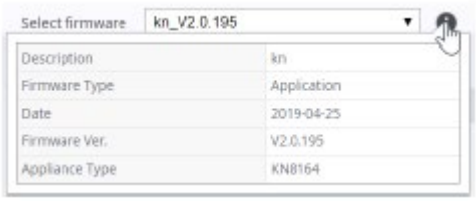
リストから「**Upgrade device firmware**」(デバイスファームウェアのアップグレード)の項目を選択すると、指定された時間に、デバイスのファームウェアをファームウェアレポジトリーからアップグレードすることができます。



1. タスクに名前を設定してください。
2. 「**Select firmware**」(ファームウェアの選択)ドロップダウンメニューから、ファームウェアファイル

を選択してください。ファームウェアファイルは、ファームウェアレポジトリーから読み込みます。

ファームウェアファイルを選択してから情報アイコン( )をクリックすると、ファームウェアに関する情報が表示されます。下図はその例です。



3. ファームウェアファイルを選択すると、ファームウェアアップグレード可能なデバイスが下の一覧に全て表示されます。

4. アップグレード対象となるデバイスのチェックボックスにチェックを入れ(複数選択可)、「**Next**」(次へ)ボタンをクリックしてください。

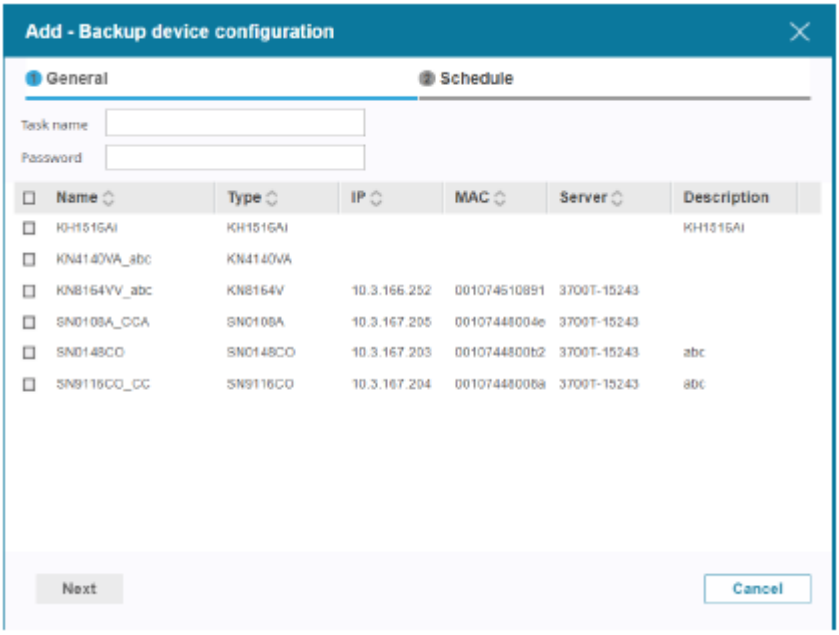
5. 設定が完了したら、「**Next**」(次へ)ボタンをクリックし、「Schedule」(スケジュール)画面でスケジュールの選択を行ってください。

注意:	スケジュールの設定手順については p.263「プライマリーサーバーのデータベースのバックアップ」を参照してください。

6. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

デバイス設定のバックアップ

リストから「**Backup device configuration**」(デバイス設定のバックアップ)の項目を選択すると、下図のような画面が表示されます。



1. タスクの名前を「Task Name」(タスク名)欄に、そしてパスワードを「Password」(パスワード)欄に、それぞれ入力してください。

   注意: 設定したパスワードは控えておき、人目に付かない場所に保管しておいてください。このパスワードはデータベースのリストアの際に必要になります。詳細は、p.174「設定のリストア」を参照してください。

2. デバイス一覧で、バックアップ対象となるデバイスのチェックボックスにチェックを入れて選択してください(複数選択可)。

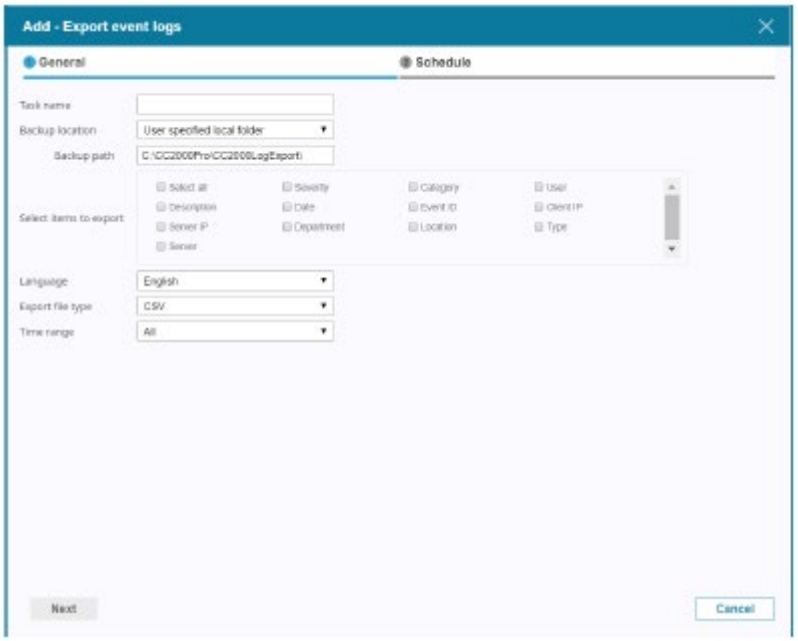
3. 設定が完了したら、「**Next**」(次へ)ボタンをクリックし、「Schedule」(スケジュール)画面でスケジュールの設定を行ってください。

   注意: スケジュールの設定手順については p.263「プライマリーサーバーのデータベースのバックアップ」を参照してください。

4. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

イベントログのエクスポート

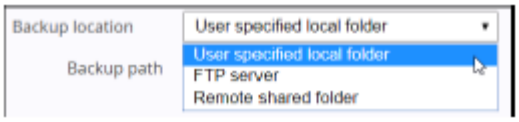
リストから「**Export event logs**」(イベントログのエクスポート)の項目を選択すると、下図のような画面が表示されます。



1. タスクに名前を設定してください。

注意:	イベントログをエクスポートするタスクは、個々のサーバーで独立して実行されます。このため、サーバーの記録を検索するには、特定のファイルで検索を行う必要があります。なお、ファイルは「Task name」(タスク名)欄で設定した名前で識別可能です。

2. バックアップファイルを保存する場所を「**Backup location**」(バックアップ場所)ドロップダウンメニューから選択してください。選択できるオプションは、「**User specified local folder**」(ユーザーが指定するローカルフォルダー)、「**FTP server**」(FTP サーバー)、「**Remote shared folder**」(リモート共有フォルダー)の 3 種類です。



- デフォルトでは、このバックアップファイルは CC2000 のローカル・インストールディレクトリーに保存されます。例:C:¥CC2000Pro¥CC2000LogExport
- 「FTP server」(FTP サーバー)または「Remote shared folder」(リモート共有フォルダー)を選択した場合は、残りの項目も入力してください。

3. 「Select items to export」(エクスポートする項目の選択)の一覧で、エクスポートファイルに追加したい項目にチェックを入れて選択してください(複数選択可)。

注意:	「Select All」(全て選択)の項目にチェックを入れると、全項目を選択します。

4. 「Language」(言語)ドロップダウンメニューを使うと、言語を変更することができます。

5. 「Export file type」(エクスポートファイルの種類)ドロップダウンメニューでは、お使いの環境に適したファイルの種類を選択することができます。暗号化オプション(AES または DES)を選択した場合は、「Password」(パスワード)欄にパスワードを入力してください。

注意:	このパスワードはファイルのインポート時に必要となりますので、忘れないように記録しておいてください。

6. 「Time Range」(時間範囲)ドロップダウンメニューには、次の 3 種類のオプションがあります。
   - **All(全て):** データベースにおける全レコードをエクスポートします。
   - **Since the last time task run(前回のタスク実行以降):** 前回、タスクが実行されてから発生したレコードをエクスポートします。
   - **Select time range(時間範囲を選択):** 特定の期間に発生したレコードをエクスポートします。期間の始点を「From」欄に、また終点を「To」欄に、それぞれ入力します。

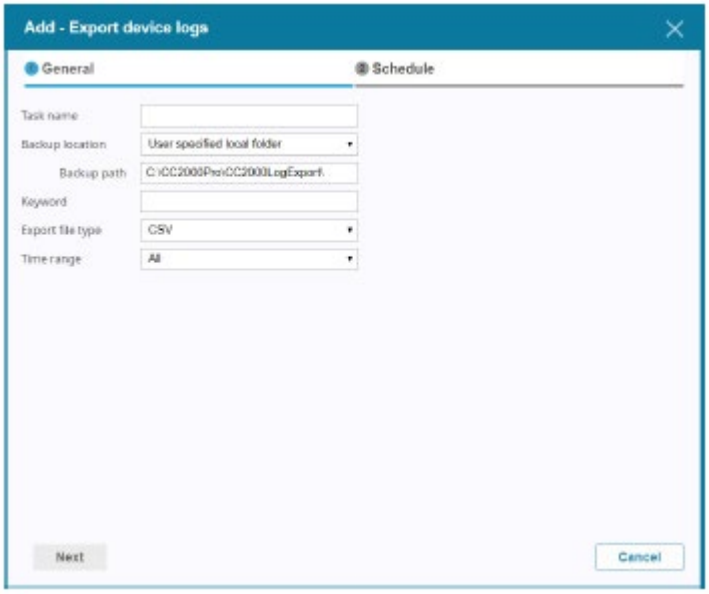
7. 設定が完了したら、「**Next**」(次へ)ボタンをクリックし、「Schedule」(スケジュール)画面でスケジュールの選択を行ってください。

注意:	スケジュールの設定手順については p.263「プライマリーサーバーのデータベースのバックアップ」を参照してください。

8. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

デバイスログのエクスポート

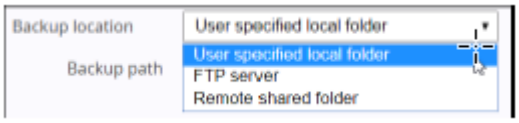
CC2000 は、ATEN 製 IP-KVM スイッチのログサーバーとして機能し、これらのデバイスで発生したシステムイベントをデータベースに記録します。リストから「**Export Device Logs**」(デバイスログのエクスポート)の項目を選択すると、データベースの内容をファイルに書き込みます。このタスクを選択すると、下図のような画面が表示されます。



1. タスクに適当な名前を設定してください。例えば、全デバイスのログをエクスポートする場合は、「All-device-logs」という名前を、また、CN8000 のログを週単位でエクスポートする場合は「cn8000-weekly-device-log」という名前をそれぞれ設定すると、後の作業に便利です。

注意:	イベントログをエクスポートするタスクは、それぞれのサーバーで実行され、エクスポートされたデータも各サーバーに保存されます。エクスポート対象となるレコードを検索する場合は、個々のサーバーにアクセスする必要があります。

2. バックアップファイルを保存する場所を「**Backup location**」(バックアップ場所)ドロップダウンメニューから選択してください。選択できるオプションは、「**User specified local folder**」(ユーザーが指定するローカルフォルダー)、「**FTP server**」(FTP サーバー)、「**Remote shared folder**」(リモート共有フォルダー)の 3 種類です。



- デフォルトでは、このバックアップファイルは CC2000 のローカル・インストールディレクトリーに保存されます。例:C:¥CC2000Pro¥DataBaseBackup
- 「FTP server」(FTP サーバー)または「Remote shared folder」(リモート共有フォルダー)を選択した場合は、残りの項目も入力してください。

3. 「Keyword」(キーワード)の項目をフィルターとして使うことでログファイルの範囲を絞り込むことができます。例えば、お使いの CN8000 の名前にはすべて「CN8K」という文字列が含まれて

おり、これらの CN8000 に関する情報だけが含まれたファイルをエクスポートしたい場合は、「Keyword」(キーワード)欄に「CN8K」と入力することでデータの絞り込みが可能です。

4. 「Export file type」(エクスポートファイルの種類)ドロップダウンメニューでは、お使いの環境に適したファイルの種類を選択することができます。暗号化オプション(AES または DES)を選択した場合は、「Password」(パスワード)欄にパスワードを入力してください。

注意:	このパスワードはファイルのインポート時に必要となりますので、忘れないように記録しておいてください。

5. 「Time Range」(時間範囲)ドロップダウンメニューには、次の 3 種類のオプションがあります。
   - **All(すべて):** データベースにおける全レコードをエクスポートします。
   - **Since the last time task run(前回のタスク実行以降):** 前回、タスクが実行されてから発生したレコードをエクスポートします。
   - **Include(含む):** 特定の期間に発生したレコードをエクスポートします。期間の始点を「From」欄に、終点を「To」欄に、それぞれ入力します。
   - **Exclude(除く):** 特定の期間に発生したイベントを除いたレコードをエクスポートします。期間の始点を「From」欄に、終点を「To」欄に、それぞれ入力します。

6. 設定が完了したら、「**Next**」(次へ)ボタンをクリックし、「Schedule」(スケジュール)画面でスケジュールの選択を行ってください。

注意:	スケジュールの設定手順については p.263「プライマリーサーバーのデータベースのバックアップ」を参照してください。

7. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

8. この画面における設定が完了したら、パネル左下にある「**Next**」(次へ)ボタンをクリックして、「Schedule」(スケジュール)画面に遷移してください。

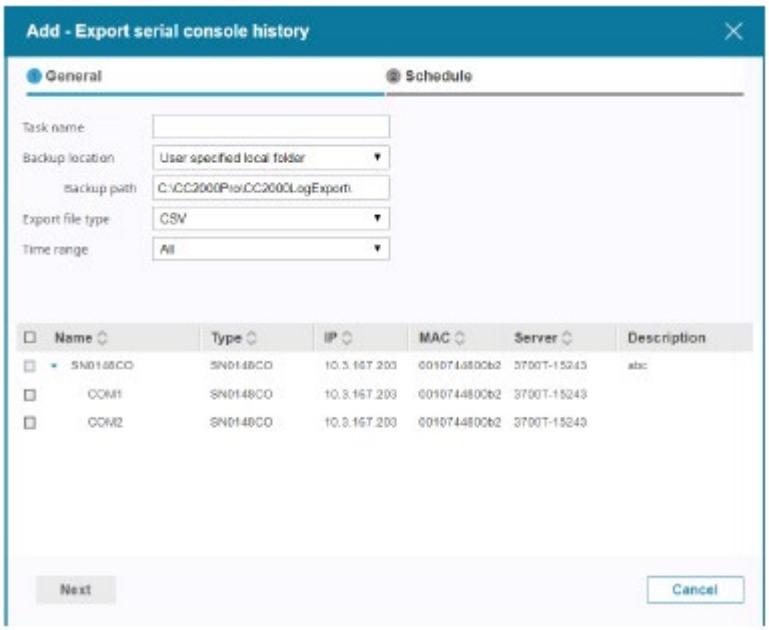
9. 「Schedule」(スケジュール)画面で、スケジュールの設定を行ってください。

注意:	「Schedule」(スケジュール)画面は、プライマリーサーバーのデータベースバックアップの画面と同様であるため、必要であれば p.263 を参照してください。

10. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

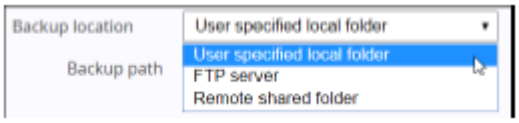
シリアルコンソールの履歴のエクスポート

CC2000 では、全ユーザーセッションで発生したイベントを記録しています(p.288 参照)。リストから「**Export serial console history**」(シリアルコンソールの履歴のエクスポート)の項目を選択すると、各デバイスにおけるシリアルコンソール履歴を保存し、ファイルにエクスポートすることができます。このタスクを選択すると、下図のような画面が表示されます。



1. タスクに名前を設定してください。

2. バックアップファイルを保存する場所を「**Backup location**」(バックアップ場所)ドロップダウンメニューから選択してください。選択できるオプションは、「**User specified local folder**」(ユーザーが指定するローカルフォルダー)、「**FTP server**」(FTP サーバー)、「**Remote shared folder**」(リモート共有フォルダー)の 3 種類です。



   - ◆ デフォルトでは、このバックアップファイルは CC2000 のローカル・インストールディレクトリーに保存されます。例:C:¥CC2000Pro¥DataBaseBackup
   - ◆ 「FTP server」(FTP サーバー)または「Remote shared folder」(リモート共有フォルダー)を選択した場合は、残りの項目も入力してください。

3. 「Export file type」(エクスポートファイルの種類)ドロップダウンメニューでは、お使いの環境に適したファイルの種類を選択することができます。暗号化オプション(AES または DES)を選択した場合は、「Password」(パスワード)欄にパスワードを入力してください。

注意:	このパスワードはファイルのインポート時に必要となりますので、忘れないように記録しておいてください。

4. 「Time Range」(時間範囲)ドロップダウンメニューには、次の 3 種類のオプションがあります。
   - **All(すべて):** データベースにおける全レコードをエクスポートします。
   - **Include(含む):** 特定の期間に発生したレコードをエクスポートします。期間の始点を「From」欄に、また終点を「To」欄に、それぞれ入力します。
   - **Exclude(除く):** 特定の期間に発生したイベントを除いたレコードをエクスポートします。期間の始点を「From」欄に、また終点を「To」欄に、それぞれ入力します。

5. デバイス一覧で、対象となるデバイスのチェックボックスにチェックを入れてください。一覧に表示されている全てのデバイスが対象となる場合は、列の見出しにあるチェックボックスを使って、一括選択または一括選択解除を行ってください。

注意:	選択されたポートのシリアルコンソールの履歴だけをエクスポートしたい場合は、そのデバイスのチェックボックスにチェックを入れるのではなく、対象となるデバイスの名前の前にある矢印をクリックし、ポートリストを展開してポートを選択してください。

6. 設定が完了したら、「**Next**」(次へ)ボタンをクリックし、「Schedule」(スケジュール)画面でスケジュールの選択を行ってください。

注意:	スケジュールの設定手順については p.263「プライマリーサーバーのデータベースのバックアップ」を参照してください。

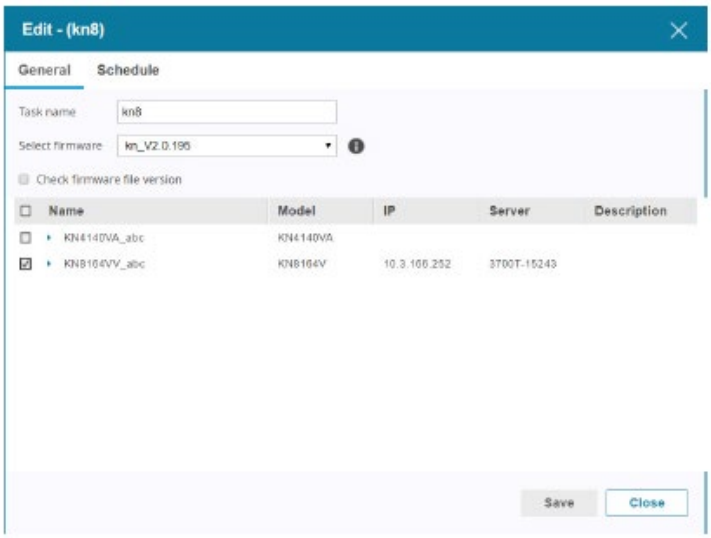
7. 「**Add**」(追加)をクリックして、タスクの設定を完了してください。

タスクの編集

タスクの編集には、タスクの全般設定の変更と、スケジュール設定の変更の 2 種類があります。

タスクのスケジュールを変更するには、以下の手順で操作してください。

1. タスクマネージャー一覧で、編集対象となるタスクのチェックボックスにチェックを入れてください。
2. 「Edit」(編集)をクリックしてください。そうすると、下図のような編集ダイアログボックスが表示されます。



各種タスクと変更可能なパラメーターに関する詳細は、p.262「追加」を参照してください。

パラメーターを編集したら、「Save」(保存)をクリックして、操作を完了してください。

すぐに実行

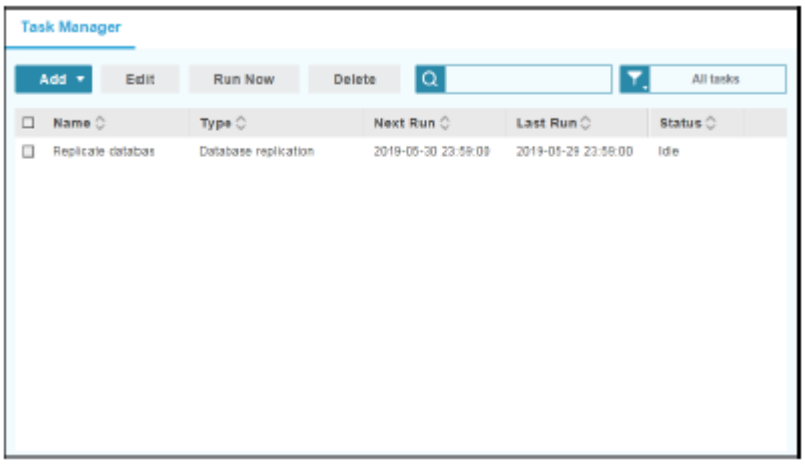
「Run Now」(すぐに実行)を使うと、タスクを即座に実行します。対象となるタスクのチェックボックスにチェックを入れたら、「Run Now」(すぐに実行)をクリックしてください。

タスクの削除

今後タスクを実行しない場合は、該当するタスクの名前の隣にあるチェックボックスにチェックを入れて、「Delete」(削除)ボタンをクリックしてください。

データベースの複製

セカンダリーサーバーの「Task Manager」(タスクマネージャー)画面は、プライマリーサーバーのもの(p.261 参照)と基本的には同じですが、リストにはデフォルトで「Replicate Database」(データベースの複製)という項目が表示されます。これは、接続しているプライマリーサーバーのデータベースを複製する機能です。



「Replicate Database」(データベースの複製)の項目にチェックを入れて「Edit」(編集)をクリックすると、「Edit」(編集)画面が表示されます。操作手順は、タスクの編集と同様の方法です。必要であれば、p.277 をご参照ください。

注意:

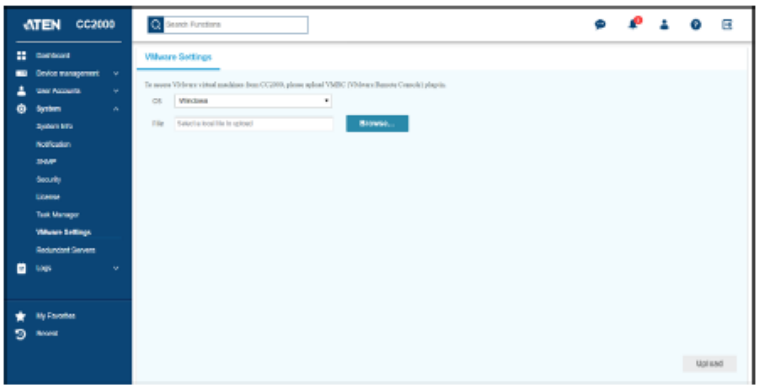
1. CC2000 サーバーはそれぞれ、そのサーバーで設定されたアカウント、ログ、デバイス、アクセス権限を独自で管理するデータベースを保持しています。複製を作成すると、これら全ての情報をプライマリーのデータベースに取り込み、他の CC2000 システムでも利用することができるようになります。
2. プライマリーサーバーでセカンダリーサーバーが登録されると、そのデータベースは自動的に複製されます。
3. デフォルトでは、毎日 0:00 にデータベースを自動的に複製するように設定されています。この画面を使うと、データベースの複製のスケジュールを変更することができますが、このタスクの実行時間の間隔が短いと、システムパフォーマンスに影響を与えるおそれがあります。また、実行時間の間隔が長すぎると、データベースの内容が同期されない期間も長くなります。

スケジュールを設定したら、「**Save**」(保存)ボタンをクリックしてください。

VMware の設定

VMRC プラグイン

VMware Remote Console（VMRC）プラグインを使うと、ブラウザーから VMware 仮想マシンにアクセスすることが可能になります。お使いの CC2000 統合管理システムに VMware 仮想マシンを追加している場合は、このプラグインをインストールする必要があります。「VMware Settings Panel Menu」（VMware 設定パネルメニュー）のエントリーを選択すると、下図のような画面が表示されます。



プラグインをインストールするには、次の手順に従って操作を行ってください。

1. VMware のウェブサイトからプラグインをダウンロードしてください。
2. 「OS」ドロップダウンメニューから、OS を選択してください。
3. 「**参照**」ボタンをクリックして表示されたファイルの選択ダイアログから、手順 1 でダウンロードしたファイルを選択してください。
4. 「**Upload**」（アップロード）ボタンをクリックしてください。

Xterm のインストール

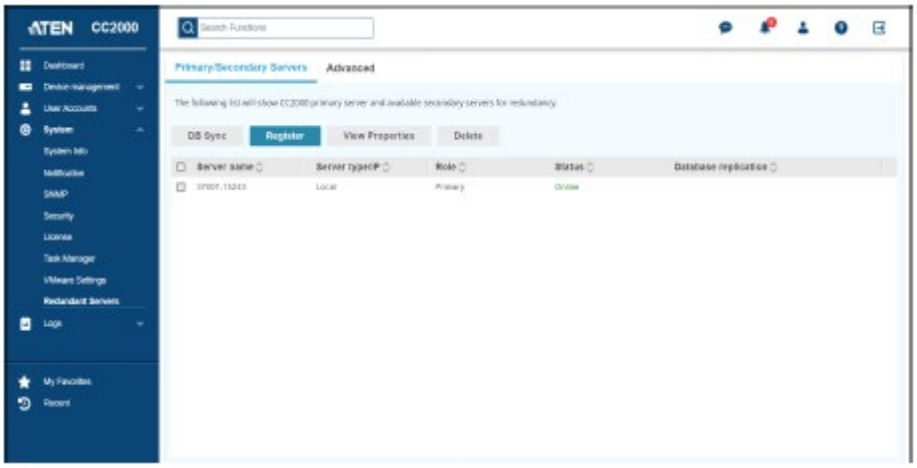
アクセスしているポートの OS で、Ubuntu 18.04_x64、CentOS 7.5_x64、Debian 9.5_x64 のいずれかが稼働している場合は、VMRC が正しく動作するよう、Xterm をインストールする必要があります。

ターミナルで、次のコマンドを実行してください。

```
sudo apt-get update
sudo apt-get install xterm
```

冗長サーバー

「**Redundant Servers**」(冗長サーバー)メニューは、下図のように「**Primary/Secondary Servers**」(プライマリー/セカンダリーサーバー)と「**Advanced**」(詳細)といった 2 つのタブメニューから構成されています。



プライマリー/セカンダリーサーバー

相互表示パネルには、CC2000 サーバーと、これらに関する基本情報が一覧表示されます。「Status」(状態)欄にグリーンの文字で「Online」(オンライン)と書かれている場合、そのサーバーはアクセス可能な状態であることを表します。また、赤色の文字で「Offline」(オフライン)と書かれている場合、そのサーバーはアクセスできない状態であることを表します。

サーバー一覧の項目の意味は下表の通りです。

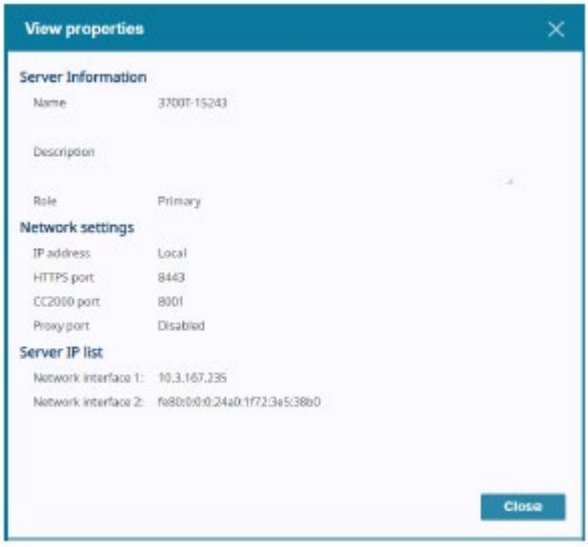
項目	説明
Server Name (サーバー名)	サーバーに設定された名前です。
Server Type /IP (サーバータイプ/IP)	「Local」(ローカル)は現在、ログインしている CC2000 を表します。 システムにおける他の CC2000 は、「Remote」(リモート)という文言と、CC2000 の IP アドレスが表示されます。

(表は次のページに続きます)

項目	説明
Role （ロール）	CC2000 統合管理システムにおける 2 つの主なロールは、プライマリーとセカンダリーです。これに加えて、代替プライマリーという 3 番目のロールがあります。これは、万が一、（ネットワークの問題などの理由で）プライマリーがシステムから切断された場合に、セカンダリーの 1 つが一時的にプライマリーのロールを引き継ぐものです。プライマリーがオンライン状態に戻ると、代替プライマリーは、セカンダリーの状態に戻ります。 **注意：** 1. 代替プライマリーとして機能する CC2000 は、CC2000 統合管理システムによって自動的に選択されます。選択は、CC2000 の登録シーケンスに基づいて決定されます（プライマリーで最初に登録されたセカンダリーの CC2000 が代替プライマリーになります）。 2. 代替プライマリーは、統合管理を提供するためにプライマリーのロールを実行します。このため、デバイスの追加や削除には使用できません。そして、セカンダリーサーバーを登録することもできません。また、セカンダリーサーバーは代替プライマリーに対してデータベースを複製することができません。
Status （状態）	CC2000 がオンラインであるか、オフラインであるかが表示されます。

プロパティーの参照

各サーバーのプロパティーを参照するには、参照したいサーバーのチェックボックスにチェックを入れ、「**View Properties**」（プロパティーの参照）をクリックしてください。



登録

「**Register**」(登録)ボタンは、より大きな CC2000 ネットワークに CC2000 サーバーをセカンダリーサーバーとして統合する際に使用します。「**Register**」(登録)をクリックすると、下図のような画面に遷移します。

プライマリーサーバーの詳細を入力したら、「**Register**」(登録)をクリックしてください。

登録が完了すると、自動的にログアウトします。再ログインすると、お使いのサーバーはプライマリーサーバーでセカンダリーサーバーとして表示されるようになります。

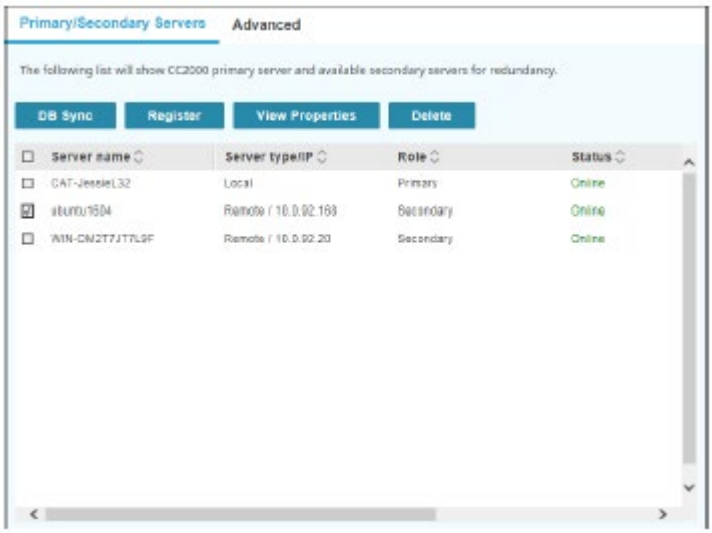
注意:

1. 「Administrator username」(管理者のユーザーネーム)と「Administrator password」(管理者のパスワード)の各欄には、お使いのシステムにおいて有効なスーパーアドミニストレーターもしくはシステムアドミニストレーターのユーザーネームとパスワードを入力するようにしてください。
2. 登録が完了すると、過去に独立していた CC2000(プライマリーまたはセカン

ダリー）における元のデータの大半は失われます。このサーバーは、セカンダリーサーバーとして、登録に使われたプライマリーサーバーの大半のデータを取得します。なお、新規に登録されたセカンダリーサーバーに接続されたデバイスは、再登録する必要があります。

3. システムにおける他の CC2000 にログインしているユーザーは、CC2000 をすぐに確認することができません。CC2000 を確認するには、「System Management」（システム管理）画面を離れて再アクセスするなど、画面の再読込が必要です。
4. 変更内容を確認するために、ブラウザーのキャッシュ消去が必要になる場合があります。

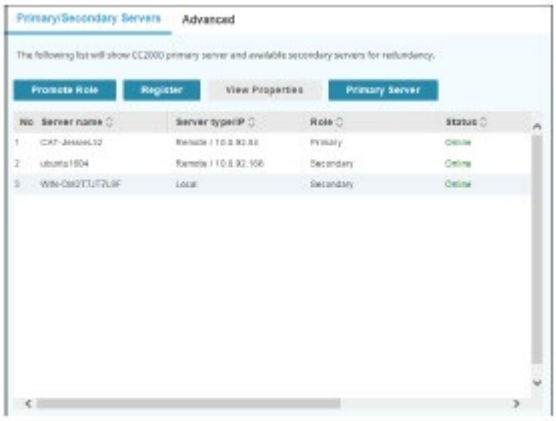
プライマリーサーバー一覧



セカンダリーサーバーを削除するには、対象となるサーバーのチェックボックスにチェックを入れ（複数選択可）、「**Delete**」（削除）をクリックしてください。

また、プライマリーサーバーのデータベースをセカンダリーサーバーと同期するには、対象となるセカンダリーサーバーのチェックボックスにチェックを入れ（複数選択可）、「**DB Sync**」（DB 同期）をクリックしてください。

セカンダリーサーバー一覧



■昇格

「Promote」(昇格)ボタンは、セカンダリーの CC2000 をプライマリーに変換する際に使用します。このボタンをクリックすると、プライマリーがセカンダリーになって、オンライン状態にある他のセカンダリーが自動的に新規プライマリーを認識するよう、自動的に変更されます。

注意:

1. 最新の変更内容を確認するには、別画面に一度遷移した後で、元の画面に戻ってくるなどの方法で、画面を再読込してください。
2. ロール昇格を行う場合には、システムにおける全ての CC2000 サーバーがオンライン状態であることが推奨されます。昇格の際に、オフライン状態のセカンダリーサーバーがあると、プライマリー設定の手順を再度実行する必要が出てきます(詳細は次の「プライマリーサーバー」セクションを参照)。また、ロール昇格の際に、古いプライマリーがオフライン状態であると、オンライン状態に戻った際に、新規プライマリーとして登録する必要があります。詳細は p.282「登録」を参照してください。

■プライマリーサーバー

この機能は、次の状況で使用されます。

- プライマリーの IP アドレスが変更される場合
- プライマリーの CC ポートまたは HTTPS ポートの変更時に、セカンダリーがオフラインになっている場合
- 別の CC2000 がセカンダリーからプライマリーに昇格した際に、セカンダリーがオフラインになっている場合

これらの条件が発生した場合、プライマリー・セカンダリー接続を維持するのに、登録の手順を踏

む必要はありません。管理者は、この機能を使って情報を更新することができます。

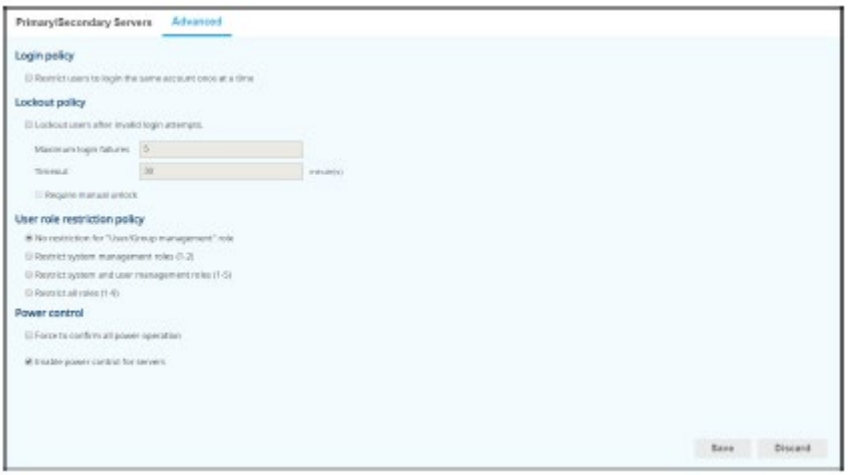
接続を維持するには、(プライマリーサーバーの)IP アドレスやポートの新規設定を入力して、「Save」(保存)をクリックしてください。

注意:

1. IP アドレスの変更が(CC2000 のサービスレベルではなく)OS レベルで行われた場合、CC2000 システムではその変更が認識されません。このため、プライマリーは、セカンダリーにこの変更を自動的に適用することができません。このような場合には、全てのセカンダリーに対して手入力で変更を行う必要があります。
2. オフライン状態の CC2000 セカンダリーは、変更されたときに自動的に通知されません。このため、セカンダリーがオンライン状態に戻った際に、この変更を適用する必要があります。
3. この手順は、セカンダリーがプライマリーと通信していないときに発生したデータベースの変更を、通常のデータベースにマージすることができます。これは、元は同じシステムの一部であったものの、一時的に相互通信ができなくなってしまった CC2000 に対して、有用な機能です。この機能を使うと、プライマリーサーバーとの通信が途絶えた間、更新されたデータベースの情報が消えてしまうことを防ぐことができます。

詳細

「**Advanced**」(詳細)タブは、「Login policy」(ログインポリシー)、「Lockout policy」(ロックアウトポリシー)、「User role restriction policy」(ユーザーロールの制限ポリシー)、「Power control」(電源制御)といった 4 つの設定カテゴリーから構成されています。



ログインポリシー

ユーザーによる同時多重ログインを許可しない場合は、「Restrict users to login in the same account once a a time」(ユーザーによる多重ログインを制限する)の項目にチェックを入れてください。

注意: ログインポリシーの設定は、デフォルトでユーザーによる同時多重ログインを許可しています。

ロックアウトポリシー

◆ ログイン試行に失敗した回数が指定された上限を超えた場合に、ユーザーをロックアウトするには、「Lockout users after invalid login attempts」(不正なログイン試行後にユーザーをロックアウトする)の項目にチェックを入れてください。この項目は、デフォルトで有効になっています。

注意: この項目にチェックが入っていない場合、ユーザーは無制限で何度でもログインを試行することが可能になってしまいます。セキュリティー上の理由から、この機能を有効にし、ロックアウトポリシーを設定することを推奨します。

◆ ユーザーがロックアウトされる前に、ログインに連続で試行できる回数を、「Maximum login failures」(最大ログイン試行回数)欄に入力してください。ここには最低でも 1 を設定してくださ

い。デフォルトでは 5 に設定されています。

◆ ログイン連続試行回数を超えてしまった場合、ロックアウトされたユーザーが次のログインを行うのに待機しなければならない時間（分）を、「Timeout」（タイムアウト）欄に入力してください。ここには最低でも 1 を設定してください。デフォルトでは 30 に設定されています。

◆ 「Require manual unlock」（ロックは手動で解除する）の項目にチェックを入れると、ユーザーは自身のアカウントがロックされた後、管理者に依頼して手動でロックを解除してもらわない限り、再ログインできなくなります。詳細は p.203「ユーザーのブロック解除」を参照してください。デフォルトでは、無効（チェックボックスが選択されていない状態）に設定されています。

ユーザーロールの制限ポリシー

この設定カテゴリーを使うと、管理者は、ロール制限がないユーザーアカウントや、プリセットされた次の 3 種類のロール制限ポリシーのいずれかが適用されたユーザーアカウントを作成することができます。オプションは次の通りです。

◆ ロール制限なし
◆ システム管理ロール（1～2）を制限
◆ システムおよびユーザー管理ロール（1～5）を制限
◆ 全てのロール（1～9）を制限

注意： ロール 1～9 に関する詳細は、p.205「システムのユーザータイプ」の一覧を参照してください。

電源制御

この設定カテゴリーを使うと、管理者はユーザーに対してデバイスやサーバー電源制御に関するパラメーターを設定することができます。

「Force to confirm all power operation」（全ての電源制御を強制的に確認する）の項目にチェックを入れると、アウトレットの設定にかかわらず、ユーザーは全ての接続デバイスにおいて電源制御の確認を行う必要があります。

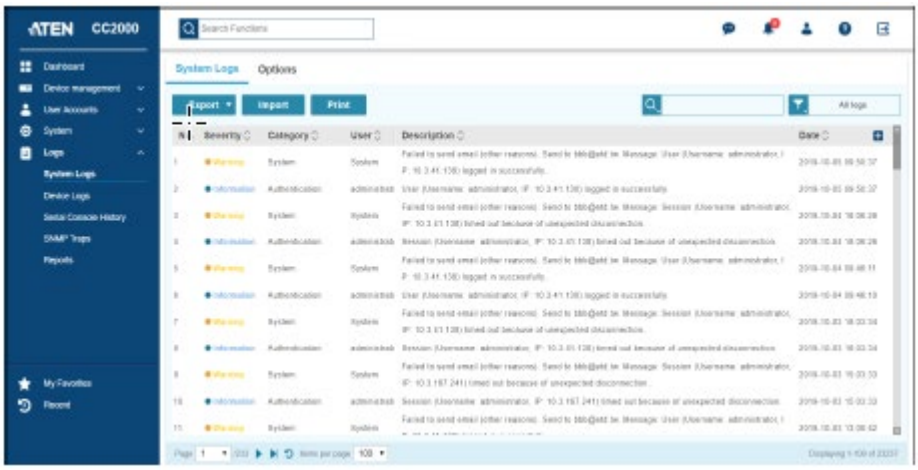
また、「Enable power control for servers」（サーバーの電源制御を有効にする）の項目にチェックを入れると、電源制御に対応したサードパーティーのサーバーが電源制御の実行を許可されていることを意味します。許可されていない場合は、関連する電源制御機能がメニューから削除されます。

第 8 章
ログ

概要

CC2000 では、管理システムで発生した全てのアクションに関する詳細データを保存しています。「Logs」(ログ)画面では、指定したログファイルのデータの参照やエクスポート、また、発生イベントのメール通知などを可能にする、強力なフィルターと機能を多数提供しています。

「Logs」(ログ)メニューをクリックすると、CC2000 は下図のような「System Logs」(システムログ)画面を表示します。

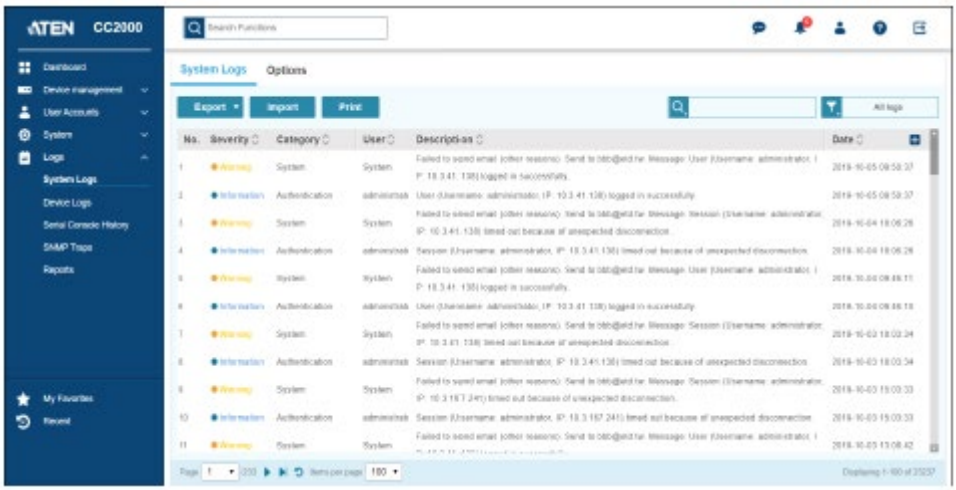


システムログ

「System Logs」(システムログ)メニューは、「System Logs」(システムログ)と「Options」(オプション)といった 2 つのタブメニューから構成されています。

システムログ

「System Logs」(システムログ)タブはデフォルト画面で、下図のような外観です。



◆ デフォルトのレイアウトでは、CC2000 全体で発生した全イベントに関する情報が新しい順に表示されます。

◆ 表の項目名をクリックすると、その項目で並び順を変更することができます。

- 「Date」(日付)列の見出しをクリックすると、日付の昇順または降順で表示します。
- 「Description」(説明)列の見出しをクリックすると、説明をアルファベットの昇順または降順で表示します。

注意: 通常、ブランク画面はそのカテゴリーで記録されたイベントがないことを表します。

エクスポート

「Export」(エクスポート)ボタンは、現在の画面におけるログ、全てのログ、カスタムログといった 3 つのオプションを提供しています。

■現在の画面におけるログ

「Logs in current page」(現在の画面におけるログ)を選択すると、現在のシステムログ画面に表示されている記録済みログイベントレコードの全件を自動的にダウンロードします。

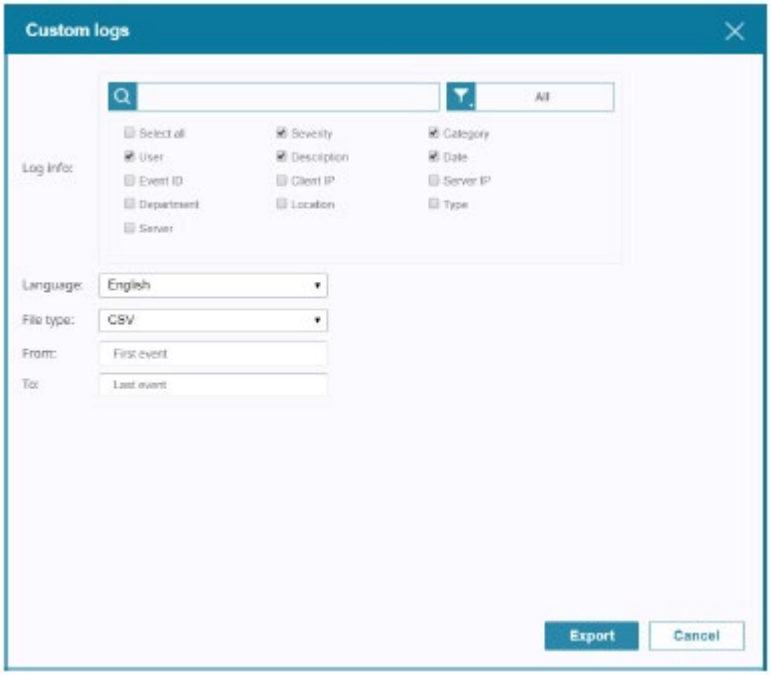
注意:	現在の画面でログとしてダウンロードされるレコードの件数は、「Items per page」(1 画面あたりの件数)ドロップダウンメニューによって決まります。

■全てのログ

「All logs」(全てのログ)を選択すると、記録されたログイベントのレコード全件をシステムログから自動的にダウンロードします。

■カスタムログ

「Custom Logs」(カスタムログ)画面は、特定の記録済みイベントログのレコードをダウンロードする場合にのみ使用します。「Custom Logs」(カスタムログ)をクリックすると、下図のような画面が表示されます。



特定の記録済みログイベントをファイルに保存するには、次の手順に従って操作を行ってください。

1. エクスポートされたファイルに追加したいログ情報アイテムを、「**Log info**」(ログ情報)一覧から選択してください。

   注意: デフォルトでは、「Severity」(重要度)、「Category」(カテゴリー)、「User」(ユーザー)、「Description」(説明)、「Date」(日付)の各項目が有効になっています。

2. 「**Language**」(言語)ドロップダウンメニューには、システムで利用可能な言語が列挙されています。デフォルトでは、英語に設定されています。ファイルをエクスポートする際に使用する言語を選択し、確認してください。

3. 「**File type**」(ファイルの種類)ドロップダウンメニューでは、お使いの環境に適したファイルの種類を選択することができます。暗号化オプション(AES でファイルを暗号化、または DES でファイルを暗号化)を選択した場合は、「Password」(パスワード)欄にパスワードを入力してください。

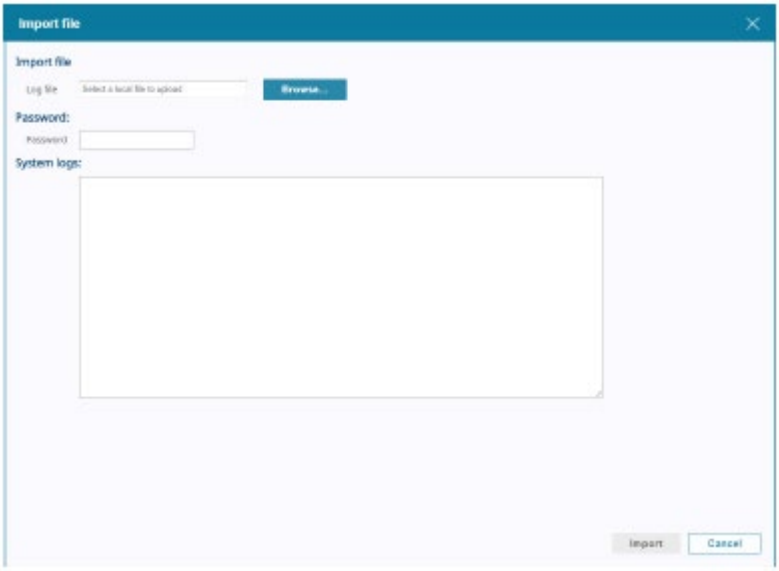
   注意: このパスワードはファイルのインポート時に必要となりますので、忘れないように記録しておいてください。

4. 特定の期間に記録されたログイベントのレコードをエクスポートする場合は、期間のパラメーターを設定してください。「**From**」欄には期間の始点となる日時を、また「**To**」欄には期間の終点となる日時をそれぞれ設定してください。

5. 項目の設定が完了したら、パネル右下にある「**Export**」(エクスポート)ボタンをクリックしてください。

インポート

「Import」(インポート)画面は、過去に保存されたログを参照するためにファイルを開くのに使用されます。画面は下図のような外観です。



保存済みのログファイルをインポートするには、次の手順に従って操作を行ってください。

1. 「Log file」(ログファイル)欄にファイルのフルパスを入力するか、「**参照...**」ボタンをクリックして、このファイルをダイアログから選択してください。

2. ファイルが暗号化されている場合には、ファイルへのエクスポート時に設定されたパスワードと同じ文字列を「Password」(パスワード)欄に入力してください。

3. パネル右下にある「Import」(インポート)ボタンをクリックしてください。

ファイルがインポートされると、そのファイルの内容が「System logs」(システムログ)のメイン画面に表示されます。

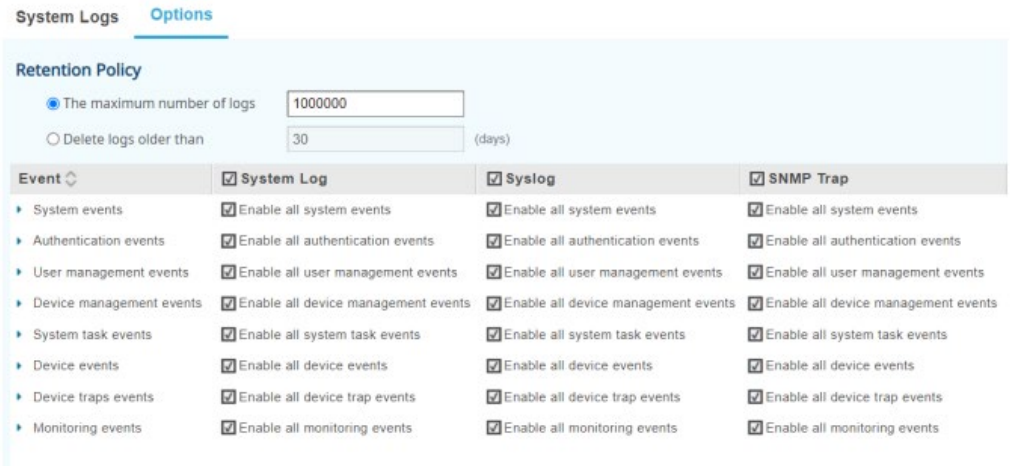
印刷

ログ一覧を印刷するには、「Print」(印刷)を選択してください。

注意:	印刷対象となるのは、一覧に表示されているログ(全件またはフィルタリングされたデータ)だけです。

オプション

「Options」(オプション)画面では、システムログファイルの保存ポリシーに関する設定を行うことができます。「Options」(オプション)を選択すると、下図のような画面が表示されます。



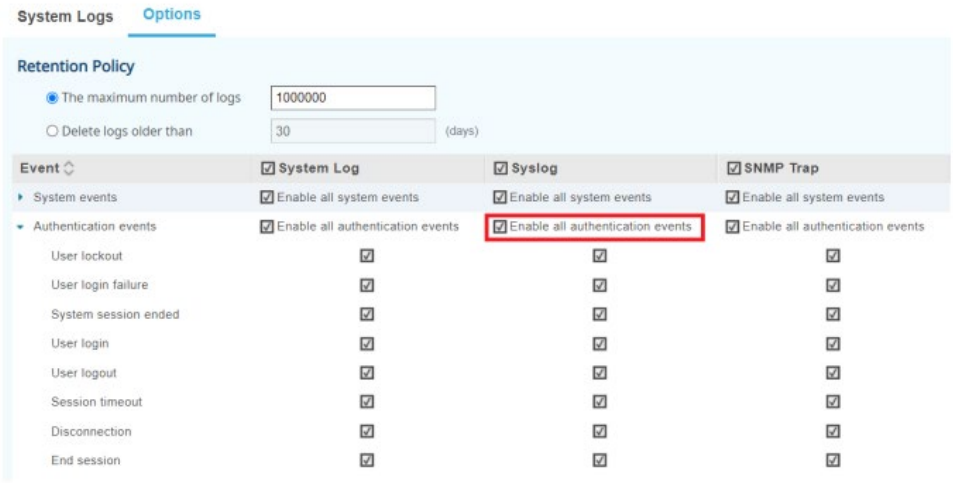
システムログファイルの保存ポリシーを調整するには、次の手順に従って操作を行ってください。

1. 保存ポリシーに対して、ラジオボタンでオプションをクリックして選択してください。オプションには、「The maximum number of logs」(ログの最大件数)と「Delete logs older than」(次の日付以前のログは削除)の 2 つがあります。
   - ◆ ログデータベースをログレコード単位でメンテナンスする場合は、「The maximum number of logs」(ログの最大件数)を選択してください。
   - ◆ ログデータベースを時間的な条件でメンテナンスする場合は、「Delete logs older than」(次の日付以前のログは削除)を選択してください。

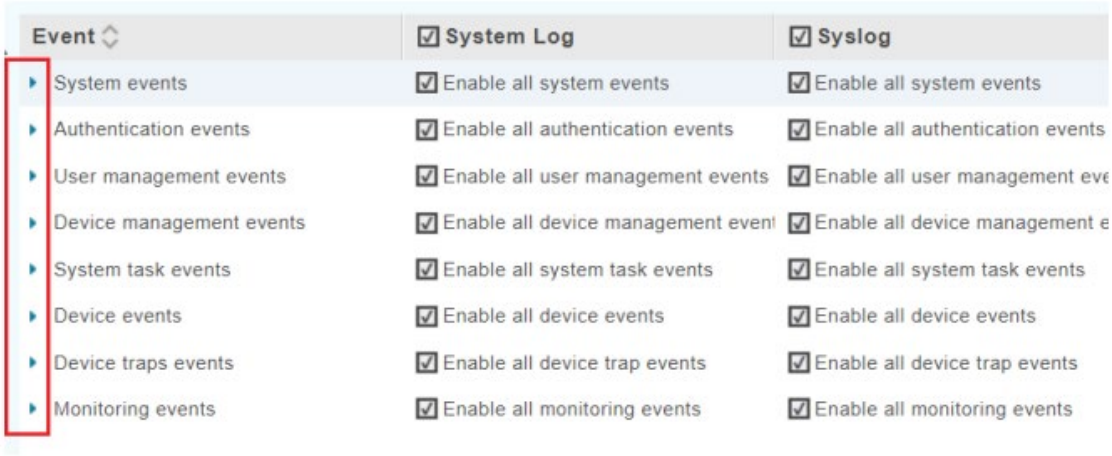
   注意:
   - ◆ 日数やレコードの件数が上限に達した場合、イベントは先入れ先出しの原則に基づいて削除されます。
   - ◆ ログ件数の最大有効範囲は、10,000～1,000,000 件です。
   - ◆ 日数の有効範囲は、30～1096 日間です。

2. イベントは、追跡したいイベントを選択したり、これらのイベントをシステムログ、Syslog、SNMP Trap、あるいは、これら全てのどこに保存するかを選択したりすることができます。有効にしたいイベントの前にあるチェックボックスにチェックを入れて選択してください。
   - ◆ イベントカテゴリーは 7 種類あり、各カテゴリーにはイベント別の一覧が含まれています。カテゴリーに対して全てのイベントを記録するには、「Enable all ... events」(全ての～イベントを有効にする)の前にあるチェックボックスにチェックを入れてください。下図はその例

です。



◆ カテゴリーのイベントで選択されたレコードだけを保存するには、対象となるカテゴリー名の前にある矢印マークをクリックして、配下にあるイベントを表示してからチェックボックスを操作して選択してください。



3. 項目の設定が完了したら、パネル右下にある「Save」(保存)ボタンをクリックしてください。

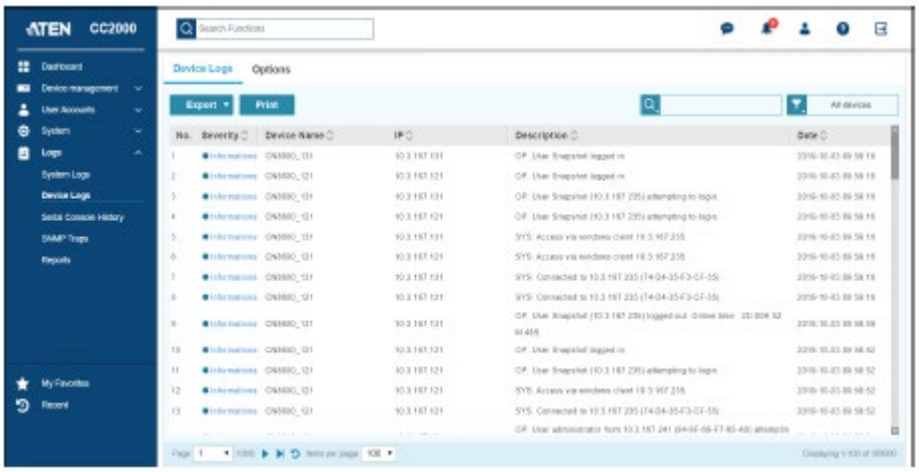
デバイスログ

CC2000 は、ATEN の全 Over IP 対応製品のログサーバーとして機能し、これらのデバイスで発生したシステムイベントをデータベースに記録します。

「Device Logs」(デバイスログ)メニューは、「Device Logs」(デバイスログ)と「Options」(オプション)といった 2 つのタブメニューから構成されています。

デバイスログ

「Device Logs」(デバイスログ)画面はデフォルト画面で、下図のような外観です。



- デフォルトのレイアウトでは、CC2000 全体における全デバイスのイベントログ全件が、新しい順に表示されます。
- 表の項目名をクリックすると、その項目で並び順を変更することができます。
  - 「Date」(日付)列の見出しをクリックすると、日付の昇順または降順で表示します。
  - 「Description」(説明)列の見出しをクリックすると、説明をアルファベットの昇順または降順で表示します。

注意: 通常、ブランク画面はそのカテゴリーで記録されたイベントがないことを表します。

エクスポート

「Export」(エクスポート)タブは、「Logs in current page」(現在の画面におけるログ)と「All logs」(全てのログ)といった 2 つのパネルサブメニューから構成されています。

■現在の画面におけるログ

「Logs in current page」(現在の画面におけるログ)を選択すると、現在、デバイスログ画面に表示されている記録済みログイベントレコードの全件を自動的にダウンロードします。

注意:	現在の画面でログとしてダウンロードされるレコードの件数は、「Items per page」(1 画面あたりの件数)ドロップダウンメニューによって決まります。

■全てのログ

「All logs」(全てのログ)を選択すると、記録されたログイベントのレコード全件をデバイスログから自動的にダウンロードします。

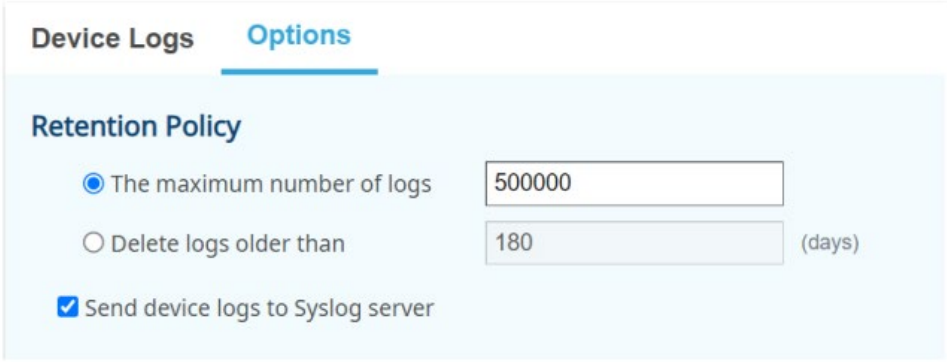
■印刷

デバイスログ一覧を印刷するには、「Print」(印刷)を選択してください。

注意:	印刷対象となるのは、一覧に表示されているログ(全件またはフィルタリングされたデータ)だけです。

オプション

「Options」(オプション)画面では、デバイスログファイルの保存ポリシーを設定することができます。「Options」(オプション)を選択すると、下図のような画面が表示されます。



デバイスログファイルの保存ポリシーを調整するには、次の手順に従って操作を行ってください。

1. 保存ポリシーに対して、ラジオボタンでオプションをクリックして選択してください。オプションには、「**The maximum number of logs**」(ログの最大件数)と「**Delete logs older than**」(次の日付以前のログは削除)の 2 つがあります。
   - ◆ ログデータベースをログレコード単位でメンテナンスする場合は、「**The maximum number of logs**」(ログの最大件数)を選択してください。
   - ◆ ログデータベースを時間的な条件でメンテナンスする場合は、「**Delete logs older than**」(次の日付以前のログは削除)を選択してください。

   注意:
   - ◆ 日数やレコードの件数が上限に達した場合、イベントは先入れ先出しの原則に基づいて削除されます。
   - ◆ ログ件数の最大有効範囲は、10,000～1,000,000 件です。
   - ◆ 日数の有効範囲は、30～1096 日間です。

2. Syslog 機能を有効にする場合は、「**Send device logs to Syslog server**」(デバイスログを Syslog サーバーに送信する)の項目にチェックを入れてください。この項目にチェックを入れると、CC2000 はデバイスログを Syslog サーバーへと送信します。

   注意: CC2000 は、デフォルトで Syslog へのデバイスログ送信が行われるように設定されています。

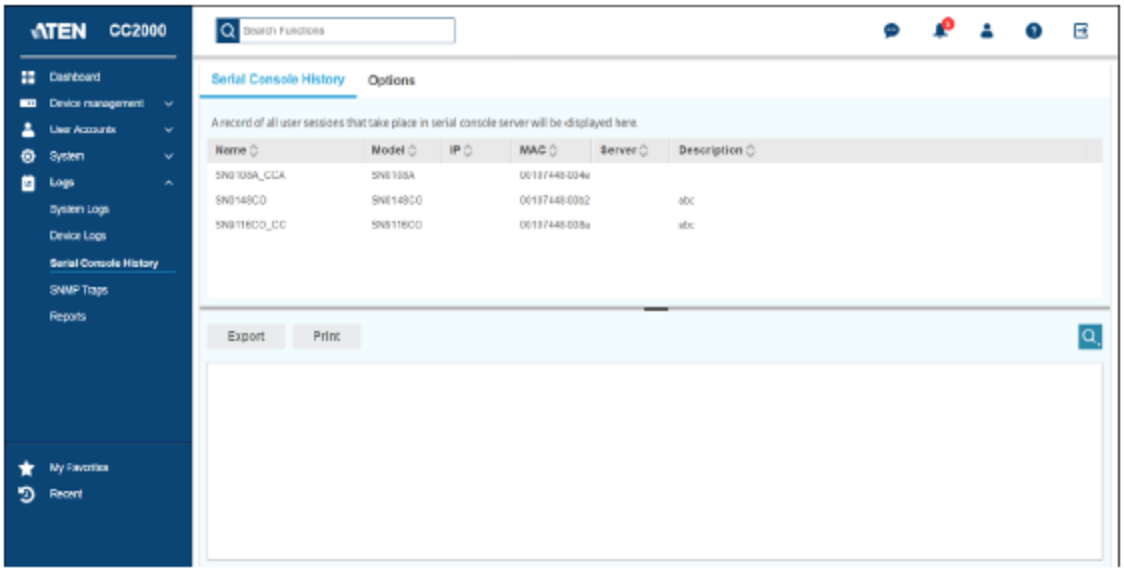
3. 項目の設定が完了したら、パネル右下にある「**Save**」(保存)ボタンをクリックしてください。

シリアルコンソールの履歴

CC2000 では、接続されたシリアルコンソールサーバーで発生した全ユーザーセッションの大量のレコードを保持します。「Serial Console History」(シリアルコンソールの履歴)メニューは、「Serial Console History」(シリアルコンソールの履歴)と「Options」(オプション)といった 2 つのパネルメニューから構成されています。

シリアルコンソールの履歴

「Serial Console History」(シリアルコンソールの履歴)画面は、デフォルト画面で、下図のような外観です。

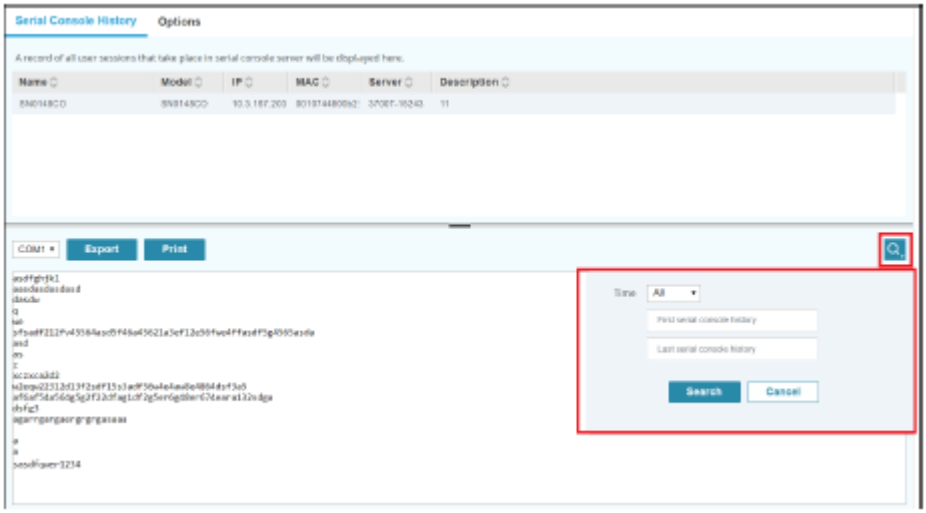


◆ 表の項目名をクリックすると、その項目で並び順を変更することができます。

- 「Name」(名前)列の見出しをクリックすると、名前をアルファベットの昇順または降順で表示します。
- 「Description」(説明)列の見出しをクリックすると、説明をアルファベットの昇順または降順で表示します。

シリアルコンソールの履歴のレコードを検索する場合は、以下の手順で操作してください。

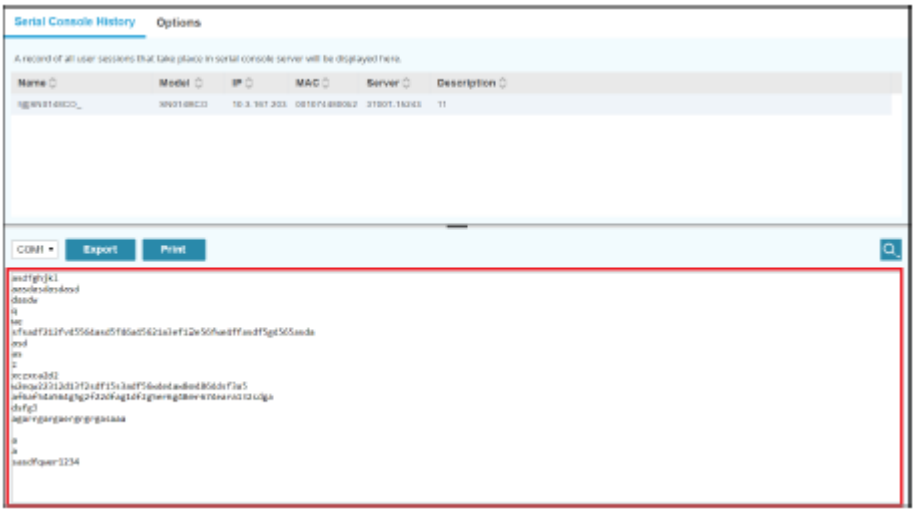
1. 「Model」(型番)をクリックして選択したら、検索アイコンをクリックしてください。そうすると、下図のような画面が表示されます。



2. 「Time」(時間)ドロップダウンメニューから、オプションを選択してください。オプションには、「All」(全て)、「Include」(含む)、「Exclude」(除く)の 3 種類があります。特定の期間に記録されたレコードのみを検索する場合は、ドロップダウンメニューから「Include」(含む)または「Exclude」(除く)を選択し、「First serial console history」(最初のシリアルコンソールの履歴)欄と「Last serial console history」(最後のシリアルコンソールの履歴)欄を使って期間のパラメーターを設定してください。
   - ◆ 「All」(全て)を選択すると、データベースに保存されているレコードを全件検索します。
   - ◆ 「Include」(含む)を選択すると、指定された期間に保存されたレコードを全件検索します。
   - ◆ 「Exclude」(除く)を選択すると、指定された期間に保存されたレコード以外を全件検索します。

3. パラメーターの設定が完了したら、パネル右下にある「Search」(検索)ボタンをクリックしてください。

検索結果は、メインパネルにあるシリアルコンソールの履歴一覧に、日付の降順で表示されます。



エクスポート

シリアルコンソールの履歴をエクスポートするには、次の手順に従って操作を行ってください。

1. 「Serial Console History」(シリアルコンソールの履歴)一覧から「Model」(型番)を選択してください。
2. ドロップダウンメニューからデバイスの USB ポート番号を選択してください。
3. 「**Export**」(エクスポート)をクリックして、シリアルコンソールの履歴をエクスポートしてください。

印刷

シリアルコンソールの履歴を印刷するには、次の手順に従って操作を行ってください。

1. 「Serial Console History」(シリアルコンソールの履歴)一覧から「Model」(型番)を選択してください。
2. ドロップダウンメニューからデバイスの USB ポート番号を選択してください。
3. 「**Print**」(印刷)をクリックして、印刷を実行してください。

オプション

「Options」(オプション)画面では、シリアルコンソールの履歴の保存ポリシーを設定することができます。「Options」(オプション)を選択すると、下図のような画面が表示されます。

シリアルコンソールの履歴の保存ポリシーを調整するには、次の手順に従って操作を行ってください。

1. 保存ポリシーに対して、ラジオボタンでオプションをクリックして選択してください。オプションには、「**The maximum number of records**」(レコードの最大件数)と「**Delete records older than**」(次の日付以前のレコードは削除)の 2 つがあります。
   - ◆ シリアルコンソールの履歴データベースをレコード単位でメンテナンスする場合は、「**The maximum number of records**」(レコードの最大件数)を選択してください。
   - ◆ シリアルコンソールの履歴データベースを時間的な条件でメンテナンスする場合は、「**Delete records older than**」(次の日付以前のレコードは削除)を選択してください。

   注意:
   - ◆ 日数やレコードの件数が上限に達した場合、イベントは先入れ先出しの原則に基づいて削除されます。
   - ◆ レコード件数の最大有効範囲は、10,000～1,000,000 件です。
   - ◆ 日数の有効範囲は、30～1096 日間です。

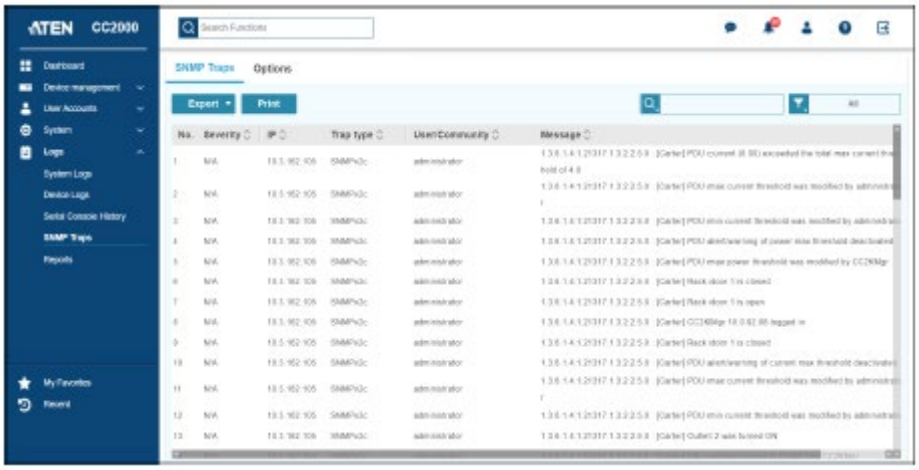
2. 項目の設定が完了したら、画面右下にある「**Save**」(保存)ボタンをクリックしてください。

SNMP トラップ

「SNMP Traps」(SNMP トラップ)メニューは、「SNMP Traps」(SNMP トラップ)と「Options」(オプション)といった 2 つのタブメニューから構成されています。ここでは、SNMP トラップのイベントを検索したり、検索や表示機能に対する詳細オプションを設定したりすることができます。

SNMP トラップ

「SNMP Traps」(SNMP トラップ)画面はデフォルト画面で、下図のような外観です。



- デフォルトのレイアウトでは、CC2000 全体における SNMP トラップ全件が、新しい順に表示されます。
- 表の項目名をクリックすると、その項目で並び順を変更することができます。
  - 「Date」(日付)列の見出しをクリックすると、日付の昇順または降順で表示します。
  - 「Severity」(重要度)列の見出しをクリックすると、重要度の昇順または降順で表示します。

エクスポート

「Export」(エクスポート)タブは、「SNMP traps in current page」(現在の画面における SNMP トラップ)と「All SNMP traps」(全ての SNMP トラップ)といった 2 つのオプションから構成されています。

■現在の画面における SNMP トラップ

「**SNMP traps in current page**」(現在の画面における SNMP トラップ)を選択すると、現在、SNMP トラップ画面に表示されている SNMP トラップレコードの全件を自動的にダウンロードします。

注意：	現在の画面でログとしてダウンロードされるトラップの件数は、「Items per page」(1 画面あたりの件数)ドロップダウンメニューによって決まります。

■全ての SNMP トラップ

「**All SNMP traps**」(全ての SNMP トラップ)を選択すると、SNMP トラップのレコード全件を自動的にダウンロードします。

印刷

SNMP トラップ一覧を印刷するには、「**Print**」(印刷)を選択してください。

注意：	印刷対象となるのは、一覧に表示されているトラップ(全件またはフィルタリングされたデータ)だけです。

オプション

「Options」(オプション)画面では、SNMP トラップの保存ポリシーを管理することができます。「Options」(オプション)を選択すると、下図のような画面が表示されます。

SNMP トラップの保存ポリシーを調整するには、次の手順に従って操作を行ってください。

1. 保存ポリシーに対して、ラジオボタンでオプションをクリックして選択してください。オプションに

は、「The maximum number of SNMP traps」（SNMP トラップの最大件数）と「Delete SNMP traps older than」（次の日付以前の SNMP トラップは削除）の 2 つがあります。

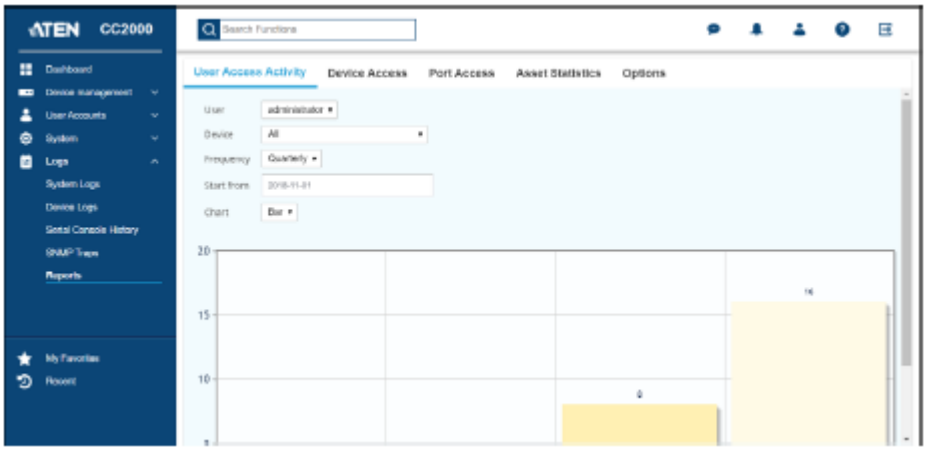
- ◆ SNMP トラップのデータベースをレコード単位でメンテナンスする場合は、「The maximum number of SNMP traps」（SNMP トラップの最大件数）を選択してください。
- ◆ ログデータベースを時間的な条件でメンテナンスする場合は、「Delete SNMP traps older than」（次の日付以前の SNMP トラップは削除）を選択してください。

注意：
- ◆ 日数やレコードの件数が上限に達した場合、イベントは先入れ先出しの原則に基づいて削除されます。
- ◆ レコード件数の最大有効範囲は、10,000～1,000,000 件です。
- ◆ 日数の有効範囲は、30～1096 日間です。

2. 項目の設定が完了したら、パネル右下にある「Save」（保存）ボタンをクリックしてください。

レポート

「Reports」(レポート)タブは、「User Access Activity」(ユーザーアクセスのアクティビティー)、「Device Access」(デバイスアクセス)、「Port Access」(ポートアクセス)、「Asset Statistics」(資産統計)、「Options」(オプション)といった 5 つのタブメニューから構成されています。ここでは、CC2000 システムにおけるユーザーやデバイスのアクセス関連の統計を参照したり、レポートの表示方法を設定したりすることができます。



ユーザーアクセスのアクティビティー

「User Access Activity」(ユーザーアクセスのアクティビティー)画面では、デバイスやポートに対するアクセスに関する統計をユーザーごとに表示します。この画面はデフォルト画面で、下図のような外観です。

パラメーターに従って円グラフや棒グラフ、またはその両方を作成するには、メインパネルにある項目を入力してください。

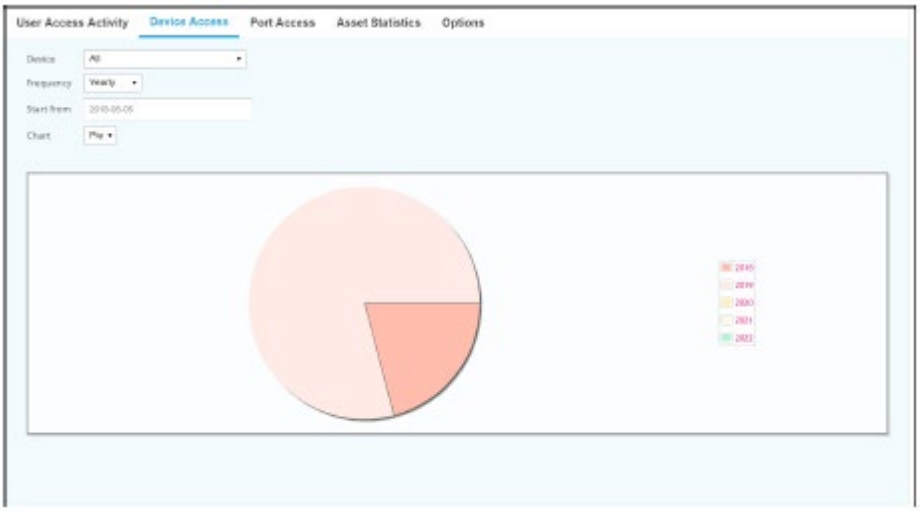
各項目の詳細は下表の通りです。

項目	説明
User (ユーザー)	アクセス統計の表示対象となるユーザーを、ドロップダウンメニューで確認して選択してください。
Device (デバイス)	統計の表示対象となる個々のポートやデバイス、または、それらすべてを選択してください。ここでは、選択した「Frequency」(頻度)に基づいて、ユーザーがデバイスにアクセスした回数をグラフで表示します。 デバイスにアクセスした回数(日・週・月・四半期・年ごと)は、色分けされたグラフで表され、それが全体に占める割合も表示されます。
Frequency (頻度)	グラフ分けする期間を選択してください。グラフは、ここで設定した期間内にデバイスがアクセスした回数を、指定された時間ごとに表示します。 ◆ Daily(日次):「Start From」(開始日)に入力した日から7日間の間、デバイスが 1 日に何回アクセスされたのかを表示します。 ◆ Weekly(週次):「Start From」(開始日)に入力した日から 4 週間の間、デバイスが 1 週間に何回アクセスされたのかを表示します。「2013-W42」は、2013 年の第 42 週を表します。 ◆ Monthly(月次):「Start From」(開始日)に入力した日から12ヶ月の間、デバイスが 1 ヶ月に何回アクセスされたのかを表示します。 ◆ Quarterly(四半期):「Start From」(開始日)に入力した日から 1 年(4 四半期)の間に、デバイスが四半期ごとに何回アクセスされたのかを表示します。 ◆ Yearly(年次):「Start From」(開始日)に入力した日から 5 年の間に、毎年、デバイスが何回アクセスされたのかを表示します。 **注意:**デバイスにアクセスしていない場合、データは表示されません。
Start From (開始日)	カレンダーをクリックして、グラフに反映させたい期間の開始日を選択してください。
Chart (グラフ)	情報を反映させるグラフの種類を選択してください。 ◆ Pie(円グラフ):選択した期間で区切った円グラフを表示します。 ◆ Bar(棒グラフ):選択した期間で区切った個々の棒グラフを表示します。 ◆ All(すべて):円グラフと棒グラフの両方を表示します。

デバイスアクセス

「Device Access」（デバイスアクセス）画面は、デバイスアクセスに関する統計を提供します。

パラメーターに従って円グラフや棒グラフ、またはその両方を作成するには、メインパネルにある項目を入力してください。「**Chart**」（グラフ）で「**Pie**」（円グラフ）が選択されると、「Device Access」（デバイスアクセス）画面は下図のように表示されます。



各項目の詳細は下表の通りです。

項目	説明
Device （デバイス）	統計を表示する全デバイス、上位 10 ポート、あるいは特定のデバイスを選択してください。ここでは、選択した「Frequency」（頻度）に基づいて、デバイスがアクセスされた回数をグラフで表示します。 ◆ Top 10 port（上位 10 ポート）：上位 10 台のデバイス統計を表示します。 デバイスがアクセスされた回数（日・週・月・四半期・年ごと）は、色分けされたグラフで表され、それが全体に占める割合も表示されます。

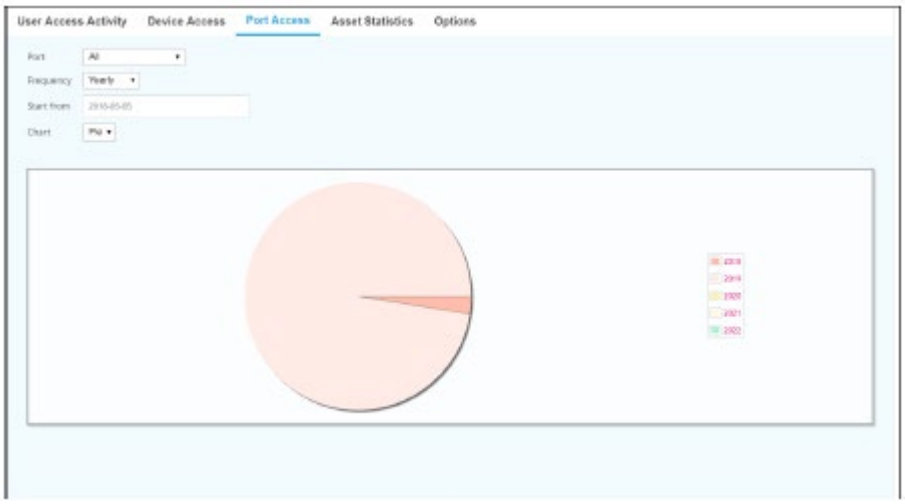
（表は次のページに続きます）

項目	説明
Frequency （頻度）	グラフ分けする期間を選択してください。グラフは、ここで設定した期間内にデバイスがアクセスした回数を、指定された時間ごとに表示します。 ◆ Daily（日次）:「Start From」（開始日）に入力した日から7日間の間、デバイスが 1 日に何回アクセスされたのかを表示します。 ◆ Weekly（週次）:「Start From」（開始日）に入力した日から 4 週間の間、デバイスが 1 週間に何回アクセスされたのかを表示します。「2013-W42」は、2013 年の第 42 週を表します。 ◆ Monthly（月次）:「Start From」（開始日）に入力した日から12ヶ月の間、デバイスが 1 ヶ月に何回アクセスされたのかを表示します。 ◆ Quarterly（四半期）:「Start From」（開始日）に入力した日から 1 年（4 四半期）の間に、デバイスが四半期ごとに何回アクセスされたのかを表示します。 ◆ Yearly（年次）:「Start From」（開始日）に入力した日から 5 年の間に、毎年、デバイスが何回アクセスされたのかを表示します。 **注意:** デバイスがアクセスされていない場合、データは表示されません。
Start From （開始日）	カレンダーをクリックして、グラフに反映させたい期間の開始日を選択してください。
Chart （グラフ）	情報を反映させるグラフの種類を選択してください。 ◆ Pie（円グラフ）:選択した期間で区切った円グラフを表示します。 ◆ Bar（棒グラフ）:選択した期間で区切った個々の棒グラフを表示します。 ◆ All（すべて）:円グラフと棒グラフの両方を表示します。

ポートアクセス

「Port Access」（ポートアクセス）画面は、ポートアクセスに関する統計を提供します。

パラメーターに従って円グラフや棒グラフ、またはその両方を作成するには、メインパネルにある項目を入力してください。「Chart」（グラフ）で「Pie」（円グラフ）が選択されると、「Port Access」（ポートアクセス）画面は下図のように表示されます。



項目	説明
Port （ポート）	統計を表示する全ポート、上位 10 ポート、あるいは特定のポートを選択してください。ここでは、選択した「Frequency」（頻度）に基づいて、ポートがアクセスされた回数をグラフで表示します。 ◆ Top 10 port（上位 10 ポート）：上位 10 台のデバイス統計を表示します。 ポートがアクセスされた回数（日・週・月・四半期・年ごと）は、色分けされたグラフで表され、それが全体に占める割合も表示されます。

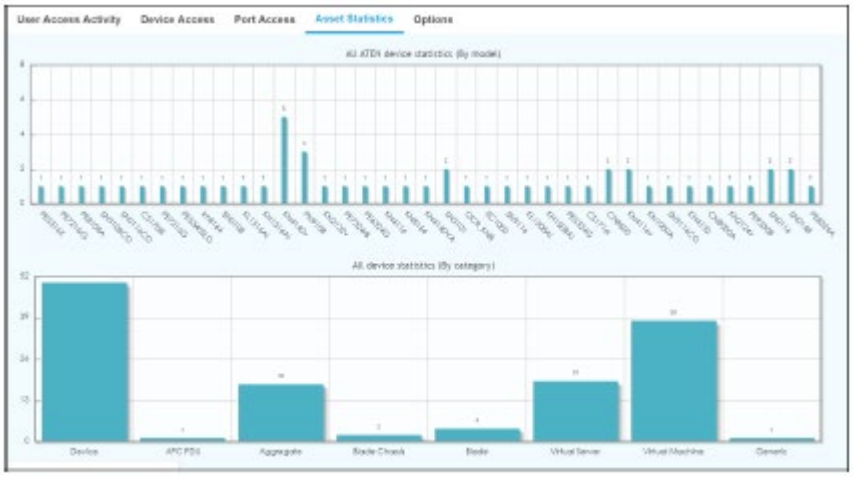
（表は次のページに続きます）

項目	説明
Frequency （頻度）	グラフ分けする期間を選択してください。グラフは、ここで設定した期間内にポートがアクセスされた回数を、指定された時間ごとに表示します。 ◆ Daily（日次）:「Start From」（開始日）に入力した日から7日間の間、ポートが 1 日に何回アクセスされたのかを表示します。 ◆ Weekly（週次）:「Start From」（開始日）に入力した日から 4 週間の間、ポートが 1 週間に何回アクセスされたのかを表示します。「2013-W42」は、2013 年の第 42 週を表します。 ◆ Monthly（月次）:「Start From」（開始日）に入力した日から12ヶ月の間、ポートが 1 ヶ月に何回アクセスされたのかを表示します。 ◆ Quarterly（四半期）:「Start From」（開始日）に入力した日から 1 年（4 四半期）の間に、ポートが四半期ごとに何回アクセスされたのかを表示します。 ◆ Yearly（年次）:「Start From」（開始日）に入力した日から 5 年の間に、毎年、ポートが何回アクセスされたのかを表示します。 **注意:**ポートがアクセスされていない場合、データは表示されません。
Start From （開始日）	カレンダーをクリックして、グラフに反映させたい期間の開始日を選択してください。
Chart （グラフ）	情報を反映させるグラフの種類を選択してください。 ◆ Pie（円グラフ）:選択した期間で区切った円グラフを表示します。 ◆ Bar（棒グラフ）:選択した期間で区切った個々の棒グラフを表示します。 ◆ All（すべて）:円グラフと棒グラフの両方を表示します。

資産統計

「Asset Statistics」（資産統計）画面には、CC2000 システムに登録された全ての資産が表示されます。ここには、「**All ATEN device statistics (By model)**」（全ての ATEN デバイス統計（型番別））と、「**All device statistics (By category)**」（全てのデバイス統計（カテゴリー別））といった 2 つのグラフが表示されます。

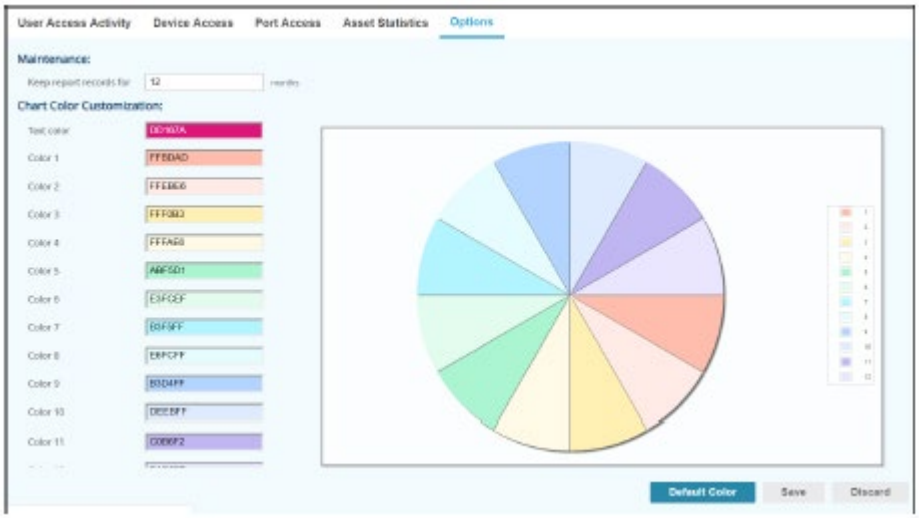
「Port Access」（ポートアクセス）画面の外観は、下図の通りです。



- **All ATEN device statistics (By model)(全ての ATEN デバイス統計(型番別)):**現在、CC2000 システムに関連付けられている ATEN デバイスが型番別に表示されます。
- **All device statistics (By category)(全てのデバイス統計(カテゴリー別)):**現在、CC2000 システムに関連付けられている全デバイスが、カテゴリー別(デバイス(ATEN デバイス)、APC PDU、アグリゲート、ブレードシャーシ、ブレード、仮想サーバー、仮想マシン、ジェネリック)に表示されます。

オプション

「Options」(オプション)画面には、レポート色をカスタマイズしたり、レコードのレポートを保存したりする際に用いられるオプションが提供されています。この画面は下図のような外観です。



レポートをカスタマイズするには、次の手順に従って操作を行ってください。

1. 「**Maintenance**」(メンテナンス)セクションにある「**Keep report records for *n* months**」(*n*か月分のレポートレコードを保持する)欄に、レポートを保持する月数を入力してください。
2. 「**Chart Color Customization**」(グラフ色のカスタマイズ)セクションの項目でグラフの色を調整してください。
3. 項目の設定が完了したら、パネル右下にある「**Save**」(保存)ボタンをクリックしてください。

各項目の詳細は下表の通りです。

項目	説明
Maintenance (メンテナンス)	レポートが削除されるまで、システムがレポートを保存する月数を入力してください。
Chart Color Customization (グラフ色のカスタマイズ)	◆ Text Color(文字色):ボックスをクリックすると、小ウィンドウが表示されます。レポートで使用する文字の色を選択してください。 ◆ Color 1～12(色 1～12):ボックスをクリックすると、小ウィンドウが表示されます。グラフの各キーで使用する色を選択してください。 色を選択すると、右側のテストグラフが選択した内容に変更され、外観を確認することができます。

◆ Default Color(デフォルト色)タブ:このタブをクリックすると、デフォルト設定の色に戻ります。

付録 A
技術情報

使用許諾契約

CC2000 シリーズに関するエンドユーザー・ソフトウェア使用許諾契約

本使用許諾契約は、ユーザーによるライセンス許諾ソフトウェアのインストール日（以下、「発効日」）をもって、ATEN International Co.,Ltd.（所在地：3F, 125, Sec.2, Da-Tung Rd., Si-Jhih, Taipei, Taiwan221, R.O.C.）（以下、「ATEN」）およびユーザーとの間で締結されます。

本契約は、ユーザー（個人または単一の事業体）とATENとの間における法的契約です。本契約書をよくお読みください。本契約の条件に付随するソフトウェア（以下、「ソフトウェア」）のインストールまたは使用により、本契約に同意したものと見なされます。本契約に同意しない場合は、このソフトウェアを使用することができません。ユーザーは次の権利を有します。

第1条　定義：

1.1　「許諾ソフトウェア」とは、ATEN が機械可読なフォーマットでユーザーに提供するオブジェクトコード版のソフトウェアプログラムまたはファイルと定義します。

1.2　「文書」とは、ATEN がユーザーに提供した許諾ソフトウェアに付随するマニュアル、ユーザードキュメント、およびその他の関連資料を意味します。

第2条　使用許諾

2.1　ATEN は、本契約の規約および条件に従って、本許諾対象ソフトウェアをコピーのみでハードウェアにインストールし、組み込まれた本許諾対象ソフトウェアおよび関連文書を使用するための、非独占的かつ譲渡不能で、二次ライセンスがなく、譲渡不能で撤回不能な、限定的なライセンスを、ユーザーに許諾し、ユーザーはここにこれを受諾します。

2.2　上記の許諾は、次のように制限されます。（a）本契約に基づく許諾ソフトウェアは、

ATEN によりユーザーにライセンス許諾され、販売されません。ユーザーは、ATEN がユーザーに提供するいかなる形式においても、許諾ソフトウェアにおける全ての著作権および知的財産権は、ATEN およびそのライセンサーの独占的財産であることを認めます。ユーザーは、許諾ソフトウェアにおける著作権および知的財産権におけるいかなる権利、権原または権益も有さないものとします。ATEN は、明示的に許諾されていない全ての権利を留保します。(b)ユーザーは、許諾ソフトウェアの保存用コピーを 1 部のみ作成することができますが、許諾ソフトウェアをコピー・変更・配布・再販することはできません。(c)ユーザーは、許諾ソフトウェアをレンタル・リース・貸与・抵当に入れることはできません。(d)ユーザーは、許諾ソフトウェアを逆コンパイルまたはリバースエンジニアリングすることはできません。(e)本契約の条件は、ATEN の裁量でユーザーに提供される本許諾対象ソフトウェアの更新に適用されます。(f)許諾ソフトウェアは、原子力施設の設計、建設、操作または保守において使用することを目的として、設計、使用許諾または意図されていません。ATEN およびライセンサーは、そのような使用に対する適応性の明示的または暗示的な保証を放棄します。(g)ATEN またはそのライセンサーの商標・サービスマーク・ロゴまたは商号に対するいかなる権利、権原または権益も、本契約に基づき付与されません。

第3条　限定保証

3.1　ATEN は、本許諾期間ソフトウェアの受領日から 30 日間、いかなる種類の保証もなしに ATEN が提供する機能を満たすことを唯一保証します。ユーザーの所在地における法律により黙示の保証または条件が設定され、その放棄が禁止されている場合、ユーザーは、本限定保証期間中に発見された瑕疵に関してのみ、黙示の保証または条件を有するものとします。それ以外の場合、許諾ソフトウェアは、現状のまま使用許諾されます。上記に別段の記載がない限り、ユーザーは、それを使用するリスクを負うものとします。ATEN は、明示の保証または条件を一切付与しません。ユーザーは、本契約を変更することができないユーザーの地域法に基づき、追加的な消費者権利を有することができます。ユーザーの現地法に基づき許可される範囲内で、ATEN は、商品性、特定目的への適合性および非侵害性に関する暗示的保証を排除します。

3.2　ATEN はここに次を宣言します。(a)本許諾対象ソフトウェアに Java 技術を含めることができます。ユーザーは、互換性要件に基づく Java 技術の修正または使用に関して、www.java.net で別途契約を締結するものとします。(b)本許諾対象ソフトウェアには、オープンソース開発者のグローバル・コミュニティーからのオープンソース・コードも含めることができます。付録 A の許諾ソフトウェアに関して、Java 互換性（JavaMail API、JavaBeans Activation Fremawork(JAF)、AXL-RADIUS、AXL-TACACS、

JavaServiceWrapper(3.2.3)を含むが、これらに限定されない）、およびオープンソース（J2SE JRE、Apache Tomcat、Apache Derby データベース、Apache Struts フレームワーク、JSR80）、またはサードパーティーに属するその他のテクノロジーを含むが、これらに限定されない）で具体化されている文書およびその更新および変更に関して、このようなテクノロジーの特許権者は、ユーザーに通知し、ロイヤルティーの支払いを要求することができます。ユーザーは、ATEN が当該ロイヤルティーの支払に責任を負わないこと、およびユーザーが各特許権保有者と良好な交渉を行い、その請求に対応し、ライセンスを必要に応じて取得することを承認します。いかなる場合にも、上記の侵害またはロイヤルティー請求に対する損失および費用は一切責任を負わないものとします。さらに、明示か黙示かを問わず、本許諾対象ソフトウェアに組み込まれているオープンソースまたは Java テクノロジーに関する侵害に対する、全ての保証を放棄します。

第4条　責任の制限

いかなる場合においても、本ソフトウェアの本ライセンスもしくは使用または本ソフトウェア、本文書のエラーもしくは欠陥に起因するもしくは関連する利益の喪失、間接的、付随的、特別の、懲罰的もしくは派生的損害につき、ユーザーまたはエンドユーザーに一切責任を負いません。いずれかの時間において、ATEN は、本契約からまたはそれにより発生する責任を負うものとし、当該責任が本契約に基づくその本関連会社の過失、違反またはその他によるものであるか否かにかかわらず、いかなる場合にも、ユーザーが被るクレーム、損失または損傷に対するATEN およびその関連会社の全責任は、本契約に基づいて発生するライセンス料を超えないものとします。この責任の制限は、完全かつ排他的であり、AMD またはその関連会社に通知された場合でも適用されるものとします。

第5条　輸出規制

本契約に基づき引き渡される全てのソフトウェア、文書および他の資料は、適用される輸出管理法に準拠し、他国の輸出入規制の対象となる可能性があります。ユーザーは、本法律および規則を厳守することに同意し、ユーザーへの引渡し後に要求される輸出、再輸出または輸入の許諾を取得する責任を負うことを承認します。

第6条　終了

本契約は、発効日に効力を生じるものとし、いかなる理由も伴うことなく、30 日前の書面による通知または ATEN のウェブサイト上での 30 日前の通知により、ATEN が終了するまで有効に存続するものとします。

第7条　雑則

7.1　本契約における第 2 条、第 3 条、第 4 条、第 5 条および第 6 条は、その終了または満了後も存続するものとします。

7.2　本契約の各当事者の権利および義務は、国際物品売買契約に関する国連条約に準拠しないものとし、代わりに、本契約は、中華民国の法律に準拠し、同法に従って解釈されるものとします。

7.3　本契約のいずれかの条項が正当な管轄権を有する裁判所により違法、無効または強制不可と判定された場合、残余の条項は、引き続き全面的に有効に存続します。

7.4　本契約は、ATEN の書面の通知または ATEN のウェブサイトにおける 30 日前の通知により、補足・変更・修正・公表・解除することができます。

7.5　確認救済または差止救済を求める訴訟を含め、コモンローまたは衡平法上の訴訟が本契約の条項を執行または解釈するために提起された場合、勝訴当事者は、当事者が権利を有する他の救済に加えて、合理的な弁護士費用を受け取る権利を有するものとします。

7.6　本契約に基づく不履行または違反に対するいずれかの当事者の権利放棄は、本契約のいずれかの条項または同一もしくは異なる種類のその後の不履行もしくは違反に対する権利放棄を構成しないものとします。

USB ライセンスキー　仕様

CC2000 USB ライセンスキー　仕様		
動作環境	動作温度	0～40℃
	保管温度	-20～60℃
	湿度	0～80% RH、結露なきこと
ケース材料		メタル、プラスチック
重量		14g
サイズ(W×D×H)		84×28×14mm

対応 ATEN 製品

対応製品については、弊社ウェブサイトにおける CC2000 の製品ページをご確認ください。

デバイスの ANMS 設定

「ANMS」画面で、CC2000 によるデバイスの管理を有効にするには、以下の手順で設定を行ってください。

1. デバイスにログインしてください。
2. 必要であればこのデバイスのマニュアルを参考にしながら、操作メニューに従って「ANMS」メニューにアクセスしてください。
3. 「ANMS」メニューで、「enable CC Management」(CC 管理を有効にする)のチェックボックスにチェックを入れ、このデバイスを管理する CC2000 サーバーの IP アドレスとデバイスポート番号(デフォルトでは 8000)を入力してください(p.25 参照)。

VPN

一般的に、VPN (ブイピーエヌ:virtual private network)は、公共ネットワーク(通常はインターネット)を使って複数のサイトをつなぐプライベートネットワークのことを指し、通常、複数の WAN を包含しています。サイト間で安全なネットワーク接続を行うために、独自の VPN 構築をしている企業も多く見られます。しかしながら、VPNの欠点はネットワークを安全に保てる一方で、スループットが遅いという点にあります。

CC2000 がセットアップされた環境下で複数のサイトの接続に VPN を使っている場合、そのシステムの管理に必要となるCC2000 サーバーは、シングルプライマリーサーバーです。(標準的なインターネット環境での CC2000 導入に必要となるプライマリーとセカンダリーの CC2000 サーバーのネットワークではありません。) しかしながら、接続されたデバイスを二重化するには、最低でも 1 台以上の CC2000 のセカンダリーサーバーが必要となります。

CC2000 セカンダリーを追加してセットアップするもうひとつのメリットは、ネットワークのトラフィックを高速化することで、操作や管理がより効率的に行えるという点にあります。

ファイアウォール

複数の CC2000 が別々のファイアウォールの内側にセットアップされている場合、サーバー側に以下のサービスポートを設定し、そのポートをファイアウォール側でも開放する必要があります。

1. CC ポート

注意: 各 CC2000 サーバーの使用ポートはそれぞれ異なるポートを使用することも可能ですが、ファイアウォールで開放されたポートは CC ポートの設定と同じでなければなりません。(例えば、サーバー1 は 8001、サーバー2 は 8005 をそれぞれ使用した場合、サーバー1 のファイアウォールは 8001 に、サーバー2 のファイアウォールは 8005 にそれぞれ設定する必要があります。)

2. CC2000 プライマリーサーバーの HTTPS ポート

3. CC2000 プロキシポート (次のセクションにおける「CC2000 プロキシ機能」を参照)

4. CC2000 セカンダリーサーバーの HTTPS ポート (オプション)

注意:
1. CC2000 クライアントワークステーションは、同じファイアウォールの内側にある CC2000 セカンダリーサーバーに対してウェブブラウザーのセッションを開くことができます。ファイアウォールの外側にある CC2000 へのアクセスは、CC ポートとプロキシポートを使って行いますので、この場合 HTTPS ポートは必要ありません。しかしながら、この場合の欠点は、ファイアウォールの外側にあるデバイスの設定を行うことができないという点にあります。
2. ファイアウォールの外側にある CC2000 クライアントワークステーションから、ファイアウォールの内側にあるセカンダリーサーバーに対してウェブブラウザーのセッションを直接開くようにしたい場合は、このポートを開放することができます。

CC2000 プロキシ機能

CC2000 のプロキシ機能を有効にすると、クライアント PC が（CC2000 サーバーによって管理されている）KVM スイッチに対してビューワー経由で直接通信できない場合に、CC2000 サーバー経由でデータ送信を行うことが可能になります。

「Always use proxy」（常にプロキシを使用する）の項目にチェックを入れると、データは必ず CC2000 サーバー経由で送信されます。

データは CC2000 サーバー経由で送信されるため、バンド幅はアクティブなビューワーの数、すなわち KVM セッションの数に応じて変わります。

ファイアウォールの外側にある CC2000 クライアントワークステーション（クライアント PC）が、ファイアウォールの内側にある CC2000 サーバーで管理されている KVM デバイスやシリアルデバイスにアクセスするためには、CC2000 サーバー上で CC2000 プロキシ機能を有効にし、次の 2 つのポートをファイアウォール上で設定（開放）しなければなりません。

- CC2000 とクライアント PC の間でセキュアなインターネット通信（https://）を行う TCP ポート（デフォルトでは 443）
- ビューワーのイメージおよび Telnet データの通信を行う TCP ポート（デフォルトでは 8002）

注意： プロキシ機能を使用したくない場合は、そのデバイスで必要となる全てのサービスポート(HTTPS、プログラム、バーチャルメディア、Telnet、SSH など)をファイアウォール側で開放する必要があります。

設定項目と入力可能な値

CC2000 における各設定項目の名前、説明および入力可能な値の範囲は下表の通りです。

注意: 特に記載がない限り、項目には対応言語であれば、どの言語でも入力が可能です。

カテゴリー		長さ/範囲	デフォルト
Users (ユーザー)	Login name (ログインネーム)	半角英数字および記号を使用し最大 32 文字で入力してください。最小入力文字数はアカウントポリシーの設定に従います(p.225 参照)。 ただし、以下の文字を使用することはできません。 / ¥ [ ] : ; | = , + * ? < > @ " '	
	Password (パスワード)	半角英数字および記号を使用し 0～16 文字で入力してください。最小入力文字数はアカウントポリシーの設定に従います(p.225 参照)。 入力文字数が 0 の場合、パスワード認証を行いません。	
	Description (説明)	最大 256 バイトで入力してください。	
	Session Timeout (セッションタイムアウト)	1～99 分で入力してください。	3 分
	Unexpected disconnection timeout (予期せぬ切断によるタイムアウト)	2～10 分で入力してください。	2 分
	Email	256 バイトで入力してください。 **From:** 0～64 バイトで入力してください。 **To:** 0～128 バイトで入力してください。 **Subject:** 1～128 バイトで入力してください。	

(表は次のページに続きます)

カテゴリー		長さ/範囲	デフォルト
Groups （グループ）	Name （名前）	2～32 バイトで入力してください。ただし、以下の文字を使用することはできません。 “ ‘	
	Description （説明）	256 バイトで入力してください。	
User Types （ユーザータイプ）	Name （名前）	2～32 バイトで入力してください。ただし、以下の文字を使用することはできません。 “ ‘	
	Description （説明）	256 バイトで入力してください。	
Authentication Server （認証サーバー）	Server name （サーバーネーム）	2～32 バイトで入力してください。ただし、以下の文字を使用することはできません。 “ ‘	
	Description （説明）	256 バイトで入力してください。	
	Browser Method （参照方法）	ユーザーネーム、パスワードともに制限はありません。 **注意：**極端に長い文字列を設定すると、CC2000 のパフォーマンスに影響を与える場合があります。	

（表は次のページに続きます）

カテゴリー		長さ/範囲	デフォルト
CC2000 Authentication (CC2000 認証)	Username Minimum (最小ユーザーネーム文字数)	半角英数字および記号を使用し最大 32 文字で入力してください。最小入力文字数はアカウントポリシーの設定に従います (p.225 参照)。 ただし、以下の文字を使用することはできません。 / ¥ [ ] : ; | = , + * ? < > @ " '	6
	Password Minimum (最小パスワード文字数)	半角英数字および記号を使用し 0～32 文字で入力してください。最小入力文字数はアカウントポリシーの設定に従います (p.225 参照)。入力文字数が 0 の場合、パスワード認証は不要になります。	6
	Password Expires (パスワード有効期間)	日数に上限はありません。	
Devices (デバイス)	Name (名前)	0～32 バイトで入力してください。	
	Description (説明)	最大 256 バイトで入力してください。	
	Contact name (連絡先)	バイト数に上限はありません。	
	Telephone (電話番号)	バイト数に上限はありません。	
	Email notification (Email 通知)	バイト数に上限はありません。	
Aggregate Devices (アグリゲートデバイス)	Name (名前)	1～32 バイトで入力してください。	
	Description (説明)	最大 256 バイトで入力してください。	

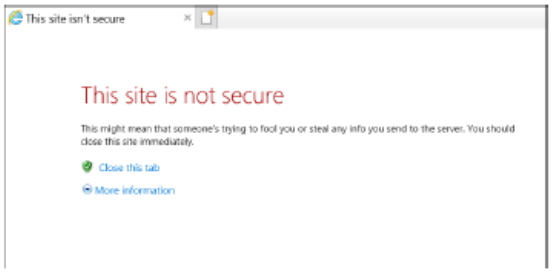
(表は次のページに続きます)

カテゴリー		長さ/範囲	デフォルト
Departments / Locations (部署/場所)	Name (名前) Description (説明)	1～32 バイトで入力してください。 最大 256 バイトで入力してください。	
Tasks (タスク)	All Tasknames (全てのタスク名)	バイト数に上限はありません。	
	Primary Database Backup Password (プライマリーデータベースのバックアップ時に使用するパスワード)	0～32 バイトで入力してください。 入力文字数が 0 の場合、パスワード認証を行いません。	
	Export Device Log Pattern (デバイスログをエクスポートするパターン)	バイト数に上限はありません。	
System Log Options (システムログオプション)	By Period(ピリオドごと)	30～1096 日で入力してください。	
	By Record (レコードごと)	10,000～1,000,000 件で入力してください。	
	Records per page (ページあたりの最大ログ表示数)	100、300、500から選択してください。	
Log Notification Settings (ログ通知設定)	Subject(件数)	1～128 バイトで入力してください。	
	Mail from (メール差出人)	最大 64 バイトで入力してください。	
	Send to (メール宛先)	最大 128 バイトで入力してください。	

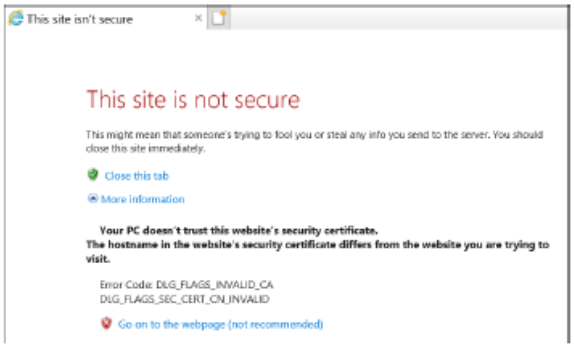
信頼された証明書

概要

ウェブブラウザーからデバイスにログインしようとすると、下図のようなセキュリティー警告ダイアログが表示され、デバイスの証明書が信頼できないものであるため、アクセスを続行するかを問われるメッセージが表示されます。



この証明書は信頼できるものですが、証明書の名前が Microsoft の信頼された認証局のリストに存在しないため、このようなダイアログが表示されます。



この警告メッセージは無視しても構いません。「More Information」(さらに表示する)をクリックし、「Yes」ボタンを押して、処理を続行してください。

注意:	ログイン時に毎回この証明書の警告メッセージを表示しないようにするためには、サードパーティーの認証局(CA)を使って署名済みの証明書を入手することも可能です。詳細については、p.251「署名済み SSL サーバー証明書のインポート」をご参照ください。

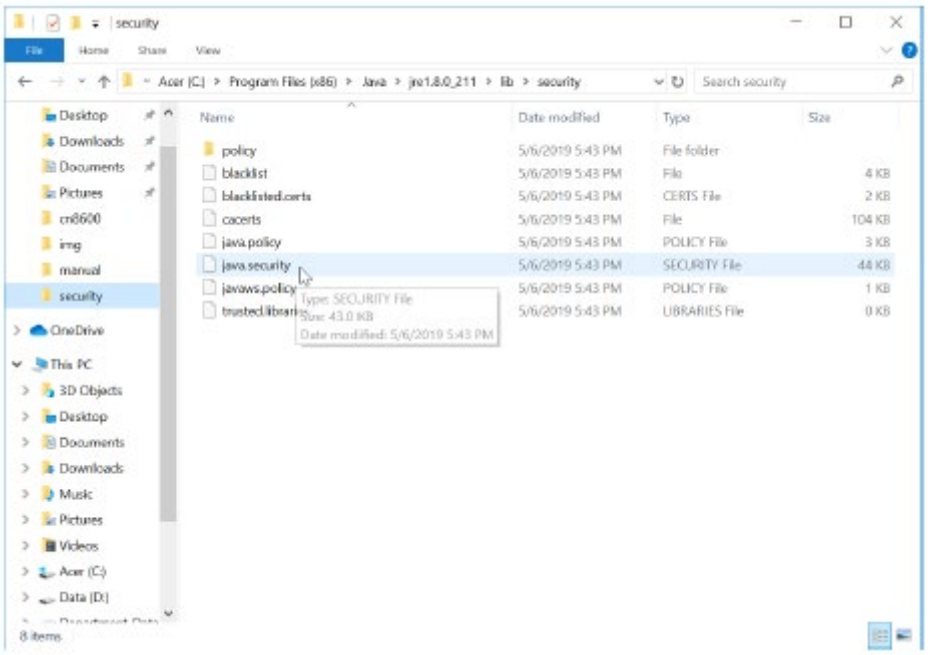
ARM ベースの PE シリーズ PDU の追加

Java の互換性設定によって、ARM ベースの PE シリーズ PDU が追加できない場合があります。

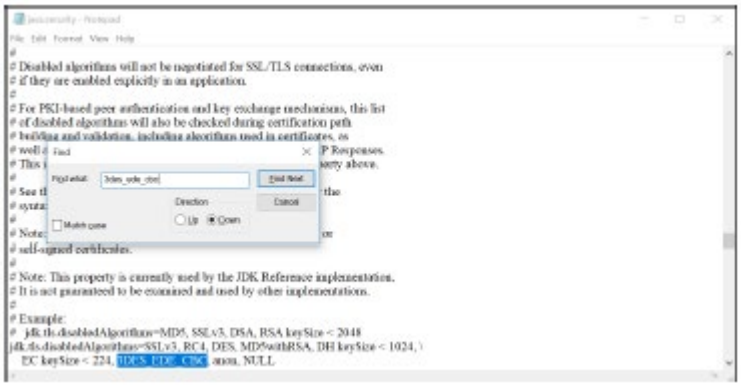
そのような場合には、次の手順に従って、互換性の問題を解消してください。

1. お使いの環境における Java フォルダーに移動してください。
   （例） C:¥Program Files (x86)¥Java¥jre1.8.0_211¥lib¥security

2. ファイル「java.security」の場所を確認してください。



3. テキストエディター（例：ノートパッド）を開いて、「**検索**」機能を呼び出してください。
4. 「**検索**」ダイアログボックスで、検索する文字列のテキストボックスに「3DES_EDE_CBC」と入力してください。下図はその例です。



5. 「3DES_EDE_CBC」という文字列が含まれている部分を削除し、ファイルを保存してください。

注意： 後でこの設定を戻す可能性がある場合は、該当部分を別のテキストファイルに保存しておくことを推奨します。

6. コンピューターを再起動したら、p.80「ATEN KVM の追加」に記載されている方法で、ARM ベースの PE シリーズ PDU を追加してください。

問題	解決法
CC2000 をインストールして数分経つと、「Error 1067」のエラーメッセージが表示される。	このエラーメッセージは OS 側から出されたもので、CC2000 サーバーが起動できないことを表します。この問題を解決するには、以下の手順で対応してください。 1. コンピューターを再起動してください。 2. お使いのコンピューターが CC2000 のシステム要件（p.15 参照）を満たしているかどうか確認してください。 3. 古いバージョンの CC2000 が既に存在し、このバージョンでアップグレードではなく上書きインストールしようとしている場合は、以前にインストールされたときにできたファイルが完全に削除されていない可能性があります（p.34 参照）。本マニュアルに記載されている方法で CC2000 をアンインストールし、再インストールしてください。
ウェブブラウザーの URL バーに CC2000 の IP アドレスを入力したが、ログインページが表示されない。	1. CC2000 は HTTPS のリクエスト以外は受け付けません。ウェブブラウザーからの HTTP リクエストは自動的に HTTPS リクエストにリダイレクトされます。HTTP ポートのデフォルトは 80 番、HTTPS ポートのデフォルトは 443 番です。これらのポートが管理者によって変更されている場合は、変更されたポート番号を URL の文字列に含めなければなりません。 例えば、CC2000 の IP アドレスが「10.10.10.10」で、SSL ポートが 8443 に設定されている場合、ウェブブラウザーでは以下の URL を入力しなければなりません。 https://10.10.10.10:8443 2. CC2000 サーバーがインストールされたサーバー上で稼働しているサービスが既にこのデフォルトポートを使用している可能性があります。CC2000 ユーティリティー（p.339 参照）を使ってポートの設定を変更してください。

（表は次のページに続きます）

問題	解決法
ウェブブラウザーの URL バーに CC2000 の IP アドレスを入力したが、ログインページが表示されない。(続き)	3. CC2000 のサービスが立ち上がっていることを確認してください。サービスのステータスを確認するには、Windows をお使いの場合は p.28 を、また、Linux をお使いの場合は p.32 をそれぞれご参照ください。
CC2000 の「Preferences」(設定)メニューで設定した言語と異なる言語でログイン画面が表示される	ログイン画面を表示する言語の優先順位は、ウェブブラウザーで設定されている言語が最も高く、その次に OS で使用している言語が参照されます。CC2000 にログインすると、「Preferences」(設定)メニューで設定された言語で画面が表示されます。
CC2000 にログインできない。	ユーザーネームとパスワードが正しいことをご確認ください。
CC2000 にログインしようとすると、「ログイン失敗。既にブラウザーセッションがオープンされたコンピューターからログインしようとしています。」という内容のメッセージが表示されます。	一部の Mozilla ベースのブラウザーは、同じサーバーに対する複数の接続で同一のセッション ID を共有します。同一のセッション ID で開いているセッションが既に存在する場合、CC2000 はログインリクエストを拒否します。このような場合には、以下のいずれかの方法で対応してください。 1) 現在開いているセッションを終了して、ログインし直す。 2) 別のコンピューターからログインする。 3) Mozilla ベースではないブラウザーからログインする。
ログインすると、ブラウザーから CA ルート証明書が信頼できないという内容のメッセージが表示されたり、証明書エラーの応答が返ってきたりする。	これは証明書の名前が Microsoft の信頼された認証局のリストに存在しないことに起因します。この証明書は信頼できるものですので、受け入れても問題ありません。詳細は p.325「信頼された証明書」をご参照ください。
CC2000 にログインすると、「Device Management」(デバイス管理)画面に遷移する。	どのポートに対してもアクセス権限が設定されていない可能性があります。ポートへの操作権限があるかどうかを CC2000 の管理者に確認し、権限がない場合は操作したいポートへの権限を設定してください。

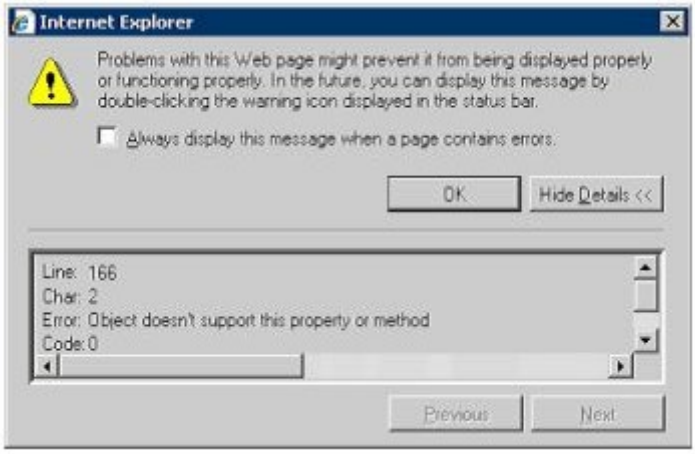
(表は次のページに続きます)

問題	解決法
CC2000 にログインしても、アクセスしたいデバイスの画面が立ち上がらない。	このデバイスへのアクセス権限があるかどうかを CC2000 の管理者に確認し、権限がない場合は操作したいデバイスへの権限を設定してください。
CC2000 にログインしても、「System Management」(システム管理)タブには「This Server」(このサーバー)と「License」(ライセンス)の 2 つのメニューしか表示されない。	ライセンスの競合が発生しています。解決方法の詳細については、p.259「ライセンスの競合」をご参照ください。
イベントトラップの通知メールが受信できない。	1. CC2000 マネジャーにおけるメールサーバーの設定が正しいことを確認してください。 2. 関連デバイスの設定で入力されたメールアドレスが正しいことを確認してください。 3. 関連デバイスのイベントトラップの設定が正しいことを確認してください。
「Device Management」(デバイス管理)画面からジェネリックデバイスにアクセスしても反応がない。	ジェネリックデバイスには、そのデバイスに設定された IP アドレスを使って直接アクセスします。DHCP の変更などの理由で IP アドレスが変更されると、新しい IP アドレスが設定されたデバイスには古い IP アドレスを使ってアクセスできなくなります。デバイスの新しい IP アドレスを確認し、その内容で設定を変更してください。
追加したいデバイスが見つからない。	1. CC2000 マネジャーが起動していて、全てのサービスが正常に立ち上がったことを確認してください。 2. 「CC Management」(CC 管理)の項目が有効になっており、デバイスの「ANMS」メニューにおける設定が正しいことを確認してください。
Cat 5e タイプの KVM スイッチを追加した際に、全ポートを同時に追加することは可能か？	全てのポートにコンピューターモジュールが接続されており、これらのデバイスがオンラインであれば、全ポートを同時に追加することが可能です。詳細は p.83 の注意書きをご参照ください。

(表は次のページに続きます)

問題	解決法
ポートのアイコンはオンラインになっているにも関わらず、そのポートに接続されたデバイスのアイコンはオフラインの表示になっており、このデバイスやポートにアクセスすることができない。	このデバイスのファームウェアが CC2000 に対応していないことに起因します。デバイスのファームウェアを最新版に更新してください。
CC2000 セカンダリーサーバーに接続されているデバイスが、プライマリーサーバーの利用可能なデバイスリストに表示されない。	1. デバイスが追加されていることを確認してください。追加されている場合は、一覧には表示されません。 2. 各セカンダリーサーバーで、「Auto Discovery」（自動検出）ボタンをクリックしてください。 3. 手順 2 の操作を行っても、デバイスが表示されなかった場合は、そのデバイスの ANMS が有効になっており、なおかつ、デバイスに認識させたい CC2000 の IP アドレスとポートが正しく設定されていることを確認してください。 4. 手順 2 の操作を行った後、デバイスが表示された場合は、ネットワークに問題があることが考えられます。この場合はプライマリーデータベースの複製を行ってください。詳細については p.278 をご参照ください。
ATEN デバイスが CC2000 で認識されない。	1. 問題になっているデバイスは、CC2000 に対応していない可能性があります。対応デバイスの一覧については p.317「対応 ATEN 製品」をご参照ください。 2. CC2000 で管理するためには、デバイスのファームウェアを最新版に更新する必要があります。
設定の変更を行い、保存ボタンをクリックすると、HTTP Status 500 のエラーメッセージが表示される。	設定内容に誤りがある可能性があります。これは、不明な設定を受け取った場合に表示される Apache Tomcat のエラーメッセージです。このエラーから回復するには、他のタブを選択したあと元のタブに戻って、正しい値で変更を行ってください。
CC2000 でのタイムアウト機能を無効にしているにもかかわらず、操作がタイムアウトしてしまう。	設定の変更は、次回ログイン時に初めて有効になります。

Q1:ビューワーを立ち上げると、ウェブ画面に何も表示されない、または画面が正しく動作せず、下図のようなエラーメッセージが表示される。



1. Internet Explorer のセキュリティーに関する設定をリセットし、アクティブスクリプト、Active X、Java Web Start を有効にしてください。

   デフォルトでは、Internet Explorer 6 と一部の Internet Explorer 5.x では制限付きサイトのセキュリティーレベルが高に、また、Microsoft Windows Server 2003 では、制限付きサイトおよびインターネットの各ゾーンにおけるセキュリティーレベルが高にそれぞれ設定されていますが、アクティブスクリプト、ActiveX コントロール、Java Web Start を有効にすることも可能です。この場合は、以下の手順で操作してください。

   a) Internet Explorer を起動してください。
   b) メニューバーから[ツール]→[インターネットオプション]をクリックしてください。
   c) 「インターネットオプション」ダイアログから、「セキュリティー」タブをクリックしてください。
   d) 「既定のレベル」ボタンをクリックしてください。
   e) 「OK」ボタンをクリックしてください。

2. アクティブスクリプト、Active X、Java がブロックされていないことを確認してください。
   コンピューターによっては、Internet Explorer の他にも、ウイルス対策ソフトやファイアウォール側でブロックされている可能性がありますので、ここでもアクティブスクリプト、Active X、Java Web Start がそれぞれブロックされていないことを確認してください。

3. ウイルス対策ソフトが、インターネット一時ファイルやダウンロードされたプログラムファイルをスキャンしないように設定されていることを確認してください。

4. インターネット一時ファイルをすべて削除してください。
お使いのコンピューターからこれらのファイルを削除する場合は、以下の手順で操作してください。

   a) Internet Explorer を起動してください。
   b) メニューバーから[ツール]→[インターネットオプション]をクリックしてください。
   c) 「全般」タブをクリックしてください。
   d) 「インターネット一時ファイル」で「設定」ボタンをクリックしてください。
   e) 「ファイルの削除」ボタンをクリックしてください。
   f) 「OK」ボタンをクリックしてください。
   g) 「Cookie の削除」ボタンをクリックしてください。
   h) 「OK」ボタンをクリックしてください。
   i) 「履歴」で「履歴のクリア」ボタンをクリックし、表示されたダイアログで「はい」ボタンをクリックしてください。
   j) 「OK」ボタンをクリックしてください。

5. Microsoft Direct X の最新版がインストールされていることを確認してください。
インストールの方法に関する詳細は、Microsoft のウェブサイトを参考にしてください。

6. OpenJDK 8 または Java JRE 8 がインストールされていることを確認してください。
最新の OpenJDK のインストールについては http://www.azul.com を、最新の Java のインストールについては https://java.com/ja/を、それぞれ参考にしてください。

OpenJDK 8 のインストール

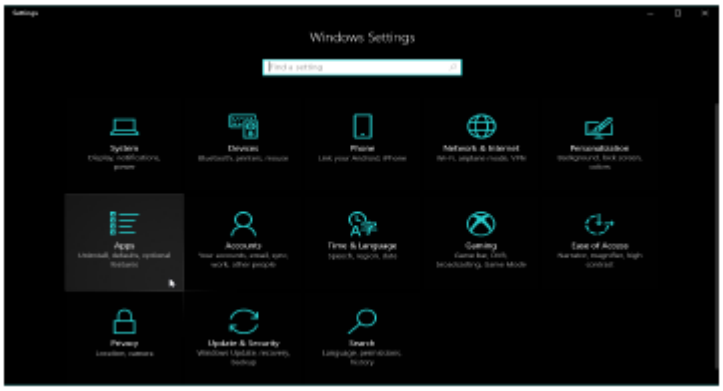
OpenJDK 8 のインストールに関して、既に JRE をインストールしている場合は、その JRE を削除しておいてください。また、OpenJDK 8 をインストールしたら、お使いの CC2000 サービスを再起動してください。

Windows

操作方法は、Windows の大半のバージョンで同じです。ここでは、Windows 10 を例に挙げて操作方法を説明します。

JRE のアンインストール

1. 「**スタート**」 → 「**設定**」をクリックしてください。

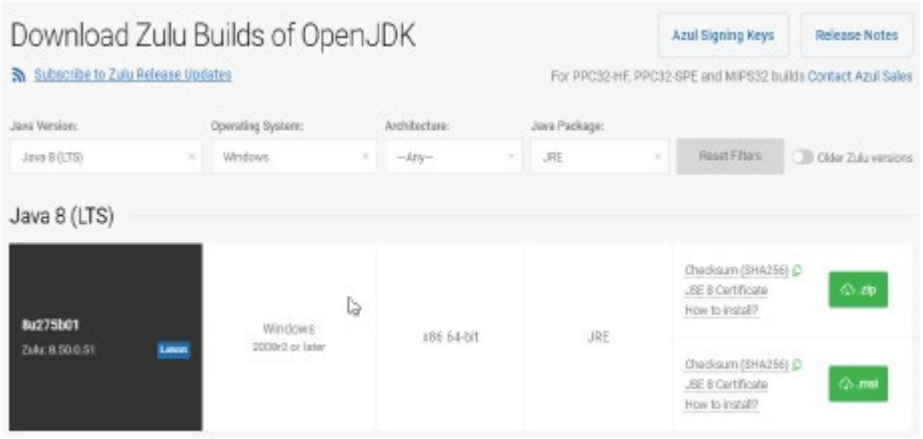


2. アプリ一覧で「**アプリ**」をクリックし、「Java」の項目をクリックしてください。
3. 「**アンインストール**」をクリックしたら、画面内の手順に従って操作を行ってください。
   お使いのシステムに複数の Java がインストールされている場合は、これらを全てアンインストールしてください。

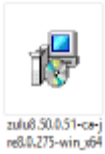
OpenJDK のダウンロードとインストール

1. OpenJDK のウェブサイト（www.azul.com）にアクセスしたら、「Download now」（今すぐダウンロード）をクリックしてください。
2. 画面を下方向にスクロールし、「Download Azul Zulu Builds of OpenJDK」（OpenJDK の Azul Zulu ビルドをダウンロード）というセクションに移動してください。
3. 「Java Version」（Java バージョン）、「Operating System」（オペレーティングシステム）、「Java Package」（Java パッケージ）の各ドロップダウンメニューから、それぞれ「**Java 8 (LTS)**」、

「Windows」、「JRE」を選択してください。「Architecture」(アーキテクチャー)のドロップダウンメニューからは、お使いの OS のアーキテクチャーに適したものを選択してください。この画面は、下図の例のような外観です。



4. 「.msi」を選択し、実行ファイルを直接ダウンロードしてください。このときのファイルのアイコンは、下図のような外観となります。



5. ファイルを実行し、画面内の指示に従いながら操作を行って、セットアップを完了してください。

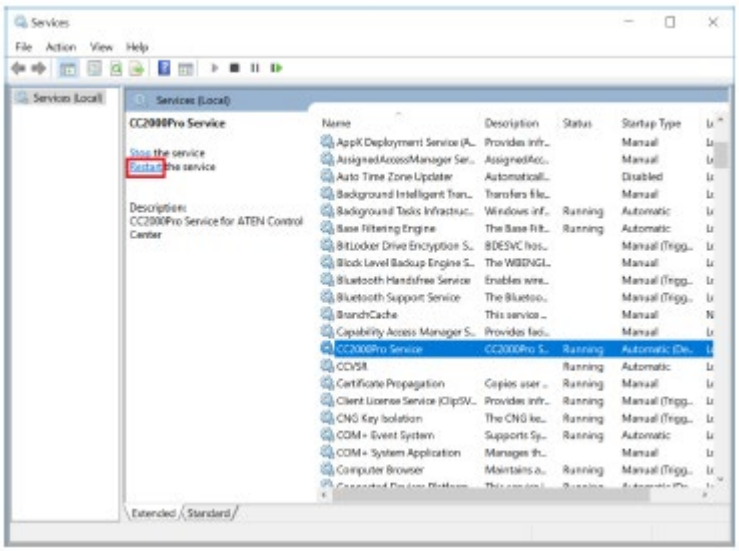
IcedTea-Web のダウンロードとインストール

セットアップ方法は、OpenJDK の場合とほぼ同様です。次の URL にアクセスしたら、お使いの環境に適した「.msi」ファイルをダウンロードし、インストールを行ってください。

https://www.azul.com/products/components/icedtea-web/

CC2000 の再起動

1. お使いの Windows のデスクトップで、「サービス」というキーワードを検索し、このデスクトップアプリをクリックして起動してください。
2. CC2000 サービスをクリックして選択してください。



3. 「再起動」をクリックして、サービスを再起動してください。

Linux

JRE を削除する方法については、次の URL を参照してください。
https://java.com/en/download/help/linux_uninstall.xml

OpenJDK のダウンロードとインストールの方法については、次の URL を参照してください。
https://openjdk.java.net/install/

CC2000 サービスを再起動する方法には、p.32「インストール後の確認」を参照してください。

自己署名(プライベート)証明書

独自の自己署名暗号鍵や証明書を作成したい場合は、フリーツール「openssl.exe」をウェブサイト(**www.openssl.org**)からダウンロードすることができます。独自のプライベートキーや証明書を作成する場合は、下記の手順に従って操作を行ってください。

1. ダウンロードして解凍した openssl.exe のディレクトリーに移動してください。
2. 以下のパラメーターを指定して openssl.exe を実行してください。
   openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -keyout CA.key -out CA.cer -config openssl.cnf

注意:
1. 上記のコマンドは1行で続けて入力してください。パラメーターの入力途中で[Enter]キーを押さないでください。
2. 入力値にスペースが含まれている場合は、その値をダブルクォートで囲んでください(例:"ATEN International")。
3. 最新版のバイナリーなどはパラメーターの仕様変更がされていることもあるため、必ずリリースノートや技術資料をご確認ください。

以下のパラメーターを使用して、作成時に入力するキーを少なくすることも可能です。

/C /ST /L /O /OU /CN /emailAddress

例

openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -
keyout CA.key -out CA.cer -config openssl.cnf -subj /
C=yourcountry/ST=yourstateorprovince/L=yourlocationorcity/
O=yourorganiztion/OU=yourorganizationalunit/
CN=yourcommonname/emailAddress=name@yourcompany.com
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -
keyout CA.key -out CA.cer -config openssl.cnf -subj /C=CA/ST=BC/
L=Richmond/O="ATEN International"/OU=ATEN /CN=ATEN/
emailAddress=eservice@aten.com.tw

ファイルのインポート

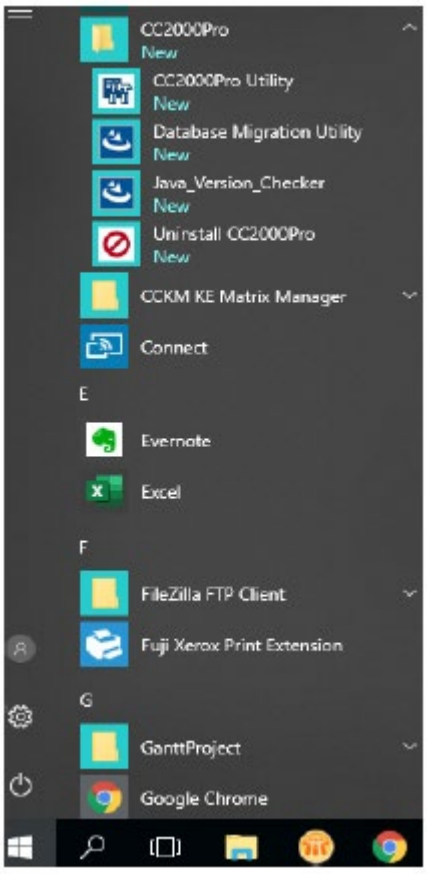
openssl.exe のプログラムが終了すると、このプログラムを実行したディレクトリーに「CA.key」（プライベートキー）と「CA.cer」（自己署名済 SSL 証明書）という 2 つのファイルが作成されます。これらのファイルは、「Update CC2000 Server Certificate」（CC2000 サーバー証明書のアップデート）パネルでアップロードします（p.252「プライベートキーと証明書のインポート」参照）。

付録 B
CC2000 ユーティリティー

概要

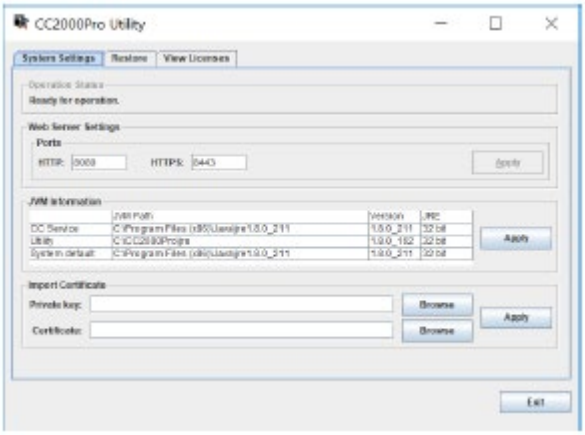
CC2000Pro ユーティリティーは、CC2000 が動作しているコンピューターのデスクトップからウェブブラウザーを使わずに CC2000 のパラメーターの設定が行えるツールで、CC2000 のインストールと同時にインストールされます。

CC2000 が Windows にインストールされている場合、[スタート]メニューから[プログラム]→[CC2000Pro]→[CC2000Pro Utility]を選択し、ツールを起動してください。



Linux の場合は、root ユーザーでログインし、「/opt/CC2000Pro/Runable」ディレクトリーに移動し、「CC2000Pro_Utility」ファイルを実行してください。

プログラムを起動すると、下図のような画面が表示されます。



このユーティリティーのメニューは、「System Settings」(システム設定)、「Restore」(リストア)、「View Licenses」(ライセンスの参照)という 3 つのタブに分かれています。各タブの詳細は以下のセクションで説明します。

システム設定

CC2000 のウェブ画面の表示には Apache Tomcat が使用されています。CC2000 のインストール時には、Apache Tomcat がリクエストに対して通信を行うポートの設定を求められます。

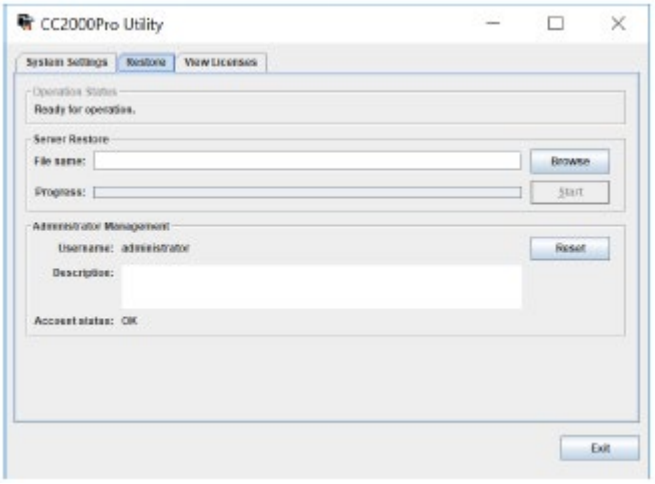
- HTTP ポートは、Apache Tomcat が通常の通信を行うポートです。デフォルトでは 80 番のポートを使用します。これ以外のポートを使用する場合、ユーザーが CC2000 にウェブブラウザーでアクセスする際に URL バーにこのポートを入力する必要があります。
- HTTPS ポートは、Apache Tomcat が通信を行うセキュアなポートです。デフォルトでは 443 番のポートを使用します。これ以外のポートを使用する場合、ユーザーが CC2000 にウェブブラウザーでアクセスする際に URL バーにこのポートを入力する必要があります。

設定されたポートが競合しウェブ画面が表示されなくなった場合は、このユーティリティーを使ってポートの設定を変更してください。

設定を変更したら、「Apply」(適用)ボタンをクリックして変更内容を保存してください。

リストア

「Restore」(リストア)タブをクリックすると、下図のようなダイアログが表示されます。



この画面は、以下の 3 つのパネルに分かれています。

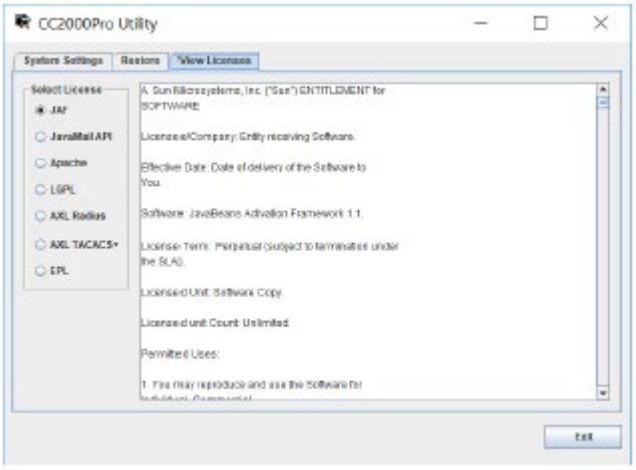
パネル	説明
Operation Status (動作状況)	この部分で CC2000 のサービスの動作状況を確認することができます。
CC2000 Restore (CC2000 のリストア)	CC2000 プライマリーサーバーのデータベースに過去のデータをリストアする際にこの部分を使用します(p.263 参照)。「**Browse**」(参照)ボタンを押した際に表示されるダイアログからリストアするファイルを選択し、この「CC2000 Utility」(CC2000 ユーティリティー)ダイアログの「**Start**」(開始)ボタンをクリックするとリストアを開始します。処理の進捗状況は「Progress」(進行状況)欄に表示されます。

(表は次のページに続きます)

パネル	説明
Administrator Management (アドミニストレーター管理)	「Reset」(リセット)ボタンをクリックすると、デフォルトのシステムアドミニストレーターのアカウントをデフォルト(administrator/password)にリセットします。このアカウントがロック(p.286 参照)されている場合は、自動的にロックが解除されます。

ライセンスの参照

「View License」(ライセンスの参照)タブでは、CC2000 パッケージに関連したライセンスを参照することができます。ライセンスを参照する場合は、そのライセンスに対応したラジオボタンをクリックしてください。

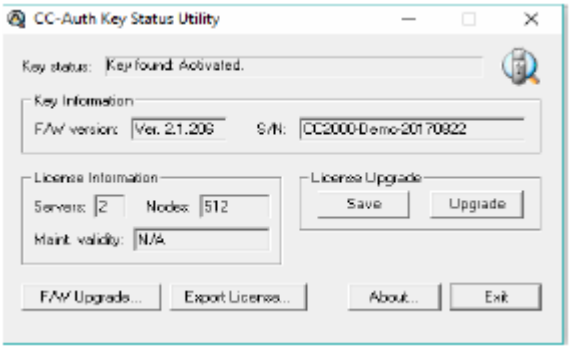


付録 C
認証キーユーティリティー

概要

認証キーユーティリティー(CCAuthKeyStatus.exe)は、Windows ベースのユーティリティーで、CC2000 認証キーに含まれるデータにアクセスしたり更新したりするためのプログラムです。このプログラムは、CC2000 の製品ページからダウンロードできます。

このプログラムを起動すると、下図のような画面が表示されます。



キーのステータス情報

このダイアログに表示される項目は下表の通りです。

セクション	用途
Key Status (キーの状態)	キーが存在するかどうか、また、キーが有効になっているかどうかを確認することができます。
Key Information (キー情報)	キーの現在のファームウェアバージョンとシリアルナンバーが表示されます。
License Information (ライセンス情報)	サーバー(プライマリーおよびセカンダリー)の数と、そのキーが使用できるノードの数が表示されます。
License Upgrade (ライセンスの アップグレード)	オフラインでライセンスアップグレードを行う場合は、これらのボタンを使ってください。
F/W Upgrade (F/W アップグレード)	認証キーのファームウェアアップグレードを行う場合は、このボタンを使ってください。

キーユーティリティー

「License Upgrade」(ライセンスのアップグレード)と「F/W Upgrade」(F/W アップグレード)の各セクションでは、キーのファームウェアのアップグレード(F/W アップグレード)や、そのライセンスで許可されたサーバー数およびノード数の更新(ライセンスのアップグレード)を行うことができます。

キーのファームウェアアップグレード

CC2000 認証キーのファームウェアはアップグレードすることができます。ファームウェアの新しいバージョンがリリースされると、アップグレードファイルは弊社ダウンロードサイトに公開されます。このサイトに定期的にアクセスし、最新版があるかどうか確認してください。

アップグレードの開始

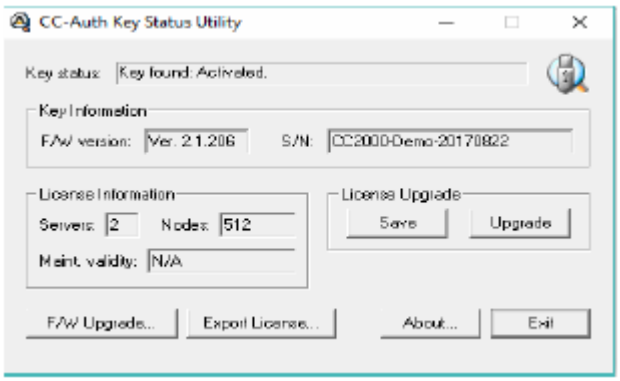
ファームウェアのアップグレードを行う場合は、以下の手順で操作してください。

1. ダウンロードサイトにアクセスし、新しいファームウェアファイルをお使いのコンピューターのハードディスク上の適当な場所に保存してください。

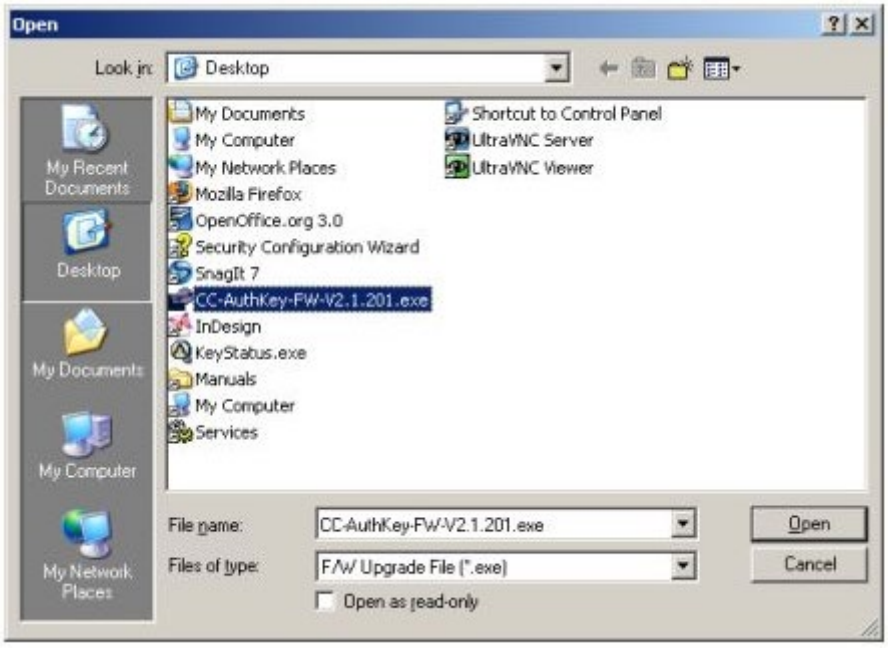
2. 認証キーをコンピューターに接続し、キーステータスユーティリティー(CCAuthKeyStatus.exe)を起動してください。

注意:	1. CCAuthKeyStatus.exe は Windows 上でのみ動作します。 2. バージョン 2.1.204 以降のファームウェアでは、ライセンスアップグレード機能に対応するために CC2000 の認証キーが必要です。

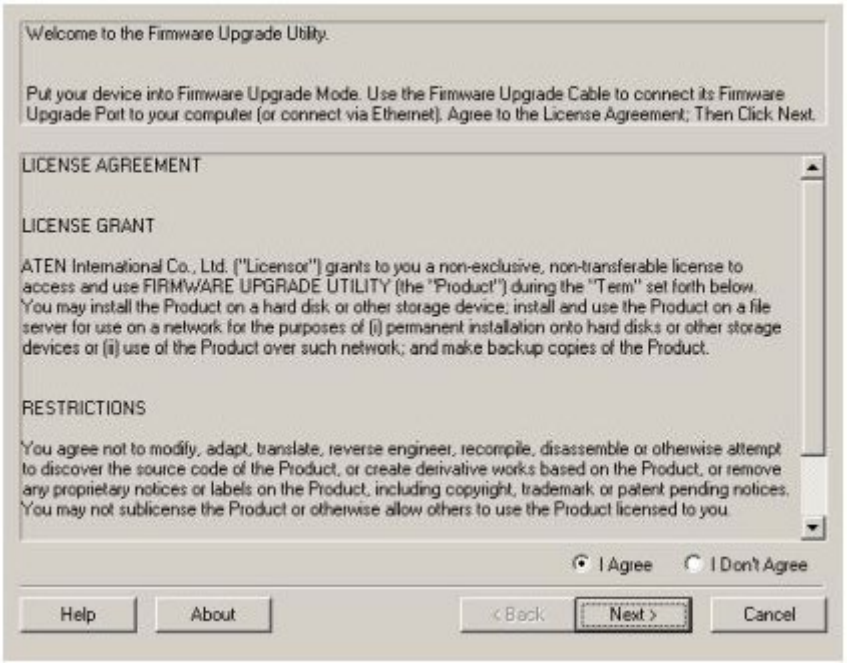
3. 表示された画面で、「F/W Upgrade…」ボタンをクリックしてください。



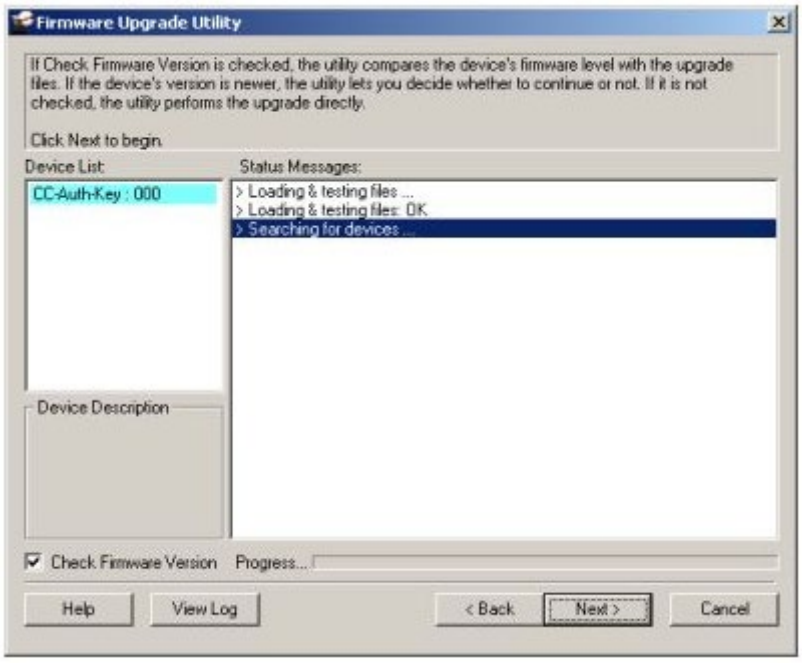
4. 「ファイルを開く」ダイアログが表示されたら、ファームウェアアップグレードファイルを選択し、「**開く**」ボタンをクリックしてください。



5. ライセンス使用許諾に目を通し、同意される場合は「I Agree」(同意する)ラジオボタンを選択し「Next」(次へ)ボタンをクリックして次に進んでください。



6. ユーティリティーは自動的にデバイスの検索を行います。デバイスが検索されると、「Device List」(デバイスリスト)パネルに表示されます。

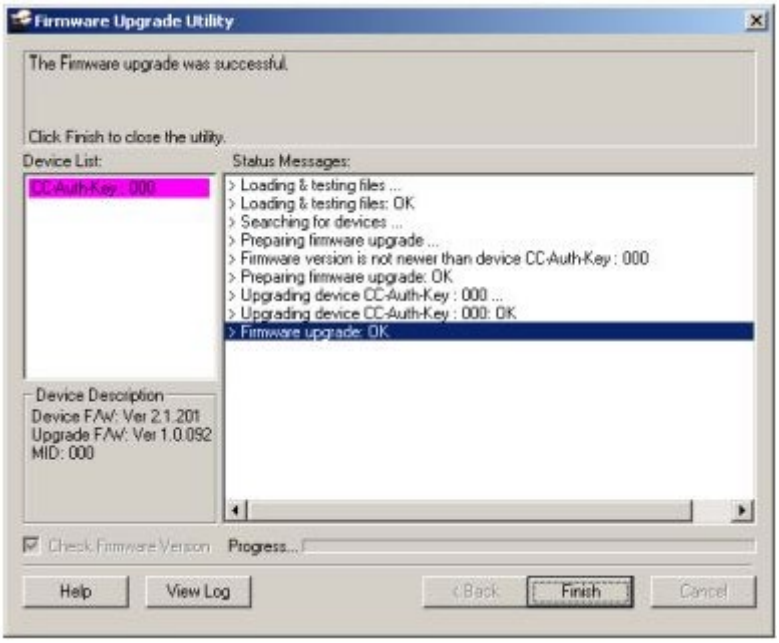


注意:	「Check Firmware Version」(ファームウェアバージョンを確認する)のチェックボックスにチェックを入れると、ユーティリティーはデバイスとアップグレードファイルの間でファームウェアバージョンの比較を行います。このとき、デバイスにインストールされたバージョンの方がアップグレードファイルよりも新しいと、ダイアログが表示され、処理を続行するかどうかの選択を促されます。 この項目にチェックが入っていないと、ユーティリティーはバージョンの比較を行わずにアップグレードファイルのインストールを行います。

「**Next**」(次へ)ボタンをクリックして、次に進んでください。

アップグレード成功

アップグレードが完了すると、下図のような画面に、アップグレードが正常終了したことを示すメッセージが表示されます。



ファームウェアアップグレードユーティリティーを終了する場合は「Finish」(完了)ボタンをクリックしてください。

キーライセンスのアップグレード

概要

CC2000 には、エンドユーザー(クライアント)が認証キーを更新し、ライセンス数の追加を反映させる機能があります。キーライセンスのアップグレードは、クライアントからでも、また代理店や販売店からでも実行することができます。また、インターネットを介したブラウザーセッション(オンラインアップグレード)からでも、スタンドアロンのユーティリティープログラム(オフラインアップグレード)からでも、実行が可能です。

クライアントは、まず代理店・販売店に更新するライセンスの数を連絡します。これを受けて、代理店・販売店はATENの担当営業に追加ライセンス数の発注を行います。注文処理が進むと、ATENから確認メールおよび承認メールで、アップグレードの実行に関する詳細が通知されます。

注意: ライセンスを追加する際には、キー単位での注文が必要になります。

キーのアップグレードには以下の 2 つの方法があります。

- **オンライン:** アップグレードを実行する際には、キーをコンピューターの USB ポートに挿入し、ブラウザーを起動してキーを直接アップグレードしてください。クライアントがアップグレードを実行する場合は、代理店・販売店からユーザーに対して確認メールの詳細が連絡されます。代理店・販売店がアップグレードを実行する場合は、クライアントから代理店・販売店に対して認証キーの情報を提供します。

- **オフライン:** Windows ベースのキーステータスユーティリティーは、キー情報を抽出したり、キー情報データファイルとして保存したりする場合に使用します。キー情報データファイルをブラウザーセッションで使用して、ライセンスアップグレードファイルを生成します。ライセンスアップグレードファイルが生成されると、キーステータスユーティリティーを再び使用して、アップグレードファイルの情報をライセンスキーに書き込みます。
  - クライアントが CC クライアントデータベースの更新を行う場合、代理店・販売店はこのユーザーに対して確認メールの詳細情報を提供し、キーライセンスアップグレードファイルが生成できるようにします。クライアントはキーステータスユーティリティーやキーライセンスアップグレードファイルを使って、認証キーのライセンス情報を更新します。

- 代理店・販売店が CC クライアントデータベースの更新を行う場合、クライアントから代理店・販売店に対して、クライアントのキーライセンスアップグレードファイルの生成時に使用するキー情報データファイル(キーステータスユーティリティーにより抽出)が、提供されます。そして、代理店・販売店からはキーライセンスアップグレードファイルがクライアントに送られ、クライアントはキーステータスユーティリティーを使って認証キーのライセンス情報をアップグレードします。

オンラインアップグレード

クライアントは代理店・販売店に連絡して、アップグレードの発注を行います。発注はキー単位で行う必要があります。代理店・販売店は ATEN 担当営業に対してアップグレードの発注を行うと、下記のような確認メールを受信します。

Your order is ready to be processed. Please go to http://xxx.xxx.x.xxx to upgrade your key's license.

Login Information:

- Username: myname2
- Password: mypassword5678

Order Information:

- Order ID: 1017000700 (authorized number: 2068919892). This order requests CCMA512 (1YR SUP FOR 512 NODES)

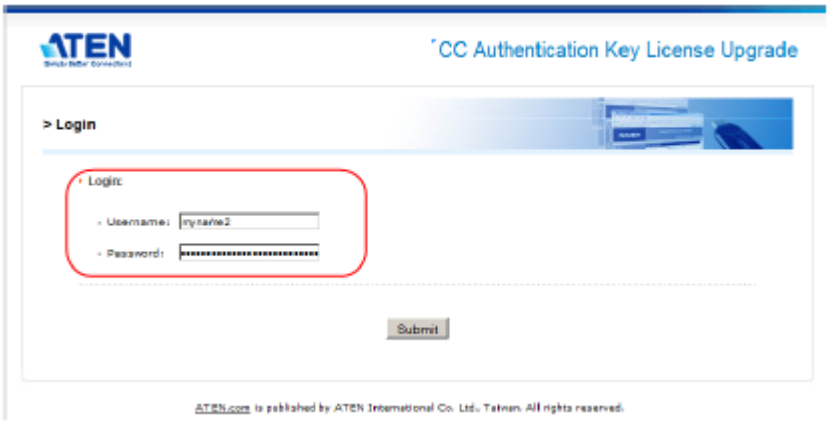
アップグレードは、クライアント、代理店・販売店のどちらからでも実行することができます。代理店・販売店がアップグレードを行う場合、クライアントは代理店・販売店に対してライセンスキーを提供します。また、クライアントがアップグレードを行う場合、代理店・販売店は確認メールをクライアントに転送します。

オンラインアップグレードを実行する場合は、下記の手順に従って操作してください。

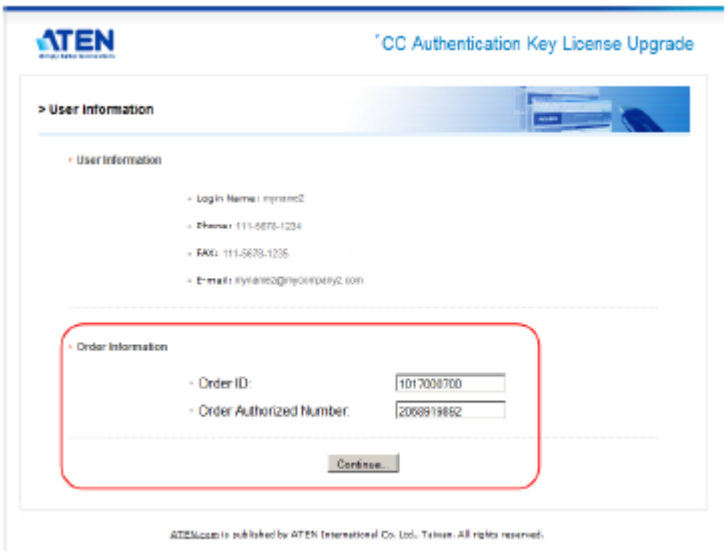
1. 認証キーを、お使いのコンピューターの USB ポートに挿してください。

2. ブラウザーを起動し、CC 認証キーのライセンス更新ページにアクセスしてください。更新ページの URL は下記の通りです。
   https://cc.aten.com.tw:10443/

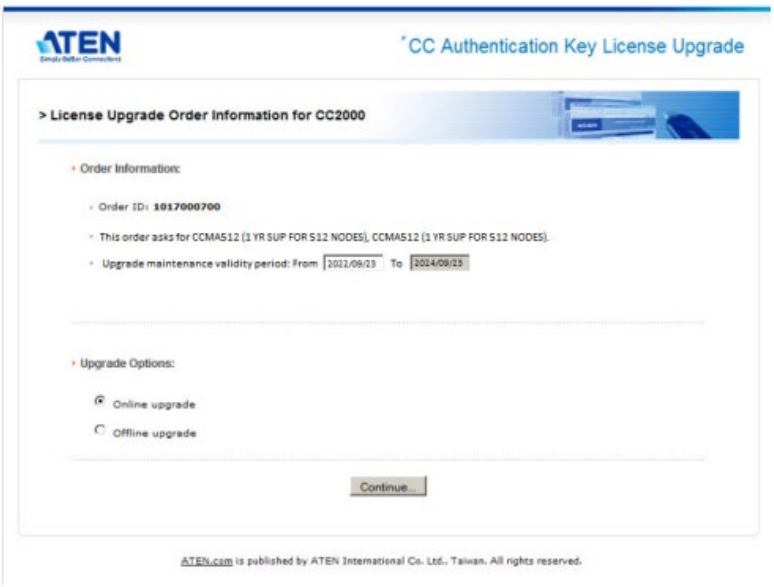
3. ログイン画面が表示されたら、確認メールに記載されていたユーザーネームとパスワードを使ってログインしてください。



4. 表示された画面で、アップグレードに適用する「Order ID」(発注 ID)、「Order Authorization」(発注権限)の各番号を入力し、「**Continue**」(続行)ボタンをクリックしてください。



5. ライセンスアップグレード発注情報画面で、「From」欄に現在のライセンス数を入力し(「To」欄は自動入力)、「**Online upgrade**」(オンラインアップグレード)ボタンを選択してください。



注意:	現在のライセンス数はキーステータスユーティリティー(CCAuthKeyStatus.exe)を使って確認することができます。

6. 「Continue」(続行)をクリックしてください。

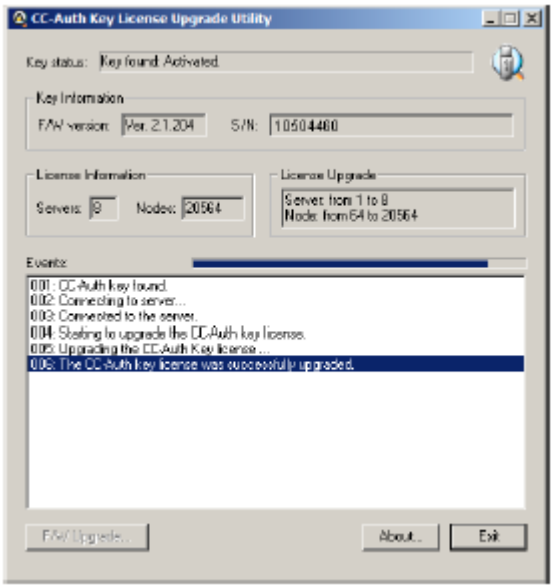
7. 代理店による CC 認証キーライセンスアップグレード画面が表示されたら、「Download」(ダウンロード)ボタンをクリックしてください。

8. ブラウザーからファイル(KeyUpgrade.exe)の処理方法の選択を促すメッセージが表示されたら、「ディスクに保存する」を選択してください。

9. ブラウザーを表示したまま、上記の手順でダウンロードしたファイルのあるディレクトリーに移動し、このファイルを実行してください。

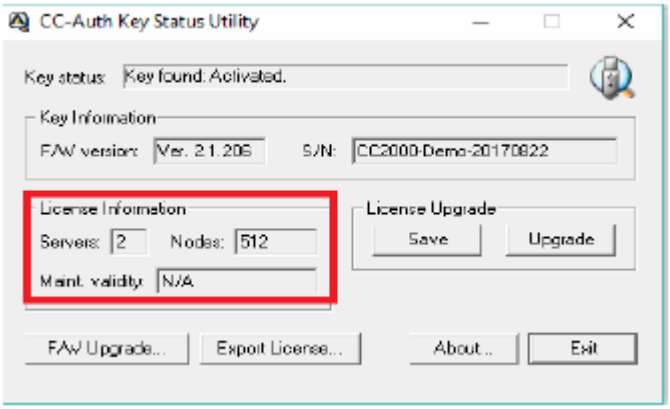
注意:	この手順は、ファイル「KeyUpgrade.exe」をダウンロードした時と同じウェブセッションで行う必要があります。同じウェブセッションで操作しないと、アップグレードが正常に終了しない場合があります。

アップグレードユーティリティーが起動して、アップグレードを開始します。実行アクションの内容はメインパネルに表示されます。



10. アップグレードが完了すると、アップグレードが成功したことを通知するメッセージがポップアップ画面で表示されます。「OK」ボタンをクリックして、ポップアップ画面を閉じてください。ブラウザーには、アップグレード処理の要約が表示されます。

11. 「Logout」(ログアウト)ボタンをクリックして終了してください。
キーステータスユーティリティー(CCAuthKeyStatus.exe)を使って、キー上のライセンス数が正しく更新されていることを確認することができます。


CC-Auth Key Status Utility
Key status: Key found. Activated.
Key Information
FAV version: Ver. 2.1.206
S/N: CC2000-Demo-20170822
License Information
Servers: 2
Nodes: 512
Maint. validity: N/A
License Upgrade
Save
Upgrade
FAV Upgrade...
Export License...
About...
Exit

アップグレード成功

アップグレードが成功すると、代理店・販売店はオンラインアップグレードが完了したことをメールで通知されます。以下は、その通知例です。

Your order (Order ID: 1017000700) has been completed successfully by the online utility.
The key (PSN: 10504460) server number has been upgraded from 1 to 8, and node number from 64 to 20564.

オフラインアップグレード

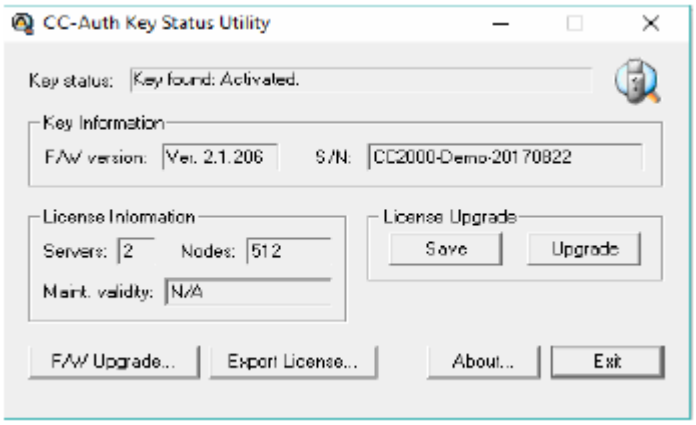
オフラインアップグレードは、代理店・販売店、エンドユーザーのどちらからでも実行することができます。オフラインアップグレードのメリットは、ユーザーが自分のキーを中断せずに使用できるという点にあります。ユーザー側に必要とされる手順は、キー情報データファイルを代理店・販売店にメールで送付し、ライセンス交付後にキー更新ファイルを受け取るだけです。

事前準備

アップグレードを実行するためにクライアントがまず行わなければならない作業は、下記のように、「Key Information Data File」(キー情報データファイル)を作成することです。

1. 認証キーを接続したまま、キーステータスユーティリティー(CCAuthKeyStatus.exe)を実行してください。

2. ライセンス更新パネルのダイアログが表示されたら、「Save」(保存)ボタンをクリックしてキー情報データファイル(KeyUpload.dat)ファイルを作成してください。



注意：	キー情報データファイルは、キーステータスユーティリティーと同じディレクトリーに作成されます。

キー情報データファイルが作成されたら、クライアントはこのファイルを代理店・販売店に送付します。

アップグレードの実行

代理店・販売店は ATEN 担当営業に対してアップグレードの発注を行うと、下記のような確認メールを受信します。

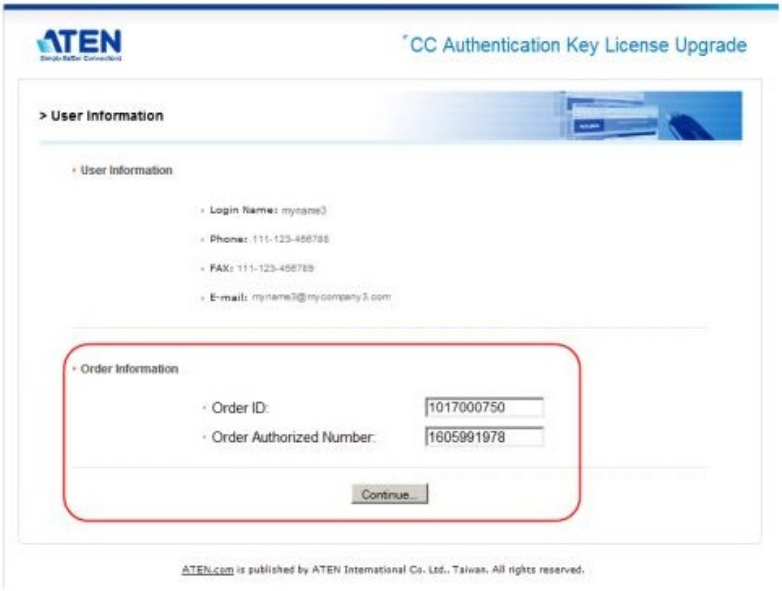
> Your order is ready to be processed. Please go to http://xxx.xxx.x.xxx to upgrade your key's license.
>
> Login Information:
>
> - Username: myname3
> - Password: mypassword3
>
> Order Information:
>
> - Order ID: 1017000750 (authorized number: 1605991978). This order requests 1 more server(s) and 448 more node(s)

アップグレードを実行する場合は、下記の手順に従って操作してください。

1. オンラインアップグレード（p.350 参照）の手順 1～3 の操作を行ってください。

2. アップグレードのログイン画面が表示されたら、確認メールに記載されているユーザーネームとパスワードでログインしてください。

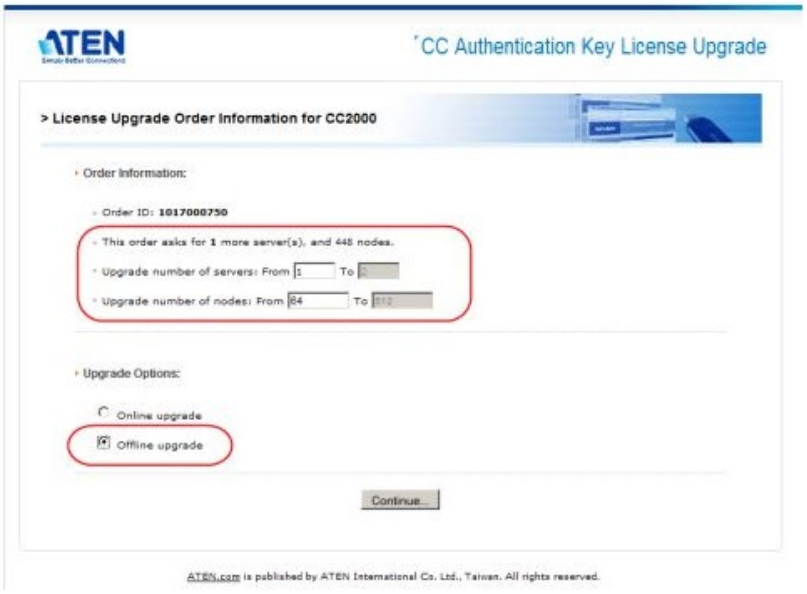
3. 表示された画面で、アップグレードに適用する「Order ID」(発注 ID)と「Order Authorization」(発注権限)の各番号を入力し、「**Continue**」(続行)ボタンをクリックしてください。



4. ライセンスアップグレード発注情報画面が表示されたら、「From」欄に現在のライセンス数を入力してください。「To」欄は自動で入力されます。

> **注意:** 必要であれば、現在のライセンス数はキーステータスユーティリティー(CCAuthKeyStatus.exe)を使って確認することができます。

5. アップグレードオプションから「Offline upgrade」(オフラインアップグレード)を選択して、「**Continue**」(続行)ボタンをクリックしてください。

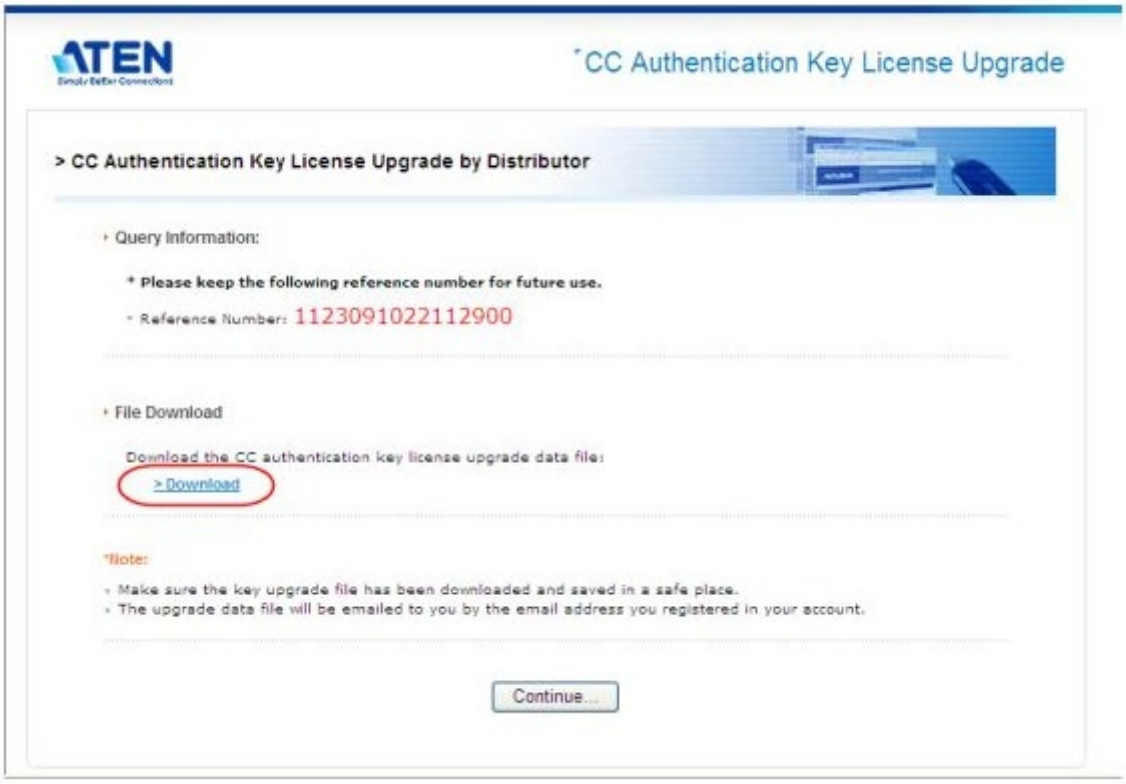

CC Authentication Key License Upgrade
> License Upgrade Order Information for CC2000
Order Information:
Order ID: 1017000750
This order asks for 1 more server(s), and 448 nodes.
Upgrade number of servers: From 1 To 2
Upgrade number of nodes: From 64 To 512
Upgrade Options:
Online upgrade
Offline upgrade
Continue...
ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

6. アップロードキー情報画面が表示されたら、「Browse...」(参照)ボタンをクリックし、「Preliminary Steps」(事前手順)セクションで生成された「KeyUpload.dat」ファイルを読み込んで、「Continue」(続行)ボタンをクリックしてください。

7. この画面には、ここまでの処理のサマリーが表示されます。

「Continue」(続行)ボタンをクリックして先に進んでください。

8. 次に表示される画面で、「Download」(ダウンロード)ボタンをクリックして、キーライセンスアップグレードファイル(KeyUpgrade.dat)をクリックしてください。



9. キーアップグレードファイルをどう扱うかを問うメッセージがブラウザーで表示されたら、「ファイルに保存する」方法を選択してください。ファイルがディスクに保存されたら、「Continue」(続行)ボタンをクリックして処理を続行してください。

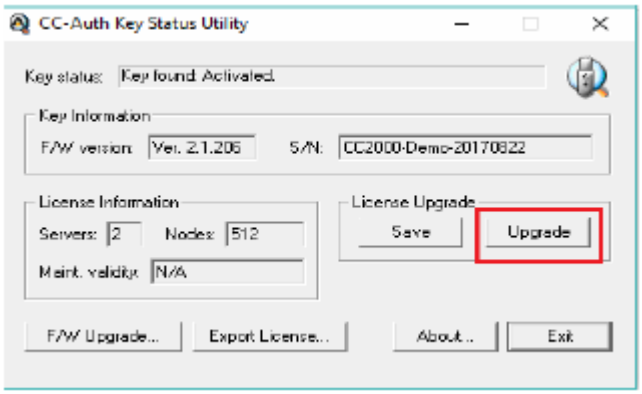
10. 確認用ポップアップダイアログが表示されたら、「Yes」(はい)ボタンをクリックしてください。注文を確認するサマリー画面が表示されます。

11. 「Logout」(ログアウト)ボタンをクリックして操作を終了してください。

注意:
1. 複数のキーをアップグレードする場合、ファイルを識別するために、「KeyUpgrade.dat」ファイル名に別の名前を付けることができますが、拡張子の部分(.dat)は変更しないでください。
2. クライアントがアップグレードを実行する場合は、代理店・販売店が「KeyUpgrade.dat」ファイルをクライアントに提供します。

12. 「キーステータスユーティリティー」を再度実行してください。

13. ライセンスアップグレードパネルで、「Upgrade」(アップグレード)ボタンをクリックしてください。



14. 表示されたダイアログで、アップグレードファイル(KeyUpgrade.dat)を検索して、このファイルを選択してください。
    - ◆ 「Open」(開く)ボタンをクリックすると、アップグレードが成功したことを通知するウィンドウがポップアップ表示されます。
    - ◆ ライセンス情報パネルにおけるライセンス数の数字は変更され、アップグレード内容を反映します。

オフラインアップグレードに失敗した場合

オフラインアップグレードに失敗した場合、キーアップグレードファイル(KeyUpgrade.dat)がファイルの転送中に何らかの理由で壊れた可能性があります。対処方法には下記の 2 種類があります。

◆ アップグレードファイルをダウンロードすると、メールが代理店または販売店に送られますが、このときに、オリジナルのファイルの転送に問題が起こった場合に備えて、アップグレードに関する詳細とともに、アップグレードファイルのコピーが送られます。以下はその例です。

```
Offline upgrade email response:

Your CC-Authentication key's upgrade data file is
attached. Please upgrade your CC-Auth key with the
attached file.

Key Info:

* F/W Version: 2.1.204

* Serial number: 0917280288

License Upgrade Info:

* From 1 to 2 concurrent servers

* From 64 to 512 concurrent nodes

Confirmation Info:

* Username: newname

* Password: 1123091022112900

If you have any problem with upgrading your CC-
Authentication key's license, please confirm it online
at http://xxx.xxx.x.xxx using the username and
password above.
```

この時に、代理店・販売店のメールに添付されていたキーアップグレードファイル(KeyUpgrade.dat)のコピーを使って、手順 11(キーステータスユーティリティーの起動)および手順 12(アップグレードをクリック)の操作を繰り返すことができます。

◆ 上記の方法でも問題が解決しない場合は、「Offline email upgrade response」に含まれる情報を使ってオンラインアップグレードを試みることができます。この時、代理店・販売店がエンドユーザーに対して確認の詳細を提供することもできますし、また、エンドユーザーが自身のキーを代理店・販売店に提供することもできます。

注文が期限切れになった場合

ATEN から代理店・販売店に対して、注文が処理可能であるという内容の確認メールが送られると、代理店・販売店は注文処理の期限までに 2 週間の時間が与えられます。この間に注文処理が行われないと、注文の未処理に関するメールが 2 通以上送付されます。

1. 注文はあと 1 週間で期限切れとなります…。
2. 注文はあと 1 日で期限切れとなります…。

注文が期限までに処理されないと、代理店・販売店に注文が期限切れになる旨が通知される、最後のメールが送られます。以下はその内容例です。

Your order has expired and has been cancelled...
If you still wish to add licenses, you must place a new order.

付録 D
外部認証サービス

概要

CC2000 では、内部のユーザーネームとパスワードを使用した認証に加え、サードパーティーのサービスを使用した外部認証にも対応しております。ユーザーを特定するのにサードパーティーサービスが使用されている場合、CC2000 は暗号化された HTTPS(SSL)接続経由で認証ログイン情報を受信します。CC2000 が対応しているサードパーティーの外部認証サーバーは、LDAP、LDAPS、Active Directory、RADIUS、TACACS+、Windows NT Domain、MOTP です。

動作確認済み認証サービス

以下のサービスは CC2000 認証の動作確認が完了しており、本製品との併用が可能です。

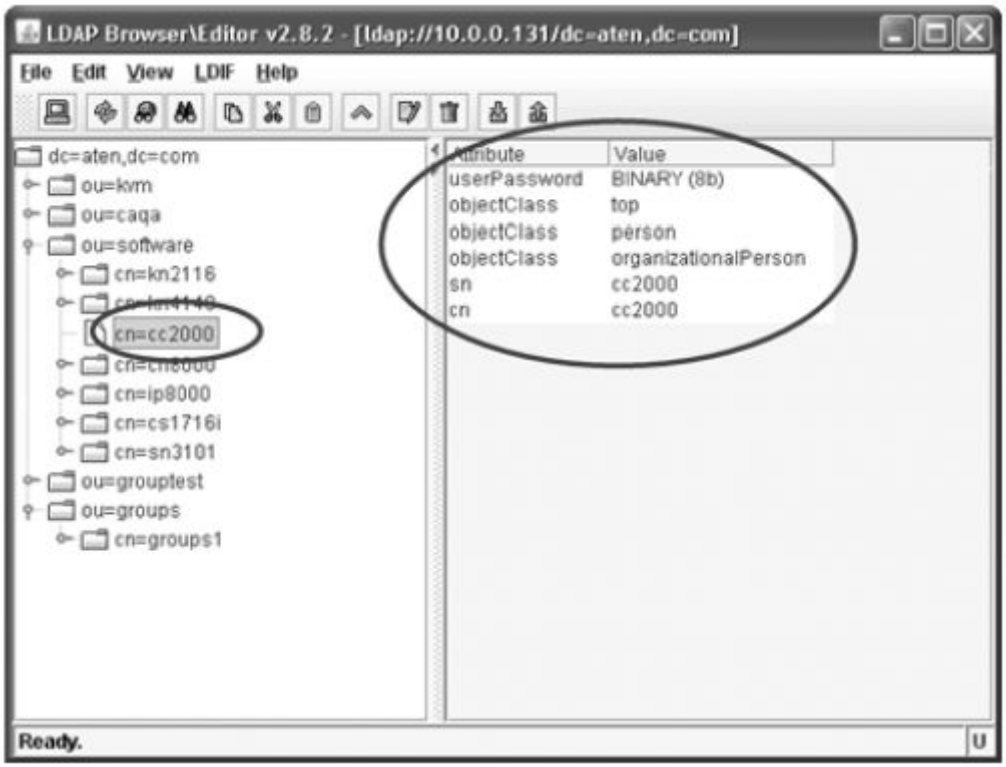
- AD Server ： Microsoft Windows Server 2003
- LDAP ： Microsoft Windows Server 2003、OpenLDAP
- RADIUS ： Microsoft IAS for Windows Server 2003、FreeRADIUS
- TACACS+ ： Microsoft Windows Server 2003 (ClearBox)
- Microsoft Windows NT Domain
- MOTP ： モバイルワンタイムパスワード

LDAP/LDAPS – OpenLDAP 設定例

以下は、外部サーバーには OpenLDAP を使用し、IP アドレスは「192.168.10.100」、サービスポートは 389 番ポートにそれぞれ設定され、サーバー管理者が OpenLDAP ディレクトリーで「cc2000ldap.ldif」というファイルを作成した場合の設定例です。

dn: cn=cc2000,ou=software,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: cc2000
sn: cc2000
userPassword: password

LDAP の管理者は、LDAP ブラウザーで LDAP の定義を確認することができます。確認する場合は、下図で示された部分をご覧ください。



CC2000 の管理者は、この情報を使って外部認証サーバーを追加します（p.219「LDAP」参照）。この場合、各項目に対して以下のように設定を行います。

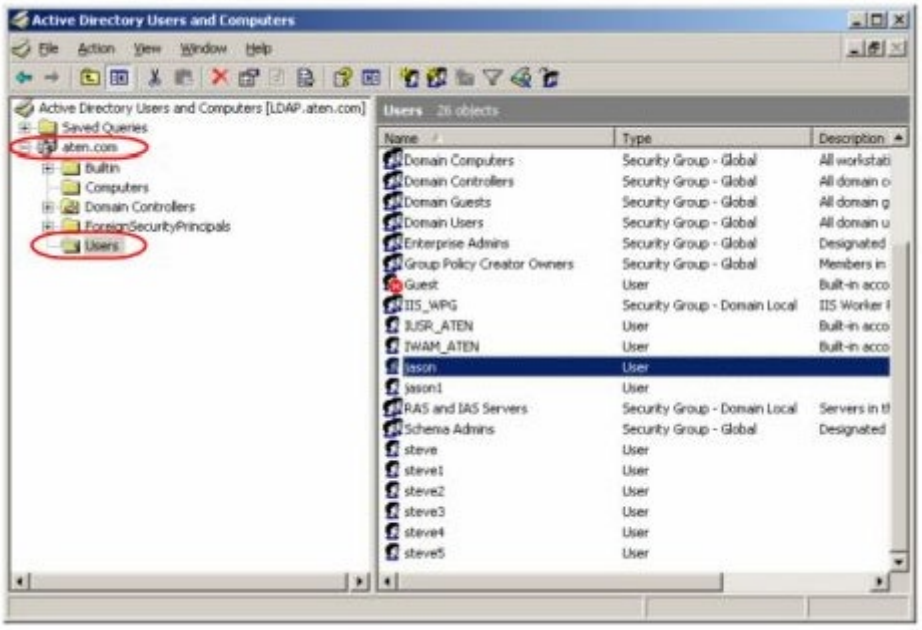
IP ： 192.168.10.100
Port ： 389
BaseDN ： dc=aten,dc=com
UserRDN ： ou=software
Key attribute ： cn
Object class ： person
Full name attribute ： sn

LDAP/LDAPS 認証サーバーが追加されると、CC2000 の管理者は「Browse」ボタンをクリックして、software ディレクトリーで全ユーザーの名前を参照することができます。

Active Directory 設定例

以下は、外部サーバーには Windows Server 2003 上の Active Directory を使用し、IP アドレスを「192.168.10.100」に設定した場合の例です。Windows Server 2003 上での Active Directory の設定は以下の手順で行ってください。

1. [スタート]ボタンをクリックし、[コントロールパネル]→[管理ツール]→[Active Directory ユーザーとコンピューター]で、ドメイン(例:aten.com)から「Users」(ユーザー)を選択してください。下図のような画面が表示されます。



CC2000 の管理者は、この情報を使って外部認証サーバーを追加します(p.217 参照)。この例では、各項目に対して以下のように設定を行います。

IP : 192.168.10.100
UserRDN : cn=users

Active Directory 認証サーバーが追加されると、CC2000 の管理者は「Browse」(参照)ボタンをクリックして、Users ディレクトリーで全ユーザーの名前を参照することができます。

RADIUS 設定例

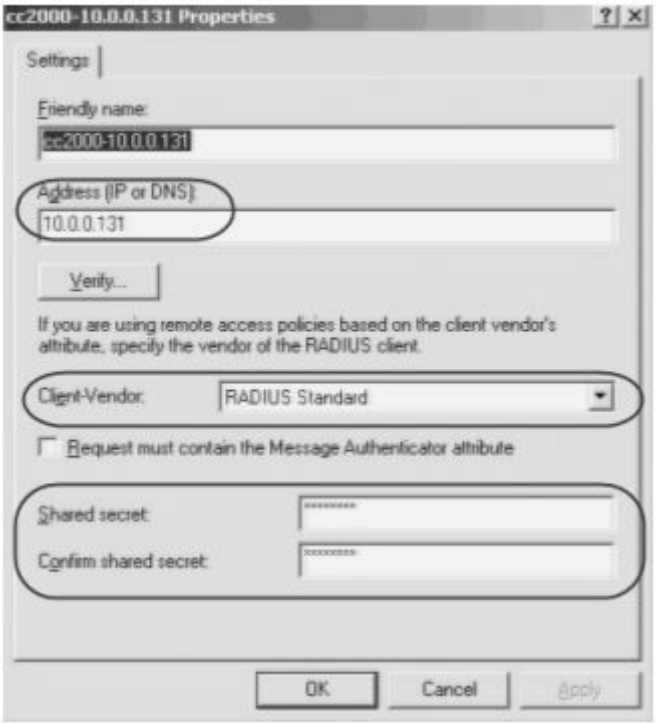
以下は、外部サーバーには RADIUS：Microsoft IAS for Windows Server 2003 を使用し、IP アドレスを「10.0.0.100」に設定した場合の設定例です。

1. [スタート]ボタンをクリックし、[コントロールパネル]→[管理ツール]→[インターネット認証サービス]を起動してください。

2. 表示された画面で、「**RADIUS Client**」(RADIUS クライアント)を右クリックしてください。

3. 「**New RADIUS Client**」(新規 RADIUS クライアント)を選択してください。

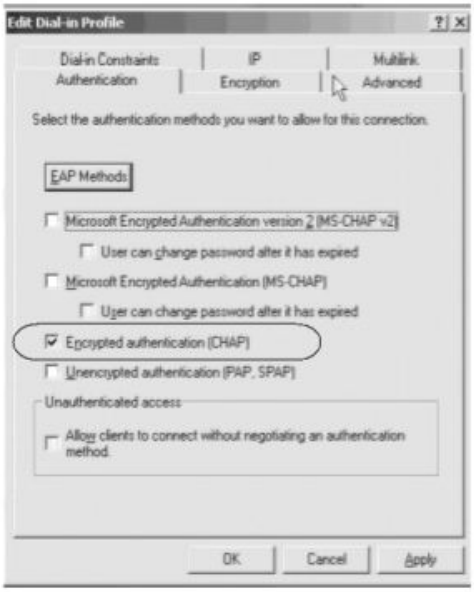
4. 表示された画面で、「Friendly name」(フレンドリ名)欄に例えば「cc2000-10.0.0.131」という文字列を入力し、「**Next**」(次へ)ボタンをクリックしてください。下図のような画面が表示されます。



5. 上図の例では、CC2000 の IP アドレスは「10.0.0.131」に、クライアントベンダーは「RADIUS Standard」にそれぞれ設定されています。「Shared secret」(共有シークレット)欄には「**password**」という文字列を設定してください。

6. 「OK」ボタンをクリックすると、インターネット認証サービスの画面に戻ります。左パネルで、「Remote Access Policies」(リモートアクセスポリシー)をクリックし、メインパネルで「Use Windows authentication for all users」(全てのユーザーに対して Windows の認証を使用する)を右クリックして、「プロパティー」を選択してください。

7. 表示された画面で、「Edit Profile」(プロファイルの編集)ボタンをクリックし、「Authorization」タブを選択してください。下図のような画面が表示されます。



8. この例では、暗号化認証には CHAP を使用します。

CC2000 の管理者は、この情報を使って外部認証サーバーを追加します(p.220 参照)。この場合、各項目に対して以下のように設定を行います。

IP : 10.0.0.100
Authentication type : CHAP
Shared secret : password

RADIUS 認証サーバーが追加されると、CC2000 の管理者がユーザーアカウントを追加する際に、RADIUS サーバーの、[スタート]→[コントロールパネル]→[管理ツール]→[コンピューターの管理]→[ローカル ユーザーとグループ]のログインネームのユーザーの部分で設定された名前を使用しなければなりません。

TACACS+設定例

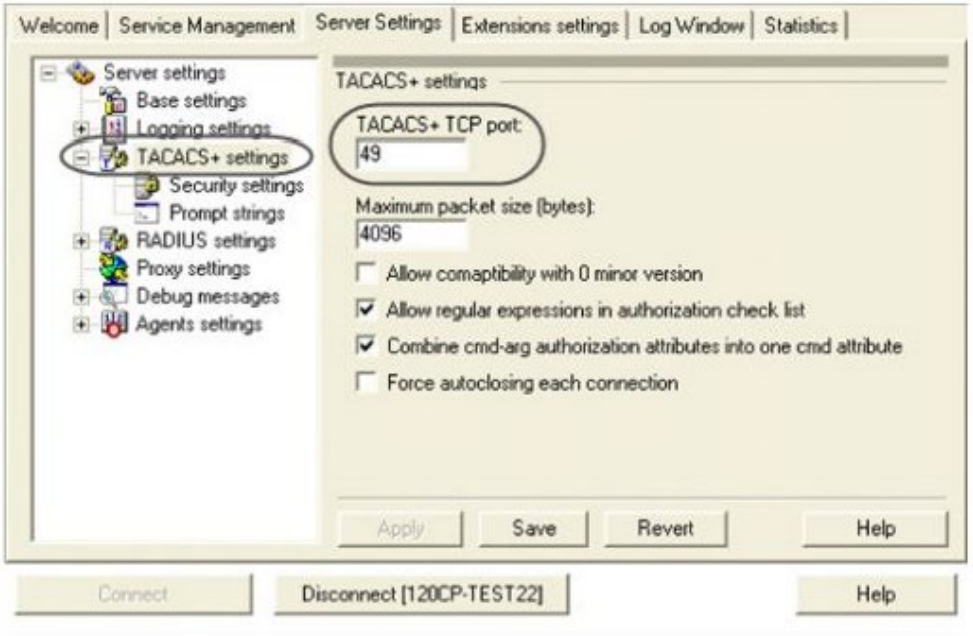
以下は、外部サーバーには TACACS+：Microsoft IAS for Windows Server 2003(Clear Box)を使用し、IP アドレスを「10.0. 0.100」に設定した場合の設定例です。

1. [スタート]ボタンをクリックし、[全てのプログラム]→[ClearBox RADIUS TACACS+ Server]→[Server Manager]を起動してください。

2. 表示された画面で、「**Connect**」ボタンをクリックしてください。

3. ClearBox RADIUS TACACS+ Server をインストールした際に設定したパスワードを入力してください。

4. 「ClearBox Server Configurator」画面が表示されたら、「**Server Settings**」タブを選択してください。下図のような画面が表示されます。

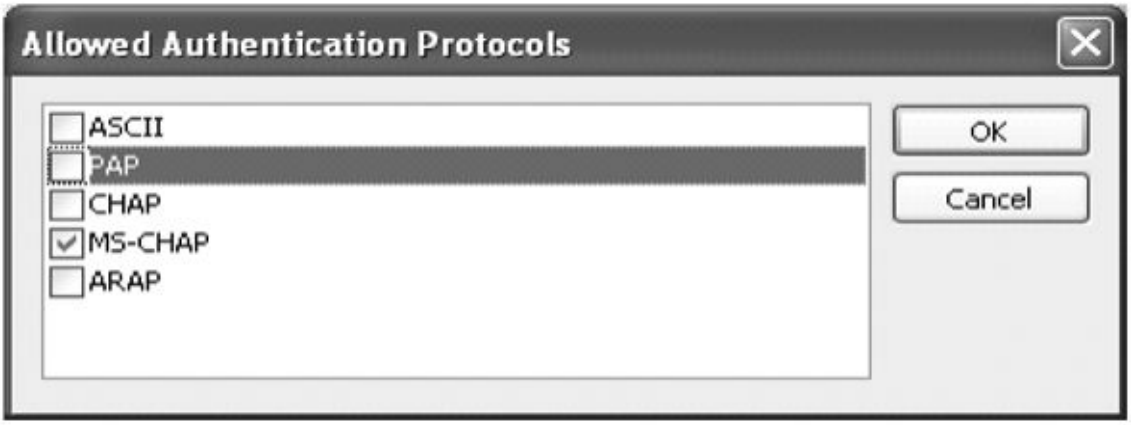


5. この例では、TACACS+サービスポートとして 49 番のポートを使用します。

6. [スタート]ボタンをクリックし、[全てのプログラム]→[ClearBox RADIUS TACACS+ Server]→[Configurator]を起動してください。

7. 表示された画面の左パネルで、「Realms」→「def」を選択し、「Authentication」タブを選択してください。

8. 「Allowed Protocols…」ボタンをクリックしてください。下図のような画面が表示されます。



9. この例では、許可された認証プロトコルに MS-CHAP を使用します。

10. 「ClearBox Server Configurator」画面に戻ったら、左パネルで「Data Sources」→「users」を選択してください。

11. 表示された画面のメインパネルに、「general.mdb」ファイルへのパスが記された MS Access の項目欄があります。このファイルに含まれたアカウントは MS Access で生成されたものです。

CC2000 の管理者は、この情報を使って外部認証サーバーを追加します(p.220 参照)。この場合、各項目に対して以下のように設定を行います。

IP ： 10.0.0.100
Port ： 49
Authentication type ： MSCHAP
Shared secret ： *ClearBox RADIUS TACACS+ Server をインストールした際に設定したパスワード*

TACACS+認証サーバーが追加されると、CC2000 の管理者がユーザーアカウントを追加する際に、TACACS+サーバーの general.mdb ファイルで設定された名前を使用しなければなりません。

NT Domain 設定例

以下は、外部サーバーには Microsoft NT Domain を使用し、ドメイン名を「QA_NT_SERVER」に設定した場合の設定例です。

[スタート]ボタンをクリックし、[プログラム]→[管理ツール]→[ドメインユーザーマネージャー]を起動してください。下図のような画面が表示されます。

CC2000 の管理者は、この情報を使って外部認証サーバーを追加します(p.220 参照)。この場合、各項目に対して以下のように設定を行います。

Server IP ： QA_NT_SERVER

NT Domain サーバーが追加されると、CC2000 の管理者がユーザーアカウントを追加する際に、ドメインユーザーマネージャーで設定された名前を使用しなければなりません。

LDAP によるグループ認証の設定例

例 1

以下は、p.364 で説明したケースと同様、外部サーバーとして Windows Server 2003 上にインストールされた OpenLDAP を使用した場合の例です。

1. CC2000 の「ユーザー管理」タブから、「認証サービス」→「認証サーバー」を選択してください。

2. タイプが「OpenLDAP server」の項目を選択し、「**グループ権限**」をクリックしてください。

3. 「グループにメンバー属性を与える」のラジオボタンをクリックしてください。

4. パネル右上の「**追加**」ボタンをクリックしてください。

5. この例では、「groups1」グループを追加します。下図のような画面が表示されます。

OpenLDAP の管理者は、この名前(本マニュアルの例では「groups1」)を使って、CC2000 サーバーで作成されたものと同じ名前を持つグループを OpenLDAP でも作成します。作成手順は以下の通りです。

1. 「core.schema」ファイルを開いてください。必要な部分のデフォルトの設定は以下の通りです。

```
attributetype ( 2.5.4.31 NAME 'member'
    DESC 'RFC2256: member of a group'
    SUP distinguishedName )
objectclass ( 2.5.6.9 NAME 'groupOfNames'
    DESC 'RFC2256: a group of names (DNs)'
    SUP top STRUCTURAL
    MUST ( member $ cn )
    MAY ( businessCategory $ seeAlso $ owner $ ou $ o $ description ) )
```

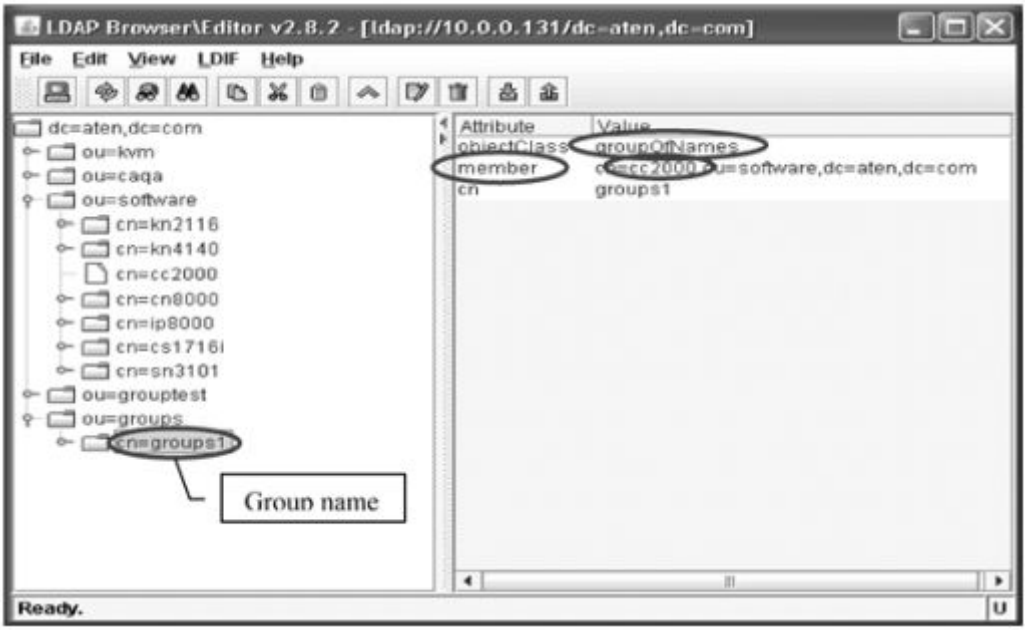
2. 「cc2000ldap.ldif」ファイルを開いて、以下を参考にしながら「groups1」の定義を追加し、CC2000 のユーザーアカウントを「groups1」に登録してください。

```
dn: cn=groups1,ou=groups,dc=aten,dc=com
objectclass: groupofnames
member: cn=cc2000,ou=software,dc=aten,dc=com
cn: groups1
```

注意:

1. 「dn: cn=」の後には、CC2000 サーバーの「グループ権限」メニューで作成された実際のグループ名を設定してください。
2. 「objectclass:」の後には、CC2000 サーバーでグループが作成された際に「Object class」に入力された名前と同じものを設定してください。名前が一致するように、このファイルにあるデフォルトエントリーを変更してください。
3. 「member: cn=」の後には、実際のログインユーザーの名前と同じものを設定してください。

3. LDAP ブラウザーでグループの定義を確認してください。下図で示された部分を確認してください。



4. 上記の例では、「cc2000」という名前のメンバーを「groups1」グループに登録しました。他のメンバーもグループに追加する場合は、ファイルを同様の方法で編集してください。以下、設定例です。

member: cn=***cc2000-1***,ou=software,dc=aten,dc=com

member: cn=***cc2000-2***,ou=software,dc=aten,dc=com

設定が完了すると、LDAP/LDAPS サーバーで認証される CC2000 ユーザーは、グループに割り当てられた操作権限に基づいて認証されます。

例 2

デフォルトでは、OpenLDAP はグループ関連のスキーマに対して「グループにメンバー属性を与える」の設定のみをサポートしています。これは例 1 で使用した設定です。

別の LDAP サーバーで使用する代替設定は「ユーザーはメンバーの特性があります」の項目です。これは、スキーマを拡張することによって設定を行うもので、OpenLDAP でもサポートされています。

以下は、p.373 で説明したケースと同様、外部サーバーとして Windows Server 2003 上にインストールされた OpenLDAP を使用した場合の例です。

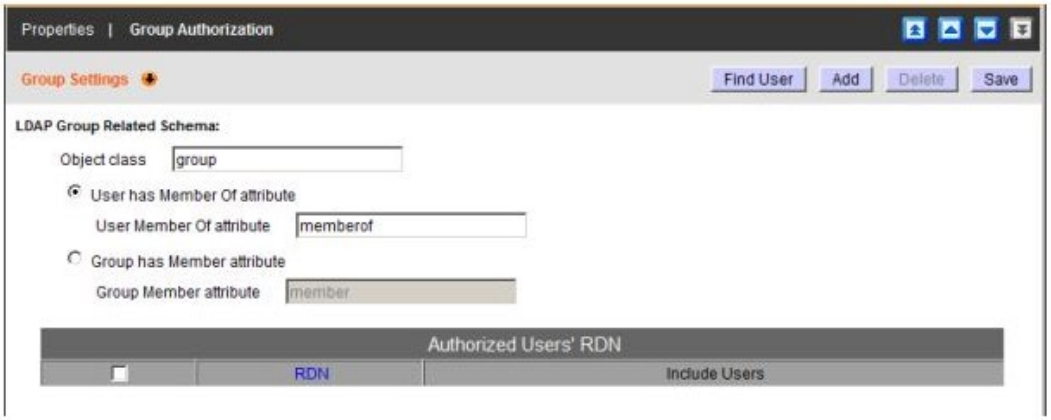
1. CC2000 の「ユーザー管理」タブから、「認証サービス」→「認証サーバー」を選択してください。

2. タイプが「OpenLDAP server」の項目を選択し、「**グループ権限**」をクリックしてください。

3. 「ユーザーはメンバーの特性があります」のラジオボタンをクリックしてください。

4. パネル右上の「**追加**」ボタンをクリックしてください。

5. この例では、「**groups1**」グループを追加します。下図のような画面が表示されます。



OpenLDAP の管理者は、この名前(本マニュアルの例では「groups1」)を使って、CC2000 サーバーで作成されたものと同じ名前を持つグループを OpenLDAP でも作成します。作成手順は以下の通りです。

1. 「core.schema」ファイルを開いてください。必要な部分のデフォルトの設定は以下の通りです。

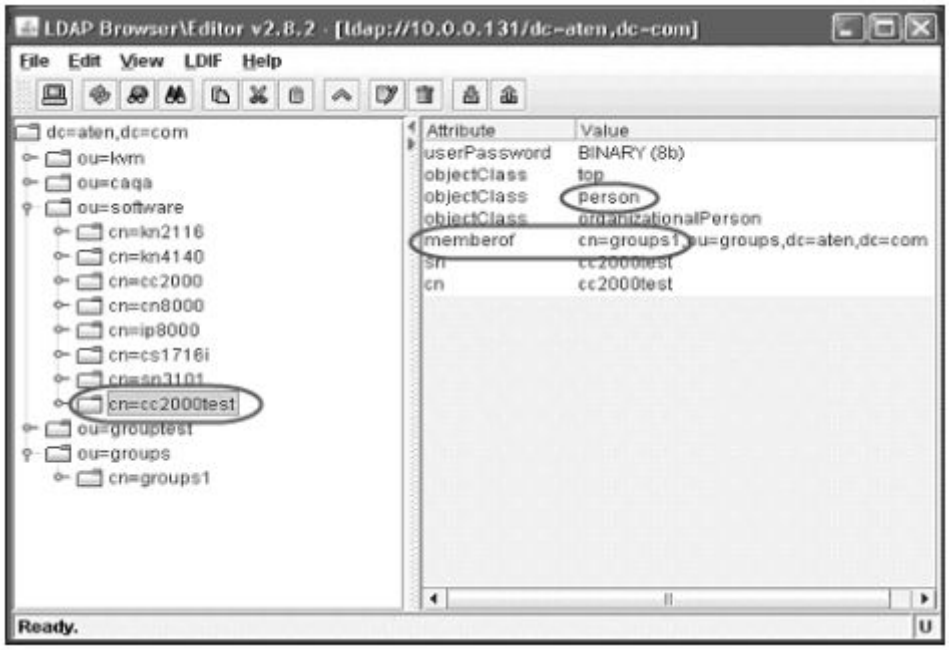
```
attributetype ( 1.2.840.113556.1.2.102
    NAME 'memberof'
    DESC 'RFC2256: member of a group'
    SUP distinguishedName )
objectclass ( 1.2.840.113556.1.5.9
    NAME 'person'
    SUP organizationalPerson
    STRUCTURAL
    MUST ( cn )
    MAY ( userPassword $ description $ sn $ mail $ memberof ) )
```

2. 「cc2000ldap.ldif」ファイルを開いて、以下を参考にしながら「groups1」の定義を追加し、CC2000 のユーザーアカウントを「groups1」に登録してください。

```
dn: cn=cc2000test,ou=software,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: cc2000test
sn: cc2000test
memberof: cn=groups1,ou=groups,dc=aten,dc=com
userPassword: password
```

注意：	1. 「dn: cn=」の後には、実際のログインユーザーの名前と同じものを設定してください。 2. 「objectclass:」の後には、拡張されたスキーマの「NAME」で入力された名前と同じものを設定してください。 3. 「member: cn=」の後には、CC2000 サーバーの「グループ権限」メニューで作成された実際のグループ名を設定してください。

3. LDAP ブラウザーでグループの定義を確認してください。下図で示された部分を確認してください。



4. 他にもグループに登録したいユーザーアカウントがある場合は、手順 2 の操作を繰り返してください。

設定が完了すると、LDAP/LDAPS サーバーで認証される CC2000 ユーザーは、グループに割り当てられた操作権限に基づいて認証されます。

Active Directory によるグループ認証の設定例

以下は、p.367 で説明したケースと同様、外部サーバーとして Windows Server 2003 上にインストールされた Active Directory を使用した場合の例です。

1. CC2000 の「ユーザー管理」タブから、「認証サービス」→「認証サーバー」を選択してください。

2. タイプが「Active Directory server」を選択し、「**グループ権限**」をクリックしてください。

3. 「グループ権限の追加」画面で「**CC2000GP**」グループを追加します。

Active Directory の管理者は、この名前(本マニュアルの例では「CC2000GP」)を使って、CC2000 サーバーで作成されたものと同じ名前を持つグループを Active Directory でも作成します。作成手順は以下の通りです。

1. [スタート]ボタンをクリックし、[コントロールパネル]→[管理ツール]→[Active Directory ユーザーとコンピューター]でドメイン(例:CA-QA.com)を選択してください。

2. 左パネルで、「**Domain Controllers**」を右クリックし、「**新規作成**」を選択した後で「**グループ**」を選択してください。

3. 表示されたダイアログで、グループ名(例:CC2000GP)を入力してください。下図のような画面が表示されます。

4. 右パネルで、「CC2000GP」を右クリックし、「プロパティー」を選択した後で「Members」を選択してください。下図のような画面が表示されます。

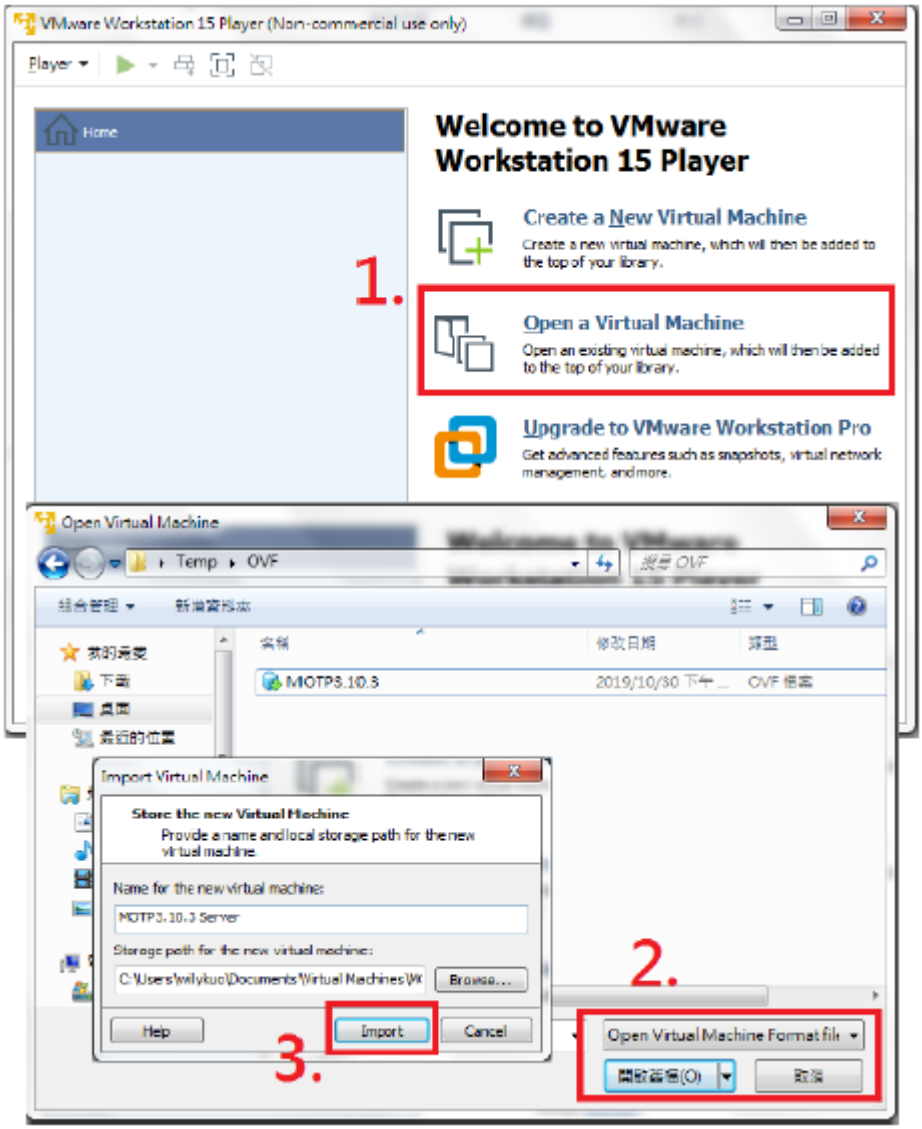
5. 「Add」ボタンをクリックしてください。

表示されたダイアログでは、メンバーをグループに追加することができます。これらのメンバーは「Users」フォルダーにあるアカウントから選択されたものです(元画面の左パネルを参照)。

MOTP 設定

MOTP VM サーバーのセットアップ

VMware Workstation Player または VMware Player を使って、「Open a Virtual Machine」(仮想マシンを開く)をクリックし、MOTP サーバーの ovf/ova ファイルを開いて、システムのインポート処理を開始してください。



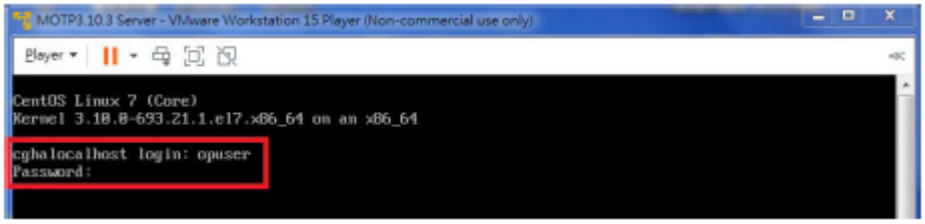
システム組み込みの「opuser」を使ったセットアップ

「opuser」は、システムに組み込まれたアドミニストレーターアカウントです。初回セットアップ時には、このアカウントを使って IP アドレスを設定し、ウェブブラウザーを介して MOTP VM システムに接続することができます。

IP アドレスの設定

MOTP VM を開いてください。初期画面にはログインに関するヒントが表示されます。

アカウント名には「opuser」を、パスワードには「op123pass」をそれぞれ入力して、ログインしてください。



1. MOTP サーバーの IP を動的 IP で検索してください。
   デフォルトで、MOTP サーバーは、DHCP サーバー経由で IP を自動的に取得します。取得済み IP を検索するには、ifconfig と入力してください。

2. MOTP サーバーに静的 IP を設定してください。
   次の点について、事前に確認を行ってください。
   - ◆ 使用するアドレス(例:192.168.1.200)が、最初の VM ネットワークカードで利用可能であること。
   - ◆ 管理者がセットアップに使用するコンピューターも、この IP アドレスに接続できること。

   最初のネットワークカードの MOTP の初期画面が 192.168.1.200 に設定したと想定し、次のように操作を行ってください。

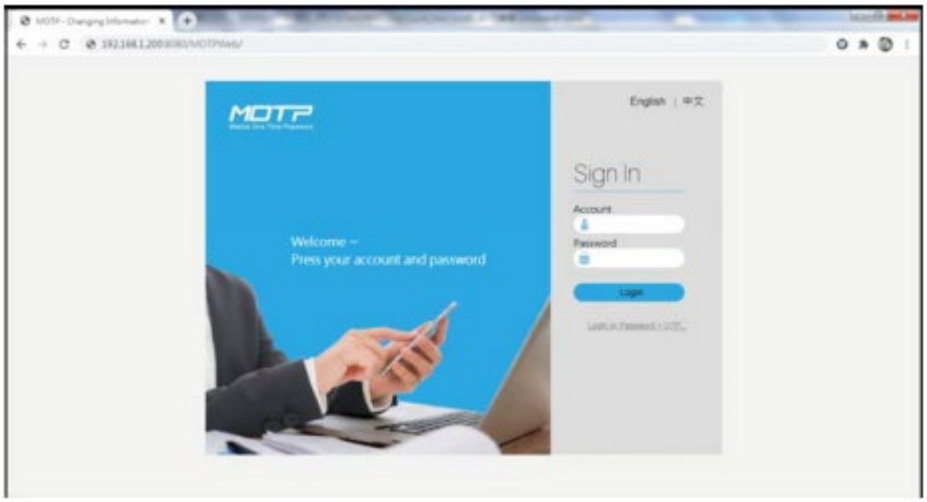
1. 次を入力してください。
   sudo /sbin/ifconfig ens0 192.168.1.200 netmask 255.255.255.0

2. opuser のパスワード(op123pass)を入力してください。

   ネットワークカードの名前は、ifconfig コマンドを使って確認することができます。

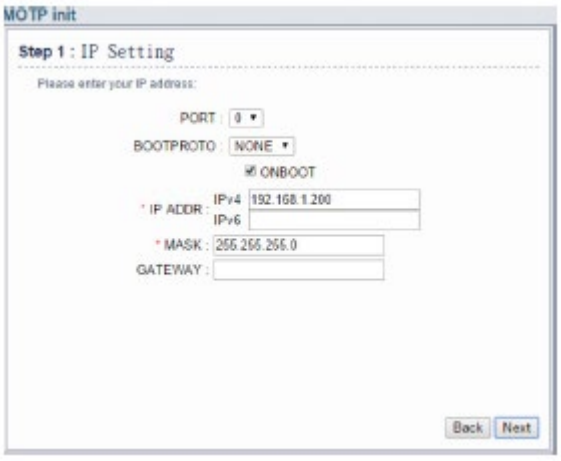
MOTP サーバーの初期化

IP アドレスを設定したらブラウザーを起動し、次のフォーマットに合わせて URL を入力して、MOTP サーバーの初期化を行ってください。
http://192.168.1.200:8080/MOTPWeb



アカウント名に「admin」を、パスワードに「admin」を、それぞれ入力してください。

手順 1:IP 設定



次の情報を設定してください：

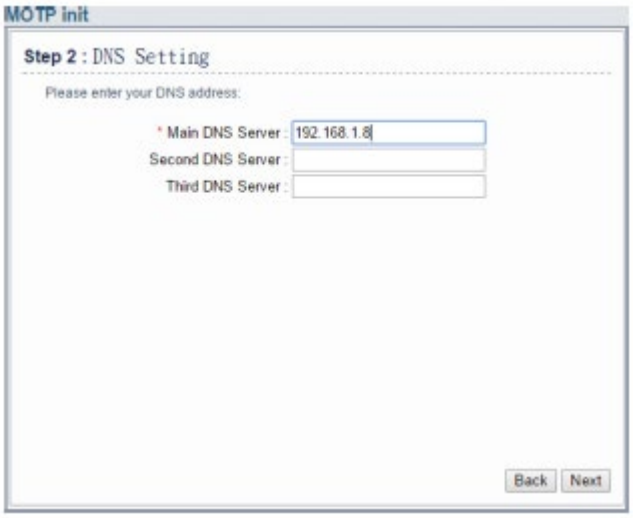
Bootproto: NONE

IPV4: 192.168.1.200

Mask: 255.255.255.0

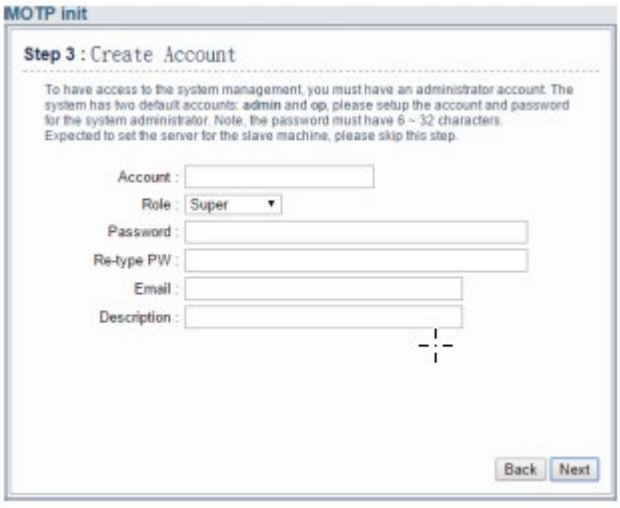
赤い＊印が付いた項目は、必須項目です。

手順 2:DNS 設定



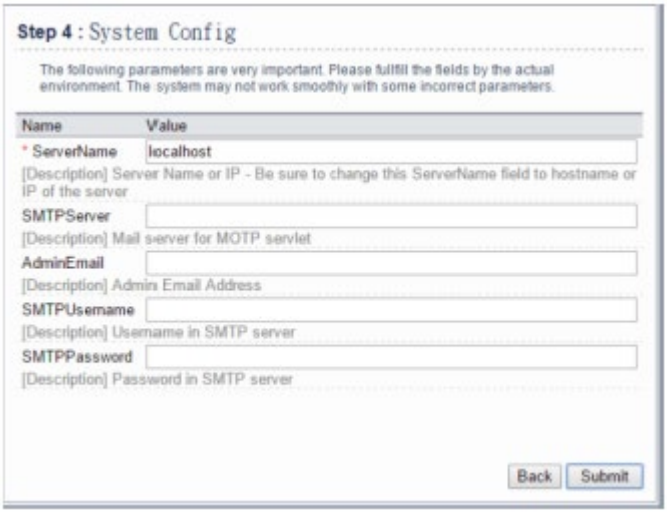
メイン DNS サーバーの IP を設定してください。

手順 3:アカウント作成



注意:	この手順は省略して、後から設定を行うこともできます。

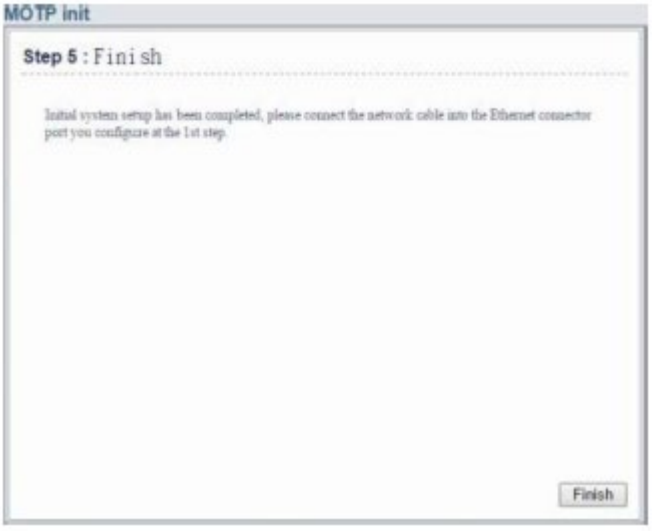
手順 4:システム設定



注意:	この手順は省略して、後から設定を行うこともできます。

手順 5:完了

これで、初期化が完了しました。



MOTP サーバーの設定

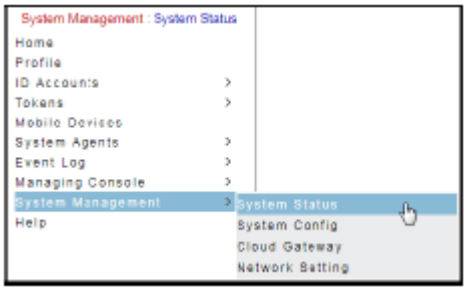
MOTP サーバー（例：http://192.168.1.200:8080/MOTPWeb）にアクセスし、アカウント名（admin）とパスワード（admin）を使ってログインしてください。

そうすると、下図のようなサーバーの管理画面が表示されます。

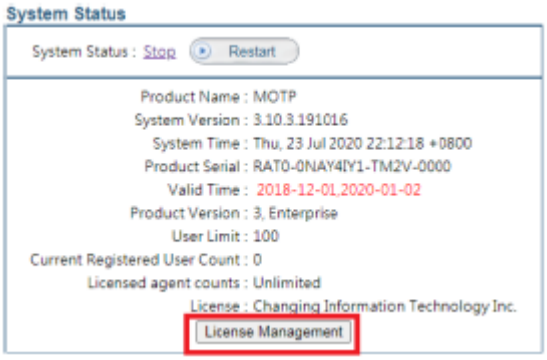
ライセンスのインポート

MOTP サーバーのサービスを有効化するには、CHANGING Information Technology Inc.（https://www.changingtec.com/EN/）からライセンス（*.pem）とトークン（*.csv）を購入する必要があります。ライセンスとトークンがお手元に届きましたら、これらの情報を次の手順に従ってインポートしてください。

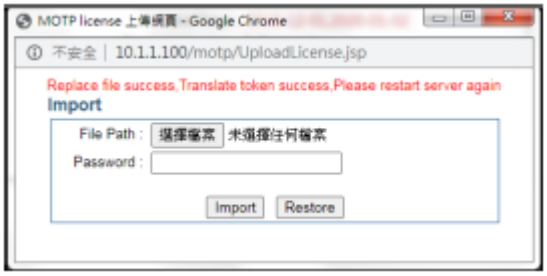
1. 「System Management」（システム管理）→「System Status」（システムの状態）に進んでください。



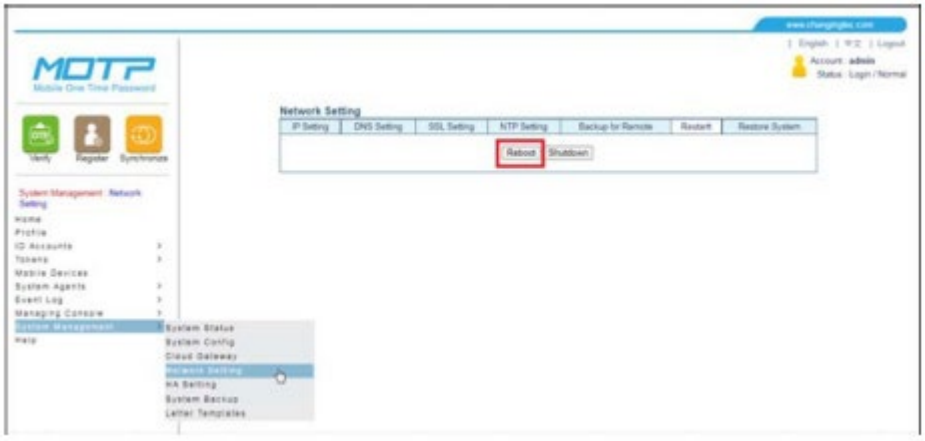
2. 「System Status」（システムの状態）で、「License Management」（ライセンスの管理）をクリックして購入済みライセンスのインポートを開始してください。



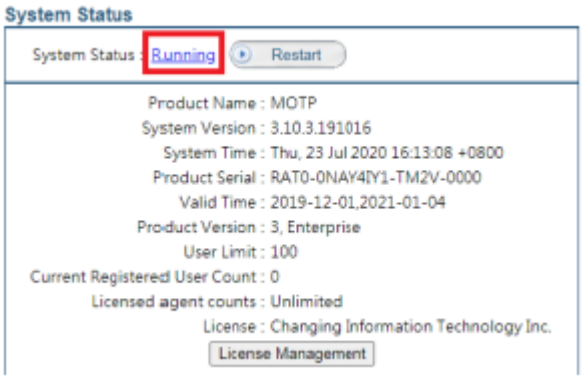
3. 「Browse」(参照)をクリックしてライセンスファイル(*.pem)を選択したら、CHANGING 社から発行されたパスワードを入力し、「Import」(インポート)をクリックして、ライセンスをアップグレードしてください。



4. 「System Management」(システム管理)→「Network Setting」(ネットワーク設定)→「Restart」(再起動)に進み、「Reboot」(再起動)をクリックして、MOTP サーバーの再起動を行ってください。



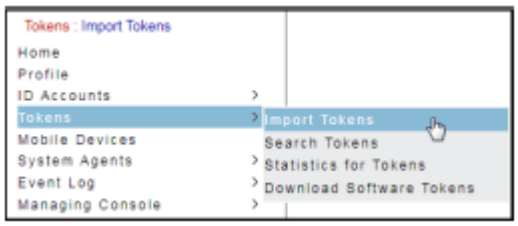
5. 再起動が完了したら、ログインして「System Status」(システムの状態)にアクセスし、ライセンスが有効でサービスが起動していることを確認してください。



トークンのインポート

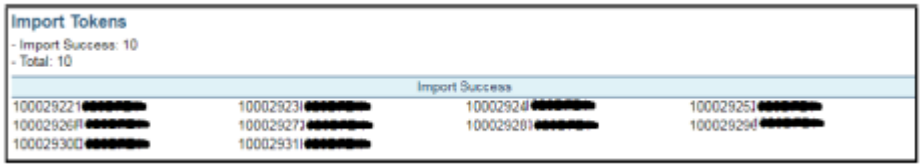
トークンライセンス(*.csv / *.dat)を使うと、ユーザーがアプリケーションサーバーにサインインする際に MOTP クライアントがワンタイム・パスコードを受け取るようになります。トークンライセンスをインポートするには、次の手順に従って操作を行ってください。

1. 「Tokens」(トークン)→「Import Tokens」(トークンのインポート)に進んでください。



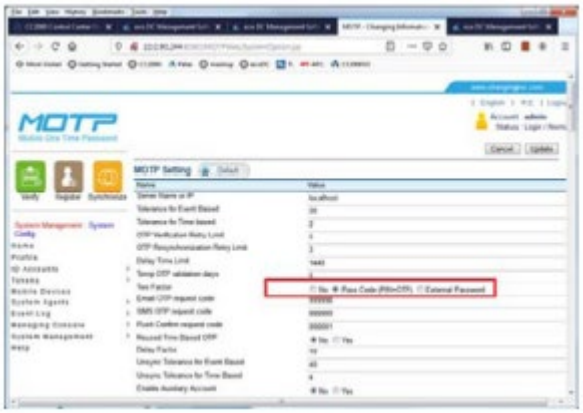
2. 「Browse」(参照)をクリックしてトークンライセンスを選択したら、「Submit」(送信)をクリックしてインポートを行ってください。

3. インポートが完了すると、インポート済みトークンの一覧を確認することができます。

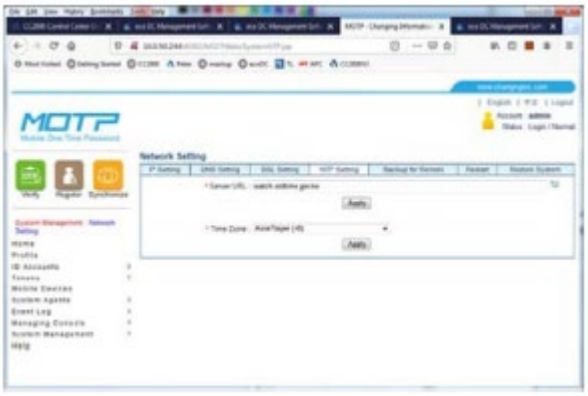


注意:	◆ MOTP VM サーバーのセットアップが完了したら、「Two Factor」(二要素)に対する MOTP サーバーが「Pass Code (PIN+OTP)」(パスコード

(PIN＋OTP))に設定されていることを確認してください(デフォルトでは「No」が選択されています)。「System Management」(システム管理)→「System Config」(システム設定)に進んでください。下図はその例です。

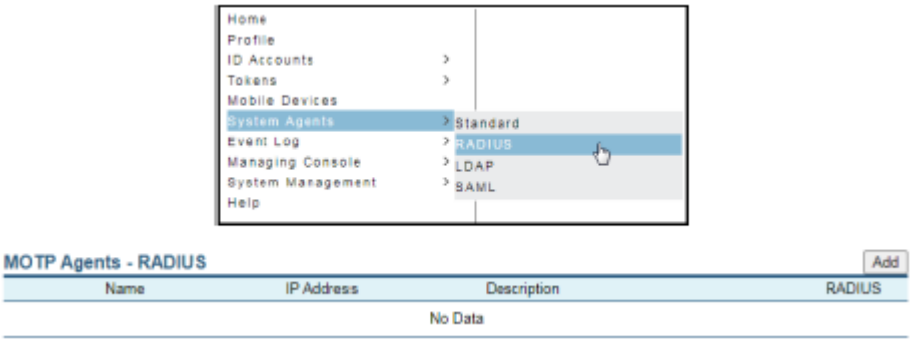


◆ 確認の目的で、MOTP サーバーは NTP サーバーと同期する必要があります。このような場合には、「System Management」(システム管理)→「Network Setting」(ネットワーク設定)→「NTP Setting」(NTP 設定)に進んで NTP 設定を確認してください。下図はその例です。

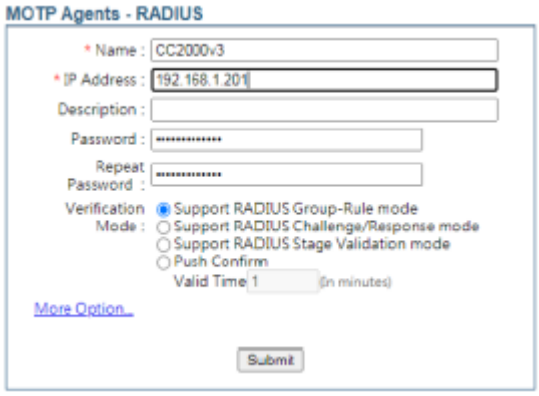


RADIUS の設定

1. 「System Agents」(システムエージェント)→「RADIUS」に進んでください。

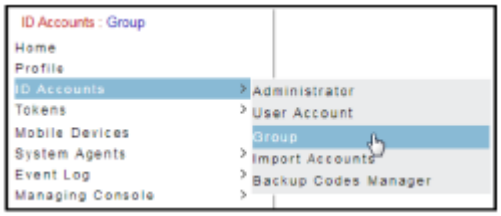


2. 「Add」(追加)をクリックして、CC2000 のサーバーエントリーを作成してください。
3. CC2000 サーバー(MOTP エージェント)に関する情報を入力し、CC2000 が MOTP サーバーにアクセスするのに必要となるパスワードを設定してください。パスワードが CC2000 における共有シークレットと同じであることを確認してください。

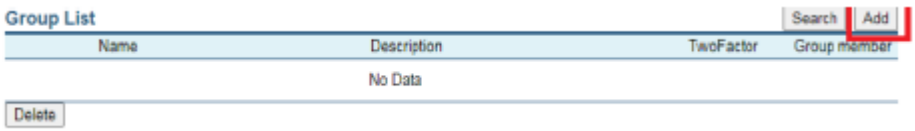


トラストグループの作成

1. 「ID Accounts」(ID アカウント)→「Group」(グループ)に進んでください。



2. 右上にある「Add」(追加)をクリックして、グループを作成してください。



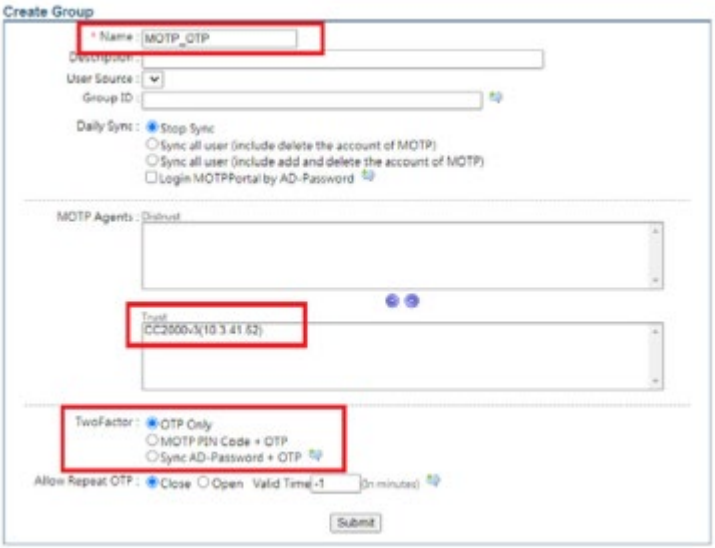
3. グループ名を入力してください。MOTP エージェントでは、CC2000 を「Distrust」(信頼しない)から「Trust」(信頼する)に移動させてください。二要素認証では、「OTP Only」(OTP のみ。

CC2000 ログインにユーザーネームと OTP のみを使用）を選択してください。

「MOTP PIN Code + OTP」（MOTP PIN コード＋OTP）は、CC2000 へのログイン時に、ユーザーネーム、OTP、および PIN（デフォルト = 000000）が必要になることを意味します。

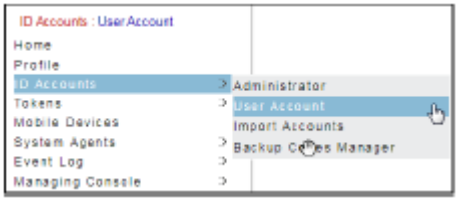
注意:	PIN を変更する場合は、MOTP のユーザーポータル（http://192.168.1.200/MOTPPortal）に進んで、プロファイルカテゴリーで変更を行ってください。

「Sync AD-Password + OTP」（AD パスワード＋OTP を同期する）は、CC2000 へのログイン時に、管理者のユーザーネーム、OTP、および管理者のパスワードが必要になることを意味します。

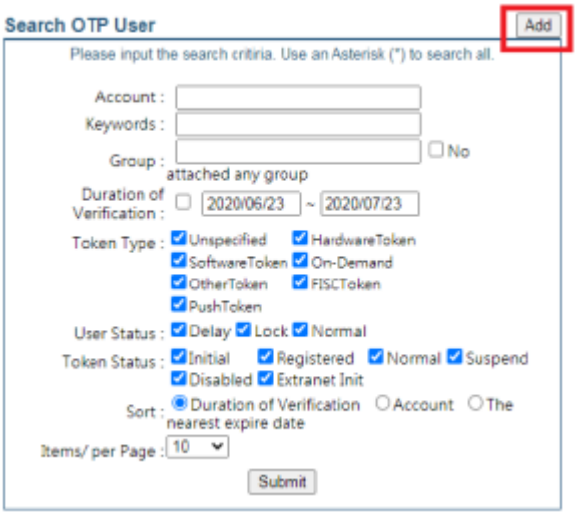


アカウントの手入力作成

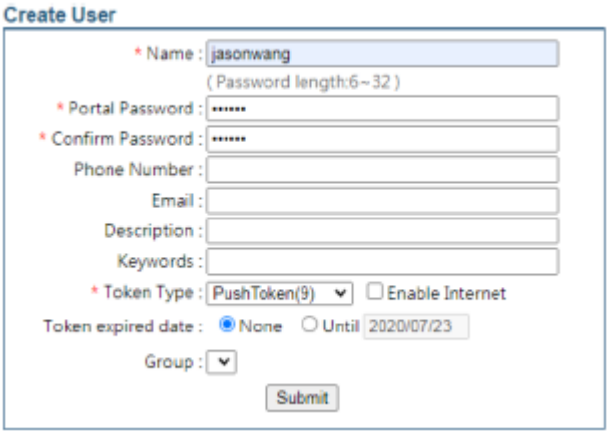
1. 「ID Accounts」（ID アカウント）→「User Account」（ユーザーアカウント）に進んでください。



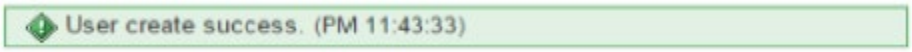
2. 右上にある「Add」（追加）をクリックして、ユーザーアカウントを作成してください。



3. 各欄に情報を入力することでアカウントを作成してください（ここで入力した情報は、後で、MOTP クライアントポータルへのサインインに必要になります）。また、既にインポートしたトークンの種類を選択してください。



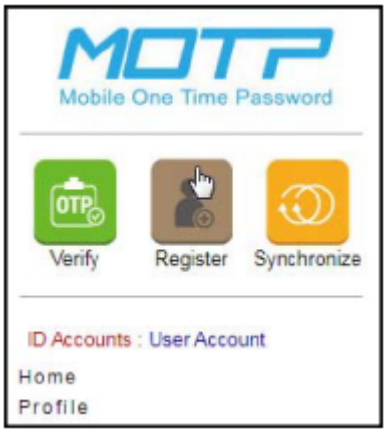
登録に成功すると、次のようなメッセージを確認することができます。



ソフトウェアトークンの登録

1. モバイルデバイスのアプリケーションストアで「MOTP Client」を検索したら、アプリをダウンロードして起動してください。

2. （コンピューターの）MOTP 管理画面で「Register」（登録）をクリックしてください。



3. トークンの登録：
   トークンの種類としてソフトウェアトークンを選択してください。
   「Account」（アカウント）にユーザーアカウントを入力したら、「Get Initial Key」（初期キーを取得）をクリックして、生成された初期キーを表示してください（中央上部）。
   モバイルデバイスで、MOTP クライアントのモバイルアプリを起動したら、利用可能な項目に初期キーを入力してください。

4. シリアル番号（SN）とデバイス ID が MOTP Client モバイルアプリで生成されますので、これらの文字列を MOTP サーバーで入力し、「Submit」（送信）をクリックして登録を完了してください。

5. 登録後は、OTP 認証と同期が必要になります。MOTP 管理画面の左側にある「Synchronize」（同期）をクリックしてください。

6. サーバーの画面で、作成したユーザーアカウントを入力したら、「Get Serial List」（シリアルリストの取得）をクリックしてください。そうすると、SN 欄が自動的に入力されます。
7. 同期することを目的として MOTP Client から取得した「OTP」および「Sync Code」（同期コード）を各欄に入力してください。
   同期に成功すると、次のようなメッセージを受信します。

8. 既に OTP 認証と同期を行っている場合は、MOTP 管理画面で「Verify」（検証）をクリックしてください。


MOTP
Mobile One Time Password
Verify
Register
Synchronize
Verify OTP
Home
Profile
ID Accounts
Verify OTP
* Account : jasonwang
* OTP : 715662
Submit
Statement
Please input the OTP on the mobile phone.
797974

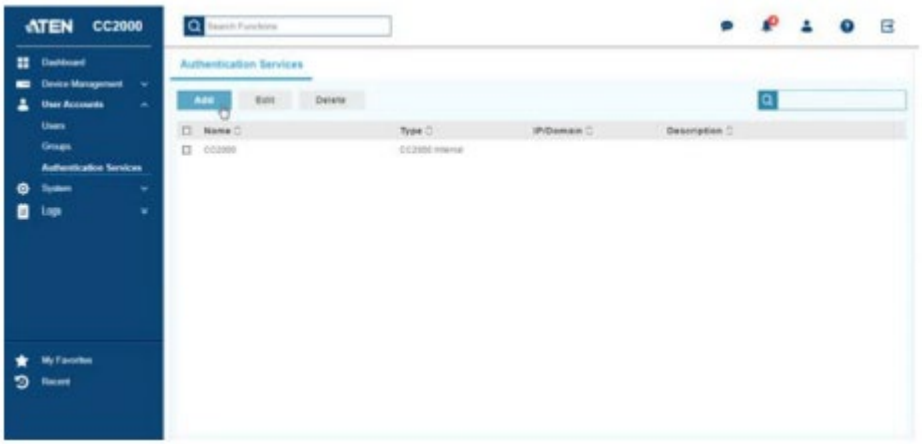
CC2000 における MOTP 認証サービス

これ以降の内容は、CC2000 における MOTP 認証サービスのセットアップ、また、MOTP 認証を行うユーザーの作成、および、これらのユーザーが MOTP 認証を介してログインする方法を例として示します。

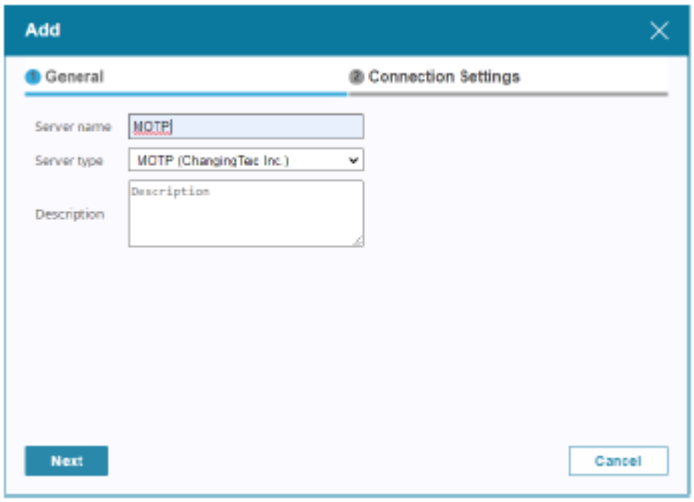
MOTP 認証サービスの設定

CC2000 に管理者でログインしていることを確認してください。

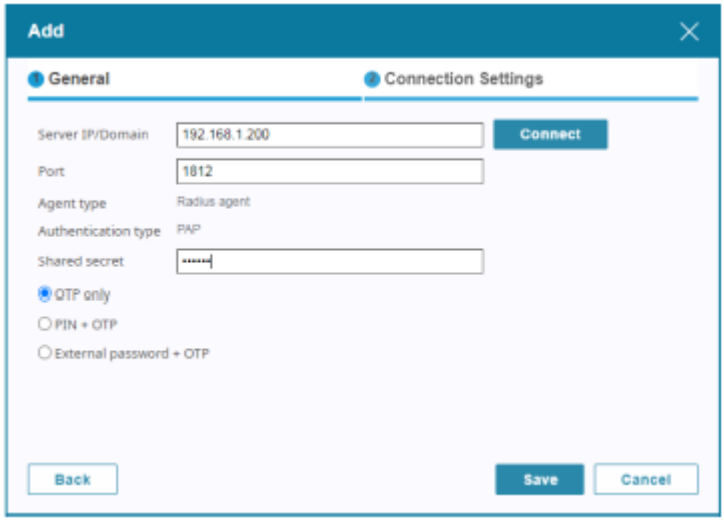
1. サイドバーのメニューで、「User Accounts」(ユーザーアカウント)→「Authentication Services」(認証サービス)に進んでください。



2. 次のダイアログボックスで「Add」(追加)をクリックしてください。



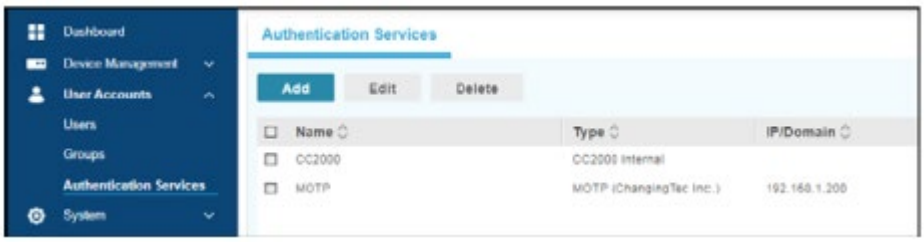
3. サーバー名を入力し、サーバータイプに「MOTP (ChangingTec Inc)」を選択したら、「**Next**」(次へ)をクリックしてください。
4. MOTP サーバーの IP アドレスおよび MOTP サーバーの RADIUS エージェントで入力した共有シークレットを入力してください。



注意:	サーバータイプで「Dual Authentication」(二要素認証)が選択されている場合、CC2000 はユーザーに対してログイン認証と OTP 認証の両方を要求します。

保存する前に接続をテストする場合は、「Server IP/Domain」(サーバーIP/ドメイン)欄の後ろにある「**Connect**」(接続)ボタンをクリックしてください。

5. 「**Save**」(保存)をクリックして、認証サービスを保存してください。そうすると、下図の例のようにサービス一覧に表示されます。

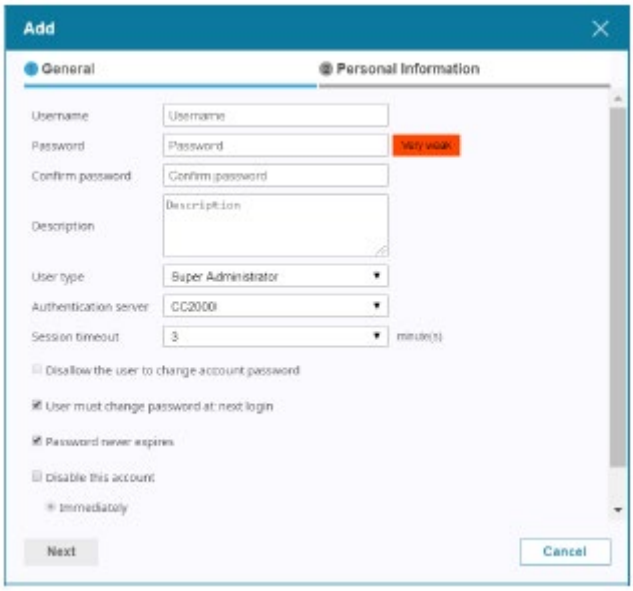


MOTP 認証サービスに対するユーザーアカウントの作成

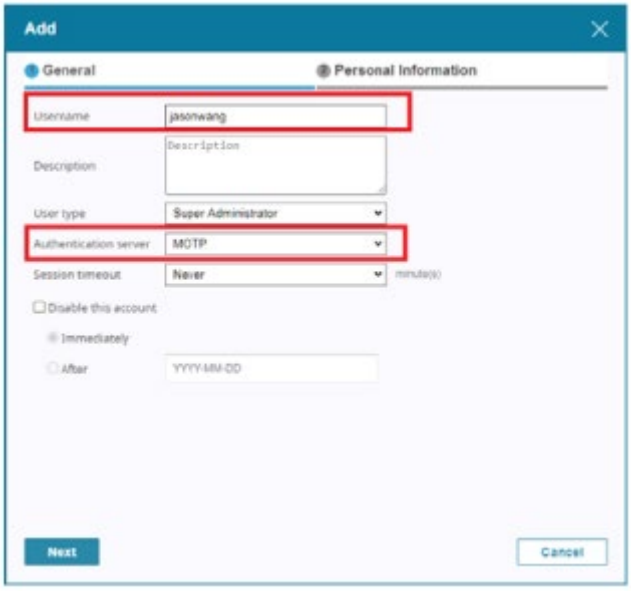
CC2000 に管理者でログインしていることを確認してください。

1. 「**User Accounts**」(ユーザーアカウント)→「**Users**」(ユーザー)に進んで、「**Add**」(追加)をクリッ

クしてください。



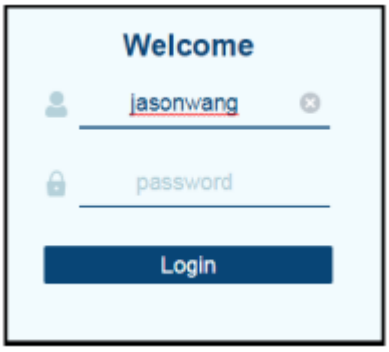
2. 下図のように、認証サーバーに「MOTP」を選択してください。そうしたら、MOTP サーバーで作成したものと同じユーザーネームを入力してください（例：jasonwang）。「**Next**」（次へ）をクリックして、次に進んでください。



3. 「Personal Information」（個人情報）タブの利用可能な項目に、適切な値を入力したら、「**Save**」（保存）をクリックしてください。「Personal Information」（個人情報）タブの詳細については、p.196「ユーザーの追加」を参照してください。
4. 追加されたユーザーは、ユーザーリストに表示されます。

CC2000 へのログイン

1. CC2000 のログイン画面に進んで、MOTP 認証ユーザーのユーザーネーム（例：jasonwang）を入力したら、「**Login**」（ログイン）をクリックしてください。

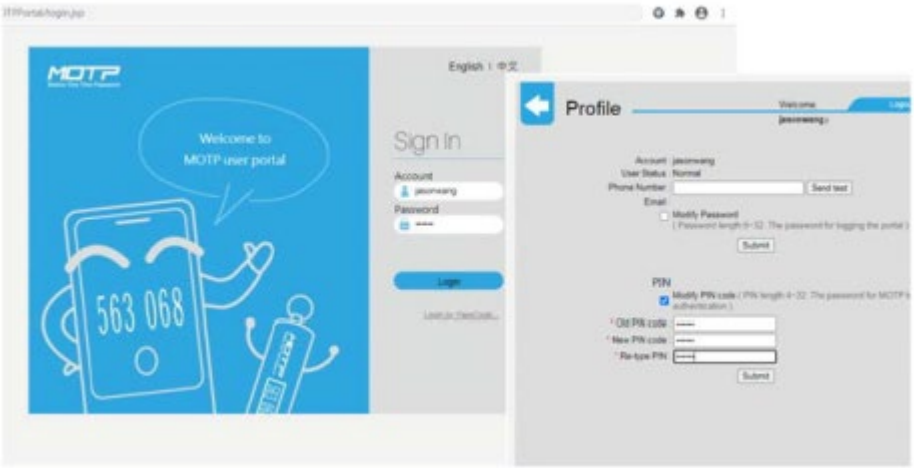


2. そうすると、MOTP 認証ウィンドウが表示されます。（お使いのモバイルデバイスにある）モバイルアプリ MOTP Client で生成された OTP を入力し、CC2000 にログインしてください。

注意：
1. OTP は 60 秒ごとに変更されます。
2. サーバータイプで「Dual Authentication」（二要素認証）が選択されている場合、CC2000 はユーザーに対してログイン認証と OTP 認証の両方を要求します。

MOTP サーバーにおける二要素認証が「OTP + PIN」である場合、CC2000 へのログインに使用する OTP および PIN（デフォルト = 000000）を入力してください。

PIN を変更するには、MOTP サーバーのユーザーポータル（例：http://192.168.1.200/MOTPPortal）にログインし、プロファイルカテゴリーで変更を行ってください。



付録 E
シングルサインオン
HTML サンプルコード

概要

シングルサインオン（SSO）が有効になっている場合、ユーザーは別のウェブシステムからフォームベース認証を介して CC2000 へと自動的にログインすることができます。HTML サンプルコードの例は次のセクションを参照してください。

シングルサインオン HTML サンプルコード

```
<html>
<head><title>Sample page for CC2000 SSO (Single Sign On) Sample</title></head>
<script language="JavaScript">
<!--
function doLogin()
{
form1.submit();
}
-->
</script>
<body>
<table>
<div align="center">
<form id="form1" name="form1" method="post"
action="https://10.3.166.65:443/ccadmin/singlesignon.do">
<!-- Server_IP_port: CC2000 server IP/port (default port could be omitted)
-->
<tr>
<td>
```

Test page for CC2000 SSO (Single Sign On)

</td>
</tr>
<tr>
<td>
CC Username: <input class="sw4" type="text" name="MySSO_Username"
value="administrator" size="15">

<!-- signonusername: Username field in CC2000 SSO setting page -->
</td>
</tr>
<tr>
<td>
CC Password: <input class="sw4" type="password" name="MySSO_Password"
value="password" size="15">

<!-- signonpassword: Password field in CC2000 SSO setting page -->
</td>
</tr>
<tr>
<td>
<!--
CC Username: <input class="sw4" type="text" name="loginname" value="administrator"
size="15">   CC Password: <input class="sw4" type="password"
name="loginpass" value="password" size="15">

-->
<input class="bw" type="button" value="SSO to CC2000" name="login" onClick="doLogin();">
</td>
</tr>
</form>

</body>
</html>