ASUS Control Center Express

ユーザーマニュアル

バージョン: 01.05

J22036
改定第5版
2023年9月

もくじ

目次

もくじ

もくじ

もくじ

もくじ

本書について

本書にはASUS Control Center Express（ACCE）を使用および設定をするために必要な情報が記載されています。

本書の概要

本書は次のように構成されています。

1. **1章：はじめに**

   本章はASUS Control Center Expressの概要と、インストール方法と設定方法を説明します。

2. **2章: メインメニューの概要**

   本章はメインコントロールパネルの機能を説明します。

3. **3章: 配置管理**

   本章はASUS Control Center Expressのエージェントを自動または手動で配置、削除、更新する方法を説明します。

4. **4章: デバイス情報**

   本章はデバイスを管理するためのデバイス情報とソフトウェア制御の機能を説明します。

5. **5章: 管理機能**

   本章はメタデータ管理、ソフトウェア管理、タスクスケジューラー、ハードウェアベースの管理機能を説明します。

6. **6章: 設定の移行ツール**

   本章はACC CSMの設定情報をASUS Control Center Expressへインポートする方法と、ASUS Control Center Expressのエージェントを ACC CSMが管理するデバイスへ配置する方法を説明します。

7. **7章: レポートジェネレーター**

   本章はクライアントデバイスに関する各種レポートを生成する方法を説明します。

8. **8章: アカウントと全般設定**

   本章はユーザー設定とASUS Control Center Expressの設定を説明します。

本書の表記について

本書には、製品を安全にお使いいただき、お客様や他の人々への危害や財産への損害を未然に防止していただくために、守っていただきたい事項が記載されています。次の内容をよくご理解いただいた上で本文をお読みください。

注意: ハードウェアの損傷やデータの損失の可能性があることを示し、その危険を回避するための方法を説明しています。

重要: 作業を完了するために必要な指示や設定方法を記載しています。

メモ: 製品を使いやすくするための情報や補足の説明を記載しています。

表記

太字	選択するメニューや項目を表示します。
<Key>	< >で囲った文字は、キーボードのキーです。 例: <Enter>→Enter もしくはリターンキーを押してください。
`Command`	表示されているとおりにコマンドを正確に入力し、必要な項目または値を括弧で囲んで指定する必要があります。 例:DOSプロンプトで、コマンドライン 「**`format A:/S`**」と入力します。

- 本書に記載している画面は一例です。画面の背景、画面デザイン、表示される項目名、アイコンなどの種類や位置などが実際の画面と異なる場合があります。
- 本書は、本書作成時のソフトウェアおよびハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに搭載されている機能および名称が異なる場合があります。また、本書の内容は、製品やサービスの仕様変更などにより将来予告なく変更することがあります。本製品の最新情報については弊社Webサイトをご覧ください。

参考

ASUSのハードウェアおよびソフトウェア製品に関する最新情報は世界各国のASUSウェブサイトをご覧ください。

1章

本章はASUS Control Center Expressの概要と、インストール方法と設定方法を説明します。

はじめに

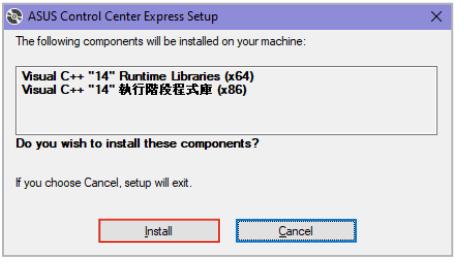
1.1 セットアップ

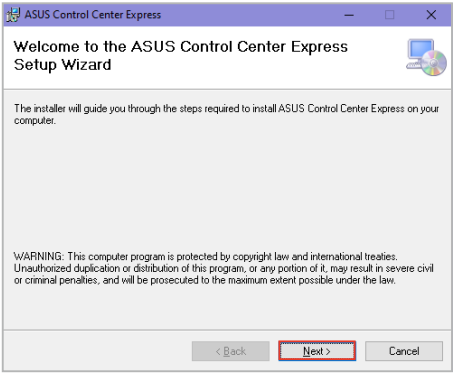
1.1.1 ASUS Control Center Express（ACCE）のインストール

ASUS Control Center Expressを更新する前に、データや設定をバックアップすることをおすすめします。詳しくは、**8.6 バックアップと復元** を参照してください。

1. お使いのASUS製品のウェブサイトへ移動し、ASUS Control Center Expressのインストーラーをダウンロードしてください。
2. インストールファイル（Zip形式）を解凍し、Setup.exeを実行します。vcredist_x64、vcredist_x86、データベース、ASUS Control Center Expressのインストールが開始されます。

- ASUS Control Center Expressをインストールする前に、Microsoft .NET Framework V4.6.1以降がインストールされていることを確認してください。
- ご利用のシステムに旧バージョンのASUS Control Center Expressが既にインストールされており、旧バージョンの設定を削除した場合は、まずデータをバックアップし、続いてインストール中に**Clear original configuration（オリジナルの設定を消去）**オプションを選択してください。
- 必要な場合を除き、旧バージョンのASUS Control Center Expressの設定は消去しないことが推奨されます。

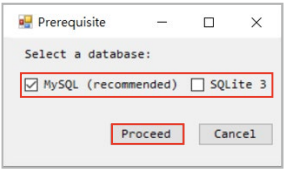




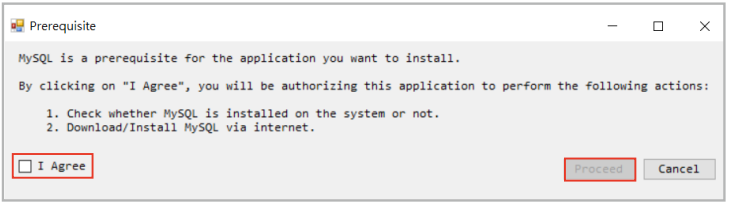
本章では、MySQLを例に説明していますが、他のデータベースを使用したい場合は、選択したデータベースのインストール手順に従ってください。

3. ASUS Control Center Expressにインストールするデータベース（**MySQL, SQLite 3**）を選択し、**Proceed**（**続行**）をクリックします。今回の例では、**MySQL**を選択します。

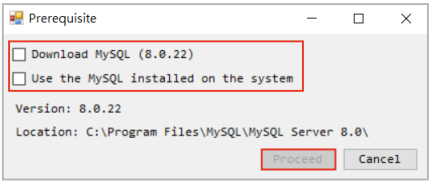
- ASUS Control Center Expressのデータベースとして、**MySQL**の選択をお勧めします。
- データベースのインストール前に、メインサーバーが安定した接続でパブリックWANに接続されていることを確認してください。



4. 前提条件をお読みいただき、**I Agree**（**同意する**）にチェックを入れ、**Proceed**（**続行**）をクリックします。

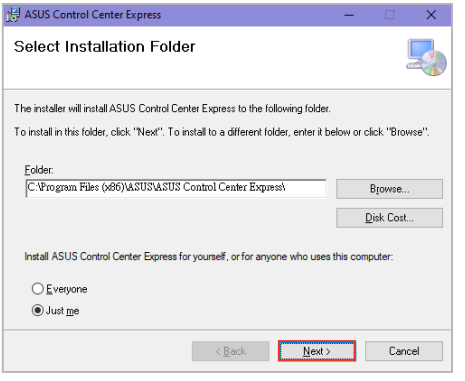


5. MySQLのインストールファイルをインターネットからダウンロードするか、システムにインストールされている既存のMySQLを使用するかを選択し、**Proceed（続行）**をクリックします。



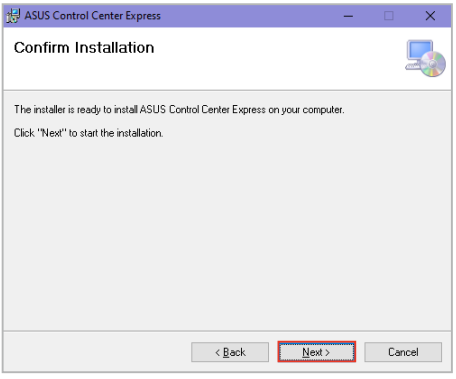
- **Download MySQL（MySQLをダウンロードする）**をクリックすると、**MySQL**のインストールファイルをダウンロードします。ダウンロードの完了後、手動でインストールします。
- インストールされている既存の**MySQL**を自動的に検出するには、**Use the MySQL installed on the system（システムにインストールされている MySQLを使用する）**をクリックします。

6. データベースの設定が完了すると、ASUS Control Center Expressのインストールが始まります。
7. ASUS Control Center Expressをインストールするフォルダーを選択します。デフォルトのフォルダー設定を使用することが推奨されます。終了したら、**Next（次へ）**をクリックします。



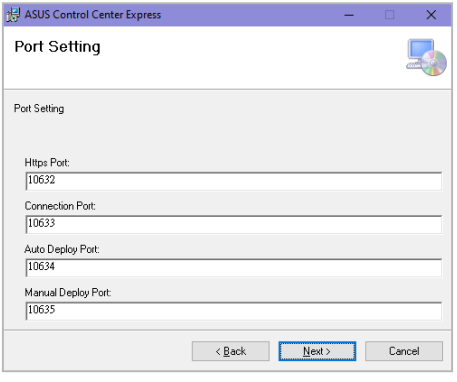
- **Browse...（参照）**をクリックして、ASUS Control Center Expressをインストールするフォルダーを新たに設定することができます。
- **Disc Cost...（ディスク容量）**をクリックすると、サーバーのディスク容量と、ASUS Control Center Expressのインストールに必要なディスク要領が表示されます。

8. **Next（次へ）**をクリックするとインストールが開始されます。



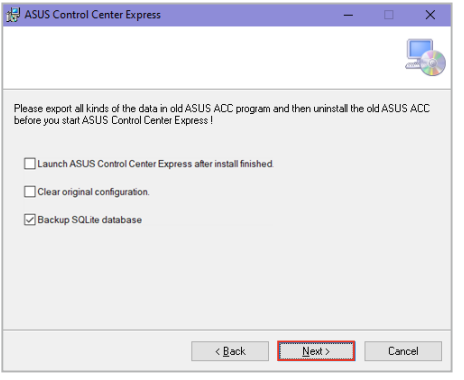
9. Port Setting（ポート設定）ページでは、表示されるポートがすでに使われている場合、デフォルトのポート設定を変更することができます。ポート変更を完了したか、デフォルトのポートを使用する場合は、**Next（次へ）**をクリックします。

Https Port（Httpsポート）	ACCEメインサーバーのログインポートです。
Connection Port（接続ポート）	ACCEメインサーバーとクライアントデバイスの接続ポートです。
Auto Deploy Port（自動配置ポート）	ACCEメインサーバーの自動配置ポートです。
Manual Deploy Port（手動配置ポート）	ACCEメインサーバーの手動配置ポートです。
KVM Port（KVMポート）	ACCEメインサーバーのOOB KVMポートです。
Broadcast Port（ブロードキャストポート）	ACCE メインサーバーのブロードキャストポートです。
MySQL Port（MySQLポート）	ACCE メインサーバーのデータベースポートです。
Indication（インジケーション）	ACCE メインサーバーのアラート通知機能ポートです。

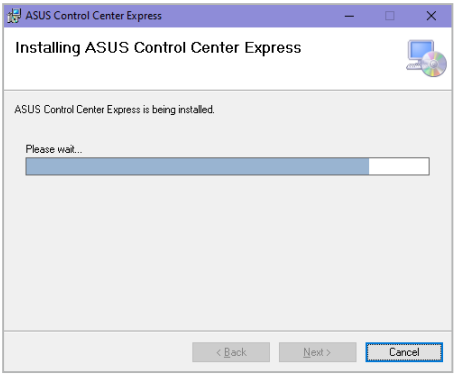


10. インストール時に実行するオプションを選択し、**Next（次へ）**をクリックします。

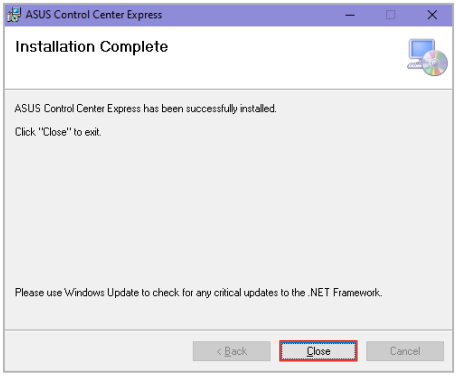
- **Launch ASUS Control Center Express after install finished（インストールの終了後にASUS Control Center Expressを起動）：**インストールが完了したらASUS Control Center Expressを起動します。
- **Clear original configuration（オリジナルの設定を消去）：**（推奨されません）ASUS Control Center Expressの旧設定を削除します。このオプションを使用する場合は、先にASUS Control Center Expressのデータをバックアップすることが推奨されます。
- **Backup SQLite database（SQLiteデータベースのバックアップ）：**（推奨）インストール時に既存のSQLiteデータベースをバックアップします。デフォルトのバックアップ先は、C:\Program Files (x86)\ASUS\ASUS Control Center Express\apro_console\backup に設定されています。



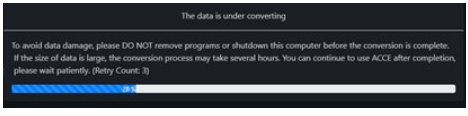
11. ASUS Control Center Expressのインストールが終了するまで待ちます。



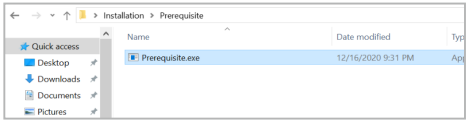
12. インストールが完了したら、**Close（閉じる）**をクリックしてインストール画面を閉じます。



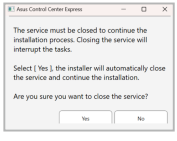
- ASUS Control Center Express v1.4.x以前のバージョンからアップグレードする場合、またはSQLiteからMySQLにアップグレードする場合は、データベースの変換に時間がかかることがあります。データの損失を防ぐため、データベースの変換が完了するまで、アプリケーションをアンインストールしたり、メインサーバーの電源を切ったりしないでください。何らかの理由でデータベースの変換が完了しない場合でも、既存のデータベースを使用してASUS Control Center Expressを引き続き使用することができます。



- データベースのインストール前に、メインサーバーが安定した接続でパブリックWANに接続されていることを確認してください。
- MySQLデータベースを手動でインストールする必要がある場合は、**Installation > Prerequisite** フォルダ内にある**Prerequisite.exe**を起動します。



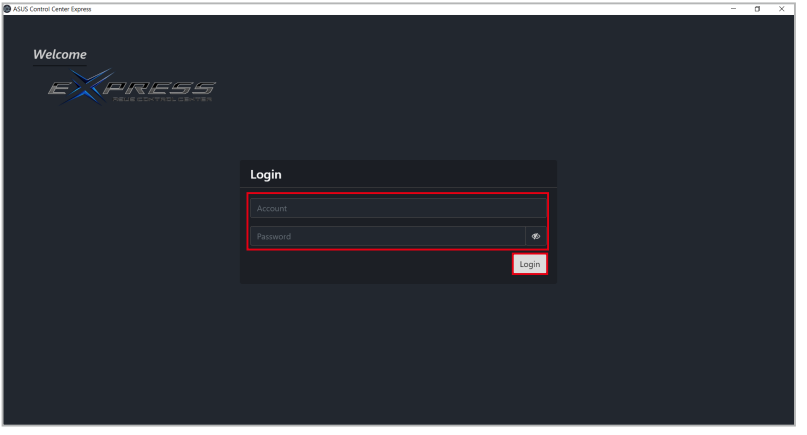
- アップグレード中にASUS Control Center Expressのサービスを終了するよう要求された場合は、**Yes（はい）**をクリックしてバックグラウンドサービスを終了し、インストールを続行します。



1.1.2 ASUS Control Center Expressへのログイン

1. **ASUS Control Center Express.exe**アプリケーション をダブルクリックして、ASUS Control Center Expressを起動します。
2. **Account（アカウント名）**と**Password（パスワード）**を入力します。**Login**（ログイン）をクリックして、**ASUS Control Center Express**のメインメニューを開きます。

- デフォルトのアカウント名は「**administrator**」、パスワードは「**admin**」です。デフォルトのアカウント名とパスワードを変更する場合は、**1.1.3 アカウントのパスワードの変更** を参照してください。
- アカウント名とパスワードは大文字と小文字が区別されます。
- ASUS Control Center Expressは、9つの言語（英語、繁体字中国語、簡体字中国語、日本語、ドイツ語、フランス語、ロシア語、韓国語、スペイン語）に対応しています。初回起動時は、オペレーティングシステムの言語に合わせて表示言語が設定されます。オペレーティングシステムの言語が対応していない場合、表示言語は英語に設定されます。
- データと設定をバックアップするために、データベースのインストールを強くおすすめします。詳しくは、**8.6 バックアップと復元** を参照してください。

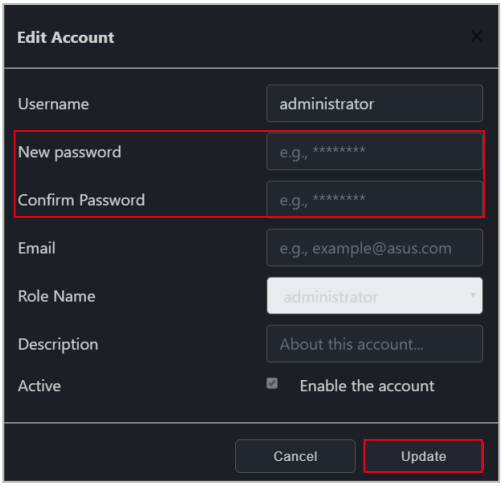


1.1.3 アカウントのパスワードの変更

1. デフォルトのアカウント名とパスワードでログインします。

- デフォルトのアカウント名は「**administrator**」、パスワードは「**admin**」です。
- アカウント名とパスワードは大文字と小文字が区別されます。

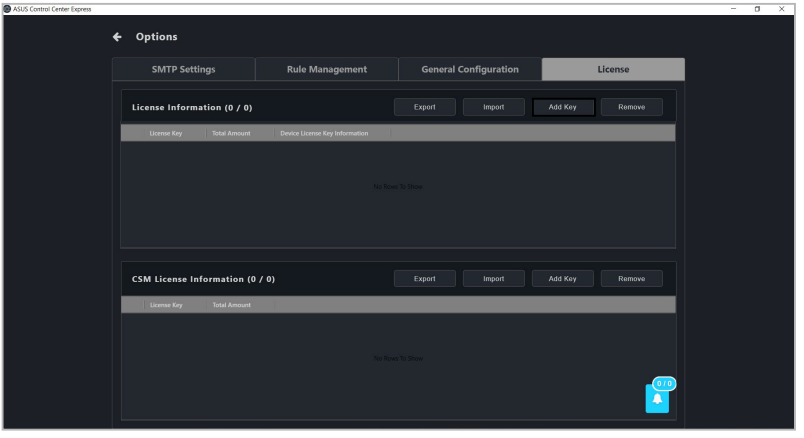
2. 右上のメニューバーに表示される アイコンをクリックし、続いて**Settings（設定）**をクリックします。
3. アカウント名をクリックして新しいパスワードを入力し、続いて**Update（更新）**をクリックして変更内容を保存します。



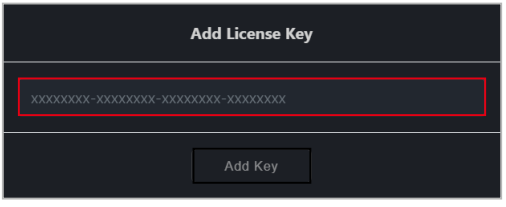
1.1.4 ライセンスキーのアクティベーション

- エージェントを配置する前に、ライセンスキーを有効にする必要があります。エージェントを配置する各クライアントデバイスには、対応するライセンスキーが必要です。
- インポートするライセンスキーか、以前にエクスポートしておいたライセンスキーがすでに存在する場合は、**Import（インポート）**機能を使用してください。ライセンスキーの詳細は、**8.1.4 ライセンス**を参照してください。

1. マザーボードに付属するASUS Control Center Expressカードに記載されたライセンスキーを確認してください。
2. アイコンをクリックし、続いて**Options（オプション）** > **License（ライセンス）**タブを選択します。
3. **Add Key（キーを追加）**をクリックします。



4. ライセンスキーを入力し、続いて**Add Key（キーを追加）**をクリックして、単一デバイスに対するASUS Control Center Expressのライセンスを登録します。



1.1.5 言語の変更

アイコンをクリックし、続いてドロップダウンリストから言語を選択すれば、ASUS Control Center Expressの表示言語を変更することができます。

1.1.6 ASUS Control Center Expressバージョンの更新

ASUS Control Center Expressをインストールして使用している場合は、次の方法でASUS Control Center Expressのバージョンを更新することができます。

インストールファイルのダウンロードと手動更新

1. ASUS Webサイトから、最新版のASUS Control Center Expressのインストールファイルをダウンロードします。
2. インストールファイルを解凍し、**1.1.1 ASUS Control Center Express（ACCE）のインストール** を参照して、メインサーバーのASUS Control Center Expressメインソフトウェアを更新します。
3. メインサーバーのASUS Control Center Expressメインソフトウェアの更新完了後、**3.4 クライアントエージェントアップデーター** または **3.2.7 エージェントのアップグレードまたは修復** を参照して、クライアントデバイスのエージェントを更新します。

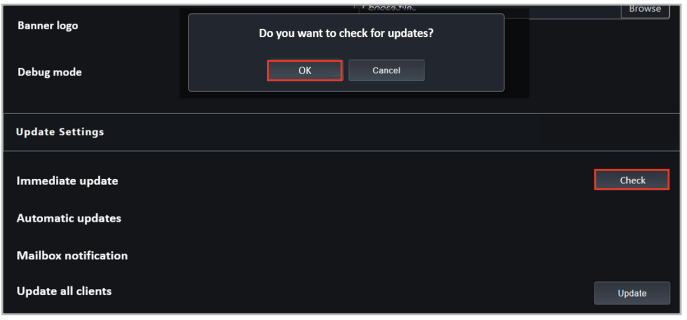
- ASUS Control Center Expressを更新する前に、データや設定をバックアップすることをおすすめします。詳しくは、**8.6 バックアップと復元** を参照してください。
- ASUS Control Center Expressの更新時に、ASUS Control Center Expressメインソフトウェアのみを更新し、クライアントデバイスのエージェントを更新しなかった場合、監視・管理機能に影響が出る可能性があります。**3.2.7 エージェントのアップグレードまたは修復** を参照して、クライアントエージェントのバージョンを更新してください。
- ASUS Control Center Express v1.4.xをインストールして使用しており、ASUS Control Center Express v1.5.x以上にアップグレードする場合は、データベース更新とデータ変換のため、更新版の初回読み込みに時間がかかる場合があります。データ変換の完了後、引き続きASUS Control Center Expressを使用することができます。
- 更新中にASUS Control Center Expressのサービスを終了するよう要求された場合は、**Yes（はい）** をクリックしてバックグラウンドサービスを終了し、インストールを続行します。

即時更新を利用した更新

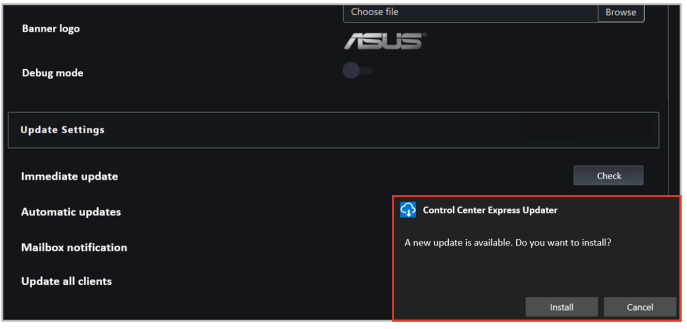
ASUS Control Center Expressの更新は、**Options（オプション）**の**Update Settings（更新設定）**タブからただちに行うことができます。

1. 右上のメニューバーの をクリックして、**Options（オプション）>General Configuration（全般設定）**を選択し、**Update Settings（更新設定）**までスクロールします。

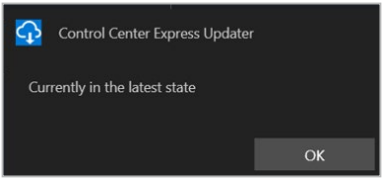
2. **Immediate update（即時更新）**欄の**Check（チェック）**をクリックして、**OK**をクリックします。



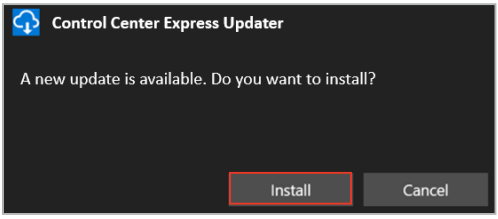
3. 新しい更新が利用可能な場合は、ASUS Control Center Expressで利用可能な新しい更新を知らせるポップアップ通知が表示されます。ポップアップ通知の**Install（インストール）**をクリックすると新しい更新がインストールされ、**Cancel（キャンセル）**をクリックすると更新がキャンセルされます。



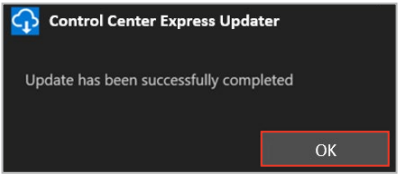
お使いのASUS Control Center Expressがすでに最新のバージョンである場合、ポップアップ通知に**Currently in the latest state（現在、最新の状態です）**というメッセージが表示されます。



4. **Install（インストール）**をクリックすると更新が開始されます。ASUS Control Center Expressは更新が進行中の場合、自動的に終了します。更新完了後、ASUS Control Center Expressを再度起動してください。



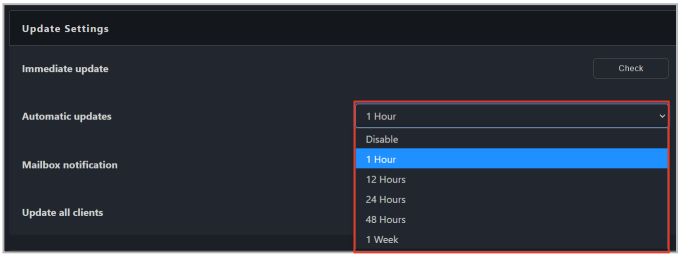
5. 更新が完了したら**OK**をクリックします。



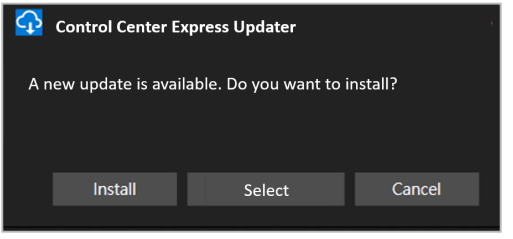
自動更新の設定による更新

Automatic updates（自動更新）機能を有効にすると、ASUS Control Center Expressウィンドウの右下に新しい更新のポップアップ通知が表示されます。このポップアップウィンドウから、更新をインストールするかキャンセルするかを選択することができます。

1. 右上のメニューバーの をクリックして、**Options（オプション）> General Configuration（全般設定）**を選択し、**Update Settings（更新設定）**までスクロールします。
2. 更新をチェックする頻度と更新の通知を促す頻度を、**Automatic updates（自動更新）**ドロップダウンメニューから選択します。



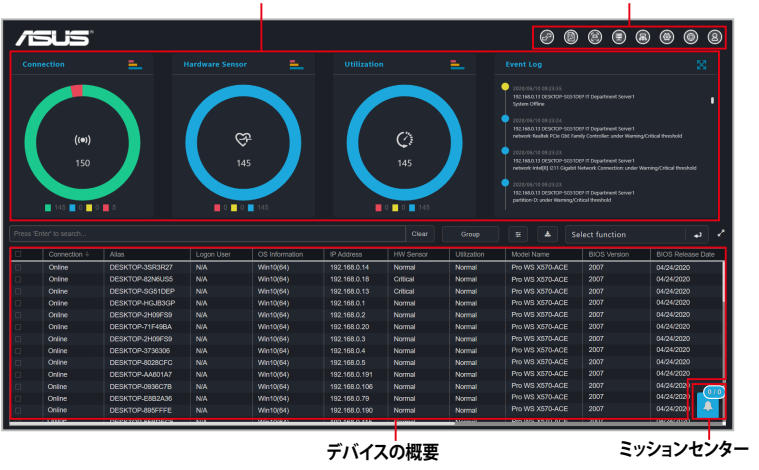
3. 新しい更新が利用可能になると、ASUS Control Center Expressウィンドウの右下にポップアップ通知が表示されます。通知が表示されたら、次のいずれかの操作を行うことができます。
   - **Install（インストール）**をクリックすると、すぐにダウンロードされ更新が開始されます。
   - **Select（選択）**をクリックすると、更新の通知を促す別の時間を選択することができます。
   - （非推奨）ASUS Control Center Expressの更新を行わない場合は、**Cancel（キャンセル）**をクリックします。このオプションを選択すると、選択した**Automatic updates（自動更新）**の通知時間に次回到達したとき、更新の通知が再び表示されます。



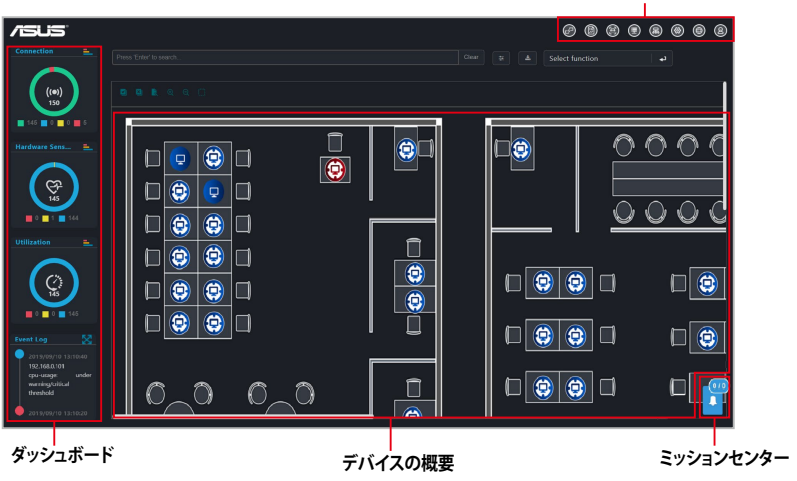
1.2 メインメニューの概要

をクリックすればクラシックビューとグラフィックビューを切り替えることができます。
ASUS Control Center Expressの2つのビューの例を以下に示します。

クラシックビュー



グラフィックビュー



メニューバーの項目：

画面上部のメニューバーには次の項目が表示されます：

上部メニューバーの項目		説明
	**Switch view（ビューの切替）**	ユーザーインターフェースを切り替えます。
	**Report generator（レポートジェネレーター）**	クライアントデバイスのオンライン/オフライン状態を示すグラフとレポートを生成します。また、ソフトウェアのインストールとハードウェアの一覧とレポートも生成します。
	**Management control（管理制御）***	リモート管理コントローラーを使用して、電源がオフのデバイス、オペレーティングシステムがインストールされていないデバイス、オペレーティングシステムを起動できないデバイスなどで、デバイスのハードウェアを検査し特定の機能を実行します。
	**Metadata（メタデータ）**	単一または複数のデバイスでデバイスのメタデータをカスタマイズします。
	**Deploy（配置）**	ASUS Control Center Expressエージェントを自動または手動で配置または削除します。
	**Settings（設定）**	SMTP設定、通知ルール、ASUS Control Center Expressメインサーバーの設定、ライセンスキーの管理、データ転送の設定を行います。
	**Language（言語）**	ASUS Control Center Expressの表示言語を選択します。
	**Account（アカウント）**	• アカウントを追加または編集し、権限を設定します。 • QRコードをスキャンします。 • ログアウトします。
	**Mailbox（メールボックス）**	ASUS Control Center Expressに関連するお知らせを表示します。

* 管理制御機能を使用する場合は、制御対象のマザーボードがリモート管理コントローラーをサポートしているかをご確認ください。

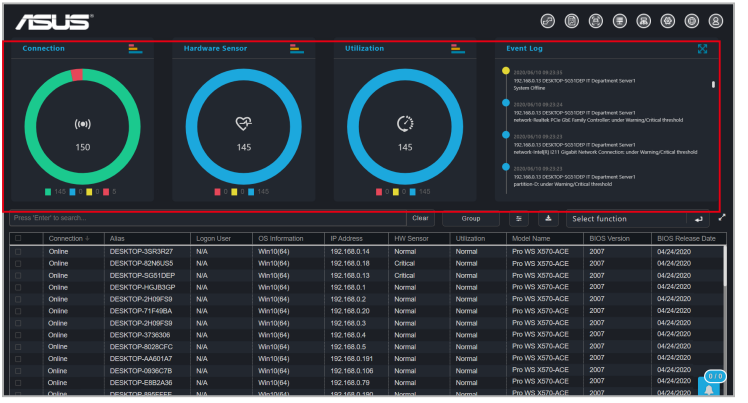
2章

本章はメインコントロールパネルの機能を説明します。

メインメニューの概要

2.1 ダッシュボードの概要

ダッシュボードの全体像を把握し、活動のアラートやイベントログを確認して、リアルタイムにクライアントのデバイスをモニタリングすることができます。



Connection（接続）

このグラフには、すべてのクライアントデバイスの接続状態の概要が表示されます。

色	状態
緑	オンライン
青	メンテナンス
黄	スタンバイ
赤	オフライン

Hardware Sensor（ハードウェアセンサー）

このグラフには、すべてのオンラインクライアントデバイスのハードウェアステータスの概要が表示されます。

色	状態
赤	重大
黄	警告
青	正常

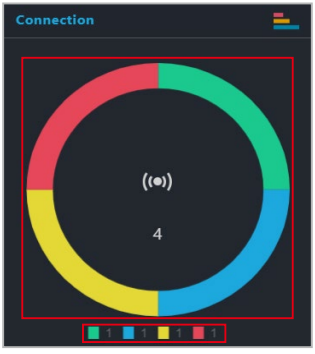
Utilization（使用率）

このグラフには、すべてのオンラインクライアントデバイスの使用状況の概要が表示されます。

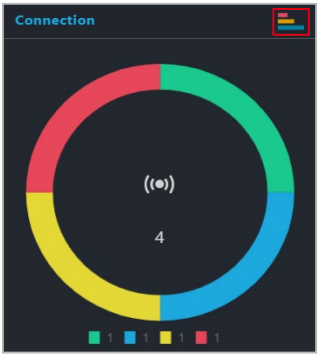
色	状態
赤	重大
黄	警告
青	正常

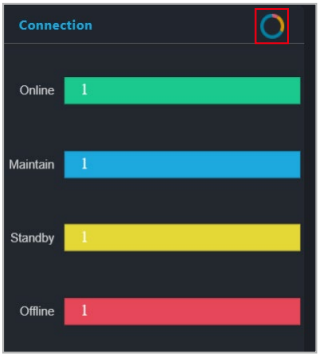
2.1.1 センサービューの切替

グラフの各ブロックをクリックする、またはグラフキーを使用して選択したステータスに一致するデバイスをフィルタリングし、グラフに表示される情報をカスタマイズすることができます。



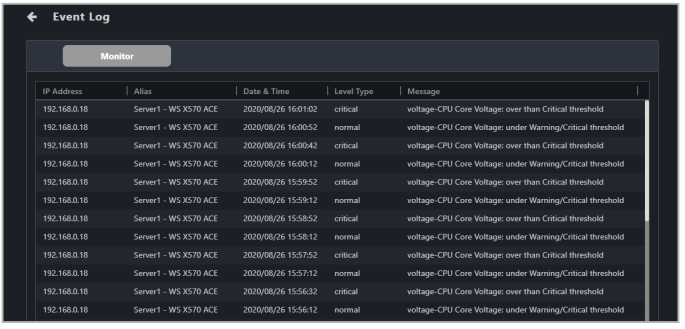
各グラフの右上をクリックして、円グラフと棒グラフの間で表示を切り替えることができます。





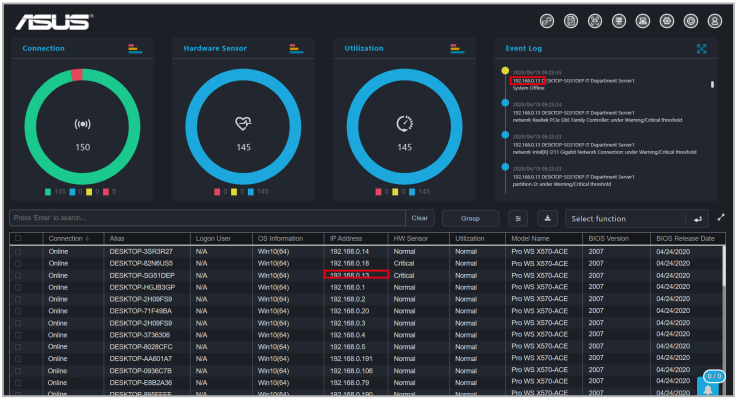
2.1.2 イベントログ

イベントログ表示は、すべてのクライアントデバイスの状態をリアルタイムで表示します。クライアントデバイスの状態変化を一目で確認することができます。イベントログの右上をクリックして表示内容を拡張し、各イベント項目の詳細情報を確認することもすることができます。



通知ルール管理メニューを使用して、イベントログに表示するイベントの通知ルールを追加または編集することができます。通知ルールを設定するには、ダッシュボードの右上のメニューバーにある をクリックし、**Optopms（オプション）> Rule Management（ルール管理）**を選択します。詳細は、**8.1.2 ルール管理**を参照してください。

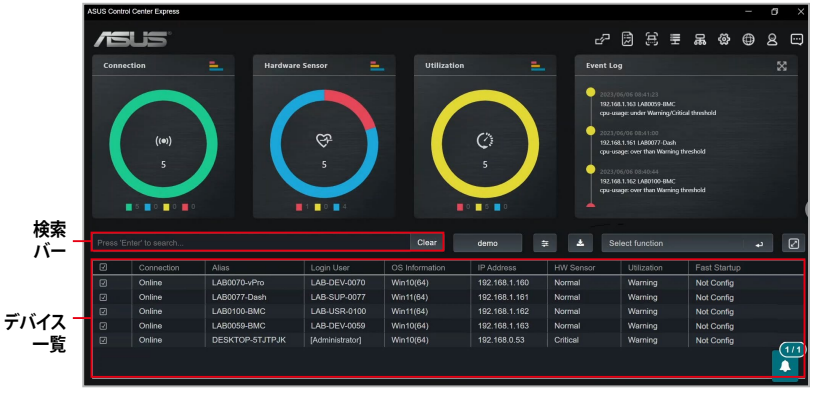
イベントログでクライアントデバイスのIPアドレスをクリックすると、デバイスの一覧で対象のデバイスが強調表示されます。デバイスを検索する手間を省いて、一目でデバイスを判別することができます。



2.2 デバイスの概要

デバイスの概要にはクライアントデバイスがすべて表示されます。キーワードを使用してクライアントデバイスを検索したり、クライアントデバイスの一覧をエクスポートしたり、ショートカット機能を使用して選択したデバイスで特定の操作を行えます。

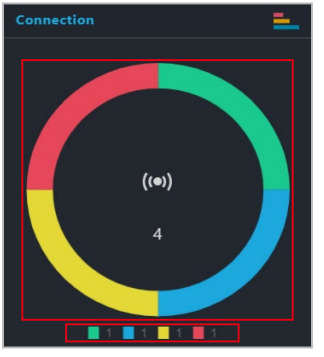
- ASUS Control Center Expressを使用してまだ設定されていない場合、特定のフィールドに「Not Config（未構成）」と表示されることがあります。
- クライアントデバイスが、電源オフ、オフライン、ログアウトされている場合、Login User（ログインユーザー）欄には、最後にログインしたユーザー名が括弧（[]）で囲まれて表示されます。



2.2.1 クライアントデバイスのフィルタリング

検索バーで**Clear（消去）**をクリックすると、フィルターが消去されてすべてのデバイスが表示されます。

- **検索バーを使用してデバイスをフィルタリング：**
  検索バーへキーワードを入力して<Enter>キーを押すと、検索条件に合致したデバイスが検索されます。キーワードを削除する場合は、「**X**」をクリックします。
- **ダッシュボードを使用してデバイスをフィルタリング：**
  グラフの各ブロックをクリックする、またはグラフキーを使用して選択したステータスに一致するデバイスをフィルタリングし、グラフに表示される情報をカスタマイズすることができます。



- **デバイスの一覧を使用してデバイスをフィルタリング：**

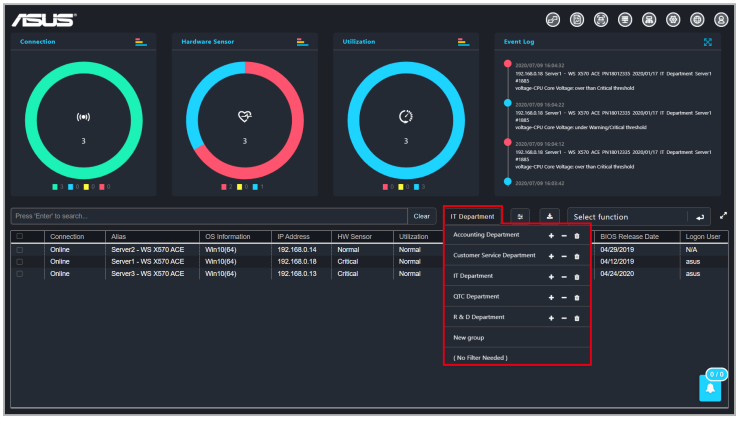
  1. デバイスの一覧で、条件として使用する列の上にポインターを移動させます。
  2. ☰ をクリックし、フィルタリングのルール（**Equals（等しい）**、**Not equal（等しくない）**、**Starts with（～で始まる）**、**Ends with（～で終わる）**、**Contains（～を含む）**、**Not contains（～を含まない）**を選択したうえで、検索キーワードを入力します。

  - 列のヘッダー名をクリックすると、フィルタリング結果をアルファベットの昇順または降順に並べ替えることができます。
  - デバイス一覧の右上にある ⤢ をクリックすることで、一覧画面を拡張して表示することができます。⤡ をクリックすると、一覧画面は元のサイズに戻ります。
  - 列のタイトルをクリックしてドラッグすると、デバイス一覧の列を入れ替えることができます。

- **グループを使用してデバイスをフィルタリング：**

  Group（グループ）のドロップダウンメニューで**（No Filter Needed）（フィルター不要）**をクリックすると、フィルターが消去されてすべてのデバイスが表示されます。

  Group（グループ）をクリックし、ドロップダウンメニューからグループを選択すると、そのグループに属するデバイスのみが表示されます。



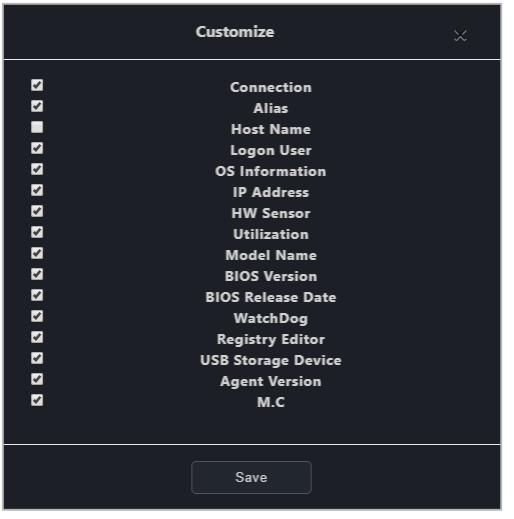
2.2.2 デバイス情報の表示

デバイスの概要一覧でクライアントデバイスのセルをクリックすると、デバイス情報のページへ移動します。クライアントデバイスの詳細情報を確認したり、デバイスに関するその他の機能を操作することができます。

デバイス情報ページに表示される情報について、詳しくは **4章 デバイス情報** を参照してください。

2.2.3 デバイス一覧のメタデータのカスタマイズ

クライアントデバイスの一覧で表示する項目を選択する場合は、**Customize（カスタマイズ）**アイコン をクリックします。新しく追加されたメタデータ項目にチェックを入れると、デバイスの概要一覧でメタデータの列を追加して表示できます。



2.2.4 デバイス一覧のエクスポート

デバイス一覧をバックアップする場合は、一覧を .csvファイル形式でエクスポートすることができます。

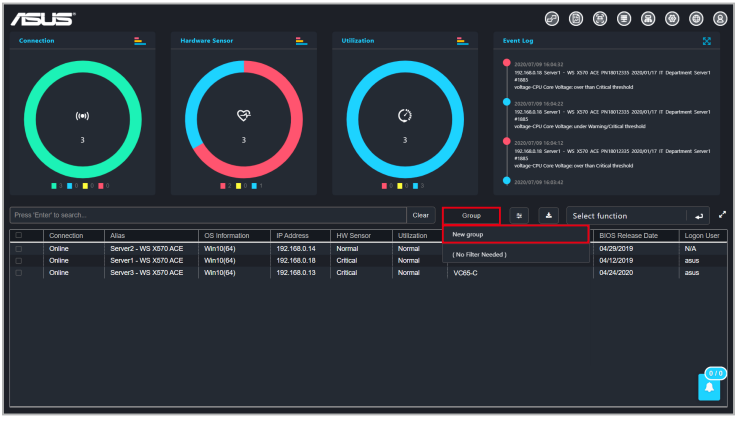
デバイス一覧をエクスポートする場合は、 （**Export（エクスポート）**）をクリックし、ファイル名を入力して**Save（保存）**をクリックすれば、デバイス一覧が.csv形式で保存されます。

2.2.5 クライアントデバイスのグループ作成

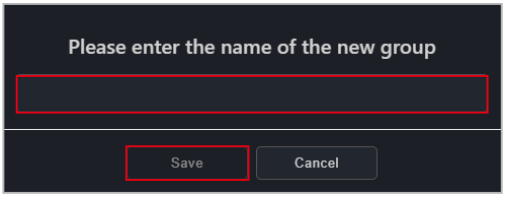
必要に応じて、クライアントデバイス一覧のクライアントデバイスをグループ分けすることができます。グループ機能とフィルター機能を使用することで、クライアントデバイスをすばやく検索、表示、管理することができます。また、作成したグループに通知ルールの設定を適用したり、**Report generator（レポートジェネレーター）**のレポートに表示されるデバイスを既存のグループに簡単に追加することができます。

新規デバイスグループを作成する方法は次の通りです：

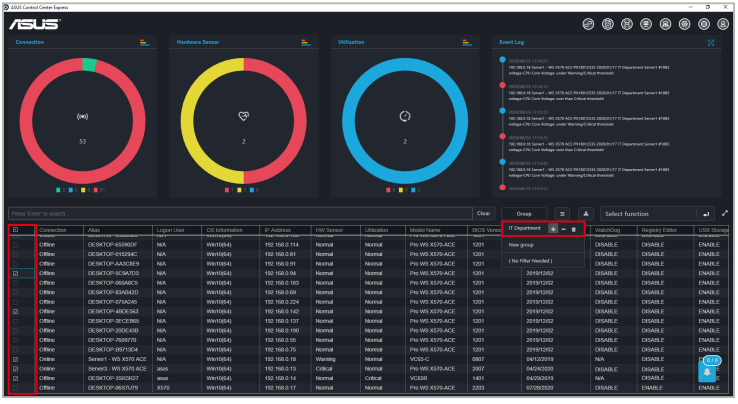
1. **Group（グループ）**をクリックします。
2. ドロップダウンメニューから**New group（新規グループ）**を選択します。



3. グループ名を入力して、**Save（保存）**をクリックします。



4. グループに追加するデバイスを選択し、**Group（グループ）**をクリックして ＋ をクリックします。



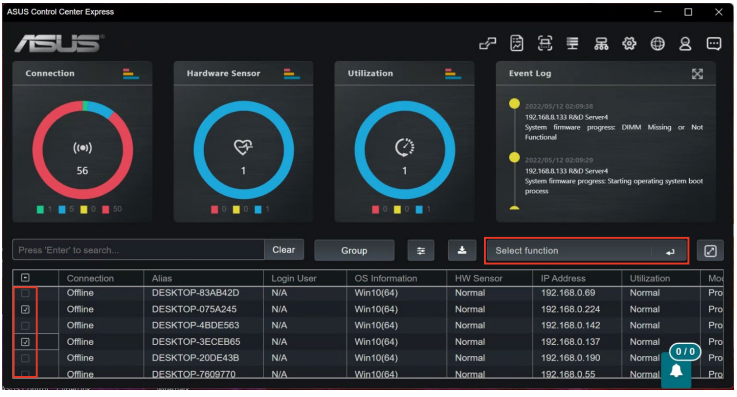
- ➖をクリックすると選択したデバイスがグループから削除されます。
- 🗑をクリックするとグループが削除されます。

5. 確認ウィンドウで**Yes（はい）**をクリックし、続いて**OK**をクリックするとデバイスがグループに追加されます。

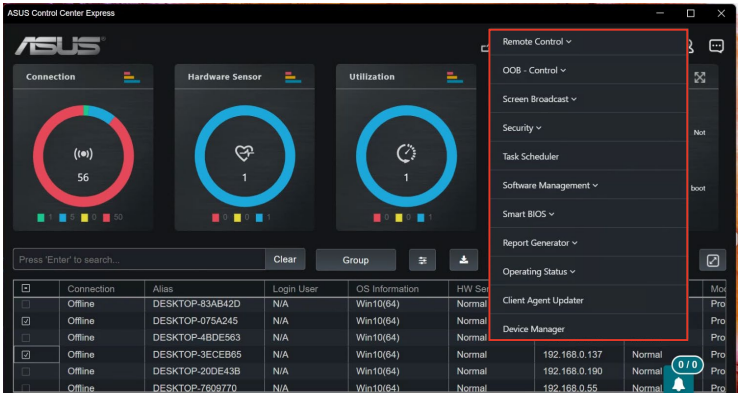
2.2.6 ショートカット機能の使用

クライアントデバイスで所定の操作を行ったり、タスクのスケジュールを設定することができます。

1. アクションを実行したいデバイスのチェックボックスにチェックを入れます。



2. **Select function（機能を選択）**をクリックし、使用する機能を選択します。次の表に、各機能の内容が短く紹介されています。



一部の機能は、クライアントデバイスを再起動した後に有効になります。

3. ミッションセンターを使用して、タスクが正常に完了したことを確認します。詳しくは **2.4 ミッションセンター** を参照してください。

Remote Control（リモート制御）

Restart Computer	選択したデバイスを再起動します。
Power Off	選択したデバイスの電源をオフにします。
Power On	選択したデバイスの電源をオンにします。 電源オフのクライアントデバイスは、ウェイクオンLANをサポートしている場合にのみ、電源オンにできます。

OOB-Control（OOB-制御）*

- リモート管理コントローラーをサポートするマザーボードを搭載し、管理LANポートを使用して接続されたクライアントデバイスでのみ使用できます。
- OOB-Controlメニューには、4つのリモート管理コントローラーの機能が含まれています（BMC、DASH、RTL8117、vPro）。選択されたデバイスが選択された機能をサポートしていない場合、機能の実行後にミッションセンターで関連情報を確認できます。

- **Power Control（電源制御）**

Power On（G0/S0）	リモート管理コントローラーを介して選択したデバイスの電源をオンにします。
Power Off - Soft（G2/S5）	リモート管理コントローラーを介して選択したデバイスの電源をオフにします。
Power Off - Hard（G3）	リモート管理コントローラーを介して選択したデバイスの電源を強制的にオフにします。
Power Cycle - Soft off（G2/S5）	リモート管理コントローラーを介してオペレーティングシステムをシャットダウンした後に、選択したデバイスを再起動するように設定します。
Sleep - Deep （G1/S3）	リモート管理コントローラーを介して選択したデバイスをスリープモード（G1/S3）に設定します。
Master Bus Reset	リモート管理コントローラーを介して選択したデバイスのハードウェアを再設定します。
Hibernate（G1/S4）	リモート管理コントローラーを介して選択したデバイスをハイバネーションモード（G1/S4）に設定します。
Restart Computer to BIOS	リモート管理コントローラーを介して再起動後、選択したデバイスがBIOSに入るよう設定します。
Power On to BIOS	リモート管理コントローラーを介して起動後、選択したデバイスがBIOSに入るよう設定します。
Restart Computer to IDE-R Floppy	リモート管理コントローラーを介して再起動後、選択したデバイスがIDE-Rフロッピードライブに入るよう設定します。
Power On to IDE-R Floppy	リモート管理コントローラーを介して起動後、選択したデバイスがIDE-Rフロッピードライブに入るよう設定します。

Restart Computer to IDE-R CDROM	リモート管理コントローラーを介して再起動後、選択したデバイスがIDE-R CD-ROMに入るよう設定します。
Power On to IDE-R CDROM	リモート管理コントローラーを介して起動後、選択したデバイスがIDE-R CD-ROMに入るよう設定します。
Sleep - Light （G1/S2）	リモート管理コントローラーを介して選択したデバイスをスリープモード（G1/S2）に設定します。
Power Cycle - Hard Off （G3）	リモート管理コントローラーを介して選択したデバイスの電源をオフにしてから再起動します。
Diagnostic Interrupt （NMI）	リモート管理コントローラーを介して選択したデバイスがエラーレポートを印刷し再起動するよう設定します。
Power Off - Soft Graceful （G2/S5）	リモート管理コントローラーを介して選択したデバイスをOS経由で通常シャットダウンします。
Power Off - Hard Graceful （G3）	リモート管理コントローラーを介して選択したデバイスをハードウェア経由で通常シャットダウンします。
Master Bus Reset Graceful	リモート管理コントローラーを介して選択したデバイスのハードウェアを通常シャットダウンしてから再設定します。
Power Cycle （Graceful Soft Off）（G2/S5）	リモート管理コントローラーを介して選択したデバイスをOS経由で通常シャットダウンします。
Power Cycle （Graceful Hard Off）（G3）	リモート管理コントローラーを介して選択したデバイスをハードウェア経由で通常シャットダウンしてから再起動します。

- **Watchdog（ウォッチドッグ）**

WatchDog Enable	選択したデバイスでRTL8117ウォッチドッグ監視を有効にします。
WatchDog Disable	選択したデバイスでRTL8117ウォッチドッグ監視を無効にします。

- **BIOS**

Clear CMOS	RTL8117またはBMCを介して選択したデバイスのCMOSを消去し、工場出荷状態へリセットします。

- **Account Management（アカウント管理）**

Set password	選択したRTL8117またはvProデバイスのリモート管理コントローラーのアカウントパスワードを設定します。
Login	選択したBMCまたはDASHデバイスのリモート管理コントローラーのアカウントにログインします。

- **System（システム）**

Restart service	選択したデバイスのRTL8117サービスを再起動します。
Port	選択したデバイスのBMCポートを設定します。
Sync OEM port	選択したデバイスのBMCポートを同期します。

- **KVM**

KVM Remote Multi-display	選択したデバイスのRTL8117 KVMをリモートマルチディスプレイとして設定します。
KVM Local Multi-display	選択したデバイスのRTL8117 KVMをローカルマルチディスプレイとして設定します。
KVM Remote Single-display	選択したデバイスのRTL8117 KVMをリモートシングルディスプレイとして設定します。
KVM Enable	選択したRTL8117およびvProマシンのKVMを有効にします。
KVM Disable	選択したvProマシンのKVMを無効にします。
KVM Password	選択したデバイスのvPro KVMパスワードを設定します。

- **USB Redirection（USB リダイレクト）**

USB Redirection	クライアントデバイスのリモート管理コントローラーを介して選択したデバイスのUSBリダイレクトを設定します。
Enable USB Redirection	選択したデバイスのUSBリダイレクトを有効にします。
Disable USB Redirection	選択したデバイスのUSBリダイレクトを無効にします。

- **Firmware Update（ファームウェアの更新）**

Firmware Update	選択したデバイスのRTL8117またはBMCファームウェアを更新します。 KVMが有効な場合はファームウェアの更新は無効にされます。

- **Trust Zone（トラストゾーン）**

Trust Zone	クライアントデバイスでRTL8117機能を実行できるメインサーバーのIPアドレスを設定します。

- **Certificate Management（証明書管理）**

Certificate Management	選択したデバイスのvPro証明書を管理します。

- **System Trap Alert（システムトラップアラート）**

Enable Trap Alert	選択したデバイスでDASHとvProのシステムトラップアラートを有効にします。
Enable Trap Alert - Info	選択したデバイスの情報レベルとして、DASHとvProのシステムトラップアラートを設定します。
Enable Trap Alert - Warning	選択したデバイスの警告レベルとして、DASHとvProシステムのトラップアラートを設定します。
Enable Trap Alert - Error	選択したデバイスのエラーレベルとして、DASHとvProのシステムトラップアラートを設定します。
Disable Trap Alert	選択したデバイスでDASHとvProのシステムトラップアラートを無効にします。

- **IPMI**

IPMI Tool Lanplus Command Redirect	選択したBMCデバイスにコマンドリダイレクトを設定します。
FRU Info. Write	BMCデバイスに情報を書き込みます。

- **Settings（設定）**

Settings	選択したBMCデバイスの設定を行います。

- **OOB - Control Help（OOB-制御ヘルプ）**

OOB - Control Help	サポートしているOOB制御機能の説明を見ることができます。

Screen Broadcast（スクリーンブロードキャスト）

Create a broadcast room	ブロードキャストルームを作成し、選択したデバイスにブロードキャストします。

Security and boot settings（セキュリティとブート設定）

ASUS Control Center Expressを使用して設定を行っていない場合、初期値として「Not Config（未構成）」が表示されます。

Enable Regedit	デバイスでWindowsレジストリエディタを有効にします。
Disable Regedit	デバイスでWindowsレジストリエディタを無効にします。
Enable USB	デバイスでUSBポートを有効にします。
Disable USB	デバイスでUSBポートを無効にします。
USB Read Only	デバイスのUSBポートを読み取り専用に設定します。
Fast Startup Enable	デバイスで高速スタートアップを有効にします。
Fast Startup Disable	デバイスで高速スタートアップを無効にします。
Enable Windows Update	デバイスでWindows Updateを有効にします。
Disable Windows Update	デバイスでWindows Updateを無効にします。

Task Scheduler（タスクスケジューラー）

Task Scheduler	選択したデバイスのタスクのスケジュールを設定します。

Software Management（ソフトウェアの管理）

Software Dispatch	ソフトウェアやスクリプトをデバイスへ配布します。
Software Information	デバイスのアプリケーション、プロセス、サービスを表示または設定します。
Software Blacklist	デバイスで禁止されているソフトウェアを表示または追加します。
Installer	デバイスのドライバー、ユーティリティアプリケーション、BIOSをダウンロードまたは更新します。
Software Rule Management	ソフトウェアのブラックリストやホワイトリスト、および通知のメール受信者に関するルールを設定します。

Smart BIOS（スマートBIOS）

BIOS	選択したデバイスのBIOSをアップロード、更新、フラッシュする
Enable BIOS setting	クライアントデバイスのBIOS設定を有効にします。

Report Generator（レポートジェネレーター）

Connection	クライアントデバイスの接続状態（オンライン/オフライン）に関するレポートと分析を生成します。
Software	ソフトウェアのインストールと権限の一覧とレポートを生成します。
Hardware	クライアントデバイスのハードウェアの一覧とレポートを生成します。

Operating Status（動作状態）

Maintenance	デバイスの動作状態をメンテナンスに設定します。
Standby	デバイスの動作状態をスタンバイに設定します。
Normal	デバイスの動作状態を通常に設定します。

Client Agent Updater（クライアントエージェントアップデーター）

Client Agent Updater	クライアントデバイスのエージェントを更新します。

Device Manager（デバイスマネージャー）

Device Manager	デバイスのデバイスマネージャー情報を表示します。

System restore（システム復元）

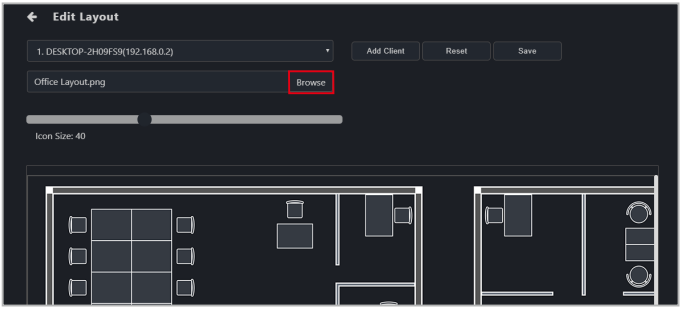
Quick Create	選択したデバイスのシステム復元ポイントを作成します。
System Restore Point	選択したデバイスをシステム復元ポイントから復元します。

2.3 グラフィックビューのカスタマイズ

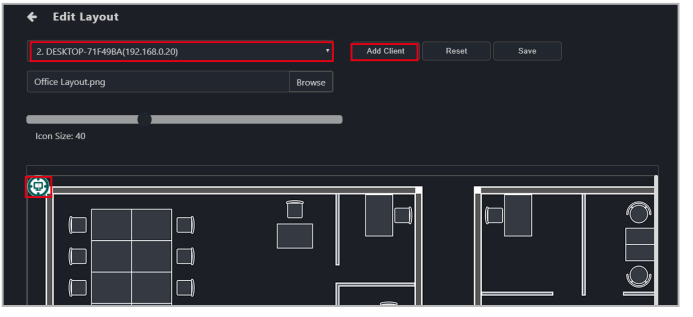
クラシックビューとグラフィックビューを切り替えることができます。グラフィックビューではオフィスのフロアレイアウトイメージなどをアップロードし、レイアウトでクライアントデバイスのショートカットアイコンを配置することができます。

2.3.1 グラフィックビューのカスタマイズ方法（初回）

1. をクリックしてグラフィックビューへ切り替えます。
2. **Edit（編集）**をクリックしてレイアウトファイルを追加します。
3. **Browse（参照）**をクリックして、レイアウトイメージとして使用するイメージファイルを選択しアップロードします。



4. ドロップダウンリストから、クライアントデバイスとして追加するデバイスを選択し、**Add Client（クライアントの追加）**をクリックします。クライアントデバイスのアイコンがバックグラウンドエリアに表示されます。

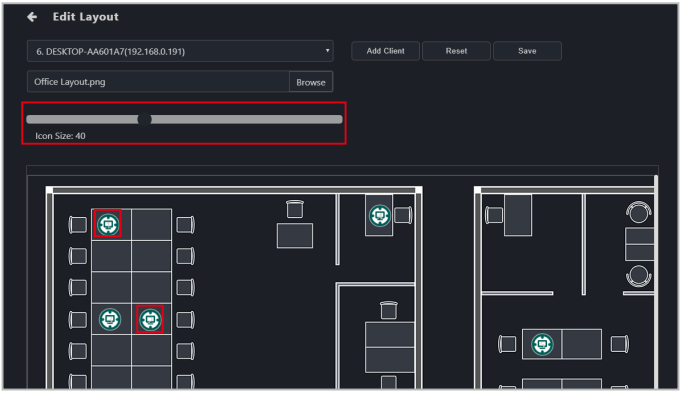


クライアントデバイスには、追加された順に番号が割り当てられます。クライアントデバイスが再配置された場合は、元の番号ではなく新しい連番が割り当てられます。

5. 手順4を繰り返して、複数のクライアントデバイスのアイコンを追加します。

すべてのクライアントデバイスを一度に削除する場合は、**Reset（リセット）**をクリックします。

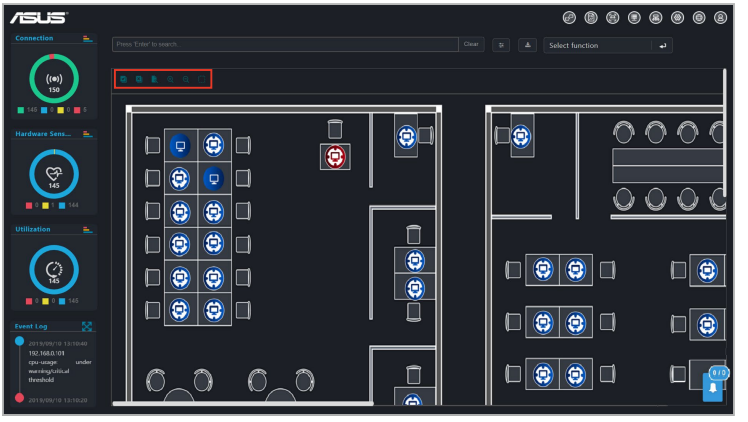
6. クライアントデバイスをクリックして好みの位置へ移動させて、配置することができます。**Icon Size（アイコンサイズ）**スクロールバーを使用して、クライアントデバイスのアイコンのサイズを調整することもできます。



7. カスタマイズが終了したら**Save（保存）**をクリックします。グラフィックビューが再び表示されます。

2.3.2 グラフィックビューのメニュー項目の操作

グラフィックビューで利用可能な各種機能については、次の表を参照してください。



	Check all machines（すべての機器を選択）	レイアウト上のクライアントデバイスすべてを選択します。
	Uncheck all machines（すべての機器の選択を解除）	レイアウト上のクライアントデバイスすべての選択を解除します。
	Edit（編集）	ショートカットアイコンとバックグラウンドを編集します。詳細な手順は **2.3.1 グラフィックビューのカスタマイズ方法（初回）**の手順3～7を参照してください。
	Zoom In（ズームイン）	レイアウトエリアへズームインします。
	Zoom Out（ズームアウト）	レイアウトエリアからズームアウトします。

2.3.3 クライアントデバイスのアイコンの操作

- **クライアントデバイスのアイコンの上にポインターを移動:**
  クライアントデバイスのアイコン上にポインターを移動させると、クライアントの詳細情報が表示されます。表示される情報をカスタマイズする場合は、  （**Customize（カスタマイズ）**）をクリックし、表示する/表示を隠すメタデータの項目にチェックを入れ/外し、続いて**Save（保存）**をクリックします。

- **クライアントデバイスのアイコンをクリック:**
  クライアントデバイスのアイコンをクリックするとアイコンが選択されます。クライアントデバイス（複数を選択可能）の機能を利用できるようになります。選択を解除する場合は、クライアントデバイスのアイコンをもう一度クリックします。

機能の詳細は、**4章 デバイス情報**と**5章 管理機能**を参照してください。

- **クライアントデバイスのアイコンをダブルクリック:**
  クライアントデバイスのアイコンをダブルクリックすると、デバイス情報画面が表示されます。

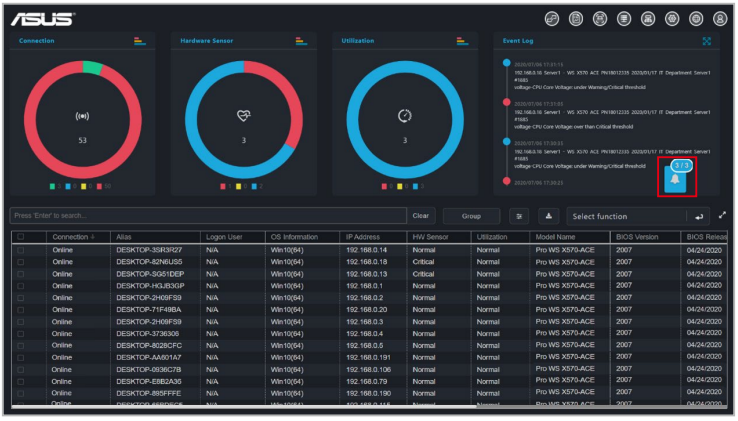
デバイス情報ページの詳細情報については、**4章 デバイス情報**を参照してください。

- **クライアントデバイスのアイコン状態:**
  クライアントデバイスのアイコンは状態に応じて形状や色を変化させます。

未選択	選択済	状態
		オフライン。
		デバイスはオンラインです。ハードウェアセンサーと利用状態は正常です。
		デバイスはオンラインです。ハードウェアセンサーと利用状態は警告状態です。
		デバイスはオンラインです。ハードウェアセンサーと利用状態は重大状態です。

2.4 ミッションセンター

ミッションセンターではタスクの進捗と状況を確認することができます。保留中、終了、進行中のタスク、およびタスクの進捗度と実行結果をすべて、ミッションセンターで確認できます。



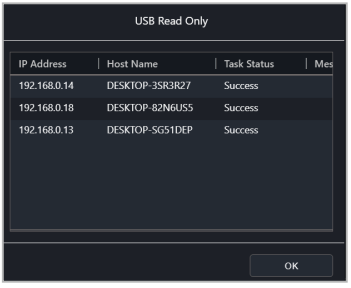
2.4.1 ミッションセンターの操作

ミッションセンターでは多数の操作を実行することができます。詳細は次の一覧をご覧ください。

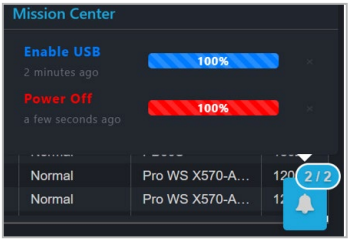
- **ミッションセンターの配置変更：**
  ミッションセンターをクリックし、別の場所へドラッグします。
- **終了したタスク数と合計タスク数の確認：**
  ミッションセンターのアイコン上に、終了したタスク数（左側）と合計タスク数（右側）が表示されます。

- **ミッションセンターの展開/縮小：**
  ミッションセンターのアイコンをクリックするとミッションセンターが展開され、タスクの進捗状況と開始時刻が表示されます。もう一度クリックすると、展開ウィンドウを最小化します。

- **タスク情報の表示：**
  ミッションセンターを展開した状態でタスク名をクリックすると、タスクが実行されているクライアントデバイスを確認でき、各クライアントデバイスの状態または結果も表示されます。



- **失敗したタスク：**
  失敗したタスクは、ミッションセンターに赤で表示されます。タスク名をクリックすると、失敗したタスクの詳細が表示されます。



2.4.2 ミッションセンターのタスク

次の表は、ミッションセンターで確認可能なタスクの一覧です。

- タスクの進捗バー脇にある「**X**」をクリックすると、終了したタスクが削除されます。削除できるのは終了したタスクのみです。保留中または進行中のタスクは、終了するまで削除できません。
- 複数のステップに分割されたタスクも、ミッションセンターで完了させることができます。例えば、BIOSの更新後にクライアントデバイスを再起動するタスクの場合、BIOS更新のステップが終了次第、ミッションセンターを介してクライアントデバイスを再起動することができます。
- ミッションセンターはASUS Control Center Expressのメインサーバーへ現在進行中のタスクを記録します。ASUS Control Center Expressのメインサーバーがシャットダウンされ再起動された場合、ミッションセンターのタスクはリセットされ、ASUS Control Center Expressのメインサーバーが再起動した後に、進行中のタスクのみを記録します。

Power Control（電源制御）		Power Off（電源オフ）/Power On（電源オン）/ Restart Computer（コンピューターの再起動）
Security Control（セキュリティ制御）	**Registry Tool（レジストリツール）**	Enable Regedit（レジストリエディタを有効）
		Disable Regedit（レジストリエディタを無効）
	USB Control（USB制御）	Enable（有効）/Disable（無効）
		Read Only（読み取り専用）
	Fast Startup（高速スタートアップ）	Enable（有効）/Disable（無効）
Software Management（ソフトウェアの管理）		Software Dispatch（ソフトウェアを配信）
		Software Blacklist（ソフトウェアのブラックリスト）
		Installer（インストーラー）
Smart BIOS（スマートBIOS）		BIOS update（BIOS更新）
Client Agent Updater（クライアントエージェントアップデーター）		Update client device's agent（クライアントデバイスエージェントの更新）
Settings Migrator（設定の移行ツール）		Migrate server settings（サーバー設定を移行）
Main Server Settings（メインサーバーの設定）		Agent deployment（エージェントの配置）
OOB-Control（OOB-制御）*		Power Control（電源制御）
		Watchdog（ウォッチドッグ）
		BIOS
		Account Management（アカウント管理）
		System（システム）
		KVM
		USB Redirection（USB リダイレクト）
		Firmware Update（ファームウェアの更新）
		Trust Zone（トラストゾーン）
		Certificate Management（証明書管理）
		System Trap Alert（システムトラップアラート）
		IPMI
		Settings（設定）
		Configuration（構成）

* **この機能はリモート管理コントローラーをサポートするマザーボードでのみ使用できます。**

3章

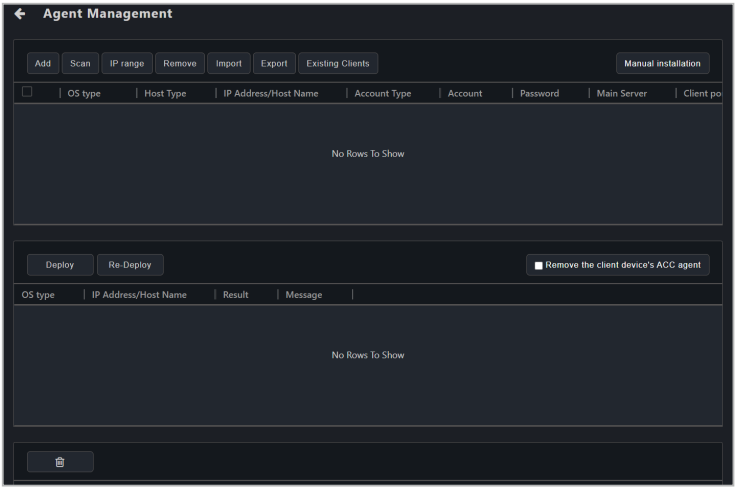
本章はASUS Control Center Expressの
エージェントを自動または手動で配置、
削除、更新する方法を説明します。

配置管理

3.1 エージェント管理の概要

エージェント管理メニューでは、ASUS Control Center Expressのエージェントを管理することができます。エージェントの自動インストールや手動削除などを実行できます。

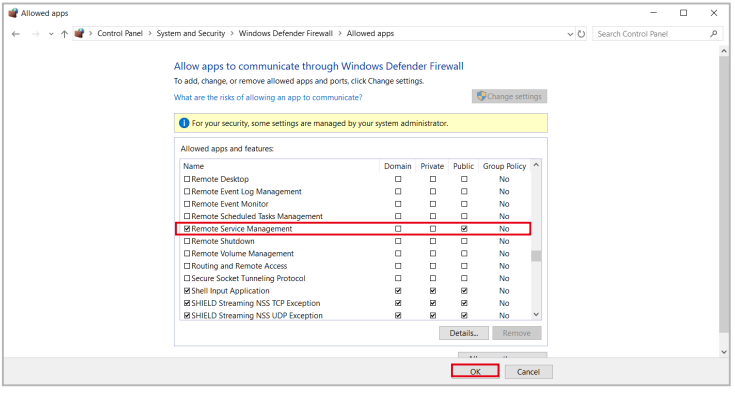
右上のメニューバーで をクリックすると**Agent Management（エージェント管理）**の画面が開きます。



Add（追加）	エージェントを配置するデバイスを1台追加します。
Scan（スキャン）	エージェント配置が可能なメインサーバーと同じサブネット内のすべてのクライアントデバイスを自動的にスキャンします。
IP Range（IP範囲）	スキャンしたいIP範囲を入力します。
Remove（削除）	エージェントを配置しないクライアントデバイスを削除します。
Import（インポート）	すでにエクスポートされているデバイスリスト（.csvファイル）をインポートします。
Export（エクスポート）	追加またはスキャンされたデバイスの現在のデバイスリストを.csvファイルにエクスポートします。
Existing Clients（既存クライアント）	エージェントが配置されているクライアントデバイスをすべて表示します。
Manual Installation（手動インストール）	エージェントのインストールファイルをダウンロードして、手動でクライアントデバイスにエージェントをインストールするか、サイレントモードでエージェントをインストールします。
Deploy（配置）	選択されたクライアントデバイスにエージェントを自動的に配置します。
Re-Deploy（再配置）	すでにエージェントがインストールされているクライアントデバイスのエージェントを修復します。
Remove the client device's ACC agent（クライアントデバイスのACCエージェントの削除）	ACC CSMエージェントがすでにクライアントデバイスにインストールされている場合、このオプションをチェックすると、ASUS Control Center Expressエージェントを配置する際にACC CSMエージェントが自動的に削除されます。

配置を開始する前に、次のことをご確認ください：

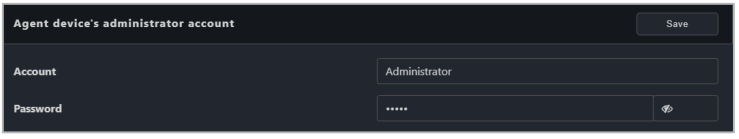
- エージェントを配置する前に、ライセンスキーを有効にする必要があります。エージェントを配置する各クライアントデバイスには、対応するライセンスキーが必要です。ライセンスのアクティベーション方法については、**8.1.4 ライセンス** を参照してください。
- クライアントとACCEサーバーは同じネットワークドメインに配置する必要があります。
- クライアントデバイスのファイアウォール設定でリモートサービス管理を有効にしてください。（Windows**Start（スタート）**アイコンを右クリックし、**Settings（設定）** > **Update & Security（更新とセキュリティ）** > **Windows Security（Windowsセキュリティ）** > **Firewall & network protection（ファイアウォールとネットワーク保護）** > **Allow an app through firewall（ファイアウォールによるアプリケーションの許可）**を選択します。）



- クライアントデバイスのアンチウイルスファイアウォールを一時的に無効にします。エージェントの配置が完了したら、アンチウイルスのファイアウォールを再度有効にすることができます。アンチウイルスのファイアウォールを無効にする手順は、お使いのアンチウイルスの取扱説明書や製品ウェブサイトを参照してください。
- システム言語に応じて、エージェントデバイスでデフォルト設定された管理者アカウント名とパスワードは異なる場合があります。配置前に、エージェントデバイスの管理者アカウント名とパスワードが、クライアントデバイスの管理者アカウント名とパスワードに一致することを確認してください。
- クライアントデバイスのシステム時刻と日付は、必要でない限り変更しないでください。

- クライアントの管理者アカウントではパスワードを設定できるようにしてください。このデバイスへ配置する際に、そのアカウント名とパスワードを正確に入力してください。アカウント名とパスワードが入力されない場合、デフォルトのアカウント名とパスワードが使用されます。アカウント情報を確認して編集する場合は、**Settings（設定）** > **Options（オプション）** > **General Configurations（全般設定）** > **Agent device's administrator account（エージェントデバイスの管理者アカウント）**で行えます。詳細は**8.1.3 全般設定**を参照してください。

  管理者アカウント設定はWindowsのバージョンに応じて異なります。Windowsのアカウント設定に関する詳細情報は、Microsoftのウェブサイトを参照してください。



- エージェントがクライアントデバイスに配置済みであり、再配置が必要な場合、事前にエージェントをクライアントデバイスから削除してください。詳細は**3.3 エージェントの削除**を参照してください。
- **再配置**機能は、ASUS Control Express v1.5以前のバージョンをアップグレードする場合と、エージェントを修復する場合にのみ使用されます。
- メインサーバーまたはクライアントデバイスがWindows 7 オペレーティングシステムを使用している場合は、エージェントを配置する前にメインサーバーへ.Net Framework 4.6.1以上、SHA-2、TLS 1.2 をインストールしてください。詳細は、**3.2.8 Windows 7 配置環境の設定** を参照してください。
- Windows 7 オペレーティングシステムのクライアントデバイスがSHA-2およびTLS 1.2に対応していない場合でも、クライアントデバイスにエージェントを配置する際に必要なインストールが行われます。エージェント配置の終了後、指示に従ってクライアントデバイスをリセットしてから、クライアントデバイスでエージェント配置プロセスをやり直してください。
- メインサーバーまたはクライアントデバイスがWindows 11 オペレーティングシステムを実行している場合は、インターネットに接続してからWindows Updateを実行し、エージェントを配置する前にWindows Defenderが最新のバージョンに更新されていることを確認してください。

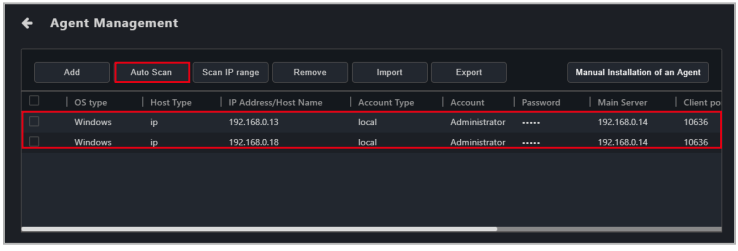
3.2 エージェントの配置

デバイスへエージェントを新しくインストールし、ASUS Control Center Express サーバーへ追加すれば、管理、監視、制御を手軽に行えます。

エージェントを配置する前に、ライセンスキーを有効にする必要があります。エージェントを配置する各クライアントデバイスには、対応するライセンスキーが必要です。ライセンスのアクティベーション方法については、**8.1.4 ライセンス** を参照してください。

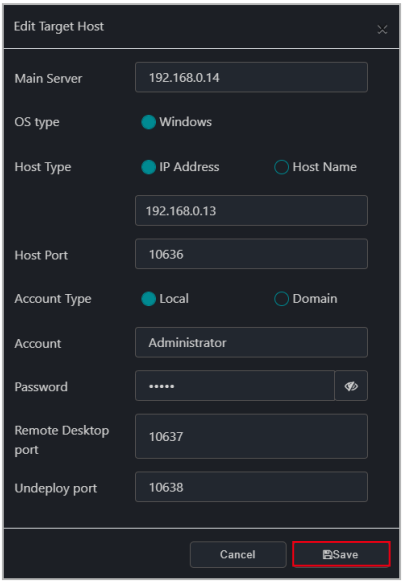
3.2.1 自動的にスキャンしてデバイスへ配置

1. **Auto Scan（自動スキャン）**をクリックします。
2. スキャンが完了すると、次のような画面にスキャン結果が表示されます。



3. スキャンされたデバイスをダブルクリックするとデバイス情報を編集することができます。編集が終了したら、**Save（保存）**をクリックしてください。

- **Account（アカウント）**欄には管理者権限を有するアカウントを入力してください。
- デフォルトで表示されるアカウントはエージェントデバイスの管理者アカウント名とパスワードです。編集する場合は、**Settings（設定）** > **Options（オプション）** > **General Configurations（全般設定）** > **Agent device's administrator account（エージェントデバイスの管理者アカウント）**で行えます。詳細は**8.1.3 全般設定**を参照してください。



4. スキャンされたデバイス情報の編集が終了したら、エージェントを配置するデバイスを選択し、**Deploy（配置）**をクリックします。

ACC CSMがすでにクライアントデバイスにインストールされている場合は、エージェントを配置する前にデータをエクスポートしてバックアップし、**Remove the client device's ACC agent（クライアントデバイスのACCエージェントを削除）**を有効にしてください。

5. 配置終了後に、配置結果を一覧で確認することができます。

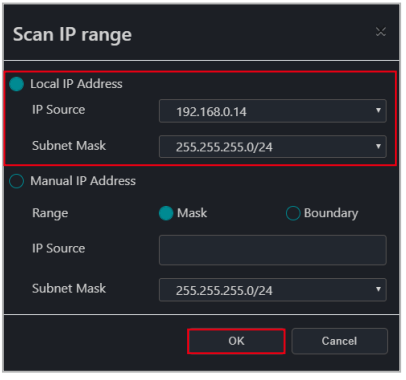
3.2.2 IP範囲のスキャン

ネットワーク環境によっては、スキャンするデバイスのIPアドレスの範囲を指定し、エージェントを素早く効率的に配置することができます。

メインサーバーのIPアドレス

メインサーバーのIPアドレスをスキャン範囲として設定することができます。

1. **Scan IP range**（**IP範囲のスキャン**）をクリックし、**Local IP Address**（**ローカルIPアドレス**）を選択します。
2. **IP Source**（**IPソース**）欄でメインサーバーのIPアドレスを選択し、**Subnet Mask**（**サブネットマスク**）欄でスキャンするサブネットマスクの範囲を選択します。
3. **OK**をクリックしてスキャンを開始します。



4. スキャンされたデバイスをダブルクリックするとデバイス情報を編集することができます。編集が終了したら、**Save**（**保存**）をクリックしてください。
5. スキャンされたデバイス情報の編集が終了したら、エージェントを配置するデバイスを選択し、**Deploy**（**配置**）をクリックします。

ACC CSMがすでにクライアントデバイスにインストールされている場合は、エージェントを配置する前にデータをエクスポートしてバックアップし、**Remove the client device's ACC agent**（**クライアントデバイスのACCエージェントを削除**）を有効にしてください。

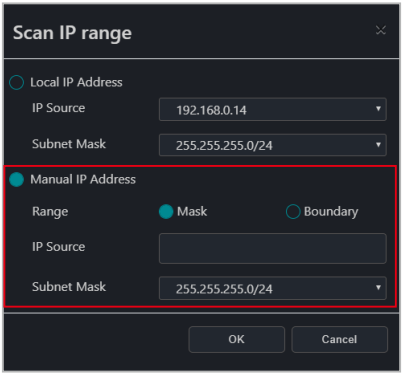
6. 配置終了後に、配置結果を一覧で確認することができます。

クライアントデバイスのIPアドレス

クライアントデバイスのIPアドレスをスキャン範囲として設定することができます。

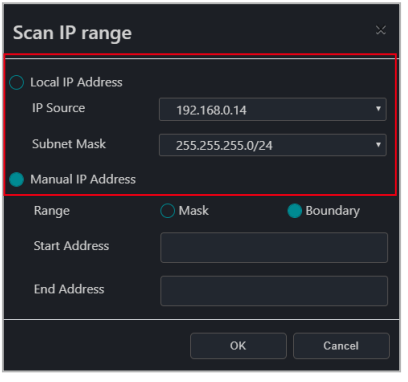
1. **Scan IP range（IP範囲のスキャン）**をクリックし、**Manual IP Address（手動IPアドレス）**を選択します。
2. **Mask（マスク）**を選択して暗いアンドデバイスのサブネットマスクの範囲をスキャンするか、**Boundary（境界）**を選択して**Range（範囲）**欄に開始IPアドレスと終了IPアドレスを入力します。

Mask（マスク）：



IP Source（IPソース）	クライアントデバイスのIPアドレスを入力します。
Subnet Mask（サブネットマスク）	スキャンするサブネットマスクの範囲を選択します。
NIC（ネットワークカード）	スキャンするメインサーバーのネットワークカード（NIC）のIPアドレスを選択します。

Boundary（境界）：



Start Address（開始アドレス）	スキャンするクライアントデバイスの開始IPアドレスを入力します。
End Address（終了アドレス）	スキャンするクライアントデバイスの終了IPアドレスを入力します。
NIC（ネットワークカード）	スキャンするメインサーバーのネットワークカード（NIC）のIPアドレスを選択します。

3. **OK**をクリックしてスキャンを開始します。
4. スキャンされたデバイスをダブルクリックするとデバイス情報を編集することができます。編集が終了したら、**Save（保存）**をクリックしてください。
5. スキャンされたデバイス情報の編集が終了したら、エージェントを配置するデバイスを選択し、**Deploy（配置）**をクリックします。

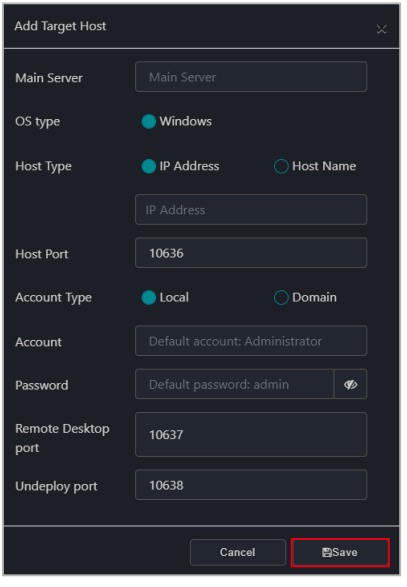
ACC CSMがすでにクライアントデバイスにインストールされている場合は、エージェントを配置する前にデータをエクスポートしてバックアップし、**Remove the client device's ACC agent（クライアントデバイスのACCエージェントを削除）**を有効にしてください。

6. 配置終了後に、配置結果を一覧で確認することができます。

3.2.3 追加してデバイスへ配置

単一デバイスを追加

1. **Add（追加）**をクリックします。
2. 追加するデバイスの情報を入力し、**Save（保存）**をクリックします。



Main Server（メインサーバー）	ASUS Control Center Expressサーバーの IPアドレスを入力します。
OS Type（オペレーティングシステムタイプ）	クライアントのオペレーティングシステムのタイプを選択します。
Host Type（ホストタイプ）	**IP Address（IPアドレス）**を選択してクライアントのIPアドレスを入力します。 または **Host name（ホスト名）**を選択してクライアントの名前を入力します。
Host Port（ホストポート）	ポート名を入力します。
Account Type（アカウントタイプ）	クライアントのアカウントをローカルまたはドメインから選択します。 **Local:** エージェントの管理者権限はエージェントがインストールされたデバイスのみを管理することができます。 **Domain:** エージェントの管理者権限はドメイン内のデバイスすべてを管理することができます。
Domain（ドメイン）*	ドメイン名を入力します。
Account（アカウント）	クライアントの管理者アカウント名を入力します。
Password（パスワード）	クライアントの管理者アカウントのパスワードを入力します。
Remote Desktop port（リモートデスクトップポート）	このクライアントへリモートでアクセスする際のポートを入力します。
Undeploy（配置解除）	このクライアントからエージェントを削除する際のポートを入力します。

* **この項目はアカウントのタイプとしてドメインを選択した場合にのみ表示されます。**

3. **Save（保存）**をクリックすると、デバイスがデバイス一覧に出現します。
4. デバイス一覧からエージェントを配置するデバイスを選択して、**Deploy（配置）**をクリックします。

ACC CSMがすでにクライアントデバイスにインストールされている場合は、エージェントを配置する前にデータをエクスポートしてバックアップし、**Remove the client device's ACC agent（クライアントデバイスのACCエージェントを削除）**を選択してください。

5. 配置終了後に、配置結果を一覧で確認することができます。

複数デバイスを追加

ASUS Control Center Expressのエクスポート済デバイス一覧のCSVファイルが既に存在する場合は、Import（インポート）機能を使用して複数のデバイスを一度にインポートし配置することができます。

1. **Import（インポート）**をクリックします。
2. インポートするCSVファイルを選択し、**Open（開く）**をクリックします。
3. インポートされるデバイスがデバイス一覧に表示されます。エージェントを配置するデバイスを選択し、**Deploy（配置）**をクリックします。

ACC CSMがすでにクライアントデバイスにインストールされている場合は、エージェントを配置する前にデータをエクスポートしてバックアップし、**Remove the client device's ACC agent（クライアントデバイスのACCエージェントを削除）**を有効にしてください。

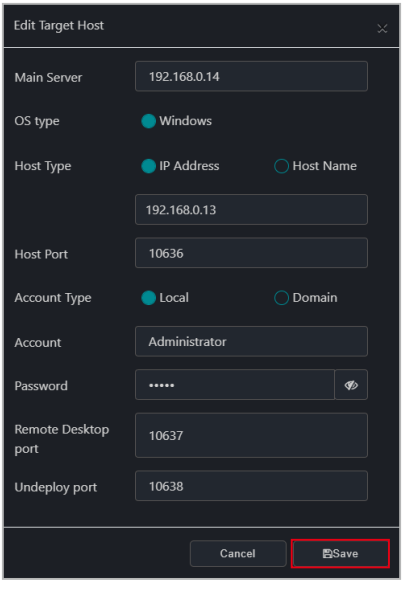
4. 配置終了後に、配置結果を一覧で確認することができます。

Export（エクスポート）をクリックすると現在のデバイス一覧がCSVファイルへエクスポートされます。テキストエディタを使用して編集することができます。

3.2.4 デバイス情報の編集

エージェントを配置する前に、スキャンまたは追加したデバイスのデバイス情報を編集することができます。

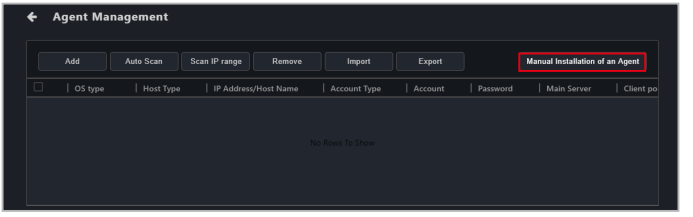
1. 編集するデバイスをダブルクリックします。
2. 終了したら**Save（保存）**をクリックします。



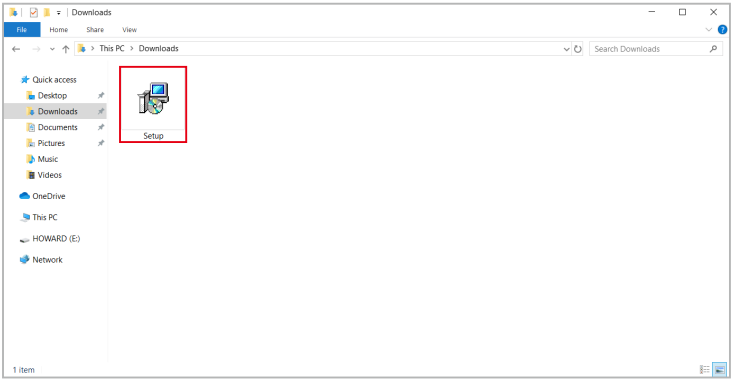
3.2.5 エージェントの手動インストール

クライアントデバイスへのエージェントのインストール

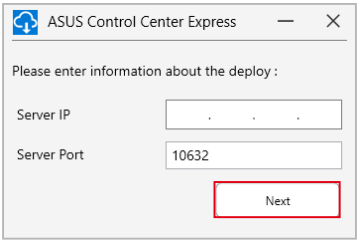
1. **Manual Installation of an Agent（エージェントの手動インストール）**をクリックして、インストールファイル（Setup.msi）をダウンロードします。



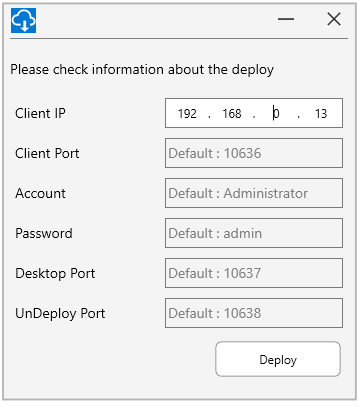
2. USBメモリーなどの外付けストレージデバイスを使用し、エージェントをインストールするクライアントへ**Setup.msi**をコピーして貼り付けます。
3. クライアントデバイスで**Setup.msi**ファイルをダブルクリックし、インストールを開始します。



4. メインサーバーのIPアドレスを**Server IP（サーバーIP）**欄へ入力し、**Next（次へ）**をクリックします。必要であれば、**Server Port（サーバーポート）**欄のデフォルトのポートを変更することもできます。



5. メインサーバーがクライアントデバイスの情報を受信できるか、確かめてください。デフォルトのポートが既に使用されている場合、ASUS Control Center Expressのメインサーバーを介して、インストール後に調整を行ってください。



6. **Deploy（配置）**をクリックし、配置が完了するまで待ちます。

メインサーバーへのエージェントのインストール

メインサーバーにエージェントを手動でインストールして、ASUS Control Center Expressを介して管理およびメンテタンスタスクを実行することもできます。

- メインサーバーは、スクリーンブロードキャストのブロードキャストソースとしてのみ使用できます。
- リモートデスクトップ機能を使用してメインサーバーを制御した場合、ビデオフィードバックループエフェクトが発生することがあります。

1. **Manual Installation of an Agent**（エージェントの手動インストール）をクリックして、インストールファイル（Setup.msi）をダウンロードします。
2. Setup.msiファイルをダブルクリックし、インストールを開始します。
3. メインサーバーのIPアドレスまたは 127.0.0.1 を**Server IP（サーバーIP）**欄へ入力し、**Next（次へ）**をクリックします。必要であれば、**Server Port（サーバーポート）**欄のデフォルトのポートを変更することもできます。
4. メインサーバーがクライアントデバイスの情報を受信できることを確認します。デフォルトのポートが既に使用されている場合、ASUS Control Center Expressのメインサーバーを介して、インストール後に調整を行ってください。
5. **Deploy（配置）**をクリックし、配置が完了するまで待ちます。

3.2.6　サイレントモードでのエージェントのインストール

サイレントモードのインストールパラメータ

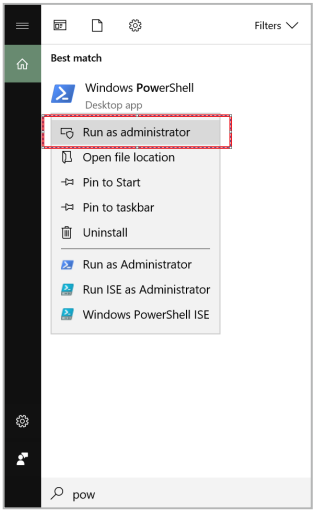
Server IP（サーバーIP）	ASUS Control Center Expressサーバー IP（必須）
Client IP（クライアントIP）	ローカルホストIP（必須）
Client port（クライアントポート）	ローカルホストポート（オプション）
Account（アカウント）	ローカルホストユーザーアカウント（オプション）
Password（パスワード）	ローカルホストユーザーパスワード（オプション）
Outfail（アウトフェイル）	配置失敗をファイルにダンプ（オプション）

フィードバック結果

0 ERROR_SUCCESS	アクションが正常に完了
1602 ERROR_INSTALL_USEREXIT	ユーザーによるインストールのキャンセル
1603 ERROR_INSTALL_FAILURE	インストール時の致命的なエラー
1639 ERROR_INVALID_COMMAND_LINE	無効なコマンドライン引数

下記の例をご参照ください

1.Windows PowerShellを管理者として実行します。



2. エージェントのインストールを実行するコマンドを入力します。
(Start-Process msiexec '/i "C:\Setup.msi" serverip=192.168.1.2 /qb -Wait -Passthru) .ExitCode

配置時の詳細

1. コマンドラインにoutfailパラメータを追加してください。
(Start-Process msiexec '/i "F:\ Setup.msi" serverip=192.168.1.2 clientip=192.168.1.200 **outfail**="D:\New folder\Fail.txt" /qb ' -Wait -Passthru) .ExitCode

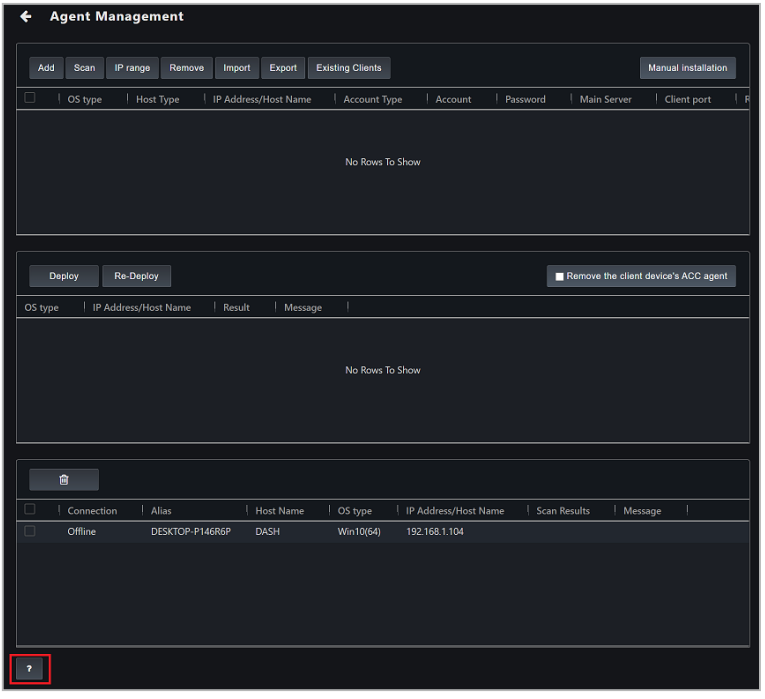
2. インストールが完了すると、結果がD:\New Folder\Fail.txt.に保存されます。

クライアントデバイスが既にエージェントにインストールされており、再インストールする必要がある場合

1. インストールしたエージェントをクライアントデバイスから削除してください。
(Start-Process msiexec '/x "C:\ Setup.msi" /q ' -Wait -Passthru) .ExitCode
2. エージェントのインストールコマンドを実行します。
(Start-Process msiexec '/i "C:\Setup.msi" serverip=192.168.1.2 /qb -Wait -Passthru) .ExitCode

3.2.7 エージェントのアップグレードまたは修復

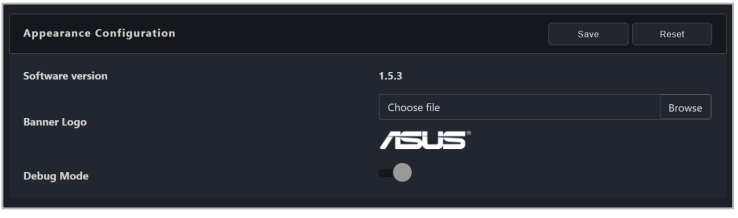
ASUS Control Center Expressのバージョンが1.4.27以前の場合、クライアントデバイスを再起動すると、一部機能が正常に動作しない場合があります。次の手順、または**Agent Management（エージェント管理）**ページ下部の情報アイコンをクリックして、エージェントのアップグレードまたはエージェントの修復を行ってください。



エージェントのアップグレードや修理を行う前に、ASUS Control Center Expressのバージョンを確認してください。

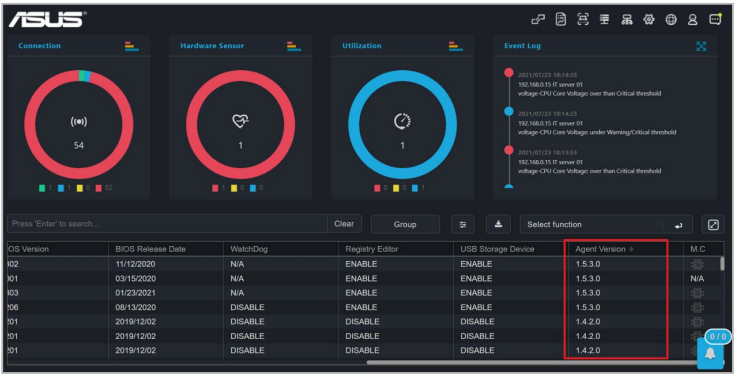
- ASUS Control Center Expressメインソフトウェアバージョン

  Settings（設定）>**Options（オプション）**>**General Configuration（全般設定）**と進み、**Appearance Configuration（表示設定）**ブロックまでスクロールすると、ソフトウェアのバージョンが表示されます。

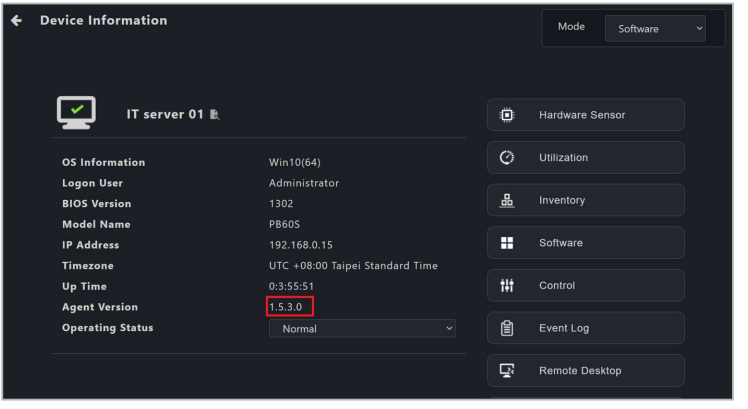


- クライアントデバイスのエージェントバージョン

  クライアントデバイスのエージェントバージョンは、デバイス概要のデバイスリストの**Agent Version（エージェントバージョン）**欄に表示されます。



また、クライアントデバイスをクリックすると、**Device Information（デバイス情報）**ページでシングルクライアントデバイスのエージェントバージョンが表示されます。

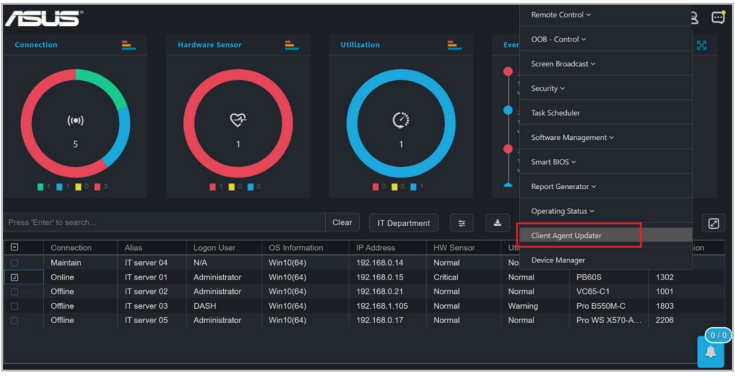


バージョン1.4.XXからバージョン1.5.Xへの更新

1. ASUS Control Center Expressの最新版（1.5.X以降）をダウンロードし、メインサーバーにASUS Control Center Expressメインソフトウェアのインストールを実行します。

2. インストールの完了後、デバイスリストから更新や修復を行いたいデバイスにチェックを入れ、ショートカット機能のドロップダウンメニューから**Client Agent Updater**（**クライアントエージェントアップデータ**）を選択します。

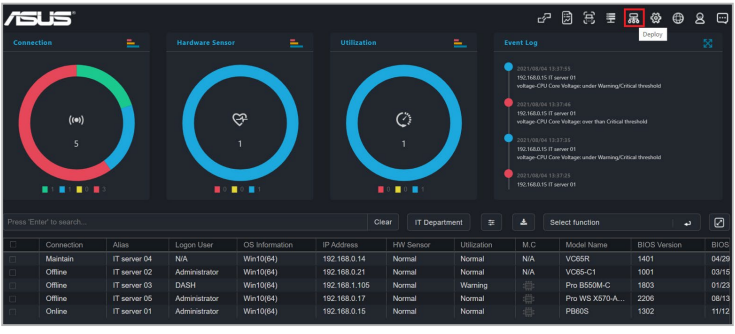
詳細は**2.2.6 ショートカット機能の使用** を参照してください。



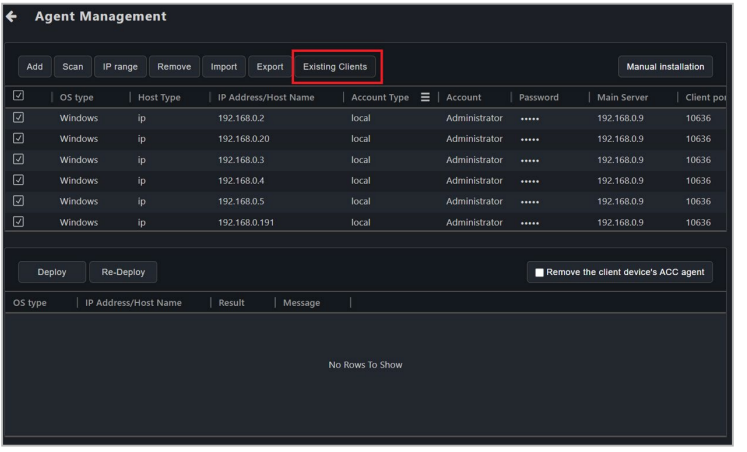
3. 確認のポップアップウィンドウで**Yes**（はい）をクリックし、更新を続行します。
4. ミッションセンターで配置されるエージェントと更新の結果を確認することができます。

バージョン1.3.X以前のバージョンからバージョン1.5.Xへの更新

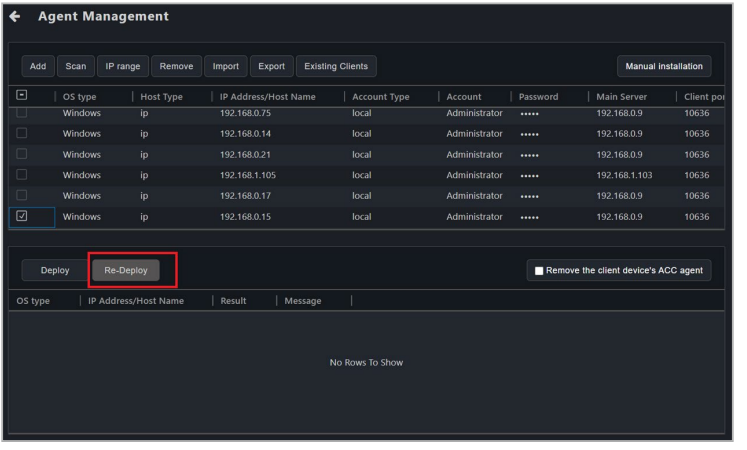
1. ASUS Control Center Expressの最新版（1.5.X以降）をダウンロードし、メインサーバーにASUS Control Center Expressメインソフトウェアのインストールを実行します。
2. メインメニューの右上のメニューバーにある をクリックします。



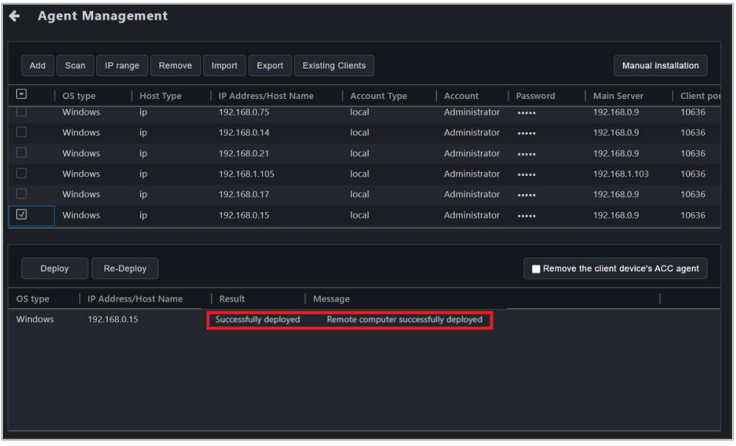
3. **Existing Clients（既存クライアント）**をクリックすると、エージェントが配置されているすべてのクライアントデバイスが読み込まれ、表示されます。



4. エージェントが配置されているクライアントデバイス一覧が読み込まれたら、管理者アカウントやパスワードなど、クライアントデバイスの情報が正しいかどうかを確認してください。詳細は **3.2.4 デバイス情報の編集** を参照してください。クライアントデバイスの情報が正しいことを確認したら、**Re-Deploy（再配置）**をクリックします。



5. 再配置終了後に、再配置結果を一覧で確認することができます。



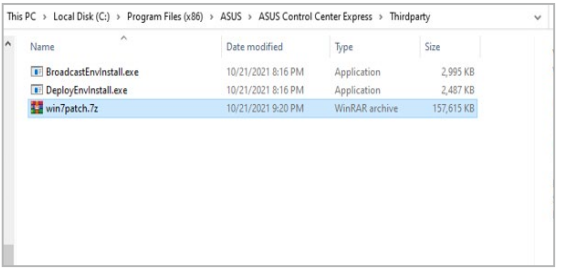
3.2.8 Windows 7 配置環境の設定

メインサーバーまたはクライアントデバイスがWindows 7 オペレーティングシステムを使用している場合、エージェントの配置前にWindows 7 オペレーティングシステム環境を設定する必要があります。

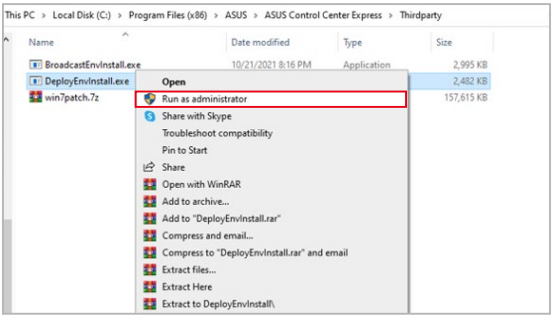
ウイルス対策ソフトウェアの互換性がないため、Windows 7 を実行しているクライアントデバイスでは一部機能が利用できない場合があります。

1. Windows 7のエージェント配置環境を設定するために必要な**win7patch**インストールファイルをASUS Webサイトからダウンロードします。
2. **win7patch**のZIPファイルをASUS Control Center Express\Thirdparty のインストールフォルダにある配置環境設定ファイル（**DeployEnvInstall.exe**）と同じフォルダに移動します。

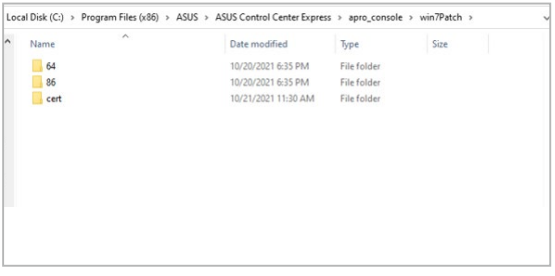
ASUS Control Center Expressのデフォルトインストールパスは、ASUS Control Center Express\Thirdpartyです。ASUS Control Center Expressのインストール時に異なるパスを選択した場合、それに応じてインストールフォルダのパスを変更してください。



3. 管理者として**DeployEnvInstall.exe**を実行し、配置環境の設定を行います。



4. Windows 7の配置に必要なファイルが、ASUS Control Center Express\apro_consoleフォルダに正しくインストールされていることを確認します。

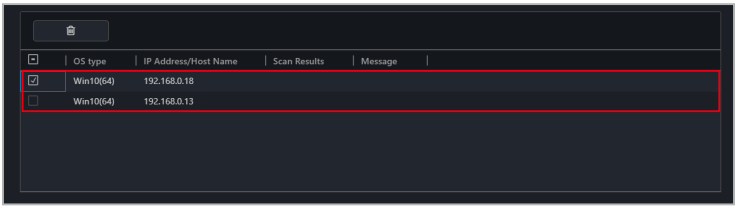


3.3 エージェントの削除

本セクションは、エージェントを再配置または削除する場合にエージェントを削除する手順を紹介します。

3.3.1 メインサーバーからのエージェントの削除

1. Agent Management（エージェント管理）ページで、1台のクライアントデバイスをダブルクリックしてそのデバイス上のエージェントを削除するか、エージェントを削除したい複数のクライアントデバイスをクリックしてチェックします。



2. **Remove（削除）**アイコン をクリックし、**OK**をクリックして選択したデバイスからエージェントを削除します。

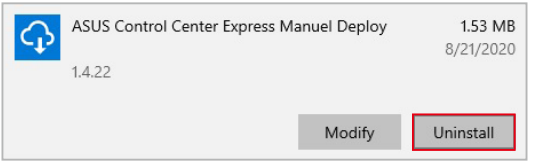
選択したクライアントデバイスがオフラインの場合、エージェントはクライアントデバイスがオンラインに復帰した際に削除されます。

3.3.2 手動でインストールしたエージェントの削除

クライアントデバイスへエージェントを手動でインストールした場合、次の手順に従ってエージェントを削除してください。

- エージェントが配置されているクライアントデバイスが修理やメンテナンスの最中の場合、まずクライアントデバイスからエージェントを削除し、続いてそのデバイスへ別のエージェントを再配置してください。デバイスへエージェントを配置する手順は、**3.2 エージェントの配置**を参照してください。
- クライアントデバイスから手動でエージェントを削除するだけでなく、クライアントデバイスをASUS Control Center Expressからも削除してください。

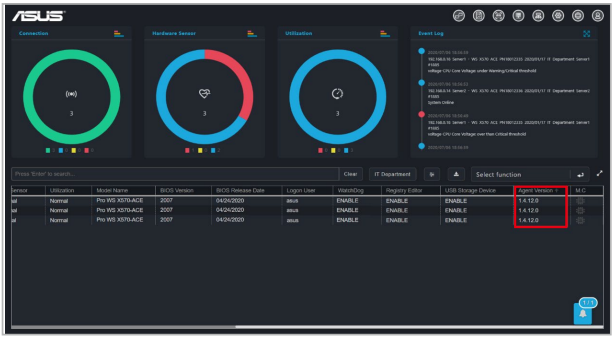
1. ASUS Control Center Expressサーバーからデバイスを削除します。詳細は**3.3.1 メインサーバーからのエージェントの削除**を参照してください。
2. クライアントデバイスで、**Apps & features（アプリと機能）**メニューを選択します。
3. ASUS Control Center Express Manual Deploy（ASUS Control Center Expressの手動配置）をクリックして、**Uninstall（アンインストール）**をクリックします。

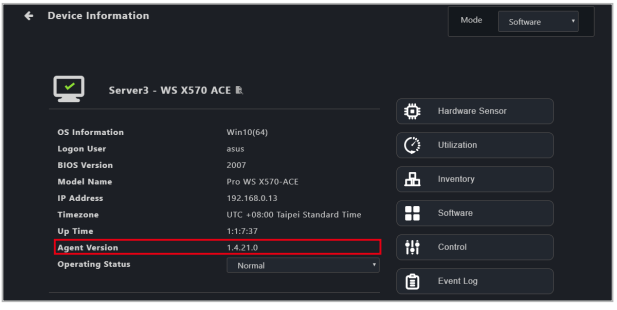


3.4 クライアントエージェントアップデーター

ASUS Control Center Expressのメインサーバーが更新された場合、**Client Agent Updater（クライアントエージェントアップデーター）**を使用してすべてのクライアントデバイスのエージェントを簡単に更新することができ、メインサーバーとクライアントのエージェントの両方を素早く最新の状態に保つことができます。

メインメニューページのデバイス概要または**Device Information（デバイス情報）**のページから、エージェントの現在のバージョンを確認することができます。

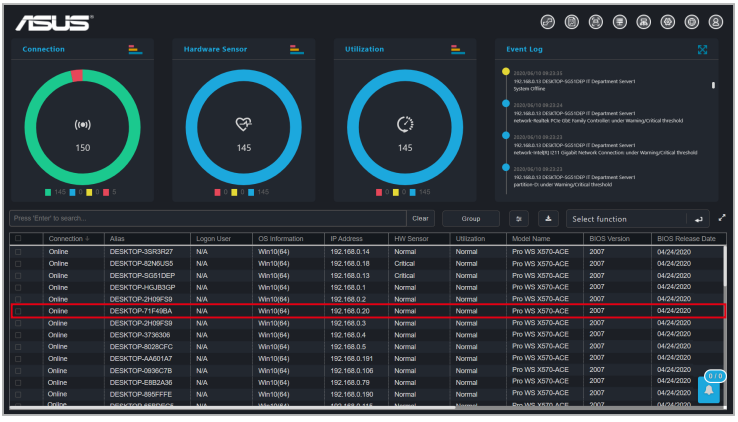




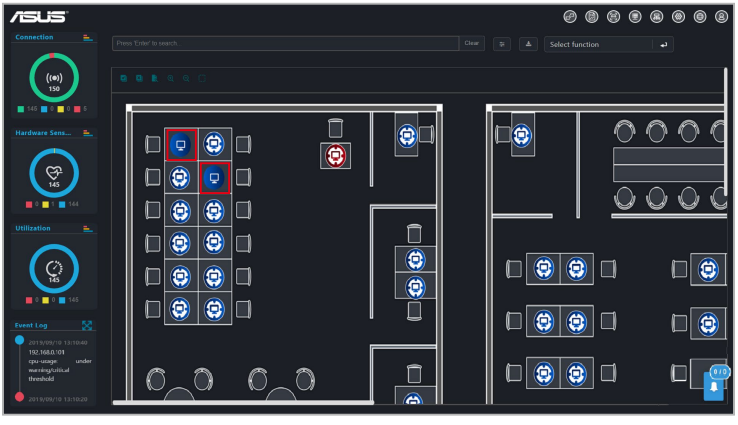
3.4.1 エージェントの更新

1. エージェントを更新するデバイスを選択します。

クラシックダッシュボード

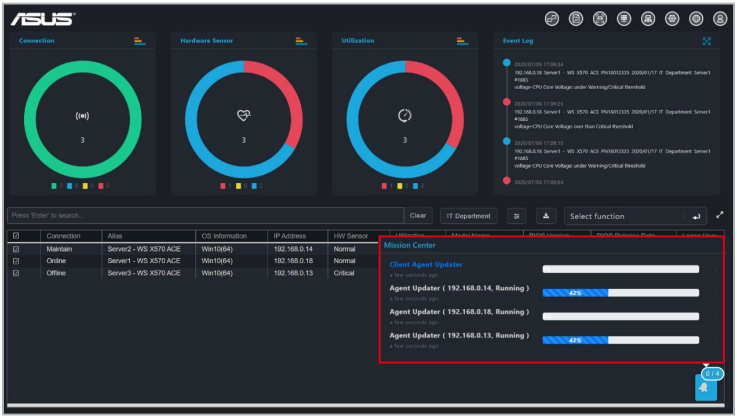


グラフィックダッシュボード

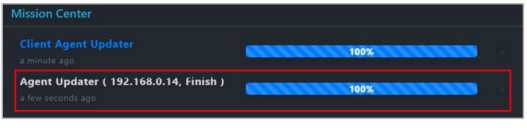


2. **Select function（機能の選択）**をクリックし、ドロップダウンメニューから**Client Agent Updater（クライアントエージェントアップデーター）**を選択します。
3. 確認用のポップアップウィンドウで**Yes（はい）**をクリックします。

4. ミッションセンターで配置されるエージェントと更新の進捗状況を確認することができます。



- エージェントの更新は、オンラインのクライアントデバイスでのみ実行することができます。複数のデバイスを選択した際に一部のデバイスがオフラインとなっている場合、ミッションセンターで配置と更新の失敗に関するメッセージを表示します。オフラインのデバイスは、オンラインに復帰後に再度更新することができます。
- エージェントの更新時に接続が不安定な場合、ミッションセンターのエージェント更新の状態は**Finish**(**終了**)と表示され、タスク名がグレーアウトしてクリックすることはできません。クライアントデバイスのエージェントは更新前のバージョンへ戻ります。オフラインのデバイスは、オンラインに復帰後に再度更新することができます。
- エージェントの更新時にクライアントデバイスが電源オフまたは再起動された場合、ミッションセンターのエージェント更新の状態は**Finish**(**終了**)と表示され、タスク名がグレーアウトしてクリックすることはできません。クライアントデバイスが再起動されオペレーティングシステムに移行すると、更新プロセスが再開されます。



- ASUS Control Center Expressのメインサーバーのバージョンが既に v1.4.x 以降に更新されているが、クライアントデバイスのエージェントが更新されていない場合 (v1.3.x) は、一部の機能に影響が出る可能性があります。

4章

本章はデバイスを管理するためのデバイス情報とソフトウェア制御の機能を説明します。

デバイス情報

4.1 デバイス情報の概要

Device Information Overview（デバイス情報の概要）には選択したクライアントデバイスの詳細情報が表示されます。また、電源制御機能など、ソフトウェア制御の管理機能も提供されます。

クライアントデバイスの**Device Information（デバイス情報）**は複数の方法で表示することができます。

- クラシックビュー：デバイス一覧でクライアントデバイスを1回クリックします。
- グラフィックビュー：クライアントデバイスのショートカットアイコンをダブルクリックします。

- 本章では**Software Mode（ソフトウェアモード）**の機能のみを説明しています。ハードウェアモードの機能に関しては、**5章 管理機能**を参照してください。**Hardware Mode（ハードウェアモード）**（アウトオブバンド管理）の機能は、RTL 8117 LAN ICに対応した管理LANポートを使用してクライアントデバイスが接続されている場合にのみ使用できます。
- ほとんどの機能は、クライアントデバイスがオンライン状態にあり、オペレーティングシステムへログインされた状態でのみ使用することができます。
- 一部の機能は、次の要件が満たされた場合にのみ使用することができます：
  - クライアントデバイスがオンラインにありオペレーティングシステムにログインしている
  - エージェントがすでに配置されている
  - RTL 8117 LAN ICに対応した管理LANポートを使用して接続されている

Device Name（デバイス名）	デバイス名を表示します。  をクリックするとデバイス名を編集できます。
OS Information（オペレーティングシステム情報）	オペレーティングシステムの情報を表示します。
Logon user（ログオンしたユーザー）	クライアントデバイスにログオンしたユーザーを表示します。クライアントデバイスが、電源オフ、オフライン、ログアウトされている場合、Login User（ログインユーザー）欄には、最後にログインしたユーザー名が括弧（[]）で囲まれて表示されます。
BIOS Version（BIOSバージョン）	BIOSのバージョン情報を表示します。
Model Name（モデル名）	クライアントデバイスのモデル名を表示します。
IP Address（IPアドレス）	クライアントデバイスのIPアドレスを表示します。
Time Zone（タイムゾーン）	クライアントデバイスの所在地のタイムゾーンを表示します。
Up Time（稼働時間）	クライアントデバイスの稼働時間を表示します。
Agent Version（エージェントのバージョン）	エージェントのバージョン情報を表示します。
Operating Status（動作状態）	デバイスの動作状態（**メンテナンス**、**スタンバイ**、**通常**）を設定することができます。詳細は、**4.2 動作状態**を参照してください。

デバイス情報のページでは、各種情報を確認したり、画面右側の機能を使用してデバイスを制御し管理することもできます。

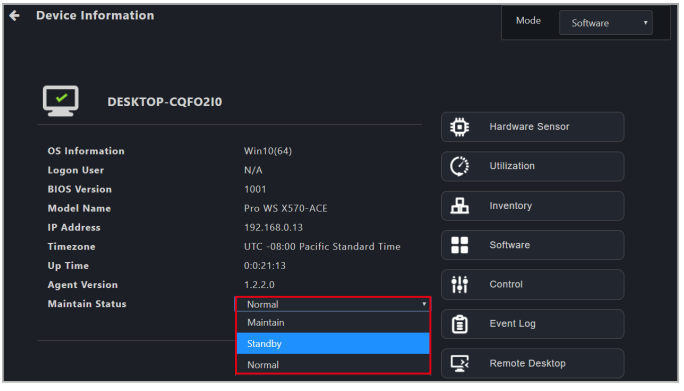
Hardware Sensor（ハードウェアセンサー）	デバイスのハードウェアセンサーの情報を表示します。
Utilization（使用率）	デバイスの使用率情報を表示します。
Inventory（インベントリ）	デバイスのディスク情報と資産情報を表示します。
Software（ソフトウェア）	デバイスにインストールされたソフトウェアを確認して管理することができます。
Control（制御）	レジストリエディタ、USBストレージデバイス、リモート電源機能の設定を確認して調整することができます。
Event Log（イベントログ）	デバイスのイベントログを確認、インポート、エクスポートすることができます。
Remote Desktop（リモートデスクトップ）	デバイスをリモートで制御することができます。
USB Redirection（USB リダイレクト）*	特定のデバイスのドライブを共有できるようにします。
BIOS	デバイスのBIOSを管理することができます。
Installer（インストーラー）	デバイスのドライバー、アプリケーション、BIOSをダウンロードして更新することができます。
Device Manager（デバイスマネージャー）	デバイスのデバイスマネージャー項目を確認することができます。
System Restore（システム復元）	クライアントデバイスのシステム復元ポイントの作成と削除、システム復元ポイントからの復元をすることができます。

4.2 動作状態

デバイスの動作状態を**Maintenance（メンテナンス）**、**Standby（スタンバイ）**、**Normal（通常）**に設定することができます。動作状態の設定は、デバイス情報画面から行うか、メインメニューページに戻り、複数の機器を選択し、**Select Function（機能の選択）**ドロップダウンメニューから**Operating Status（動作状態）**欄で動作状態を選択することができます。

動作状態の変化は接続概要画面で確認することができます。**Maintenance（メンテナンス）**または**Standby（スタンバイ）**の動作状態は、クライアントデバイスがオフラインまたは電源オフにされた場合にのみ表示されます。デバイスがオフラインでなかったり電源オフされていない場合は、現在の接続状態が動作状態として表示されます。

- 電源オフまたはオフラインのデバイスが**Maintenance（メンテナンス）**または**Standby（スタンバイ）**に設定されたうえで電源がオンになるかネットワークに接続されている場合、接続の概要画面では**Online(オンライン)**として表示されます。
- 次の画面は、**Device Information（デバイス情報）**画面の**Operating Status（動作状態）**ドロップダウンメニューを表示したものです。



4.3 ハードウェアセンサー（ソフトウェア）

この機能ではS.M.A.R.T.属性を確認したり、電圧/温度/ファン動作/グラフィックスカードなどのしきい値を編集することができます。この機能はソフトウェアによって制御されており、表示される値はハードウェアのバージョンによって異なる場合があります。**ハードウェア**モードについては、以下をご参照ください。

- DASHデバイス：**5.7.1 ハードウェアセンサー**
- RTL8117デバイス：**5.8.1 ハードウェアセンサー**
- BMC デバイス: **5.10.1 ハードウェアセンサー**

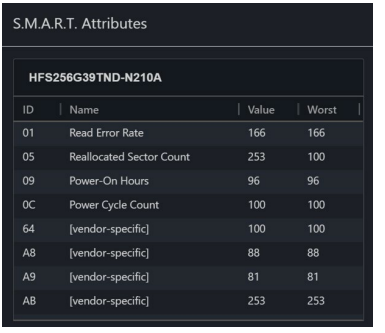
- グラフィックスカードなどの一部機能は、クライアントデバイスにコンポーネントが取り付けられている場合にのみ使用することができます。
- ▼をクリックするとサブアイテムの表示/非表示を切り替えることができます。
- この機能はデバイスがオペレーティングシステムへログインされていない場合、DASHまたはRTL8117リモート管理コントローラーをサポートする管理LANポートを使用して接続されていない場合、利用できません。
- マザーボードがDASHまたはRTL8117リモート管理コントローラーに対応している場合、**ハードウェアモード**に切り替えることができます。デバイスの電源がオフの場合は、前回デバイスが電源オンだった際のハードウェアセンサー情報を表示することができます。

S.M.A.R.T.

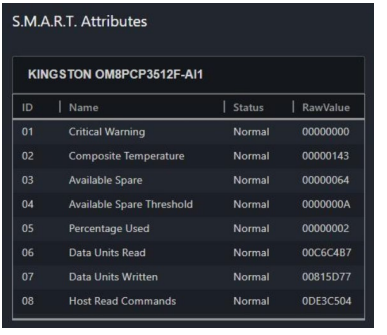
ディスクのステータスを表示します。このアイテムをクリックすると、詳細なS.M.A.R.T.属性情報が表示されます。

S.M.A.R.T.情報は、ディスクの仕様やブランドが提供する情報によって異なります。

SATA HDD:



NVMe SSD:



Voltage（電圧）

CPUのコア電圧や、その他の電圧関連のアイテムを表示します。アイテムのしきい値を編集することもできます。

Temperature（温度）

CPUの状態と温度を表示します。アイテムのしきい値を編集することもできます。

Fans（ファン）

接続されている冷却ファンの状態と回転数を表示します。アイテムのしきい値を編集することもできます。

Graphics Card（グラフィックスカード）

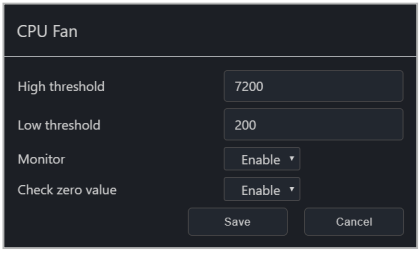
AMDまたはNVIDIAグラフィックスカードのファン回転数、電圧、温度を表示します。アイテムのしきい値を編集することもできます。

表示される情報はグラフィックスカードのドライバーのサポート状況によって異なります。サポートされないアイテムの場合は、「**Hardware sensor is not supported by the graphics driver**」（**グラフィックスドライバーはハードウェアセンサーをサポートしていません**）メッセージが表示されます。

しきい値の編集

電圧やファンなどのアイテムでは、しきい値を編集することができます。編集するアイテムをクリックし、編集が終わったら**Save（保存）**をクリックします。

- 各項目のしきい値オプションは異なる場合があります。
- アイテムによっては、編集可能なしきい値がないものもあります。

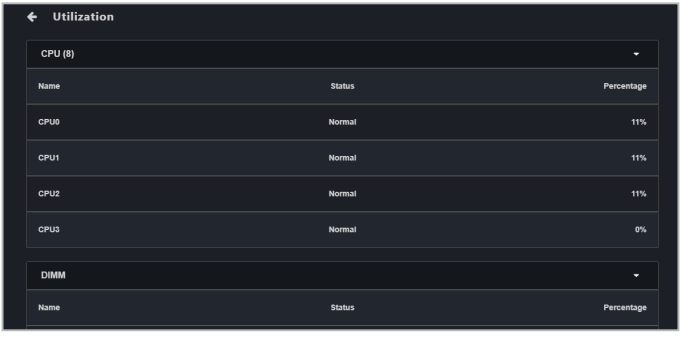


High threshold（最大しきい値）	値がこのしきい値を超えると、センサーは**警告（黄色）**を表示します。 値がこのしきい値を20%超えると、センサーは**重大（赤色）**を表示します。
Low threshold（最小しきい値）	値がこのしきい値を下回ると、センサーは**警告（黄色）**を表示します。 値がこのしきい値を20%下回る場合、センサーは**重大（赤色）**を表示します。
Monitor（監視）	アイテムの監視を有効または無効にします。
Check zero value（ゼロ値のチェック）	ゼロ値のチェックを有効または無効にします。**Enabled（有効）**に設定すると、ファンの回転数が0（ゼロ）の場合、警告が表示されます。**Disabled（無効）**に設定すると、ファンの回転数が0（ゼロ）の場合は取り外されたファン（未接続）として認識されます。

4.4 使用率

デバイスのCPU、メモリー、パーティション、ネットワークの使用率のしきい値を表示および設定することができます。

▼をクリックするとサブアイテムの表示/非表示を切り替えることができます。



CPU	CPUの使用状況と使用率(%)を表示します。アイテムのしきい値を編集することもできます。
DIMM(メモリー)	メモリーの使用状況と使用率(%)を表示します。アイテムのしきい値を編集することもできます。
Partition(パーティション)	ディスクパーティションの使用状況と使用率(%)を表示します。アイテムのしきい値を編集することもできます。
Network(ネットワーク)	ネットワークの使用状況と使用率(%)を表示します。アイテムのしきい値を編集することもできます。

しきい値の編集

編集するアイテムをクリックし、編集が終わったら**Save(保存)**をクリックします。

High Critical(高:重大)	値がこのしきい値を超えると、センサーは**重大(赤色)**を表示します。
High Warning(高:警告)	値がこのしきい値を超えると、センサーは**警告(黄色)**を表示します。

4.5 インベントリ（ソフトウェア）

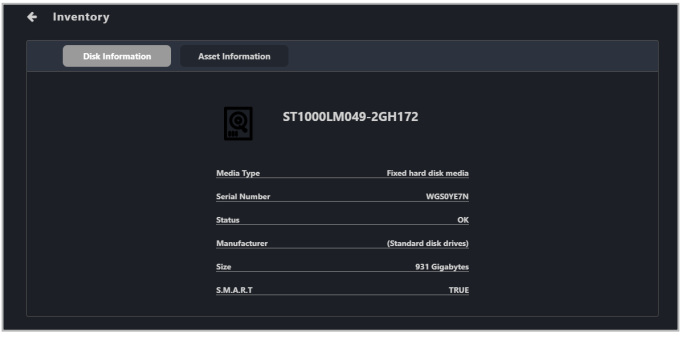
オペレーティングシステム環境にログインしていない場合、リモートマネジメントコントローラーに対応した管理用LANポートで接続していない場合は、この項目は表示されません。

単一のクライアントデバイスとディスクの詳細情報を表示します。この機能はソフトウェアによって制御されており、表示される値はハードウェアのバージョンによって異なる場合があります。**ハードウェア**モードについては、以下をご参照ください。

- DASHデバイス：**5.7.2 インベントリ**
- RTL8117デバイス：**5.8.2 インベントリ**
- vProデバイス：**5.9.1 インベントリ**
- BMC デバイス: **5.10.2 インベントリ**

4.5.1 ディスク情報

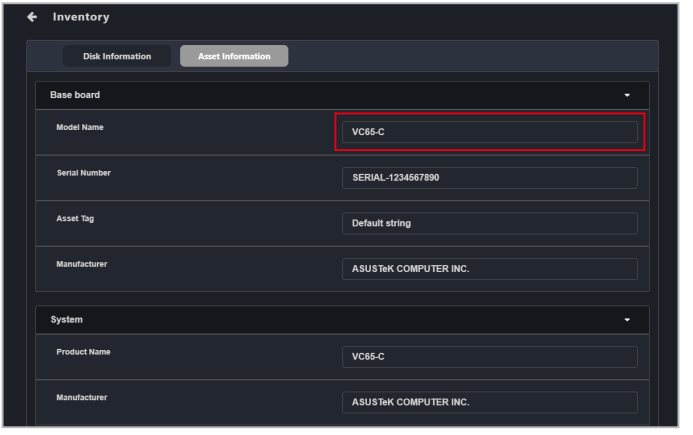
Disk Information（ディスク情報）をクリックするとディスクの詳細情報が表示されます。



Disk Name（ディスク名）	ディスク名を表示します。
Media Type（メディアタイプ）	メディアタイプを表示します。
Serial Number（シリアル番号）	ディスクのシリアル番号を表示します。
Status（状態）	ディスクの状態を表示します。
Manufacture（製造元）	ディスクの製造元を表示します。
Size（サイズ）	ディスクの合計サイズを表示します。
S.M.A.R.T.	ディスクのS.M.A.R.T.属性を表示します。

4.5.2 アセット情報

Asset Information（アセット情報）をクリックするとクライアントデバイスの詳細情報が表示されます。灰色の線で囲まれたアイテムをダブルクリックすると、アイテムを編集することができます。



Baseboard（マザーボード）	マザーボードのモデル名、シリアル番号、アセットタグ、製造元情報を表示します。
System（システム）	製品名と製造元情報を表示します。
Memory（メモリー）	メモリーの位置とサイズを表示します。
BIOS	BIOSのリリース日、バージョン、製造元情報を表示します。
Processor（プロセッサー）	プロセッサー名とクロックを表示します。
Network Adapter（ネットワークアダプター）	ネットワークアダプター名、MACアドレス、接続状態、アダプタータイプの情報を表示します。
Graphics Card（グラフィックスカード）	グラフィックスカード名、ドライバーのバージョン、その他の情報を表示します。
OEM String（OEMストリング）	デバイスのSMBIOS TYPE情報を表示します。

4.6 ソフトウェア

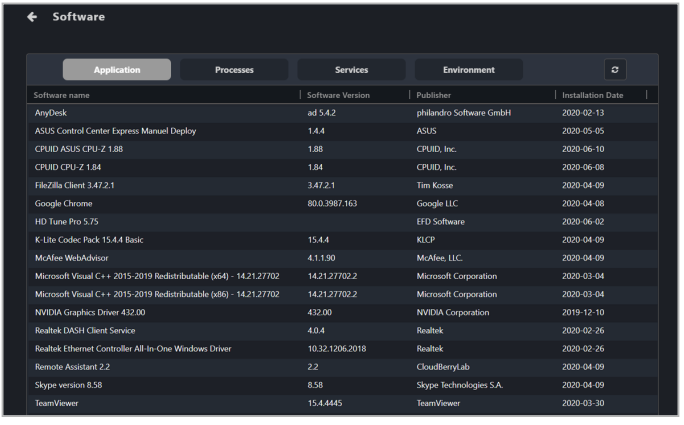
単一のデバイスに関するソフトウェアとアプリケーションの詳細情報を、**Application（アプリケーション）**、**Processes（プロセス）**、**Services（サービス）**、**Environment（環境）**タブに分けて表示します。

- 一部のオペレーティングシステムアプリケーション、プロセス、サービスは削除、終了、停止することができません。
- 列のヘッダーをクリックすると、列内のアイテムがアルファベット順に整列されます。

4.6.1 アプリケーションタブ

Application（アプリケーション）タブで、クライアントデバイスにインストールされたアプリケーションの詳細情報を確認することができます。アプリケーションをクリックし、**Uninstall（アンインストール）**を選択してアプリケーションをアンインストールすることもできます。

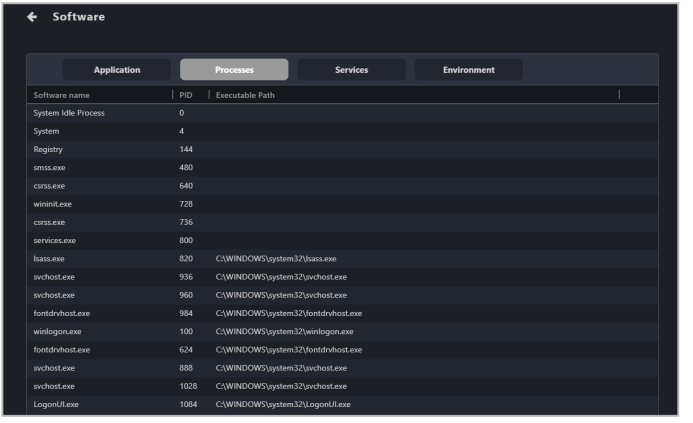
- 選択したアプリケーションをアンインストールすることができない場合は、**Uninstall（アンインストール）**ボタンはグレーアウト表示されます。
- (更新)ボタンをクリックするとソフトウェア一覧が更新されます。



Software name	Software Version	Publisher	Installation Date
AnyDesk	ad 5.4.2	philandro Software GmbH	2020-02-13
ASUS Control Center Express Manuel Deploy	1.4.4	ASUS	2020-05-05
CPUID ASUS CPU-Z 1.88	1.88	CPUID, Inc.	2020-06-10
CPUID CPU-Z 1.84	1.84	CPUID, Inc.	2020-06-08
FileZilla Client 3.47.2.1	3.47.2.1	Tim Kosse	2020-04-09
Google Chrome	80.0.3987.163	Google LLC	2020-04-08
HD Tune Pro 5.75		EFD Software	2020-06-02
K-Lite Codec Pack 15.4.4 Basic	15.4.4	KLCP	2020-04-09
McAfee WebAdvisor	4.1.1.90	McAfee, LLC.	2020-04-09
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.21.27702	14.21.27702.2	Microsoft Corporation	2020-03-04
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702	14.21.27702.2	Microsoft Corporation	2020-03-04
NVIDIA Graphics Driver 432.00	432.00	NVIDIA Corporation	2019-12-10
Realtek DASH Client Service	4.0.4	Realtek	2020-02-26
Realtek Ethernet Controller All-In-One Windows Driver	10.32.1206.2018	Realtek	2020-02-26
Remote Assistant 2.2	2.2	CloudBerryLab	2020-04-09
Skype version 8.58	8.58	Skype Technologies S.A.	2020-04-09
TeamViewer	15.4.4445	TeamViewer	2020-03-30

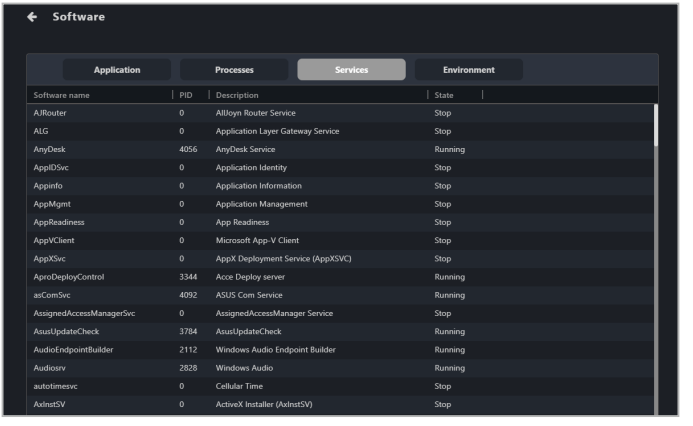
4.6.2 プロセスタブ

Processes（プロセス）タブではアクティブなプロセスの情報を確認できます。プロセスをクリックし、**End Task（タスクの終了）**を選択してプロセスを終了させることもできます。



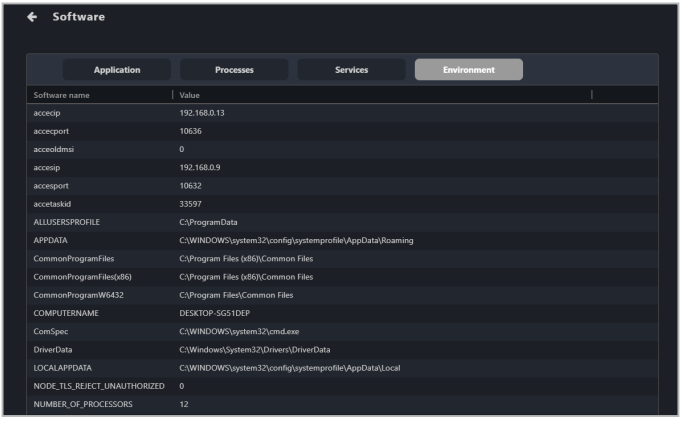
4.6.3 サービスタブ

Services（サービス）タブでは利用できるサービスの情報を確認することができます。サービスをクリックして**Start（開始）**をクリックすればサービスが開始され、**Stop（停止）**をクリックすれば実行中のサービスが停止します。



4.6.4 環境タブ

Environment（環境）タブでは環境変数の情報を確認することができます。

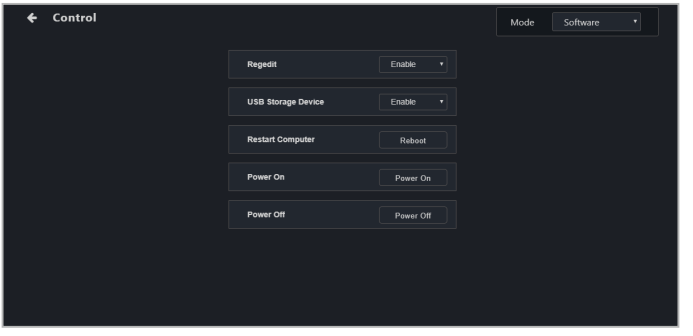


4.7 制御（ソフトウェア）

- デバイスがオペレーティングシステムにログインしていない場合、この項目は表示されません。
- ASUS Control Center Expressを使用して設定を行っていない場合、初期値として「Not Config（未構成）」が表示されます。
- タスクが正常に完了したかどうかを確認するには、ミッションセンターで確認することができます。詳しくは **2.4 ミッションセンター** を参照してください。

システム、USB、電源、ブートオプションを設定することができます。この機能はソフトウェアによって制御されており、表示される値はハードウェアのバージョンによって異なる場合があります。**ハードウェア**モードについては、以下をご参照ください。

- DASH デバイス： **5.7.3 制御**
- RTL8117 デバイス：**5.8.3 制御**
- vPro デバイス： **5.9.2 制御**
- BMC デバイス : **5.9.3 制御**



Enable/Disable Regedit（レジストリエディタを有効/無効）	Windowsのレジストリエディタを有効または無効にします。
USB Storage Device（USBストレージデバイス）	USBポートを有効または無効にするか、読み取り専用に設定します。
Restart Computer（コンピューターの再起動）	クライアントデバイスを再起動します。
Power On（電源オン）	クライアントデバイスの電源をオンにします。  クライアントデバイスがWake-On-LANをサポートしている場合、クライアントデバイスの電源がオフの状態でも、この機能を使用して電源オンにできます。
Power Off（電源オフ）	クライアントデバイスの電源をオフにします。
Fast Startup（高速スタートアップ）	クライアントデバイスの高速スタートアップを有効または無効にします。
Windows Update	クライアントデバイスのWindows Updateを有効または無効にします。
Set Management Controller（管理コントローラー設定）	vPro管理コントローラーのIPアドレスを設定します。  この機能はクライアントデバイスがvProリモート管理をサポートしている場合にのみ有効です。

4.8 イベントログ

Monitor（監視）、**Application（アプリケーション）**、**System（システム）**、**Security（セキュリティ）**タブをクリックして、ASUS Control Center Expressのクライアントデバイスのイベントログを表示することができます。各イベントログのタブでは、イベントをクリックして詳細情報を確認することができます。

一覧を.csvファイルへエクスポートしたり、ACC CSMイベントログの.csvファイルをインポートすることもできます。

- 一覧をエクスポートする場合は**Export（エクスポート）**ボタンをクリックし、ファイル名を入力して**Save（保存）**をクリックします。
- ACC CSMイベントログ表をインポートする場合は**Import（インポート）**ボタンをクリックし、インポートするACC CSMイベントログの.csvファイルを選択して、**Open（開く）**をクリックします。

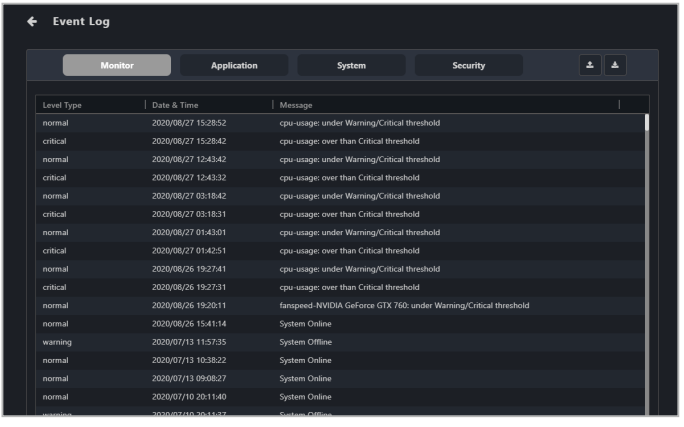
この機能はソフトウェアによって制御されており、表示される値はハードウェアのバージョンによって異なる場合があります。**ハードウェア**モードについては、以下をご参照ください。

- RTL8117 デバイス: **5.8.9 イベントログ**

列のヘッダーをクリックすると、列内のアイテムがアルファベット順に整列されます。

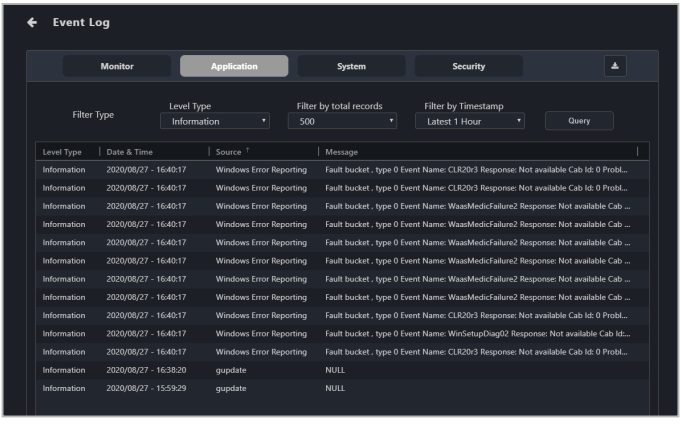
4.8.1 監視タブ

Monitor（監視）タブでは、**Connection（接続）**、**Hardware（ハードウェア）**、**Utilization（使用率）**センサーが検出した、クライアントデバイスの状態変化が記録されたイベントログを確認することができます。



4.8.2 アプリケーションタブ

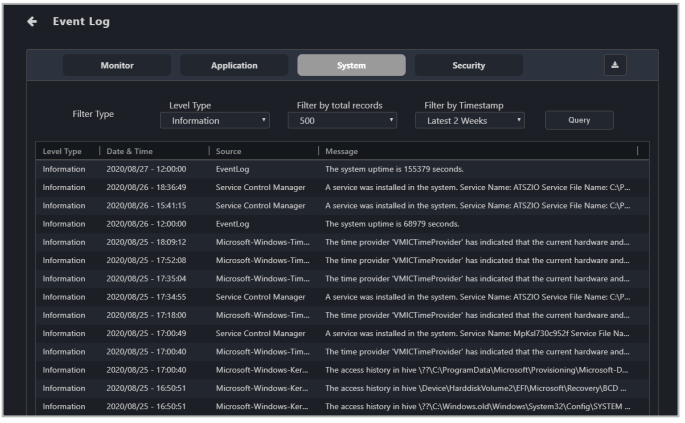
Application（アプリケーション）タブでは、**Filter Type（フィルタータイプ）**ブロックからフィルタリングの条件を選択して**Query（クエリ）**をクリックすることで、アプリケーションに関連するイベントをフィルタリングすることができます。



Level Type（レベルタイプ）	**-**	このフィルターを無視します。
	Information（情報）	通常、情報レベルのイベントは、問題または異常なく発生したイベントを示します。
	Warning（警告）	警告レベルのイベントは、直ちに対処する必要がない、潜在的な問題を示します。
	Error（エラー）	エラーレベルのイベントは、読み込みまたは動作上の障害を示します。
	Critical（危険）	危険レベルのイベントは最も深刻な問題を示し、直ちに対処する必要があります。
Filter by total records（記録数を基にフィルタリング）	表示するイベント数を選択するか、「-」を選択してフィルターを無視します。	
Filter by Timestamp（タイムスタンプを基にフィルタリング）	表示するイベントの期間を選択するか、「-」を選択してフィルターを無視します。	

4.8.3 システムタブ

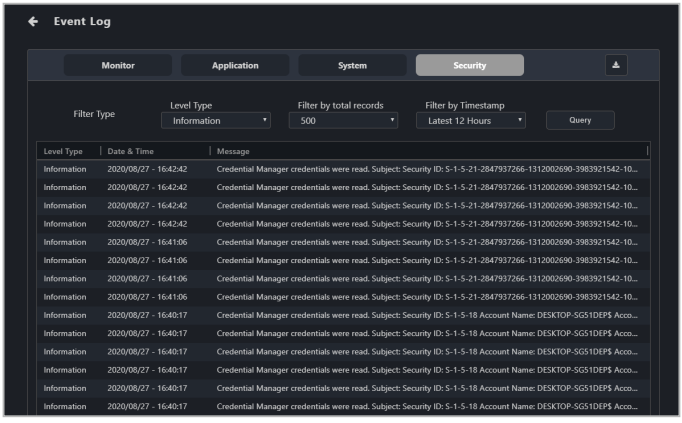
System（システム）タブでは、**Filter Type（フィルタータイプ）**ブロックからフィルタリングの条件を選択して**Query（クエリ）**をクリックすることで、システムに関連するイベントをフィルタリングすることができます。



Level Type（レベルタイプ）	**-**	このフィルターを無視します。
	Information（情報）	通常、情報レベルのイベントは、問題または異常なく発生したイベントを示します。
	Warning（警告）	警告レベルのイベントは、直ちに対処する必要がない、潜在的な問題を示します。
	Error（エラー）	エラーレベルのイベントは、読み込みまたは動作上の障害を示します。
	Critical（危険）	危険レベルのイベントは最も深刻な問題を示し、直ちに対処する必要があります。
Filter by total records（記録数を基にフィルタリング）	表示するイベント数を選択するか、「-」を選択してフィルターを無視します。	
Filter by Timestamp（タイムスタンプを基にフィルタリング）	表示するイベントの期間を選択するか、「-」を選択してフィルターを無視します。	

4.8.4 セキュリティタブ

Security（セキュリティ）タブでは、**Filter Type（フィルタータイプ）**ブロックからフィルタリングの条件を選択して**Query（クエリ）**をクリックすることで、セキュリティに関連するイベントをフィルタリングすることができます。



Level Type（レベルタイプ）	**-**	このフィルターを無視します。
	Information（情報）	通常、情報レベルのイベントは、問題または異常なく発生したイベントを示します。
	Warning（警告）	警告レベルのイベントは、直ちに対処する必要がない、潜在的な問題を示します。
	Error（エラー）	エラーレベルのイベントは、読み込みまたは動作上の障害を示します。
	Critical（危険）	危険レベルのイベントは最も深刻な問題を示し、直ちに対処する必要があります。
Filter by total records（記録数を基にフィルタリング）	表示するイベント数を選択するか、「-」を選択してフィルターを無視します。	
Filter by Timestamp（タイムスタンプを基にフィルタリング）	表示するイベントの期間を選択するか、「-」を選択してフィルターを無視します。	

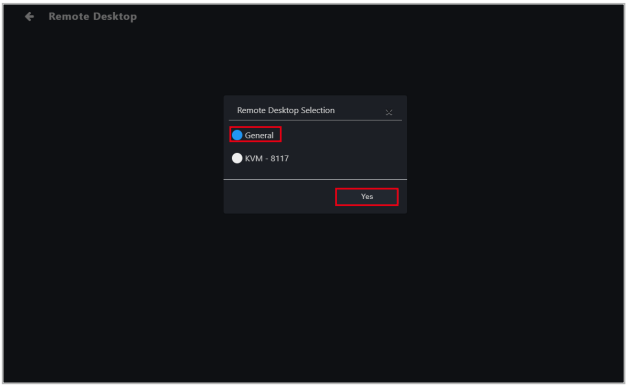
4.9 リモートデスクトップ（一般）

Remote Desktop（リモートデスクトップ）機能は、ASUS Control Center Expressでアクセスするデスクトップを介したデバイス管理のための柔軟なインターフェースを提供します。

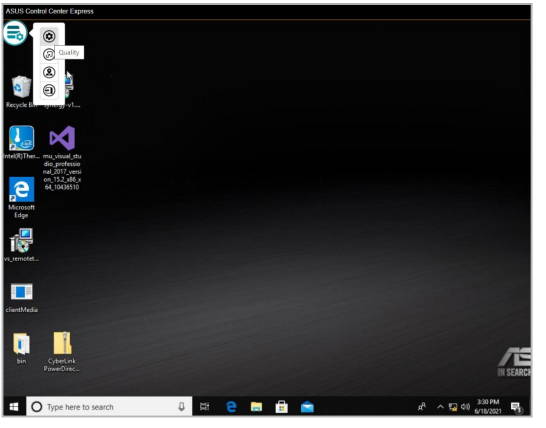
クライアントデバイスがリモート管理コントローラー（RTL8117）またはvProをサポートしている場合、ウィンドウが出現して**General（一般）**または**KVM - 8117**のどちらかを選択することができます。クライアントデバイスをリモートで制御する場合は**General（一般）**を選択します。それ以外を選択した場合はリモートデスクトップへ直接移動します。**ハードウェア**モードについては、以下をご参照ください。

- RTL8117 デバイス：**5.8.4 リモートデスクトップ**
- vPro デバイス：**5.9.3 リモートデスクトップ**

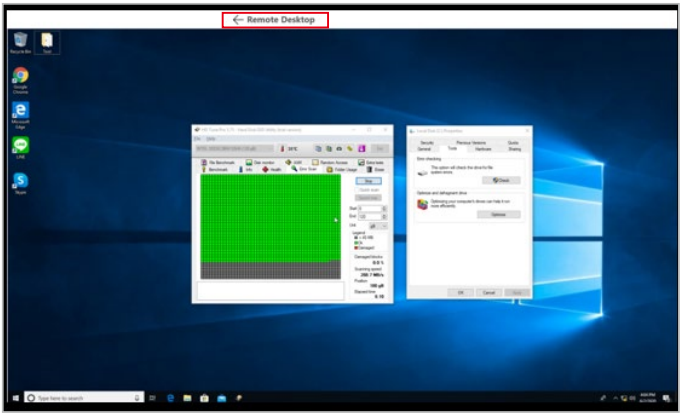
クライアントデバイスの電源をオンにし、オペレーティングシステム環境へログインしている必要があります。



接続が成功すると、リモートデスクトップ機能を選択したり、接続されたデバイスをリモート制御することができます



リモート制御セッションを終了する場合は、ページの上端で
← **Remote Desktop**（**リモートデスクトップ**）をクリックします。



リモートデスクトップ機能

画質や画面サイズ、ファンクションボタンの位置など、さまざまなリモートデスクトップ機能を調整することができます。

- リモートデスクトップの機能は、**KVM - 8117** と **General**（**一般**）で異なります。
- **Mouse display status (マウス表示状態)** 機能ボタンはデフォルトでは表示となっており、クライアントデバイスにディスプレイが接続されていない、かつ1つ以上のマウスが接続されている場合にのみ表示されます。

Quality（画質）	リモートデスクトップの画質調整
Resize（リサイズ）	ウィンドウサイズと画面サイズの選択
Set button position（セットボタンの位置）	画面上でのリモートデスクトップ機能のデフォルト位置の調整
Mouse display status（マウス表示状態）	接続されたクライアントのマウスカーソルの表示設定
Exit（終了）	リモートデスクトップを終了し、ASUS Control Center Express メインソフトウェアに戻る

4.10 BIOS

単一または複数のデバイスで各種のBIOS設定（**Advanced（詳細）**、**Boot（起動）**、**Monitor（監視）**、**Security（セキュリティ）**を調整することができます。また、BIOSファイルを手動でアップロードするか、BIOSキャッシュからアップロードして、単一または複数のデバイスのBIOSを更新することもできます。

デバイス情報からBIOSページへアクセスすると、選択したデバイスのBIOS設定を確認して管理するか、更新する作業のみが行えます。複数のデバイスでBIOS設定を確認して管理または更新する場合は、メインメニューのページへ戻り、複数のデバイスを選択してから、**Selection Function（機能の選択）**ドロップダウンメニューで**Smart BIOS（スマートBIOS）**を選択してください。

この機能はソフトウェアによって制御されており、表示される値はハードウェアのバージョンによって異なる場合があります。Hardware Mode（ハードウェアモード）について、詳しくは **5章 管理機能** を参照してください。

4.10.1 BIOSフラッシュ管理

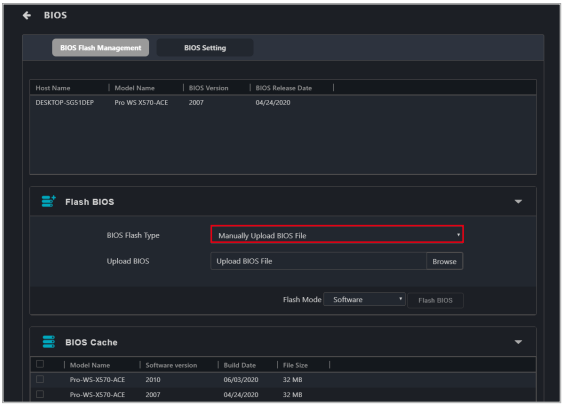
BIOSファイルを手動でアップロードしたり、BIOSキャッシュから以前にフラッシュされたBIOSファイルを選択して、BIOSをフラッシュすることができます。必要であれば、BIOSキャッシュからBIOSファイルを削除することもできます。

BIOSファイルを手動でアップロードしてBIOSをフラッシュ

BIOSファイルを手動でアップロードして、クライアントデバイスのBIOSをフラッシュします。アップロードされフラッシュされたBIOSファイルはBIOSキャッシュへ追加されます。

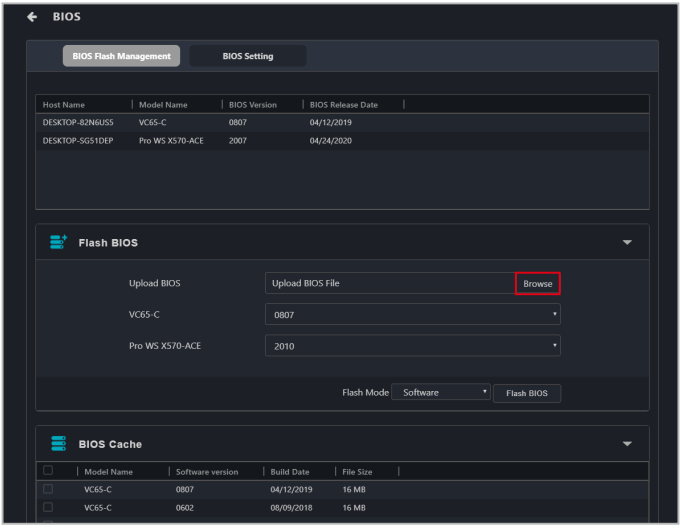
1. **BIOS Flash Type（BIOSのフラッシュタイプ）**欄で**Manually Upload BIOS File（BIOSファイルを手動でアップロード）**を選択します。

このオプションは、単一のデバイスを選択した場合にのみ表示されます。

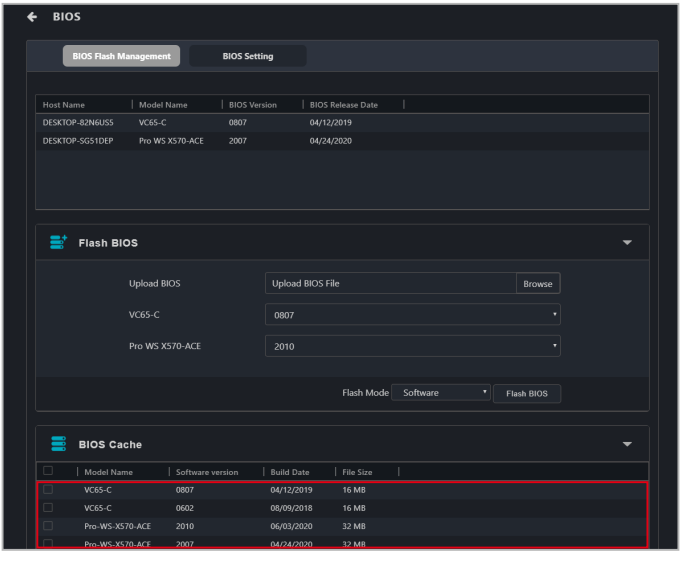


2. **Browse（参照）**をクリックしてBIOSファイルを追加します。

- 複数のデバイスのBIOSファイルは個別にアップロードする必要があります。
- 次の画面は、複数のデバイスを選択した場合のオプションを示します。

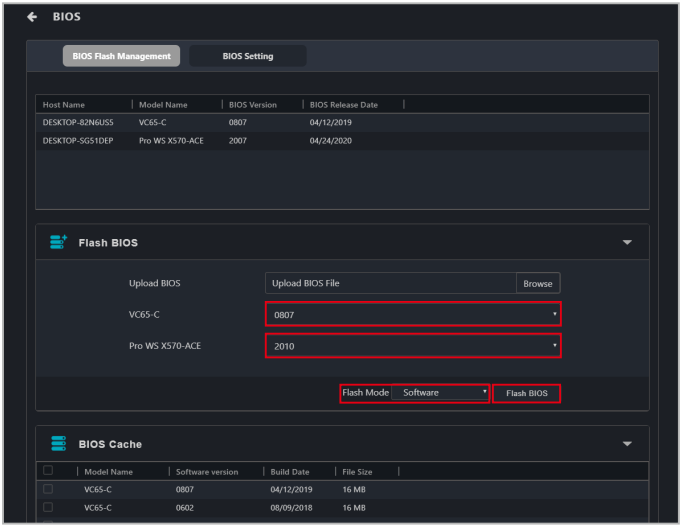


3. BIOSファイルが正常にアップロードされたことを確認し、**OK**をクリックします。アップロードされたBIOSファイルは**BIOS Cache（BIOSキャッシュ）**に追加されます。



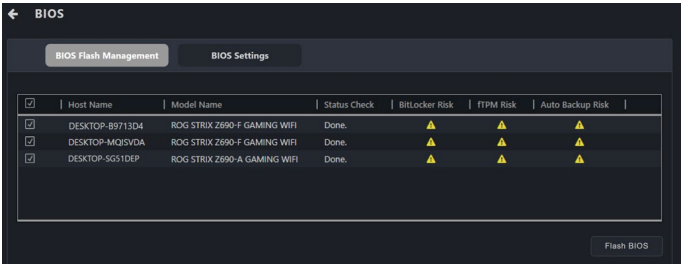
4. （複数のデバイスの場合）各モデル名の脇にあるドロップダウンメニューで、デバイスでフラッシュするBIOSを選択します。
5. **Flash Mode（フラッシュモード）**を選択し、**Flash BIOS（BIOSのフラッシュ）**をクリックします。

ハードウェアフラッシュモードは、リモート管理コントローラーに対応した管理LANポートを使用してクライアントデバイスが接続されている場合にのみ使用できます。



6. クライアントデバイスに、BIOSフラッシュに影響を与える可能性のある問題がないか自動的にチェックされます。発見された問題を解決せずにフラッシュを続行した場合、データ損失や重大なリスクが発生する可能性があります。続行する前に［**Status Check**］［**BitLocker Risk**］［**fTPM Risk**］［**Auto Backup Risk**］を必ず確認してください。

- **Status Check**では、クライアントデバイスのASUS Control Center Expressエージェントがバージョン1.6.3以降に更新されていることを確認します。
- **BitLocker Risk**では、クライアントデバイスでBitLockerが一時停止されていることを確認します。続行すると、BitLocker回復キーがなければ元に戻すことができないBitLocker暗号化がトリガーされる可能性があります。
- **fTPM Risk**では、クライアントデバイスでfTPMが無効に設定されていることを確認します。続行すると、fTPMセキュリティデータが不可逆的に消去される可能性があります。
- **Auto Backup Risk**では、ASUS Control Center ExpressがBitLocker回復キーを自動的にバックアップできるかどうかを確認します。アラートが表示された場合は、BitLocker回復キーを手動でバックアップすることを強くおすすめします。



7. BIOSの更新が完了した際にクライアントデバイスを自動的にシャットダウンする場合は、ポップアップウィンドウで**Yes（はい）**をクリックしてください。クライアントデバイスを手動でシャットダウンする場合は、**No（いいえ）**をクリックします。

   Yes（はい）を選択すると、デバイスは更新後に自動的にシャットダウンします。シャットダウンしたことがミッションセンターに表示されます。

   No（いいえ）を選択すると、デバイスはBIOSを更新し、更新の結果がミッションセンターに表示されます。ミッションセンターで更新の結果をクリックし、**Shutdown（シャットダウン）**をクリックするとデバイスを手動でシャットダウンすることができます。

BIOSをBIOSキャッシュからフラッシュ

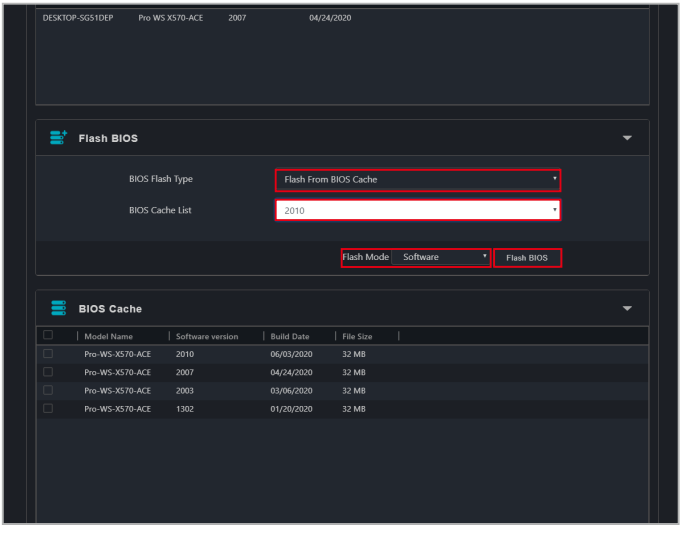
BIOSキャッシュからBIOSファイルを選択することができます。

1. **BIOS Flash Type（BIOSのフラッシュタイプ）**欄で**Flash from BIOS Cache（BIOSキャッシュからフラッシュ）**を選択します。

このオプションは、単一のデバイスを選択した場合にのみ出現します。

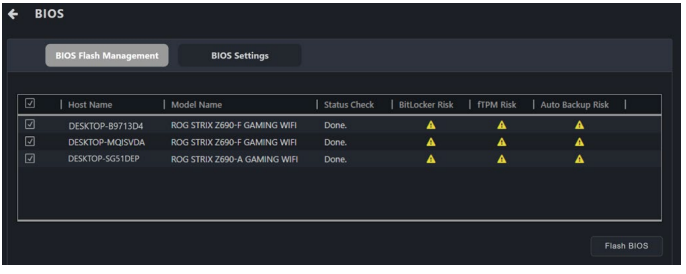
2. 適用されるBIOSファイルが自動的に選択されます。別のBIOSファイルを選択する場合は、**BIOS Cache List（BIOSキャッシュ一覧）**のドロップダウンメニューをクリックします。複数のデバイスでBIOSを更新する場合は、すべてのデバイスのBIOSファイルを選択してください。
3. **Flash Mode（フラッシュモード）**を選択し、**Flash BIOS（BIOSのフラッシュ）**をクリックします。

ハードウェアフラッシュモードは、RTL 8117 LAN ICに対応した管理LANポートを使用してクライアントデバイスが接続されている場合にのみ使用できます。



4. クライアントデバイスに、BIOSフラッシュに影響を与える可能性のある問題がないか自動的にチェックされます。発見された問題を解決せずにフラッシュを続行した場合、データ損失や重大なリスクが発生する可能性があります。続行する前に［**Status Check**］［**BitLocker Risk**］［**fTPM Risk**］［**Auto Backup Risk**］を必ず確認してください。

- **Status Check**では、クライアントデバイスのASUS Control Center Expressエージェントがバージョン1.6.3以降に更新されていることを確認します。
- **BitLocker Risk**では、クライアントデバイスでBitLockerが一時停止されていることを確認します。続行すると、BitLocker回復キーがなければ元に戻すことができないBitLocker暗号化がトリガーされる可能性があります。
- **fTPM Risk**では、クライアントデバイスでfTPMが無効に設定されていることを確認します。続行すると、fTPMセキュリティデータが不可逆的に消去される可能性があります。
- **Auto Backup Risk**では、ASUS Control Center ExpressがBitLocker回復キーを自動的にバックアップできるかどうかを確認します。アラートが表示された場合は、BitLocker回復キーを手動でバックアップすることを強くおすすめします。



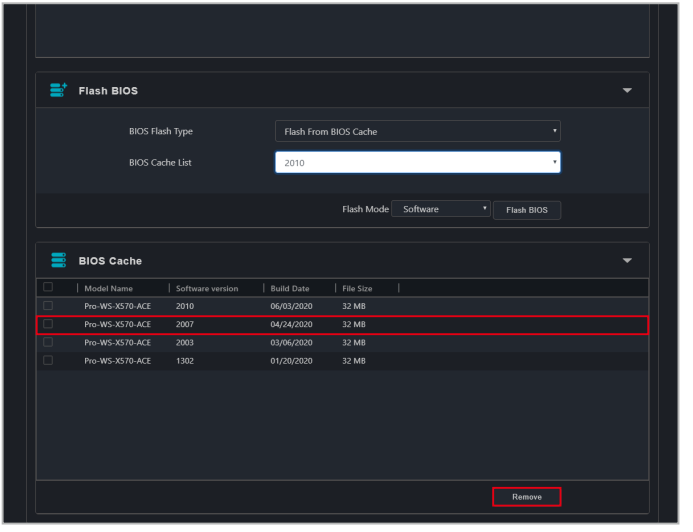
5. BIOSの更新が完了した際にクライアントデバイスを自動的にシャットダウンする場合は、ポップアップウィンドウで**Yes（はい）**をクリックしてください。クライアントデバイスを手動でシャットダウンする場合は、**No（いいえ）**をクリックします。

Yes（はい）を選択すると、デバイスは更新後に自動的にシャットダウンします。シャットダウンしたことがミッションセンターに表示されます。

No（いいえ）を選択すると、デバイスはBIOSを更新し、更新の結果がミッションセンターに表示されます。ミッションセンターで更新の結果をクリックし、**Shutdown（シャットダウン）**をクリックするとデバイスを手動でシャットダウンすることができます。

BIOSキャッシュからBIOSファイルを削除

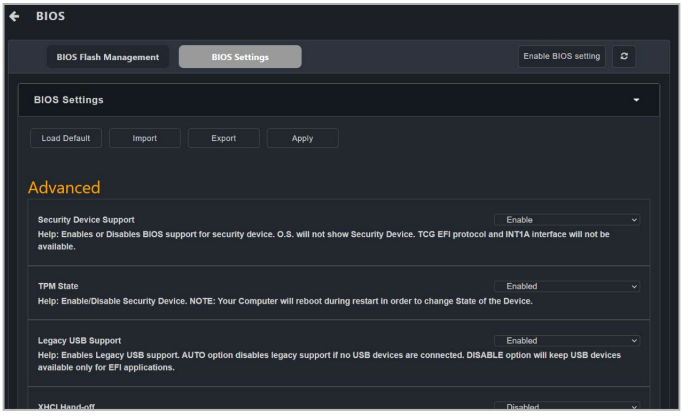
BIOSキャッシュブロックにある、クライアントデバイスで利用可能なBIOSファイルを確認することができます。BIOSキャッシュからBIOSファイルを削除する場合は、削除するBIOSファイルを選択し、**Remove（削除）**をクリックします。



4.10.2 BIOS設定

単一または複数のクライアントデバイスでBIOSの**Advanced**（**詳細**）、**Boot**（**起動**）、**Monitor**（**監視**）、**Security**（**セキュリティ**）設定を調整することができます。

- BIOS設定を開始する際、クライアントデバイスのBIOSパスワードの入力が要求されます。BIOSパスワードが設定されていない場合は、空欄のまま**OK**をクリックして続行します。
- 保護されたBIOSシステム環境変数をサポートするクライアントデバイスでは、間違ったパスワードが5回入力されるとBIOS設定がロックされます。BIOS設定のロックを解除するにはクライアントデバイスを再起動する必要があります。
- BIOS設定はクライアントデバイスに応じて異なる場合があります。BIOS設定の詳細は、クライアントデバイスのマザーボードのユーザーガイドを参照してください。
- 複数のデバイスが選択されている場合、すべてのデバイスで利用可能なBIOS設定のみが、**BIOS Setting**（**BIOS設定**）タブに表示されます。共通の項目で、デバイスごとに値や設定が異なる場合は、構成は空白のオプションとして表示されます。



BIOS設定機能：

オペレーティングシステム設定ページで利用可能な各種機能については、次の表を参照してください。

Enable BIOS setting（BIOS設定の有効化）	BIOS設定が無効に設定されているクライアントデバイスに対して、BIOS設定を有効にすることができます。
Load Default（デフォルトの読み込み）	BIOS設定の既定値を読み込みます。この機能を使用する際には、クライアントデバイスに設定されているBIOS管理者パスワードの入力が必要となります。
Import（インポート）	クライアントデバイスのBIOS設定をインポートします。
Export（エクスポート）	クライアントデバイスのBIOS設定をエクスポートします。
Apply（適用）	BIOS設定ページの変更内容をクライアントデバイスのBIOSへ適用します。この機能を使用する際には、クライアントデバイスに設定されているBIOS管理者パスワードの入力が必要となります。

- BIOSが変更されたりBIOS設定の既定値を読み込んだ場合は、必ずクライアントデバイスを再起動してくだあい。
- クライアントデバイスでBIOS管理者パスワードが設定されていない場合、デフォルトの読み込みおよび適用機能を使用する際は、パスワードを入力せずに、パスワードプロンプトウィンドウで**OK**をクリックします。

BIOS設定項目：

Advanced（詳細）	クライアントデバイスBIOSの詳細メニューを設定します。
Boot（ブート）	クライアントデバイスBIOSのブートメニューを設定します。
Monitor（監視）	クライアントデバイスBIOSのモニターメニューを設定します。
Security（セキュリティ）	クライアントデバイスBIOSのパスワードを設定します。

- クライアントデバイスのBIOS設定が有効に設定されていない場合、ASUS Control Center Expressは、クライアントデバイスのBIOS設定を表示することができません。BIOS設定の有効化をクリックし、クライアントデバイスを再起動すると、クライアントデバイスのBIOSを設定することができます。
- クライアントデバイスのBIOSがサポートしている場合、Boot Priorityメニューの項目を変更することができます。

4.11 インストーラー

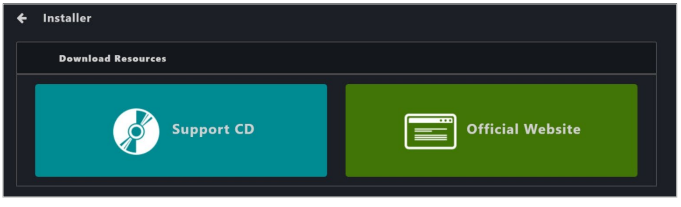
メインサーバーがインターネットに接続され、安定した接続が確立されていることをご確認ください。

ドライバー、ユーティリティアプリケーション、BIOSをダウンロードして単一または複数のデバイスで更新することができます。

デバイス情報からインストーラーページへアクセスすると、選択したデバイスのドライバー、ユーティリティアプリケーション、BIOSをダウンロードして更新する作業のみが行えます。複数のデバイスでドライバー、ユーティリティアプリケーション、BIOSをダウンロードして更新する場合は、メインメニューのページへ戻り、複数のデバイスを選択してから、**Selection Function（機能の選択）**ドロップダウンメニューで**Software Management（ソフトウェアの管理）** > **Installer（インストーラー）**を選択してください。

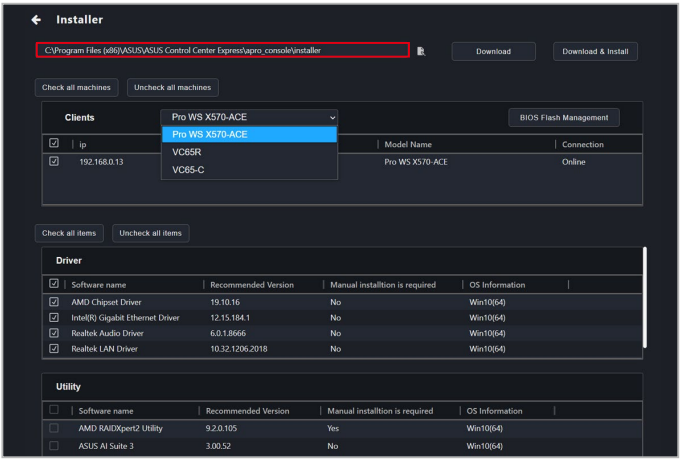
- 複数のデバイスを選択する場合、大多数のデバイスがオンラインであるようにしてください（一部のデバイスはオフラインでも可能です）。ダウンロードとインストールのプロセスはオンラインのデバイスに限定されます。選択したデバイスすべてがオフラインの場合、オンラインのデバイスを選択するよう促すメッセージが表示されます。
- ASUS Control Center Expressは、単一のデバイスを選択した場合にのみ、既にインストールされているドライバー、アプリケーション、BIOSバージョンを表示します。
- ASUS Control Center Expressは、単一のデバイスを選択した場合にのみ、更新または推奨されるドライバー、アプリケーションのダウンロードとインストールを自動的にチェックします。

1. インストーラーページでは、サポートCDからダウンロードするか、Webサイトからダウンロードするかを選択します。

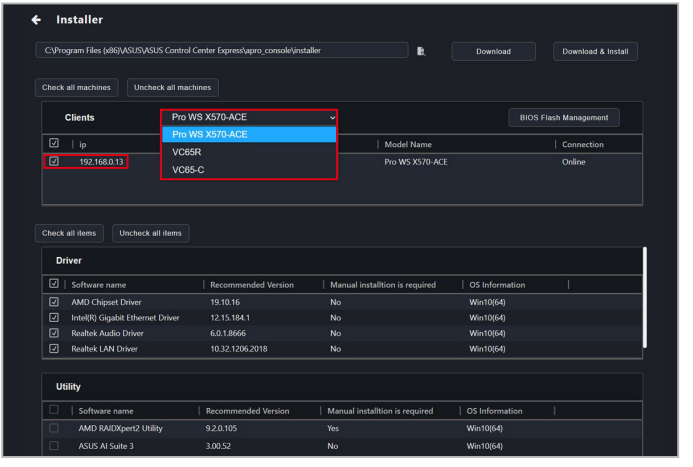


Support CD（サポートCD）	選択したデバイスの最新のサポートCDバージョンから、ドライバー、アプリケーション、BIOSをダウンロードしてインストールします。
Official Website（Webサイト）	選択したデバイスのWebサイトから、推奨バージョンのドライバー、アプリケーションをダウンロードします。

2. ダウンロードパスを新たに設定する場合は  をクリックします。選択しない場合はデフォルトのダウンロードパスが使用されます。



3. ドロップダウンリストからモデルを選択し、ソフトウェアをダウンロードするクライアントデバイスを選択します。

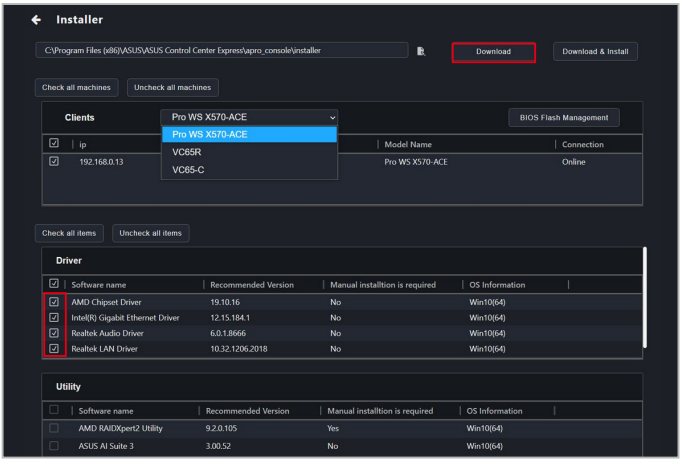


4. ダウンロード元で**Official Website（Webサイト）**を選択した場合は、ドロップダウンリストでクライアントデバイスのオペレーティングシステムを選択します。

オペレーティングシステムのドロップダウンリストは、ダウンロード元でOfficial Website（Webサイト）を選択した場合にのみ表示されます。

5. ダウンロードしたいドライバーまたはユーティリティを選択し、**Download（ダウンロード）**または**Download & Install（ダウンロードとインストール）**をクリックします。

- Download & Install（ダウンロードとインストール）はダウンロード元でSupport CD（サポートCD）を選択した場合にのみ選択できます。
- 表示されるアイテムはモデルにより異なります。
- **Driver（ドライバー）**、**Utility（ユーティリティ）**、**BIOS**ブロックはすでにインストールされているアイテムと、利用可能な推奨される更新を表示します。
- **Manual installation is required（手動のインストールが必要）**列で**Yes（はい）**と表示されているドライバーとユーティリティアプリケーションは、クライアントデバイスに手動でインストールする必要があります（インストールファイルは、クライアントデバイスで選択したダウンロードパスに存在します）。
- メインサーバーにダウンロードされたBIOSファイルは、自動的にBIOSキャッシュにアップロードされます。ダウンロード完了後**BIOS Flash Management（BIOSフラッシュ管理）**からBIOSを更新することができます。
- 利用可能なダウンロードをすべて選択するには**Check all items（すべてのアイテムをチェック）**をクリックします。
- 選択したソフトウェアは、ASUS Control Center Expressメインメニューで設定されたダウンロードパスに保存されます。



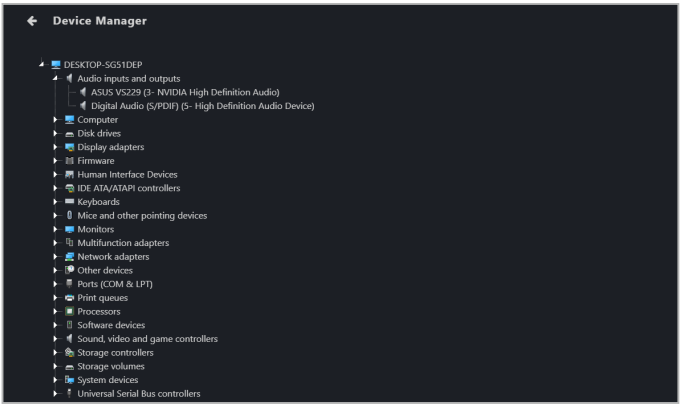
6. ステータスバーが出現し、ダウンロードの状況を表示します。ダウンロードが完了したら**OK**をクリックします。

4.12 デバイスマネージャー

クライアントデバイスのデバイスマネージャー情報を確認し、ハードウェアを検査し、ハードウェア障害/システムリソースの問題/ドライバーの問題を検出して解決することができます。

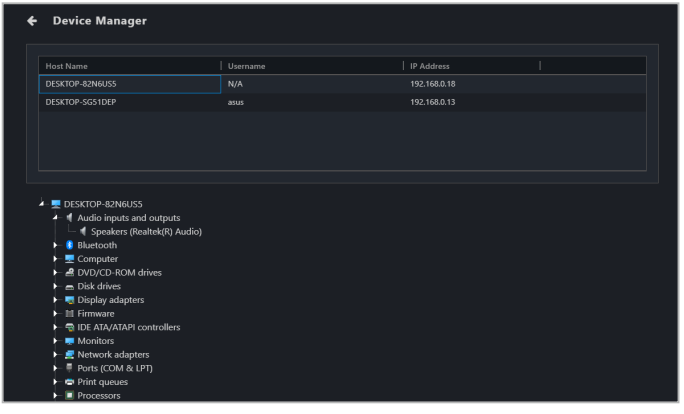
Device Information（デバイス情報）からDevice Manager（デバイスマネージャー）ページへアクセスすると、選択したデバイスのデバイスマネージャーを確認することができます。複数のデバイスでデバイスマネージャーを確認する場合は、メインメニューのページへ戻り、複数のデバイスを選択してから、**Select Function（機能の選択）**ドロップダウンメニューで**Device Manager（デバイスマネージャー）**を選択してください。

単一デバイス

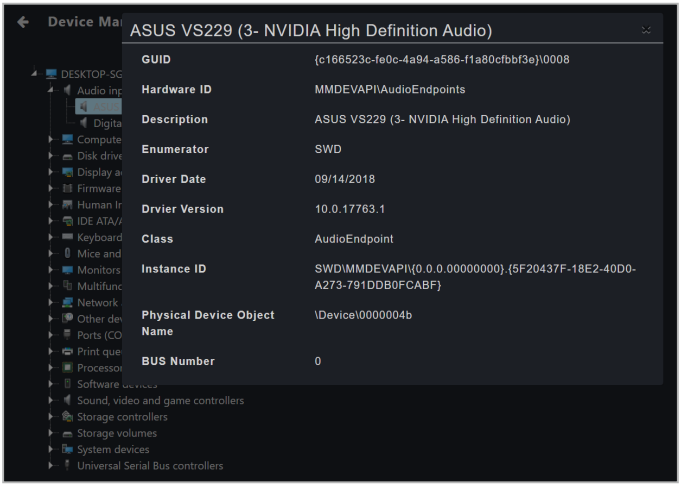


複数デバイス

デバイスをクリックすると、画面下部にそのデバイスのデバイスマネージャー情報が表示されます。

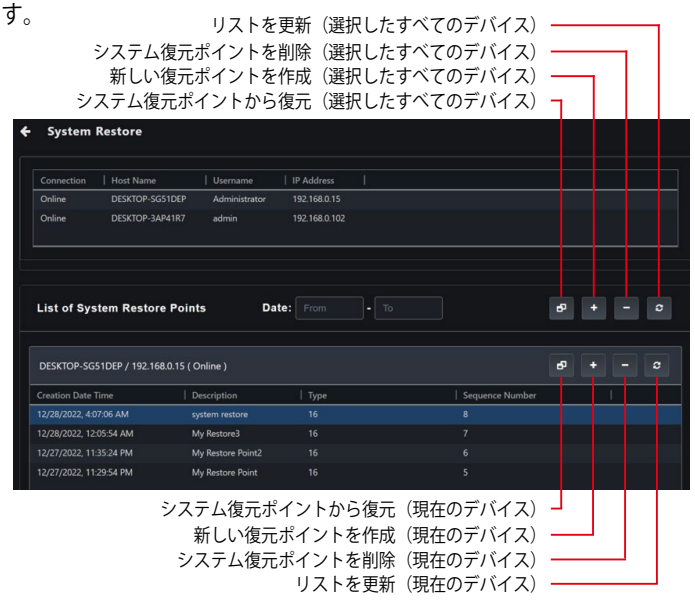


ハードウェアデバイスをクリックすると、ハードウェアデバイスの詳細が表示されます。



4.13 システム復元

デバイスリストから1つまたは複数のクライアントデバイスを選択して、システム復元ポイントの作成、削除、およびシステム復元ポイントからシステムを復元します。



- クライアントデバイスのシステムの復元（システムの保護）が無効の場合、有効になります。
- システム復元ポイントの作成、削除、およびシステム復元ポイントからシステムを復元機能は、クライアントデバイスの電源がオンで、接続されている場合にのみ使用できます。
- ネットワークの状態によっては、システム復元ポイントリストが更新されるまで時間が掛かる場合があります。リストを手動で更新するには ボタンをクリックしてください。

システム復元ポイントの作成

1. ボタンをクリックします。
2. **Restore Point Description（復元ポイントの説明）**欄に任意の説明を入力します。
3. **Create（作成）**をクリックします。

システム復元ポイントの削除

1. システム復元ポイントリストから削除したい復元ポイントを選択します。
2. ボタンをクリックします。
3. **Delete（削除）**をクリックします。

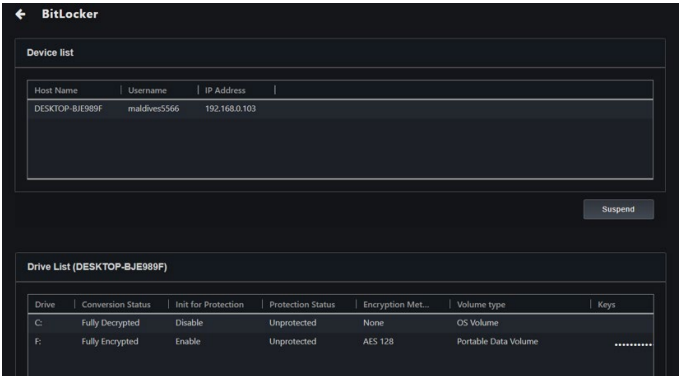
システム復元ポイントから復元

1. システム復元ポイントリストから復元したい復元ポイントを選択します。
2. ボタンをクリックします。
3. **Automatically restart the client device(s) after the system restore is complete（システムの復元完了後、クライアントデバイスを自動的に再起度する）**をチェックし、**Restore（復元）**をクリックします。

Automatically restart the client device(s) after the system restore is complete（システムの復元完了後、クライアントデバイスを自動的に再起度する）がチェックされていない場合、システム復元後にクライアントデバイスを手動で再起動する必要があります。

4.14 BitLocker

BitLockerの状態の表示と設定、BitLocker回復キーのバックアップまたは復元を行うことができます。



BitLocker暗号化の中断

1. **Suspend（中断）**をクリックします。

BitLocker暗号化を中断すると、パーティションに関係なくドライブ全体の暗号化が中断されます。

2. **Count（カウント）**欄にBitLocker暗号化が自動的に再有効化されるまでのクライアントデバイスの再起動回数を入力し**Save（保存）**をクリックします。

例として、Countを2に設定すると、クライアントデバイスが２回再起動されるとBitLockerが自動的に再有効化されます。

3. タスクが正常に完了したかどうかを確認するには、ミッションセンターで確認することができます。詳しくは **2.4 ミッションセンター** を参照してください。

BitLocker情報の表示

各ドライブのBitLocker状態を確認することができます。

クライアントデバイスのオペレーティングシステムがBitLockerをサポートしていない場合、**Drive List（ドライブリスト）**の**Protection Status（保護状態）**には［Unknown］と表示されます。

Drive（ドライブ）	ドライブレターを表示します。
Conversion status（変換状態）	暗号化状態を表示します。
Initialize protection（保護の初期化）	保護の初期化状態を表示します。
Protection status（保護状態）	保護状態を表示します。
Encryption method（暗号化方式）	暗号化方式を表示します。
Volume type（ボリュームタイプ）	ボリュームタイプを表示します。
Keys（キー）	暗号化キーを表示します。
Hide keys（キーを非表示）	クリックして暗号化キーを非表示にします。
Backup（バックアップ）	クリックして暗号化キーをバックアップします。

5章

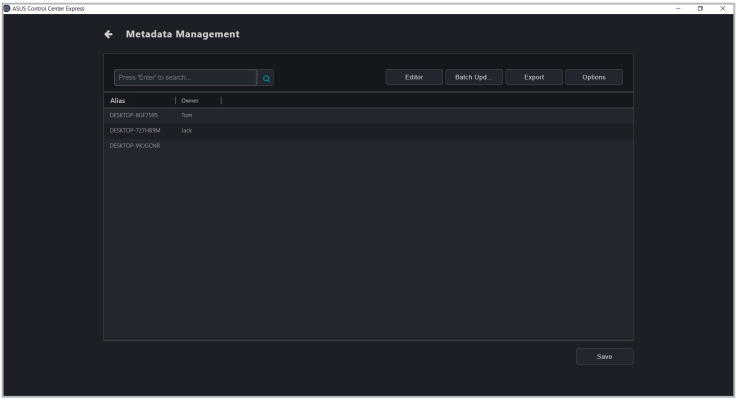
本章はメタデータ管理、ソフトウェア管理、タスクスケジューラー、ハードウェアベースの管理機能を説明します。

管理機能

5.1 メタデータの管理

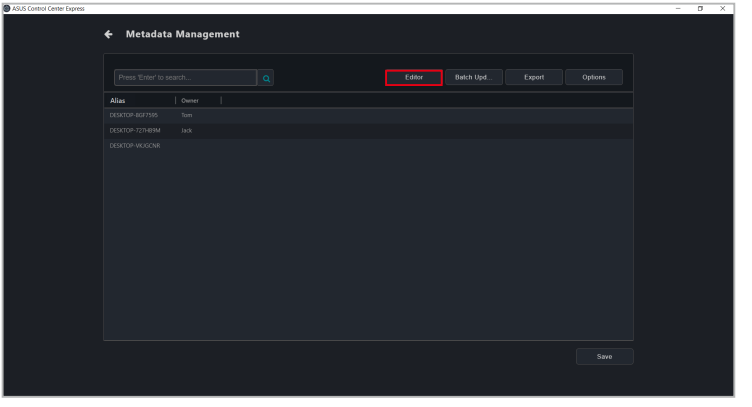
デバイス情報を確認する際に表示されるメタデータ欄と情報を追加または編集することができます。

右上のメニューバーで  をクリックすると**Metadata Management（メタデータ管理）**の画面が開きます。



5.1.1 メタデータ欄の追加

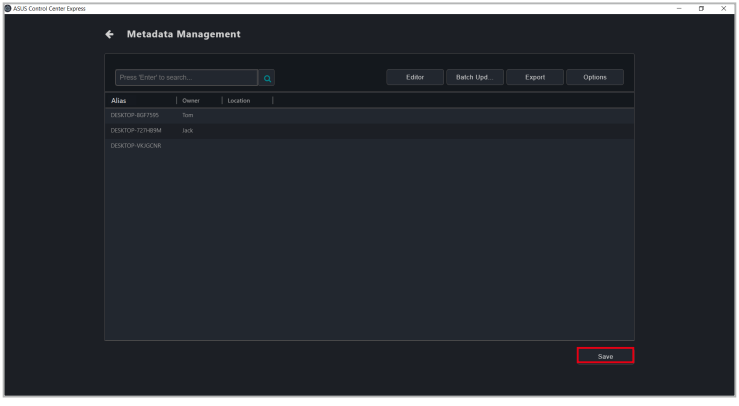
1. **Editor（エディター）**をクリックします。



2. 追加するメタデータ欄の名前を入力し、**Add（追加）**をクリックします。

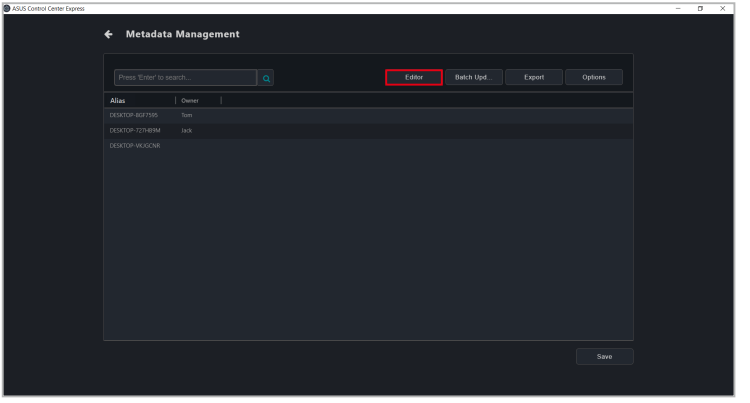
3. 新規メタデータ欄がメタデータの管理一覧に表示されます。**Save（保存）**をクリックして変更内容を保存します。

この例では、「Location（場所）」メタデータ欄を追加しています。

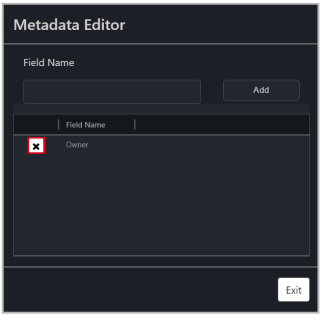


5.1.2 メタデータ欄の削除

1. **Editor（エディター）**をクリックします。

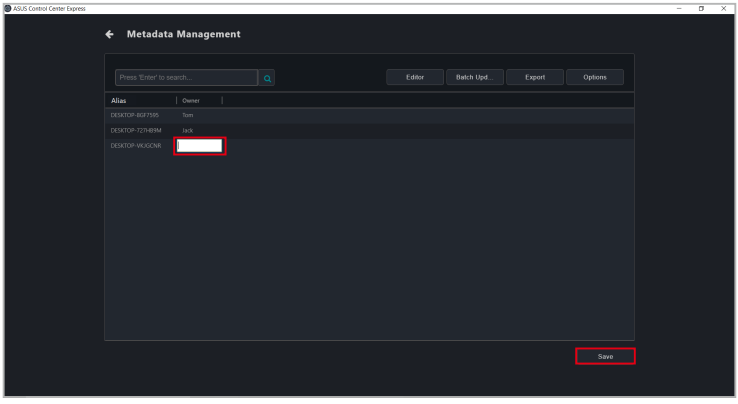


2. 削除するメタデータ欄の脇にある「**X**」をクリックし、**Yes（はい）**をクリックします。



5.1.3 メタデータを手動で更新

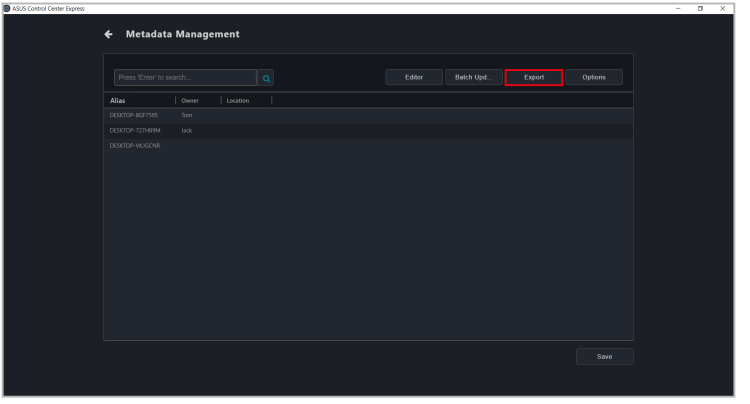
各デバイスで、Alias（エイリアス）などのデフォルトメタデータや、ユーザー定義されたメタデータの欄をクリックすることで、内容を編集して更新することができます。変更が終了したら**Save（保存）**をクリックしてください。複数のデバイスのメタデータを素早く編集することができます。



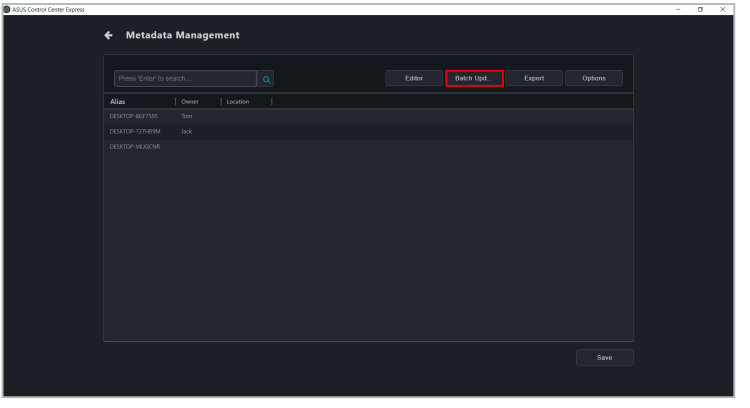
5.1.4 バッチ更新を使用したメタデータの更新

1. まず、**Export（エクスポート）**をクリックして、更新するメタデータ欄の.csvファイルをエクスポートします。

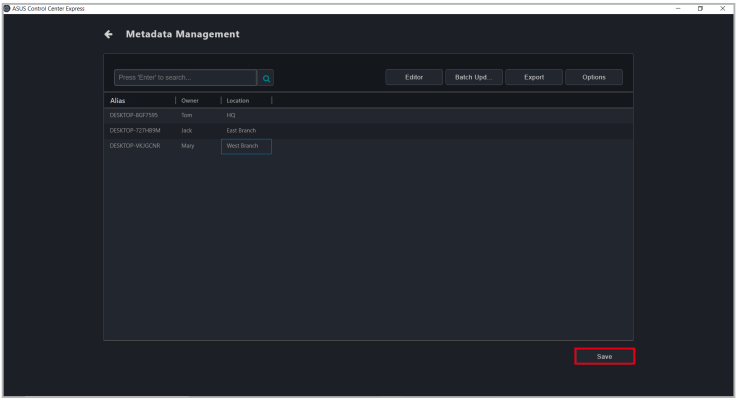
エクスポートするメタデータをカスタマイズする場合は、**Options（オプション）**をクリックし、続いてエクスポートするメタデータ欄を選択します。メタデータ欄の選択を解除するとその欄は非表示になり.csvファイルへはエクスポートされません。



2. エクスポートした.csvファイルへメタデータ欄のデータを入力して更新します。
3. **Batch Update（バッチ更新）**をクリックし、更新したした.csvファイルを選択して**Open（開く）**をクリックします。
メタデータ欄には.csvファイルの情報が自動的に入力されます。



4. **Save**（**保存**）をクリックし、更新内容を保存します。



5.2 ソフトウェアの管理

選択したデバイスへソフトウェアのセットアップとスクリプトファイルを配布、ソフトウェアプールへソフトウェアパッケージを追加、ソフトウェア情報を確認、ソフトウェアをブラックリストに追加、選択したクライアントデバイスへソフトウェアのルールを設定など、ソフトウェアを一元管理することができます。

5.2.1 ソフトウェアの配布

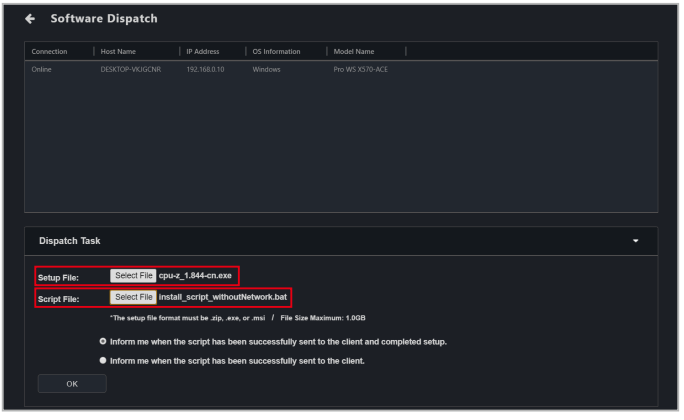
ソフトウェアのセットアップとスクリプトのファイルを配布することができます。

Software Dispatch（ソフトウェアの配布）へアクセスする場合は、クライアントデバイスを選択し、続いて**Select Function（機能の選択）** > **Software Management（ソフトウェアの管理）** > **Software Dispatch（ソフトウェアの配布）**をクリックします。

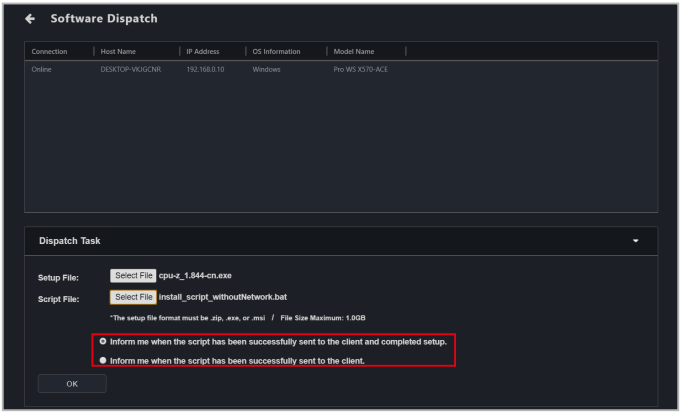
ソフトウェアのクライアントデバイスへの配布

1. クライアントデバイスへアップロードして配布する**Setup File（セットアップファイル）**と**Script File（スクリプトファイル）**を選択します。

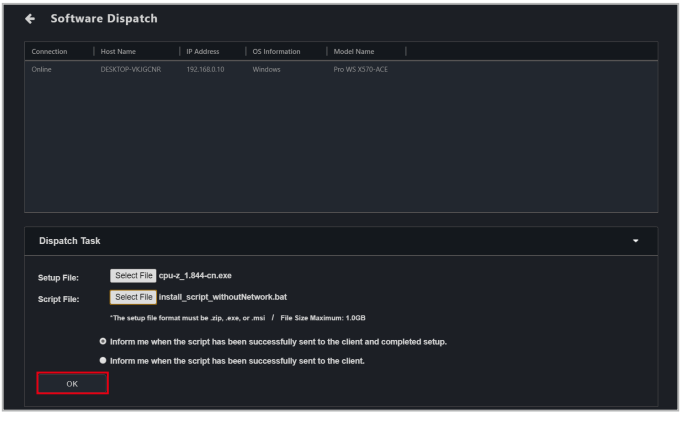
- 次のファイル形式をサポートします：.zip .exe .msi
- セットアップファイルのサイズは1.0 GBを超えないようにしてください。
- ソフトウェアのセットアップファイルとバッチファイルをZIP形式でパッケージする場合は、バッチファイルの名前を**install_script.bat**に変更してからパッケージしてください。



2. （任意）スクリプトがクライアントに正常に送信され設定が完了した場合、またはスクリプトがクライアントに正常に送信された場合の通知シナリオを選択します。

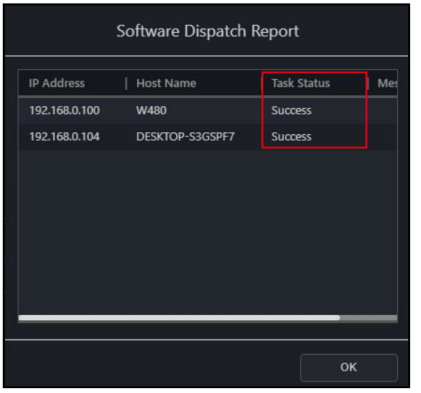


3. **OK**をクリックし、ソフトウェアの配布が終了するまで待ちます。完了したら、選択した通知シナリオに基づき、通知を受け取れます。

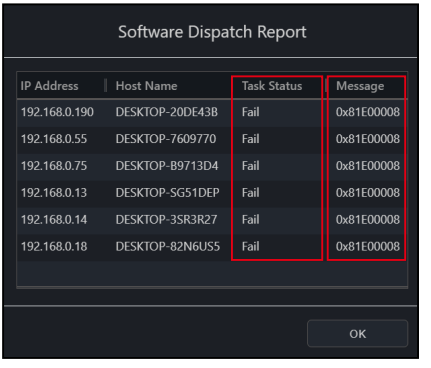


ソフトウェア配布プロセスでは、ソフトウェアインストールのユーザーインターフェイスや通知は表示されません。配布するソフトウェアが、ユーザーの操作を必要としないサイレントモードのインストールをサポートしていること、およびソフトウェアをバックグラウンドで自動的にインストールするためにインストール・プロセスを実行するスクリプトファイルがあることを確認してください。

4. 配布処理が開始され、結果がミッションセンターに表示されます。配布が成功すると**Task Status（タスクの状態）**列に**Success（成功）**が表示されます。

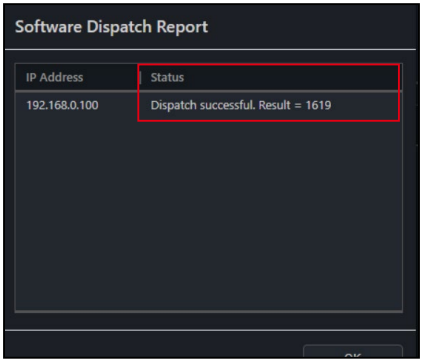


配布が失敗した場合**Task Status（タスクの状態）**列に**Fail（失敗）**が表示され、Message（メッセージ）列に配布メッセージのコードが表示されます。メッセージコードについて、詳しくは次の表をご参照ください。



メッセージコード	詳細
0x81E00000	サーバーが返したデータを抽出できませんでした。
0x81E00004	サーバーが返したデータを解析できませんでした。
0x81E00007	サーバーが返したデータを取得できませんでした。
0x81E00008	クライアントデバイスの接続状態を確認してください。

セットアップの結果はソフトウェア配布レポートで確認することができます。



- Windows Installer応答ファイルスクリプトがソフトウェア配布結果とメッセージコードを返す場合は、MsiExec.exeとInstMsi.exeのエラーメッセージを参照してください。
- ソフトウェアのインストールはオペレーティングシステムのアンチウイルスソフトウェアに影響を受けることがあります。ソフトウェアパッケージとスクリプトファイルに問題がないことが確認されている状態でインストールに失敗する場合は配布とインストールを実行する前にクライアントデバイスのアンチウイルスを一時的に無効にしてください。

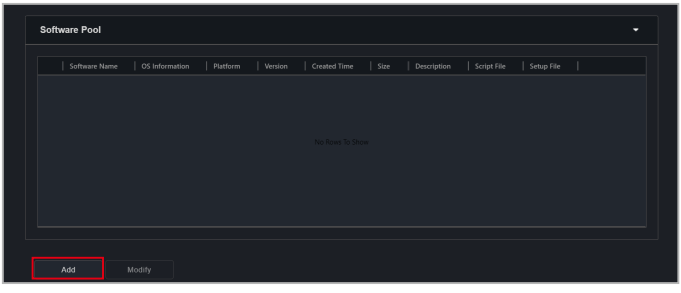
5.2.2 ソフトウェアプール

ソフトウェアプールへアップロードしたソフトウェアパッケージは配布、削除、変更することができます。

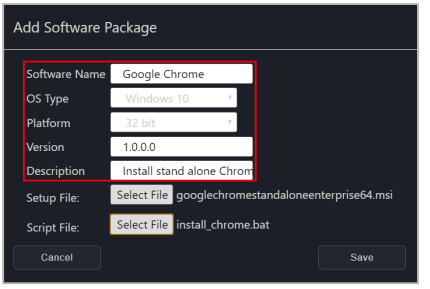
ソフトウェアプールへアクセスする場合は、クライアントデバイスを選択して、**Select Function（機能の選択）** > **Software Management（ソフトウェアの管理）** > **Software Dispatch（ソフトウェアの配信）**をクリックし、**Software Dispatch（ソフトウェアの配信）**画面の下端までスクロールしてください。

ソフトウェアプールへのソフトウェアパッケージの追加

1. **Add（追加）**をクリックします。

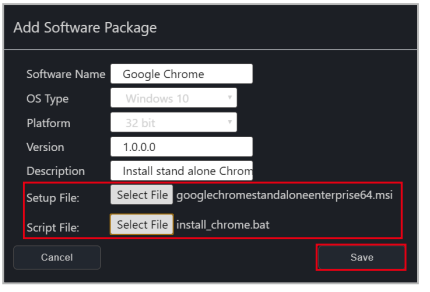


2. **Software Name（ソフトウェア名）**、**OS Type（OS タイプ）**、**Platform（プラットフォーム）**、**Version（バージョン）**欄へ必要な情報を入力します。**Description（説明）**欄にはソフトウェアの簡単な説明を入力することもできます。

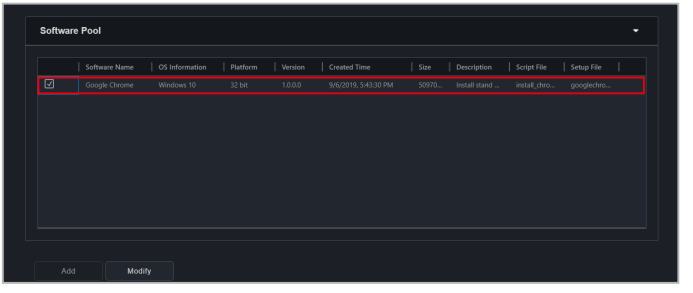


3. アップロードする**Setup File（セットアップファイル）**と**Script File（スクリプトファイル）**を選択します。終了したら**Save（保存）**をクリックします。

- 次のファイル形式をサポートします：.zip .exe .msi
- セットアップファイルのサイズは1.0 GBを超えないようにしてください。

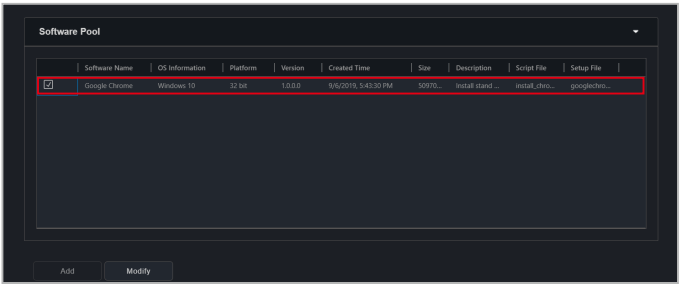


4. 追加されたソフトウェアパッケージはソフトウェアプールの一覧に表示されます。

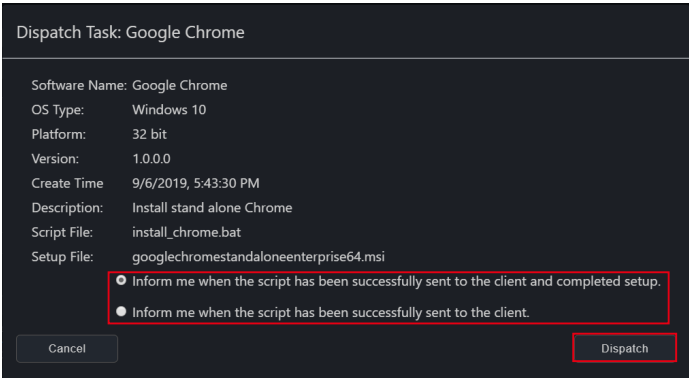


ソフトウェアプールを使用したソフトウェアの配布

1. **Software Pool**（**ソフトウェアプール**）で、配布するソフトウェアパッケージをクリックします。

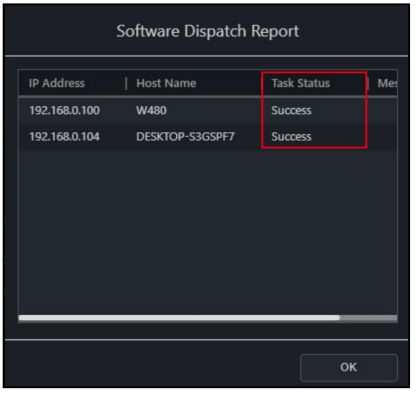


2. 通知シナリオを選択し、**Dispatch**（**配布**）をクリックします。ソフトウェアの配布プロセスが完了したら、選択した通知シナリオに基づき、通知を受け取ることができます。

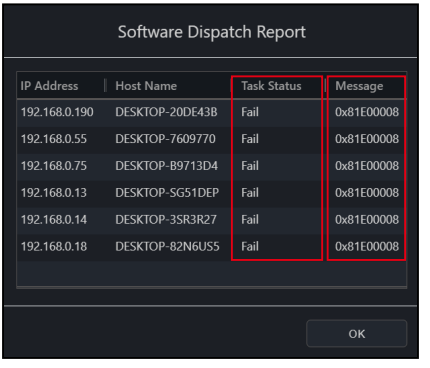


ソフトウェア配布プロセスでは、ソフトウェアインストールのユーザーインターフェイスや通知は表示されません。配布するソフトウェアが、ユーザーの操作を必要としないサイレントモードのインストールをサポートしていること、およびソフトウェアをバックグラウンドで自動的にインストールするためにインストール・プロセスを実行するスクリプトファイルがあることを確認してください。

3. 配布処理が開始され、結果がミッションセンターに表示されます。配布が成功すると**Task Status（タスクの状態）**列に**Success（成功）**が表示されます。



配布が失敗した場合**Task Status（タスクの状態）**列に**Fail（失敗）**が表示され、Message（メッセージ）列に配布メッセージのコードが表示されます。メッセージコードについて、詳しくは次の表をご参照ください。

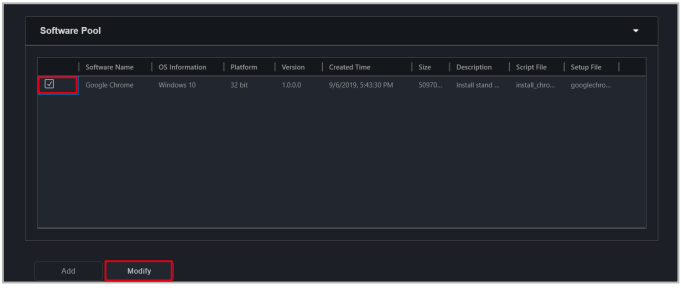


メッセージコード	詳細
0x81E00000	サーバーが返したデータを抽出できませんでした。
0x81E00004	サーバーが返したデータを解析できませんでした。
0x81E00007	サーバーが返したデータを取得できませんでした。
0x81E00008	クライアントデバイスの接続状態を確認してください。

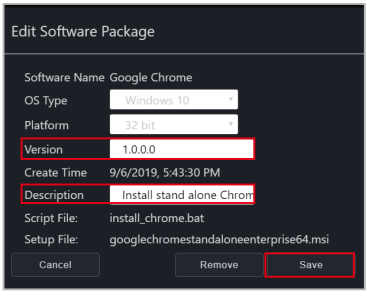
- Windows Installer応答ファイルスクリプトがソフトウェア配布結果とメッセージコードを返す場合は、MsiExec.exeとInstMsi.exeのエラーメッセージを参照してください。
- ソフトウェアのインストールはオペレーティングシステムのアンチウイルスソフトウェアに影響を受けることがあります。ソフトウェアパッケージとスクリプトファイルに問題がないことが確認されている状態でインストールに失敗する場合は配布とインストールのプロセス中にクライアントデバイスのアンチウイルスを一時的に無効にしてください。

ソフトウェアパッケージの編集

1. **Software Pool（ソフトウェアプール）**で、編集するソフトウェアパッケージを選択し、**Modify（編集）**をクリックします。

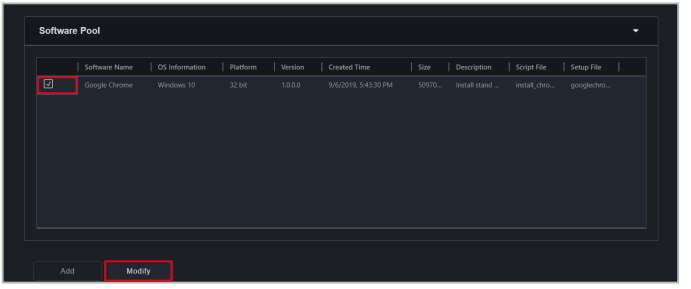


2. **Version（バージョン）**と**Description（説明）**を編集することができます。終了したら、**Save（保存）**をクリックして編集内容を保存します。

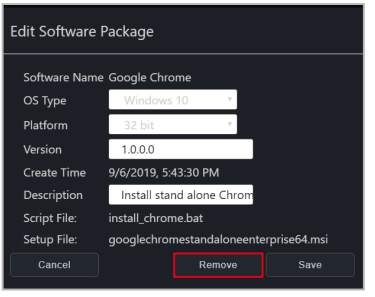


ソフトウェアパッケージの削除

1. **Software Pool**（**ソフトウェアプール**）で、削除するソフトウェアパッケージを選択し、**Modify**（**編集**）をクリックします。



2. **Remove**（**削除**）をクリックし、ソフトウェアパッケージをソフトウェアプールから削除します。

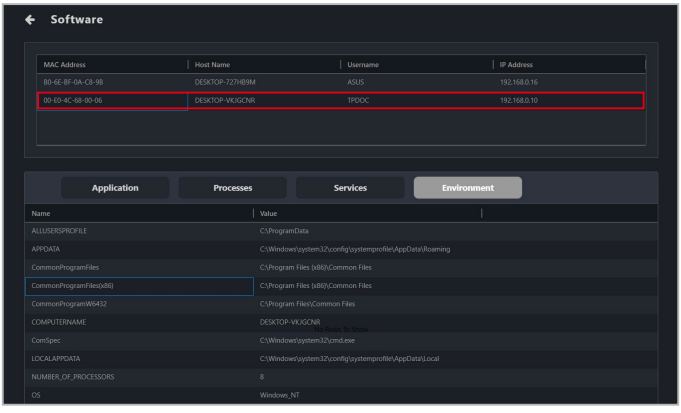


5.2.3 ソフトウェア情報

ソフトウェア情報を閲覧するクライアントデバイスを選択し、**Select Function（機能の選択）**> **Software Management（ソフトウェアの管理）**> **Software Information（ソフトウェア情報）**の順に進むことで、アプリケーション、プロセス、サービス、環境変数の情報を確認することができます。

ソフトウェア情報画面の上部ブロックでデバイスをクリックすると、選択したデバイスのアプリケーション、プロセス、サービス、環境変数がタブ別に表示されます。

一部のオペレーティングシステムアプリケーション、プロセス、サービスは削除、終了、停止することができません。



アプリケーションタブ

Application（アプリケーション）タブで、選択したクライアントデバイスにインストールされたアプリケーションの詳細情報を確認することができます。アプリケーションをクリックし、**Uninstall（アンインストール）**を選択して、選択したデバイスすべてからアプリケーションをアンインストールすることもできます。

- 選択したアプリケーションをアンインストールすることができない場合は、**Uninstall（アンインストール）**ボタンはグレーアウト表示されます。
- （更新）ボタンをクリックするとソフトウェア一覧が更新されます。

プロセスタブ

Processes（プロセス）タブではアクティブなプロセスの情報を確認することができます。プロセスをクリックし、**End Task（タスクの終了）**を選択してプロセスを終了することもできます。

サービスタブ

Services（サービス）タブでは選択したデバイスで利用できるサービスの情報を確認することができます。サービスをクリックして**Start（開始）**をクリックすればサービスが開始され、**Stop（停止）**をクリックすれば実行中のプロセスが停止します。

環境タブ

Environment（環境）タブでは、共通の環境変数の情報を確認することができます。

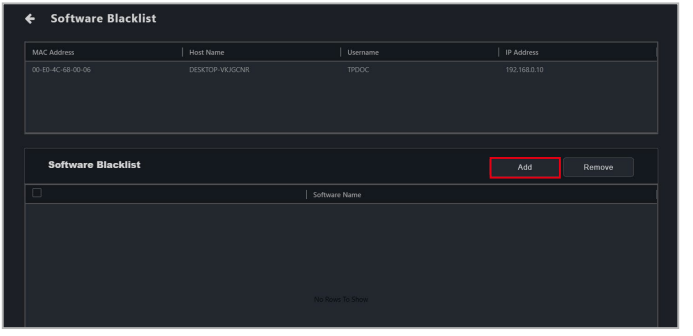
5.2.4 ソフトウェアのブラックリスト

選択したデバイスすべてで、ソフトウェアをブラックリストへ追加することができます。

Software Blacklist（ソフトウェアのブラックリスト）へアクセスする場合は、クライアントデバイスを選択し、続いて**Select Function（機能の選択）** > **Software Management（ソフトウェアの管理）** > **Software Blacklist（ソフトウェアのブラックリスト）**をクリックします。

ソフトウェアをブラックリストへ追加

1. **Add（追加）**をクリックします。

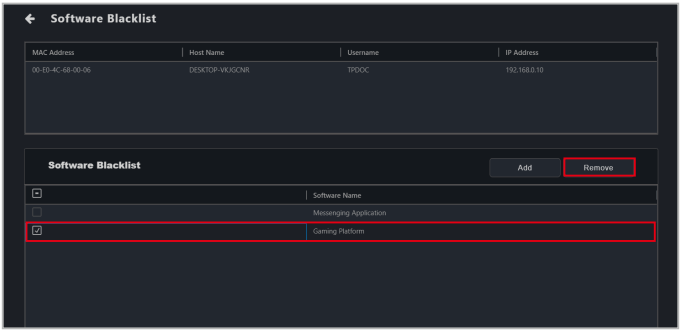


2. ブラックリストへ追加するソフトウェアの名前を入力し、**Save（保存）**をクリックします。

ブラックリストへ追加するソフトウェアのフルネーム（例：cmd.exe）を入力してください。ASUS Control Center Expressの**Software Information（ソフトウェア情報）**ページ、またはWindowsコマンドライン/タスクマネージャーでソフトウェアのフルネームを確認することができます。ソフトウェア情報の詳細については、**5.2.3 ソフトウェア情報**を参照してください。

ソフトウェアをブラックリストから削除

ブラックリストからソフトウェアを選択し、**Remove（削除）**をクリックして、**OK**をクリックします。



5.2.5 インストーラー

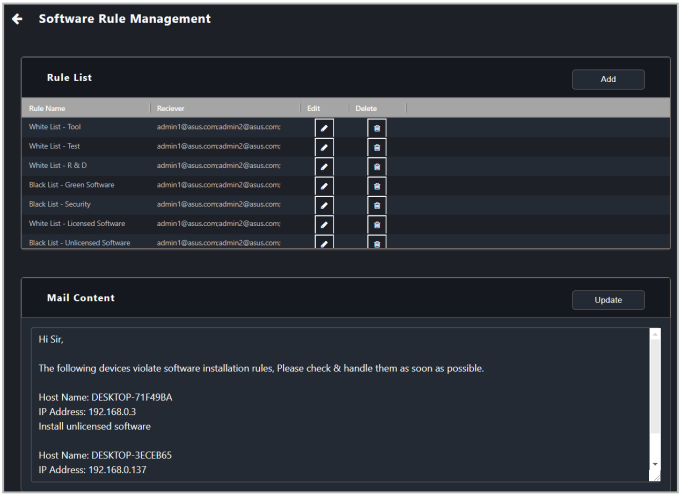
ドライバー、ユーティリティアプリケーション、BIOSをダウンロードして単一または複数のデバイスへ更新することができます。インストーラーの詳細については、**4.11 インストーラー**を参照してください。

5.2.6 ソフトウェアルールの管理

ソフトウェアルールの管理を使用してソフトウェアルールを設定し、ユーザーがクライアントデバイスへインストールできるソフトウェアアプリケーションを管理することができます。ソフトウェアをホワイトリストまたはブラックリストへ追加でき、ユーザーがホワイトリストに適合しないか、ブラックリストに適合するソフトウェアをインストールした場合、ユーザーが定義した受信者に、ソフトウェアのインストールを通知するメールが送信されます。

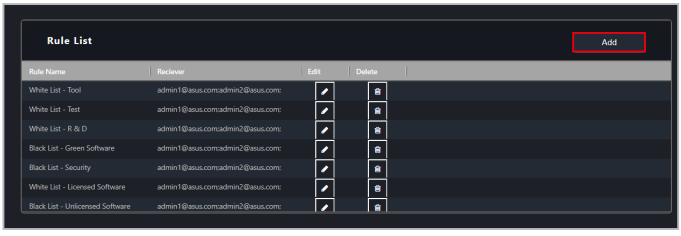
Software Rule Management（ソフトウェアルールの管理）へアクセスする場合は、クライアントデバイスを選択し、続いて**Select Function（機能の選択）**> **Software Management（ソフトウェアの管理）** > **Software Rule Management（ソフトウェアルールの管理）**をクリックします。

- ソフトウェアルール管理機能を使用する前に、SMTPが設定されており、テストメールを受信できることをご確認ください。詳細は、**8.1.1 SMTP 設定**を参照してください。
- ソフトウェアがクライアントデバイスにインストールされるなど、通知条件が満たされると通知メールが送信されます。ブラックリストの条件を満たし、かつホワイトリストの条件に違反した条件には、2つの通知メールが送信されます。
- ソフトウェアルールに適合しないソフトウェアがオフラインのクライアントデバイスにインストールされた場合、システムは違反状況を確認し、デバイスがオンラインになった時点で通知メールを送信します。

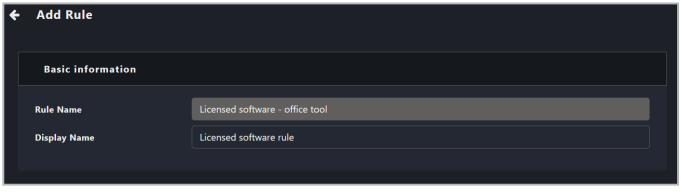


ルール一覧へ新規ルールを追加

1. **Add（追加）**をクリックします。



2. **Basic Information（基本情報）**ブロックに必要な情報を入力します。

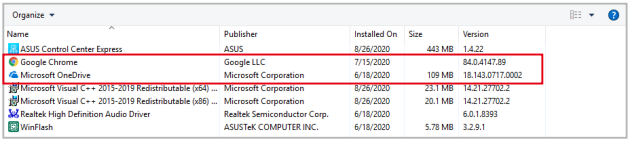


Rule Name（ルール名）	ルール名を入力します。
Display Name（表示名）	このルールの通知メールの件名を入力します。

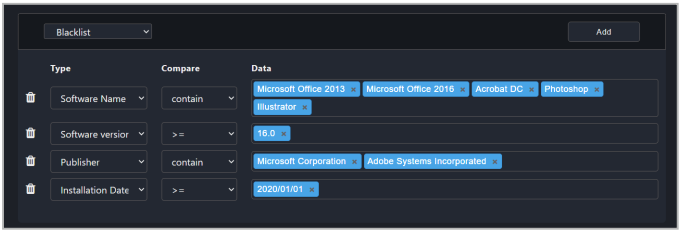
3. **Blacklist（ブラックリスト）**または**Whitelist（ホワイトリスト）**条件を追加し、**Type（タイプ）**と**Condition（条件）**を選択してルールのキーワードを**Data（データ）**欄に入力します。**Add（追加）**をクリックしてブラックリストまたはホワイトリストの条件を追加します。

- ブラックリストの条件とホワイトリストの条件が矛盾する場合は、システムはブラックリストの条件を優先します。
- 複数のキーワードが1つのブラックリスト/ホワイトリスト条件で入力された場合、キーワードのいずれかが条件を満たすか違反しただけで、ブラックリスト/ホワイトリストの条件は有効になります。
- 1つのルール内で複数のブラックリスト/ホワイトリスト条件を設定した場合、ルールを有効にするにはすべての条件が満たされる必要があります。

- 複数のキーワードを入力する場合、各キーワードの後に<Enter>キーを押して各キーワードを区切ります。
- 表示される情報はソフトウェアに応じて異なります。**Control Panel（制御パネル）** > **Programs（プログラム）** > **Programs and Features（プログラムと機能）**に表示されるソフトウェア情報を参照することをお勧めします。



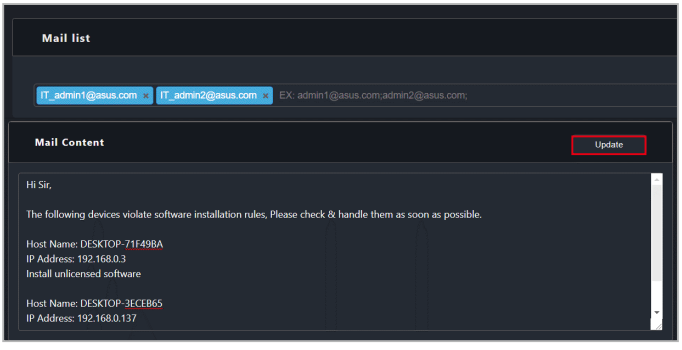
- ホワイトリストとブラックリストの条件一覧は、**ホワイトリストの条件** と **ブラックリストの条件**のセクションを参照してください。



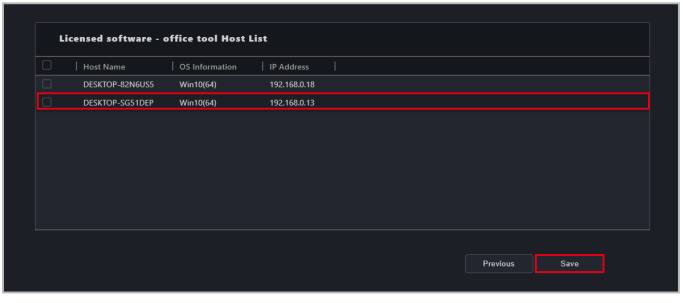
Blacklist / Whitelist（ブラックリスト/ホワイトリスト）	ブラックリストまたはホワイトリストの条件としてルールを設定します。
Type（タイプ）	ブラックリストまたはホワイトリストのキーワードとして**Data（データ）**欄へ入力するデータのタイプ（**Software Name（ソフトウェア名）**、**Software Version（ソフトウェアバージョン）**、**Publisher（発行者）**、**Installation Dat（インストール日）**を選択します。
Compare（比較）	比較条件を選択します。選択した**Type（タイプ）**に応じて、選択肢は異なります。
Data（データ）	選択した**Type（タイプ）**に対応するキーワードを入力します。

4. 手順3を繰り返して、ブラックリストまたはホワイトリストの条件を追加します。
5. 通知を送信するメールアドレスを入力します。続いて、通知メールのコンテンツを入力し、終了したら**Update（更新）**をクリックします。

複数のメールアドレスを入力する場合、各アドレスの後に<Enter>キーを押してアドレスを区切ります。



6. 終了したら**Next（次へ）**をクリックします。
7. このソフトウェアルールを提供するクライアントデバイスを選択し、続いて**Save（保存）**をクリックしてソフトウェアルールの追加を終了します。



ホワイトリストの条件

Type（タイプ）	Compare（比較）	Data（データ）
Software Name（ソフトウェア名）	Contains（含む）	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致した場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致しない場合、通知メールが送信されます。
	Does not contain（含まない）	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致しない場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致した場合、通知メールが送信されます。
Version（バージョン）	>	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも高い場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも低い場合、通知メールが送信されます。
	<	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも低い場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも高い場合、通知メールが送信されます。
	=	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しい場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しくない場合、通知メールが送信されます。
	!=	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しくない場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しい場合、通知メールが送信されます。
	>=	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと同じかそれよりも高い場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも低い場合、通知メールが送信されます。

Version（バージョン）	**<=**	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと同じかそれよりも低い場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと同じかそれよりも高い場合、通知メールが送信されます。
Developer（開発者）	**Contains（含む）**	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致した場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致しない場合、通知メールが送信されます。
	Does not contain（含まない）	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致しない場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致した場合、通知メールが送信されます。
Installation Date（インストール日）	**>**	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも新しい場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも古い場合、通知メールが送信されます。
	<	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも古い場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも新しい場合、通知メールが送信されます。
	=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しい場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しくない場合、通知メールが送信されます。
	!=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しくない場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しい場合、通知メールが送信されます。

Installation Date（インストール日）	>=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しいかそれよりも新しい場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも古い場合、通知メールが送信されます。
	<=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しいかそれよりも古い場合、通知メールは送信されません。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも新しい場合、通知メールが送信されます。

ブラックリストの条件

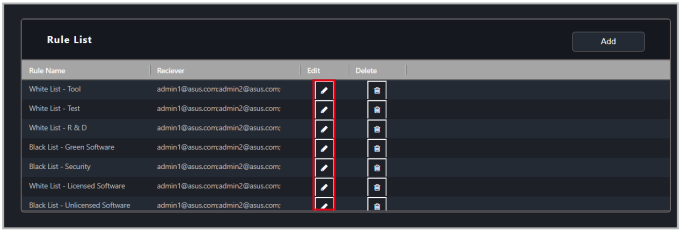
Type（タイプ）	Compare（比較）	Data（データ）
Software Name（ソフトウェア名）	Contains（含む）	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致した場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致しない場合、通知メールは送信されません。
	Does not contain（含まない）	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致しない場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される名前に一致した場合、通知メールは送信されません。
Version（バージョン）	>	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも高い場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも低い場合、通知メールは送信されません。
	<	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも低い場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも高い場合、通知メールは送信されません。
	=	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しい場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しくない場合、通知メールは送信されません。

Version（バージョン）	**!=**	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しくない場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと等しい場合、通知メールは送信されません。
	>=	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと同じかそれよりも高い場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンよりも低い場合、通知メールは送信されません。
	<=	クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと同じかそれよりも低い場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのバージョンがここに入力されるバージョンと同じかそれよりも高い場合、通知メールは送信されません。
Developer（開発者）	**Contains（含む）**	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致した場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致しない場合、通知メールは送信されません。
	Does not contain（含まない）	クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致しない場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアの名前がここに入力される開発者名に一致した場合、通知メールは送信されません。
Installation Date（インストール日）	**>**	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも新しい場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも古い場合、通知メールは送信されません。
	<	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも古い場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも新しい場合、通知メールは送信されません。

Installation Date（インストール日）	=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しい場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しくない場合、通知メールは送信されません。
	!=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しくない場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しい場合、通知メールは送信されません。
	>=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しいかそれよりも新しい場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも古い場合、通知メールは送信されません。
	<=	クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付と等しいかそれよりも古い場合、通知メールが送信されます。
		クライアントデバイスにインストールされたソフトウェアのインストール日がここに入力される日付よりも新しい場合、通知メールは送信されません。

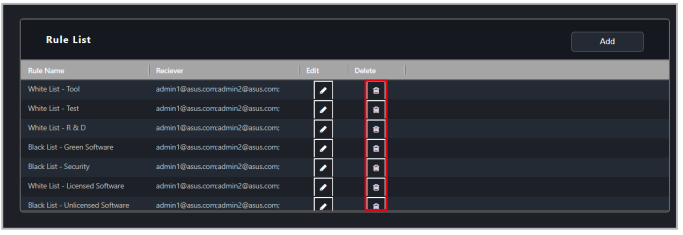
ソフトウェアルールの編集

1. 編集するルールの横にある  をクリックします。
2. ルールを編集したら**Next（次へ）**をクリックします。
3. このソフトウェアルールを適用するクライアントデバイスを選択し、**Save（保存）**をクリックしてソフトウェアルールの編集を完了します。

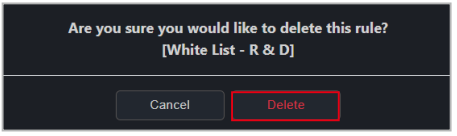


ソフトウェアルールの削除

1. 削除するルールの横にある をクリックします。



2. **Delete（削除）**をクリックしてソフトウェアのルールを削除します。

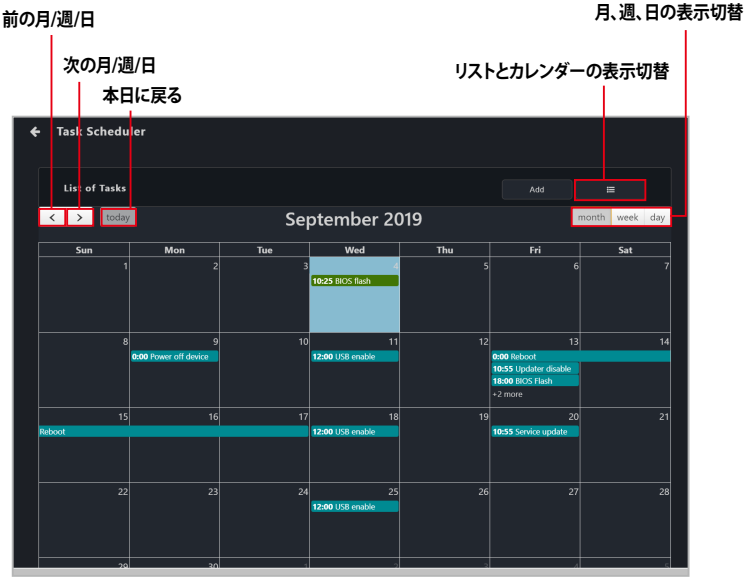


5.3 タスクスケジューラー

クライアントデバイスでタスクのスケジュールを設定し、指定された日に実行させたり、定期的に繰り返して実行させることができます。タスクの設定を開始する場合は、デバイス一覧からタスクのスケジュールを設定するデバイスを選択し、Select Function（機能の選択）ドロップダウンリストから**Task Scheduler（タスクスケジューラー）**機能を選択します。

5.3.1 タスクスケジューラーカレンダーの概要

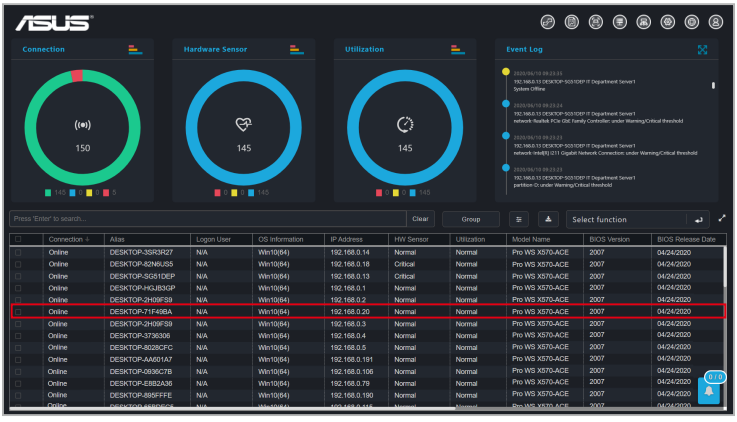
タスクスケジューラーのカレンダーで、設定済みのタスクを確認することができます。



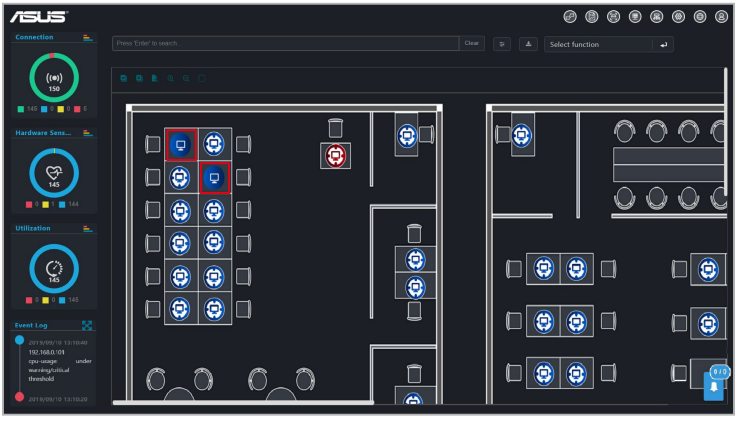
5.3.2 新しいタスクの設定

1. タスクを新たにスケジュール設定するデバイスを選択します。

クラシックダッシュボード

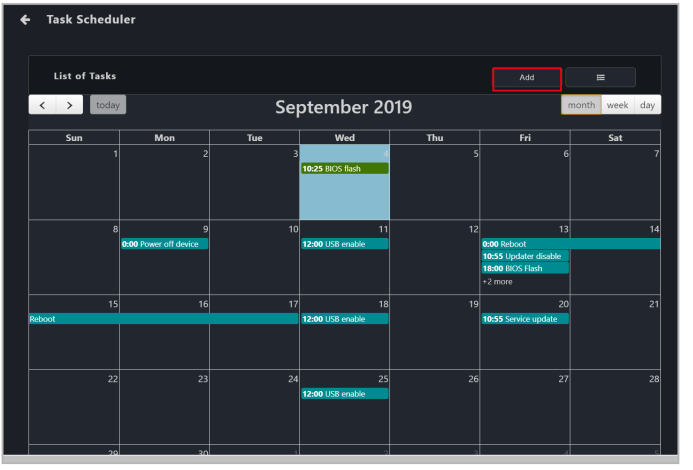


グラフィックダッシュボード



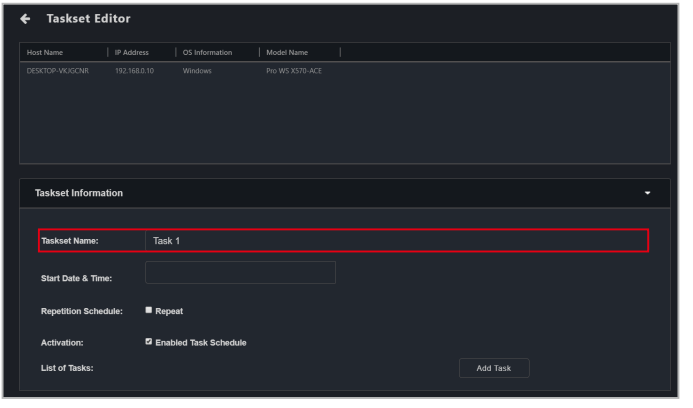
2. **Select function（機能の選択）**をクリックし、ドロップダウンメニューから**Task Scheduler（タスクスケジューラー）**を選択します。

3. **Add（追加）**をクリックします。



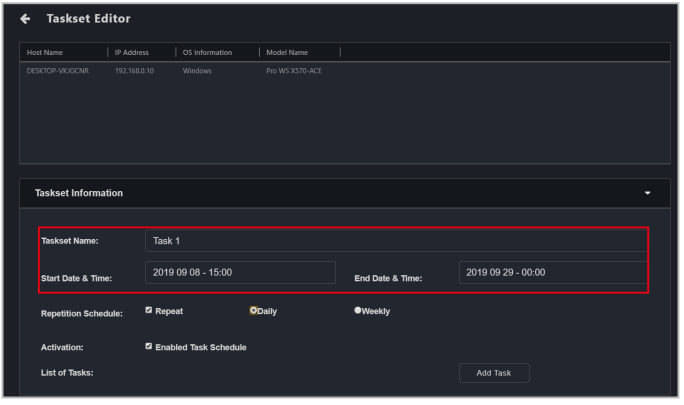
4. タスクセット（Taskset）の名前を入力します。

一度タスクを作成したら、タスクセット名は変更できません。

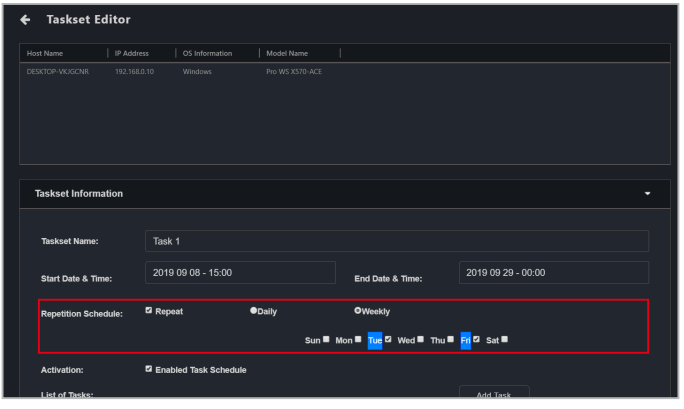


5. **Start Date & Time（開始日と時刻）**を選択します。一定期間の間タスクを繰り返す場合は、**Repeat（繰り返し）**を選択し、**End Date & Time（終了日と時刻）**を選択します。

End Date & Time（終了日と時刻）は**Repeat（繰り返し）**を選択した場合にのみ出現します。

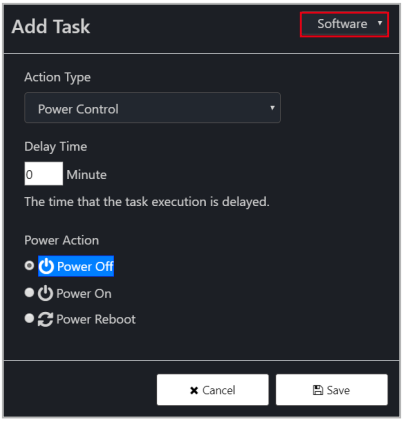


6. 前の手順で**Repeat（繰り返し）**を選択した場合は、タスクを**Daily（毎日）**または**Weekly（毎週）**のどちらで繰り返すかを選択します。**Weekly（毎週）**を選択すると、毎週タスクを実行する曜日を選択することができます。

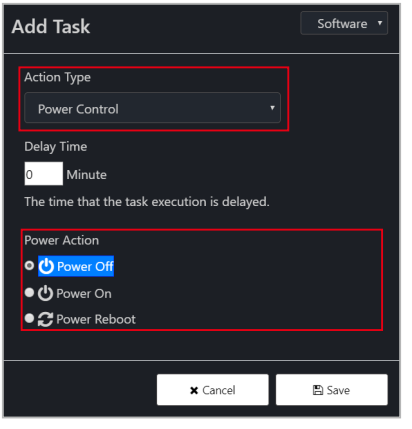


7. **Add Task（タスクの追加）**をクリックし、ソフトウェアベースの機能には**Software（ソフトウェア）**を、管理機能には**ハードウェアを**、電源制御機能には**DASH**または**vPro**を選択します。

Hardware（ハードウェア）機能は、リモート管理コントローラーをサポートするマザーボードを搭載し、管理LANポートを使用して接続されたクライアントデバイスでのみ使用できます。



8. ドロップダウンメニューから**Action Type（アクションのタイプ）**を選択します。Action Type（アクションタイプ）については、次ページ以降の表をご覧ください。



Software（ソフトウェア）

アクションのタイプ	アクションのオプション		説明
Power Control（電源制御）	Power Off（電源オフ）		デバイスの電源をオフ
	Power On（電源オン）		デバイスの電源をオン
	Power Reboot（電源再起動）		デバイスを再起動
Service Control（サービス制御）	Service Name（サービス名）		サービスの名前を入力
	Start（開始）		サービスを開始
	Stop（停止）		サービスを停止
	Restart（再起動）		サービスを再起動
Software Dispatch（ソフトウェアの配信）	Package Name（パッケージ名）		ソフトウェアプールからソフトウェアパッケージを選択
Security and Boot（セキュリティとブート）	Registry Tool（レジストリツール）	Enable（有効）	Windowsレジストリエディタを有効
		Disable（無効）	Windowsレジストリエディタを無効
	USB Control（USB制御）	Enable（有効）	USBポートを有効
		Disable（無効）	USBポートを無効
		Read Only（読み取り専用）	USBポートを読み取り専用に設定
	Fast Startup（高速スタートアップ）	Enable（有効）	高速スタートアップを有効
		Disable（無効）	高速スタートアップを無効
	Windows Update	Enable（有効）	Windows Updateを有効
		Disable（無効）	Windows Updateを無効
BIOS Cache（BIOSキャッシュ）	BIOS Cache List（BIOSキャッシュ一覧）		BIOSキャッシュからBIOSファイルを選択

- BitLockerまたはfTPMのリスクが検出された場合、BIOSキャッシュタスクが完了しないことがあります。事前にリスクを回避するための措置を行うことを強くおすすめします。詳しくは **4.10 BIOS** を参照してください。
- 関連するリスクを理解している場合は、**Allow updating BIOS when BitLocker is unsuspended or unknown（BitLockerが中断されていないか不明な場合にBIOSの更新を許可する）**、**Allow updating BIOS when BitLocker automatic backup of recovery key failed（BitLockerの回復キーの自動バックアップに失敗した場合にBIOSの更新を許可する）**、**Allow erasing fTPM security data when updating BIOS when creating a BIOS Cache task（BIOSキャッシュタスクを作成してBIOSを更新する際にfTPMセキュリティデータの消去を許可する）**をチェックすることで、これらのリスクを無視して作業を続行できます。

Hardware（ハードウェア）*

アクションのタイプ	アクションのオプション	説明
Power Control（電源制御）	Power Off（電源オフ）	デバイスの電源をオフ
	Force Power Off（電源を強制的にオフ）	デバイスの電源を強制的にオフ
	Power On（電源オン）	デバイスの電源をオン
	Power Reboot（電源再起動）	デバイスを再起動
Enable/ Disable Watchdog（ウォッチドッグを有効/無効）	Heartbeat Interval（ハートビートの間隔）	ハートビートの間隔を設定
	Enable（有効）	ウォッチドッグを有効
	Disable（無効）	ウォッチドッグを無効
Clear CMOS（CMOSの消去）	-	デバイスのCMOSを消去
Enable/ Disable KVM（KVMを有効/無効）	Enable（有効）	KVMを有効

* **これらのアクションカテゴリーは、リモート管理コントローラーをサポートするマザーボードでのみサポートされています。**

DASH

アクションのタイプ	アクションのオプション	説明
Power Control（電源制御）	Power On（電源オン）（G0/S0）	デバイスの電源をオン
	Power Off - Soft（電源オフ-ソフト）（G2/S5）	デバイスの電源をオフ
	Power Off - Hard（電源オフ-ハード）（G3）	デバイスの電源を強制的にオフ
	Power Cycle - Soft off（電源サイクル-ソフトオフ）（G2/S5）	オペレーティングシステムをシャットダウンした後、デバイスを再起動
	Sleep - Deep（スリープ-ディープ）（G1/S3）	スリープモードに入る（G1/S3）
	Master Bus Reset（マスターバスリセット）	ハードウェアのリセット
	Hibernate（ハイバネーション）（G1/S4）	ハイバネーションモードに入る（G1/S4）
	Restart Computer to BIOS（コンピュータを再起動してBIOSへ）	デバイスの再起動後、BIOSに入る
	Power On to BIOS（起動後にBIOSへ）	デバイスの電源を入れた後、BIOSに入る
	Restart Computer to IDE-R Floppy（コンピュータを再起動してIDE-Rフロッピーへ）	デバイスを再起動後、IDE-Rフロッピードライブに入る
	Power On to IDE-R Floppy（起動後にIDE-Rフロッピーへ）	デバイスの電源を入れた後、IDE-Rフロッピードライブに入る
	Restart Computer to IDE-R CDROM（コンピュータを再起動してIDE-R CD-ROMへ）	デバイスを再起動後、IDE-R ODDに入る
	Power On to IDE-R CDROM（起動後にIDE-R CD-ROMへ）	デバイスの電源を入れた後、IDE-R ODDに入る
	Sleep - Light（スリープ-ライト）（G1/S2）	スリープモードに入る（G1/S2）
	Power Cycle - Hard Off（電源サイクル-ハードオフ）（G3）	デバイスの電源を切り、再起動
	Diagnostic Interrupt（診断割り込み）（NMI）	エラーレポートの印刷とデバイスの再起動
	Power Off - Soft Graceful（電源オフ-ソフトグレースフル）（G2/S5）	オペレーティングシステムによる通常シャットダウン
	Power Off - Hard Graceful（電源オフ-ハードグレースフル）（G3）	ハードウェアによる通常シャットダウン
	Master Bus Reset Graceful（マスターバスリセットグレースフル）	通常シャットダウンとハードウェアのリセット
	Power Cycle (Graceful Soft Off)（電源サイクル（グレースフルソフトオフ））（G2/S5）	オペレーティングシステムによる通常シャットダウン後、デバイスを再起動
	Power Cycle (Graceful Hard Off)（電源サイクル（グレースフルハードオフ））（G3）	ハードウェアによる通常シャットダウン後、デバイスを再起動

*** これらのアクションカテゴリーは、リモート管理コントローラーをサポートするマザーボードでのみサポートされています。**

vPro

アクションのタイプ	アクションのオプション	説明
Power Control（電源制御）	Power On（電源オン）（G0/S0）	デバイスの電源をオン
	Power Cycle - Soft off（電源オフ-ソフト）（G2/S5）	デバイスの電源をオフ
	Master Bus Reset（マスターバスリセット）	ハードウェアのリセット
	Sleep - Deep（スリープ-ディープ）（G1/S3）	スリープモードに入る（G1/S3）
	Hibernate（ハイバネーション）（G1/S4）	ハイバネーションモードに入る（G1/S4）
	Power Off - Soft（電源オフ-ソフト）（G2/S5）	デバイスの電源をオフ
	Power Off - Soft Graceful（電源オフ-ソフトグレースフル）（G2/S5）	オペレーティングシステムによる通常シャットダウン
	Master Bus Reset Graceful（マスターバスリセットグレースフル）	通常シャットダウンとハードウェアのリセット
	Restart Computer to BIOS（コンピュータを再起動してBIOSへ）	デバイスの再起動後、BIOSに入る
	Power On to BIOS（起動後にBIOSへ）	デバイスの電源を入れた後、BIOSに入る
	Restart Computer to IDE-R Floppy（コンピュータを再起動してIDE-Rフロッピーへ）	デバイスを再起動後、IDE-Rフロッピードライブに入る
	Power On to IDE-R Floppy（起動後にIDE-Rフロッピーへ）	デバイスの電源を入れた後、IDE-Rフロッピードライブに入る
	Restart Computer to IDE-R CDROM（コンピュータを再起動してIDE-R CD-ROMへ）	デバイスを再起動後、IDE-R ODDに入る
	Power On to IDE-R CDROM（起動後にIDE-R CD-ROMへ）	デバイスの電源を入れた後、IDE-R ODDに入る

* これらのアクションカテゴリーは、リモート管理コントローラーをサポートするマザーボードでのみサポートされています。

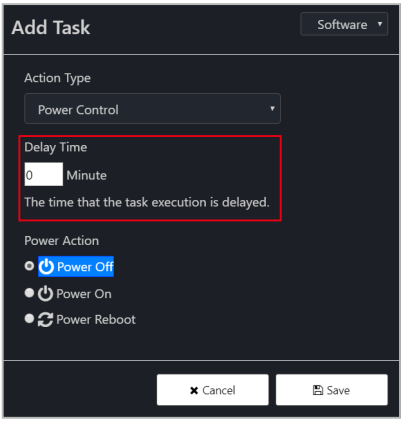
BMC

アクションのタイプ	アクションのオプション	説明
Power Control（電源制御）	Power On（電源オン）（G0/S0）	デバイスの電源をオン
	Power Off - Soft（電源オフ-ソフト）（G2/S5）	デバイスの電源をオフ
	Power Off - Hard（電源オフ-ハード）（G2/S5）	デバイスの電源を強制的にオフ
	Power Cycle - Soft Graceful（電源サイクル-ソフトグレースフル）（G2/S5）	オペレーティングシステムをシャットダウンした後、デバイスを再起動
	Power Cycle - Hard Off（電源サイクル-ハードオフ）（G3）	デバイスの電源を強制的にオフにした後、デバイスを再起動

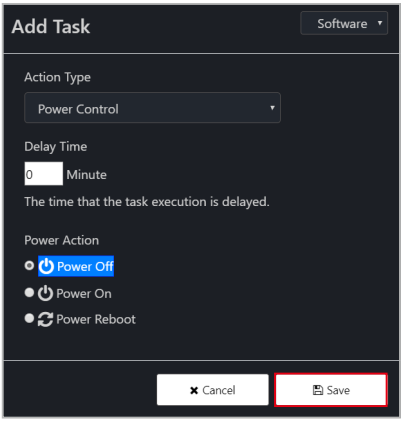
* これらのアクションカテゴリーは、リモート管理コントローラーをサポートするマザーボードでのみサポートされています。

9. **Delay Time（遅延時間）**を入力します。遅延時間は、直前のタスクが終了した後、このタスクが実行を開始するまで待機する時間を設定します。

複数のタスクのスケジュールを設定する場合は、各タスクが適切に実行されるよう、それぞれに遅延時間を設けてください。



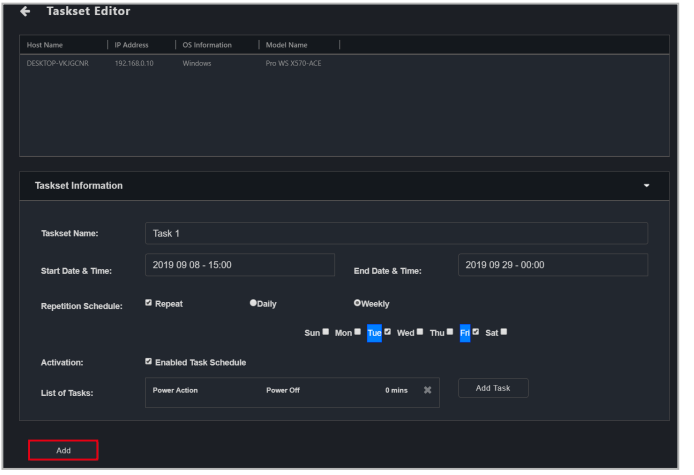
10. **Save（保存）**をクリックし、タスクを保存します。



11. 手順7～10を繰り返してタスクを追加します。タスクは**List of Tasks（タスク一覧）**に表示されます。

タスクを削除する場合は、**List of Tasks（タスク一覧）**でタスクの横にある「**X**」をクリックします。

12. 終了したら**Add（追加）**をクリックして、スケジュール設定されたタスクをタスクスケジューラーのカレンダーへ追加します。

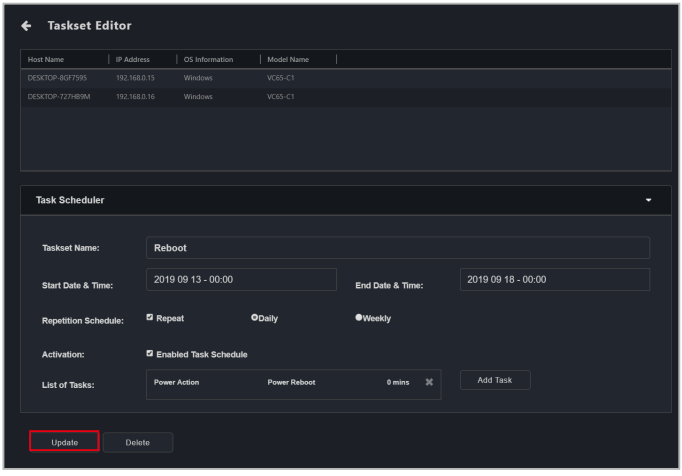


5.3.3 タスクの編集

1. タスクスケジューラーのカレンダーで、編集するスケジュール済みのタスクをクリックします。
2. **Start Date & Time（開始日と時刻）**、**End Date & Time（終了日と時刻）**、**Repetition Schedule（繰り返しスケジュール）**、**Activation（有効）**、**List of tasks（タスク一覧）**を編集することができます。

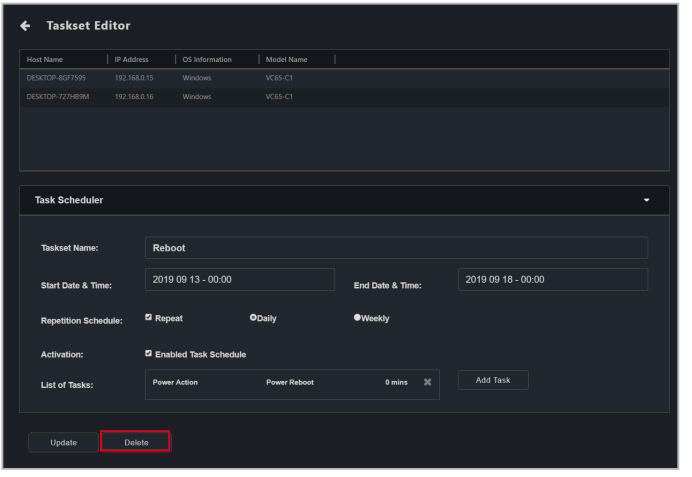
タスクを削除する場合は、**List of Tasks（タスク一覧）**でタスクの横にある「X」をクリックします。

3. スケジュールされたタスクの編集が終了したら、**Update（更新）**をクリックします。



5.3.4 タスクの削除

1. タスクスケジューラーのカレンダーで、削除するスケジュール済みのタスクをクリックします。
2. **Delete（削除）**をクリックしてスケジュールされたタスクを削除します。



5.4 OOB 制御

ASUS Control Center Expressが提供するOOB（Out of Band）制御機能は、デバイスの1対複数の管理を可能にし、BMC、DASH、RTL8117、vProリモート管理コントローラーを搭載したクライアントデバイスの制御にも対応しています。

- OOB制御機能を使用するには、クライアントデバイスのマザーボードが、BMC、DASH、RTL8117、vProリモート管理コントローラーに対応している必要があります。
- クライアントデバイスでOOB機能を使用する前に、リモート管理コントローラーの設定がクライアントデバイスのBIOSで設定されていることを確認してください。

5.4.1 リモート管理コントローラーの認証情報の設定

クライアントデバイスのOOB機能を使用する前に、ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーにログインするためのログインアカウントとパスワードを設定してください。これにより、OOBリモート機能の安全性が確保されます。

ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーにログインする際に使用するログイン情報の設定方法については、以下をご参照ください。

設定でアカウントとパスワードを設定する（BMC/DASH/vPro）

1. をクリックし、**Options（オプション）**>**General Configuration（全般設定）**と進み、**vPro Account（vProアカウント）**および**BMC Account（BMCアカウント）**までスクロールします。
   - vProコントローラーを設定するには、**vPro Account（vProアカウント）**にクライアントデバイスのリモート管理コントローラーのアカウントとパスワードを入力し、**Save（保存）**をクリックします。

MEBxはIntel BIOS拡張オプションであり、Intelクライアントデバイス用の設定です。MEBxに設定されたアカウントとパスワードは、Intel vProリモート管理コントローラーのアカウントとパスワードではありません。

- vProアカウントのパスワードは、8文字以上で、大文字（A～Z）1文字、数字（0～9）、特殊文字1文字を含む必要があります。
- 入力するアカウントとパスワードは、すでにクライアントデバイスに設定されているアカウントとパスワードと一致している必要があります。

- DASHコントローラーを設定するには、**DASH Account（DASHアカウント）**にクライアントデバイスのリモート管理コントローラーのアカウントとパスワードを入力します。DASHに使用するポートを入力したり、TLS（Transport Layer Security）の有効/無効を選択することができます。設定が完了したら**Save（保存）**をクリックします。

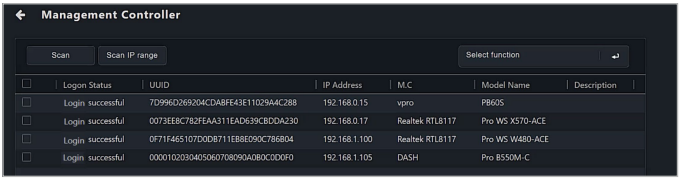
- **DASH Account（DASHアカウント）**のアカウントとパスワードは15文字までです。
- 入力するアカウントとパスワードは、すでにクライアントデバイスに設定されているアカウントとパスワードと一致している必要があります。

- BMCコントローラーを設定するには、**BMC Account（BMCアカウント）**にクライアントデバイスのリモート管理コントローラーのアカウントとパスワードを入力します。BMCに使用するポートを入力することもできます。設定が完了したら**Save（保存）**をクリックします。

- BMCアカウントは、アルファベット（A-z）ではじまり、1つ以上の数字（0-9）を含む、16文字以内である必要があります。パスワードは8文字以上で設定する必要があります。
- 入力するアカウントとパスワードは、すでにクライアントデバイスに設定されているアカウントとパスワードと一致している必要があります。

2. **BMC Account（BMCアカウント）**、**vPro Account（vProアカウント）**、**DASH Account（DASHアカウント）**を設定すると、ASUS Control Center Expressは自動的にクライアントデバイスのリモート管理コントローラーにログインします。**Management Controller（管理コントローラー）**ページでスキャンを実行し、クライアントデバイスのリモート管理コントローラーのログイン状態を確認することができます。

デフォルトのログインアカウントとパスワードがクライアントデバイスのリモート管理コントローラーと一致する場合、スキャン実行後に管理コントローラーページのログイン状態はLogin successful（ログイン成功）と表示されます。



入力したデフォルトのアカウントとパスワードは、同じリモート管理コントローラーのアカウントとパスワードを持つ複数のクライアントデバイスにログインするために使用することができます。

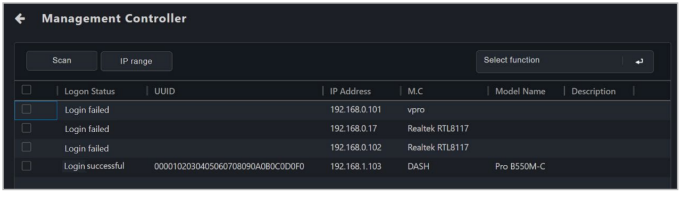
管理コントローラーによるアカウントとパスワードの設定

複数のクライアントデバイスのASUS Control Center Expressのリモート管理コントローラーのログインアカウントを管理コントローラーページから設定することができます。

リモート管理コントローラを搭載したクライアントデバイスにすでにエージェントが配置されている場合は、メインメニューページのデバイスリストからクライアントデバイスを選択します。RTL8117およびvProの場合は**Select Function（機能の選択）＞OOB - Control（OOB-制御）＞Account Management（アカウント管理）＞Set password（パスワードの設定）**を、BMCおよびDASHの場合は**Select Function（機能の選択）＞OOB - Control（OOB-制御）＞Account Management（アカウント管理）＞Login（ログイン）**をクリックします。

1 をクリックして、**Scan（スキャン）**または**Scan IP Range（IP範囲のスキャン）**を実行します。

2. スキャンの完了後、ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラに正常にログインしたかどうかを確認することができます。ASUS Control Center Expressで入力したアカウントとパスワードが、クライアントデバイスのリモート管理コントローラーのアカウントとパスワードと一致しない場合、**Login failed（ログイン失敗）**と**Login Status（ログイン状態）**欄に表示されます。



3. ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーにログインする際に使用するアカウントとパスワードを設定したいクライアントデバイスを選択します。

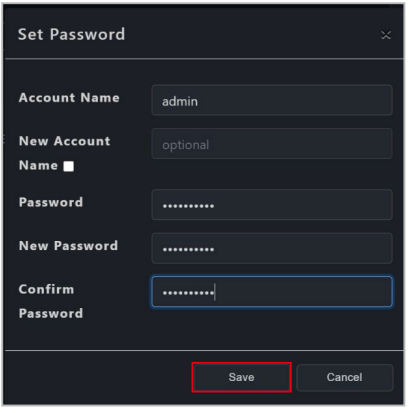
アカウントとパスワードを設定するために複数のクライアントデバイスを選択する場合は、必ず同じリモート管理コントローラーを持つクライアントデバイスを選択してください。

4. リモート管理コントローラーの種類によっては、アカウントとパスワードの設定手順が異なる場合があります。

RTL8117/vProの場合

a. **Select Function（機能の選択）＞Account Management（アカウント管理）＞Set password（パスワードの設定）**をクリックします。

b. ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーへのログインに使用するアカウントとパスワードを入力し、**Save（保存）**をクリックします。



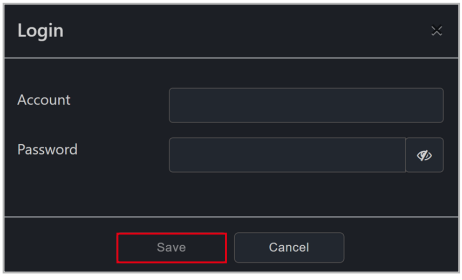
MEBxはIntel BIOS拡張オプションであり、Intelクライアントデバイス用の設定です。MEBxに設定されたアカウントとパスワードは、Intel vProリモート管理コントローラーのアカウントとパスワードではありません。

- vProアカウントのパスワードは、8文字以上で、大文字（A～Z）1文字、数字（0～9）、特殊文字1文字を含む必要があります。
- RTL8117のパスワードは、8文字以上で、大文字（A～Z）、小文字（a～z）、数字（0～9）を含む必要があります。

BMC/DASHの場合

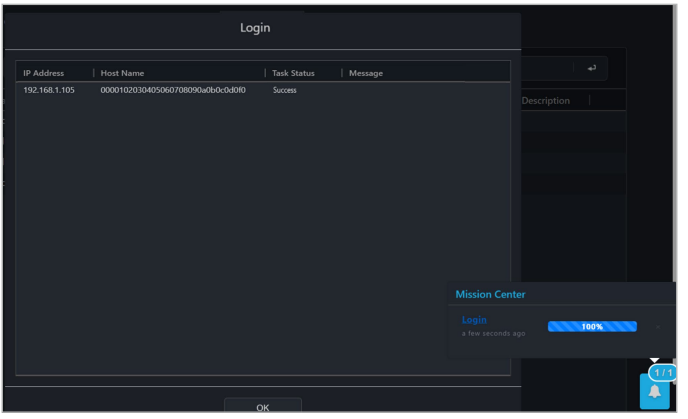
a. **Select Function（機能の選択）**>**Account Management（アカウント管理）**>**Login（ログイン）**をクリックします。

b. ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーへのログインに使用するアカウントとパスワードを入力し、**Save（保存）**をクリックします。

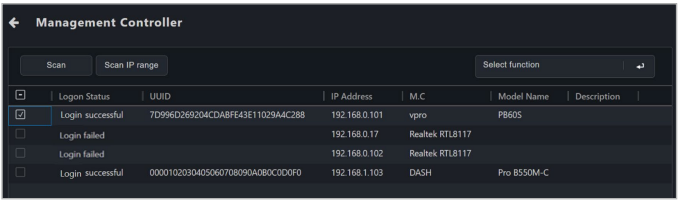


- また、**Device Management Information（デバイス管理情報）**ページの**Account Management（アカウント管理）**から、DASHリモート管理コントローラーを搭載した単一のデバイスのアカウントとパスワードを設定することができます。アカウント管理の詳細については、**5.7.7 アカウント管理** を参照してください。
- 選択されたクライアントデバイスが複数のBMCまたはDASHリモート管理コントローラーのアカウントを持っている場合、**OOB - Control（OOB-制御）**>**Account Management（アカウント管理）**>**Login（ログイン）**でアカウントを切り替えることができます。

5. アカウントやパスワードの設定状況や結果は、ミッションセンターで確認することができます。



6. アカウントとパスワードの設定が完了すると、ASUS Control Center Expressはクライアントデバイスのリモート管理コントローラーにログインします。ログインに成功した場合、**ログイン状態欄**に**ログイン成功**と表示され、クライアントデバイスのリモート管理コントローラーとデバイス名も表示されます。



7. BMCまたはDASHリモート管理コントローラーを搭載したクライアントデバイスでは、**デバイス管理情報**ページでどのアカウントでログインしたかを確認することができます。

単一デバイスの管理制御情報によるアカウントとパスワードの設定

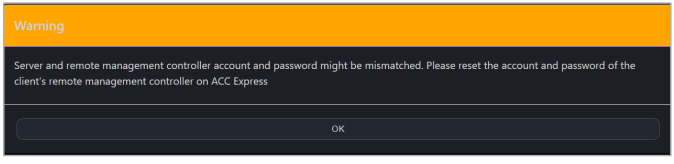
単一クライアントデバイスのASUS Control Center Expressのリモート管理コントローラーログインアカウントを管理制御ページから設定することができます。

リモート管理コントローラを搭載したクライアントデバイスにすでにエージェントが配置されている場合は、メインメニューページのデバイスリストからクライアントデバイスを選択します。RTL8117およびvProの場合は**Select Function（機能の選択）**>**OOB-Control（OOB-制御）**>**Account Management（アカウント管理）**>**Set password（パスワードの設定）**を、BMCおよびDASHの場合は**Select Function（機能の選択）**>**OOB-Control（OOB-制御）**>**Account Management（アカウント管理）**>**Login（ログイン）**をクリックします。

1. 管理制御情報ページに入るには、次のいずれかの方法があります。
   - メインメニューページで、**Management Control Information（マネジメントコントロール情報）**を入力したいデバイスのM.C列 をクリックします。

この方法を使用するには、クライアントデバイスにすでにエージェントが配置されている必要があります。

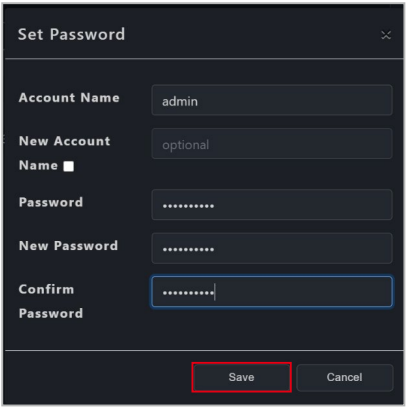
   - をクリックして**Scan（スキャン）**または**Scan IP Range（IP範囲のスキャン）**を実行し、管理制御情報を入力したいデバイスのM.C欄の をクリックすると、そのデバイスの管理制御情報が表示されます。
   - デバイスの**Device Information（デバイス情報）**ページに入り、**Mode（モード）**を**Hardware（ハードウェア）**に切り替えます。
2. ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーへのログインに使用しているログインアカウントとパスワードが一致しない場合は、ポップアップメッセージが表示されます。



3. リモート管理コントローラーの種類によっては、アカウントとパスワードのポップアップウィンドウが異なる場合があります。

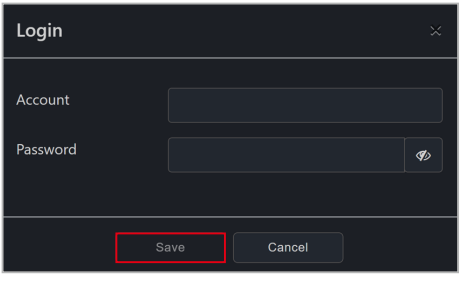
RTL8117/vProの場合

ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーへログインする際に使用するアカウントとパスワードを入力し、**Save（保存）**をクリックします。



BMC/DASHの場合

ASUS Control Center Expressがクライアントデバイスのリモート管理コントローラーへログインする際に使用するアカウントとパスワードを入力し、**Save（保存）**をクリックします。



4. アカウントやパスワードの設定状況や結果は、ミッションセンターで確認することができます。アカウントとパスワードの設定が成功し、アカウントとパスワードが一致した場合、ASUS Control Center Expressは自動的にクライアントデバイスのリモート管理コントローラーにログインし、**OOB - Control**（**OOB-制御**）機能の使用を開始することができます。

- **Device Management Information**（**デバイス管理情報**）ページの**Account Management**（**アカウント管理**）から、DASHリモート管理コントローラーを搭載した単一のデバイスのアカウントとパスワードを設定することができます。アカウント管理の詳細については、**5.7.7 アカウント管理** を参照してください。
- MEBxは、インテルのクライアントデバイス用インテルBIOS拡張オプションおよび設定です。MEBxに設定されているアカウントとパスワードは、インテルvProリモート管理コントローラーのアカウントとパスワードではありません。

- vProアカウントのパスワードは、8文字以上で、大文字（A～Z）1文字、数字（0～9）、特殊文字1文字を含む必要があります。
- RTL8117のパスワードは、8文字以上で、大文字（A～Z）、小文字（a～z）、数字（0～9）を含む必要があります。

5.4.2 OOB-制御機能の使用

OOB-制御機能を使用するには、以下の方法があります。

- OOB-制御機能を実行したいクライアントデバイスを選択してから **Select Function（機能の選択）>OOB-Control（OOB-制御）**を選択し、使用する機能を選択します。
-  をクリックしてスキャンまたはIP範囲のスキャンを実行します。OOB-制御機能を実行したいクライアントデバイスを選択し、機能の選択をクリックして使用する機能を選択します。

各リモート管理コントローラーで利用可能なOOB-制御機能の一覧は、次の表をご覧ください。

機能一覧		BMC	DASH	RTL8117	vPro
Power Control（電源制御）	Power On (G0/S0)	V	V	V	V
	Power Off - Soft (G2/S5)	V	V	V	V
	Power Off - Hard (G3)	V	V	V	
	Power Cycle - Soft off (G2/S5)	V	V	V	V
	Sleep - Deep (G1/S3)		V		V
	Master Bus Reset		V		V
	Hibernate (G1/S4)		V		V
	Restart Computer to BIOS				V
	Power On to BIOS				V
	Restart Computer to IDE-R Floppy				V
	Power On to IDE-R Floppy				V
	Restart Computer to IDE-R CDROM				V
	Power On to IDE-R CDROM				V
	Sleep - Light (G1/S2)		V		
	Power Cycle - Hard Off (G3)	V	V		
	Diagnostic Interrupt (NMI)		V		
	Power Off - Soft Graceful (G2/S5)		V		
	Power Off - Hard Graceful (G3)		V		
	Master Bus Reset Graceful		V		
	Power Cycle (Graceful Soft Off) (G2/S5)		V		
	Power Cycle (Graceful Hard Off) (G3)		V		
WatchDog（ウォッチドッグ）	WatchDog Enable			V	
	WatchDog Disable			V	
BIOS	Smart BIOS- BIOS update management	V		V	
	Smart BIOS - User profile	V			
	Clear CMOS	V		V	
Account Management（アカウントマネージャー）	Set Password			V	V
	Login	V	V		
System（システム）	Restart service				
	Sync OEM port	V			

機能一覧		BMC	DASH	RTL8117	vPro
KVM	KVM Remote Multi-display			V	
	KVM Local Multi-display			V	
	KVM Remote Single-display			V	
	KVM Enable				V
	KVM Disable			V	V
	KVM Password				V
USB Redirection（USBリダイレクト）	USB Redirection		V	V	V
	Enable USB Redirection				V
	Disable USB Redirection				V
Firmware Update（ファームウェア更新）		V		V	
Trust Zone（信頼ゾーン）				V	
Certificate Management（証明書管理）					V
System Trap Alert（システムトラップアラート）	Enable Trap Alert		V		V
	Enable Trap Alert - Info		V		V
	Enable Trap Alert - Warning		V		V
	Enable Trap Alert - Error		V		V
	Disable Trap Alert		V		V
IPMI	IPMI Tool Lanplus Command Redirect	V			
	FRU Info. Write	V			
Settings（設定）		V			
Configuration（構成）		V			
OOB - Control Help（OOB-制御ヘルプ）		V	V	V	V

機能の説明

Power Control（電源制御）	リモート管理コントローラーを介して選択したデバイスの電源操作を実行します。
WatchDog（ウォッチドッグ）	選択したRTL8117デバイスのウォッチドッグを有効または無効にします。
BIOS	Smart BIOS機能を使用するか、選択したデバイスのBMCまたはRTL8117を介してCMOSをクリアします。
Account Management（アカウントマネージャー）	ASUS Control Center Expressが、選択したデバイスのRTL8117、vPro、BMC、DASHリモート管理コントローラーにログインする際に使用するログインアカウントとパスワードを設定します。
System（システム）	BMCに使用するポートを設定するか、選択したデバイスのRTL8117サービスを再起動します。
KVM	RTL8117のKVM表示モード、vPro KVMの有効/無効、選択したデバイスのパスワード設定などを行います。
USB Redirection（USBリダイレクト）	選択したRTL8117、DASH、vProデバイスのUSBリダイレクト機能を使用するか、選択したRTL8117およびvProデバイスのUSBリダイレクト機能を有効または無効にします。
Firmware Update（ファームウェア更新）	選択したデバイスのBMCまたはRTL8117ファームウェアを更新します。
Trust Zone（信頼ゾーン）	クライアントデバイスでのRTL8117機能動作を許可するメインサーバーのIPアドレスを設定します。
Certificate Management（証明書管理）	選択したvProデバイスの証明書を管理します。
System Trap Alert（システムトラップアラート）	システムのトラップアラートレベルを設定したり、DASHやvProデバイスのトラップアラートを有効/無効にします。
IPMI	コマンド リダイレクトの設定、または選択したBMCデバイスのFRUからの情報の書き込みを行います。
Settings（設定）	選択したBMCデバイスの設定を行います。
Configuration（構成）	選択したBMCデバイスの構成設定、バックアップ、復元、工場出荷状態にリセットを行います。
OOB - Control Help（OOB-制御ヘルプ）	選択したデバイスがサポートするOOB機能に関する情報を表示します。

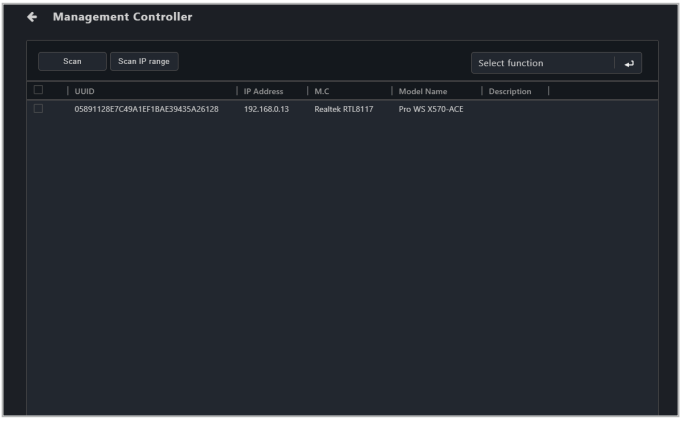
- OOB-制御機能は、BMC、DASH、RTL8117、vProリモート管理コントローラ機能の集合体です。選択したデバイスが、選択したOOB-制御機能をサポートしていない場合、ミッションセンターでアクションの詳細と結果を確認することができます。
- 選択されたOOB-vPro用USBリダイレクト機能をDASHやRTL8117用USBリダイレクト機能と同時に実行できないなど、リモート管理コントローラーの違いにより、制御機能を同時に実行できない場合があります。
- DASHおよびvProのUSBリダイレクト機能は、NTFS形式のUSBデバイスをサポートしていません。
- vProのUSBリダイレクト機能を使用した場合、マウントに成功すると、クライアントデバイスはフロッピーディスクA、CDドライブ（ドライブコード）」を表示します。
- vProデバイスのKVMリモートデスクトップ機能を使用している場合、クライアントデバイスの画面の枠が赤と黄色に点滅し、クライアントデバイスが現在KVMリモートデスクトップ機能を実行していることを示します。
- システムトラップアラートを有効にする前に、ポート162が開いていることを確認してください。
- 通知ルールでは、リモート管理コントローラーの通知を追加・編集することができます。ダッシュボードのイベントログには、設定したシステムトラップアラートの通知が表示されます。

- 複数のクライアントデバイスを選択してアカウントとパスワードを設定する場合は、必ず同じリモート管理コントローラーを持つクライアントデバイスを選択してください。
- KVMパスワードは8文字で、大文字（A～Z）、小文字、数字（0～9）、および特殊文字を含む必要があります。
- クライアントデバイスがリモート管理制御にRTL8117を使用しており、初回使用または工場出荷状態へリセットされた直後の場合は、クライアントデバイスのRT8117が有効になっていることを確認してください。デバイスのBIOSで、**Advanced（詳細）＞ RTL8117 setting（RTL8117設定）**へ移動し、RTL8117を有効にします。
- クライアントデバイスにエージェントが配置されている場合、ASUS Control Center ExpressのBIOS設定機能により、クライアントデバイスのRTL8117管理コントローラを有効にすることもできます。
- KVMが有効な場合、RTL8117リモート管理コントローラのファームウェアを更新することはできません。RTL8117リモート管理コントローラのファームウェアを更新する場合は、KVMを無効にしてから行ってください。

5.5 管理制御の概要

管理制御オプションを使用して、リモート管理コントローラーをサポートするマザーボードを搭載し、管理LANポートを使用して接続されたクライアントデバイスをリモート管理することができます。

右上のメニューバーで をクリックすると**Management Control**（**管理制御**）の画面が開きます。



5.5.1 デバイスのスキャン

Scan（**スキャン**）または**Scan IP Range**（**IP範囲のスキャン**）をクリックすると、管理制御機能をサポートするクライアントデバイスをスキャンすることができます。スキャン結果からデバイスをクリックすると、**Management Control Information**（**管理制御情報**）のページへ移動します。

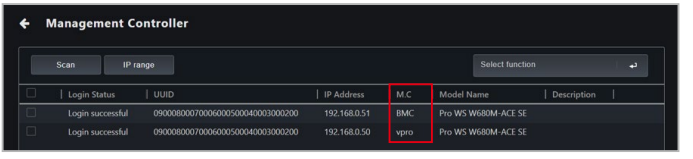
IP範囲のスキャンについては、**3.2.2 IP範囲のスキャン**を参照してください。

5.5.2 複数のリモート管理コントローラーによるデバイスの管理

クライアントデバイスが複数のリモート管理コントローラーをサポートしている場合、ASUS Control Center Expressを使用してリモート管理コントローラーをすばやく切り替えることができます。

Management Control（管理制御）から管理コントローラーを選択

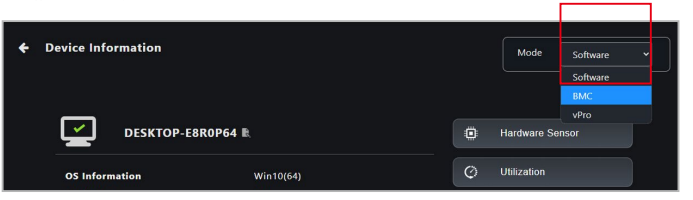
1. メインメニューページで**Management Control（管理制御）**を選択し、**Scan（スキャン）**をクリックします。検出されたリモート管理コントローラーのタイプが**M.C**列に表示されます。
2. 目的のリモート管理コントローラーに対応するエントリーを選択して**Management Control Information（管理制御情報）**ページを開くか、**Select function（機能選択）**をクリックしOOB-制御機能を実行します。



Login Status（ログイン状態）欄に［Login Failure（ログイン失敗）］と表示されている場合は、**5.4.1 リモート管理コントローラーの認証情報の設定** を参照してアカウントとパスワードを設定するか、該当するデバイスのリモート管理コントローラーにログインしてください。

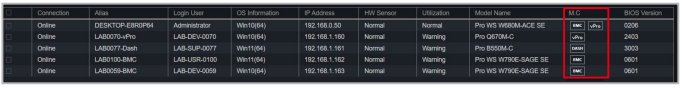
Device Information（デバイス情報）から管理コントローラーを選択

デバイスリストからデバイスを選択して**Device Information（デバイス情報）**画面を開き、**Mode**ドロップダウンメニューから目的のリモート管理コントローラーを選択します。



デバイスリストから管理コントローラーを選択

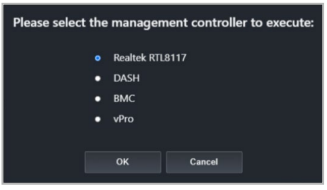
デバイスリストの**M.C**列で目的のリモート管理コントローラーのアイコンをクリックするか、**Select function（機能選択）**をクリックしてOOB-制御機能を実行します。



vProリモート管理コントローラーのIPアドレスが変更されている場合、vProアイコンが表示されない場合があります。vPro IPアドレスを更新するには、**Device Information（デバイス情報）> Control（制御）> Set Management Controller（管理コントローラー設定）**をクリックし、デバイスを再起動します。

オフラインデバイスのリモート管理コントローラーを選択

デバイスリストからデバイスを選択して**Device Information（デバイス情報）**画面を開き、必要な機能と管理コントローラーを選択します。



- ハードウェアセンサーには、BMC、DASH、RTL8117 コントローラーが必要です。
- USBリダイレクトには、DASH、RTL8117、vPro コントローラーが必要です。
- 電源制御には、vPro コントローラーが必要です。
- リモートデスクトップには、BMC、RTL8117、vPro コントローラーが必要です。

5.6 管理制御情報の概要

Management Control Information（管理制御情報）には選択したクライアントデバイスの詳細情報が表示されます。また、オペレーティングシステムがインストールされていないデバイスの電源制御オプションなど、ハードウェアで制御される管理機能も提供します。

DASH、vPro、RTL8117、BMCの管理制御情報は、それぞれ異なる場合があります。

- DASHについては、**5.7 DASH管理制御情報** を参照してください。
- RTL8117については、**5.8 RTL8117管理制御情報** を参照してください。
- vProについては、**5.9 vPro管理制御情報** を参照してください。
- BMCについては、**5.10 BMC管理制御情報**を参照してください。

次の方法で、クライアントデバイスの**Management Control Information（管理制御情報）**へアクセスすることができます。

- クラシックビュー：デバイス一覧でクライアントデバイスをクリックし、続いて**Mode（モード）**ドロップダウンメニューで**Hardware（ハードウェア）**を選択します。または、デバイスリストのM.C列の をクリックしてください。
- グラフィックビュー：クライアントデバイスのショートカットアイコンをダブルクリックし、続いて**Mode（モード）**ドロップダウンメニューで**Hardware（ハードウェア）**を選択します。
- 管理制御：**Management Control（管理制御）**画面のスキャン結果でクライアントデバイスをクリックします。

- 一部の機能は、クライアントデバイスがオンライン状態にあり、オペレーティングシステムへログインされた状態でのみ使用することができます。
- **Management Control（管理制御）**を介して**Management Control Information（管理制御情報）**ページへアクセスした場合は、**Hardware（ハードウェア）**モードと**Software（ソフトウェア）**モードを切り替えることはできません。または、メインメニューページのデバイスリストのM.C欄にある をクリックします。
- 本章では**Hardware Mode（ハードウェアモード）**の機能のみを説明しています。**Software Mode（ソフトウェアモード）**の機能に関しては、**4章 デバイス情報**を参照してください。

管理制御情報には、マザーボード上のリモート管理コントローラーのサポートが必要です。

5.7 DASH管理制御情報

DASH管理制御情報では、クライアントデバイスがオフラインのときに、ハードウェアの状態の監視、リモート電源制御、USBリダイレクト、コンソールリダイレクト、またはハードウェア資産の表示を行うことができます。

この機能はハードウェアによって制御されており、表示される値はソフトウェアのバージョンによって異なる場合があります。ソフトウェアモードの詳細は、4章を参照してください。

クライアントデバイスがDASHリモート管理コントローラーに対応しており、クライアントデバイスのBIOS設定でDASH機能が有効になっている必要があります。

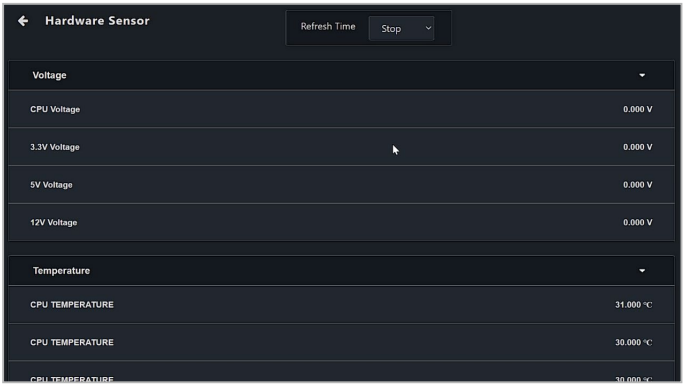
* 管理制御を介して管理制御情報ページへアクセスした場合は、この機能は利用できません。

Device icon（デバイスアイコン）	クライアントデバイスのDASHリモート管理コントローラーの接続状態を表示します。
Login user（ログインユーザー）	クライアントデバイスのDASHリモート管理コントローラーに現在ログインしているユーザーアカウントを表示します。ログインユーザーを切り替えることができます。
Login Status（ログイン状態）	クライアントデバイスのDASHリモート管理コントローラーへの現在のログイン状態を表示します。

Management Controller（管理コントローラー）	クライアントデバイスのリモート管理コントローラーを表示します。
Model Name（モデル名）	クライアントデバイスのモデル名を表示します。
IP Address（IPアドレス）	クライアントデバイスのIPアドレスを表示します。
Profile versions（プロファイルバージョン）	クライアントデバイスのDASHのさまざまなプロファイルバージョン情報を表示します。この情報は、クライアントデバイスのDASHリモート管理コントローラーの対応状況によって異なる場合があります。

5.7.1 ハードウェアセンサー

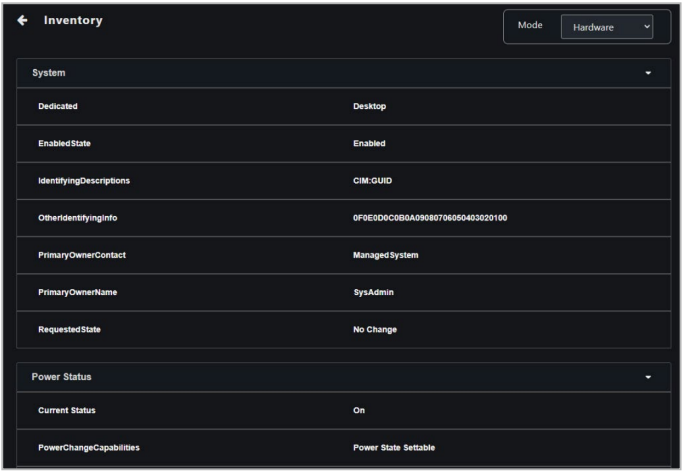
クライアントDASHデバイスの電圧、温度、ファン回転数の情報を見ることができます。



Refresh Time（更新タイム）	ハードウェアセンサーの更新時間間隔を設定します。
Voltage（電圧）	デバイスハードウェアの電圧を表示します。
Temperature（温度）	デバイスハードウェアの温度を表示します。
Fan（ファン）	デバイスハードウェアのファン回転数を表示します。

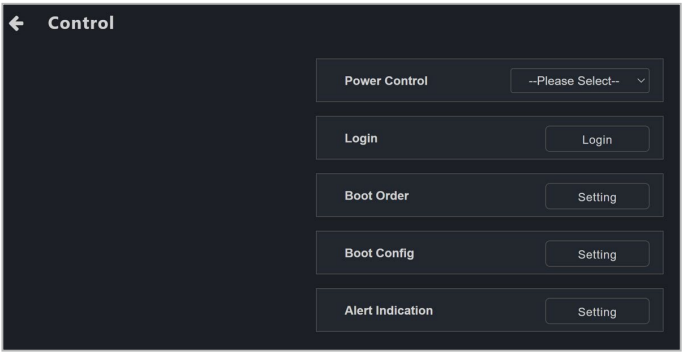
5.7.2 インベントリ

システムの製品、モデル、CPUバージョン、BIOSバージョン、メモリーなどのハードウェア情報を確認することができます。



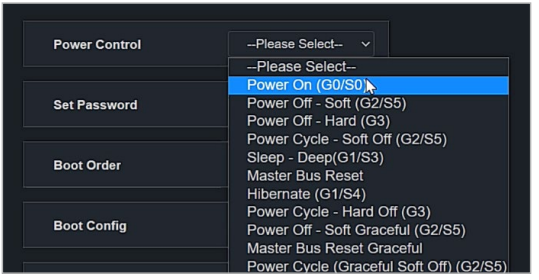
5.7.3 制御

クライアントDASHデバイスのパスワードを設定・変更したり、電源制御の操作を行うことができます。



電源管理

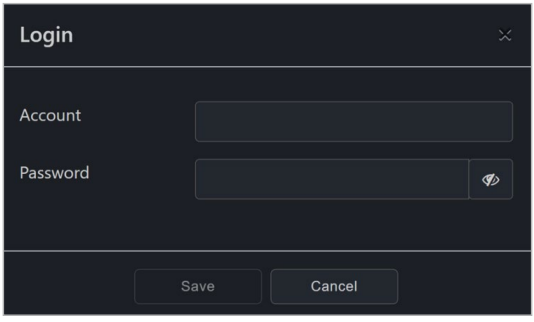
システムの再起動など、DASHリモート管理コントローラーを介してクライアントデバイスの電源制御機能をリモートで実行することができます。



Power On（電源オン）（G0/S0）	DASHリモート管理コントローラーを介してクライアントデバイスの電源をオンにします。
Power Off - Soft（電源オフ-ソフト）（G2/S5）	DASHリモート管理コントローラーを介してクライアントデバイスの電源をオフにします。
Power Off - Hard（電源オフ-ハード）(G3)	DASHリモート管理コントローラーを介してオペレーティングシステムが応答しないときにクライアントデバイスの電源を強制的にオフにします。
Power Cycle - Soft off（電源サイクル-ソフトオフ）（G2/S5）	DASHリモート管理コントローラーを介してオペレーティングシステムからシャットダウンした後、クライアントデバイスを再起動します。
Sleep - Deep（スリープ-ディープ）（G1/S3）	DASHリモート管理コントローラーを介してクライアントデバイスをスリープモード（G1/S3）に設定します。
Master Bus Reset（マスターバスリセット）	DASHリモート管理コントローラーを介してクライアントデバイスのハードウェアをリセットします。
Hibernate（休止状態）（G1/S4）	DASHリモート管理コントローラーを介してクライアントデバイスを休止状態（G1/S4）に設定します。
Power Cycle - Hard Off（電源サイクル-ハードオフ）(G3)	DASHリモート管理コントローラーを介してクライアントデバイスの電源をオフにしてから再起動します。
Power Off - Soft Graceful（電源オフ-ソフトグレースフル）（G2/S5）	DASHリモート管理コントローラーを介してクライアントデバイスをオペレーティングシステム経由で通常シャットダウンします。
Master Bus Reset Graceful（マスターバスリセットグレースフル）	DASHリモート管理コントローラーを介してクライアントデバイスのハードウェアを通常シャットダウンしてから再設定します。
Power Cycle (Graceful Soft Off)（電源サイクル（グレースフルソフトオフ））（G2/S5）	DASHリモート管理コントローラーを介してクライアントデバイスをオペレーティングシステム経由で通常シャットダウンします。

ログイン

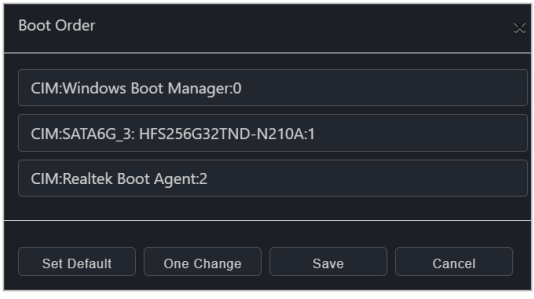
ASUS Control Center Expressがクライアントデバイスの DASHリモート管理コントローラーにログインする際に使用するアカウントとパスワードを設定することができます。ログインに成功すると、DASHリモート管理コントローラーは自動的に新しくログインしたアカウントに切り替わります。



ブート順

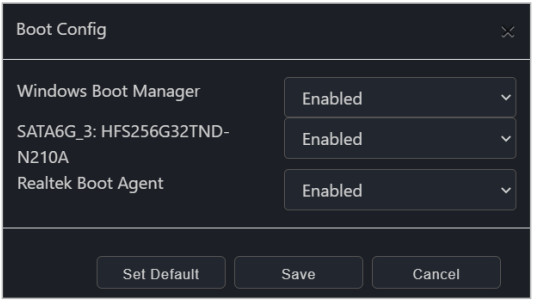
DASHリモート管理コントローラーを使って、クライアントデバイスのブート順序を設定することができます。

順番を調整したい項目を左クリックしたまま、上下にドラッグしてブート順を再調整することができます。



ブート設定

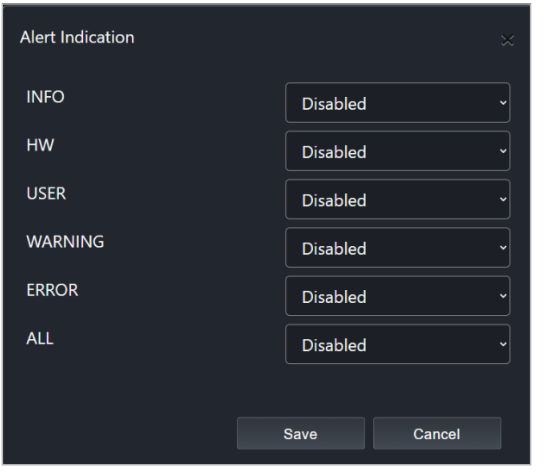
DASHリモート管理コントローラーを使って、クライアントデバイスのブート設定を行うことができます。



アラート表示

クライアントデバイスのDASHプラットフォームイベントアラート表示を設定することができます。

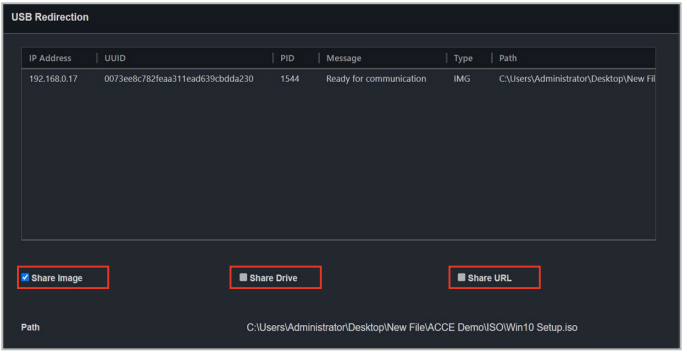
- 設定できるアラート表示のカテゴリーは、クライアントデバイスのDASHリモート管理コントローラーの対応状況によって異なる場合があります。
- リモート管理コントローラの通知ルールは、**Rule Management（ルール管理）**から追加または編集することができます。**Rule Management（ルール管理）**の詳細については、**8.1.2 ルール管理**を参照してください。ルールが設定されると、ダッシュボードのイベントログにイベントログが表示されます。



5.7.4 USBリダイレクト

USBストレージデバイスやクライアントDASHデバイスのイメージファイルをリダイレクトすることができます。

- USBリダイレクト機能を使用する前に、クライアントデバイスでUSBストレージデバイス機能が有効になっていることを確認してください。
- DASHのUSBリダイレクト機能は、NTFS形式のUSBデバイスには対応していません。



USB and device information（USBとデバイス情報）	USBリダイレクトリストには、USBが接続されているデバイスのIPアドレスとその他の情報が表示されます。
Share Image（イメージの共有）	クライアントデバイスにマウントしたいイメージファイルを選択します。
Share Drive（ドライブの共有）	メインサーバーに接続されたUSBストレージデバイスへクライアントデバイスがアクセスできるようにします。
Share URL（URLの共有）	クライアントデバイスへマウントするパス、リンク、イメージをコピーして貼り付けます。
Image Path（イメージパス）	リダイレクトされたUSBデバイスまたはイメージファイルのパスです。

イメージの共有

イメージファイルを共有することができます。

1. **Share Image（イメージの共有）**をチェックします。
2. マウントしたいイメージファイルを選択し、ファイルピッカーウィンドウの**Mount（マウント）**をクリックします。
3. イメージファイルのマウントに成功すると、**Ready for communication（通信準備が整いました）**、と**Message（メッセージ）**欄に表示されます。

ドライブの共有

USBストレージデバイスを共有します。

1. **Share Drive**（**ドライブの共有**）を確認し、リモートデバイスのUSB機能が有効になっていることを確認します。
2. マウントしたいUSBストレージデバイスを選択します。
3. USBストレージのマウントに成功すると、**Message**（**メッセージ**）欄に**Ready for communication**（**通信準備完了**）と表示されます。

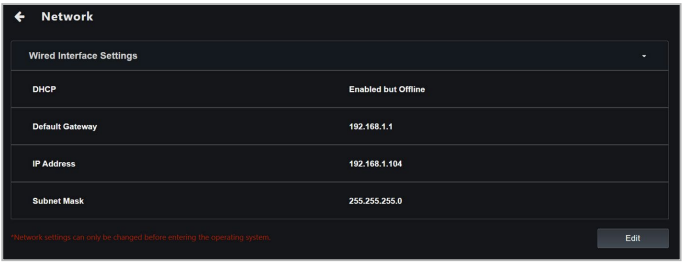
URLの共有

イメージファイルのURLを共有することができます。

1. **URLの共有**をチェックします。
2. イメージファイルのURLを入力して、マウントをクリックします。
3. イメージファイルのマウントに成功した場合、**Message**（**メッセージ**）欄に**Ready for communication**（**通信準備完了**）と表示されます。

5.7.5 ネットワーク

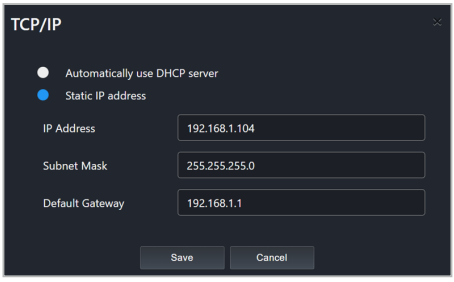
クライアントDASHデバイスの有線/無線ネットワークの設定を行います。



DHCP	DHCP（Dynamic Host Configuration Protocol）の状態を表示します。
Default Gateway（デフォルトゲートウェイ）	デフォルトゲートウェイを表示します。
IP Address（IPアドレス）	IPアドレスを表示します。
Subnet Mask（サブネットマスク）	サブネットマスクを表示します。

ネットワーク設定

ネットワークの設定は、クライアントデバイスがオペレーティングシステムを起動していない場合にのみ行うことができます。クライアントデバイスがオペレーティングシステムを起動している場合、ネットワーク設定は表示のみで設定を行うことはできません。

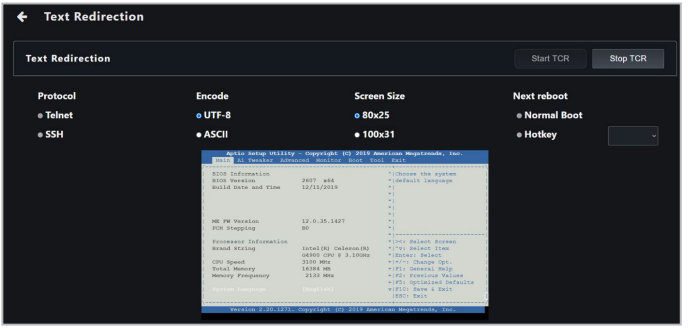


Client IP（クライアントIP）	クライアントデバイスのIPに**Static IP address（静的IPアドレス）**を使用するか、**Automatically use DHCP server（DHCPサーバーを自動的に使用）**を使用するかを選択します。
IP Address（IPアドレス）	IPアドレスを設定することができます。
Subnet Mask（サブネットマスク）	サブネットマスクを設定することができます。
Default Gateway（デフォルトゲートウェイ）	デフォルトゲートウェイを設定することができます。

5.7.6 テキストリダイレクト

BIOS設定を介してクライアントDASHデバイスのキーボードやコンソールをリダイレクトすることができます。

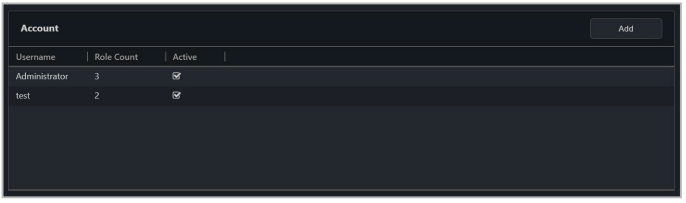
テキストリダイレクト機能を使用する前に、クライアントデバイスのBIOSで、シリアルポートコンソールリダイレクト接続用のCOMポート設定を完了してください。



Protocol（プロトコル）	接続方法をTelnetまたはSSHから選択します。
Encode（エンコード）	文字の暗号化をUTF-8またはASCIIから選択します。
Screen Size（画面サイズ）	コンソールの解像度を選択します。
Next Reboot（次回の再起動）	次回の再起動時に通常の起動を行うか、電源投入時にホットキーを設定するかを選択します。

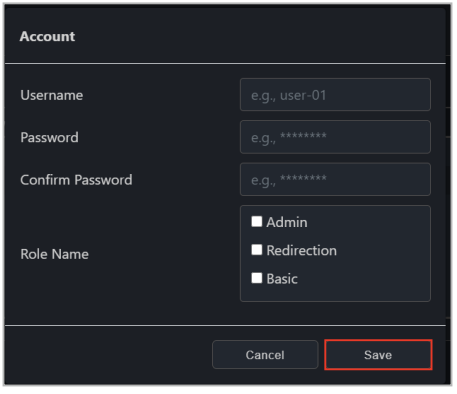
5.7.7 アカウント管理

DASHリモート管理コントローラーのアカウントの追加、削除、有効化、無効化をすることができます。



新規アカウントの追加

1. **Add（追加）**をクリックします。
2. 新しいアカウントの情報を入力し、**Save（保存）**をクリックします。



Username（ユーザー名）	ユーザー名を入力します。
Password（パスワード）	パスワードを入力します。
Confirm Password（パスワードの確認）	パスワードを再入力します。
Role Name（役割名）	アカウントの役割を選択します。

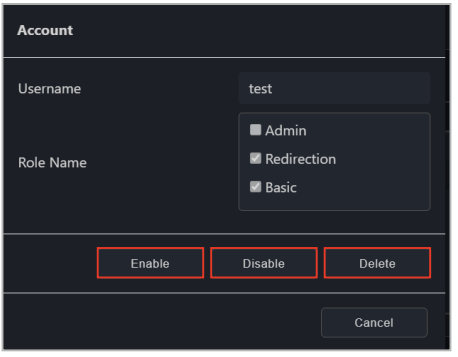
DASHリモート管理コントローラーのアカウントとパスワードは、最大15文字まで設定することができます。

アカウントとパスワードを設定すると、ASUS Control Center Expressはクライアントデバイスのリモート管理コントローラーにログインします。ログインに成功した場合は、**管理コントローラー情報**ページの**ログイン状態**にログイン成功と表示されます。

新規アカウントの有効化・無効化・削除

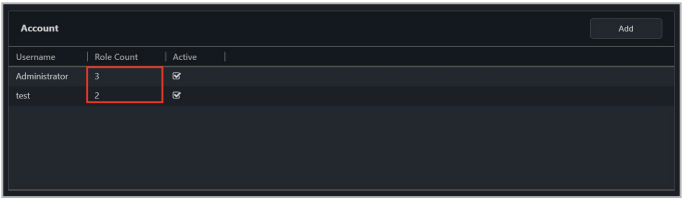
削除できるのは新しく追加されたアカウントのみです。デフォルトの管理者アカウントは編集のみ可能で、削除はできません。

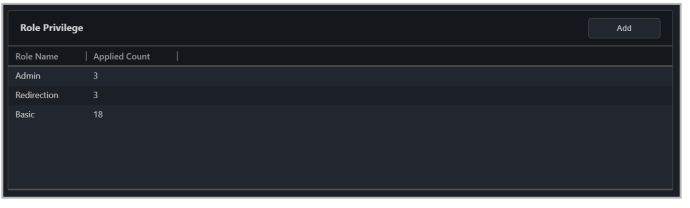
1. アカウントリストから有効化、無効化、削除したいアカウントをクリックします。
2. **Enable（有効）**、**Disable（無効）**、**Delete（削除）**のいずれかをクリックします。
3. アクションの結果（**有効、無効、削除**）はミッションセンターで確認することができます。



5.7.8 役割権限

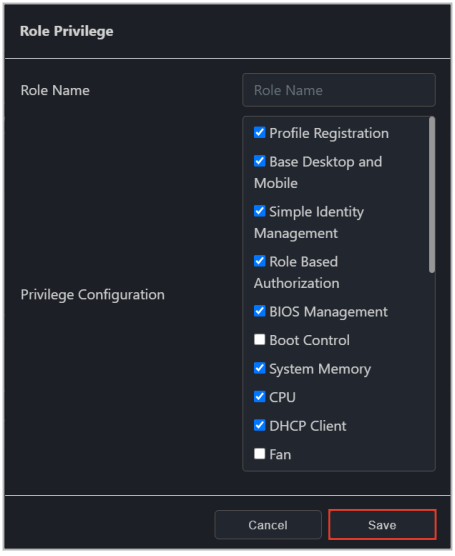
DASHアカウントの役割権限を管理します。役割権限にアクセスするには、役割権限を管理したいアカウントの**Role Count（役割数）**をクリックします。





新規役割の追加

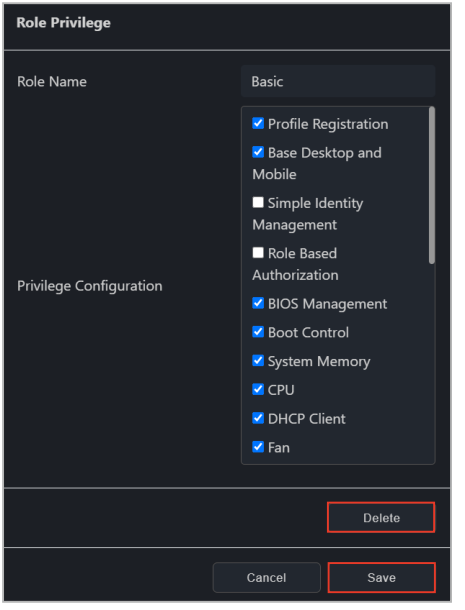
1. **Role privileges（役割権限）**ページの右上にある**Add（追加）**をクリックします。
2. **Role Name（役割名）**を入力します。
3. **Privilege Configuration（権限設定）**リストから、新規役割が持つ権限を確認します。
4. 完了したら、**Save（保存）**をクリックします。



役割の編集・削除

削除できるのは、新しく追加された役割のみです。デフォルトの管理者役割は、編集のみ可能で、削除はできません。

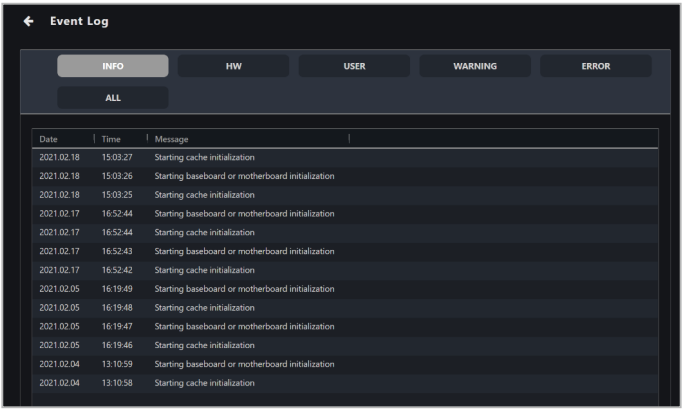
1. 編集または削除したい役割をクリックします。
2. 役割名や役割権限を編集したり、**Delete（削除）**をクリックして役割を削除することができます。
3. 役割の編集を選択した場合は、完了したら**Save（保存）**をクリックします。



5.7.9 イベントログ

クライアントDASHデバイスのシステム上の問題や不具合を確認することができます。

- 表示されるイベントカテゴリーは、DASHリモート管理コントローラーの対応状況によって異なります。
- リモート管理コントローラーの通知ルールは、**Rule Management（ルール管理）**から追加・編集することができます。ルール管理の詳細については、**8.1.2 ルール管理**を参照してください。ルールが設定されると、ダッシュボードのイベントログにイベントログが表示されます。



5.8 RTL8117 管理制御情報

RTL8117管理制御情報は、クライアントデバイスにオペレーティングシステムがインストールされていない場合や、クライアントデバイスのオペレーティングシステムに入れない場合に、RTL8117リモート管理コントローラを使ってハードウェアの状態を監視したり、機能を実行することができます。

この機能はハードウェアによって制御されており、表示される値はソフトウェアのバージョンによって異なる場合があります。ソフトウェアモードの詳細は、4章を参照してください。

- クライアントデバイスがRTL 8117リモート管理コントローラーに対応している必要があります。
- 新規デバイスで初めて使用する場合や、工場出荷時の設定にリセットされている場合は、クライアントデバイスのRTL8117が有効になっていることを確認してください。デバイスのBIOSで、**Advanced（詳細）＞ RTL8117 setting（RTL8117設定）**へ移動し、RTL8117を有効にします。

* 管理制御を介して管理制御情報ページへアクセスした場合は、この機能は利用できません。

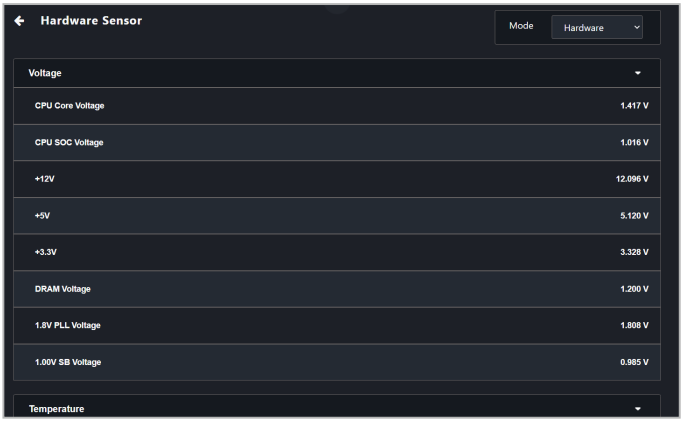
Machine Name（コンピューター名）	コンピューター名を表示します。 をクリックするとコンピューター名を編集できます（最大32文字）。
Device icon（デバイスアイコン）	デバイスのイベントログを表示します。
Login User（ログインユーザー）	クライアントデバイスのRTL 8117リモート管理コントローラーに現在ログインしているユーザーアカウントを表示します。

Login Status（ログイン状態）	クライアントデバイスのRTL 8117リモート管理コントローラーへの現在のログインステータスを表示します。
Management Controller（管理コントローラー）	クライアントデバイスのリモート管理コントローラーを表示します。
Model Name（モデル名）	クライアントデバイスのモデル名を表示します。
Up Time（稼働時間）	前のセッションのクライアントデバイスの稼働時間を表示します。
Firmware Version（ファームウェアバージョン）	クライアントデバイスのRTL8117リモート管理コントローラーのファームウェアバージョンを表示します。
Kernel Version（カーネルバージョン）	クライアントデバイスのRTL8117リモート管理コントローラーのカーネルバージョンを表示します。
U-Boot Version（U-Bootバージョン）	クライアントデバイスのRTL8117リモート管理コントローラーのU-Bootバージョンを表示します。

5.8.1 ハードウェアセンサー

クライアントデバイスの前回電源投入時の電圧、温度、ファン回転数などのしきい値を表示します。

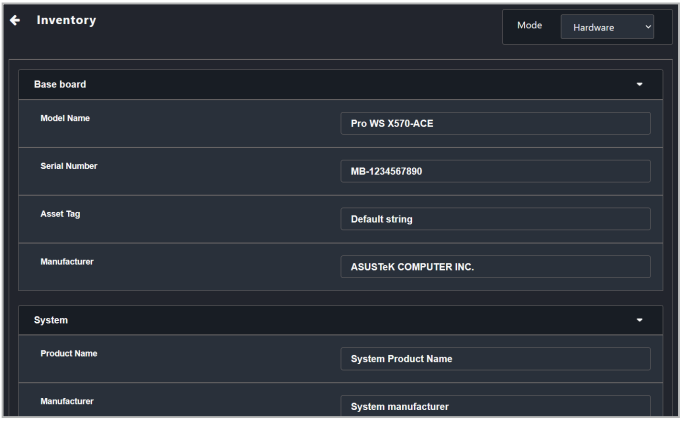
RTL8117ハードウェアセンサーは、クライアントデバイスの電源投入プロセス中（クライアントデバイスの再起動時）にのみデータを更新します。



Voltage（電圧）	デバイスハードウェアの電圧を表示します。
Temperature（温度）	デバイスハードウェアの温度を表示します。
Fan（ファン）	デバイスハードウェアのファン回転数を表示します。

5.8.2 インベントリ

クライアントデバイスの前回電源投入時のハードウェアの詳細情報を表示します。

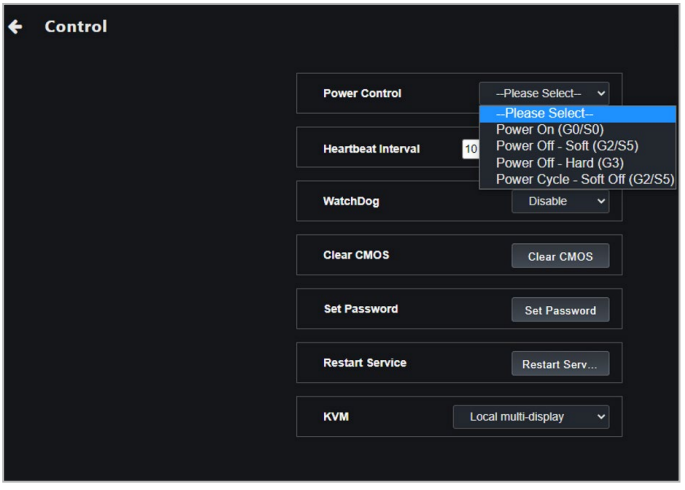


Base board（ベース基板）	マザーボードのモデル名、シリアル番号、アセットタグ、製造元情報を表示します。
System（システム）	製品名と製造元情報を表示します。
Memory（メモリー）	メモリーロケーションと容量を表示します。
BIOS	BIOSのリリース日、バージョン、製造元情報を表示します。
Processor（プロセッサー）	プロセッサー名とクロック情報を表示します。

5.8.3 制御

クライアントデバイスにオペレーティングシステムがインストールされていない場合や、オペレーティングシステムを起動できない場合に、ハードウェアレベルの機能を管理・制御することができます。

一部の機能は、クライアントデバイスを再起動した後に有効になります。



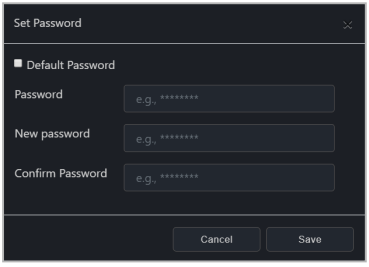
Power On（電源オン）（G0/S0）	RTL8117リモート管理コントローラーを介してクライアントデバイスの電源をオンにします。
Power Off - Soft（電源オフ-ソフト）（G2/S5）	DASHリモート管理コントローラーを介してクライアントデバイスの電源をオフにします。
Power Off - Hard（電源オフ-ハード）(G3)	DASHリモート管理コントローラーを介してオペレーティングシステムが応答しないときにクライアントデバイスの電源を強制的にオフにします。
Power Cycle - Soft off（電源サイクル-ソフトオフ）(G2/S5)	DASHリモート管理コントローラーを介してオペレーティングシステムからシャットダウンした後、クライアントデバイスを再起動します。
Heartbeat Interval（ハートビートの間隔）*	ハードウェア信号を確認する間隔を秒単位で設定します。

Watchdog（ウォッチドッグ）*	ウォッチドッグ監視機能を有効または無効にします。  ウォッチドッグ機能が有効になり、ウォッチドッグを通じてトリガーされたクライアントデバイスが再起動した場合、ウォッチドッグはデフォルトの無効状態へ戻ります。クライアントデバイスのウォッチドッグを再度有効にしてください。
Clear CMOS（CMOSの消去）	オーバークロックやその他のエラーでクライアントがハングアップした場合、RTL8117を介してBIOSの設定情報を消去します。  CMOSを消去する前に、クライアントデバイスの電源が完全にオフになっていることを確認してください。CMOSを消去した後にクライアントデバイスの電源をオンにします。
Set password（パスワードの設定）	RTL8117暗号化パスワードを設定します。  新しいパスワードの設定が完了したら、変更を有効にするためにクライアントデバイスを再起動してください。
Restart Service（サービスの再起動）	RTL8117を介してサービスを再起動します。
KVM	KVMを有効/無効にします。

*** これらの機能は、エージェントが既にデバイスへ配置され、ソフトウェアモードからハードウェアモードへ切り替えた場合にのみ表示されます。**

RTL8117のパスワード設定

RTL8117の暗号化パスワードは、**Set Password（パスワードの設定）**機能で設定することができます。



Default Password（デフォルトパスワード）	この項目をチェックすると、予め設定されたパスワードを**Password（パスワード）**欄に読み込むことができます。RTL8117パスワードがまだ設定されていない場合は、**Default Password（デフォルトパスワード）**を選択するとシステムのデフォルトパスワードが読み込まれます。
Password（パスワード）	現在のパスワードを入力するか、**Default Password（デフォルトのパスワード）**をチェックして、予め設定されたパスワードを読み込むことができます。
New Password（新しいパスワード）	新しいパスワードを入力します。
Confirm Password（パスワードの確認）	パスワードを再入力します。

- パスワードは8文字以上で、大文字、小文字、数字のみで構成される必要があります。
- 新しいパスワードの設定が完了したら、変更を有効にするためにクライアントデバイスを再起動してください。

5.8.4 リモートデスクトップ

リモートデスクトップ機能は、ASUS Control Center Expressでアクセスするデスクトップを介して、柔軟なアウトオブバンドデバイス管理のインターフェースを提供します。このリモートデスクトップ機能を使用して、クライアントデバイスがBIOSなどのオペレーティングシステム環境を開けない場合でも、デバイスを制御することができます。

- このリモート制御方法では、クライアントデバイスのKVMが有効に設定されており、RTL8117 LAN ICに対応する管理LANポートを使用して接続されている必要があります。
- メインサーバーは現在のKVM状態を保存します。この状態が変更された場合は、システムを再起動して変更内容を保存してください。

リモートデスクトップを使用する前にKVMをセットアップする

アウトオブバンド管理リモートデスクトップ機能を使用する前に、KVMを有効にし、KVM表示モードを選択してください。

1. メインダッシュボードの概要でアウトオブバンド管理リモートデスクトップを使用するデバイスを選択し、**Select function（機能の選択） > OOB-Control（OOB-制御） > KVM > KVM Enable（KVM有効化）**をクリックしてKVMを有効にします。

KVMを無効にする場合は、**Select function（機能の選択） > OOB-Control（OOB-制御） > KVM > KVM Disable（KVM無効化）**をクリックしてKVMを無効にし、クライアントデバイスを再起動します。

2. 次に、**Select function（機能の選択） > OOB-Control（OOB-制御） > KVM**をクリックして**KVM Display Mode（KVM表示モード）**を選択します。詳細は次の表をご参照ください。

Remote Mulit-Display（リモートマルチディスプレイ）	BIOS画面はサーバーのリモートデスクトップとクライアントデバイスの両方で表示されます。 オペレーティングシステム画面はサーバーのリモートデスクトップでのみ表示されます。
Local Multi-Display（ローカルマルチディスプレイ）	BIOS画面はサーバーのリモートデスクトップとクライアントデバイスの両方で表示されます。 オペレーティングシステム画面はクライアントデバイスでのみ表示されます。
Remote Single-Display（リモートシングルディスプレイ）	BIOSとオペレーティングシステムの画面はサーバーのリモートデスクトップでのみ表示されます。
Disable（無効）	BIOSとオペレーティングシステムの画面はクライアントデバイスでのみ表示されます。

3. クライアントデバイスを再起動してBIOS Setup Utilityを起動し、**Advanced（詳細）> RTL8117 setting（RTL8117設定）**へ進み、**RTL8117 Manager Controller（RTL8117管理コントローラー）**を**[Enabled]（有効）**に設定します。

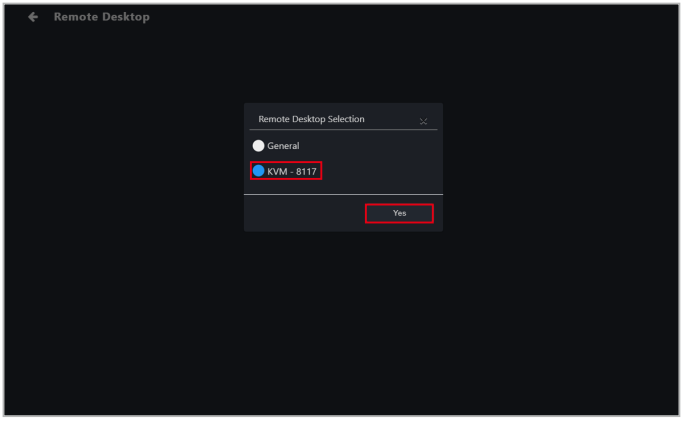
BIOS設定はクライアントデバイスに応じて異なる場合があります。BIOS設定の詳細は、クライアントデバイスのマザーボードのユーザーガイドを参照してください。

4. **KVM Display Mode（KVM表示モード）**機能のドロップダウンメニューをクリックし、手順2で選択したものと同じディスプレイモードを選択します。

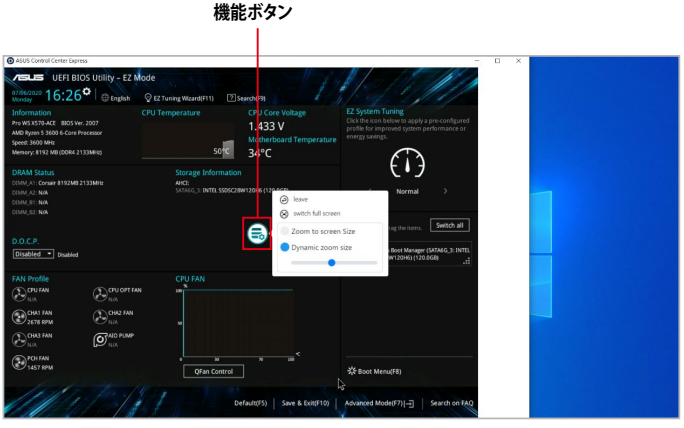
アウトオブバンド管理リモートデスクトップの使用

RTL8117デバイスの管理制御情報ページで、リモートデスクトップをクリックします。**KVM - 8117**を選択して**Yes（はい）**をクリックし、クライアントデバイスがオペレーティングシステム環境を開けない場合でもリモートで制御できるようにします。

- **Management Control（管理制御）**をクリックし、クライアントデバイスの**Management Control Informatio（管理制御情報）**からクライアントデバイスをクリックして**Remote Desktop（リモートデスクトップ）**にアクセスした場合、**Remote Desktop（リモートデスクトップ）**は自動的にKVM - 8117モードになります。
- KVMリモートデスクトップは、ハードウェアモードの機能です。KVMリモートデスクトップとソフトウェアモードリモートデスクトップでは、機能が異なる場合があります。



機能ボタンをクリックすると、リモートデスクトップ画面を操作するためのオプションが表示されます。



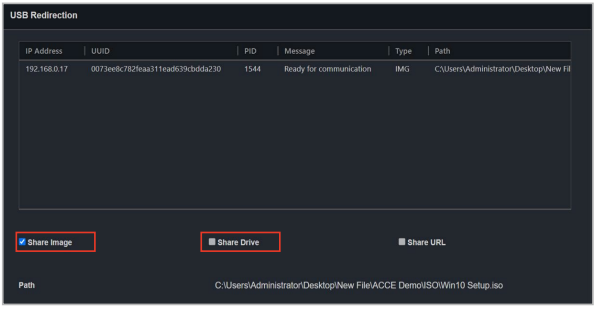
	Leave（退出）	:前のオプションに戻ります。
	Display remote mouse cursor（リモートマウスカーソル表示）	:クライアントにマウスが接続されていない場合、リモート画面ではマウスカーソルを使用できない場合があります。ここをクリックすれば、リモートデスクトップ画面にリモートのマウスカーソルが表示されます。
	Leave（退出）	:前のオプションに戻ります。
	Switch full screen（フルスクリーン表示）	:リモートデスクトップ画面をスクリーン全体へ拡大します。
	Zoom to screen size（画面サイズへズーム）	:リモートデスクトップ画面を中央に配置します。
	Dynamic zoom size（ダイナミックズーム）	:水平方向のスライドバーを使用してズームイン/ズームアウトします。

: リモート制御セッションを終了します。

5.8.5 USBリダイレクト

USBリダイレクト機能を使用して、メインサーバーへ接続されたUSBドライブをクライアントデバイスから読み取ることができます。これは、USBデバイスを使用してクライアントデバイスを起動する必要があったり、メインサーバーへ接続されたUSBを遠隔地からアクセスする必要がある場合に便利です。

- この機能は、RTL 8117 LAN に対応した管理LANポートを使用してクライアントデバイスが接続されている場合のみ使用できます。
- USBリダイレクト機能を使用する前に、クライアントデバイスでUSBストレージデバイス機能が有効になっていることを確認してください。
- RTL8117のUSBリダイレクト機能は、**Share URL（URLの共有）**機能に対応していません。



USB and device information（USBとデバイス情報）	USBリダイレクトリストには、USBが接続されているデバイスのIPアドレスやその他の情報が表示されます。
Share Image（イメージの共有）	クライアントデバイスにマウントしたいイメージファイルを選択します。
Share a local drive（ローカルドライブの共有）	メインサーバーへ接続されたUSBストレージデバイスへクライアントデバイスがアクセスできるようにします。
Share URL（URLの共有）	クライアントデバイスにマウントするイメージファイルへのパスまたはリンクをコピーします。
Image Path（イメージパス）	リダイレクトされたUSBデバイスまたはイメージファイルのパスです。

Share Image（イメージの共有）

イメージファイルを共有することができます。

1. **Share Image（イメージの共有）**をチェックします。
2. マウントしたいイメージファイルを選択し、ファイルピッカーウィンドウの **Mount（マウント）**をクリックします。
3. イメージファイルのマウントに成功すると、**Message（メッセージ）**欄に **Ready for communication（通信準備完了）**と表示されます。

Share Drive（ドライブの共有）

USBストレージデバイスを共有します。

1. **Share Drive（ドライブの共有）**をチェックし、リモートデバイスのUSB機能が有効になっていることを確認します。
2. マウントしたいUSBストレージデバイスを選択します。
3. USBストレージデバイスのマウントに成功すると、**Message（メッセージ）**欄に**Ready for communication（通信準備完了）**と表示されます。

5.8.6 Smart BIOS（スマートBIOS）

Smart BIOS（スマートBIOS）機能では、BIOSファイルを手動でアップロードしたり、デバイスの電源を入れてBIOSの更新や修復を実行できない場合にBIOSキャッシュからアップロードして、デバイスのBIOSを更新することができます。

クライアントデバイスは、シャットダウン後にBIOSの更新を開始します。更新に時間がかかる場合がありますので、更新が終了するまでお待ちください。BIOSフラッシュが終了すると、クライアントデバイスが再起動します。

BIOSフラッシュ中は、絶対に電源を切らないでください。

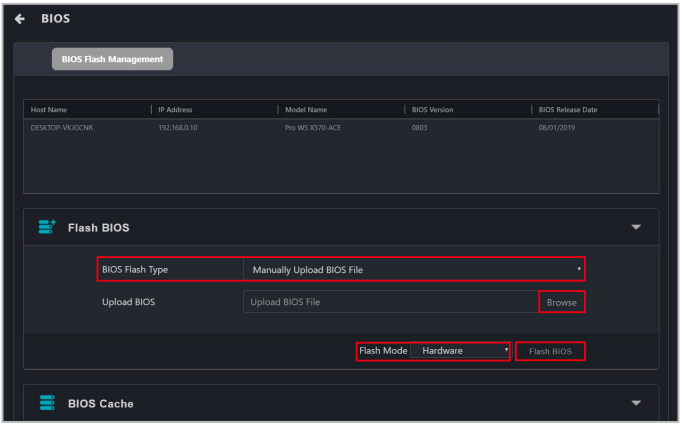
BIOSファイルを手動でアップロードしてBIOSをフラッシュ

BIOSファイルを手動でアップロードして、クライアントデバイスのBIOSをフラッシュします。アップロードされフラッシュされたBIOSファイルはBIOSキャッシュへ追加されます。

1. **BIOS Flash Type（BIOSのフラッシュタイプ）**欄から**Manually Upload BIOS File（BIOSファイルを手動でアップロード）**を選択します。
2. **Browse（参照）**をクリックしてBIOSファイルを選択し、続いて**OK**をクリックして、BIOSファイルが正常にアップロードされたことを確認します。アップロードされたBIOSファイルは**BIOS Cache（BIOSキャッシュ）**にも追加されます。

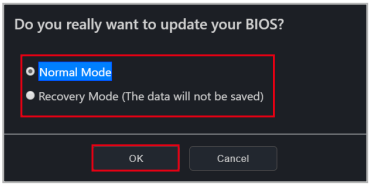
3. **Flash BIOS（BIOSのフラッシュ）**をクリックします。

Flash Mode（フラッシュモード）の既定値は**Hardware Mode（ハードウェアモード）**です。



4. **Normal Mode（通常モード）**または**Recovery Mode（回復モード）**でBIOSをフラッシュするかを選択し、**OK**をクリックします。

Recovery Mode（回復モード）でBIOSをフラッシュすると、すべてのBIOS設定がリセットされ、以前の設定内容が削除されます。

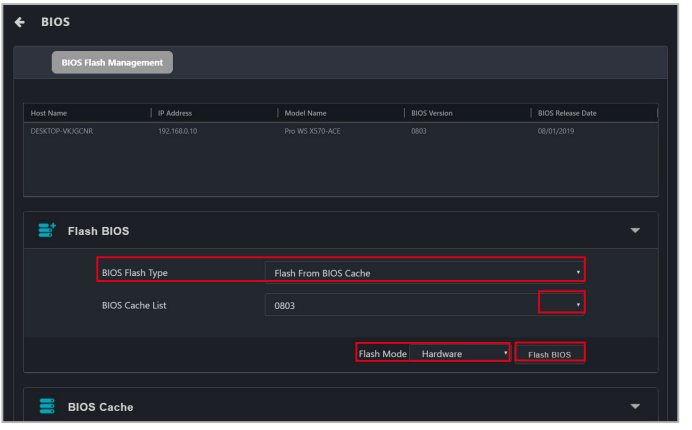


BIOSをBIOSキャッシュからフラッシュ

BIOSキャッシュからBIOSファイルを選択します。

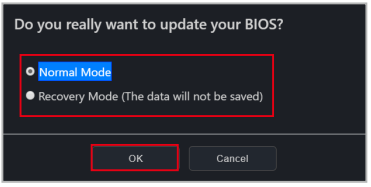
1. **BIOS Flash Type（BIOSのフラッシュタイプ）**欄から**Flash from BIOS Cache（BIOSキャッシュからフラッシュ）**を選択します。
2. **BIOS Cache List（BIOSキャッシュ一覧）**ドロップダウンメニューからBIオペレーティングシステムファイルを選択します。
3. **Flash BIOS（BIOSのフラッシュ）**をクリックします。

Flash Mode（フラッシュモード）の既定値は**Hardware Mode（ハードウェアモード）**です。



4. **Normal Mode（通常モード）**または**Recovery Mode（回復モード）**でBIOSをフラッシュするかを選択し、**OK**をクリックします。

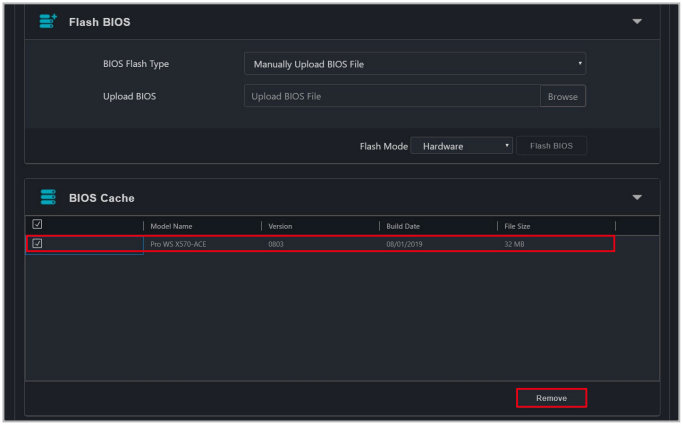
Recovery Mode（回復モード）でBIOSをフラッシュすると、すべてのBIOS設定がリセットされ、以前の設定内容が削除されます。



5. **Recovery Mode（回復モード）**では以前のBIOSデータと設定がすべて削除されるため、**Recovery Mode（回復モード）**を選択すると警告メッセージが表示されます。**Flash（フラッシュ）**をクリックし、**Recovery Mode（回復モード）**での使用を続行します。

BIOSキャッシュからBIOSファイルを削除

クライアントデバイスで使用可能なBIOSファイルがBIOS Cashe（BIOSキャッシュ）リストに表示されます。BIOSキャッシュからBIOSファイルを削除する場合は、削除するBIOSファイルを選択し、**Remove（削除）**をクリックします。



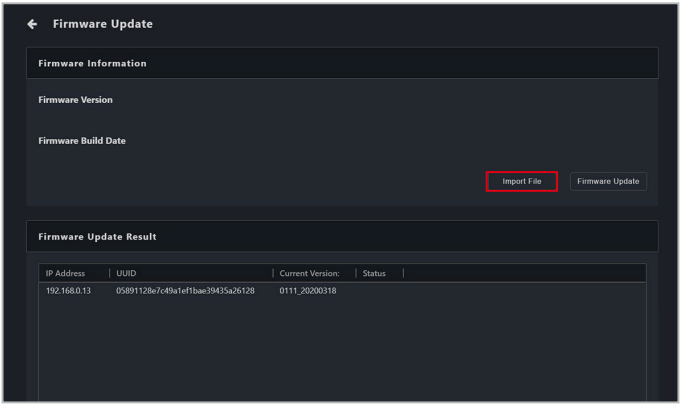
5.8.7 ファームウェア更新

Firmware Update（ファームウェア更新）機能を使用すればRTL8117 LAN ICのファームウェアを更新し、更新の結果を確認することができます。

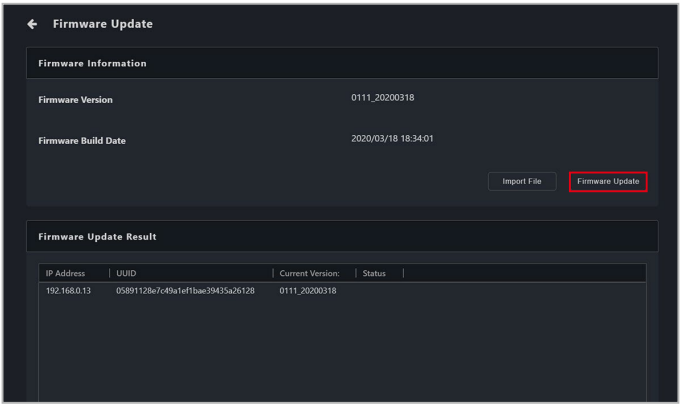
KVMが有効に設定されている場合、**Firmware Update（ファームウェア更新）**機能は無効になります。ファームウェアを更新する場合は、KVMを無効にしてください。

ファームウェアのアップロードと更新

1. **Import File（ファイルのインポート）**をクリックし、ファームウェアファイル（.img）を選択して**Open（開く）**をクリックします。



2. **Firmware Update（ファームウェア更新）**をクリックし、更新が完了するまで待ちます。



3. ファームウェアの更新結果が、**Firmware Update Result（ファームウェアの更新結果）**に表示されます。
4. クライアントデバイスが電源オンの状態でファームウェアを更新した場合、更新後にデバイスを再起動してください。

5.8.8 信頼ゾーン

この機能はデバイスがオペレーティングシステムへログインされていなかったり、RTL 8117 LAN ICに対応した管理LANポートを使用して接続されていない場合は利用できません。

Trust Zone（信頼ゾーン）は、未認証または信頼できない接続経由でクライアントデバイスがアクセスされないよう保護する手段を提供します。この機能はメインサーバーのIPアドレスをクライアントデバイスの信頼ゾーンへ設定し、信頼ゾーンへ追加されたメインサーバーのIPアドレスのみが、クライアントデバイスでリモート管理制御機能を実行できるようにします。

次の方法で信頼ゾーンページにアクセスできます：

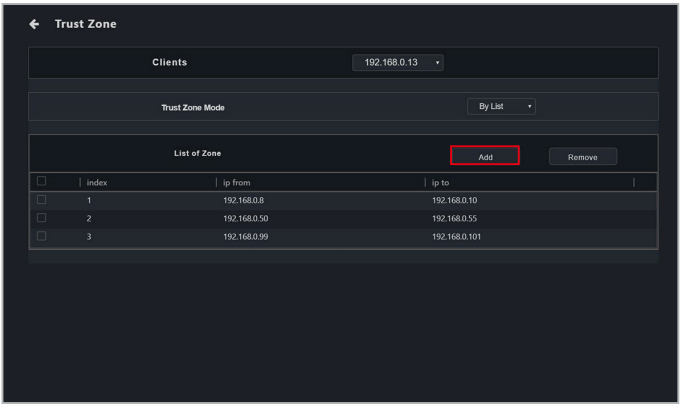
- デバイスリストのM.C列の  をクリックします。
- スキャンして、管理コントローラーページからデバイスを選択します。

選択したデバイスの信頼ゾーンのみ設定することができます。複数のデバイスで信頼ゾーンを確認する場合は、メインメニューのページへ戻り、複数のデバイスを選択してから、**Select Function（機能の選択）**ドロップダウンメニューで**OOB-Control（OOB-制御）** > **Trust Zone（信頼ゾーン）**を選択してください。

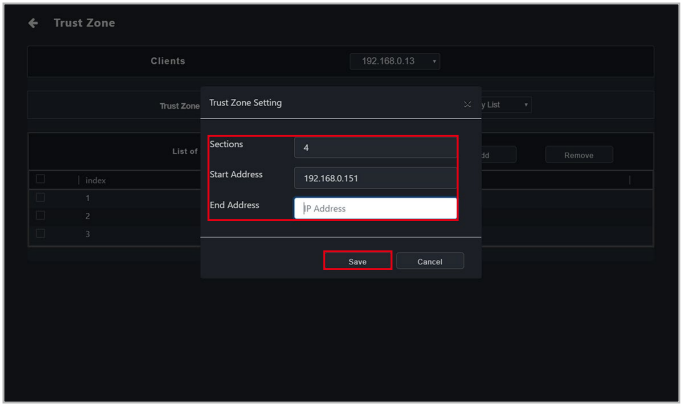
信頼ゾーンの追加

クライアントデバイスへは最大8セットのメインサーバーIPアドレスを追加することができます。すでに8セットある状態で追加したい場合は、まず信頼ゾーンの一覧から既存のIPアドレスを削除してから追加してください。

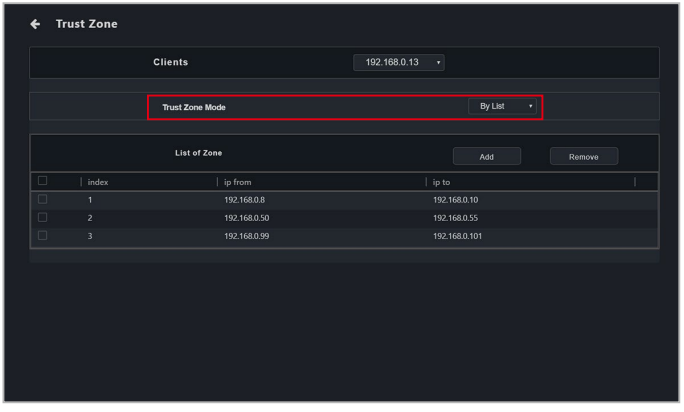
1. **Add（追加）**をクリックします。



2. クライアントデバイスの信頼ゾーンに追加するメインサーバーのIPアドレスを入力し、**Save（保存）**をクリックします。

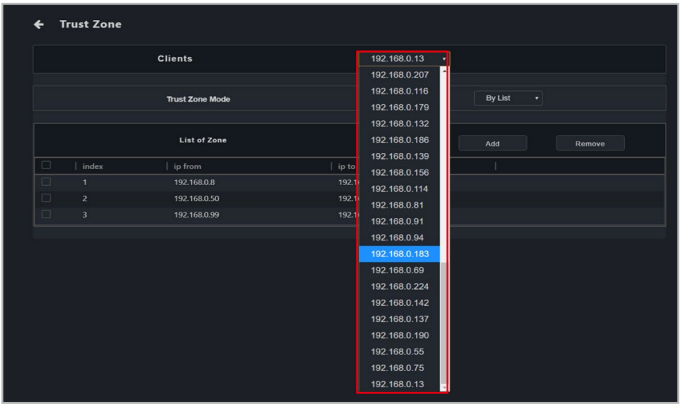


3. 手順1と2を繰り返して、信頼ゾーンへ他のIPアドレスを追加します。
4. **Trust Zone Mode（信頼ゾーンモード）**欄のドロップダウンメニューで**By List（リスト別）**を選択して、信頼ゾーン一覧に追加されたIPアドレスを有効にします。



5. （任意）**Clients（クライアント）**ドロップダウンリストから別のデバイスを選択し、そのデバイスへ信頼ゾーンを設定することができます。

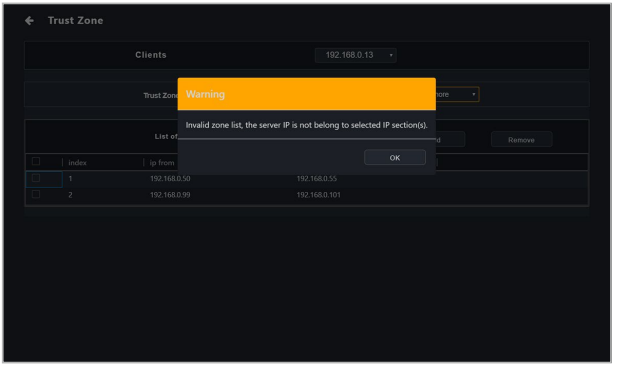
信頼ゾーンを設定するデバイスを複数選択した場合にのみ、この手順を実行してください。



6. （任意）新たに選択されたデバイスの信頼ゾーンへメインサーバーのIPアドレスを追加する場合は、手順1～4を繰り返してください。

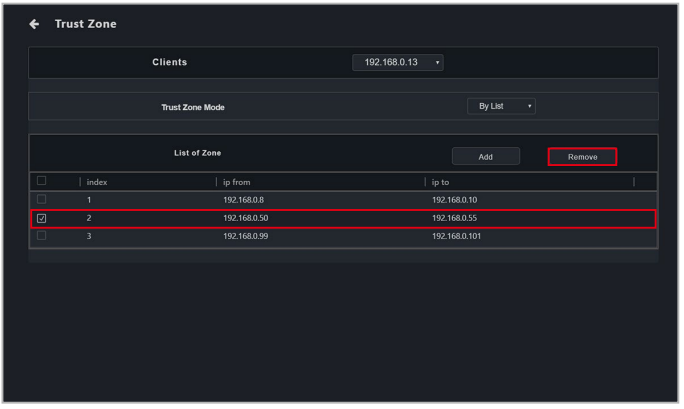
信頼ゾーンを設定するデバイスを複数選択した場合にのみ、この手順を実行してください。

信頼ゾーンリストにメインサーバーのIPアドレスが含まれていることを確認してください。信頼ゾーンリストにメインサーバーのIPアドレスが含まれていない場合は、信頼ゾーンを有効にできません。



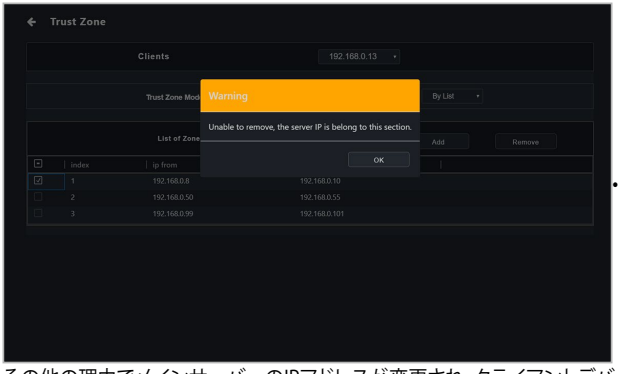
信頼ゾーンの削除

信頼ゾーンリストから削除するIPアドレスを選択して、**Remove（削除）**をクリックします。



有効な信頼ゾーンリストを無効にする場合は、**Trust Zone Mode（信頼ゾーンモード）**欄のドロップダウンメニューから**Disable（無効）**を選択してください。

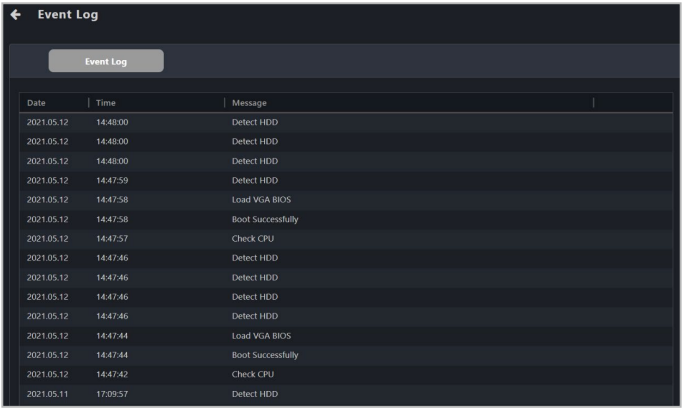
- メインサーバーのIPアドレスは有効な信頼ゾーンリストから削除することはできません。削除するIPアドレスの範囲にメインサーバーのIPアドレスが含まれていないことを確認してください。



その他の理由でメインサーバーのIPアドレスが変更され、クライアントデバイスの有効化された信頼ゾーンに含まれている場合、新しいIPアドレスはクライアントデバイスの信頼ゾーンに含まれていないため、メインサーバーを介してクライアントデバイスでリモート管理制御機能を実行できません。新しいメインサーバーのIPアドレスをクライアントデバイスに設定するには、**BIOS > Advanced（詳細）> RTL8117 Settings（RTL8117 設定）**で設定します。

5.8.9 イベントログ

クライアントデバイスの最後の電源投入時のイベントログを見ることができ、問題やトラブルの原因を分析するための情報を得ることができます。

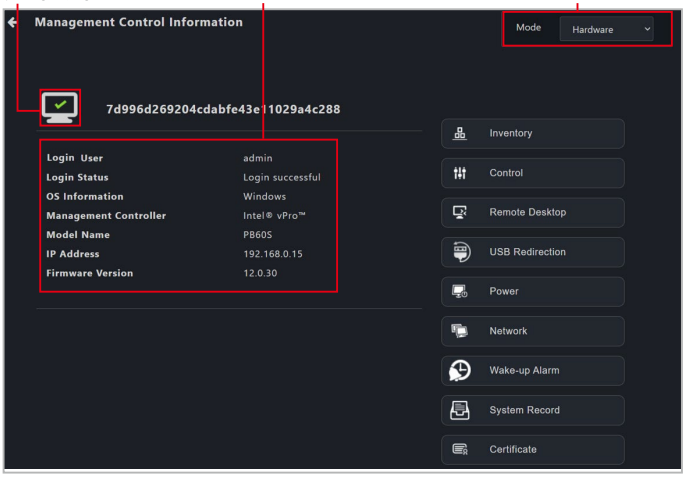


5.9 vPro 管理制御情報

vPro Management Control Information（vPro管理制御情報）により、クライアントオペレーティングシステムにエラーが発生した際のリモートでの修復、デバイスの電源オフ時のハードウェア資産の確認、イベントログやトラップアラートシステムによるシステムエラーの特定、クライアントデバイスのネットワーク管理やネットワーク保護を行うことができます。

この機能はハードウェアによって制御されており、表示される値はソフトウェアのバージョンによって異なる場合があります。ソフトウェアモードの詳細は、**4章 デバイス情報**を参照してください。

- クライアントデバイスがIntel vProリモート管理コントローラーに対応している必要があります。
- クライアントデバイスがIntel® Standard Manageability （ISM）、Intel® Active Management Technology（AMT）、Intel® Small Business Technology（SBT）に対応しているかによって、利用できる機能は異なります。クライアントデバイスがサポートしている機能は、Intel® Management Engine BIOS Extension（MEBX）を使用して確認することができます。
- 管理コントローラーを介してこれらの機能を使用する前に、クライアントデバイスのBIOS AMTおよびIntel MEBxの設定を行い、クライアントデバイスのvPro機能が有効に設定されていることを確認してください。
- IntelまたはIntel vProの商標は、Intel Corporationまたはその子会社の商標です。



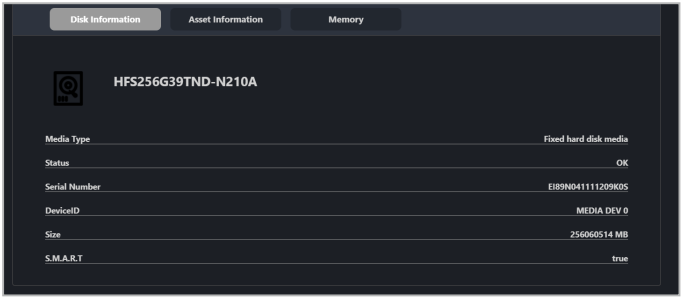
* **Management Control（管理制御）からManagement Control Information（管理制御情報）ページにアクセスした場合、この機能は使用できません。**

Device icon（デバイスアイコン）	クライアントデバイスのvProリモート管理コントローラーの接続状態を表示します。
Login user（ログインユーザー）	クライアントデバイスのvProリモート管理コントローラーに現在ログインしているユーザーアカウントを表示します。
Login Status（ログイン状態）	クライアントデバイスのvProリモート管理コントローラへの現在のログイン状態を表示します。
Management Controller（管理コントローラー）	クライアントデバイスのリモート管理コントローラを表示します。
Model Name（モデル名）	クライアントデバイスのモデル名を表示します。
IP Address（IPアドレス）	クライアントデバイスのIPアドレスを表示します。
Firmware Version（ファームウェアバージョン）	クライアントデバイスのvProリモート管理コントローラーのファームウェアバージョンを表示します。

5.9.1 インベントリ

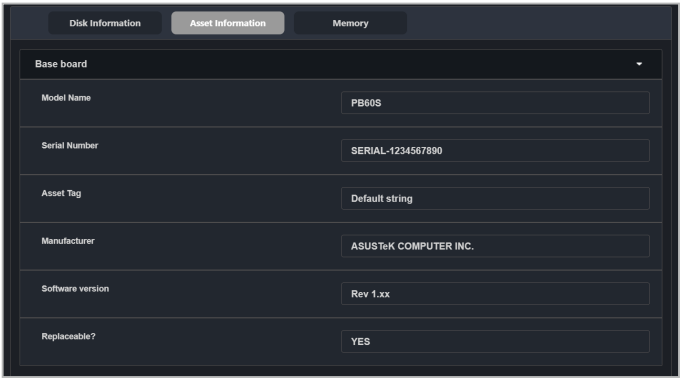
クライアントデバイスのディスク、ハードウェア資産、メモリー情報が表示されます。

Disk Information（ディスク情報）



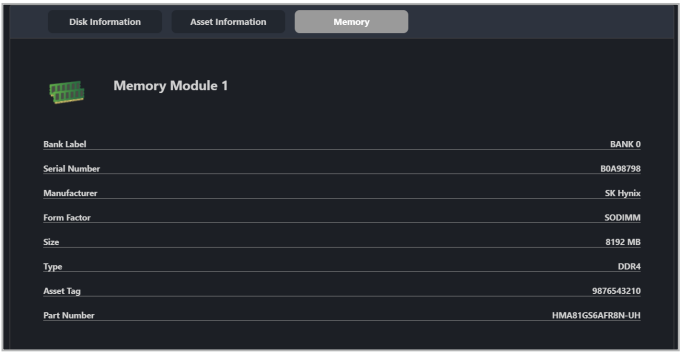
Device Name（デバイス名）	ディスクデバイス名を表示します。
Media Type（メディアタイプ）	ディスクデバイスのメディアタイプを表示します。
Status（状態）	ディスクデバイスの現在の状態を表示します。
Serial Number（シリアル番号）	ディスクデバイスのシリアル番号を表示します。
DeviceID（デバイスID）	ディスクデバイスのIDを表示します。
Size（サイズ）	ディスクデバイスの容量を表示します。
S.M.A.R.T.	S.M.A.R.T.属性の状態を表示します。

Asset Information（アセット情報）



Baseboard（マザーボード）	マザーボードのモデル名、シリアル番号、アセットタグ、製造元などの情報を表示します。
Platform（プラットフォーム）	製品名、シリアル番号、製造元などの情報を表示します。
BIOS	BIOSのリリース日、バージョン、製造元などの情報を表示します。
Processor（プロセッサー）	プロセッサーの製造元、ファミリー、モデル、クロック周波数などの情報を表示します。

Memory（メモリー）



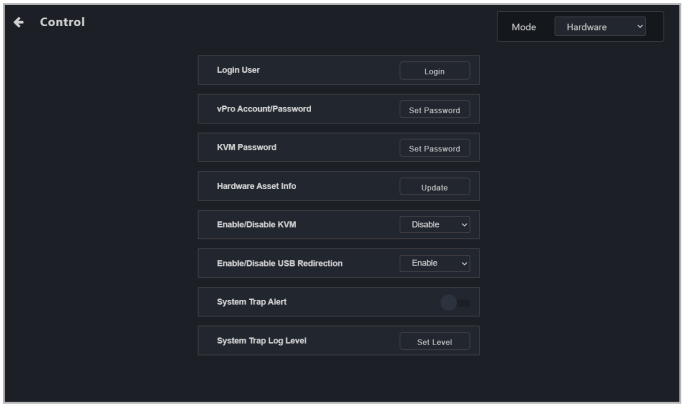
Bank Label（バンクラベル）	メモリモジュールのバンクラベルを表示します。
Serial Number（シリアル番号）	メモリモジュールのシリアル番号を表示します。
Manufacturer（製造元）	メモリモジュールの製造元名を表示します。
Form Factor（フォームファクター）	メモリモジュールのフォームファクターを表示します。
Size（サイズ）	メモリモジュールの容量を表示します。
Type（タイプ）	メモリモジュールの種類を表示します。
Asset Tag（アセットタグ）	メモリモジュールのアセットタグを表示します。
Part Number（部品番号）	メモリモジュールの部品番号を表示します。

5.9.2 制御

vProデバイスのアカウントとパスワード、KVM、USBリダイレクト、システムトラップアラート、システムトラップログレベルの機能を設定することができます。

通知ルールでは、リモート管理コントローラーの通知を追加・編集することができます。ダッシュボードのイベントログには、設定したシステムトラップアラートの通知が表示されます。

- vProアカウントのパスワードは、8文字以上で、大文字（A～Z）1文字、数字（0～9）、特殊文字1文字を含む必要があります。
- KVMパスワードは8文字で、大文字（A～Z）、小文字、数字（0～9）、および特殊文字を含む必要があります。
- システムトラップアラートを有効にする前に、ポート162が開いていることを確認してください。



vPro Account/Password（vProアカウント/パスワード）	vProデバイスのアカウントとパスワードを設定します。
Hardware Asset Information（ハードウェア資産情報）	クライアントデバイスのハードウェア資産情報を更新します。
KVM Password（KVMパスワード）	vProデバイスのKVMパスワードを更新・設定します。
Enable/Disable KVM（KVMの有効化/無効化）	デバイスのKVMを有効または無効にします。
Enable/Disable USB Redirection（USBリダイレクトの有効化/無効化）	USBリダイレクト機能を有効または無効にします。
System Trap Alert（システムトラップアラート）	システムトラップアラートを有効または無効にします。
System Trap Log Level（システムトラップログレベル）	システムトラップのログレベル（情報、警告、エラー）を設定します。

5.9.3 リモートデスクトップ

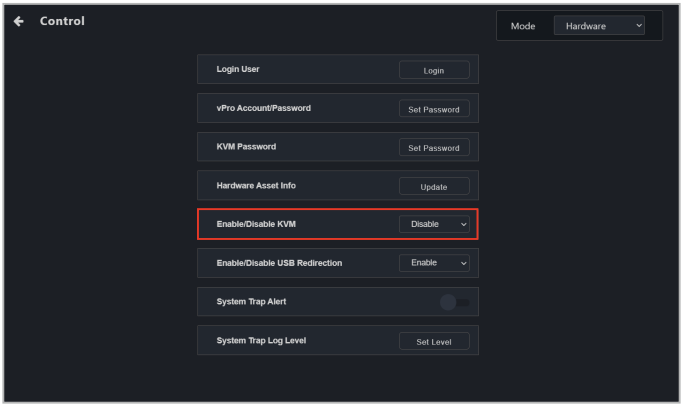
Remote Desktop（リモートデスクトップ）機能では、KVMを通じてvProクライアントデバイスを操作することができます。これは、クライアントデバイスのオペレーティングシステムにエラーが発生した場合に、クライアントデバイスをリモートで監視・修復するのに便利です。

- vProの対応やMEのバージョンによって利用できる機能が異なる場合があります。リモートデスクトップは、Intel® Standard Manageability（ISM）ではサポートされていません。
- クライアントデバイスがIntel MEBxで動作している場合、KVMを使って接続することはできません。
- KVMの使用中にクライアントデバイスが再起動された場合、デバイスはIntel®MEBxの設定画面に入ることができません。
- vProデバイスのKVMリモートデスクトップ機能を使用している場合、クライアントデバイスの画面の枠が赤色と黄色に点滅し、クライアントデバイスが現在KVMリモートデスクトップ機能を実行していることを示します。

リモートデスクトップを使用する前にKVMをセットアップする

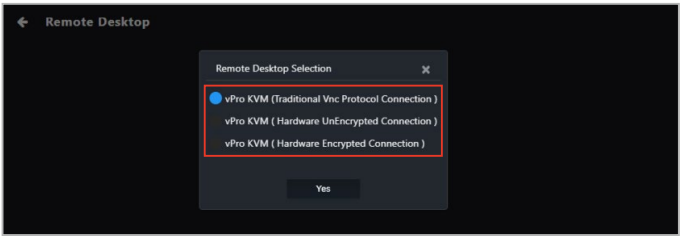
アウトオブバンド管理リモートデスクトップ機能を初めて使用する場合は、事前にKVMパスワードの設定とKVMの有効化が完了していることを確認してください。vPro Management Control Information （vPro管理制御情報）ページで**Control（制御）**をクリックし、**Enable/Disable KVM（KVMの有効化/無効化）を Enable（有効化）**に設定します。

KVMを無効にする必要がある場合は、**Disable（無効化）**オプションを選択し、クライアントデバイスを再起動します。



アウトオブバンド管理リモートデスクトップの使用

vPro Management Control Information （vPro管理制御情報）ページで**Remoote Desktop（リモートデスクトップ）**をクリックし、目的の接続方法を選択します。



Traditional VNC protocol connection（従来のVNCプロトコル接続）	VNCプロトコルを使用して暗号化接続を確立します。
Hardware unencrypted connection（ハードウェア非暗号化接続）	暗号化されていない接続を確立します。
Hardware encrypted connection（ハードウェア暗号化接続）	TLSプロトコルを使用して暗号化接続を確立します。

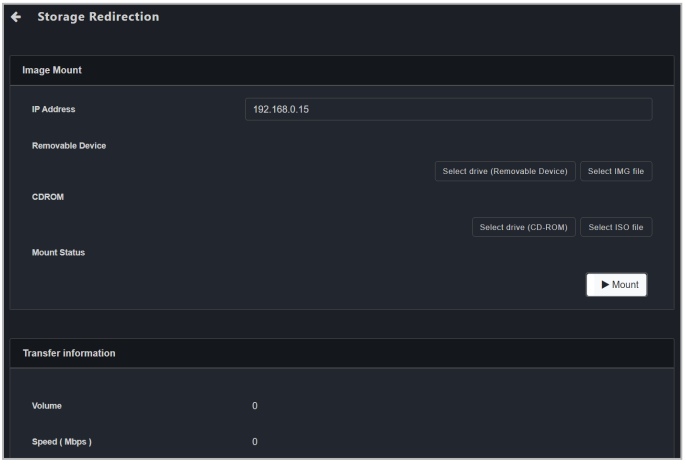
- Hardware encrypted connection（ハードウェア暗号化接続）の品質はデフォルトでLow（低）に設定されています。接続後にファンクションボタンを使用して品質を調整してください。vProの対応やMEのバージョンによって利用できる品質オプションが異なる場合があります。
- Traditional VNC protocol connection（従来のVNCプロトコル接続）を確立する前に、KVMパスワードが設定されていることを確認します。KVMパスワードを設定するには、**Control（制御）**ページを開き**KVM Password（KVMパスワード）**をクリックします。KVMパスワードは8文字で、大文字（A～Z）、小文字、数字（0～9）、および特殊文字を含む必要があります。

接続確立後、ファンクションボタンをクリックするとリモートデスクトップ画面を操作するためのオプションが表示されます。詳しくは **4.9 リモートデスクトップ（一般）** を参照してください。

5.9.4 ストレージリダイレクト

vProデバイスがUSB-R/IDE-Rストレージをリダイレクトできるよう設定することができます。

- vProのUSBリダイレクト機能は、NTFS形式のUSBデバイスをサポートしていません。
- vProのUSBリダイレクト機能を使用した場合、マウントに成功すると、クライアントデバイスはフロッピーディスクA、CDドライブ（ドライブコード）と表示されます。

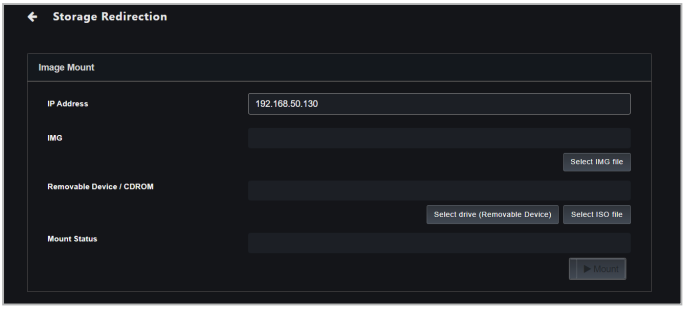


IP Address（IPアドレス）	クライアントデバイスのIPアドレスを表示します。
IMG	転送するイメージファイル（.img）ファイルを選択します。
CDROM	転送する光ディスクドライブ（ODD）または.isoファイルを選択します。
Removable Device / CDROM（リムーバブルディスク/CDROM）	デバイスやファイルのマウント状態を表示します。
Volume（容量）	データの転送容量を表示します。
Speed（スピード）（Mbps）	データの転送速度を表示します。

イメージファイルのマウント

Control（制御）でUSBリダイレクトを有効にした後、次の手順に従ってイメージファイルをマウントします。

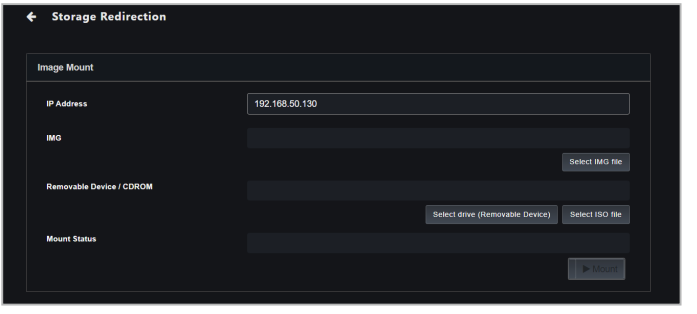
1. **Select IMG file（IMGファイルの選択）**をクリックし、マウントしたいイメージファイルを選択して**OK**をクリックします。
2. **Mount（マウント）**をクリックします。



リムーバブルデバイスまたはCDROM（ISOファイル）のマウント

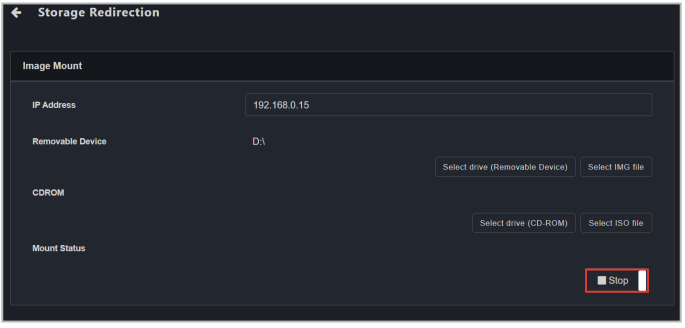
Control（制御）でUSBリダイレクトを有効にした後、次の手順に従ってリムーバブルディスクまたはISOファイルをマウントします。

1. **Select drive（ドライブの選択）**または**Select ISO file（ISOファイルの選択）**をクリックし、マウントしたいデバイスまたはISOファイルを選択して**OK**をクリックします。
2. **Mount（マウント）**をクリックします。



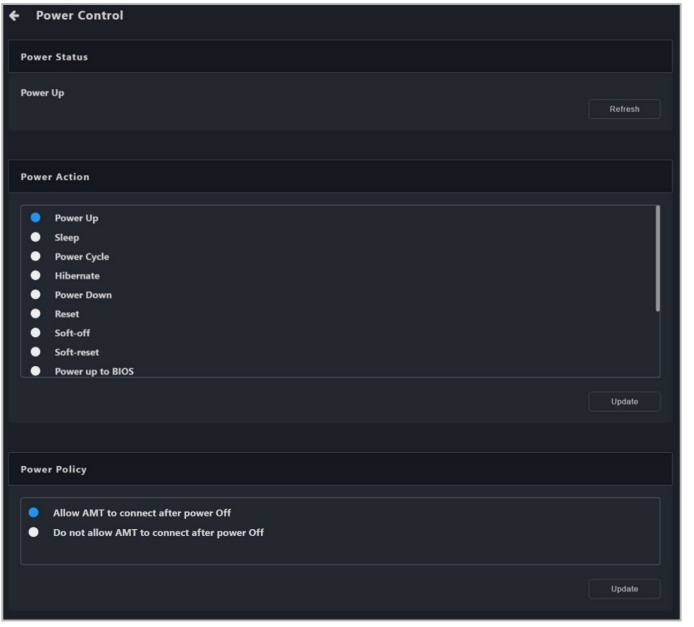
ストレージリダイレクトの終了

Stop（停止）をクリックするとストレージリダイレクトは終了します。



5.9.5 電源制御

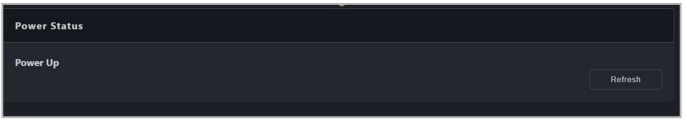
クライアントvProデバイスの電源状態を表示したり、電源制御機能を実行することができます。



電源状態

クライアントデバイスの現在の電源状態を表示します。

Refresh（更新）をクリックすると、電源状態ページに表示されている情報が最新のものに更新されます。

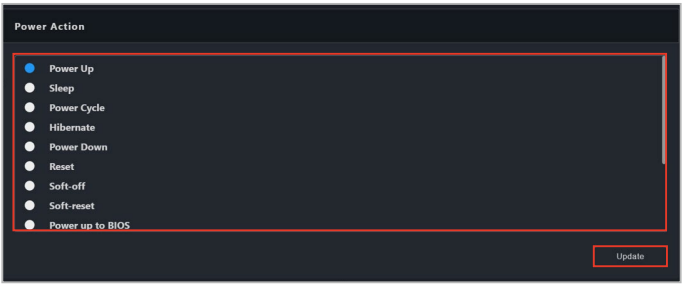


電源操作

クライアントデバイスが実行する電源操作を選択することができます。

クライアントデバイスの電源やオペレーティングシステムの状態によって、利用できる電源操作が異なる場合があります。実際の選択肢は、画面でご確認ください。

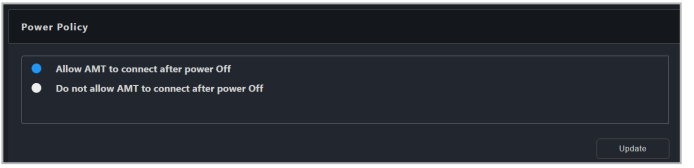
1. **Power Action（電源操作）**リストから電源操作を選択します。
2. **Update（更新）**をクリックします。



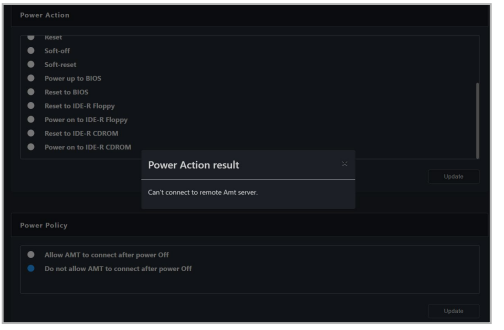
3. 確認画面で電源操作が正しいかどうかを確認し、**OK**をクリックします。
4. 電源操作が実行されたかどうかは、**Power Status（電源状態）**が選択した電源操作に更新されているかどうかで確認することができます。

電源ポリシー

電源を切った後にAMTの接続を許可するかどうかを選択することができます。



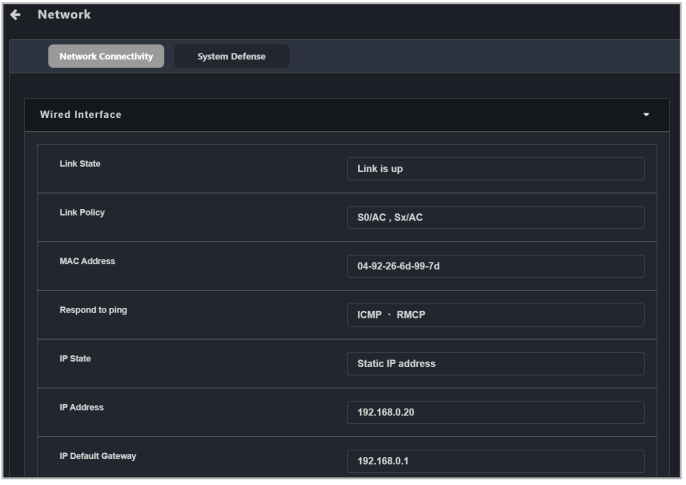
Do not allow AMT to connect after power Off（電源オフ後にAMTの接続を許可しない）を選択すると、クライアントデバイスの電源がオフの間は電源制御機能の実行、電源ステータスの更新、電源ポリシーの変更を行うことができなくなります。電源制御機能を実行する場合は、クライアントデバイスの起動または電源投入後、電源ポリシーを**Allow AMT to connect after power Off（電源切断後にAMTの接続を許可する）**に設定してください。



5.9.6 ネットワーク

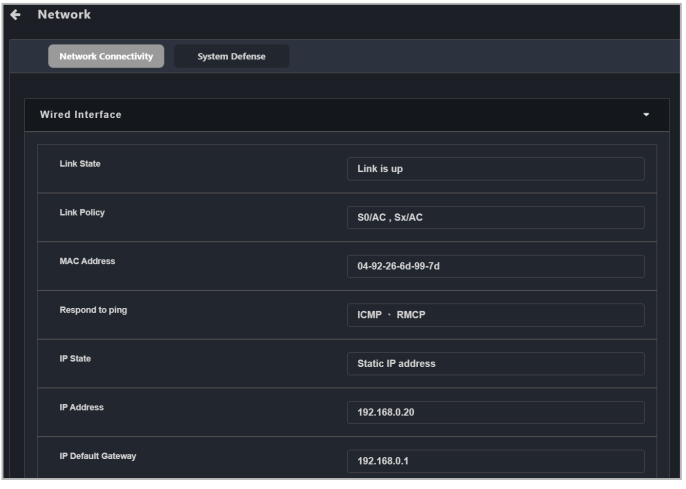
クライアントvProデバイスの有線および無線ネットワークの設定や、**System Defense（システム防御）**機能を使ってインターネットの安全対策を行うことができます。

Intel® Standard Manageability（ISM）に対応したvProクライアントデバイスでは、無線インターフェースの設定を利用できない場合があります。



ネットワークの接続性

有線/無線ネットワークの状態や設定を確認・管理することができます。

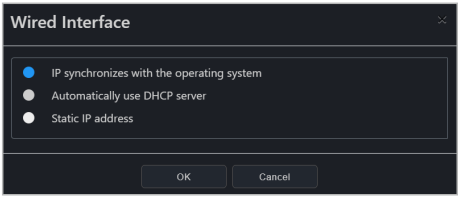


- **有線インターフェースの設定**
  クライアントデバイスの有線ネットワーク設定を表示または構成することができます。

Link State（リンク状態）	有線ネットワークのリンク状態を表示します。
Link Policy（リンクポリシー）	有線ネットワークのリンクポリシーを表示します。
MAC Address（IPアドレス）	有線ネットワークのMACアドレスを表示します。
Respond to ping（ping応答）	有線ネットワークのPing応答プロトコルを表示します。
IP State（IP状態）	有線ネットワークのIP状態を表示します。
IP Address（IPアドレス）	有線ネットワークのIPアドレスを表示します。
IP Default Gateway（IPデフォルトゲートウェイ）	有線ネットワークのIPデフォルトゲートウェイを表示します。
IP Subnet Mask（IPサブネットマスク）	有線ネットワークのIPサブネットマスクを表示します。
IP Domain Name Server（IPドメインネームサーバー）	有線ネットワークのIPドメインネームサーバーを表示します。

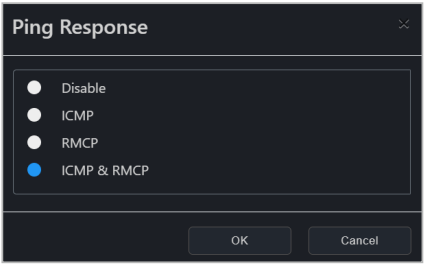
有線インターフェースIPの編集

有線インターフェース設定の**Edit（編集）**をクリックして、**IP synchronizewith the operating system（オペレーティングシステムとのIP同期）**、**Automatically use DHCP server（DHCPサーバーを自動的に使用）**、**Static IP address（静的IPアドレス）**のいずれかからクライアントデバイスのIPを設定します。



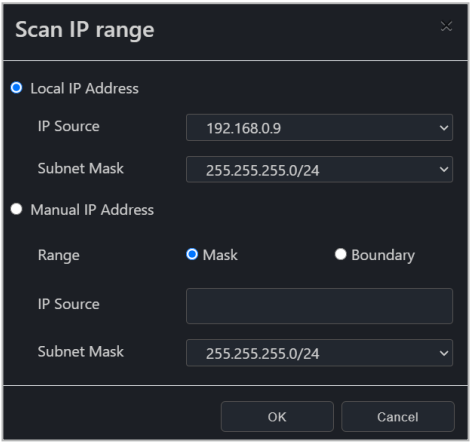
PINGパケット応答の設定

有線インターフェースの**Set ping packet response（Pingパケット応答の設定）**をクリックすると、クライアントデバイスの有線ネットワークのPingパケット応答を**Disable（無効）**、**ICMP**、**RMCP**、**ICMP & RMCP**のいずれかから設定できます。



デバイスの検索

有線インターフェースの**Search for device（デバイスの検索）**をクリックすると、指定したIP範囲内のデバイスが検索されます。IP範囲のスキャンについては、**3.2.2 IP範囲のスキャン**を参照してください。

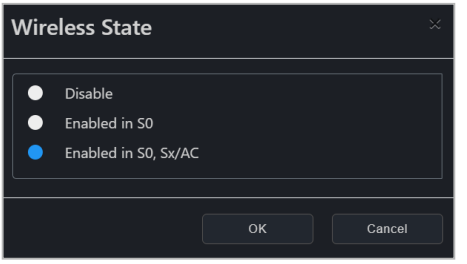


- **無線インターフェースの設定**
  クライアントデバイスの無線ネットワーク設定を表示または構成することができます。

Link State（リンク状態）	無線ネットワークのリンク状態を表示します。
Link Policy（リンクポリシー）	無線ネットワークのリンクポリシーを表示します。
MAC Address（IPアドレス）	無線ネットワークのMACアドレスを表示します。
State（状態）	無線ネットワークの設定状態を表示します。
Radio State（ラジオ状態）	無線ネットワークのラジオ状態を表示します。
IP Address（IPアドレス）	無線ネットワークのIPアドレスを表示します。
IP Default Gateway（IPデフォルトゲートウェイ）	無線ネットワークのIPデフォルトゲートウェイを表示します。
IP Subnet Mask（IPサブネットマスク）	無線ネットワークのIPサブネットマスクを表示します。
IP Domain Name Server（IPドメインネームサーバー）	無線ネットワークのIPドメインネームサーバーを表示します。

無線状態の設定：

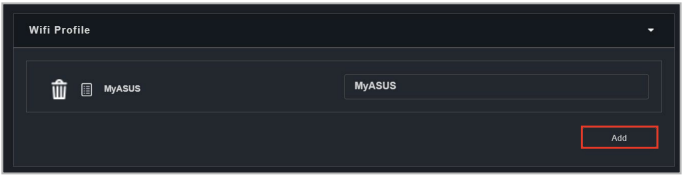
無線インターフェース設定ブロックの**Edit（編集）**をクリックして、クライアントデバイスの無線状態を**Disable（無効）**、**Enabled in S0（S0で有効）**、**Enabled in S0、Sx/AC（S0、Sx/ACで有効）**のいずれかに設定します。無線ネットワークの接続は、選択したワイヤレスの状態に応じて進みます。



- **Wi-Fiプロファイル**
  クライアントデバイスのWi-Fiプロファイルを追加・編集することができます。クライアントデバイスは、選択したWi-Fiプロファイルとワイヤレス状態にしたがって接続/切断されます。

  新しいWi-Fiプロファイルの追加

  1. **Add（追加）**をクリックします。



2. Wi-Fiプロファイルの情報を入力します。
3. すべての設定が完了したら **OK** をクリックします。新しく追加された Wi-Fiプロファイルはプロファイルリストに表示されます。

Wi-Fiプロファイルの編集

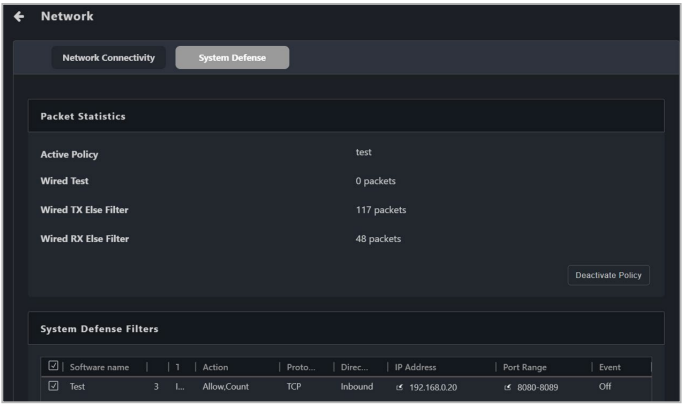
既存のWi-Fiプロファイルを編集するには、プロファイル名の横にある編集アイコン ( ) をクリックします。

Wi-Fiプロファイルの削除

既存のWi-Fiプロファイルを削除するには、プロファイル名の横にある削除アイコン ( ) をクリックします。

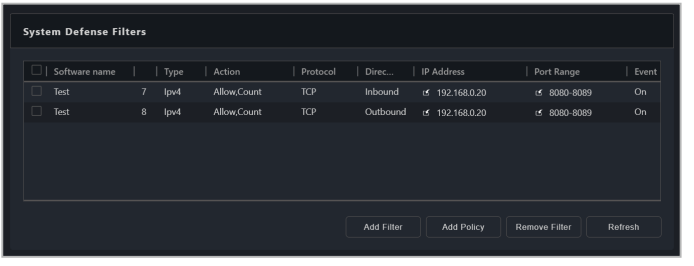
システム防御

クライアントデバイスにインターネットの安全対策を定義して実行することで、ネットワークを分離したり、侵入テスト機能を提供することができます。



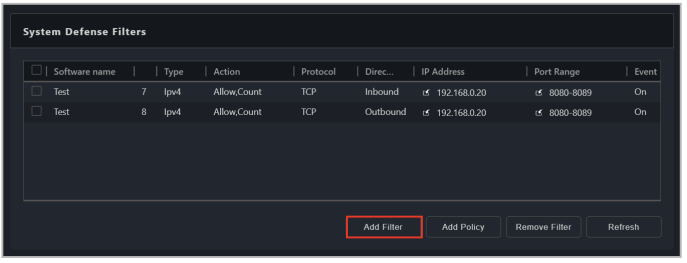
- **システム防御フィルター**
  隔離されたネットワークの発信・着信パケットの設定、特定のIPアドレスの許可・禁止、ネットワークトラフィックフィルターの設定、データ転送の計算・記録を行います。

Refresh（更新）をクリックすると、システム防御フィルターリストが最新の状態に更新されます。

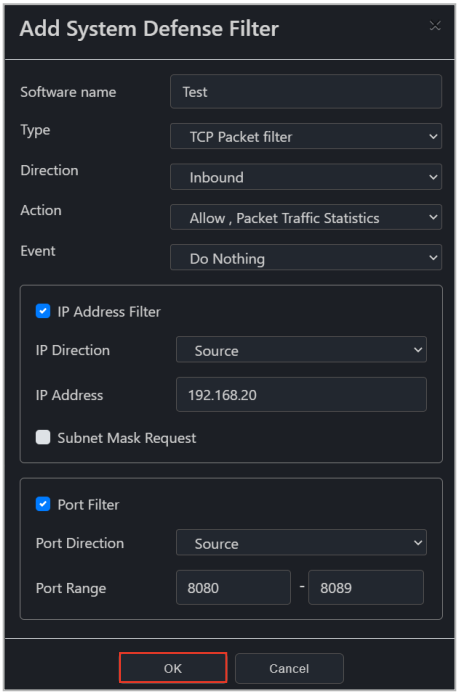


システム防御フィルターの追加

1. **Add Filter（フィルターの追加）**をクリックします。



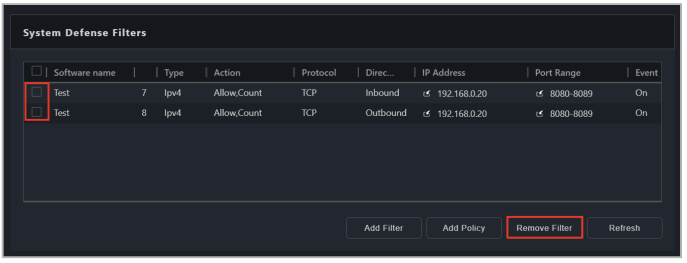
2. 新しいシステム防御フィルターの設定を選択・入力して、**OK**をクリックします。



3. 手順1と2を繰り返して、システム防御フィルターを追加します。
4. 新たに追加されたシステム防御フィルターは、システム防御フィルターリストに表示されます。

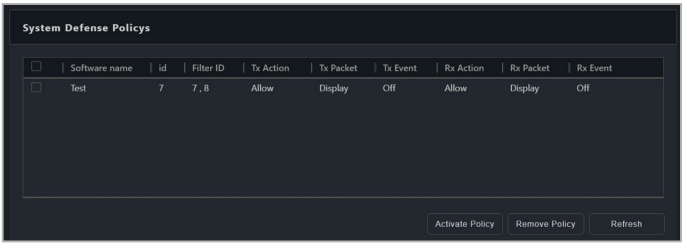
システム防御フィルターの削除

システム防御フィルターを削除するには、削除したいシステム防御フィルターを選択して、**Remove Filter（フィルターの削除）**をクリックします。



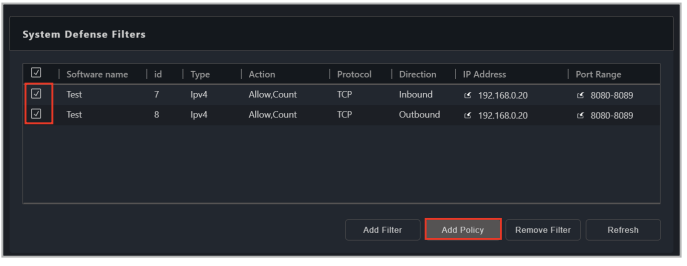
- **システム防御ポリシー**
  受信および送信されるパケットが、フィルターで設定された条件に一致するかどうかを確認し、ポリシーの設定に従って動作します。

Refresh（更新）をクリックすると、システム防御ポリシーリストが最新の状態に更新されます。

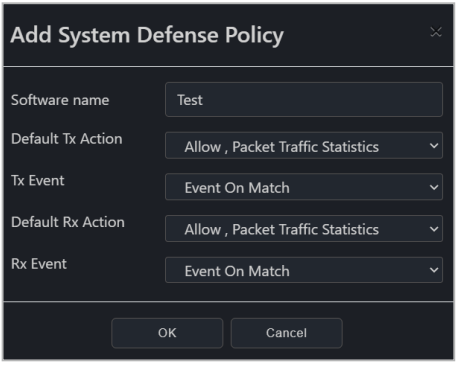


システム防御ポリシーの追加

1. ポリシーを追加したいシステムディフェンスフィルターをシステムディフェンスフィルターリストで選択し、**Add Policy（ポリシーの追加）**をクリックします。



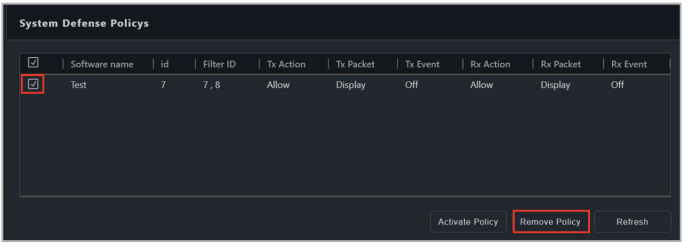
2. システム防御ポリシーの設定を選択・入力して、**OK**をクリックします。



3. 新たに追加されたシステム防御ポリシーは、システム防御ポリシーリストに表示されます。

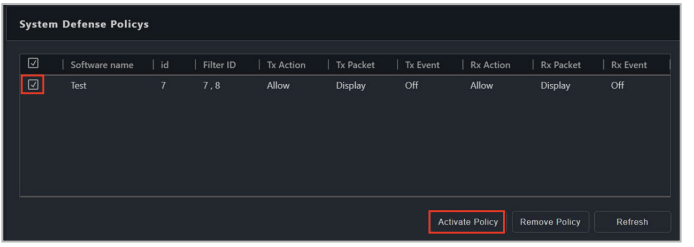
システム防御ポリシーの削除

システム防御ポリシーリストから削除したいシステム防御ポリシーを選択し、**Remove Policy（ポリシーの削除）**をクリックします。

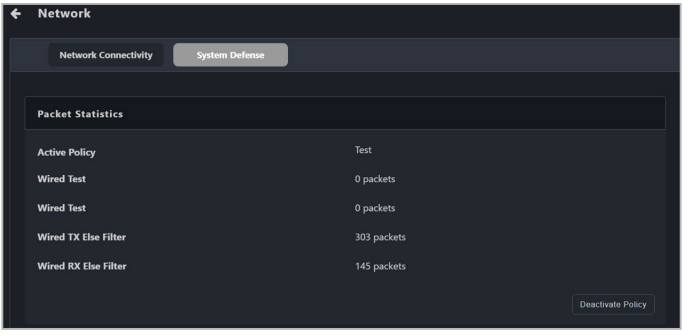


システム防御ポリシーの有効化

システム防御ポリシーリストで有効化するシステム防御ポリシーを選択し、**Activate Policy（ポリシーの有効化）**をクリックします。



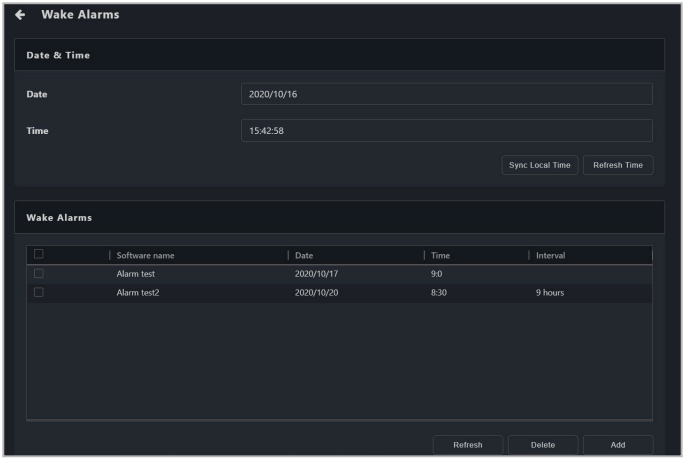
パケット統計は、**System Defense（システム防御）**ページの上部にあるパケット統計ブロックをスクロールすると表示されます。



一度に有効化できるシステム防御ポリシーは1つだけです。別のシステム防御ポリシーを使用する場合は、パケット統計の**Deactivate Policy（ポリシーの無効化）**をクリックして現在有効なポリシーを無効にしてから、新しいポリシーを有効化します。

5.9.7 ウェイクアップアラーム

クライアントデバイスがスリープモードまたは電源オフ状態の時に、クライアントvProデバイスを起動するためのアラームを設定することができます。

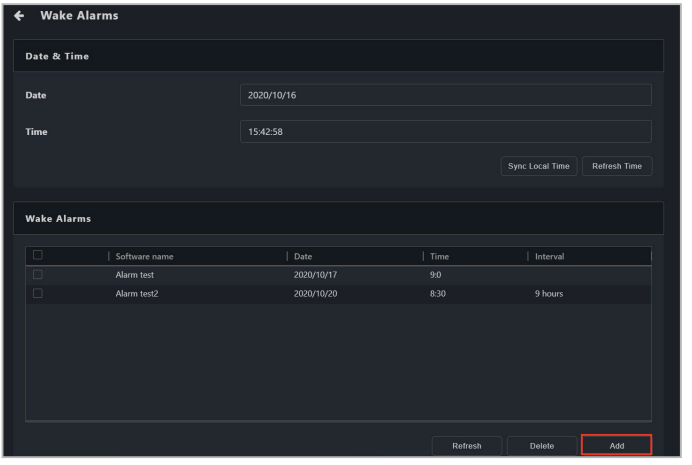


Date（日付）	クライアントvProデバイスの日付です。
Time（時間）	クライアントvProデバイスの時間です。
Sync Local Time（ローカルタイムの同期）	クライアントvProデバイスの時刻をメインサーバーの時刻と同期します。
Refresh Time（更新）	クライアントvProデバイスの時刻を最新の状態に更新します。

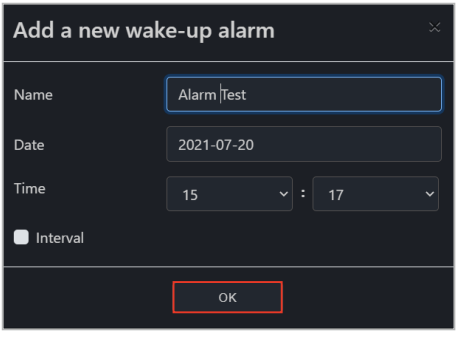
新しいウェイクアラームの追加

- 1台のクライアントvProデバイスに追加できるウェイクアラームは最大5個までです。1台のデバイスで許可されるウェイクアラームの上限に達している場合は、まず未使用のウェイクアラームを削除してください。
- **Refresh（更新）**をクリックすると、ウェイクアラームリストが最新の状態に更新されます。

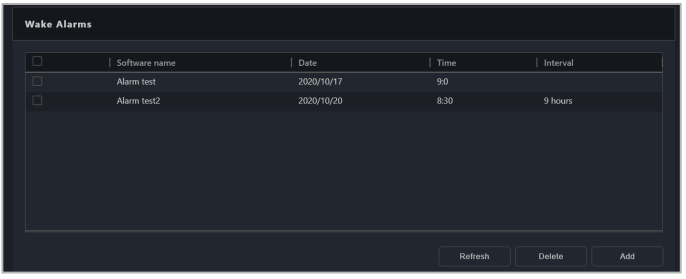
1. **Add（追加）**をクリックします。



新しいウェイクアップアラームの設定を入力し、**OK**をクリックします。

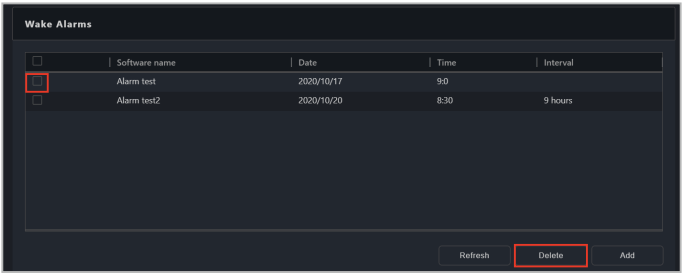


3. 新しく追加されたウェイクアラームは、ウェイクアラームリストに表示されます。



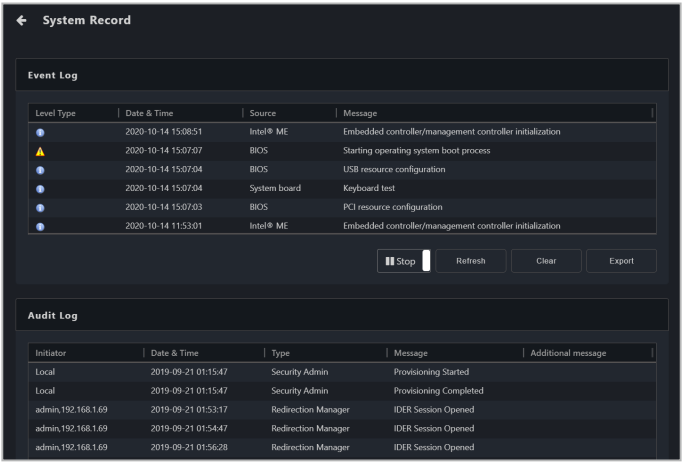
ウェイクアラームの解除

ウェイクアラームリストから削除したいウェイクアラームを選択し、**Delete（削除）**をクリックします。



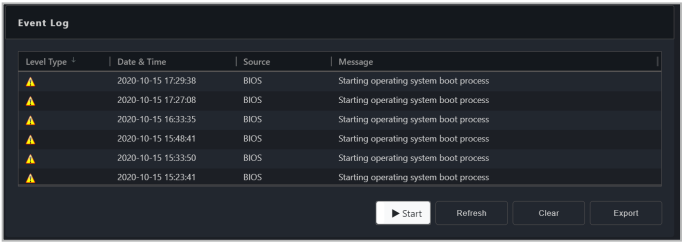
5.9.8 システム記録

イベントログやアラートの記録から、クライアントvProデバイスの問題や不具合をすばやく検出することができます。



イベントログ

クライアントvProデバイスのイベントログ記録を表示し、デバイスの問題や不具合を分析・検出します。

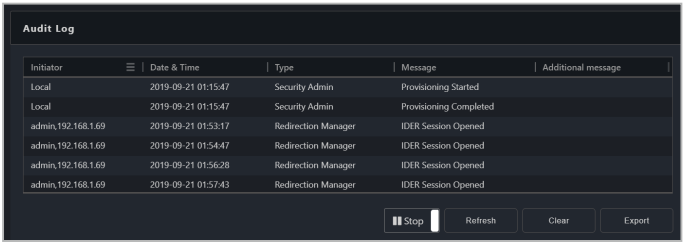


Start / Stop（開始/停止）	イベントログの記録を開始または停止します。
Refresh（更新）	イベントログを最新の状態に更新します。
Clear（クリア）	イベントログの記録を消去します。
Export（エクスポート）	イベントログの記録をエクスポートします。

監査ログ

指定されたデバイスのシステム操作や不正アクセスを監査ログに記録します。監査ログを追跡することで、様々な問題の原因や、セキュリティ違反、不正使用などを発見することができます。

- クライアントvProデバイスの監査ログは定期的にエクスポートして消去してください。
- 監査ログのストレージ容量に関するアラートが表示された場合は、監査ログをエクスポートしてから消去してください。監査ログのストレージ容量が一杯になると、クライアントデバイスで重要なイベントや深刻な問題として定義されたイベントを実行できなくなります。

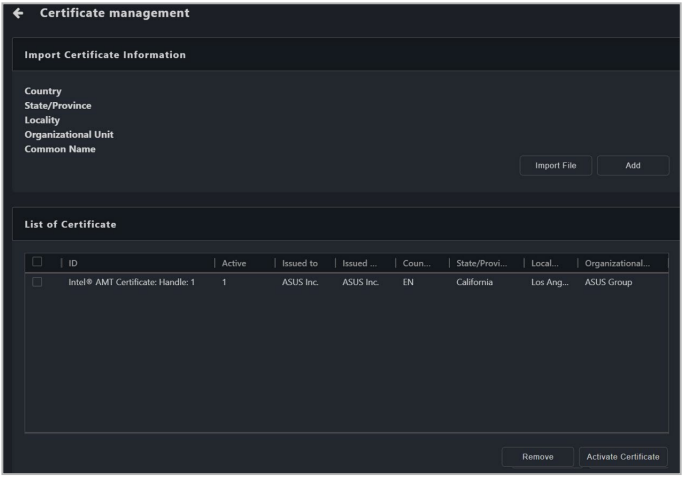


Start / Stop（開始/停止）	監査ログの記録を開始または停止します。
Refresh（更新）	監査ログを最新の状態に更新します。
Clear（クリア）	監査ログの記録を消去します。
Export（エクスポート）	監査ログの記録をエクスポートします。

5.9.9 証明書

暗号化や識別のための証明書をインポートすることができます。これにより、メインサーバーとクライアントのvProデバイス間の接続が安全かつ確実に行われます。

証明書の取得について詳しくは、IntelのWebサイトにある証明書のサプライヤー情報をご参照ください。証明書でサポートされているタイプを確認してください。



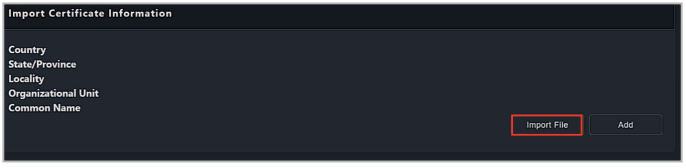
Import File（ファイルのインポート）	証明書ファイルをインポートします。
Add（追加）	インポートした証明書をリストに追加します。
Country（国）	証明書の国番号をインポートします。
State/Province（州/県）	証明書の州/県をインポートします。
Locality（地域）	証明書の地域をインポートします。
Organization Unit（組織単位）	証明書の組織単位をインポートします。
Common Name（共通名）	証明書の共通名をインポートします。
Active（アクティブ）	1は証明書が有効であることを表し、0は証明書が無効であることを示します。
Remove（削除）	選択した証明書を削除します。
Activate Certificate（証明書の有効化）	選択した証明書を有効にします。

単一デバイスの証明書の追加と有効化

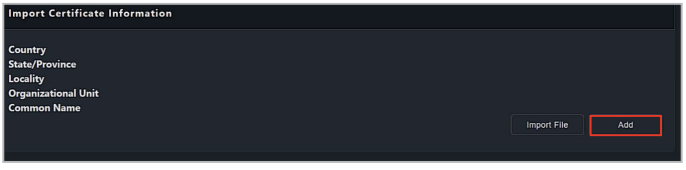
1. 単一のデバイスに証明書を追加して有効にするには、デバイスの**Management Control Information（管理制御情報）**ページで**Certificate（証明書）**をクリックします。

- 各クライアントvProデバイスは、一度に1つの証明書しか有効にできないため、証明書をインポートした後は、必ず証明書を有効化してください。
- 証明書の**Remove（削除）**および**Activate Certificate（証明書の有効化）**機能は、単一デバイスの**Management Control Information（電源制御情報）**ページから証明書機能にアクセスした場合のみサポートされます。

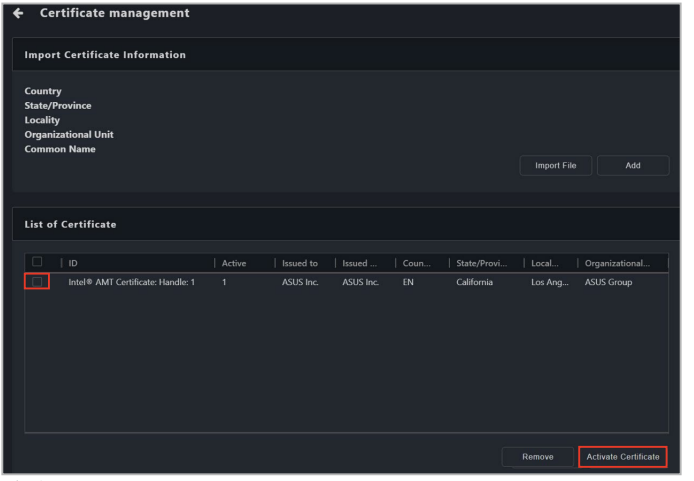
2. **Import File（ファイルのインポート）**をクリックし、インポートする証明書を選択します。



3. **Import Certificate Information（証明書のインポート情報）**でインポートされた証明書情報が正しいことを確認し、**Add（追加）**をクリックします。



4. 新しく追加された証明書は、**List of Certificate（証明書のリスト）**に表示されます。証明書リストから有効化したい証明書を選択し、**Activate Certificate（証明書の有効化）**をクリックします。



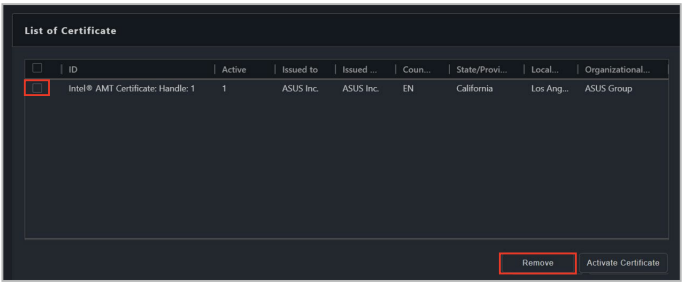
単一デバイスの証明書の削除

1. 単一のデバイスに証明書を追加して有効にするには、デバイスの**Management Control Information（管理制御情報）**ページで**Certificate（証明書）**をクリックします。

> 証明書の削除および**Activate Certificate（証明書の有効化）**機能は、単一のデバイスの**Management Control Information（管理制御情報）**ページから証明書機能にアクセスした場合のみサポートされます。

2. **List of Certificate（証明書のリスト）**から削除する証明書を選択し、**Remove（削除）**をクリックします。

> 有効化されている証明書を削除することはできません。現在有効な証明書を削除したい場合は、まず別の証明書を選択して有効化してください。

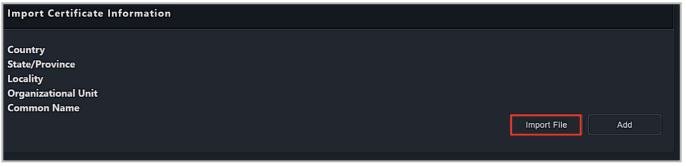


複数デバイスの証明書の追加と有効化

1. メインメニュー画面で複数のデバイスを選択し、**Select Function（機能の選択）**ドロップダウンメニューから **OOB-Control（OOB-制御）> Certificate Management（証明書管理）**を選択します。

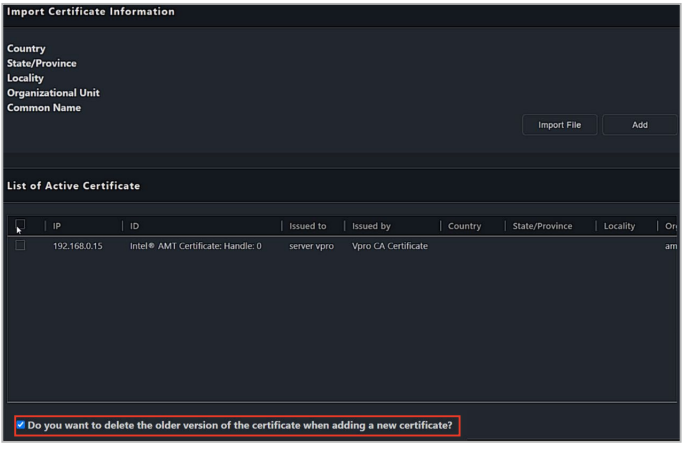
- 各クライアントvProデバイスは、一度に1つの証明書しか有効にできないため、証明書をインポートした後は、必ず証明書を有効化してください。
- 証明書の削除および**Activate Certificate（証明書の有効化）**機能は、単一のデバイスの**Management Control Information（管理制御情報）**ページから証明書機能にアクセスした場合のみサポートされます。

2. **Import File（ファイルのインポート）**をクリックし、インポートする証明書を選択します。



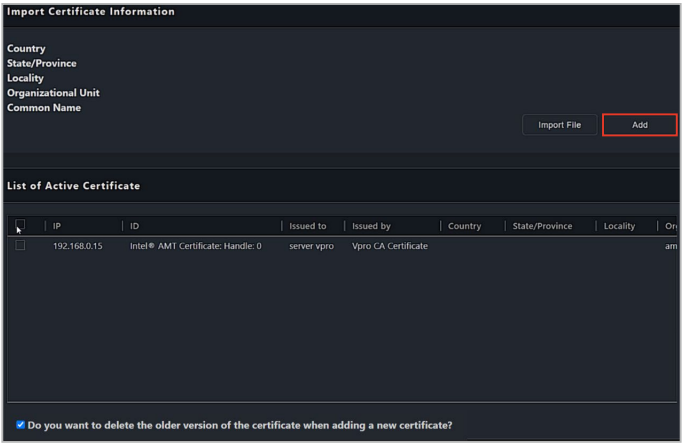
3. インポートされた証明書情報が正しいかどうかを、**Import Certificate Information（証明書情報のインポート）**で確認します。
4. 必要に応じて、**Do you want to delete the older version of the certificate when adding a new certificate?（新しい証明書を追加するときに、古いバージョンの証明書を削除しますか?）**オプションをチェックします。

オプションは、**OOB-Control（OOB-制御）> Certificate Management（証明書管理）**から証明書機能にアクセスした場合にのみ利用できます。



5. **Add（追加）**をクリックすると、新しく追加された証明書が**List of Active Certificate（有効な証明書リスト）**に表示されます。

- 手順4でオプションをチェックした場合、新しく追加された証明書は古いバージョンの証明書と置き換わります。
- オプションをチェックしなかった場合、有効だった古いバージョンの証明書は無効になり、**List of Active Certificate（有効な証明書リスト）**に表示されなくなります。古い無効な証明書を削除するには、単一デバイスの**Management Control Information（管理制御情報）**ページのCertificate（証明書）をクリックして、証明書ページにアクセスする必要があります。



5.10 BMC管理制御情報

BMC管理制御情報では、ハードウェアや資産情報を監視したり、KVMリモート制御、リモート電源制御、Serial-over-LAN（SOL）、メディアリダイレクト、IPMIToolコマンドなどの機能を管理することができます。

- この機能はハードウェアによって制御されており、表示される値はソフトウェアのバージョンによって異なる場合があります。ソフトウェアモードの詳細は4章を参照してください。
- アイコンをクリックすると、追加情報の表示・非表示を切り替えることができます。

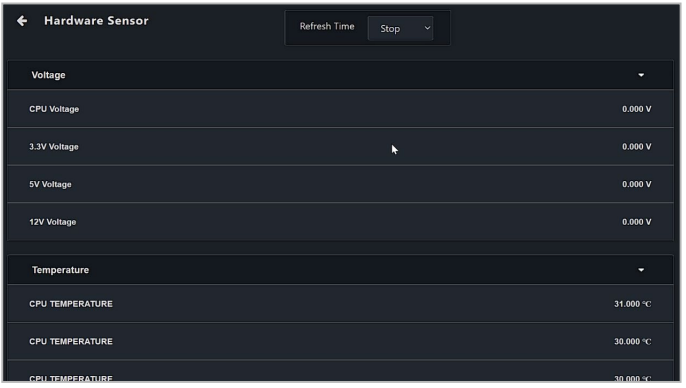
- BMC管理制御を使用する前に、クライアントデバイスのBIOSでBMC機能を有効にし、クライアントデバイスでBMCユーザー名とパスワードを設定してください。また、BMCデバイスとWebコンソールへの接続が安定していることを確認してください。
- ハードウェアや資産情報などの一部機能は、クライアントデバイスがオフラインの場合でも利用することができます。その他の機能については、予期しない動作を避けるために、ASUS Control Center ExpressがBMCリモート管理コントローラーへ接続が完了するのを待ってからご利用ください。
- クライアントデバイスがBMCリモート管理コントローラーに対応しており、すべてのセンサーが正しく動作していることをご確認ください。

* Management Control（管理制御）から Management Control Information（管理制御情報）ページにアクセスした場合、この項目は表示されません。

Device icon（デバイスアイコン）	クライアントデバイスのBMCリモート管理コントローラーの接続状態を表示します。デバイスアイコンをクリックすると、クライアントデバイスのWebコンソールを開くことができます。  ASUS Control Center Expressに戻るには、Webコンソールの左サイドバーにある**Sign Out（サインアウト）**をクリックします。
Login user（ログインユーザー）	クライアントデバイスのBMCリモート管理コントローラーに現在ログインしているユーザーアカウントを表示します。ログインユーザーを切り替えることができます。
Login status（ログイン状態）	クライアントデバイスのBMCリモート管理コントローラーへの現在のログイン状態を表示します。
Management controller（管理コントローラー）	クライアントデバイスのリモート管理コントローラーを表示します。
IP address（IPアドレス）	クライアントデバイスのIPアドレスを表示します。
Management OEM status（管理OEM状態）	クライアントデバイスがOEM管理機能をサポートしているかどうかを表示します。
Model name（モデル名）	クライアントデバイスのモデル名を表示します。
BIOS version（BIOSバージョン）	クライアントデバイスのBIOSバージョンを表示します。
BIOS build date（BIOSビルド日）	クライアントデバイスのBIOSビルド日を表示します。
Firmware model（ファームウェアモデル）	クライアントデバイスのファームウェアモデルを表示します。
Firmware version（ファームウェアバージョン）	クライアントデバイスのファームウェアバージョンを表示します。
Firmware build date（ファームウェアビルド日）	クライアントデバイスのファームウェアビルド日を表示します。
Power status（電源状態）	クライアントデバイスの現在の電源状態を表示します。
LED status（LED状態）	クライアントデバイスのLEDインジケーター状態を表示します。
Uptime（稼働時間）	クライアントデバイスの稼働時間を表示します。
Timezone（タイムゾーン）	BMCリモート管理コントローラーのタイムゾーン設定を表示します。

5.10.1　ハードウェアセンサー

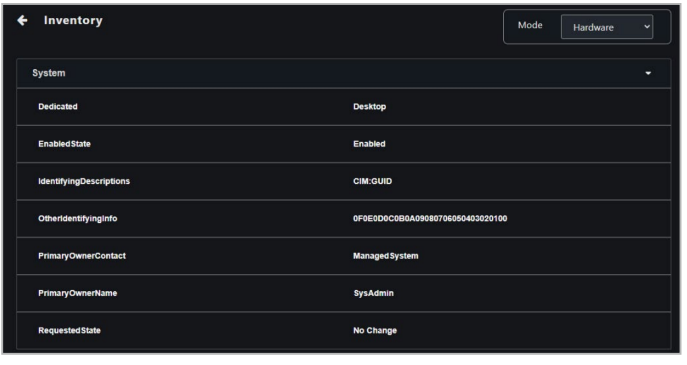
クライアントBMCデバイスの、電圧、温度、ファン回転数、センサー情報などを確認することができます。



Refresh Time（更新タイム）	ハードウェアセンサーの更新時間間隔を設定します。
Voltage（電圧）	デバイスハードウェアの電圧を表示します。
Current（電流）	デバイスハードウェアの電流を表示します。
Temperature（温度）	デバイスハードウェアの温度を表示します。
Fan（ファン）	デバイスハードウェアのファン回転数を表示します。
VERSION_ERR sensor（VERSION_ERRセンサー）	VERSION_ERRセンサーの状態を表示します。
Watchdog2 sensor（Watchdog2センサー）	Watchdog2センサーの状態を表示します。

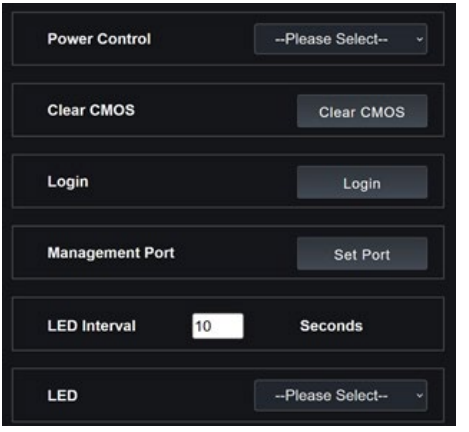
5.10.2　インベントリ

システム、プロセッサー、メモリー、PCIeデバイス、PCIe機能、ストレージコントローラー、およびその他のハードウェア情報を確認することができます。



5.10.3 制御

ログイン資格情報、ポート、LEDインジケーターの設定、CMOSの消去、クライアントデバイスで電源制御機能のリモート実行を行うことができます。



Power Control（電源制御）

BMCリモート管理コントローラーを介して、システムの再起動など、クライアントデバイスの電源制御機能をリモートで実行することができます。

Power On (G0/S0)(電源オン)	BMCリモート管理コントローラーを介してクライアントデバイスの電源をオンにします。
Power Off - Soft (G2/S5)(電源オフ-ソフト)	BMCリモート管理コントローラーを介してクライアントデバイスの電源をオフにします。
Power Off - Hard (G3)(電源オフ-ハード)	BMCリモート管理コントローラーを介してオペレーティングシステムが応答しないときにクライアントデバイスの電源を強制的にオフにします。
Power Cycle - Soft off(G2/S5)(電源サイクル-ソフトオフ)	BMCリモート管理コントローラーを介してオペレーティングシステムからシャットダウンした後、クライアントデバイスを再起動します。
Power Cycle - Hard Off(G3)(電源サイクル-ハードオフ)	BMCリモート管理コントローラーを介してクライアントデバイスの電源をオフにしてから再起動します。

Clear CMOS（CMOSの消去）

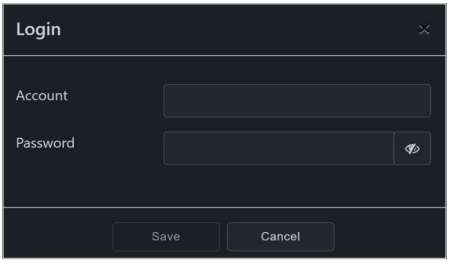
クライアントデバイスのBIOSのCMOSを消去（クリア）して、既定の設定に復元します。操作の進行状況はミッションセンターで確認することができます。

- CMOSを消去する前に、クライアントデバイスの電源をオフにする必要があります。
- この機能を使用できるかどうかは、BIOSとBMCファームウェアに依存します。

Login（ログイン）

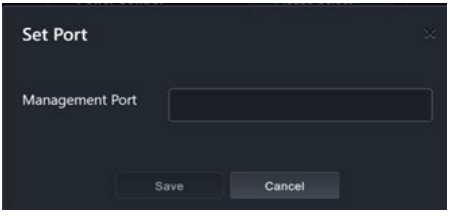
ASUS Control Center ExpressがクライアントデバイスのBMCリモート管理コントローラーへのログインに使用するアカウントとパスワードを入力します。

正常にログインすると、BMCリモート管理コントローラーは新しくログインしたアカウントに自動的に切り替わります。



Sync OEM Port（OEMポートの同期）

BMC Webコンソールに使用する管理ポートと同期することができます。



- 管理ポートはBMC Webコンソールが使用するポートと同じである必要があります。異なるポートに設定した場合、BMC機能は使用できません。
- すべてのデバイスのデフォルト管理ポートを設定するには、メインコントロールパネルのメニューバーで**Setting（設定）> Option（オプション）> General Configuration（全般設定）**の順に進み、**BMC Account（BMCアカウント）> Management Port（管理ポート）**までスクロールします。

LED Interval（LEDインターバル）

クライアントデバイスのLEDインジケータの状態と点滅間隔を設定することができます。

LED On（LEDオン）	クライアントデバイスのLEDインジケーターが点灯します。
LED Off（LEDオフ）	クライアントデバイスのLEDインジケーターが点滅します。
LED Interval（LED間隔）	クライアントデバイスのLEDインジケーターは、指定された間隔で点灯し、その後オフ状態に戻り点滅します。

5.10.4 リモートデスクトップ

リモートデスクトップ機能は、ASUS Control Center Expressでアクセスするデスクトップを通して、帯域外のデバイスを管理するための柔軟なインターフェイスを提供します。このリモートデスクトップにより、クライアントデバイスがOS環境にない場合でも制御することができます。

Video（ビデオ）	Pause Video（ビデオの一時停止）	コンソールリダイレクトを一時停止します。
	Resume Video（ビデオの再開）	セッションが一時停止された場合、コンソールリダイレクトを再開します。
	Refresh Video（ビデオの更新）	コンソールリダイレクトウィンドウに表示される内容を更新します。
	Display On（ディスプレイオン）	クライアントデバイスのディスプレイをオンにします。
	Display Off（ディスプレイオフ）	クライアントデバイスのディスプレイをオフにします。
	Capture Screen（画面キャプチャ）	コンソールリダイレクト画面のスクリーンショットをキャプチャします。
Mouse（マウス）	Show Client Cursor（クライアントカーソルの表示）	クライアントデバイスのローカルマウスカーソルの表示／非表示を切り替えます。
	Mouse Mode（マウスモード）	マウスモードを絶対座標、相対座標、その他のモード間で切り替えます。
Options（オプション）	Zoom（拡大）	画面の拡大比率を調整します。
	Block Privilege Request（ブロック権限要求）	権限要求に対して部分的または権限なしを設定します。
	Bandwidth（帯域幅）	コンソールリダイレクトに使用する帯域幅を調整します。
	Compression Mode（圧縮方式）	圧縮方式を設定します。
	DCT Quantization（DCT量子化）	コンソールリダイレクトのイメージ品質を調整します。0（高品質）-7（高パフォーマンス）
Keyboard（キーボード）		キーボードレイアウトを切り替えます。
Send keys（キー送信）	Hold Down（押したまま）	クライアントデバイスの選択したキーを押したままにします。
	Press and Release（押す／離す）	クライアントデバイスの選択したキーを押したり離したりします。
Hot Keys（ホットキー）	Add Hot Keys（ホットキーの追加）	新しいホットキーを作成します。**Add Hot keys（ホットキーの追加）> Add（追加）**をクリックして、テキストボックスにカーソルを置き、キーの組み合わせを押してマクロを定義します。
Video Record（ビデオ録画）	Record Video（ビデオ録画）	コンソールリダイレクト画面の録画を開始します。
	Stop Recording（録画停止）	コンソールリダイレクト画面の録画を停止します。
	Record Settings（録画設定）	ビデオ録画の設定をします。

Power（電源）	電源制御機能をリモートで実行します。
Active Users（アクティブユーザー）	サーバー上で現在アクティブなユーザーを表示します。
Help（ヘルプ）	H5Viewerの追加情報を表示します。
Browse File（ファイルの参照）	物理DVD/CD-ROMドライブなどディスクメディア、または .isoなどのメディアイメージを追加または変更し、**Start Media（メディアの開始）**をクリックしてリダイレクトを開始／停止します。
Start Media（メディア再生）	メディアファイルのリダイレクトを開始/停止します。

5.10.5 Smart BIOS

Smart BIOS（スマートBIOS）機能では、BIOSファイルを手動でアップロードしたり、デバイスの電源を入れてBIOSの更新や修復を実行できない場合にBIOSキャッシュからアップロードして、デバイスのBIOSを更新することができます。また、BIOSユーザープロファイルと設定のバックアップと復元を行うこともできます。

- この機能を使用できるかどうかは、BIOSとBMCファームウェアに依存します。
- クライアントデバイスは、シャットダウン後にBIOSの更新を開始します。更新に時間がかかる場合がありますので、更新が終了するまでお待ちください。BIOSフラッシュが終了すると、クライアントデバイスが再起動します。

BIOSフラッシュ中は、絶対に電源を切らないでください。

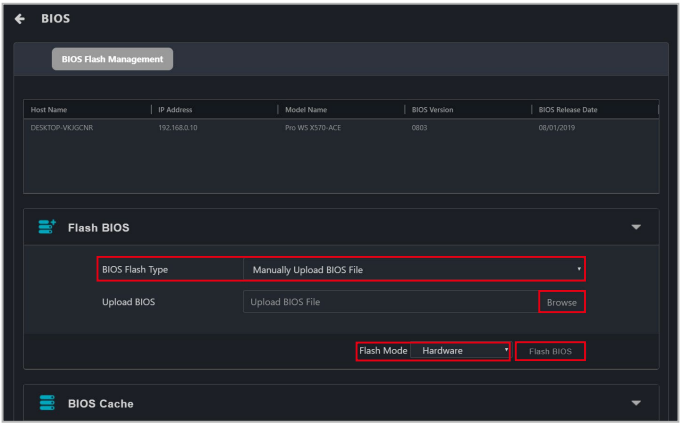
BIOSファイルを手動でアップロードしてBIOSをフラッシュ

BIOSファイルを手動でアップロードして、クライアントデバイスのBIOSをフラッシュします。

1. **BIOS Flash Type（BIOSのフラッシュタイプ）**欄から**Manually Upload BIOS File（BIOSファイルを手動でアップロード）**を選択します。
2. **Browse（参照）**をクリックしてBIOSファイルを選択し、続いて**OK**をクリックして、BIOSファイルが正常にアップロードされたことを確認します。アップロードされたBIOSファイルは**BIOS Cache（BIOSキャッシュ）**にも追加されます。

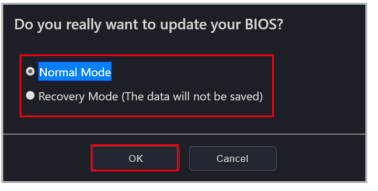
3. **Flash BIOS（BIOSのフラッシュ）**をクリックします。

Flash Mode（フラッシュモード）の既定値は**Hardware Mode（ハードウェアモード）**です。



4. **Normal Mode（通常モード）**または**Recovery Mode（回復モード）**でBIOSをフラッシュするかを選択し、**OK**をクリックします。

Recovery Mode（回復モード）でBIOSをフラッシュすると、すべてのBIOS設定がリセットされ、以前の設定内容が削除されます。



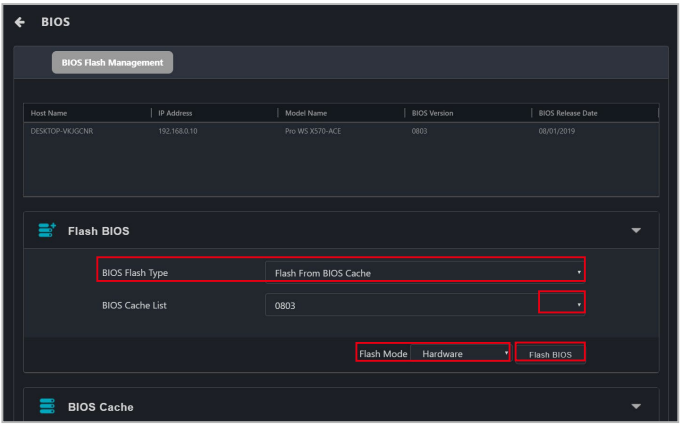
BIOSをBIOSキャッシュからフラッシュ

BIOSキャッシュからBIOSファイルを選択します。

1. **BIOS Flash Type（BIOSのフラッシュタイプ）**欄から**Flash from BIOS Cache（BIOSキャッシュからフラッシュ）**を選択します。
2. **BIOS Cache List（BIOSキャッシュ一覧）**ドロップダウンメニューからBIOSファイルを選択します。

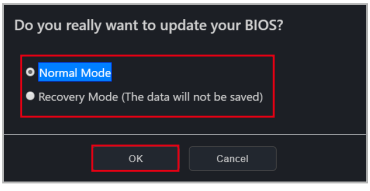
3. **Flash BIOS（BIOSのフラッシュ）**をクリックします。

Flash Mode（フラッシュモード）の既定値は**Hardware Mode（ハードウェアモード）**です。

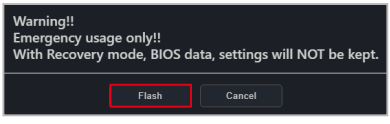


4. **Normal Mode（通常モード）**または**Recovery Mode（回復モード）**でBIOSをフラッシュするかを選択し、**OK**をクリックします。

Recovery Mode（復元モード）でBIOSをフラッシュすると、すべてのBIOS設定がリセットされ、以前の設定内容が削除されます。

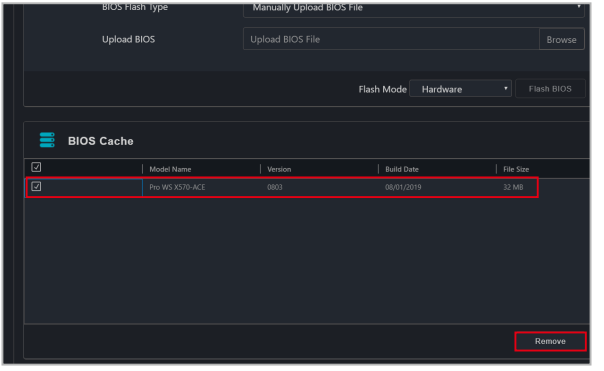


5. **Recovery Mode（回復モード）**では以前のBIOSデータと設定がすべて削除されるため、**Recovery Mode（回復モード）**を選択すると警告メッセージが表示されます。**Flash（フラッシュ）**をクリックし、**Recovery Mode（回復モード）**での使用を続行します。



BIOSキャッシュからBIOSファイルを削除

クライアントデバイスで使用可能なBIOSファイルがBIOS Cashe（BIOSキャッシュ）リストに表示されます。BIOSキャッシュからBIOSファイルを削除する場合は、削除するBIOSファイルを選択し、**Remove（削除）**をクリックします。



BIOSユーザープロファイルデータのダウンロード

- この機能を使用できるかどうかは、BIOS、IPMI、BMCファームウェアに依存します。
- BIOSユーザープロファイルデータをダウンロードする前に、クライアントデバイスのオペレーティングシステムが起動を完了していることを確認してください。
- ファームウェアの更新後は、BIOSユーザープロファイルデータをダウンロードする前に、クライアントデバイスを再起動してください。
- BMCを使用して保存されたユーザープロファイルデータは、クライアントデバイスのBIOS Setup Utilityで作成されたユーザープロファイルの設定ファイルとは互換性はありません。

1. デバイスリストからクライアントデバイスを選択します。
2. **ダウンロードパス**と**ファイル名**を入力します。
3. **Download**（**ダウンロード**）をクリックして、BIOSユーザープロファイルデータ（.CMO）をダウンロードします。

BIOSユーザープロファイルデータのアップロード

- BIOSユーザープロファイルデータがアップロードされると、クライアントデバイスは次回起動時にBIOS設定を自動的に更新します。BIOS設定の更新中は、クライアントデバイスの電源を切ったりしないでください。
- BIOSユーザープロファイルデータの更新をキャンセルするには、クライアントデバイスを再起動する前に**Cancel**（**キャンセル**）をクリックします。
- 保存したBIOSユーザープロファイルデータのBIOSバージョンとクライアントデバイスのBIOSバージョンは同じである必要があります。
- OOB-制御によるBIOS更新とBIOSユーザープロファイルデータの更新タスクを同時に実施することはおすすめしません。
- BIOSユーザープロファイルデータをアップロードする前に、現在のBIOSユーザープロファイルデータデータがバックアップされていることを確認してください。

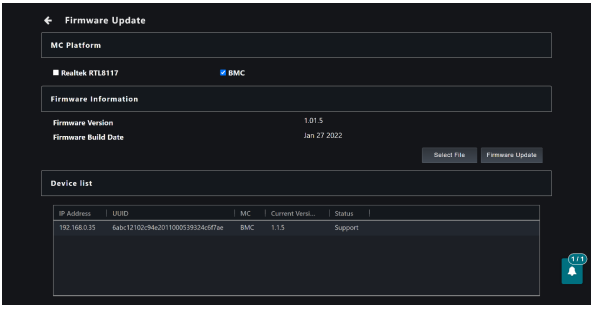
1. **アップロードファイルパス**と**ユーザープロファイルパスワード**（任意）を入力します。
2. **Upload**（**アップロード**）をクリックして、単一クライアントデバイスを更新するか、**Upload all devices**（**すべてのデバイスにアップロード**）をクリックして複数のクライアントデバイスを更新します。
3. アップロードが完了したら、クライアントデバイスを再起動します。

5.10.6　ファームウェア更新

Firmware Update（ファームウェア更新）機能を使用すればBMCリモート管理コントローラーのファームウェアを更新し、更新の結果を確認することができます。

ファームウェアのアップロードと更新

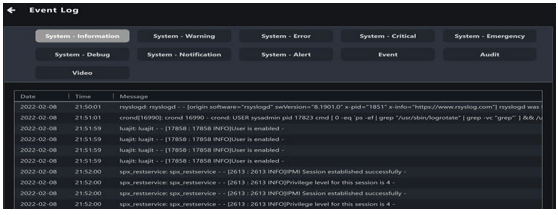
1. **MC Platform（MCプラットフォーム）**の**BMC**をチェックします。
2. **Select File（ファイルの選択）**をクリックし、ファームウェアファイル（.img）を選択して**Open（開く）**をクリックします。
3. **Firmware Update（ファームウェア更新）**をクリックし、更新が完了するまで待ちます。
4. ファームウェアの更新結果は、ミッションセンターで確認することができます。
5. クライアントデバイスが電源オンの状態でファームウェアを更新した場合、更新後にデバイスを再起動してください。



5.10.7 イベントログ

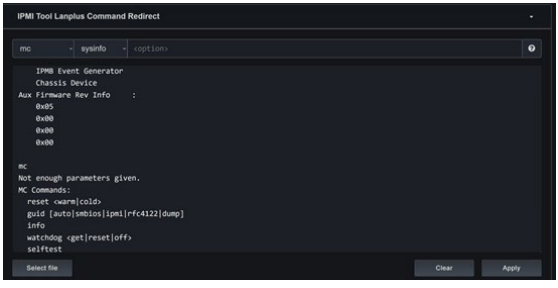
クライアントデバイスの最後の電源投入時のイベントログを見ることができ、問題やトラブルの原因を分析するための情報を取得することができます。

通知ルール管理メニューを使用して、イベントログに表示するイベントの通知ルールを追加または編集することができます。通知ルールを設定するには、ダッシュボードの右上のメニューバーにある をクリックし、**Options（オプション）> Rule Management（ルール管理）**を選択します。詳細は、**8.1.2 ルール管理**を参照してください。



5.10.8 IPMI

IPMI Tool Lanplus Command Redirectは、リモートでコマンドを実行し、コマンドをリモートで実行して設定を構成したり、クライアントデバイスの情報を表示することができます。



複数のクライアントデバイスでコマンドを実行するには、メインのコントロールパネルに戻り、コマンドを送信するデバイスを選択し、**Select Function（機能の選択）>OOB-Control（OOB-制御）> IPMI > IPMI Tool Lanplus Command Redirect（IPMIツールLanplusコマンドリダイレクト）**を選択します。

FRUデータを書き込むには、次のコマンドを実行してFRUのロックを解除してください:

```
raw 0x30 0x17 0x01
```

FRUのロックが解除されたら、次のコマンドを実行してFRUデータを書き込みます:

```
fru write <fru id> <file>
```

1. ドロップダウンメニューから目的のコマンドを選択します。
2. 必須またはオプションコマンドパラメータを入力ボックスに入力します。

- コマンドパラメータが入力ボックスに表示されます。
- **?**をクリックすると、選択したコマンドの追加情報が表示されます。

3. （任意）.binファイルをアップロードするには、**Select File（ファイルの選択）**をクリックします。
4. **Apply（適用）**をクリックしてコマンドを実行します。コマンドの進行状況はミッションセンターで確認することができます。完了したコマンドの結果は、IPMI Toolウィンドウに表示されます。

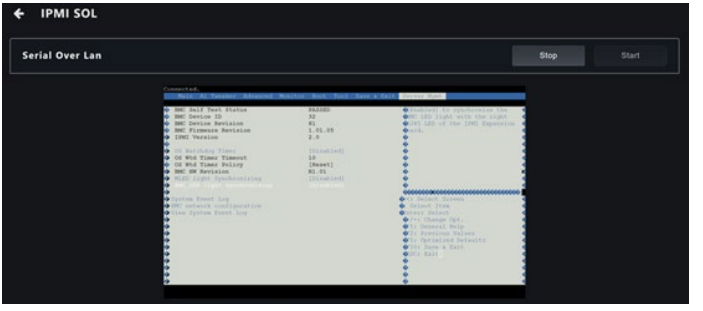
複数のデバイスでコマンドを実行した場合は、デバイスリストのデバイス名をクリックすると、コマンドの実行結果が表示されます。

5. （任意）**Clear（消去）**をクリックするとIPMI Toolウィンドウをクリアされます。

5.10.9 IPMI Serial-over-LAN (SOL)

Serial-over-LAN（SOL）経由でシリアル・コンソールにアクセスすることができます。

1. **Start（開始）**をクリックして、クライアントデバイスのBMC経由のSerial-over-LANを開始します。
2. **Stop（停止）**をクリックして、クライアントデバイスのBMC経由のSerial-over-LANを停止します。

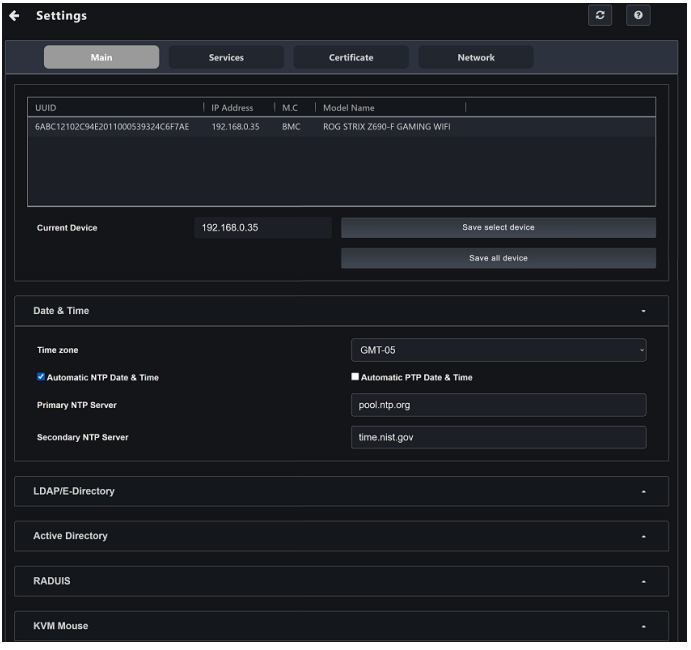


5.10.10 設定

BMC関連の設定をすることができます。

1. 設定を変更した後、**Save select device（選択したデバイスを保存）**をクリックして選択したクライアントデバイスを新しい設定で更新するか、**Save all devices（すべてのデバイスを保存）**をクリックしてすべてのBMCデバイスを新しい設定で更新します。
2. をクリックし、変更がコミットされたことを確認します。オペレーションのステータスはミッションセンターでも確認することができます。

をクリックすると、設定に関する追加情報が表示されます。



日付と時刻

BMCの日付と時刻を設定することができます。

Select Time Zone（タイムゾーンの選択）	ドロップダウンメニューからタイムゾーンを選択します。
Automatic NTP Date & Time（NTP自動日時設定）	NTPサーバーとの日時と時刻の自動同期機能の有効/無効を設定します。
Primary NTP Server*（プライマリNTPサーバー）	日時と時刻を同期する第1 NTPサーバーを設定します。
Secondary NTP Server*（セカンダリNTPサーバー）	日時と時刻を同期する第2 NTPサーバーを設定します。
Automatic PTP Date & Time（PTP自動日時設定）	PTPサーバーとの日時と時刻の自動同期機能の有効/無効を設定します。
PTP Interface*（PTPインターフェース）	PTP サーバーインターフェイスを設定します。
PTP Preset*（PTPプリセット）	PTPプリセットタイプをSlaveOnlyまたはMasterSlaveモードに設定します。（既定値: SlaveOnly）
PTP Transport*（PTP転送）	PTP転送タイプをIPv4またはEthernetモードに設定します。（既定値: IPv4）
PTP Ipmode*（PTP IPモード）	PTP IPモードをユニキャストまたはマルチキャストモードに設定します。
PTP Unicast IP*（PTPユニキャストIP）	ユニキャストモード時のマスターIPアドレスを設定します。
PTP Delay Mechanism*（PTP遅延メカニズム）	PTP遅延メカニズムをE2EまたはP2Pに設定します。（既定値: E2E）
PTP Inbound Latency*（PTP受信遅延）	PTP受信遅延をナノ秒単位で設定します。（既定値: 0ns）
PTP Outbound Latency*（PTP送信遅延）	PTP送信遅延をナノ秒単位で設定します。（既定値: 0ns）
PTP Priority1*（PTP優先順位1）	PTPクロックの優先順位を設定します。マスターは0 - 128、スレーブは255の間で設定します。
PTP Max Master Capacity*（PTP最大マスター容量）	PTPクロックの最大マスター容量を設定します。（既定値: 5）
PTP Log Request Delay*（PTPログ要求遅延）	PTPログ要求遅延を設定します。（既定値: 1）
Panic Mode*（パニックモード）	PTPクロックに1秒以上の誤差が生じた場合にリセットしないように設定します。（既定値: オフ）

アスタリスク（*）の付いたアイテムは、**Automatic NTP Date & Time（NTP自動日時設定）**または**Automatic PTP Date & Time（PTP自動日時設定）**がチェックされている場合にのみ使用することができます。

LDAP/Eディレクトリ

LDAP/Eディレクトリを設定することができます。

Enable LDAP/E-Directory Authentication（LDAP/E-Directory認証の有効化）	LDAP/Eディレクトリ認証の有効/無効を設定します。
Encryption Type（暗号化の種類）	LDAP/Eディレクトリの暗号化の種類を暗号化なし、SSL、STARTTLSに設定します。
Common Name Type（共通名の種類）	共通名の種類をIPアドレスまたはFQDNに設定します。
Server Address（サーバーアドレス）	LDAP/Eディレクトリサーバーアドレスを設定します。
Port（ポート）	LDAP/Eディレクトリポートを入力します。
Bind DN（バインドDN）	バインド操作でクライアントの認証に使用するバインドDNを設定します。
Password（パスワード）	バインド時にクライアントの認証に使用するパスワードを設定します。
Search Base（検索ベース）	LDAP/Eディレクトリサーバーが外部ディレクトリツリーのどの部分を検索するかを設定します。
Attribute of User Login（ユーザーログインの属性）	クライアントの識別に使用する属性を設定します。
CA Certificate File*（CA証明書ファイル）	信頼されたCA証明書ファイルを選択します。
Certificate File*（証明書ファイル）	クライアント証明書ファイルを選択します。
Private Key*（秘密キー）	秘密キーファイルを選択します。

アスタリスク（*）の付いたアイテムは、**SSL**または**STARTTLS**のチェックボックスが選択されている場合にのみ有効です。

アクティブディレクトリ設定

アクティブディレクトリを設定することができます。

Enable Active Directory Authentication（Active Directory認証の有効化）	Active Directory認証の有効/無効を設定します。
SSL	SSL暗号化の有効/無効を設定します。
Secret Username（シークレットユーザー名）	アクティブディレクトリサーバーの管理者ユーザー名を設定します。
Secret Password（シークレットパスワード）	アクティブディレクトリサーバーの管理者パスワードを設定します。
User Domain Name（ユーザードメイン名）	ユーザーのドメイン名を設定します。
Domain Controller Server Address 1-3（ドメインコントローラーサーバーアドレス 1-3）	少なくとも1つのアクティブディレクトリサーバーのIPアドレスを入力します。

RADIUS 設定

RADIUS認証の有効／無効と、RADIUSサーバーにアクセスするために必要な情報を入力することができます。

Enable RADIUS Authentication（RADIUS認証の有効化）	RADIUS認証の有効/無効を設定します。
Server Address（サーバーアドレス）	RADIUSサーバーアドレスを設定します。
Port（ポート）	RADIUSサーバーポートを設定します。
Secret（シークレット）	RADIUSサーバーパスワードを設定します。
Administrator*（管理者）	RADIUS管理者属性を設定します。
Operator*（オペレーター）	RADIUSオペレーター属性を設定します。
User*（ユーザー）	RADIUSユーザー属性を設定します。
OEM Proprietary*（OEM専用）	RADIUS OEM独自属性を設定します。
No Access*（アクセスなし）	RADIUSアクセスなし属性を設定します。

アスタリスク（*）の付いたアイテムは、サーバー上のRADIUSユーザーのベンダー固有の属性にしたがって設定する必要があります。

KVMマウス設定

マウスモードを設定することができます。

Relative Positioning (Linux)（相対配置）	計算された相対マウス位置の変位をサーバーに送信します。
Absolute Positioning (Windows)（絶対配置）	ローカルマウスの絶対位置をサーバーに送信します。このオプションはWindowsまたはLinuxが推奨されます。
Other Mode (SLES-11 OS Installation)	ローカルマウスから計算された中心位置の変位をサーバーに送信します。

ログ設定

イベントログのログポリシーを設定することができます。

Linear Storage Policy（リニアストレージポリシー）	SELログ設定ポリシーをリニアストレージに設定します。
Circular Storage Policy（サーキュラーストレージポリシー）	SELログ設定ポリシーをサーキュラーストレージに設定します。

ログ詳細設定

イベントログの詳細なログ設定をすることができます。

System Log（システムログ）	システムログを有効に設定すると、すべてのシステムイベントを表示することができます。エントリーは分類レベルに基づいてフィルタリングすることができます。
Local Log（ローカルログ）	この項目をチェックすると、ログがBMCデバイスのローカルに保存されます。
Remote Log（リモートログ）	この項目をチェックすると、リモートマシンにログを保存します。
Port Type（ポートの種類）	ポートの種類をTCPまたはUDPに設定します。
File Size（ファイルサイズ）	ローカルログファイルサイズを3-65535の間でbyte単位で設定します。
Rotate Count（ローテーションカウント）	ログに記録された情報が指定されたファイルサイズを超えると、ローテーションカウントの値に基づいて古いログ情報が自動的にバックアップにローテーションされます。  • ローテーションカウントの値は0または1でなければなりません。 • ローテーションカウントが0の場合、古いログ情報は毎回完全に消去されます。
Remote Log Server（リモートログサーバー）	システムログのリモートサーバーアドレスを設定します。
Remote Server Port（リモートサーバーポート）	システムログのポート番号を設定します。
Enable Audit Log（監査ログの有効化）	この項目を有効に設定すると、クライアントデバイスのすべての監査イベントを表示することができます。

メディアリダイレクト設定

メディアリダイレクトの設定をすることができます。

- この機能を使用できるかどうかは、BMCに依存します。
- アスタリスク（*）の付いたアイテムは、**CIFS**のチェックボックスが選択されている場合にのみ有効です。

Remote Media Support（リモートメディサポート）		リモートメディアサポートの有効/無効を設定します。有効に設定すると、CD/DVD/HDDのリモートメディアタイプが表示されます。ユーザーはリモートメディアの種類ごとに異なる設定を行うことができます。設定オプションは各々のメディアタイプに表示されるか、同じオプションを両方に適用することができます。
Mount CD/DVD（CD/DVD マウント）	**Server Address for CD/DVD Images（CD/DVDイメージのサーバーアドレス）**	リモートビデオが保存されているサーバーアドレスを入力します。
	Path In Server（サーバー内パス）	リモートサーバー上のメディアパスを入力します。
	Share Type for CD/DVD（CD/DVD共有の種類）	共有の種類をNFSまたはSamba（CIFS）に設定します。
	Domain Name*（ドメイン名）	リモートサーバーのドメイン名を入力します。
	Username*（ユーザー名）	リモートサーバーのユーザー名を入力します。
	Password*（パスワード）	リモートサーバーのパスワードを入力します。
	Same Settings for Harddisk Images（ハードディスクイメージに同じ設定を使用）	CD/DVDマウントで入力したサーバー情報を、ハードディスクマウントにも適用します。

Mount Harddisk（ハードディスクマウント）	Server Address for CD/DVD Images（CD/DVDイメージのサーバーアドレス）	リモートビデオが保存されているサーバーのアドレスを入力します。
	Path In Server（サーバー内パス）	サーバー上のリモートメディアのパスを入力します。
	Share Type for CD/DVD（CD/DVD共有の種類）	共有の種類をNFSまたはSamba（CIFS）に設定します。
	Domain Name*（ドメイン名）	（任意）リモートメディアのドメイン名を入力します。
	Username*（ユーザー名）	ユーザー名を入力します。
	Password*（パスワード）	パスワードを入力します。

VMediaインスタンス設定

サポートされているCD/DVDやハードディスクデバイスへの仮想メディアのリダイレクト設定をすることができます。

この機能を使用できるかどうかは、BMCに依存します。

CD/DVD device instances（CD/DVDデバイスインスタンス）	仮想メディアリダイレクトでサポートするCD/DVDデバイス数を選択します。
Hard disk instances（ハードディスクインスタンス）	仮想メディアリダイレクトでサポートするハードディスクデバイス数を選択します。
Remote KVM CD/DVD device instances（リモートKVM CD/DVDデバイスインスタンス）	仮想メディアリダイレクトでサポートするリモートKVM CD/DVDデバイス数を選択します。
Remote KVM hard disk instances(リモートKVMハードディスクインスタンス）	仮想メディアリダイレクトでサポートするリモートKVMハードディスクデバイス数を選択します。
Emulate SD Media as USB disk on the host（ホスト上でSDメディアをUSBディスクとしてエミュレート）	ホスト上でSDメディアをUSBディスクとしてエミュレートする機能の有効/無効を設定します。

メディアリモートセッション設定

リモートセッションの設定をすることができます。

KVM Single Port Application（KVMシングルポートアプリケーション）	BMCにおけるシングルポートアプリケーションサポートの有効/無効を設定します。
Keyboard Language（キーボードの言語）	キーボードの言語を選択します。
Virtual Media Attach Mode（仮想メディアアタッチモード）	仮想メディアアタッチモードを選択します。
Retry Count（再試行回数）	KVM障害発生時の再試行回数を1-20の範囲で設定します。
Retry Time Interval (Seconds)（再試行時間間隔（秒））	再試行から次の再試行まで待機する時間を5-30の範囲で設定します。
Server Monitor OFF Features Status（サーバーモニターオフ機能の状態）	サーバーモニターオフ機能の有効/無効を設定します。
Automatically OFF Server Monitor when KVM Launches（KVM起動時にサーバーモニターを自動オフ）	KVM起動時にクライアントデバイスのモニターを自動的にオフにする機能の有効/無効を設定します。

PAMオーダー設定

BMCへのユーザー認証のPAMオーダーを設定することができます。BMCがサポートするPAMモジュールのリストが表示されます。PAMモジュールをドラッグアンドドロップすることで、順番を変更することができます。

SMTP設定

SMTPメールサーバーを設定することができます。

LAN Interface（LANインターフェース）	設定するLANインターフェースを選択しします。
Sender Email ID（送信者Email ID）	SMTPサーバーで有効な送信者Email IDを入力します。Email IDの最大許容サイズは、ユーザー名とドメイン名を含む64バイトです。
Primary/Secondary SMTP Support*（プライマリ/セカンダリ SMTPサポート）	BMCのSMTPサポートの有効/無効を設定します。
Primary/Secondary Server Name*（プライマリ/セカンダリ サーバー名）	参照目的としてSMTPサーバー名を入力します。
Primary/Secondary Server IP*（プライマリ/セカンダリ サーバーIP）	SMTPサーバーのサーバーアドレスを入力します。
Primary/Secondary SMTP Port*（プライマリ/セカンダリ SMTPポート）	SMTPポートを入力します。
Primary/Secondary Secure SMTP Port*（プライマリ/セカンダリ セキュアSMTPポート）	セキュアSMTPポートを入力します。
Primary/Secondary SMTP Authentication*（プライマリ/セカンダリ SMTP認証）	SMTP認証の有効/無効を設定します。
Primary/Secondary Username*（プライマリ/セカンダリ ユーザー名）	SMTPユーザーアカウントのユーザー名を入力します。
Primary/Secondary Password*（プライマリ/セカンダリ パスワード）	SMTPユーザーアカウントのパスワードを入力します。
Primary/Secondary SMTP SSLTLS Enable*（プライマリ/セカンダリ SMTP SSLTLS 有効）	SMTP SSLTLSプロトコルの有効/無効を設定します。
Primary/Secondary SMTP STARTTLS Enable*（プライマリ/セカンダリ SMTP STARTTLS有効）	SMTP STARTTLSプロトコルの有効/無効を設定します。

アスタリスク（*）の付いたアイテムは、**Primary SMTP Support（プライマリ SMTPサポート）**または**Secondary SMTP Support（セカンダリ SMTPサポート）**のチェックボックスが選択されている場合にのみ有効です。

ファイアウォールIPアドレス規則

ファイアウォールのIPアドレス規則を設定することができます。

IP Single (or) Range Start（単一IPまたはIP範囲の開始）	単一IPアドレスまたは開始IPアドレスを入力します。
IP Range End（IP範囲の終了）	（任意）終了IPアドレスを入力します。
Enable Timeout（タイムアウトの有効化）	タイムアウトの有効/無効を設定します。
Start Date*（開始日）	ファイアウォールIPアドレス規則を開始する日付を設定します。
Start Time*（開始時間）	ファイアウォールIPアドレス規則を開始する時刻を設定します。
End Date*（終了日）	ファイアウォールIPアドレス規則を終了する日付を設定します。
End Time*（終了時間）	ファイアウォールIPアドレス規則を終了する時刻を設定します。
Rule（ルール）	指定したIPアドレスまたはIP範囲を許可/ブロックします。

アスタリスク（*）の付いたアイテムは、**Enable Timeout（タイムアウトの有効化）**のチェックボックスが選択されている場合にのみ有効です。

ファイアウォールIPアドレス既存規則

既存のファイアウォールIPアドレス規則を表示します。既存の規則を削除する場合は、削除したい規則の **X** をクリックします。

ビデオトリガー設定

KVMサーバーの自動録画機能を起動するイベントを設定することができます。

Critical Events (Temperature/Voltage)（重要なイベント（温度/電圧））	自動録画機能トリガーの有効/無効を設定します。
Non-critical Events (Temperature/Voltage)（重要ではないイベント（温度/電圧））	
Non-recoverable Events (Temperature/Voltage)（回復不可能なイベント（温度/電圧））	
Fan State Changed Events（ファン状態変更イベント）	
Watchdog Timer Events（ウォッチドッグタイマーイベント）	
Chassis Power On Events（ケース電源オンイベント）	
Chassis Power Off Events（ケース電源オフイベント）	
Chassis Reset Events（ケースリセットイベント）	
LPC Reset Events（LPCリセットイベント）	
Date and Time Events（日付と時刻イベント）	
Pre-Event Video Recordings（プリイベントビデオ録画）	プリイベントビデオ録画を有効にし、録画をPre-Crash（プリクラッシュ）またはPre-Reset（プリリセット）に設定します。

ビデオリモートストレージ設定

ビデオリモートストレージを設定することができます。

Record Video to Remote Server（リモートサーバへの録画）	リモートビデオサポートの有効/無効を設定します。
Maximum Dumps（最大ダンプ）	ダンプの上限を1-100の範囲で設定します。
Maximum Duration（最大期間）	最大期間を1-3600秒の範囲で設定します。
Maximum Size（最大サイズ）	ダンプの最大サイズを1-500MBの範囲で設定します。
Server Address（サーバーアドレス）	リモートビデオを保存するリモートサーバーの IPアドレスを設定します。
Path in Server（サーバー内パス）	リモートサーバー内のメディアパスを設定します。
Share Type（共有の種類）	共有の種類をNFSまたはSamba（CIFS）に設定します
Domain Name*（ドメイン名）	リモートサーバーのドメイン名を入力します。
Username*（ユーザー名）	リモートサーバーのユーザー名を入力します。
Password*（パスワード）	リモートサーバーのパスワードを入力します。

アスタリスク（*）の付いたアイテムは、**CIFS**のチェックボックスが選択されている場合にのみ有効です。

プリベントビデオ録画設定

プリベントビデオ録画を設定することができます。

プリイベントビデオ録画の有効/無効は、**Video Trigger Settings（ビデオトリガー設定）**で設定することができます。

Video Quality（ビデオ品質）	ビデオ品質を選択します。
Compression Mode（圧縮モード）	圧縮モードを選択します。
Frames Per Second（1秒あたりのフレーム数）	FPS（1秒あたりのフレーム数）を選択します。
Video Duration（ビデオ録画時間）	ビデオの録画時間を秒単位で選択します。

SOLトリガー設定

Serial-over-LAN（SOL）ビデオ録画のトリガーとなるイベントを設定することができます。

Critical Events (Temperature/Voltage)（重要なイベント（温度/電圧））	自動ビデオ録画機能のトリガーの有効/無効を設定します。
Non-critical Events (Temperature/Voltage)（重要ではないイベント（温度/電圧））	
Non-recoverable Events (Temperature/Voltage)（回復不可能なイベント（温度/電圧））	
Fan State Changed Events（ファン状態変更イベント）	
Watchdog Timer Events（ウォッチドッグタイマーイベント）	
Chassis Power On Events（ケース電源オンイベント）	
Chassis Power Off Events（ケース電源オフイベント）	
Chassis Reset Events（ケースリセットイベント）	
LPC Reset Events（LPCリセットイベント）	
Date and Time Events（日付と時刻イベント）	

SOLリモートビデオ設定

Serial-over-LAN（SOL）ビデオ録画の設定をすることができます。

Log Size（ログサイズ）	ログファイルのサイズをKB単位で設定します。（最大128KB）
Log File Count（ログファイル数）	ログファイル数を0-1の範囲で設定します。
Record Video to Remote Server（リモートサーバーに録画）	録画したビデオをBMCではなくリモートサーバーに保存する機能の有効/無効を設定します。
Server Address*（サーバーアドレス）	リモートビデオを保存するリモートサーバーのIPアドレスを設定します。
Path in Server*（サーバー内パス）	リモートサーバー上のメディアパスを設定します。
Share Type*（共有の種類）	共有の種類をNFSまたはSamba（CIFS）に設定します。
Domain Name*（ドメイン名）	リモートサーバーのドメイン名を入力します。
Username*（ユーザー名）	リモートサーバーのユーザー名を入力します。
Password*（パスワード）	リモートサーバーのパスワードを入力します。

アスタリスク（*）の付いたアイテムは、**Record Video to Remote Server（リモートサーバーに録画）**または**CIFS**のチェックボックスが選択されている場合にのみ有効です。

SOL録画ビデオ

Serial-over-LAN（SOL）ビデオ録画で撮影されたビデオが表示されます。クリックすることでビデオをダウロードして保存することができます。ビデオを削除するには削除したいビデオの **X** をクリックします。

SOL構成

SOL構成オプションを変更することができます。

この機能を使用できるかどうかは、クライアントデバイスのBMCに依存します。

Volatile Bit Rate（揮発性ビットレート）	揮発性ビットレートを設定します。
Non-volatile Bit Rate（不揮発性ビットレート）	不揮発性ビットレートを設定します。

ファンモード

現在のファンモードの確認およびファンモードを切り替えることができます。

特定のファンモードを使用できるかどうかは、クライアントデバイスのBMCに依存します。

Generic Mode（汎用モード）	クライアントデバイスのファンを汎用モードに設定します。
Full Speed Mode（フルスピードモード）	クライアントデバイスのファンをフルスピードモードに設定します。
Silent Mode（サイレントモード）	クライアントデバイスのファンをサイレントモードに設定します。
Turbo Mode（ターボモード）	クライアントデバイスのファンをターボモードに設定します。

ファンカスタマイズ

ファンカーブをカスタマイズすることができます。

この機能を使用できるかどうかは、クライアントデバイスのBMCに依存します。

ファン温度ソース

ファン回転数を制御するための温度センサーを選択することができます。

- 温度情報が利用できない場合は、CPU温度が使用されます。CPU温度も利用できない場合、ファン回転数はデフォルトで60%になります。
- ケースファン（CHA_FAN）センサーと制御機能を使用するには、ファンが対応するファンヘッダーに接続され、6ピンPSUコネクターが電源に接続されていることをご確認ください。
- ファン速度制御のサポートは、BMC、マザーボード、BIOS、ファームウェアに依存します。

電源装置冗長化

電源装置の冗長化を行うことで万が一電源に障害が発生した際も、冗長化した電源により電力を供給し電源断を防止することができます。

PSU Redundancy（電源装置冗長化）	電源装置冗長化の有効/無効を設定します。

電源装置冗長化を使用するには、PSU PM_BUSヘッダーとSMART_PSUスイッチジャンパーをアクティブにする必要があります。

サービスウェブ設定

ウェブサービスを設定することができます。

Active（アクティブ）	ウェブサービスの有効/無効を設定します。
Interface Name（インターフェース名）	ウェブサービスに使用するインターフェースを選択します。
Secure Port（セキュアポート）	ウェブサービスに使用するセキュアポートを入力します。（デフォルト: 443）
Timeout（タイムアウト）	セッションタイムアウト時間を60秒単位、300-1800秒の範囲で設定します。
Maximum Sessions（最大セッション数）	許可する最大セッション数を表示します。

サービスKVM設定

KVMサービスの設定をすることができます。

Active（アクティブ）	KVMサービスの有効/無効を設定します。
Interface Name（インターフェース名）	KVMサービスに使用するインターフェースを選択します。
Secure Port（セキュアポート）	KVMサービスに使用するセキュアポートを入力します。（デフォルト: 443）
Timeout（タイムアウト）	セッションタイムアウト時間を60秒単位、300-1800秒の範囲で設定します。
Maximum Sessions（最大セッション数）	許可する最大セッション数を表示します。

サービスCD-Media設定

CD-Mediaサービスの設定をすることができます。

Active（アクティブ）	CD-Mediaサービスの有効/無効を設定します。
Interface Name（インターフェース名）	CD-Mediaサービスに使用するインターフェースを選択します。
Secure Port（セキュアポート）	CD-Mediaサービスに使用するセキュアポートを入力します。（デフォルト: 443）
Maximum Sessions（最大セッション数）	許可する最大セッション数を表示します。

サービスHD-Media設定

HD-Mediaサービスの設定をすることができます。

Active（アクティブ）	HD-Mediaサービスの有効/無効を設定します。
Interface Name（インターフェース名）	HD-Mediaサービスに使用するインターフェースを選択します。
Secure Port（セキュアポート）	HD-Mediaサービスに使用するセキュアポートを入力します。（デフォルト: 443）
Maximum Sessions（最大セッション数）	許可する最大セッション数を表示します。

サービスSSH設定

SSHサービスの設定をすることができます。

Active（アクティブ）	SSHサービスの有効/無効を設定します。
Interface Name（インターフェース名）	SSHサービスに使用するインターフェースを選択します。
Secure Port（セキュアポート）	SSHサービスに使用するセキュアポートを入力します。（デフォルト: 22）
Timeout（タイムアウト）	セッションタイムアウト時間を60秒単位、300-1800秒の範囲で設定します。
Maximum Sessions（最大セッション数）	許可する最大セッション数を表示します。

SSL証明書生成

SSL証明書を生成することができます。**Generate（生成）**チェックボックスをクリックすると、SSL証明書生成セクションが表示されます。

Common Name (CN)（共通名）	生成される証明書の共通名を設定します。
Organization (O)（組織）	生成される証明書の組織を設定します。
Organization Unit (OI)（組織単位）	生成される証明書の組織単位を設定します。
City or Locality (L)（都市または地域）	組織の都市または地域を設定します。
State or Province (ST)（州または県）	組織の州または県を設定します。
Country (C)（国）	組織の国を設定します。
Email Address（メールアドレス）	組織のメールアドレスを設定します。
Valid For（有効期間）	生成される証明書の要求された有効期間を、1-3650日の範囲で設定します。
Key Length（キーの長さ）	生成する証明書のキーの長さをビットで設定します。

SSL証明書アップロード

SSL証明書をアップロードすることができます。**Upload（アップロード）**チェックボックスをクリックすると、SSL証明書アップロードセクションが表示されます。

Current Certificate（現在の証明書）	現在の証明書の日付と時刻を表示します。
New Certificate（新しい証明書）	アップロードする新しい証明書ファイルを選択します。
Current Private Key（現在の秘密キー）	現在の秘密キーの日付と時刻を表示します。
New Private Key（新しい秘密キー）	アップロードする新しい秘密キーファイルを選択します。

現在の証明書情報

現在の証明書に関する情報を表示することができます。

ネットワークIP設定

インターフェースのLANサポートを管理することができます。

Enable LAN（LAN有効）	選択したLANサポートの有効/無効を設定します。
LAN Interface（LANインターフェース）	設定するインターフェースを選択します。
MAC Address（MACアドレス）	選択したインターフェースのMACアドレスを表示します。
Enable IPv4（IPv4有効）	選択したインターフェースのIPv4の有効/無効を設定します。
Enable IPv4 DHCP（IPv4 DHCP有効）	Dynamic Host Configuration Protocol（DHCP）を使用したIPv4アドレス動的設定の有効/無効を設定します。
IPv4 Address*（IPアドレス）	静的IPv4アドレスを設定します。

IPv4 Subnet*（IPv4サブネット）	静的サブネットマスクを設定します。
IPv4 Gateway*（IPv4ゲートウェイ）	静的デフォルトゲートウェイを設定します。
Enable IPv6（IPv6有効）	選択したインターフェースのIPv6の有効/無効を設定します。
Enable IPv6 DHCP（IPv6 DHCP有効）	Dynamic Host Configuration Protocol（DHCP）を使用したIPv6アドレス動的設定の有効/無効を設定します。
IPv6 Index*（IPv6インデックス）	IPv6インデックスを設定します。
IPv6 Address*（IPv6アドレス）	静的IPv6アドレスを設定します。
Subnet Prefix Length*（サブネットプレフィックス長）	IPv6サブネットプレフィックス長を設定します。
IPv6 Gateway*（IPv6ゲートウェイ）	IPv6ゲートウェイを設定します。
Enable VLAN（VLAN有効）	選択したインターフェースのVLANサポートの有効/無効を設定します。
VLAN ID	VLAN IDを設定します。
VLAN Priority（VLAN優先度）	VLAN優先度を設定します。

アスタリスク（*）の付いたアイテムは、**IPv4/IPv6**が有効で**DHCP**が無効に設定されている場合にのみ有効です。

ネットワークDNS設定

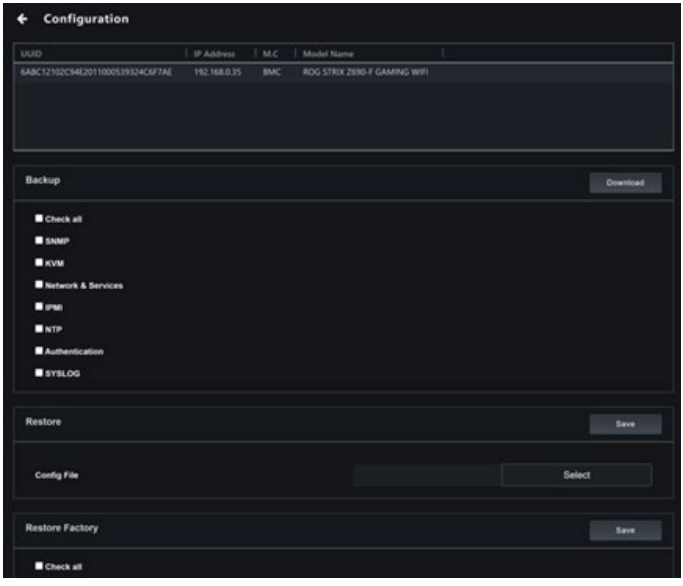
DNS設定を管理することができます。

DNS Enabled（DNS有効）	DNSサービスの有効/無効を設定します。
mDNS Enabled（mDNS有効）	マルチキャストDNSの有効/無効を設定します。
Host Name Setting（ホスト名設定）	ホスト名設定の自動/手動を設定します。
Host Name（ホスト名）	ホスト名が手動に設定されている場合、ホスト名を設定します。
BMC Interface（BMCインターフェース）	BMCインターフェース名を表示します。
Register BMC（BMCの登録）	BMC登録の有効/無効を設定します。
Registration Method（登録方法）	登録方法を選択します: - **Nsupdate**: nsupdateアプリケーションを使用してDNSに登録します。 - **DHCP Client FQDN**: DHCPオプション81を使用してDNSサーバーに登録します。 - **Hostname**: DHCPオプション12を使用してDNSサーバーに登録します。
TSIG Authentication Enabled（TSIG認証有効）	TSIG認証の有効/無効を設定します。
Current TSIG Private File Info（現在のTSIGプライベートファイル情報）	TSIG認証が有効に設定されている場合、現在のTSIGプライベートファイルの日時情報が表示されます。
New TSIG Private File（新しいTSIGプライベートファイル）	TSIG認証が有効に設定されている場合、アップロードする新しいTSIGプライベートファイルを選択します。

Domain Setting（ドメイン設定）	ドメイン設定の自動/手動を設定します。
Domain Interface（ドメインインターフェース）	ドメイン設定が自動に設定されている場合、ドメインインターフェースを設定します。
Domain Name（ドメイン名）	ドメイン設定が手動に設定されている場合、ドメイン名を設定します。
Domain Name Server Setting（ドメインネームサーバー設定）	ドメインネームサーバー設定の自動/手動を設定します。
IP Priority（IP優先度）	ドメインネームサーバーが自動に設定されている場合、IP優先度を設定します。
DNS Server 1-3（DNSサーバー1-3）	ドメインネームサーバーが手動に設定されている場合、DNSサーバーを設定します。

5.10.11 構成

設定のバックアップ、復元、工場出荷時にリセットを行うことができます。



バックアップ

1. 設定をバックアップするには、バックアップしたい項目をチェックするか、**Chekc All（すべてチェック）**をクリックしてすべての項目をチェックします。
2. **Download（ダウンロード）**をクリックすると、バックアップの保存先に設定情報が保存されます。

復元

1. バックアップから設定を復元するには、**Select（選択）**をクリックし以前作成したバックアップファイルを選択します。
2. **Save（保存）**をクリックすると、クライアントの設定がバックアップファイルから復元されます。

出荷時の設定に戻す

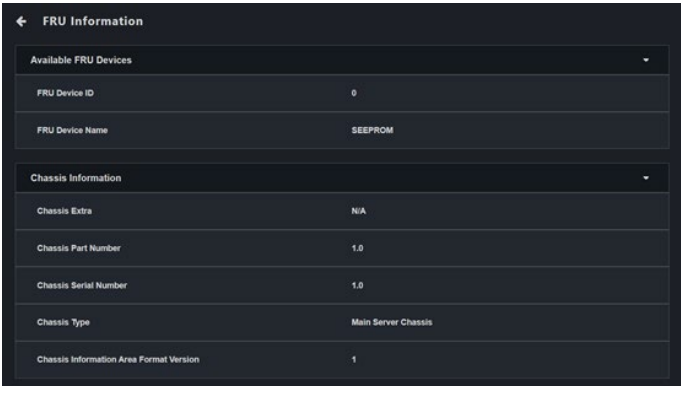
1. 設定を工場出荷時の状態にリセットするには、リセットしたい項目をチェックするか、**Chekc All（すべてチェック）**をクリックしてすべての項目をチェックします。
2. **Download（ダウンロード）**をクリックすると、バックアップの保存先に設定情報が保存されます。

一度設定を工場出荷時の状態にリセットすると、元に戻すことはできません。工場出荷時の状態にリセットする前に、現在の設定のバックアップを作成することをおすすめします。

5.10.12 FRU情報

BMCのFRU（Field Replaceable Unit）デバイスに関する基本情報、ケース情報、ボード情報、生産情報などが表示されます。

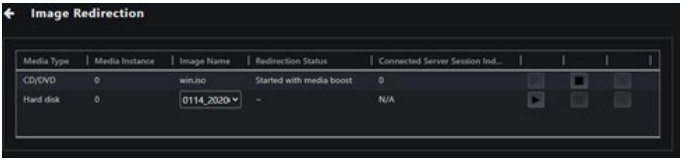
FRUデータを書き込むには、**5.10.8 IPMI**を参照してください。



5.10.13 イメージリダイレクト

BMCを介してメディアとしてホストするリモートメディアを選択することができます。利用可能なイメージの表示、クリア、リダイレクトを開始することができます。

- この機能を使用できるかどうかは、BMCに依存します。
- イメージのリダイレクトには管理者権限が必要です。
- イメージを設定するにはRemote Media Support（リモートメディアサポート）を有効にする必要があります。Settings（設定） > Media Redirection（メディアリダイレクト） > General Setting（全般設定）
- サポートしているCD/DVDフォーマット: ISO9660、UDF(v1.02~v2.60)
- サポートしているCD/DVDメディアファイルタイプ: (*.iso)、(*.nrg)
- サポートしているHDDメディアファイルタイプ: (*.img), (*.ima)
- 最大メディアファイルサイズ: 5GB



ローカルメディアのリダイレクト

Start Redirection（リダイレクト開始）	選択したイメージをリダイレクトします。
Stop Redirection（リダイレクト停止）	リモートイメージリダイレクトを停止します。
Upload image（イメージのアップロード）	イメージをクライアントデバイスにアップロードします。 • アップロードが完了するまでBMC機能は使用できません。アップロード時間はネットワークの状況とファイルサイズによって異なります。 • 進行中のアップロードがキャンセルされた場合、システムが変更をロールバックしている間BMC機能は使用できません。ロールバックが完了しない場合は、クライアントデバイスの再起動をお試しください。
Clear（消去）	選択したイメージをBMCから消去します。

リモートメディアのリダイレクト

Start Redirection（リダイレクト開始）	選択したイメージをリダイレクトします。
Stop Redirection（リダイレクト停止）	リモートイメージリダイレクトを停止します。
Clear（消去）	選択したイメージをBMCから消去します。

5.10.14 プラットフォームイベントフィルター

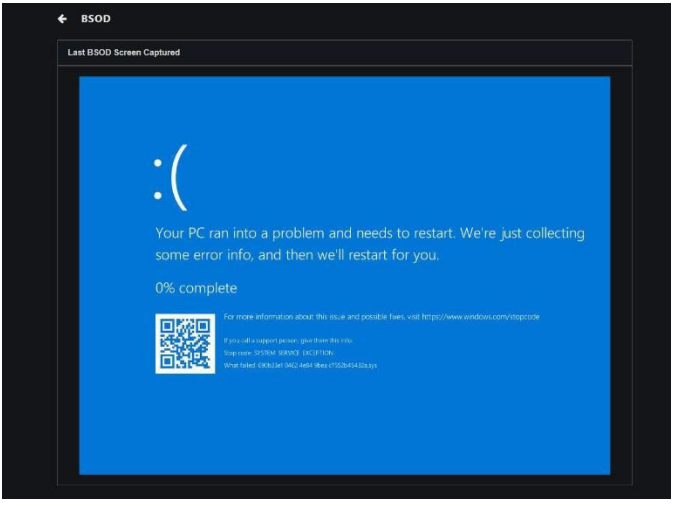
クライアントデバイスのBMCウェブコンソールに接続して、プラットフォームのイベントフィルター設定、アラートポリシー、LANの宛先を管理することができます。

ASUS Control Center Expressに戻るには、ウェブコンソールの左サイドバーで**Sign Out（サインアウト）**をクリックします。

5.10.15 BSODキャプチャー

システム異常の調査と診断を支援するために、BMCデバイスによってキャプチャーされたBSoD（Blue Screen of Death）を表示します。

BSODキャプチャーを有効にするには、**Settings（設定）> Services（サービス）> KVM** でKVMサービスを有効にする必要があります。



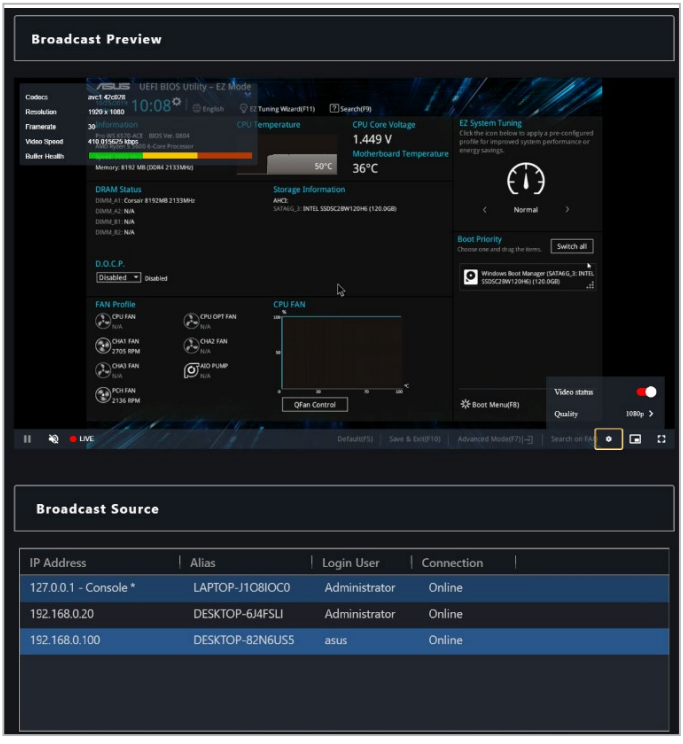
5.10.16 エラーコード

0x83100002	クライアントデバイスがBMCをサポートしていません。
0x83100003	コマンドが無効。
0x83100025	CMOSをクリアするには、クライアントデバイスの電源をオフにする必要があります。
0x83100026	SPIコネクターがマザーボードのIPMI TPMコネクター接続されていることを確認してください。
0x83100033	BMCウェブインターフェースに接続できませんでした。
0x83100034	BMCログイン認証情報が間違っています。
0x83100006	BMC機能を同期できませんでした。ネットワーク接続状態を確認して、再試行してください。問題が解決しない場合は、クライアントデバイスをシャットダウンして電源をオフにしてから、クライアントデバイスを再起動してください。
0x831F4077	クライアントデバイスでBMCにログインできませんでした。クライアントデバイスでBMCが正常に動作しているか確認するか、BMCログイン認証情報を再度入力して再試行してください。問題が解決しない場合は、クライアントデバイスをシャットダウンして電源をオフにしてから、クライアントデバイスを再起動してください。
0x831F4038	クライアントデバイス上のBMCから応答がありません。問題が解決しない場合は、クライアントデバイスをシャットダウンして電源をオフにしてから、クライアントデバイスを再起動してください。

5.11　スクリーンブロードキャスト

スクリーンブロードキャストでは、クライアントデバイスの画面、ビデオカメラデバイスにアクセスし、1対1または1対多で選択したクリップをブロードキャストすることができ、ブロードキャストするビデオまたはクリップの解像度、ビデオ品質、オーディオ品質を選択することもできます。

スクリーンブロードキャスト機能を利用するには、メインメニュー画面でブロードキャストルームを作成したいデバイスを選択し、**Select Function（機能の選択）**のドロップダウンメニューから**Screen Broadcast（スクリーンブロードキャスト）> Create a broadcast（ブロードキャストルームを作成）**を選択します。すでにブロードキャストルームが作成されている場合は、**Select Function（機能の選択）**ドロップダウンメニューから**Screen Broadcast（スクリーンブロードキャスト）>** 作成したブロードキャストルームを選択します。



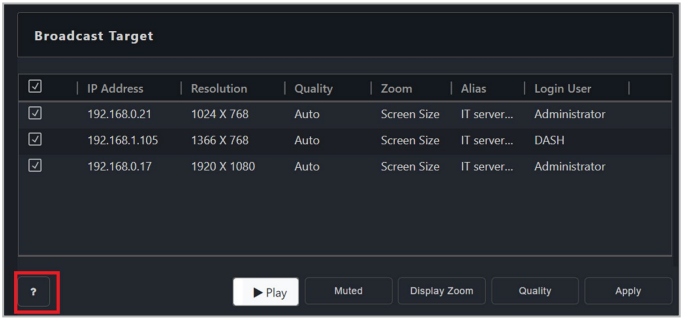
ブロードキャストルームの概要

Room Name（ルーム名）	ブロードキャストルーム名を入力します。
Broadcast Source（ブロードキャストソース）	ブロードキャストソースとなるデバイスを選択します。
Input Type（入力タイプ）	ブロードキャストソースのタイプを選択します。
Broadcast Target（ブロードキャスト対象）	ブロードキャストしたいターゲットを選択します。
Play/Stop（再生/停止）	ブロードキャストの再生・停止を行います。
Muted（ミュート）	ブロードキャスト時に、ブロードキャスト対象の音声をミュート/ミュート解除します。
Display Zoom（表示倍率）	ブロードキャストの画面サイズを選択します。
Quality（画質）	ブロードキャストの解像度を選択します。
Create（作成）	設定した内容でブロードキャストを作成します。 既存のブロードキャストルームを編集している場合、このオプションは利用できません。
Apply（適用）	ブロードキャストルームの設定を変更した内容を適用します。 新規にブロードキャストルームを作成する場合は、このオプションは利用できません。

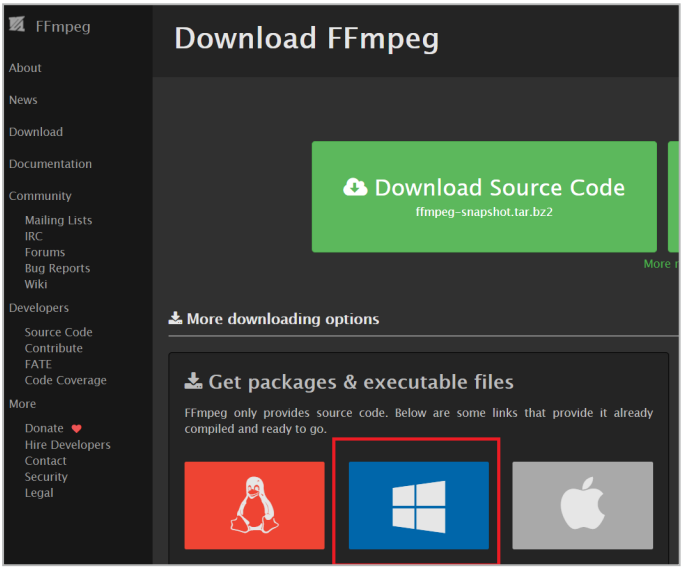
- メインサーバーはブロードキャストソースに記されます。ビデオファイルのブロードキャストは、メインサーバーがブロードキャストソースとして選択されている場合のみ可能です。ディスプレイデバイスおよびカメラデバイスは、どのブロードキャストソースからでもブロードキャストできます。
- 選択した入力タイプとその対応する解像度によって、解像度が異なる場合があります。

5.11.1 ブロードキャスト環境の設定

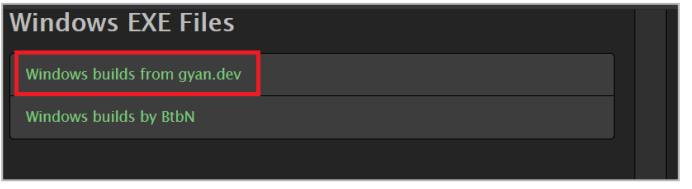
スクリーンブロードキャスト機能を使用する前に、メインサーバーの再生環境をブロードキャスト機能用に設定してください。ブロードキャスト機能の再生環境設定については、次の手順をご参照いただくか、ブロードキャストルームの左下にある ? をクリックしてください。



1. FFmpeg（https://ffmpeg.org/）にアクセスしてダウンロードページへ移動し、**Get packages&executable files**のWindows マークをクリックします。



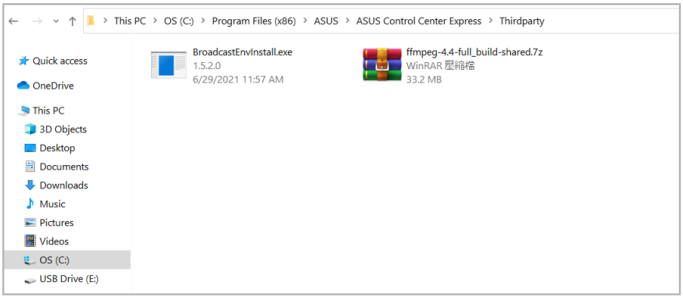
2. **Windows builds from gyan.dev** をクリックします。



3. **ffmpeg-release-full-shared.7z**ファイルを選択してダウンロードします。

ffmpeg バージョン 4.4 / 5.0.1 / 5.1.2 のいずれかをダウンロードすることをおすすめします。

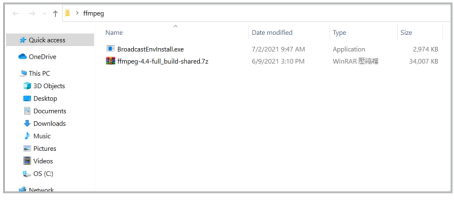
4. ダウンロードが完了したら、ダウンロードしたファイルを ASUS Control Center Express\Thirdpartyインストールフォルダにあるffmpeg環境変数ファイル（**BroadcastEnvInstall.exe**）と同じフォルダに移動します。



- ASUS Control Center Expressのデフォルトインストールパスは、ASUS Control Center Express\Thirdpartyです。ASUS Control Center Expressのインストール時に異なるパスを選択した場合、それに応じて移動するフォルダーを変更してください。
- ダウンロードしたファイルとffmpeg環境変数ファイル（BroadcastEnvInstall.exe）のフォルダパスは必要に応じて変更しても構いませんが、両ファイルは同じフォルダに配置されている必要があります。

5. **BroadcastEnvInstall.exe**を起動してffmpegの環境変数設定を行い、設定が完了したらいずれかのキーを押して終了します。

ffmpegの環境変数を設定する前に、ダウンロードしたファイルとffmpeg環境変数ファイル（BroadcastEnvInstall.exe）が同じフォルダにあることを確認してください。

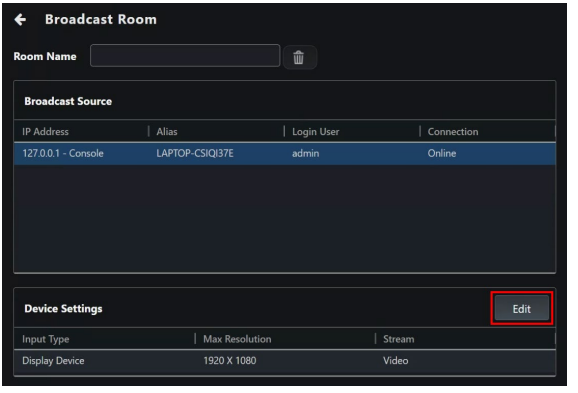



```
Run start install
start unzip
finish unzip
installation succeeded
Press any key to continue . . .
```

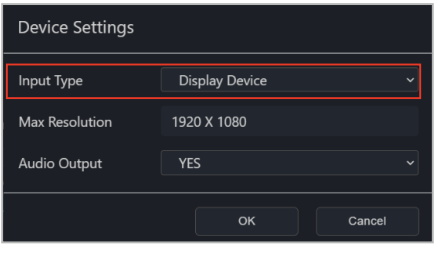
5.11.2　新しいブロードキャストルームの追加

ブロードキャスト機能を使用するには、ブロードキャストルームを作成する必要があります。ブロードキャストルームページでは、ウェブカメラやビデオをブロードキャストソースとして選択したり、ブロードキャスト対象を選択するなど、ブロードキャストに関する各種設定を行うことができます。

1. メインメニュー画面でブロードキャストルームを作成したいデバイスを選択し、**Select Function（機能の選択）**ドロップダウンメニューから**Screen Broadcast（スクリーンブロードキャスト）**＞**Create a broadcast room（ブロードキャストルームの作成）**を選択します
2. **Room Name（ルーム名）**の欄にブロードキャストのルーム名を入力します。
3. ブロードキャストソースリストからブロードキャストソースを選択します。
4. **Input Type（入力タイプ）**の横にある**Edit（編集）**をクリックして、デバイスの設定を行います。

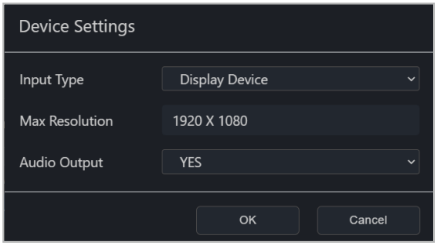


5. デバイス設定ウィンドウで**Input Type（入力タイプ）**を選択します。選択した入力タイプによって、デバイス設定の設定項目が異なる場合があります。



- **表示デバイス**

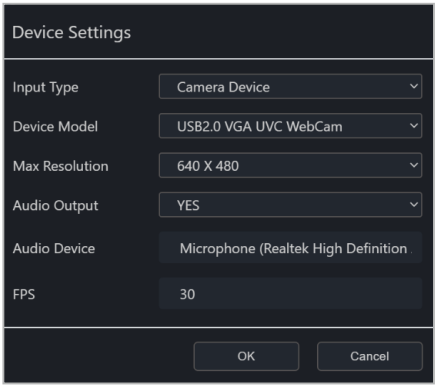
  ブロードキャストソースデバイスの表示デバイスを設定します。



Max Resolution（最大解像度）	ディスプレイデバイスの最大解像度です。
Audio Output（オーディオ出力）	ブロードキャスト音声出力の有効/無効を選択します。

- **カメラデバイス**

  ブロードキャストソースデバイスのカメラデバイスを設定します。

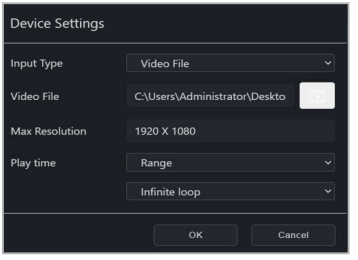


Device Model（デバイスモデル）	ブロードキャストに使用するカメラを選択します。
Max Resolution（最大解像度）	カメラの最大解像度です。
Audio Output（オーディオ出力）	ブロードキャスト音声出力の有効/無効を選択します。
Audio Device（オーディオデバイス）	ブロードキャストに使用するオーディオデバイスを選択します。
FPS	カメラのFPS（フレーム・パー・セカンド）を選択します。

Max Resolution（最大解像度）オプションは、カメラがサポートする解像度によって異なる場合があります。選択した解像度に応じてFPSが調整されます。

- **ビデオファイル**

  ブロードキャストソースデバイス上で、ブロードキャストするビデオファイルを選択します。

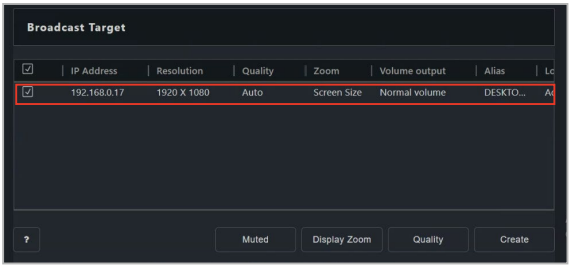


Video File（ビデオファイル）	ブロードキャストに使用するビデオファイルを選択します。対応ビデオコーデック形式：MPEG-2、MPEG-4、.AVI、.WMV
Max Resolution（最大解像度）	ビデオブロードキャストの最大解像度です。
Play time（再生回数）	ビデオファイルをループさせる回数を、設定した範囲内、または任意の回数から選択します。
	ループする回数を選択するか、手動で入力します。

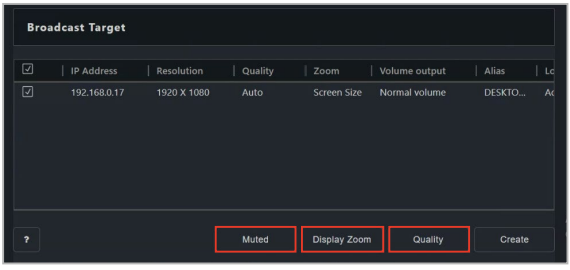
- メインサーバーはブロードキャストソースに記されます。ビデオファイルのブロードキャストは、メインサーバーがブロードキャストソースとして選択されている場合のみ可能です。
- 複数のビデオファイルを選択してプレイリストを作成するには、**Device Settings（デバイス設定）**の右側にある**Edit（編集）**をもう一度クリックし、次のビデオファイルを選択します。

6. 設定オプションを変更するには、**Device Settings（デバイス設定）**の右側にある**Edit（編集）**をもう一度クリックします。

7. ブロードキャストしたいクライアントデバイスをチェックします。



8. **Display Zoom（表示倍率）**、**Quality（品質）**、ブロードキャスト時に音声をミュートにするかどうかを設定します

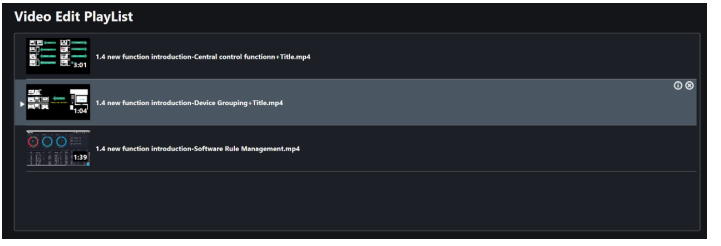


9. **Create（作成）**をクリックすると、ブロードキャストルームが作成されます

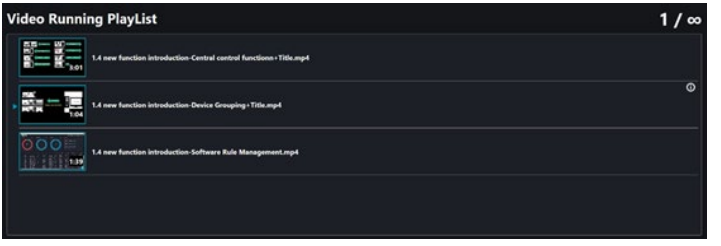
5.11.3 ビデオプレイリストの管理

ビデオファイルを追加すると、プレイリストエディターが自動的に表示され、ビデオファイルの再生順を確認、変更することができます。

- プレイリスト内のビデオファイルの位置を変更するには、ビデオファイルのタイトルをクリックしてドラッグし、プレイリスト内の位置を変更します。
- ブロードキャストで最初に再生するビデオファイルを選択するには、ビデオファイルのタイトルをクリックします。ハイライトされたファイルは、ブロードキャスト開始時に最初に再生されます。
- ビデオファイルの追加後は、アイコンをクリックしてビデオファイルの情報を表示したり、アイコンをクリックしてプレイリストからビデオを削除することができます。



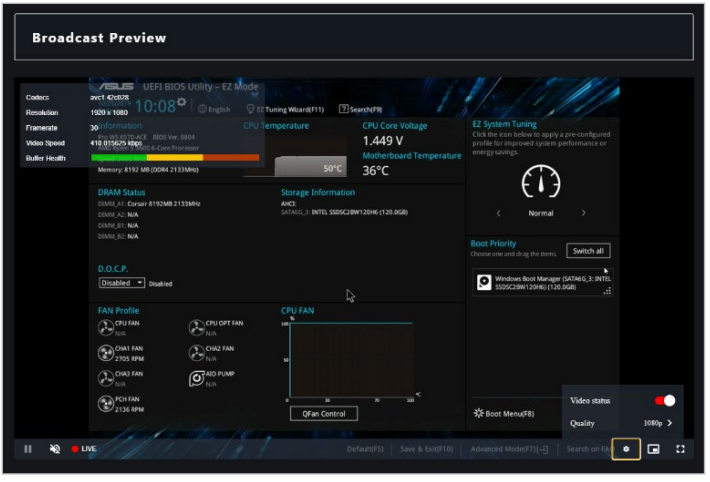
ブロードキャストがアクティブ状態の場合、代わりにプレイリストビューアが表示されます。現在再生中のビデオは、青枠と矢印のアイコンでハイライトされます。プレイリストを変更するには、まずブロードキャストを停止してください。



5.11.4　ブロードキャストの再生

既存のブロードキャストルームのブロードキャストを再生することができます。

1. 既存の **Broadcast Room（ブロードキャストルーム）**に移動します。
2. ページの一番下までスクロールし、再生をクリックします。
3. **Broadcast Source（ブロードキャストソース）**では、ブロードキャストのデータ転送レートや健康状態を確認することができます。
4. ブロードキャストプレビューの下部にある項目から、ブロードキャストの設定や表示を行うことができます。



Play / Stop（再生/停止）	ブロードキャストの再生 / 停止を行います。
Volume（音量）	メインサーバーのプレビューブロードキャストの音量を調整します。 このオプションは、ブロードキャストソースの音量にのみ影響し、クライアントデバイスの音量は調整されません。
Video Status（ビデオ状態）	現在のブロードキャストの状態を表示します。
Settings（設定）	ビデオの表示 / 非表示の切り替えや、ブロードキャストの品質を選択できます。
Picture-in-Picture（ピクチャーインピクチャー）	プレビューブロードキャストをピクチャーインピクチャー（PiP）で視聴するかどうかを選択します。
Full Screen（フルスクリーン）	プレビューブロードキャストをフルスクリーンで表示するかどうかを選択します。

5. **Stop（停止）**を押すと、進行中のブロードキャストが終了します。

- ブロードキャストが再生されているときのブロードキャストルームの設定を行うことができます。詳しくは、**5.11.5 既存のブロードキャストルームの編集** を参照してください。
- ブロードキャストルームが不要になった場合は、ブロードキャストルーム名の横にある をクリックすると、そのブロードキャストルームが削除されます。
- オフラインのクライアントデバイスにはブロードキャストできません。ブロードキャストの再生中に選択したデバイスがオフラインになった場合は、そのデバイスがオンラインになったときに自動的にブロードキャストが再生されます。
- ブロードキャスト中にブロードキャストデバイスはエージェントを更新できません。デバイスのエージェントを更新する場合は、まずブロードキャストを停止して終了してください。
- 選択した入力タイプが表示デバイスまたはカメラデバイスの場合、ブロードキャスト対象として選択したデバイスをブロードキャストソースとして設定できます。

5.11.5 既存のブロードキャストルームの編集

1. 既存のブロードキャストルームに新しいデバイスを追加する場合は、手順2に進む前に、ブロードキャストルームに追加したい新しいクライアントデバイスを選択します。
2. **Select Function（機能の選択）**ドロップダウンメニューから**Screen Broadcast（スクリーンブロードキャスト）**を選択し、編集したいブロードキャストルームを選択します。
3. **5.10.2 新しいブロードキャストルームの追加** の手順2～8に従い、ブロードキャストルームを編集します。

ブロードキャストルームに新しいデバイスを追加した場合は、**Broadcast Target（ブロードキャスト対象）**で新しく追加したデバイスを選択します。

4. 変更が完了したら**Apply（適用）**をクリックして変更内容を適用するか、**Play（再生）**をクリックして新しい変更内容でブロードキャストを再生します。

ブロードキャストルームが不要になった場合は、ブロードキャストルーム名の横にある をクリックすると、そのブロードキャストルームが削除されます。

6章

設定の移行ツール

本章はACC CSMの設定情報をASUS Control Center Expressへインポートする方法と、ASUS Control Center Expressのエージェントをを ACC CSMが管理するデバイスへ配置する方法を説明します。

6.1 設定の移行

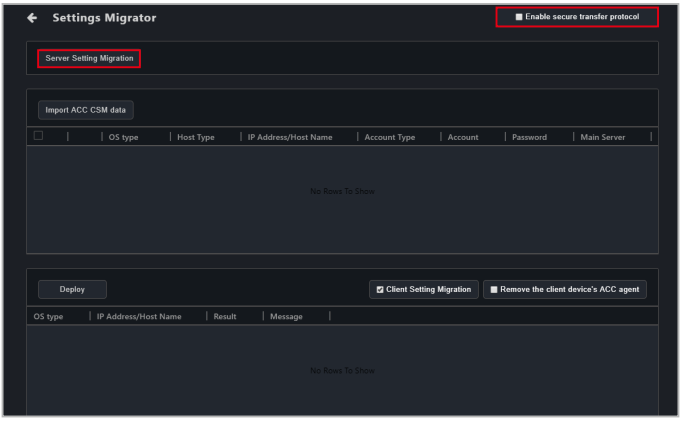
ACC CSMを既に使用しており、すべてのACC CSM設定をASUS Control Center Expressにインポートしたい場合は、Settings Migrator（設定の移行）機能を使用することができます。これにより、ACC CSMで管理されている既存のデバイスにASUS Control Center Expressエージェントを配置することもできます。

右上のメニューバーで をクリックして**Settings Migrator（設定の移行）**を選択すると設定移行画面が表示されます。

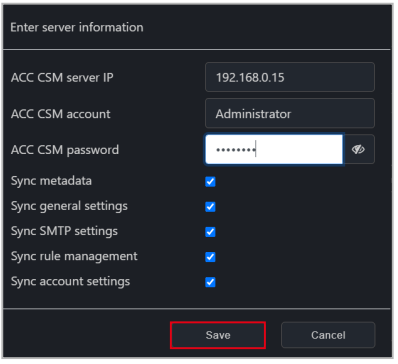
6.1.1 ACC CSMサーバーの設定を移行

以下の手順に従い、ACC CSMサーバーの設定をASUS Control Center Expressへ移行できます。

1. （任意）**Enable secure transfer protocol（セキュアな転送プロトコルを有効）**を選択すると、移行データは安全なプロトコルで保護されます。
2. **Server Setting Migration（サーバー設定の移行）**をクリックします。



3. 入力欄に必要な情報を記入し、**Save（保存）**をクリックします。

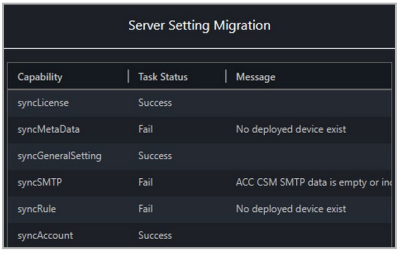


ACC CSM server IP（ACC CSMサーバーIPアドレス）	インポートするACC CSMサーバーのIPアドレスです。
ACC CSM account（ACC CSMアカウント）	インポートするACC CSMサーバーの管理者アカウント名です。
ACC CSM password（ACC CSMパスワード）	インポートするACC CSMサーバーの管理者アカウントのパスワードです。
Sync metadata（メタデータの同期）	選択するとACC CSMのメタデータ欄をインポートします。
Sync general setting（全般設定の同期）	選択するとACC CSMの全般設定の特定項目をインポートします設定項目には以下の内容が含まれます： <u>メインサーバー設定</u> - Webページ更新タイマー - 更新チェックタイマー <u>エージェント設定</u> - ハードウェアセンサーの間隔 - 使用率タイマーの間隔 - エージェント応答タイマー
Sync SMTP setting（SMTP設定の同期）	選択するとACC CSMのSMTP設定をインポートします。
Sync rule management（同期ルールの管理）	選択するとACC CSMの通知ルールをインポートします。 • インポートされた通知ルールは、ASUS Control Center Expressが管理するACC CSMクライアントデバイスのみに適用されます。 • サーバー設定を移行した後に、新たにCSMデバイスが追加された場合、配置後に**Setting Migrator（設定の移行）**を再度使用して、設定内容を同期してください。

Sync account setting（アカウント設定の同期）	選択するとACC CSMのアカウントと役割をインポートします。 ACC CSMのデフォルトアカウントはインポートできません。 セキュリティ上の理由により、インポートしたACC CSMアカウントのパスワードは、ASUS Control Center Expressにインポートされません。インポートしたアカウントのパスワードはデフォルトの「admin」に設定されます。必ずインポートしたクライアントデバイスの正しい管理者パスワードに変更してください。

移行したCSM製品のライセンスキーは、ASUS Control Center Expressの**License（ライセンス）**タブにある**CSM License Information（CSMライセンス情報）**リストに移行されます。詳細は**8.2 ライセンス情報**を参照してください。

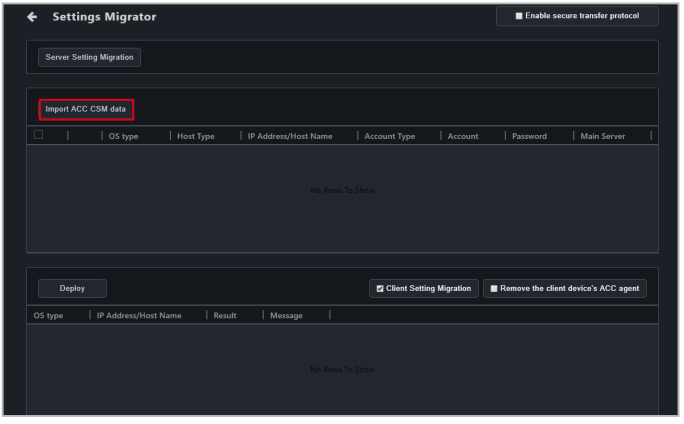
4. 設定とデータの移行結果は、ACC CSMの設定に応じて異なります。ミッションセンターで、各オプションの移行結果を確認できます。



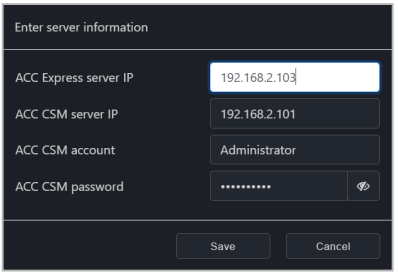
6.1.2 ACC CSMデータのインポート

ACC CSMのクライアントデバイス情報をインポートすれば、ASUS Control Center Expressのエージェントを ACC CSMクライアントデバイスへ配置できるようになります。

1. **Import ACC CSM data（ACC CSMデータのインポート）**をクリックします。



2. 入力欄へ必要な情報を記入します。



ACC Express server IP（ACC Expressサーバー IPアドレス）	ASUS Control Center Expressサーバーの IPアドレスです。
ACC CSM server IP（ACC CSMサーバーIPアドレス）	インポートするACC CSMサーバーのIPアドレスです。
ACC CSM account（ACC CSMアカウント）	インポートするACC CSMサーバーの管理者アカウント名です。
ACC CSM password（ACC CSMパスワード）	インポートするACC CSMサーバーの管理者アカウントのパスワードです。

3. 終了したら**Save（保存）**をクリックし、クライアントデバイスのデータのインポートを開始します。

4. ACC CSMが管理するクライアントデバイスのデータがインポートされ、デバイスリストに表示されます。

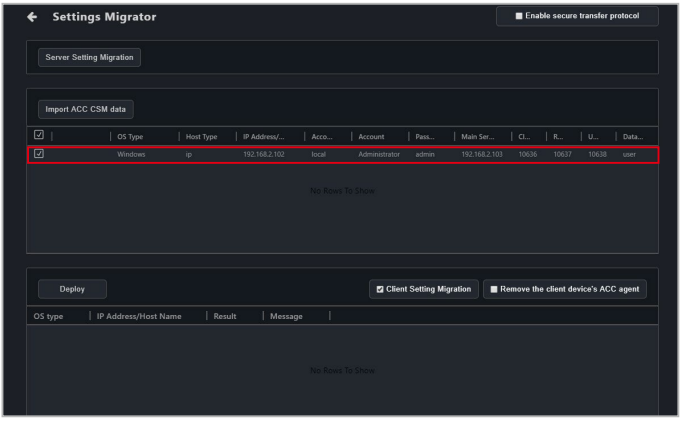
インポートしたクライアントデバイスへすでにASUS Control Center Expressのエージェントを配置している場合、**This device has already been deployed to（このデバイスはすでに配置されています）**と表示されます。このデバイスへ再配置する場合は、まずエージェントを削除してください。詳細は**3.3 エージェントの削除**を参照してください。

6.1.3 ACCEエージェントをACC CSMデバイスへ配置

1. ASUS Control Center ExpressのエージェントをACC CSMデバイスへ配置する前に、ACC CSM製品デバイス用のCSMライセンスキーが登録済みであることを確かめてください。

CSMライセンスキー登録の詳細は、**8.1.4 ライセンス**を参照してください。

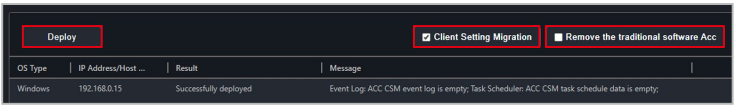
2. エージェントを配置するインポート済みのクライアントデバイスをダブルクリックし、パスワードをクライアントデバイスの管理者パスワードへ変更した後、**Save（保存）**をクリックします。また、デフォルトのエージェントデバイスの管理者アカウントとパスワードは、**Settings（設定）> Options（オプション）> General Configurations（全般設定）> Agent device's administrator account（エージェントデバイスの管理者アカウント）**で編集することができます。詳細は**8.1.4 ライセンス**を参照してください。
3. インポートされたデバイス一覧で、エージェントを配置するデバイスを選択します。



4. （任意）**Client setting migration（クライアント設定の移行）**を選択して、配置時にACC CSMクライアント設定とデータを選択したデバイスへインポートします。このオプションはデフォルトで選択されています。クライアント設定の移行機能でインポートされるクライアント設定とデータの詳細情報は、次の表を参照してください。

Utilization（使用率）	CPUしきい値
	メモリーしきい値
	パーティションしきい値
	ネットワークしきい値
Control（制御）	**Enable/Disable Regedit（レジストリエディタを有効/無効）**設定
	USB Storage Device（USBストレージデバイス）設定
Event Log（イベントログ）	デバイスのイベントログ情報
Scheduled tasks（スケジュール設定されたタスク）	**Power Control（電源制御）**関連のスケジュールされたタスク
	Service Control（サービス制御）関連のスケジュールされたタスク
	Software Dispatch（ソフトウェア配布）関連のスケジュールされたタスク
	Security Control（セキュリティ制御）関連のスケジュールされたタスク
	BIOS Cache（BIOSキャッシュ）関連のスケジュールされたタスク

5. （任意）**Remove the client device's ACC agent（クライアントデバイスのACCエージェントを削除）**を選択すると、新たにエージェントを配置する際に、選択したクライアントデバイスへインストールされた旧バージョンのASUS Control Centerエージェントがすべて削除されます。
6. **Deploy（配置）**をクリックし、エージェントの配置が完了するまで待ちます。配置の結果は、ACC CSMの設定に応じて異なります。Result（結果）欄で、各デバイスについて配置とデータ移行の結果を確認することができます。



クライアントのWindows オペレーティングシステムの管理者アカウントが有効にされており、パスワードが設定されていることを確認してください。

ASUS Control Center Expressエージェントがまだ配置されていないデバイスでインポート済みのスケジュールされたタスクが存在する場合、これらのデバイスに関連するタスクは、ASUS Control Center Expressエージェントがデバイスへ配置された瞬間にタスクスケジューラーへ追加されます。

7章

本章はクライアントデバイスに関する各種
レポートを生成する方法を説明します。

レポートジェネレーター

7.1 レポートジェネレーター

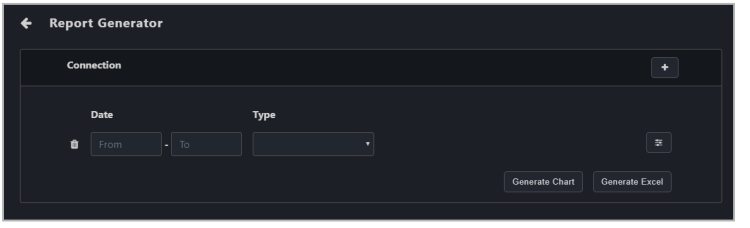
接続状態、ソフトウェアのインストール履歴、クライアントデバイスのハードウェア情報に関するレポートを生成することができます。

7.1.1 接続レポート

接続レポートは、単一または複数の選択されたデバイスでレポートを生成します。

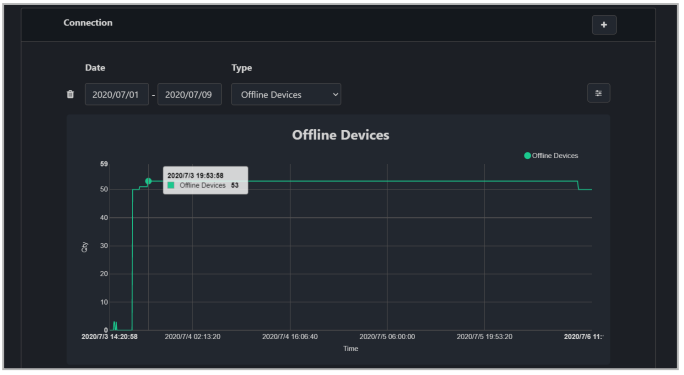
Settings（設定） > **Options（オプション）** > **General Configuration（全般設定）にて、Report Generator（レポートジェネレーター）**で接続履歴のレポート記録を有効または無効にすることができます。

すべてのデバイスに対して接続レポートを生成する場合は、右上のメニューバーで をクリックし、**Connection（接続）**を選択します。複数のデバイスで接続レポートを作成する場合は、Device Overview（デバイス概要）から接続レポートを作成するデバイスを選択し、**Select Function（機能の選択）** > **Report Generator（レポートジェネレーター）** > **Connection（接続）**をクリックします。

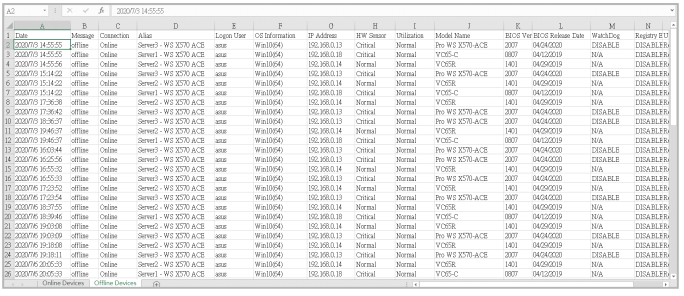


Date（日付）	レポートを生成する日付の範囲を設定します。この欄を空白にすると、メインサーバーへ記録されたすべての日付についてレポートが生成されます。
Type（タイプ）	オンラインまたはオフラインのデバイスのどちらでレポートを生成するか、選択します。
Customize（カスタマイズ）	レポートに表示するメタデータ欄を選択します。
Add（追加 ＋）	レポートを追加します。
Delete（削除）	生成されたグラフとレポートの情報欄を選択して削除します。
Generate Chart（グラフの生成）	入力または選択した情報の折れ線グラフを生成します。
Generate Excel（Excelファイルの生成）	入力または選択した情報に基づいてExcelファイルを生成します。 生成されたExcelファイルには折れ線グラフは含まれません。

生成された接続レポートのグラフ



生成された接続レポートのExcelファイル

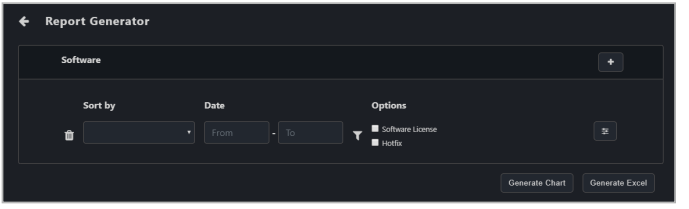


	A	B	C	D	E	F	O	H	I	J	K	L	M	N
1	Date	Message	Connection	Alias	Logon User	OS Information	IP Address	HW Sensor	Utilization	Model Name	BIOS Ver	BIOS Release Date	WatchDog	Registry EU
2	2020/7/3 14:55:55	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
3	2020/7/3 14:55:55	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC05-C	0807	04/12/2019	N/A	DISABLER
4	2020/7/3 14:55:56	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
5	2020/7/3 15:14:22	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
6	2020/7/3 15:14:22	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
7	2020/7/3 15:14:22	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC05-C	0807	04/12/2019	N/A	DISABLER
8	2020/7/3 17:36:36	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
9	2020/7/3 17:36:42	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
10	2020/7/3 18:36:37	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
11	2020/7/3 19:46:37	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
12	2020/7/3 19:46:37	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC05-C	0807	04/12/2019	N/A	DISABLER
13	2020/7/6 16:03:44	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
14	2020/7/6 16:25:56	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
15	2020/7/6 16:55:32	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
16	2020/7/6 16:55:33	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
17	2020/7/6 17:23:52	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
18	2020/7/6 17:23:54	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
19	2020/7/6 18:37:55	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
20	2020/7/6 18:39:46	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC05-C	0807	04/12/2019	N/A	DISABLER
21	2020/7/6 19:03:08	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
22	2020/7/6 19:03:09	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
23	2020/7/6 19:18:08	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
24	2020/7/6 19:18:11	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLER
25	2020/7/6 20:05:33	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC05R	1401	04/29/2019	N/A	DISABLER
26	2020/7/6 20:05:33	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC05-C	0807	04/12/2019	N/A	DISABLER

7.1.2 ソフトウェアレポート

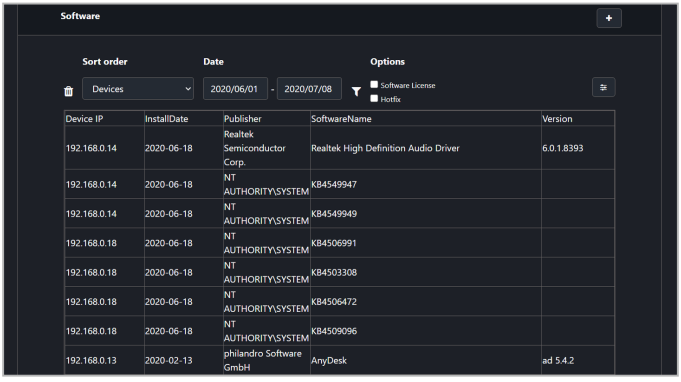
ソフトウェアレポートは、単一または複数の選択されたデバイスでソフトウェアインストールの履歴レポートを生成します。

すべてのデバイスに対してソフトウェアレポートを生成する場合は、右上のメニューバーで をクリックし、**Software（ソフトウェア）**を選択します。複数のデバイスでソフトウェアレポートを作成する場合は、Device Overview（デバイス概要）からソフトウェアレポートを作成するデバイスを選択し、**Select Function（機能の選択）** > **Report Generator（レポートジェネレーター）** > **Software（ソフトウェア）**をクリックします。



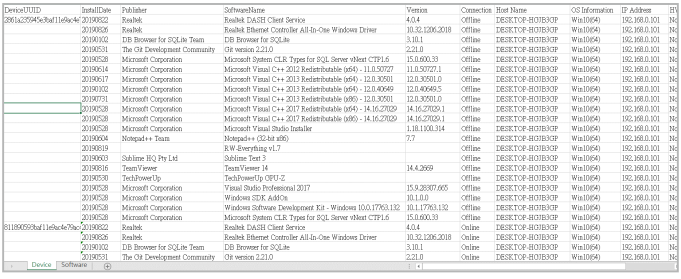
Sort by（整列）	生成されたレポートを**Devices（デバイス）**または**Software（ソフトウェア）**順に整列します。 • **Devices（デバイス）**： デバイスに基づきレポートを生成し、インストールされたソフトウェアを表示します。 • **Software（ソフトウェア）**： ソフトウェアに基づきレポートを生成し、どのデバイスにそのソフトウェアがインストールされているかを表示します。
Date（日付）	レポートを生成する日付の範囲を設定します。この欄を空白にすると、メインサーバーへ記録されたすべての日付についてレポートが生成されます。
Options （オプション）	**Software License（ソフトウェアライセンス）**を選択すると、ソフトウェアライセンスの更新のみに関するレポートが生成されます。**Hotfix（ホットフィックス）**を選択すると、ホットフィックスのみに関するレポートが生成されます。この欄を空白にすると、すべてのオプションについてレポートが生成されます。
Filter（フィルター ）	フィルター機能を使用して、レポートを生成するソフトウェアを選定します。この欄を空白にすると、メインサーバーへ記録されたすべてのソフトウェアについてレポートが生成されます。
Customize（カスタマイズ ）	レポートに表示するメタデータ欄を選択します。
Add（追加 ）	レポートを追加します。
Delete（削除 ）	生成されたグラフとレポートの情報欄を選択して削除します。
Group（グループ）	既存のグループか、新規グループに基づいてレポートをフィルタリングできます。グループの追加の詳細については、**2.2.5 クライアントデバイスのグループ作成**を参照してください。
Generate Chart（グラフの生成）	入力または選択した情報に基づいてグラフを生成します。
Generate Excel（Excelの生成）	入力または選択した情報に基づいてExcelファイルを生成します。

生成されたソフトウェアレポートのグラフ



Device IP	InstallDate	Publisher	SoftwareName	Version
192.168.0.14	2020-06-18	Realtek Semiconductor Corp.	Realtek High Definition Audio Driver	6.0.1.8393
192.168.0.14	2020-06-18	NT AUTHORITY\SYSTEM	KB4549947	
192.168.0.14	2020-06-18	NT AUTHORITY\SYSTEM	KB4549949	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4506991	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4503308	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4506472	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4509096	
192.168.0.13	2020-02-13	philandro Software GmbH	AnyDesk	ad 5.4.2

生成されたソフトウェアレポートのExcelファイル

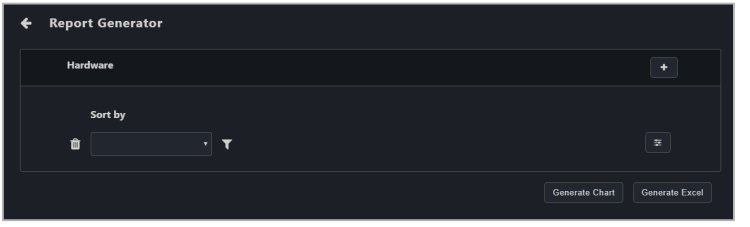


DeviceUUID	InstallDate	Publisher	SoftwareName	Version	Connection	Host Name	OS Information	IP Address	IP
2861a2f5945e8aff1e6a4e4d	20190822	Realtek	Realtek DASH Client Service	4.0.4	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190826	Realtek	Realtek Ethernet Controller All-In-One Windows Driver	10.32.1206.2018	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190102	DB Browser for SQLite Team	DB Browser for SQLite	3.10.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190531	The Git Development Community	Git version 2.21.0	2.21.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Microsoft System CLR Types for SQL Server vNext CTP1.6	15.0.600.33	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190614	Microsoft Corporation	Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.50727	11.0.50727.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190617	Microsoft Corporation	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	12.0.30501.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190102	Microsoft Corporation	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40649	12.0.40649.5	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190731	Microsoft Corporation	Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	12.0.30501.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Microsoft Visual C++ 2017 Redistributable (x64) - 14.16.27029	14.16.27029.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Microsoft Visual C++ 2017 Redistributable (x86) - 14.16.27029	14.16.27029.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Microsoft Visual Studio Installer	1.18.1100.314	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190604	Notepad++ Team	Notepad++ (32-bit x86)	7.7	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190819		RW-Everything v1.7		Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190603	Sublime HQ Pty Ltd	Sublime Text 3		Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190816	TeamViewer	TeamViewer 14	14.4.2669	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190530	TechPowerUp	TechPowerUp GPU-Z		Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Visual Studio Professional 2017	15.9.28307.605	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Windows SDK AddOn	10.1.1.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Windows Software Development Kit - Windows 10.0.17763.132	10.1.17763.132	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190528	Microsoft Corporation	Microsoft System CLR Types for SQL Server vNext CTP1.6	15.0.600.33	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
811890593baf11e8ac4e79ac	20190822	Realtek	Realtek DASH Client Service	4.0.4	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190826	Realtek	Realtek Ethernet Controller All-In-One Windows Driver	10.32.1206.2018	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190102	DB Browser for SQLite Team	DB Browser for SQLite	3.10.1	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne
	20190531	The Git Development Community	Git version 2.21.0	2.21.0	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	Ne

7.1.3 ハードウェアレポート

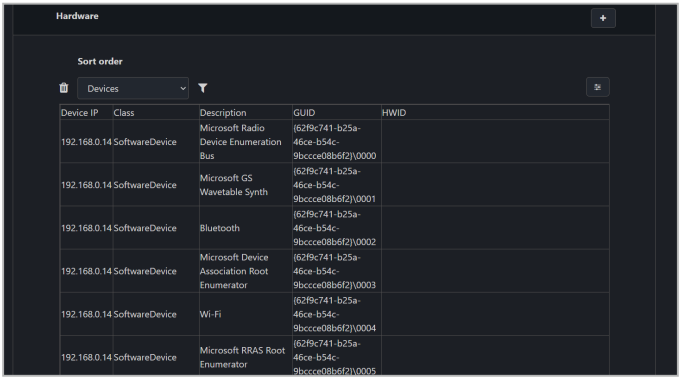
ハードウェアレポートは、単一または複数の選択されたデバイスでハードウェアに関するレポートを生成します。

すべてのデバイスに対してハードウェアレポートを生成する場合は、右上のメニューバーで をクリックし、**Hardware（ハードウェア）**を選択します。複数のデバイスでハードウェアレポートを作成する場合は、Device Overview（デバイス概要）からハードウェアレポートを作成するデバイスを選択し、**Select Function（機能の選択）** > **Report Generator（レポートジェネレーター）** > **Hardware（ハードウェア）**をクリックします。

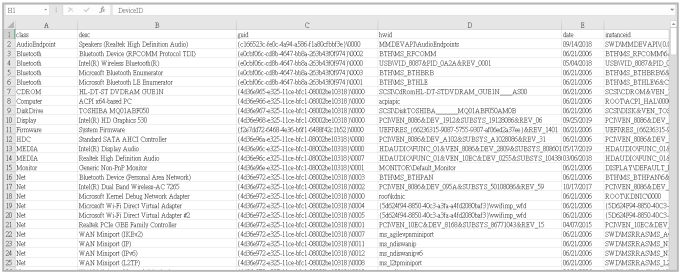


Sort by（整列）	生成されたレポートを**Devices（デバイス）**または**Hardware（ハードウェア）**順に整列します。 • **Devices（デバイス）**： デバイスに基づきレポートを生成し、インストールされたハードウェアを表示します。 • **Hardware（ハードウェア）**： ハードウェアに基づきレポートを生成し、どのデバイスにそのハードウェアがインストールされているかを表示します。
Filter（フィルター）	フィルター機能を使用して、レポートを生成するハードウェアコンポーネントを選定します。この欄を空白にすると、メインサーバーへ記録されたすべてのハードウェアコンポーネントについてレポートが生成されます。
Customize（カスタマイズ）	レポートに表示するメタデータ欄を選択します。
Add（追加）	レポートを追加します。
Delete（削除）	生成されたグラフとレポートの情報欄を選択して削除します。
Group（グループ）	既存のグループか、新規グループに基づいてレポートをフィルタリングできます。グループの追加の詳細については、**2.2.5 クライアントデバイスのグループ作成**を参照してください。
Generate Chart（グラフの生成）	入力または選択した情報に基づいてグラフを生成します。
Generate Excel（Excelの生成）	入力または選択した情報に基づいてExcelファイルを生成します。

生成されたハードウェアレポートのグラフ



生成されたハードウェアレポートのExcelファイル



8章

アカウントと全般設定

本章はユーザー設定とASUS Control Center Expressの設定を説明します。

8.1 オプションメニュー

SMTP Settings（SMTP設定）、**Rule Management（ルール管理）**、**General Configurations（全般設定）**などの設定を行ったり、**License（ライセンス）**キーを追加することができます。

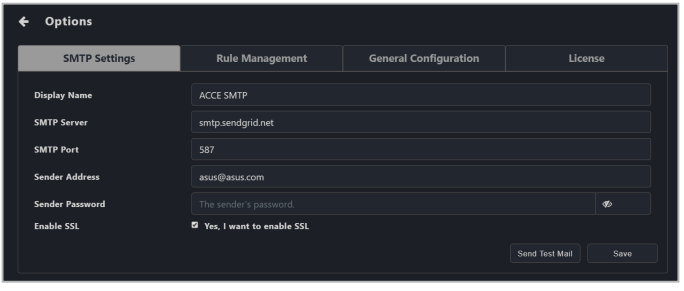
右上のメニューバーで をクリックして**Options（オプション）**を選択すると**Options（オプション）**の画面が開きます。

8.1.1 SMTP設定

ASUS Control Center ExpressでSMTP（簡易メール転送プロトコル）を設定して、システム障害のフィードバックや、システム管理者へのアラートをメール送信することができます。

入力される設定はサービスプロバイダーに応じて異なります。サービスプロバイダーから提供される情報を参照してください。

1. 必要な欄に記入してください。



Display Name（表示名）	このSMTP設定の名前です。表示名は送信メールには記載されません。
SMTP Server（SMTPサーバー）	メールの送受信を行うSMTPサーバーです。
SMTP Port（SMTPポート）	SMTPのサービスポートです。一般的に使用されるポートは25（SMTPの旧デフォルトポート）、465（暗号化SMTP）、587（SMTPの新デフォルトポート）です。
Sender Address（送信者のアドレス）	ACCE通知送信者のメールアドレスです。このメールアドレスはSMTPサーバーサービス内に存在しなければなりません。
Sender Password（送信者のパスワード）	ACCE通知メール送信者のパスワードです。
Enable SSL（SSLを有効）	このSMTPサーバーを通じて送信または転送されるメールにSSL暗号化を施します。

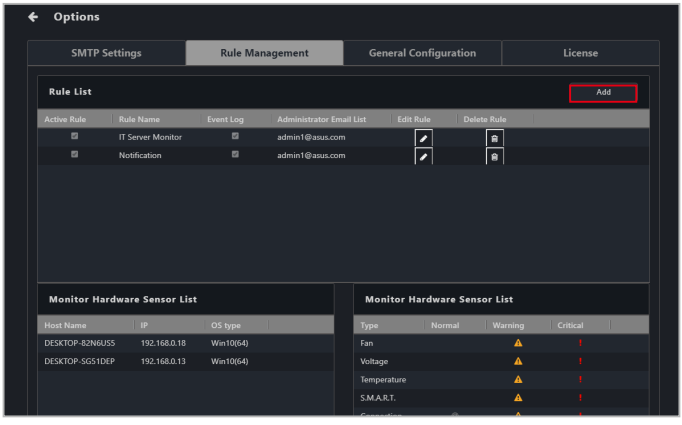
2. （任意）**Send Test Mail（テストメールの送信）**をクリックし、メールアドレスを入力して**Send（送信）**をクリックすると、SMTPの状態を検査するためのテストメールを受信することができます。SMTPが正常に機能していれば、メールが送信されます。
3. **Save（保存）**をクリックし、変更内容を保存します。

8.1.2 ルール管理

ルール管理を通じて、通知ルールを追加または削除することができます。デバイスが警告または危険状態にある時、システム管理者へ通知が送信されます。

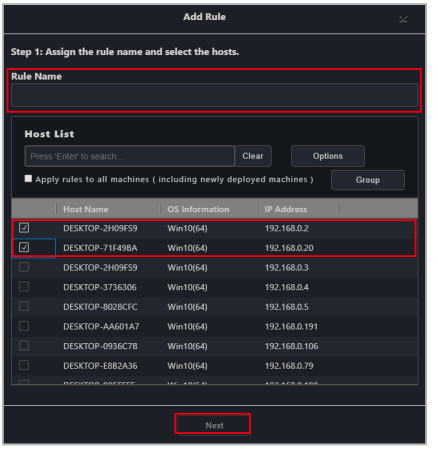
新ルールの追加

1. **Add（追加）**をクリックします。



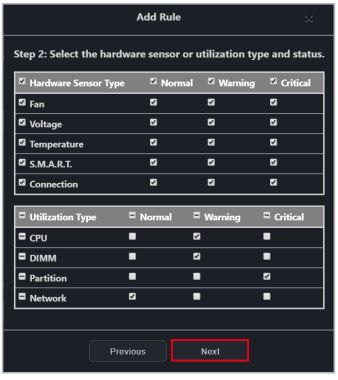
2. ルール名を入力し、ルールを適用するデバイスを選択します。**Next（次へ）**をクリックします。

- Search（検索）ボックスを使用して、入力したキーワードに基づきデバイスを検索してフィルタリングできます。**Clear（消去）**をクリックして、検索フィルターを消去することができます。
- **Group（グループ）**でグループを選択すると、そのグループに属するデバイスが**Host List（ホストー覧）**上で選択されます。
- **Host List（ホストー覧）**で表示する列を増やす場合は、**Options（オプション）**をクリックし、表示するメタデータを選択して**Save（保存）**をクリックします。
- **Apply rules to all machines（including newly deployed machines）（ルールをすべての機械へ適用（新規配置された機械を含む））**を選択すると、**Host List（ホストー覧）**内のデバイスすべてに新規ルールが適用されます。



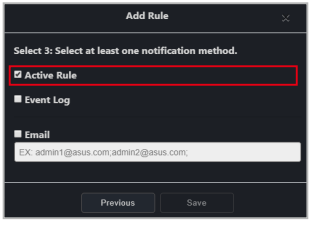
3. 通知を送信する条件（ハードウェアまたは使用率センサーの種類や状態）を選択し、**Next（次へ）**をクリックします。

ハードウェアセンサーや使用率の種類と状態を選択する際にチェックボックスにチェックを入れると、選択された状態へ他の状態から移行した場合に通知が送信されます。例えば、**Normal（正常）**を選択すると、状態が**Warning（警告）**や**Critical（危険）**から**Normal（正常）**へ変更された場合に通知が送信されます。



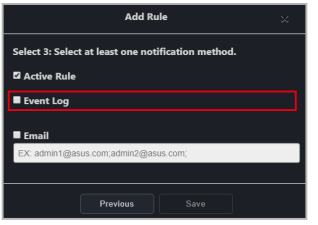
4. **Active Rule（有効なルール）**を選択すると、新たに追加されたルールを有効または無効にすることができます。

Active Rule（有効なルール）はデフォルトで選択されています。



5. 通知方法を選択します（複数の通知方法を選択できます）：

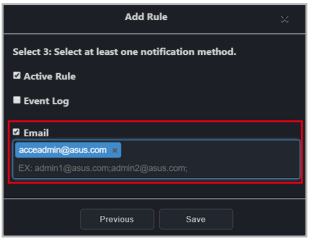
- Event Log（イベントログ）
  通知はデバイスのイベントログとシステム概要に表示されます。



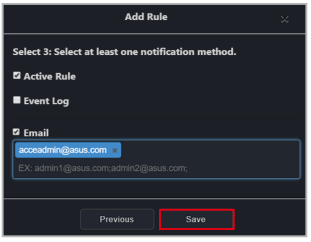
- Email（メール）
  通知は入力されたメールアドレスに送信されます。

メール機能を使用する前に、SMTPサーバー設定を行ってください。詳細は、**8.1.1 SMTP設定**を参照してください。

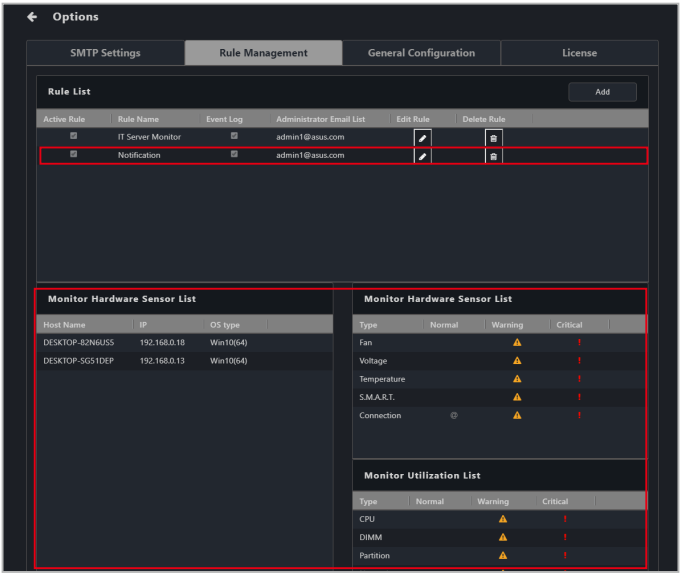
複数のメールアドレスを入力する場合、各アドレスの後に<Enter>キーを押してアドレスを区切ります。



6. 通知方法を選択したら**Save（保存）**をクリックします。



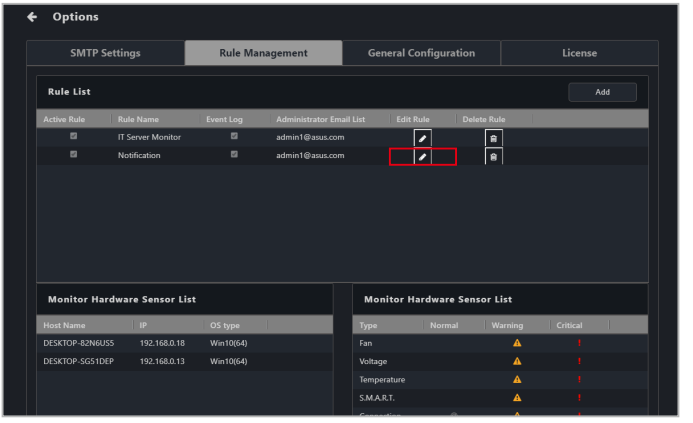
新しく追加したルールは**Rule List（ルール一覧）**に表示され、ルール名と選択した通知方法の詳細が表示されます。新しく追加されたルールをクリックすると、**Monitor Hardware Sensor List（ハードウェアセンサー監視一覧）**にルールに関連付けられたデバイスが表示され、**Monitor Hardware Sensor List（ハードウェアセンサー監視一覧）**と**Monitor Utilization List（使用率監視一覧）**に監視対象のハードウェアと使用率の一覧が表示されます。



通知ルールの編集方法：

編集機能を使用して、通知ルールへ新規デバイスや再配置されたデバイスを追加することができます。

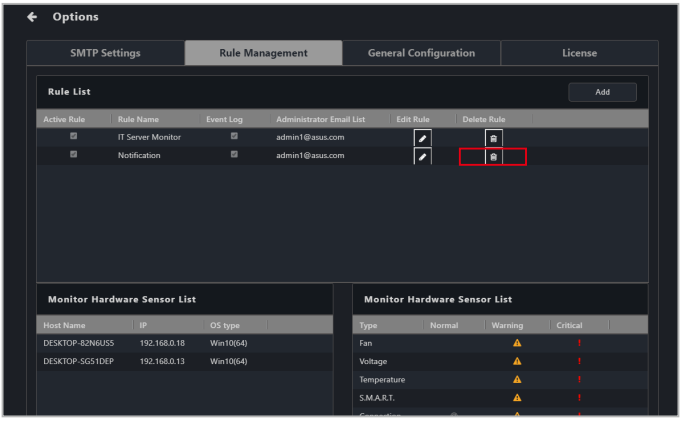
1. 編集するルールを**Rule List**（**ルール一覧**）から選択し、**Edit Rule**（**ルールの編集**）列で をクリックします。



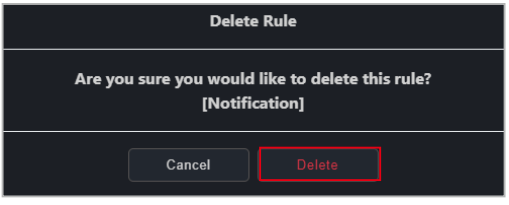
2. 手順2～5を繰り返してルールを編集し、続いて**Save**（**保存**）をクリックして変更内容を保存します。

通知ルールの削除方法：

1. 削除するルールを**Rule List**（**ルール一覧**）から選択し、**Delete Rule**（**ルールの削除**）列で をクリックします。

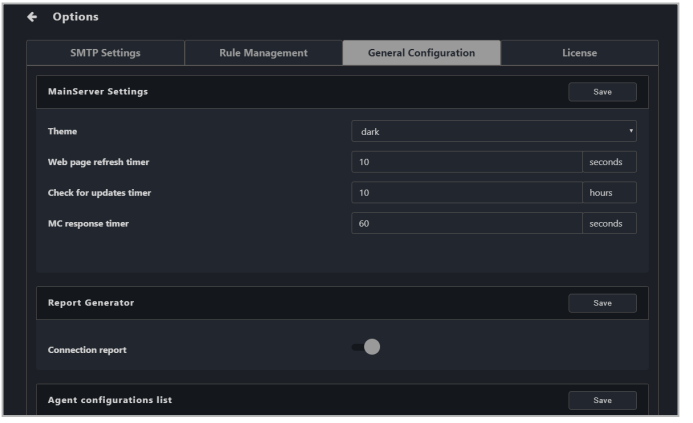


2. **Delete**（**削除**）をクリックしてルールを削除します。



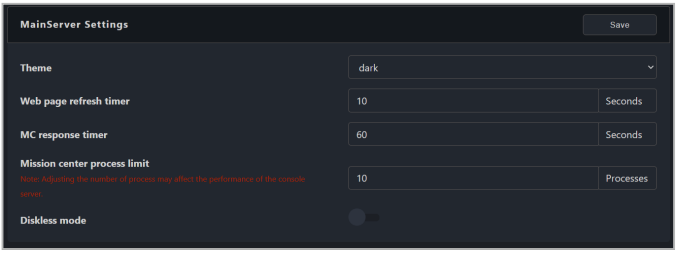
8.1.3 全般設定

全般設定を使用して、メインサーバーとエージェントへ様々な設定をすることができます。下方へスクロールするとさらに多くのオプションが表示されます。



メインサーバー設定：

ASUS Control Center Expressのメインサーバーの機能を設定します。**Save（保存）**をクリックし、変更内容を保存します。



Theme（テーマ）	メインサーバーのカラーテーマ（**acc_csm、acc、dark、metal**）を選択します。
Web page refresh timer（ウェブページのリフレッシュタイマー）	メインサーバーのすべてのWebページの更新間隔を秒単位で設定します。
Mission center process limit（ミッションセンターのプロセス制限）	ミッションセンタープロセスの最大数を設定します。
Diskless mode（ディスクレスモード）	ディスクレスモードを有効にすると、ストレージデバイスのないリモートマシンにエージェントを配置することができます。

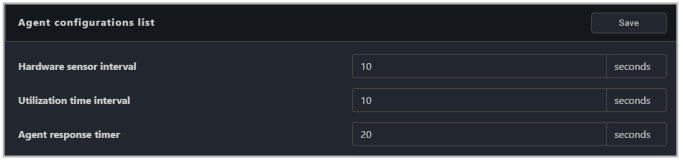
レポートジェネレーター：

接続レポートの有効/無効を切り替えます。**Save（保存）**をクリックし、変更内容を保存します。

Connection report（接続レポート）	接続レポートの有効/無効を切り替えます。

エージェントの設定一覧：

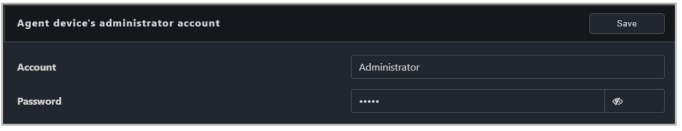
エージェントのセンサー間隔と応答時間を設定します。**Save（保存）**をクリックし、変更内容を保存します。



Hardware sensor interval（ハードウェアセンサーの間隔）	ハードウェアセンサーがセンサー値を返す間隔を秒単位で設定します。
Utilization time interval（使用率タイマーの間隔）	使用率センサーがセンサー値を返す間隔を秒単位で設定します。
Agent response timer（エージェントの応答タイマー）	エージェントがメインサーバーからタスクをクエリする間隔を秒単位で設定します。

エージェントデバイスの管理者アカウント:

エージェントを配置する際に管理者アカウントとパスワードが入力されていない場合に、デフォルトの管理者アカウントとパスワードを設定します。**Save（保存）**をクリックし、変更内容を保存します。

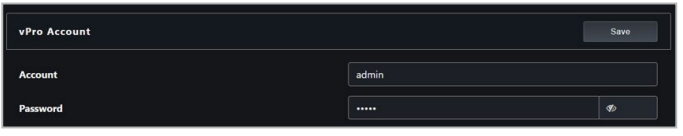


Account（アカウント）	デフォルトの管理者アカウントを設定します。
Password（パスワード）	デフォルトの管理者パスワードを設定します。

- アカウントのタイプがドメインアカウントの場合、ドメイン\アカウントの形式で入力します。ドメインアカウントへ配置する際のデフォルトアカウントとして機能します。
- 配置時にデフォルトアカウントを使用する場合、クライアントデバイスの言語を確認してください。管理者権限を持つシステムアカウントはシステム言語に応じて異なる場合があり、デバイスへのエージェント配置に影響を与えることがあります。

vProアカウント:

クライアントvProリモート管理コントローラーへのログインに使用するデフォルトのログインアカウントを設定します。**Save（保存）**をクリックすると、変更した内容が保存されます。

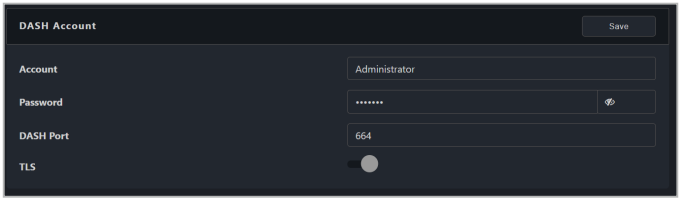


Account（アカウント）	クライアントデバイスのvProリモート管理コントローラーにログインするためのデフォルトアカウントを設定します。
Password（パスワード）	クライアントデバイスのvProリモート管理コントローラーにログインするためのデフォルトパスワードを設定します。

入力するアカウントとパスワードは、クライアントデバイスvProリモート管理コントローラーのアカウントとパスワードと一致している必要があります。

DASH アカウント:

クライアントDASHリモート管理コントローラーへのログインに使用するデフォルトのログインアカウントを設定します。**Save（保存）**をクリックすると、変更した内容が保存されます。

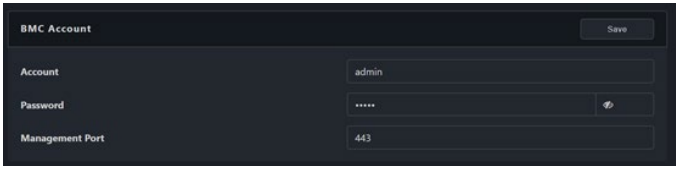


Account（アカウント）	クライアントデバイスのDASHリモート管理コントローラーにログインするためのデフォルトアカウントを設定します。
Password（パスワード）	クライアントデバイスのDASHリモート管理コントローラーにログインするためのデフォルトパスワードを設定します。
DASH port（DASHポート）	DASH用のポートを設定します。（デフォルト: 664）
TLS	TLS（Transport Layer Security）を有効/無効にします。

入力するアカウントとパスワードは、クライアントデバイスDASHリモート管理コントローラーのアカウントとパスワードと一致している必要があります。

BMC アカウント:

クライアントBMCリモート管理コントローラーへのログインに使用するデフォルトのログインアカウントを設定します。**Save（保存）**をクリックすると、変更した内容が保存されます。



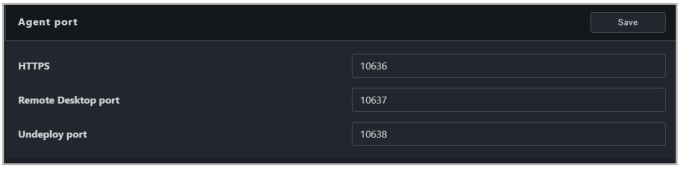
Account（アカウント）	クライアントデバイスのBMCリモート管理コントローラーにログインするためのデフォルトアカウントを設定します。
Password（パスワード）	クライアントデバイスのBMCリモート管理コントローラーにログインするためのデフォルトパスワードを設定します。
Management Port（管理ポート）	BMC用のポートを設定します。（デフォルト: 443）

入力するアカウントとパスワードは、クライアントデバイスBMCリモート管理コントローラーのアカウントとパスワードと一致している必要があります。

エージェントポート:

エージェントとメインサーバーがクライアントデバイスへ接続する場合のポートを設定します。**Save（保存）**をクリックし、変更内容を保存します。

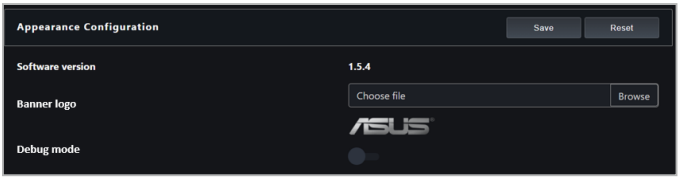
クライアントデバイスのファイアウォール設定を調整する必要がないため、デフォルト値を使用することをお勧めします。



HTTPS	Webページアクセス用のポートを設定します。（デフォルト: 10636）
Remote Desktop port（リモートデスクトップのポート）	リモートデスクトップ用のポートを設定します。（デフォルト: 10637）
Undeploy port（配置解除のポート）	クライアントからエージェントを削除するためのポートを設定します。（デフォルト: 10638）

表示設定：

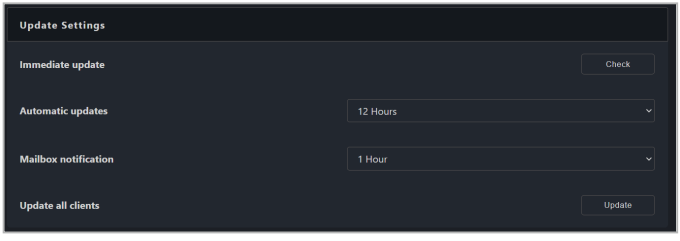
メインサーバーのバージョンを表示したり、バナーロゴをカスタマイズすることができます。**Save（保存）**をクリックし変更内容を保存するか、**Reset（リセット）**をクリックしてデフォルトのバナーロゴへ戻すことができます。



Software version（ソフトウェアバージョン）	ASUS Control Center Expressメインサーバーのバージョンを表示します。
Banner Logo（バナーロゴ）	**Browse（参照）**をクリックして、新しいバナーロゴを選択しアップロードすることができます。バナーロゴはメインダッシュボードの概要画面の左上に表示されます。
Debug mode（デバッグモード）	デバッグモードを有効または無効にします。

更新設定：

メインサーバーとクライアントの更新設定を変更します。

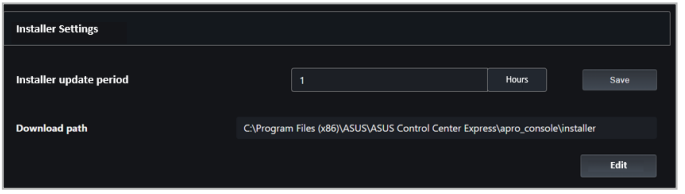


Immediate update（即時更新）	**Check（チェック）**をクリックすると、ASUS Control Center Expressメインソフトウェアの新しい更新をチェックし、ダウンロードします。
Automatic updates（自動更新）	このオプションを有効にすると、ASUS Control Center Expressの更新を自動的にチェックし、更新通知を送信します。
Mailbox notification（メールボックス通知）	ASUS Control Center Expressメールボックスの通知・更新時間を設定します。
Update All Clients（すべてのクライアントを更新）	**Update（更新）**をクリックすると、すべてのクライアントエージェントの更新を開始します。

- **Automatic updates (自動更新)**は、デフォルトでは**Disable (無効)**に設定されています。
- **Mailbox notification (メールボックス通知)**の通知は、デフォルトで**Enable (有効)**になっています。

インストーラー設定:

インストーラーの設定を変更します。**Save**(**保存**)をクリックし、変更内容を保存します。

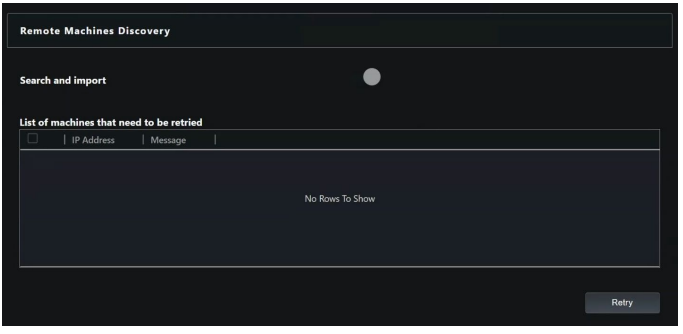


Installer Update Period（インストーラーの更新頻度）	インストーラーが新しい更新をチェックする頻度を設定します。
Download path（ダウンロードパス）	現在のダウンロードパスが表示されます。
Edit（編集）	新しいダウンロードパスを選択します。

リモートマシン検出:

デバイスリストに追加されていない配置済みデバイスを検索します。正常に追加されなかったデバイスがある場合は、ライセンスが利用可能であることを確認し**Retry（再試行）**をクリックして再試行します。

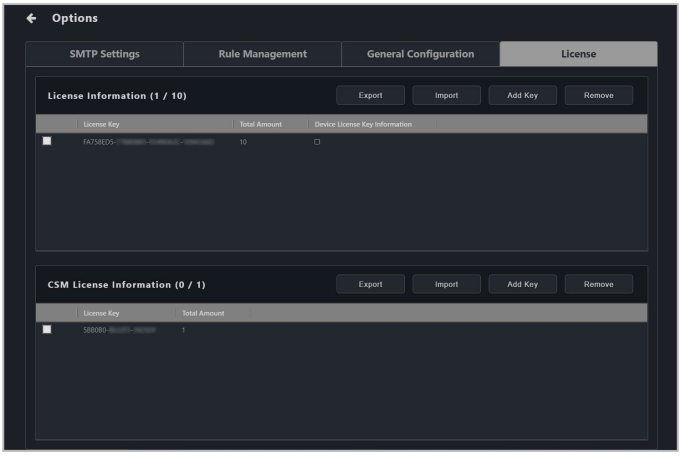
エージェント管理に支障をきたす可能性があるため、終了後はこの機能を無効に設定してください。



8.1.4 ライセンス

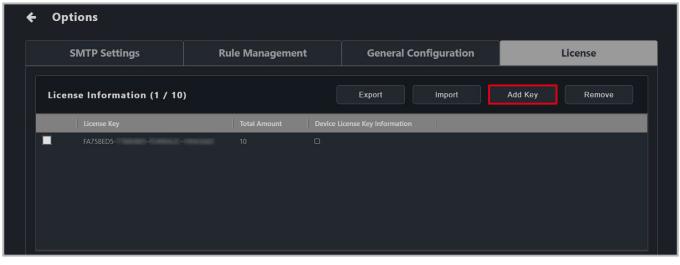
ライセンスキーを追加または削除することができます。また、ACCの旧バージョンからライセンス情報をインポートすることもできます。

エージェントを配置するクライアントデバイスそれぞれに、対応するライセンスキーが必要となります。

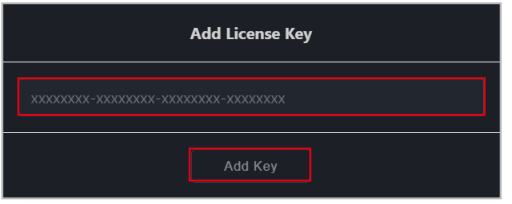


ライセンスキーの追加

1. マザーボードに付属するASUS Control Center Expressカードに記載されたライセンスキーを確認してください。
2. **Add Key（キーを追加）**をクリックします。

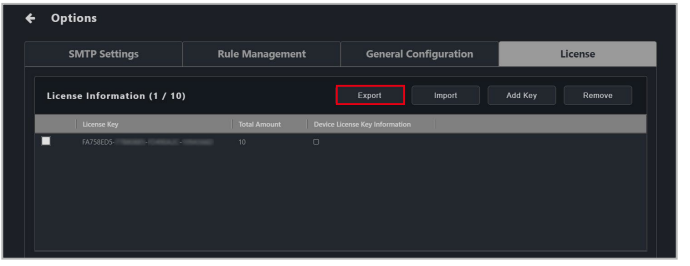


3. ライセンスキーを入力し、続いて**Add Key（キーを追加）**をクリックして、単一デバイスに対するASUS Control Center Expressのライセンスを登録します。

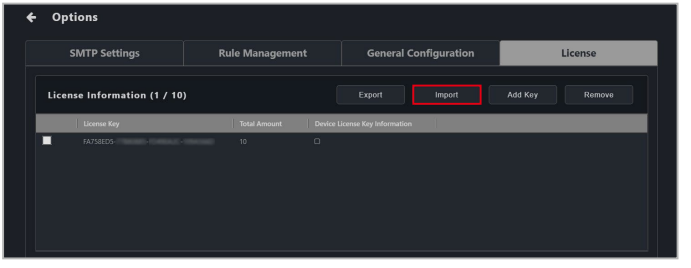


複数のライセンスキーをインポート

1. **Export（エクスポート）**をクリックしてテンプレートの.csvファイルをエクスポートした後、.csvファイルに必要な情報を入力します。



2. **Import（インポート）**をクリックして、編集した.csvファイルをインポートします。



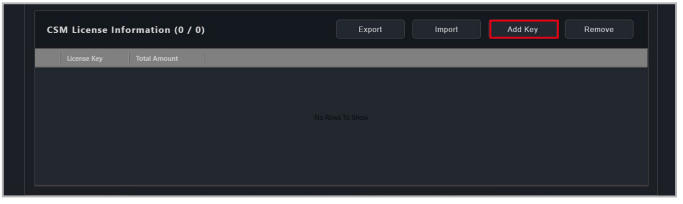
ACC CSMライセンスキーの追加

CSMクライアントデバイスへ配置する場合は、CSM License Information（CSMライセンス情報）に18文字のCSMライセンスキーを入力し、CSMクライアントデバイスを有効にしてください。
また、**Setting Migrator（設定の移行ツール）**を使用してACC CSMからCSMライセンスキーをASUS Control Center Expressへ移行することができます。設定の移行ツールの詳細については、**6章 設定の移行ツール**を参照してください。

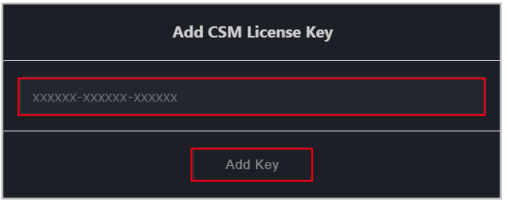
エージェントを配置するCSMクライアントデバイスそれぞれに、対応するCSMライセンスキーが必要となります。

移行したCSM製品のライセンスキーは、**CSM License Information（CSMライセンス情報）**一覧へ移行されます。

1. ACC CSMライセンスキーを準備します。
2. **Add Key（キーを追加）**をクリックします。

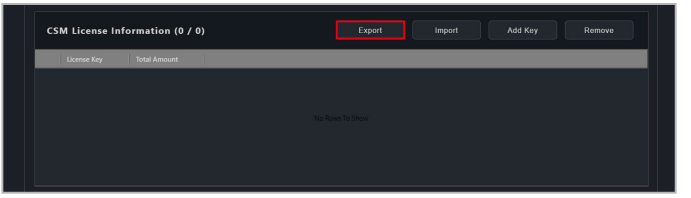


3. ライセンスキーを入力し、続いて**Add Key（キーを追加）**をクリックして、単一デバイスに対するASUS Control Center Expressのライセンスを登録します。

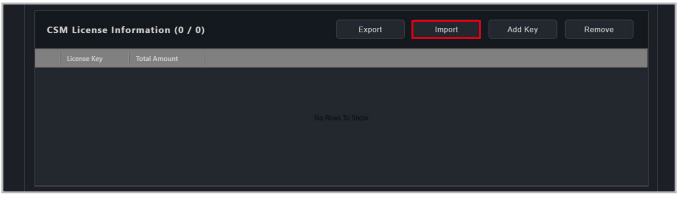


複数のACC CSMライセンスキーのインポート

1. **Export（エクスポート）**をクリックしてテンプレートの.csvファイルをエクスポートした後、.csvファイルに必要な情報を入力します。

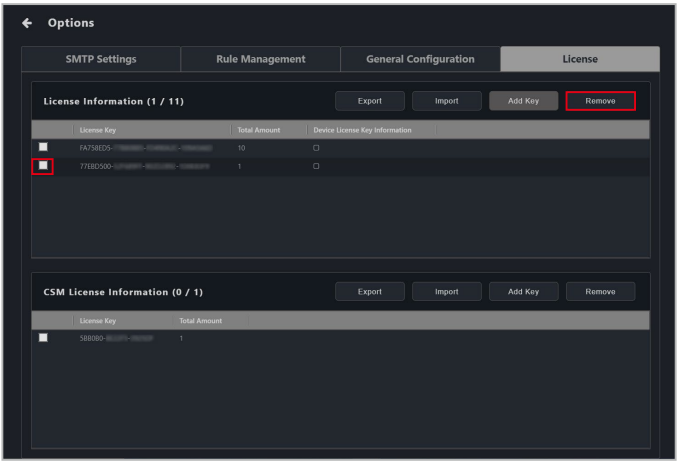


2. **Import（インポート）**をクリックして、編集した.csvファイルをインポートします。



ライセンスキーの削除

1. 削除するライセンスキーまたはACC CSMライセンスキーを選択して（複数を選択可能）、**Remove（削除）**をクリックします。



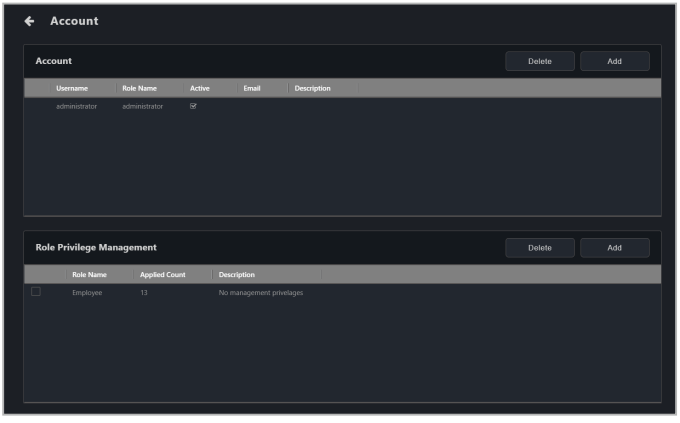
8.2 アカウントメニュー

アカウントメニューを使用して、ASUS Control Center Expressのアカウントを管理することができます。また、QRコードをスキャンすることで、Web版のASUS Control Center Expressに簡単にアクセスしたり、開発者にフィードバックを送信することができます。

8.2.1 アカウント設定

アカウント設定ではASUS Control Center Expressのユーザーアカウントすべてが表示され、アカウントを追加、編集、削除することができます。

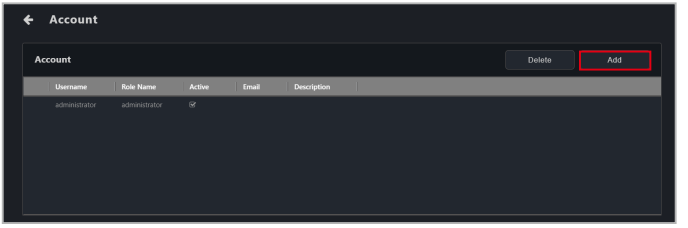
右上のメニューバーで をクリックして**Settings（設定）**を選択すると、**Account Settings（アカウント設定）**画面が開きます。



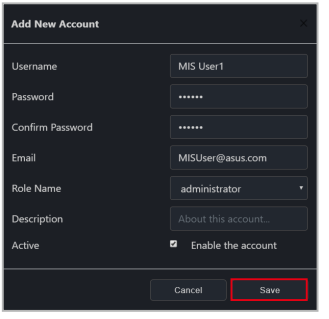
- ASUS Control Center Expressのデフォルトのアカウント名は「**administrator**」、パスワードは「**admin**」です。
- 安全にご使用いただくために、ASUS Control Center Expressのアカウント名とパスワードはデフォルトから変更することを強くお勧めします。

アカウントの追加

1. **Add（追加）**をクリックします。



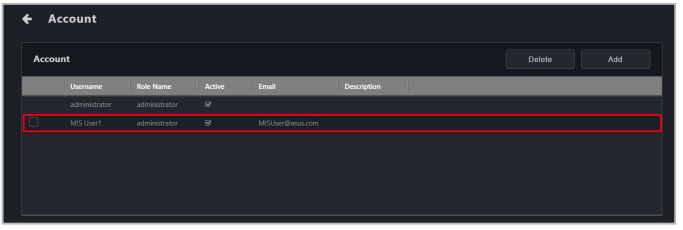
2. 必要な情報を入力し、**Active（有効）**欄で**Enable the account（アカウントを有効にする）**を選択した後、**Save（保存）**をクリックしてこの新規アカウントを追加します。



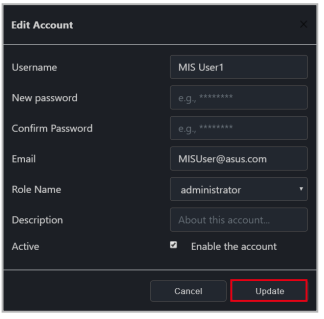
Username（ユーザー名）	アカウントのユーザー名です。
Password（パスワード）	アカウントのパスワードです。
Confirm Password（パスワードの確認入力）	アカウントのパスワードを再度入力します。
Email（メール）	アカウントに関連付けられたメールアドレスです。
Role Name（役割名）	アカウントに割り当てられる役割はアカウントの権限を規定します。プリセットされた**administrator（管理者）**または**viewer（ビューワ）**の役割を選択するか、新たな役割を追加することができます。 役割を追加または編集する場合は、**8.2.2 役割権限の管理**を参照してください。
Description（説明）	アカウントの短い説明を入力します。
Active（有効）	チェックするとアカウントが有効になります。

アカウントの編集

1. 編集するアカウントをクリックします。



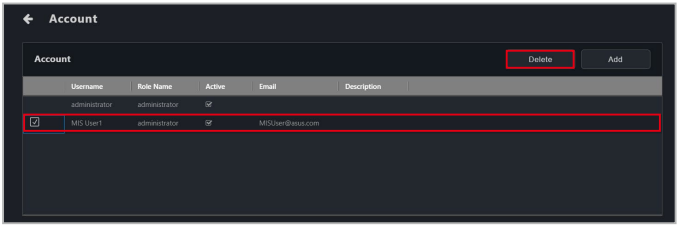
2. アカウントの詳細を編集し終えたら**Update**(**更新**)をクリックします。



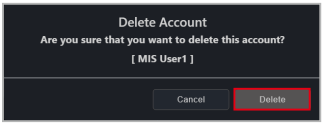
アカウントの削除

1. 削除するアカウントを選択し、**Delete（削除）**をクリックします。

ASUS Control Center Expressの管理者アカウントは削除できません。



2. アカウントの削除を確定し、**Delete（削除）**をクリックします。



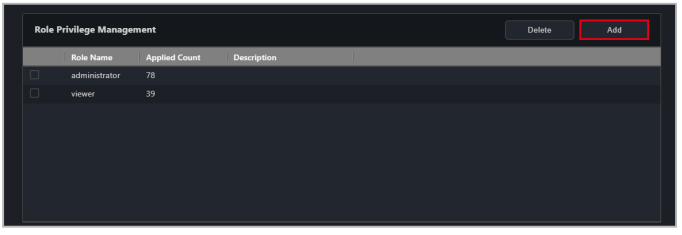
8.2.2 役割権限の管理

役割権限の管理機能はASUS Control Center Expressの役割すべてを表示します。ユーザーへ割り当てる様々な役割の権限を追加、編集、変更することができます。

右上のメニューバーで をクリックし**Settings（設定）**を選択すると、Role **Privilege Management（役割権限の管理）**画面が開きます。

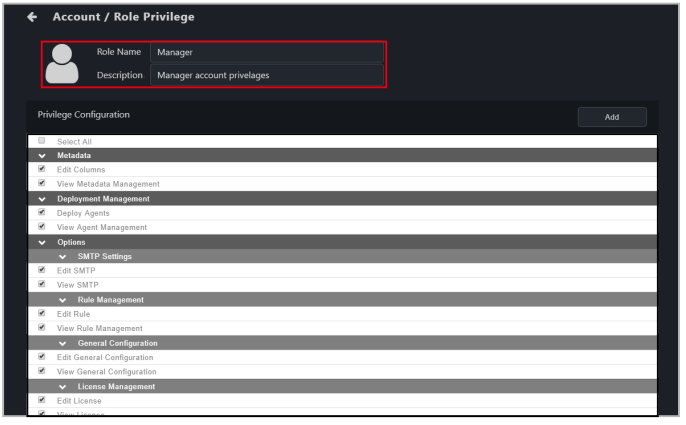
新たな役割の追加

1. **Add（追加）**をクリックします。

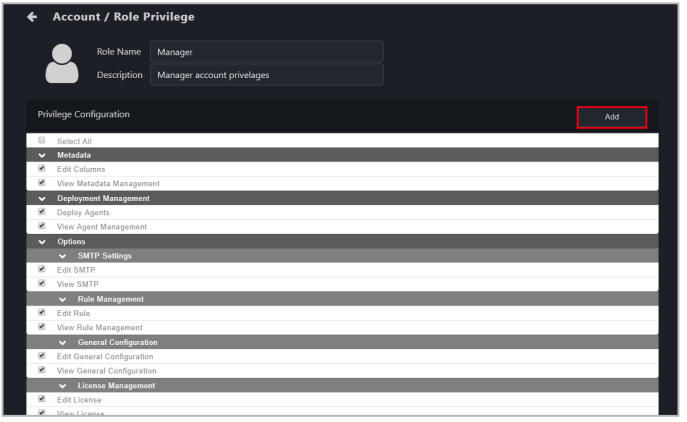


2. 役割の**Role Name（役割名）**と**Description（説明）**を入入力し、Privilege Configuration（権限設定）で役割に割り当てる権限を選択します。

Select All（すべて選択）をクリックするとすべての権限が選択されます。もう一度クリックすると、すべて選択解除されます。

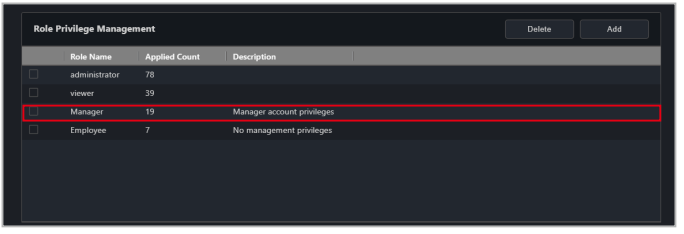


3. **Add（追加）**をクリックして新たな役割を追加します。

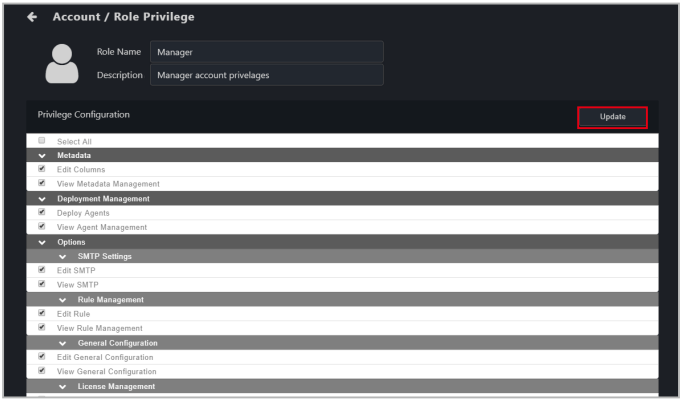


役割の編集

1. 編集する役割をクリックします。

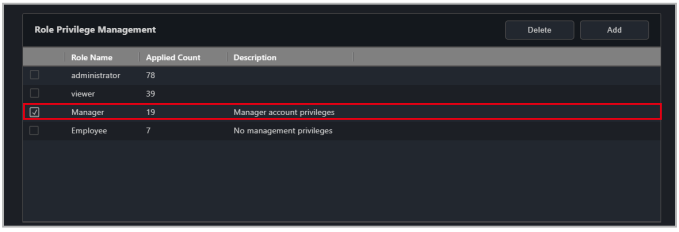


2. **Role Name（役割名）**と**Description（説明）**を編集したり、**Privilege Configuration（権限設定）**を編集することができます。終了したら**Update（更新）**をクリックします。



役割の削除

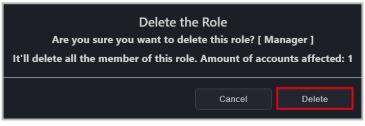
1. 削除する役割を選択し、**Delete（削除）**をクリックします。



2. アカウントの削除を確定し、**Delete（削除）**をクリックします。

プリセットされている役割は削除できません。

削除する役割が付与されているアカウントがある場合、その役割を削除するとアカウントも削除されます。役割の削除によって影響を受けるアカウントの数は、ポップアップメッセージで通知されます。



8.3 QRコード

QRコードをスキャンして、スマートデバイスでWeb版のASUS Control Center Expressに簡単にアクセスすることができます。

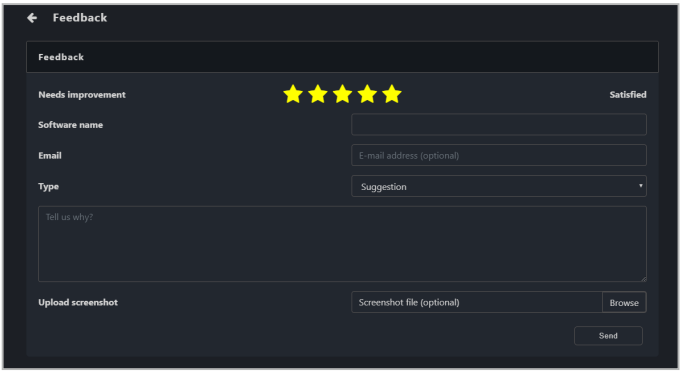
右上のメニューバーで をクリックし**QR Code**（**QRコード**）を選択すると**QR Code**（**QRコード**）の画面が開きます。

- QRコードをスキャンするスマートデバイスは、メインサーバーのIPアドレスに接続されている必要があります。
- メインサーバーのネットワーク環境がドメインまたはパーソナルネットワークの場合、QRコードをスキャンする前に、スマートデバイスが（WiFiルーターまたはVPN経由で）メインサーバーへ接続できることを確認してください。
- メインサーバーのネットワーク環境がパブリックネットワークを含む場合、QRコードをスキャンする前に、ドロップダウンメニューをクリックしてパブリックネットワークのQRコードに切り替えてください。

8.4 フィードバックの送信

フィードバック機能を使用して開発者へフィードバックを送信することができます。必要であれば、スクリーンショットをアップロードすることもできます。

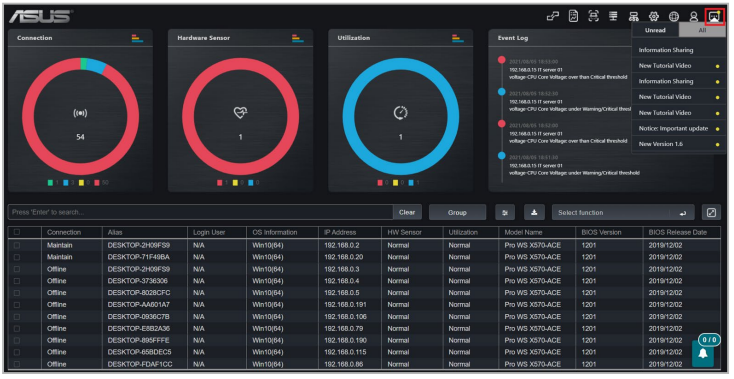
右上のメニューバーで をクリックし**Feedback**（**フィードバック**）を選択すると、フィードバックを送信できます。

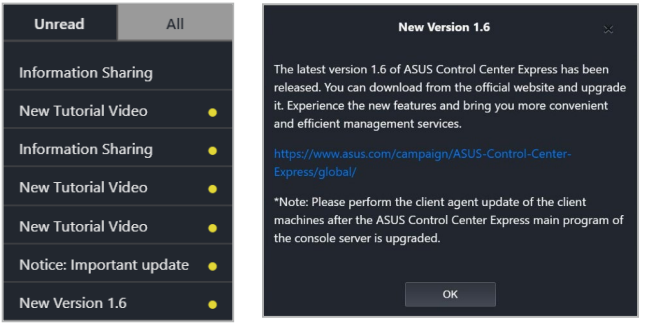


8.5 メールボックス

ASUS Control Center Expressでは、リリースされた最新の更新、更新通知、操作上の注意、新機能の紹介など、重要な情報や最新の更新情報をメールボックスから確認することができます。

Mailbox（メールボックス）内の項目を表示するには、右上のメニューバーにある をクリックします。



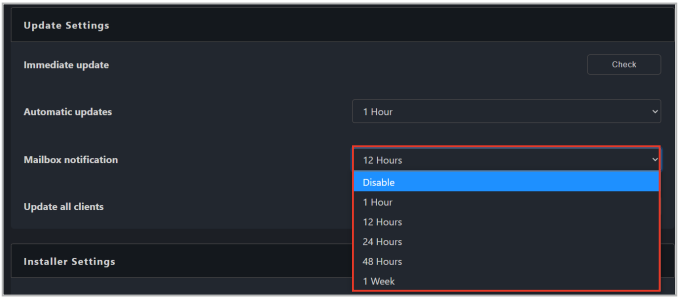


Unread（未読）	クリックすると、すべての未読メッセージが表示されます。メッセージをクリックすると、そのメッセージの詳細を確認することができます。
All（すべて）	クリックするとすべてのメッセージが表示されます。メッセージをクリックすると、そのメッセージの詳細を確認することができます。

Unread（未読）のメッセージには黄色のドットが表示され、メッセージを読むと黄色のドットは消え、次回**Mailbox（メールボックス）**にアクセスしたときに未読タブから削除されます。

8.5.1 メールボックスの通知設定

1. 右上のメニューバーの をクリックして、**Options（オプション）** > **General Configuration（全般設定）**を選択し、**Update Settings（更新設定）**までスクロールします。
2. 新規通知やメッセージ、プロンプトメール通知をチェックする頻度を、**Mailbox notification（メールボックス通知）**ドロップダウンメニューから選択します。



8.6 バックアップと復元

ASUS Control Center Expressメインサーバーのデータと設定をバックアップし復元することができます。ASUS Control Center Expressのインストール時に選択したデータベースの種類（MySQLまたはSQLite）の指示に従って操作してください。

- データと設定は定期的にバックアップすることを強くおすすめします。
- ASUS Control Center Expressを更新する前に、データと設定をバックアップすることを強くおすすめします。
- データセキュリティ上の理由から、バックアップデータは元のメインサーバー及びオペレーティングシステム上でのみ復元することができます。メインサーバーを交換したり、オペレーティングシステムを再インストールした場合、バックアップデータを復元することはできません。

8.6.1 MySQLデータベースに格納されたデータと設定の管理

ASUS Control Center Expressのインストール時にMySQLを選択した場合、ACCE DBtoolを使用するか、手動でデータと設定をバックアップおよび復元することができます。

データや設定をACCE DBtoolを使用してバックアップ、復元、修復する（推奨）：

1. メインサーバーで **スタート > ASUS Control Center Express** の順に進み、**ACCE DBTool** を右クリックして **管理者として実行** を選択します。

- MySQLデータベースを復元、修復、再インストールすると、現在のすべてのデータが削除されます。作業を開始する前に必ずバックアップをお取りいただくことを強くおすすめします。
- ASUS Control Center Expressを続けて使用する場合は、すべてのアクションが完了するまでお待ちください。

2. ファイルを開くプロンプトで、ASUS Control Center Expressのインストールディレクトリに移動し、データベースファイルを選択します。

ASUS Control Center Expressのフォルダーパスは、インストール時に選択したパスに応じて異なります。

3. MySQL通信ポートがデフォルト設定と異なる場合は、MySQL通信ポートを設定します。
4. ACCE DBToolを使用して、データのバックアップ、復元、再インストール、修復を行うことができます。
   詳しくは下記をご覧ください:
   - データをバックアップ: 現在のデータベースをバックアップします。
   - バックアップから復元: 選択したバックアップファイルからデータベースを復元します。
   - データベースの再インストール: MySQLデータベースを再インストールします。
   - データベースの修復: 選択したバックアップファイルにエラーがないかをチェックし修復を試みます。データベースが修復不可能なほど破損している場合、データは復元できないことがあります。

データや設定を手動でバックアップ、復元する:

1. メインサーバーでASUS Control Center Expressを終了し、**スタート > ASUS Control Center Express** の順に進み、**Stop ACCE Service** をクリックします。
2. 完全な管理者権限を持つコマンドプロンプトで、次のコマンドを入力してMySQLサーバーを停止します:

   sc stop DataStorage

```
C:\WINDOWS\system32>sc stop DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                               (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0x5265c00
```

3. 次のコマンドを入力してMySQLサーバーが完全に停止していることを確認します:

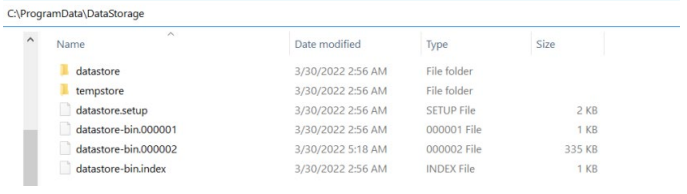
   sc query DataStorage

```
C:\WINDOWS\system32>sc query DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

必ず STATE が 1 STOPPED であることを確認します。

4. MySQLデータストレージディレクトリの内容をバックアップ先にバックアップします。



デフォルトのデータストレージディレクトリは C:\ProgramData\DataStorage に設定されています。

5. ファイルがバックアップされたら、コマンドプロンプトで次のコマンドを入力しMySQLサーバーを再起動します:

sc start DataStorage

```
C:\WINDOWS\system32>sc start DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x3a98
        PID                : 18652
        FLAGS              :
```

6. **スタート > ASUS Control Center Express** の順に進み、**Start ACCE Service** をクリックします。

データや設定を手動で修復する:

1. メインサーバーでASUS Control Center Expressを終了し、**スタート > ASUS Control Center Express** の順に進み、**Stop ACCE Service** をクリックします。
2. 完全な管理者権限を持つコマンドプロンプトで、次のコマンドを入力してMySQLサーバーを停止します:

sc stop DataStorage

```
C:\WINDOWS\system32>sc stop DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                               (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0x5265c00
```

3. 次のコマンドを入力してMySQLサーバーが完全に停止していることを確認します:

sc query DataStorage

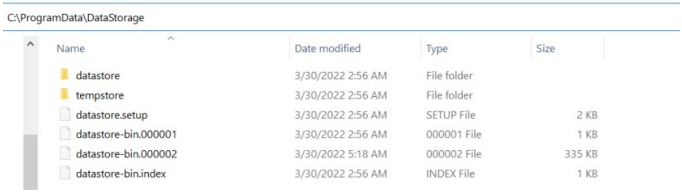
```
C:\WINDOWS\system32>sc query DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

必ず STATE が 1 STOPPED であることを確認します。

4. バックアップ場所からMySQLデータストレージディレクトリにバックアップをコピーし、**すべて置換** をクリックします。

デフォルトのデータストレージディレクトリは C:\ProgramData\DataStorage に設定されています。



5. ファイルの修復が完了したら、コマンドプロンプトで次のコマンドを入力しMySQLサーバーを再起動します:

sc start DataStorage

```
C:\WINDOWS\system32>sc start DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x3a98
        PID                : 18652
        FLAGS              :
```

6. **スタート > ASUS Control Center Express** の順に進み、**Start ACCE Service** をクリックします。

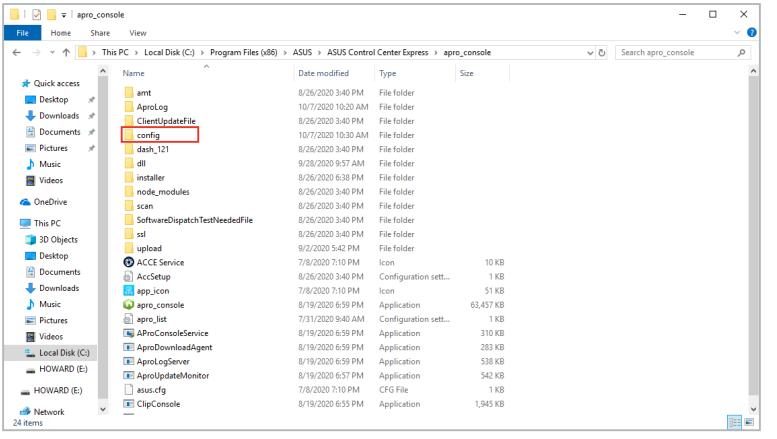
8.6.2 SQLiteデータベースに保存されているデータと設定のバックアップ

ASUS Control Center Expressのインストール時にSQLiteを選択した場合は、次の手順に従ってデータのバックアップを行ってください。

1. ASUS Control Center Expressがインストールされているメインサーバー上のフォルダを開きます。

- デフォルトのフォルダーは次の通りです：C:\Program Files（x86）\ASUS\ASUS Control Center Express
- ASUS Control Center Expressのフォルダーパスは、インストール時に選択したパスに応じて異なります。

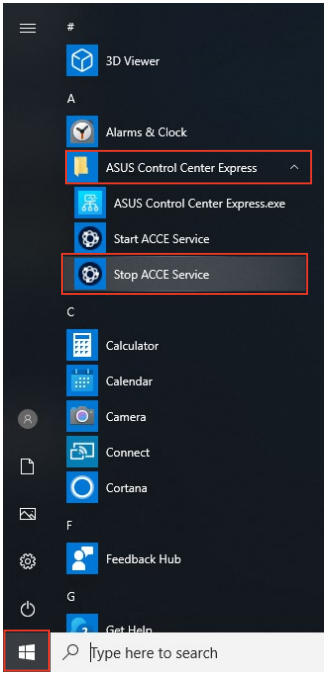
2. **apro_console**フォルダーへ進みます。
3. **config**フォルダーとフォルダー内のすべてのファイルをバックアップ場所にバックアップします。



8.6.3 SQLiteデータベースのデータと設定の復元

ASUS Control Center Expressのインストール時にSQLiteを選択した場合は、次の手順に従ってデータを復元してください。以前作成したバックアップデータから復元をする前に、現在のASUS Control Center Expressのデータと設定をバックアップすることをおすすめします。ASUS Control Center Expressのデータと設定のバックアップの詳細は、**8.6.2 SQLiteデータベースに保存されているデータと設定のバックアップ**を参照してください。

1. ASUS Control Center Expressが現在稼働しているか使用されている場合は、ASUS Control Center Expressを閉じて終了してください。
2. メインサーバーで、**Start（スタート）** > **ASUS Control Center Express**へ進み、**Stop ACCE Service（ACCEサービスの停止）**をクリックします。



3. 復元させるバックアップファイル（**config**）を選択し、**config**フォルダーとフォルダー内のすべてのファイルを含む**config**フォルダーをコピーします。

4. ASUS Control Center Expressがインストールされているメインサーバー上の**apro_console**フォルダーを開きます。

- デフォルトのフォルダーは次の通りです：C:\Program Files（x86）\ASUS\ASUS Control Center Express
- ASUS Control Center Expressのフォルダーパスは、インストール時に選択したパスに応じて異なります。

5. 手順3でコピーした**config**フォルダーとフォルダー内のすべてのファイルを**apro_console**フォルダー内に貼り付け、**config**ファイルとそのファイルをすべて置き換えます。
6. フォルダーとファイルを置き換えたら、**Start（スタート）** > **ASUS Control Center Express**へ進み、**Start ACCE Service（ACCEサービスの開始）**をクリックします。