ユーザーガイド

Avigilon ACC™ ES 分析アプライアンス

VMA-RPA-4P2 および VMA-RPA-4P4

本文書は、本文書が公開された時点での製品情報と仕様を編集および公開したものです。本文書の内容と文書内で説明されている製品の仕様は事前の通知無く変更されることがあります。Avigilon Corporation は、予告なくそのような変更を行う権限を有します。Avigilon Corporation やその関連会社は：（1）この文書の情報の完全性もしくは正確性を保証することはありません。（2）この情報の利用や信頼について責任を負うものではありません。Avigilon は、本書内の情報を信頼したことによるいかなる損害（間接損害を含む）にも責任を負うものではありません。

Avigilon Corporation
avigilon.com

20211019

このデバイスには、バッテリ駆動のリアルタイムクロック (RTC) 回路が付属しています。RCTバッテリの交換を正しく行わないと、爆発する危険があります。メーカー推奨、または同等の種類を交換してください。使用済みバッテリは、メーカーの指示に従って廃棄してください。

本機器は、工場外にルーティングされていないPoE ネットワークにのみ接続します。

目次

はじめに

Avigilon ACC ES Analytics Appliance は、ネットワークビデオ録画とサーバー側のビデオ分析を一体化したソリューションです。アプライアンスには次の機能があります。

- IP カメラを接続し、電力を供給するネットワーク スイッチ。
- Avigilon コントロールセンター サーバー ソフトウェアを実行するための内蔵サーバー。
- 接続済みのカメラで分類された対象物の検出を可能にするビデオ分析エンジン。

本書には、アプライアンスの電源が入り、ローカル エリア ネットワークに接続された後でシステムを構成する方法が記載されています。

始める前に

Avigilon推奨事項：

- ビデオ監視システムのハードウェアを保護するために、無停電電源装置（UPS）システムの使用。UPSシステムは、専用バッテリーを使用して、スパイク、電圧低下、変動、および完全な電源障害などの主電源の問題から重要な機器を保護するために使用されます。スタンバイ発電機を始動し同期させるのにかかる時間中に機器に電力を供給するためにも使用できます。

  可能な場合、UPS接続には、バッテリ残量が少ないか、15分の電力しか残っていない場合にアプライアンスのオペレーティングシステムをシャットダウンする設定を含める必要があります。
- 適切なネットワーク構成を設定するまで、カメラをアプライアンスに接続しないでください。

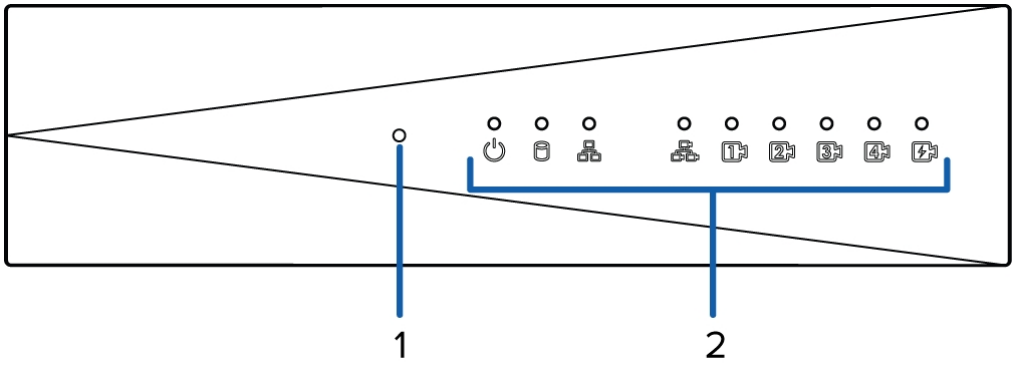
パッケージの内容

パッケージには次のものが同梱されていることを確認してください。

- Avigilon ビデオ アプライアンス
- 電源コード
- 電源装置とそれを固定するためのドライバー
- 壁面取り付け用ハードウェア
- デジタル入出力端子台コネクタ

概要

前面からの図



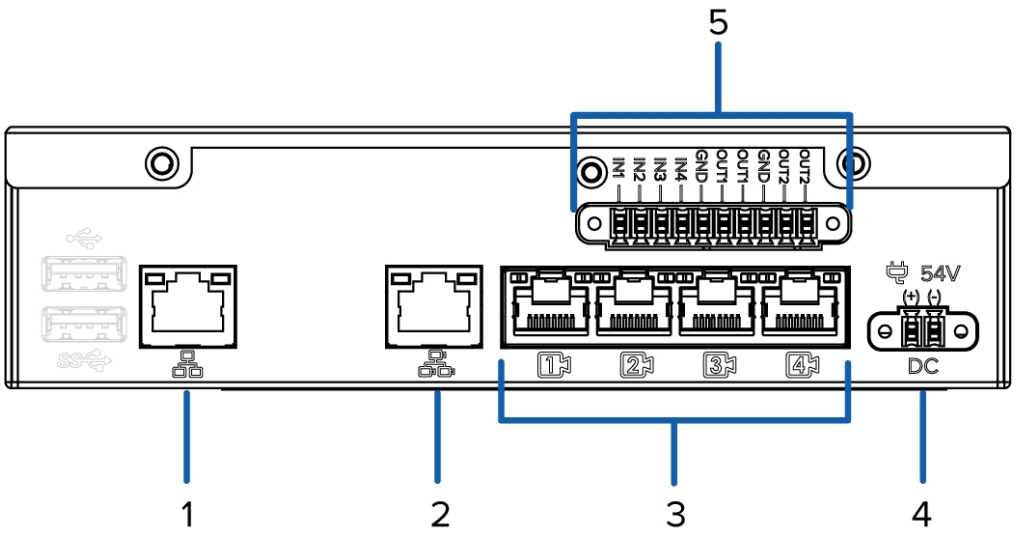
1. **リセット ボタン**

   このボタンを使用して、物理的にアプライアンスを再起動したり、工場出荷時の設定にリセットしたりします。

2. **ステータス LED**

   毎日の動作に関する情報を提供します。詳細については、「「LED インジケーター」（27ページ）」を参照してください。

背面からの図



1. **企業ネットワーク アップリンクポート**

   1GbE イーサネット接続で汎用ネットワークに接続して、ユーザーが Web インターエイスや接続済みのカメラビデオにアクセスできるようにします。

2. **カメラ ネットワーク アップリンクポート**

   1GbE イーサネット接続で、PoE スイッチ コンポーネントに接続されているカメラに接続できるようにします。他の PoE スイッチやカメラへのリンクとして使用できます。

3. **PoE スイッチ コンポーネント**

   カメラを 10/100速度の PoE スイッチ コンポーネントに接続して、カメラに電力を供給したりビデオを録画したりします。

4. **電源コネクタ**

   アプライアンスに対する電源を受け入れます。

5. **I/O コネクタ**

   外部入出力装置に接続します。詳細については、「「外部電源の接続」（25ページ）」を参照してください。

システム要件

カメラのフレームレート

ACC ES Analytics Appliance は分析用ではないカメラでも分析の機能を提供します。最適な分析パフォーマンスを達成するには、ソースカメラで 1 秒当たり最低 10 枚の画像を配信する必要があります。

Web ブラウザ

アプライアンスの管理設定は、次のいずれかのWebブラウザを使用して、任意のWindows、Mac、またはモバイルデバイスからアクセスされるWebインタフェースを介して管理されます。

- Mozilla Firefoxブラウザバージョン 3.6 以降
- Google Chrome ブラウザ 8.0 以降
- Microsoft Edge ブラウザ 25 以降
- Safari 5.0 以降
- Android 版 Chrome 2.2 以降
- Apple iOS 版 Safari 5 以降
- Windows Internet Explorer ブラウザバージョン 7.0 以降

メモ：Web ブラウザでクッキーを許可するように設定しておかないと、Web インターフェイスは正しく機能しません。

サポート対象のネットワーク構成

メモ：カメラのアップリンクポートでは動的切替えの DHCP サーバーをサポートしていません。

ネットワーク接続	カメラの Web インターフェイスアクセス	サポート対象のIP構成		メモ
		企業の LAN アップリンク	カメラの LAN アップリンク	
企業の LAN アップリンク専用	いいえ	静的/DHCP の割り当て	未接続（DHCP として残す）	カメラの LANアップリンクと接続済みカメラは Zeroconf IP アドレスを使用します。
カメラの LAN アップリンク専用	はい	未接続（DHCP として残す）	静的、DHCP割り当て、DHCP-Zeroconf	
企業とカメラの LANアップリンク	カメラの LAN アップリンク専用経由	静的、DHCP割り当て、DHCP-Zeroconf	静的、DHCP割り当て、DHCP-Zeroconf	企業とカメラの LANアップリンクは、別々のサブネットに配置する必要があります。

初回のACC ES Analytics Applianceの起動

ACC ES Analytics Applianceの電源を入れてから、以下の手順を完了します。

1. アプライアンスのポートをイーサネットケーブルでローカルネットワークに接続します。
2. アプライアンスの前面の電源ボタンを押して、アプライアンスが起動するのを待ちます。
3. ネットワークワークステーションで、アプライアンスを検出します。Windowsコンピュータではエクスプローラーを、MacintoshコンピュータではFinder®を使用します。
4. ブラウザで表示されたすべての接続メッセージをクリックしてください。ブラウザによっては2つの警告メッセージが若干異なります。例えば、ブラウザが…
    - Chromeの場合ー最初の画面で**Advanced（高度）**をクリックして、2番目の画面で**Proceedto<*IP address*>（unsafe）（<IPアドレス>（危険）に進む）**をクリックします。
    - Firefoxの場合ー最初の画面で**Advanced（高度）**をクリックして、2番目の画面で**Add Exception（例外を追加）**をクリックし、**Permanently store this exception（この例外を永久保存）**にチェックを入れて**Confirm Security Exception（セキュリティの例外を確認）**をクリックします。
5. サーバー管理ページで指示が表示されたら、管理者ユーザー名の新しいパスワードを入力します。

    強度メーターはパスワードの複雑さを測定します。赤は単純すぎ、黄は合理的に複雑、緑は複雑です。複雑さは、パスワードの安全性ではなく、パスワードを検出することの難しさを測定します。複雑なパスワードをお勧めします。

    ページが更新され、ログインするよう求めるメッセージが表示されます。
6. ユーザー名に「`administrator`」と入力し、新しいパスワードを入力します。

    サーバー管理ページ のダッシュボートパネルが表示されます。
7. サーバー管理ページの言語、ユーザーフレンドリーなホスト名とタイムゾーンを設定します。ナビゲーションサイドバーで、**デバイス**をクリックしデバイスページを開きます。
    で：
    a. 一般ドロップダウンリストから言語を選択します。
    b. ホスト名ペインで、オプションとしてアプライアンスのシリアル番号をアプライアンスの記述ホスト名に入れ替えることができます。
    c. 時刻ペインで、タイムゾーンを指定し、NTPドロップダウンとサーバーリストでタイムソースを特定します。

    詳細については、「デバイス設定の管理」（14ページ）を参照してください。

8. アプライアンスがネットワークからIPアドレスを取得する方法を選択します。ナビゲーションサイドバーで、**ネットワーク**をクリックしネットワークページを開きます。使用されている各ネットワークポートのために、自動を選択するか、手動で設定を入力します。

   詳細については、「「デバイスをカメラとACC Clientユーザーに接続する」（16ページ）」を参照してください。

サーバー管理ページの詳細については、「サーバー管理 の使用」（9ページ） を参照してください。

これで、 ACCClient ソフトウェアをインストールし、 ACC ES Analytics Appliance を ACCサイトに接続する準備ができました。

トラブルシューティング

Webブラウザからサーバー管理ページにアクセスする

ACC Clientを使わずにサーバー管理ページにアクセスしたい場合があります。

よく使われるWebブラウザを使用して、Windows®、Apple、またはモバイルデバイスからサーバー管理ページアクセスにできます。

> **メモ：**Web ブラウザでクッキーを許可するように設定しておかないと、Web インターフェイスは正しく機能しません。

1. ネットワークワークステーションで、アプライアンスを検出します。ファイルエクスプローラー（Windows）またはFinder®（Apple）を使用します。

   「VMA-RPA-4Px-<シリアル番号>」とういラベルの付いたデバイス、またはこのデバイスのサーバー管理ページで構成したホスト名を探しています。

2. ブラウザで表示されたすべての接続メッセージをクリックしてください。ブラウザによっては2つの警告メッセージが若干異なります。ブラウザが…
   - Chromeの場合ー最初の画面で**Advanced（高度）**をクリックして、2番目の画面で**Proceedto<*IP address*>（unsafe）（<IPアドレス>（危険）に進む）**をクリックします。
   - Firefoxの場合ー最初の画面で**Advanced（高度）**をクリックして、2番目の画面で**Add Exception（例外を追加）**をクリックし、**Permanently store this exception（この例外を永久保存）**にチェックを入れて**Confirm Security Exception（セキュリティの例外を確認）**をクリックします。

3. 管理者 としてログインします。

   サーバー管理ページ のダッシュボートパネルが表示されます。

デバイスを検出できません

ネットワークワークステーションからネットワークに接続されているデバイスを見つける方法はいく通りかあります。デバイスを検出するための推奨される順序は次のとおりです：

- アプライアンスがイーサネットケーブルでローカルネットワークに接続されていることを確認します。
- デバイスの電源が入っていることを確認します。入っていない場合、アプライアンスの前面の電源ボタンを押して、アプライアンスが起動するのを待ちます。
- ファイルエクスプローラー (Windows) またはFinder (Apple) の使用

  「VMA-RPA-4Px-<シリアル番号>」とういラベルの付いたデバイス、またはこのデバイスのサーバー管理ページで構成したホスト名を探しています。
- ACCクライアントソフトウェアからDHCPで割り当てられたIPアドレスを検出します。
  - 次の命名規則を使用するサイトにログインします: VMA-RPA-4Px-<シリアル番号>。

    メモ： Web インターフェイスアプリケーションのユーザー名とパスワードは、ACC サーバーの管理者ユーザー名とパスワードとは別です。
- https://VMA-RPA-4Px-<シリアル番号> の URL を使用してウェブ ブラウザからアプライアンスにアクセスします
- アドレス解決プロトコル（ARP）を使用して、デバイスのIPアドレスを決定します：
  1. シリアル番号タグに記載されているMACアドレス（MAC）を見つけます。
  2. コマンド プロンプト ウィンドウを開いて、以下のコマンドを入力します:

     ```
     arp -a
     ```
  3. 応答をスクロールし、MACアドレスに対応するIPアドレスを探します。

上記のいずれの方法も問題を解決できない場合は、Avigilonテクニカルサポートにお問い合わせください。

ネットワーク構成

デフォルトでは、ACC ES Analytics Appliance が DHCP を通じてネットワーク上の IP アドレスを取得します。静的 IP アドレスや特殊なネットワーク構成を使用するために ACC ES Analytics Applianceを設定する必要がある場合、「デバイスをカメラとACC Clientユーザーに接続する」（16ページ） ファイルで詳細を参照してください。

システムヘルスの監視

ACC Client ソフトウェアでサイトヘルス におけるシステムコンポーネントのヘルスを監視することができます。詳細については、ACC Clientソフトウェアで提供されるヘルプファイル、またはAvigilon Webサイトから入手できる *Avigilon ACC Client*ユーザー ガイドを参照してください。

サーバー管理 の使用

ACC ES Analytics Applianceは、サーバー管理で構成できますが、これはACC Clientアプリケーション（既存のマルチサーバーサイトにアプライアンスを追加する場合）、またはアプライアンスと同じネットワーク上のワークステーション上の互換性のあるブラウザからアクセスできます。サーバー管理を使用すると、アプライアンスサーバー設定を行い、サーバーによる時間の記録方法などを設定し、さらにサーバーをリモートから再起動させたり、アップグレードしたりすることができます。アプライアンスがサイトにデプロイされた最初の（または唯一の）ACCサーバーである場合は、サーバー管理にブラウザを使用してアクセスし、アプライアンスを構成した後、ACC Clientソフトウェアをワークステーションへダウンロードし、アプライアンスでACCサーバーソフトウェアをアクティベートします。このセクション全体を通して、デバイスという用語は、アプライアンスと同じ意味で使用されます。

アプライアンスを構成した後、レコーダーのシステム設定のバックアップを開始します。これらの設定には、 ACCのパスワード、およびカメラ接続の設定が含まれます。サイトおよびサーバー構成のバックアップの詳細については、ACC Clientソフトウェアで提供されるヘルプファイル、またはAvigilon Webサイトから入手できる*Avigilon ACC Client*ユーザー ガイドを参照してください。

このセクション全体を通して、デバイスという用語はレコーダーと同じ意味で使用されます。

サーバー管理の開始と停止

次のいずれかの方法を使用して、デバイスへのネットワークアクセスを持つ任意のネットワークワークステーションから、サーバー管理を開始してログインします。

- **ACC Client ソフトウェアから直接：**
    a. ACC Client ソフトウェアを起動します。
    b. System Explorer からサイトにログインします。
    c. 新しいタスクメニュー で、[**サイトのセットアップ**]をクリックします。
    d. System Explorerでデバイスを選択し、**サーバー管理** をクリックして、デバイスのサインインページを開きます。
- **ウェブブラウザからのブックマーク付き：**
    次のいずれかの方法を使用して、ブックマークを作成します：

- デバイスを発見します
    a. ファイルエクスプローラー (Windows) またはFinder (Macintosh) で [ネットワーク] タブを開き、デバイスを探します。
    b. 「VMA-RPA-4Px-<シリアル番号>」とういラベルの付いたデバイス、またはこのデバイスのサーバー管理ページで構成したホスト名を探しています。

       デバイスが見つからない場合は、「トラブルシューティング」（6ページ）を参照してください。
    c. 右クリックして**デバイスのWebページを表示**を選択し、デフォルトのWebブラウザでデバイスのサインインページを開きます。
    d. デバイスのサインインページをブックマークします
- IPアドレスまたはホスト名を使用する
    a. デバイスへのネットワークアクセスを備えたネットワークワークステーションからWebブラウザを開きます。
    b. WebブラウザにIPアドレスまたはホスト名を入力して、デバイスサインインページを開きます：

       https://<*Device IP address* >|<*Device hostname*>/

       例：

       - `https://169.254.100.100/` 、 `169.254.100.100` はデバイスパネルで構成されたIPアドレスです。
       - `https://my_AvigilonDevice/`、ここでは `my_AvigilonDevice/` がデバイス パネルで設定されたホスト名です。

       > **メモ：**インストールプロセス時に設定したIPアドレスまたはホスト名を思い出せない場合、その情報はサーバーの[セットアップ]タブにあるACCクライアントソフトウェアに記載されています。

    c. デバイスサインインページをブックマークします。

サーバー管理からログアウトして停止するには、サーバー管理タイトルバーの右側にあるログアウトアイコンをクリックします。

PoEポートのステータスの表示

「PoE」パネルでは、各ポートのステータスが [ステータス] 列に表示されます。次の状態があります。

緑色	一定出力	PoE デバイスがポートに接続され、正常に動作しています。
	高出	PoE +がオンになっています。

	カ	
灰色	切断	ポートに接続されているデバイスがありません。
	出力なし	PoEポートの電源は、サーバー管理のPoEページからスイッチオフされます。
黄色	過負荷	PoE デバイスはポートに接続されていますが、電力を受け取っていません。このステータスは、通常、一つのポートが過電流の場合や、デバイスが配分以上の電力を要求している場合などに生じます。
	低出力	デバイスはポートから低電流を得ています。
赤	エラー	デバイスがエラー状態です。

ヒント：カメラを外した後で再度デバイスに接続した場合、このページを更新して最新のステータスを確認し、値を配分しなければならないことがあります。

ACCサービスを管理する

サーバーパネルでは：

- 一般 ペイン：

タスク	操作
デバイスをシャットダウンする前に、すべてのサービスをシャットダウンします。	[**停止**] をクリックします。
サービスがシャットダウンされた後ですべてのサービスを起動します。	[**開始**] をクリックします。
ACC ES Analytics Applianceをリセットします	**リセット**をクリックします。
ストレージドライブをフォーマットします。	**再初期化**をクリックしてすべての設定と記録映像データを削除します。

- ネットワーク ストレージ管理ペインで、ACC Clientアプリケーションユーザーが ACC ES Analytics Applianceからビデオをアーカイブできるようにします。「ACC Client ウイがビデオをアーカイブできるようにする」（12ページ） を参照してください。
- [サービスおよびRTPポート] ペインを確認して、ACC ES Analytics Applianceとの通信に使用するUDP ポートと TCP ポートを変更します：
  - サービス ポートペインで、HTTP、HTTPSおよびUDPポートに使用する**基本**値を入力し、**適用**をクリックします。ポートのリストが更新されます。
  - RTP ポートペインで、UDPポートに使用される**基本**値を入力して**適用**をクリックします。RTPで利用可能なポートの範囲が更新されます。

重要：これらの変更は、システムの再起動後にのみ有効になります。プロンプトが表示されたら、システムを再起動します。

ACC Client ウイがビデオをアーカイブできるようにする

ACC Client アプリケーションのユーザーがACC ES Analytics Applianceからビデオをアーカイブできるようにするには：

1. ナビゲーションバーから、**サーバー**パネルを開きます。
2. ネットワーク ストレージ管理ペインで、**有効**をクリックします。
3. [Protocol(プロトコル)] ドロップ ダウン リストで、次のいずれかを選択します。
    - **CIFS(CIFS)** — 共通のインターネット ファイル システム。ネットワーク パスは一般的に次の形式を取ります：//<ホスト名または *IP*> / <パス>
    - **NFS(NFS)** — ネットワーク ファイル システム。ネットワークパスは一般的に次の形式を取ります：<ホスト名または*IP*> ： <パス>
4. [**ネットワークパス**]フィールドに、希望のビデオアーカイブロケーションへのパスを入力します。
5. ネットワーク ロケーションに認証が必要な場合、[**ユーザー名**] と [**パスワード**] フィールドに認証資格情報を入力します。
6. [**適用**] をクリックします。

サポートにサーバー ログとシステム ログを提供します

ログパネルを使って、サーバー ログそしてシステム ログペインを表示し、Avigilonテクニカルサポートによって要求されたログファイルを準備し、問題を解決します。

通常、 Avigilonテクニカルサポートは、このパネルのログにアクセスしてフィルタリングし、必要なログを分離するのに役立ちます。次に、ログをコピーしてテキストファイルに貼り付け、保存して、 Avigilonテクニカルサポートに送信します。

デフォルトでは、ログからの 100 件の警告メッセージがログペインに表示されます。

ログをフィルタリングして、必要な上布を表示することができます。

1. ドロップダウン リストで、必要なアプリケーション ログの種類を選択します。
    - サーバー ログの場合：
        - **例外ログ**
        - **FCP ログ**
        - **サーバー ログ**
        - **WebEndpoint ログ**
    - システム ログの場合：
        - **システム ログ**
        - **ブート ログ**
        - **Web サーバー ログ**

2. [**最大ログ**] ドロップダウン リストから、毎回表示させるログ メッセージの数を選択します。
3. **フィルター**フィールドにテキストを入力して、ログリストにフィルターを適用します。
4. 更新ログを表示するには**Sync（同期）**ボタンをクリックします。

デバイス設定の管理

ナビゲーションバーで、デバイスをクリックします。

タスク	デバイスパネルカードで...	設定
サーバー管理の言語を変更します	**一般**	ドロップダウン**言語**リストから言語を選択してください
デフォルトのサーバー名をユーザーフレンドリーなホスト名に置き換えます	**ホスト名**	**ホスト名**を変更します。 デフォルトのホスト名はサーバー名と同じです。サーバー名は、フォーム<モデル>-<シリアル番号>にあります。
タイムゾーンを設定します	**時刻**	**タイムゾーン**を指定し、**NTP**ドロップダウンと**サーバー**リストでタイムソースを特定します。「時間設定の管理」（15ページ） を参照してください。
ACC ES Analytics Appliance管理者のパスワードを変更します。	**パスワード**	「ACC ES Analytics Appliance管理者パスワードを変更する」（14ページ） を参照してください。
デバイスに最新バージョンのファームウェアをインストールします。	**ファームウェアのアップグレード**	「ファームウェアをアップグレードする」（33ページ）を参照してください。
ACC ES Analytics Applianceとサーバー管理が使用する証明書を管理します。	**証明書**	「証明書を管理する」（29ページ） を参照してください。

ACC ES Analytics Appliance管理者パスワードを変更する

変更できるのはパスワードのみで、サーバー管理のデフォルトの管理者ユーザー名は変更できません。

1. ナビゲーションバーで、**デバイス**をクリックします。
2. [一般]パネルで、**パスワード**ペインを見つけます。
3. [**古いパスワード**] フィールドに現在のパスワードを入力します。
4. **新しいパスワード**と**パスワードの確認**フィールドに新しいパスワードを入力します。

   複雑なパスワードをお勧めします。

パスワードを安全な形式と場所に物理的またはデジタル的に保存してパスワードを忘れた場合に取得できるようにし、前のパスワードの記録を破棄します。

⚠ **注意 ー** パスワードを忘れた場合、録画されたビデオと設定データは失われます。管理者パスワードをリセットするには、デバイスを工場出荷時のデフォルト設定にリセットする必要があります。こうすると、ハードドライブがフォーマットされて、構成データと録画ビデオも削除されます。工場出荷時の設定への復元の実行方法については、「工場出荷時の設定への復元」（35ページ）を参照してください。

時間設定の管理

ACC ES Analytics Appliance時間の管理方法をカスタマイズします：

1. ドロップダウンリストから [**タイムゾーン**] を選択します。あなたがここで設定したタイムゾーンはACCクライアントソフトウェアで定義された録画スケジュールで使用されています。
2. NTPフィールドで、ネットワークタイムプロトコル（NTP）サーバーにより同期された時間を維持する（推奨）かどうかを選択します。

   ヒント：ONVIFデバイス（つまり、Avigilon以外のカメラ）と時刻を同期するには、ACC ES Analytics Applianceのポート123に接続して、NTPサーバーとして使用できます。

   選択：

   - **DHCP**ーネットワークで自動的に既存のNTPサーバーを使用する。
   - **手動**ーこのオプションを選択し、続いてNTPサーバーのアドレスを[サーバー]リストに入力します。リスト内のアドレスを追加および削除し、それらを並べ替えるコントロールがアクティブになります。
   - **オフ**NTPサーバーを使用していない場合。

メモ：NTPサーバーのデフォルトのセットは、常にサーバーリストにあります。ただしこのリストは、NTPが有効になっていて、DHCPサーバーによって提供されていない場合にのみ使用されます。デフォルトのリストは再配置または削除できません。

- 0.pool.ntp.org
- 1.pool.ntp.org
- 2.pool.ntp.org
- 3.pool.ntp.org

3. [**適用**] をクリックして、時間設定を保存します。

ストレージを管理する

ストレージパネルには、ACC ES 4および8ポートアプライアンス（または古い4ポートACC ESアプライアンスのドライブ）のデバイスのストレージ容量と、ストレージドライブのステータスを表示できます。

ストレージパネルを開くには、ナビゲーションバーの**ストレージ**をクリックします。ストレージパネルのペインで次のどのアクションも実行できます：

タスク	操作
ストレージドライブの容量とステータスを表示します。	[物理ディスク] パネルには、モデルやシリアル番号など、各物理ディスクに関する情報が一覧表示されます。 ストレージドライブが次の場合： • 正しく機能している場合、**準備完了**が表示されます。 • 正しく機能していない場合、いくつかのエラー状態の1つが表示されます。

デバイスをカメラとACC Clientユーザーに接続する

ネットワークパネルでは、デバイスのネットワーク接続を変更できます。2 つのネットワーク接続をサポートしています。1 つは企業ネットワークを対象としたもので、もう 1 つはカメラ ネットワークを対象としたものです。

メモ：企業ネットワークとカメラネットワークを異なるIPサブネット上に配置する必要があります。

企業ネットワークは、通常、ユーザーにデバイスへのアクセスを提供するネットワークです。ACC Client ソフトウェア経由でビデオをモニタするユーザーは、このネットワーク経由でデバイスに接続します。

カメラ ネットワークは、通常カメラのみが含まれる閉じられたネットワークです。これにより、録画に対する干渉の量が少なくなります。

ONVIF デバイスをカメラネットワークに接続する際、アプライアンスをその時刻/NTP サーバーとして使用するように構成します。

ネットワーク接続に関する詳細は、「サポート対象のネットワーク構成」（4ページ）を参照してください。

ネットワークパネルの各ペインで次のどのアクションでも実行できます。

タスク	操作
デバイスがネットワークごとに IP アドレスを取得する方法を設定する	自動 IPをオンにすると、接続されているネットワークを自動的に検出し（デフォルト設定）、手動で接続を指定するにはオフにします。手動で接続設定を入力する場合は、以下のフィールドに適切な値を入力します。 ネットワークパネルの各ペインで、接続されたネットワークを自動的に検出するには**自動 IP**をオンに切り替え（デフォルト設定）、手動で接続を指定するにはオフにします。手動で接続設定を入力する場合は、以下のフィールドに適切な値を入力します。 • **IP アドレス** • **サブネット マスク** • **デフォルト ゲートウェイ** [**適用**] をクリックして、変更を保存します。
デバイスが DNS サーバーから名前付きアドレスを取得する方法を設定します。	**自動 DNS**をオンにすると、接続されているDNSサーバーが自動的に検出され（デフォルト設定）、手動でDNSサーバーを指定するにはオフにします。**自動 DNS**を切り替えると、リスト内のアドレスを追加および削除し、それらを並べ替えるコントロールがアクティブになります。

PoE 電源予算の割り当て

PoEパネルを使って、接続されているデバイスにどれだけの電力が供給可能であり、また使用されたかを確認します。すべてのポートのデフォルト設定は自動です。この設定は、ポートに接続されたデバイスが必要とする電力量を自動的に検出し、配分を設定します。各ポートについて、この設定を手動で調整するか、電源出力を完全にオフにすることができます。手動でポートの電力出力を調整する場合は、PoE 電力配分を計算する場合は、「PoE 電源への電力配分」（26ページ）を参照してください。

> **ヒント：**高電力 PoE を必要とするカメラにミッドスパン PoE パワーインジェクタを使用している場合は、その PoE ポートをオフに設定する必要があります。

PoEパネルを開くには、次のいずれかを実行します。

- サーバー管理起動ページのPoEステータスパネルの⚙をクリックします。
- ダッシュボードのナビゲーションバーから**PoE**をクリックします。

タスク	操作
接続されているデバイスにどれだけの電力が供給可能であり、また使用されたているかを確認できます。	パネルの上部にある2つのバーを見てください。 • **電源容量**バーは、PoEポートに接続されているすべてのデバイスに割り当てられている総電力量を示します。 • **消費量**バーは、接続されているすべてのデバイスで現在使用されている実際の電力量を示します。
各PoEポートが使用する電力を調整します。 > **ヒント：**また、**電力**バーを使用して、カメラをリモートで再起動することもできます。[電力] 設定を [オフ] に設定したら、カメラの電源が切れるのを待ち、続いて [電力] 設定を [**自動**] または**手動**に変更します。 > **ヒント：**PoEとPoE +（802.3at）の両方の動作モードに対応するデバイスは、手動の15W配分を使用して非PoE +モード（802.3af）に強制することができます。	に**電力**バーを使用して、PoE電力配分を設定します。 • **オフ**をクリックしてポートへの電力出力を無効にします。ポートへの電力が無効になると、ポートは電力を出力しなくなりますが、任意のデバイスの標準ネットワーク接続の機能を果たすことができます。 • **自動**をクリックして、接続されたデバイスの動作モードに応じてデバイスに自動的に電力が出力されるようにします。 • **手動**をクリックして、ワット単位で電力配分値を入力します。ケーブルの電力損失の可能性も配分に含めるようにしてください。

設定は [**適用**] をクリックするまで実装されません。

[**適用**] をクリックしたら、次のメッセージが表示されたときにシステムが再起動することを許可します。

> 変更内容を適用すると、*PoE*受電デバイスに対して電源サイクルが実行される可能性があります。

サーバー管理によって画面が自動更新され、新しい電力設定の適用が完了すると、更新された設定が表示されます。

サポートのためのデバイスログの提供

システム ログパネルを使用してデバイスのログを表示します。問題解決に役立てるために、通常 Avigilon テクニカルサポートからログを求められます。

デフォルトでは、ログからの 100 件の警告メッセージがページに表示されます。

通常、 Avigilonテクニカルサポートは、このパネルのログにアクセスしてフィルタリングし、必要なログを分離するのに役立ちます。次に、ログをコピーしてテキストファイルに貼り付け、保存して、 Avigilon テクニカルサポートに送信します。

ログをフィルタリングして、必要な上布を表示することができます。

1. ドロップダウン リストで、必要になるアプリケーション ログの種類を選択します。オプションは次のとおりです。
   - **システム ログ**
   - **ブート ログ**
   - **Web サーバー ログ**
2. [**最大ログ**] ドロップダウン リストから、毎回表示させるログ メッセージの数を選択します。
3. **フィルター**フィールドにテキストを入力して、ログリストにフィルターを適用します。
4. 更新ログを表示するには**Sync（同期）**ボタンをクリックします。

ACC Clientのインストール

セキュリティネットワークに最初のAvigilonアプライアンスをインストールする場合、サーバー管理ページへのアクセスに使用しているコンピュータにACC Client ソフトウェアをインストールできます。それ以外の場合は、ネットワークワークステーションでACC Client ソフトウェアを使用して、アプライアンスをセキュリティネットワークの新しいサイトとして追加するか、または既存サイトにマージします。

重要：アプライアンスを新しい ACC サイトとして追加するか、またはアプライアンスを既存の ACC サイトにマージする前に、IP アドレスを設定します。同サイト内の他のサーバーと同じ IP サブネットに配置することを強くお勧めします。

インターネットへのネットワークアクセスが可能なネットワークワークステーションにACC Client ソフトウェアの最新バージョンをインストールできます：

1. インターネットへのネットワークアクセスを備えたネットワークワークステーションからWebブラウザを開きます。
2. ACC Client ソフトウェアを、Avigilon Web サイト**avigilon.com/support/software**からダウンロードします。ACC Client ソフトウェアの最新バージョンのインストールソフトウェアにクリックスルーします。

   メモ：ソフトウェアをダウンロードするWebサイトに初めてアクセスすると、登録を求められます。必要な情報をすべて入力し、 **登録の完了**をクリックします。登録は自動的に承諾され、Webサイトに進みます。
3. ACC Client ソフトウェアを、デバイスへのネットワークアクセスを備えたワークステーションにインストールします。

ACCソフトウェアをアクティベートして、Avigilonクラウドサービスに接続する

ACC ES Analytics Appliance を展開したら、ACCソフトウェアと機能のライセンスをアクティベートし、Avigilonクラウド サービスに接続します。

ACCソフトウェアおよび機能ライセンスをアクティベートする

製品または機能のライセンスをアクティブ化、非アクティブ化、および再アクティブ化できます。ライセンスは、ACC システムではプロダクトキー、ライセンスのポータルではアクティベーション ID と呼ばれています。

重要：新規サーバーをマルチサーバーサイトに追加または削除すると、既存のサイトのライセンスは非アクティブになり、システムの変更を確認するために再度アクティベートする必要があります。「ライセンスの再アクティブ化」（23ページ） を参照してください。

- **ACC™ システム初期設定およびワークフロー ガイド**
- **ACC 7ヘルプセンター**

これらのガイドの印刷用バージョンは次のAvigilonウェブサイトでご覧いただけます：**avigilon.com/support/software/**。

ライセンスをアクティブ化すると、ライセンスを受けた新しい機能をすぐに使用できます。

Avigilonクラウド サービスへ接続する

それにより、ACCソフトウェアをアクティベートした後、ACCサイトではサブスクリプションが必要な場合がありますが、クラウドに接続し、分散システム全体に集中型アクセスを提供する機能を利用できます。

サイトをAvigilon クラウド サービスに接続するには、**help.avigilon.com/cloud** を参照してください。

クラウド サービスに関する情報については、**Avigilon クラウド サービス サポート**を参照してください。

ACC Client ソフトウェア構成後、新しいサイトのシステム設定のバックアップを開始できます。これらの設定には、 ACCのパスワード、およびカメラ接続の設定が含まれます。サイトおよびサーバー構成のバックアップの詳細については*Avigilon ACC Client*ユーザーガイドを参照してください。

ライセンスのアクティブ化

ライセンスをアクティブ化すると、ライセンスを受けた新しい機能をすぐに使用できます。

ヒント：新しいサーバーを追加するたびにサイトライセンスが再アクティベートされるのを防ぐために、新しいライセンスをアクティベートする前にマルチサーバーサイトの整理を完了してください。

将来の参照のためにライセンスのコピーを保管してください。

インターネット経由のアクティブ化

インターネット アクセスがある場合、オンライン アクティベーションを使用してください。ただし、ウェブサイトが大きく、数百のライセンスが含まれている場合は、サーバーがタイムアウトすることがあります。代わりに「オフライン アクティベーション」（22ページ）を参照してください。

1. 新しいタスクメニュー で、[**サイトのセットアップ**]をクリックします。
2. 新しいサイトを選択し、 をクリックします。
3. [**ライセンスの追加…**] をクリックします。
4. プロダクト キーを入力してください。

   1つまたは複数のコンマで区切りられたプロダクト キーをコピーして貼り付けると、システムが自動的にフォーマットします。

   - 最新のプロダクト キーを削除する必要がある場合、[**最新のキーを削除**] をクリックします。
   - プロダクト キー全部を削除するには、[**クリア**] をクリックします。
5. [**今すぐ起動**] をクリックします。
6. [**OK**] をクリックします。

オフライン アクティベーション

オフライン ライセンスは ACC Client ソフトウェアとインターネット回線付きのコンピュータを実行しているコンピュータ間でファイルを転送する必要があります。

ACC Client：

1. 新しいタスクメニュー で、[**サイトのセットアップ**]をクリックします。
2. 新しいサイトを選択し、 をクリックします。
3. [**ライセンスの追加…**] をクリックします。
4. [**手動**] タブを選択します。
5. プロダクト キーを入力してください。

   1つまたは複数のコンマで区切りられたプロダクト キーをコピーして貼り付けると、システムが自動的にフォーマットします。

- 最新のプロダクトキーを削除する必要がある場合、[**最新のキーを削除**] をクリックします。
- プロダクト キー全部を削除するには、[**クリア**] をクリックします。

6. [**ファイルの保存…**] をクリックして、`.key` ファイルを保存する場所を選択します。必要に応じてファイル名を変更できます。
7. `.key` ファイルをインターネットに接続しているコンピュータにコピーします。

ブラウザの場合：

1. activate.avigilon.com にアクセスします。
2. [**ファイルの選択**] をクリックし、`.key` ファイルを選択します。
3. [**アップロード**] をクリックします。`capabilityResponse.bin` ファイルは自動的にダウンロードされるはずです。

   ダウンロードされない場合、プロンプトが表示されてからダウンロードの実行を許可します。
4. Avigilon から製品アップデートを受け取るように製品登録ページの手続きを完了します。
5. `.bin`ファイルを ACC Client ソフトウェアを実行しているコンピュータにコピーします。

ACC Client：

1. [ライセンス管理] ダイアログ ボックスで、[**適用…**] をクリックします。
2. `.bin` ファイルを選択し、[**開く**] をクリックします。
3. **OK** をクリックして、変更を確認します。

ライセンスの再アクティブ化

Enterprise エディション向け

サーバーをサイトに追加または削除すると、そのサイトのライセンスは非アクティブになり、システムの変更を確認するために再度アクティブ化する必要があります。

影響を受けたライセンスを再アクティブ化しないと、サイトは通常の操作を中止します。

1. 新しいタスクメニュー で、[**サイトのセットアップ**]をクリックします。
2. ウェブサイト名をクリックして、[ ] をクリックします。
3. [**ライセンスの再アクティブベート…**] をクリックします。

   インターネット アクセスがある場合、

   1. [**ライセンスの再アクティベート**] をクリックします。
   2. **OK** をクリックして、変更を確認します。

   インターネットへのアクセスがない場合、

1. [**手動**] タブを選択します。
2. [**ファイルの保存…**] をクリックして、`.key` ファイルを保存する場所を選択します。
3. `.key` ファイルをインターネットを介してコンピュータにコピーします。
    1. activate.avigilon.com にアクセスします。
    2. [**ファイルの選択**] をクリックし、`.key` ファイルを選択します。
    3. [**アップロード**] をクリックします。`capabilityResponse.bin` ファイルは自動的にダウンロードされるはずです。

       ダウンロードされない場合、プロンプトが表示されてからダウンロードの実行を許可します。
    4. Avigilonから製品アップデートを受け取るように製品登録ページの手続きを完了します。
    5. `.bin`ファイルをACCClientソフトウェアを実行しているコンピュータにコピーします。
4. [ライセンス管理] ダイアログ ボックスで、[**適用…**] をクリックします。
5. `.bin` ファイルを選択し、[**開く**] をクリックします。
6. **OK** をクリックして、変更を確認します。

ACC クライアントソフトウェアのスタートアップとシャットダウン

ACC Client ソフトウェアを開く手順：

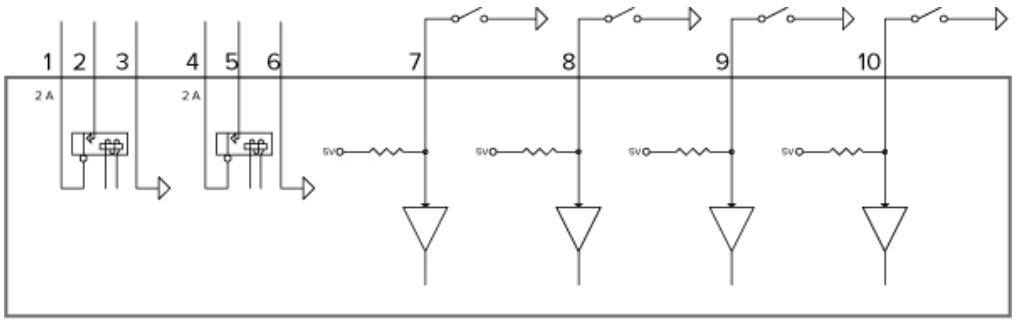
- デスクトップ ショートカット アイコン  をダブルクリックします。
- スタート メニューから、**[すべてのプログラム]** または **[すべてのアプリケーション]を選択し、Avigilon > Avigilon コントロールセンター Client**の順にクリックします。
- Avigilon コントロールセンター 管理者ツールで、[**Control Center Client の立上げ**] をクリックします。詳細については、『*Avigilon* コントロールセンター *Server* ユーザー ガイド』を参照してください。

ACC Client ソフトウェアを閉じる手順：

1. 右上隅で、 ✕ をクリックします。
2. [**はい**] をクリックします。

外部電源の接続

外部デバイスは、I/O端末経由でアプライアンスに接続されます。I/O端子のピン配列を次の図に示します。



1. 出力 2（リレー出力）— Form-A ドライ接点出力。アクティブなときは、端子が接続されています。非アクティブな場合、端子はオープン状態です。

   最大負荷は 30 V、2 A または 200 V、250 mA です。
2. 出力 2
3. アース（GND）
4. 出力 1（リレー出力）— Form-A ドライ接点出力。アクティブなときは、端子が接続されています。非アクティブな場合、端子はオープン状態です。

   最大負荷は 30 V、2 A または 200 V、250 mA です。
5. 出力 1
6. GND（アース）
7. 入力 4（アラーム入力） — アクティブ ロー入力。アクティブ化するには、入力をアースピン（GND）に接続します。非アクティブ化するには、切断された状態のままにするか、3～15 V を印加します。
8. 入力 3
9. 入力 2
10. 入力 1

PoE 電源への電力配分

4ポート式デバイス上のPoE スイッチ コンポーネントでは、合計 64W の電力を接続されているデバイスに出力することができ、8ポート式デバイス上のものでは、合計128Wの電力を出力できます。いずれのPoEポートも16 Wを標準PoEデバイスに、また30 WをPoE+デバイスに出力することができます。これは通常、4ポート式デバイスが標準 PoE デバイスを4つまで、または PoE+ デバイスを2つまでサポートでき、8ポート式デバイスが標準 PoE デバイスを8つまたはPoE+ デバイスを4つまでサポートできることを意味します。

上級ユーザーは、ポートごとに PoE の電力配分を手動で調整して、必要とされるカメラに常時対応できるようにすることができます。

各ポートの PoE 配分を手動調整する場合は、ケーブルにおける電力損失の可能性も計算に入れる必要があることにご注意ください。ケーブルにおける電力損失の量がわかっている場合を除き、次の推定値を使用してください。

- デバイスの使用電力が16 W 以下の場合 — 2.5 W の電力損失を想定します。
- デバイスの使用電力が 16 W 超の場合 — 4.5 W の電力損失を想定します。

ポートごとの推奨電力配分を計算するには、次の方程式を使用してください。

電力配分 = <カメラの消費電力> + <想定されるケーブルの電力損失>

例：次の 4 台のカメラを4ポート式デバイスに接続する場合：

HD ドーム型カメラ 2 台	$\frac{(9\ W + 2.5\ W) \times 2}{2}$	= 23 W
HD PTZ カメラ 1 台	25.5 W + 4.5 W	= 30 W
HD マイクロドーム 1 台	4 W + 2.5 W	= 6.5 W
	合計	= 59.5 W

4 台のカメラの合計消費電力は、PoE スイッチコンポーネントの制限値の範囲内です。

メモ：PoE ポートに必要な電力の計算を誤った場合、合計出力が 64 W を超えると接続されているカメラがシャットダウンすることがあります。

LED インジケーター

以下の一覧に、ACC ES Analytics Appliance の LED の意味を説明します。

フロントパネルのLED

アイコン	LEDの状態	説明
	緑色	デバイスの電源が入り、稼働中です。
	オレンジ色	デバイスを再起動中です。
	オレンジ - 点滅	工場出荷時設定への復元ボタンが押されました。
	緑色	ハードディスクドライブが接続されています。
	赤	ハードディスクドライブの接続にエラーがあります。
	緑色	カメラはネットワーク接続とパワーオーバーイーサネット（PoE）の電源のスイッチを使用しています。
	オレンジ色	カメラはネットワーク接続のみのスイッチを使用しています。
	オレンジ - ゆっくり点滅 • 一方のポート • 全ポート	システムオーバーパワーバジェット警告詳細については、Webインターフェイスの[PoE]パネルを確認してください。 システムの使用電力がPoE電力バジェットを超えているためポートがオフになっています。 システムがPoE電力バジェットを超えています。 詳細については、「PoE 電源予算の割り当て」（18ページ）および「PoEポートのステータスの表示」（10ページ）を参照してください。
	緑色 -オレンジ色が交互に点灯	エラーのためにポートがオフになっています。

アイコン	LEDの状態	説明
	オレンジ色	GigE ネットワークリンクが存在します。
	緑色	10/100 ネットワークリンクが存在します。
	オレンジ色	スイッチコンポーネントが、PoE 出力機能の上限に達しました。

バックパネルのLED

アイコン	LEDの状態	説明
	緑色	ネットワークアクティビティが存在します。
	オレンジ色	GigE 速度でオンになっています。10/100 速度でオフ。
	緑色	ネットワークアクティビティが存在します。
	オレンジ色	100M 速度でオン。10M 速度でオフ。

証明書を管理する

信頼できる証明書は、デバイスが接続に必要な他のサーバーとクライアントを認証し、それらの接続を保護するためにデバイスによって使用されます。Avigilon自己署名済みのWeb 証明書を提供して、サーバー管理とWebEndpointサービス、および信頼された認証局 (CA) からの一連のシステムレベルの署名済み証明書への接続をセキュリティ保護し、必要なあらゆるサーバーへの安全な接続を保証します。オプションで、独自の証明書とCAを提供できます。

デバイスに含まれる証明書によって提供されるセキュリティのレベルは、内部サーバーに公開キー基盤 (PKI) を展開しない組織にとって十分なものである必要があります。

アプライアンスの証明書管理機能は、サーバー管理と ACC WebEndpoint 製品で使用されるアプライアンスの Web 証明書のみを制御します。ACCサーバー内では、この機能によって構成された認証局は、ACC電子メールおよび中央集中監視機能によって使用される安全な電子メールサーバーを検証するためにのみ使用されます。ACCサーバーからACCサーバーへ、およびACCサーバーからACC Clientへの接続の制御または検証には、アプライアンスの証明書管理機能を使用しません。

たとえば、組織がGoogle Mailなどのパブリックメールサーバーを使用している場合、メール通知がトリガーされると、ACCソフトウェアはGoogleメールサーバーにアクセスし、Googleメールサーバーを識別する証明書を受け取ります。ACCソフトウェアは、Google Mail証明書に署名したCAが既知の信頼できるCAによるシステムレベルリストからのものであり、接続が保護されていることを確認して、証明書を検証します。

> **メモ：**デバイスに同梱された署名済み証明書は、Mozillaのブラウザに同梱されたものと同じであり、**The Debian Project**から公的に入手可能です。証明書により、SSLベースのアプリケーションがSSL接続の信頼性をチェックできます。Avigilonは、証明書がこのアプライアンスに含まれている証明機関が信頼性やRFC3647準拠のための監査を受けているかどうかを確認することも否定することもできません。それらを評価する完全な責任は、ローカルシステム管理者にあります。

自社のPKIを展開する組織は、サーバー管理の[証明書]ペインを使用して、デバイス上の証明書を管理できます。

たとえば、次のことができます：

- デフォルトの自己署名済みWeb 証明書を自分の組織の証明書に置き換えます。
- 組織内で使用されている内部CAなどのCAをデバイスに追加します。
- システムレベルのCA証明書を無効（および有効）にします。

Web 証明書を交換します

デバイスのWeb 証明書を [証明書] ペインの [Web 証明書] タブで管理します。サーバー管理とWebEndpointサービスは、この証明書を使用して、接続しているデバイスに対して自身を認証します。いつでもアクティブにできるWeb 証明書は1つだけです。

デフォルトのWeb 証明書をカスタム証明書に置き換えることができます。

重要：デバイスを出荷時の設定にリセットする（出荷時リセットとも呼ばれる）場合、カスタム証明書をリロードする必要があります。

新しいWeb 証明書の取得は、3 ステップのプロセスです：

1. 組織で使用されている証明書発行者に証明書署名要求 (CSR) を送信すると、発行者から新しい証明書ファイルと秘密キーファイルが返されます（通常は電子メール）。彼らがサーバー管理からCSRを受け入れない場合、[Web 証明書] タブ、または証明書発行者の好適な方法を使用してからCSRを生成できます：
    a. サーバー管理を開いて、ナビゲーションバーでデバイスをクリックし、証明書ペインまでスクロールします。
    b. [Web 証明書] タブで、証明書署名要求ボタンをクリックしてください。
    c. 標準CSRフォームに、使用しているPKIによって定義された情報を入力し、生成をクリックします。

       CSRファイルgenerated.csrは、ダウンロードフォルダに保存されます。
    d. ファイルを組織の証明書発行者に送信します。

       ヒント：証明書発行者がCSRを受け入れない場合は、証明書発行者が推奨する方法を使用してCSRを生成します。
2. 証明書発行者からの新しい証明書を含む.crtファイルを受け取ったら、デバイスにアクセスできる場所に保存します。

3. 新しい証明書をデバイスにアップロードします：
    a. サーバー管理を開いて、ナビゲーションバーでデバイスをクリックし、証明書ペインまでスクロールします。
    b. [Web 証明書] タブで、アップロードをクリックします。
    c. Web 証明書のアップロードダイアログで、証明書の名前を入力して、.crtファイルに移動するか、またはここに '.crt' 証明書 (pem) ファイルをドロップするか、クリックしてアップロードします領域にドラッグ＆ドロップします。
        - 証明書ファイルがサーバー管理から生成された最新のCSRファイルで作成された場合、アップロードがアクティブ化されます。
        - それ以外の場合は、クリックして.keyファイルに移動するか、またはここに '.key' 秘密鍵 (pem) ファイルをドロップするか、クリックしてアップロードします。領域にドラッグアンドドロップします。アップロードがアクティブ化されます。

        > **メモ：**証明書ファイル (.crt) が、証明書発行者の推奨する方法で生成されたCSRで作成された（またはデバイス上の最新のCSRファイルを使用して生成されなかった）場合は、この手順を繰り返して秘密鍵ファイルをアップロードします。

    d. [アップロード] をクリックします。
4. [Web 証明書] タブで、アップロードした証明書の名前をクリックして有効にします。これにより、以前の証明書も無効になります。

信頼できるCA証明書をアップロードする

証明書のユーザー認証局タブから、組織の内部のサーバーに配備内部のCAから署名された証明書を管理します。

たとえば、独自のPKIを展開する組織の内部電子メールサーバーは、メールサーバーにアクセスしようとすると、既知の信頼できるCAのセットに含まれていないCAによって署名された証明書をACCソフトウェアに提供する場合があります。そのCAによって署名された証明書が [証明書] ペインの [ユーザー認証局] タブにアップロードされない限り、証明書を検証できません。

CAから署名済み証明書をアップロードする必要がある場合は、以下の手順を実行します：

1. サーバー管理を開いて、ナビゲーションバーでデバイスをクリックし、証明書ペインまでスクロールします。
2. [ユーザー認証局] タブをクリックします。
3. [アップロード] をクリックします。

4. ユーザー認証局のアップロードダイアログで、証明書の名前を入力し、クリックまたはドラッグアンドドロップしてファイルをアップロードします。一度にアップロードできるファイルは1つだけです。

ファームウェアをアップグレードする

ファームウェアをアップグレードして、ACC ES Analytics Applianceが最新のソフトウェアで動作するようにします。ファームウェアをアップグレードする際に、すべての現在の設定とすべての記録映像が保持されます。

ファームウェアは、次のいずれかの方法でアップグレードします。

- Avigilonクラウドサービスからのクラウドリモートサイトアップグレードを使用して、次を更新できます：
  - ACC ES Analytics Applianceのファームウェア、
  - 他のすべてのAvigilonサーバー上のファームウェア、
  - すべてのAvigilonカメラ、および
    上のファームウェア
  - ACCすべてのネットワークワークステーション上のClientソフトウェア

  。それも、同じサイトで同時にです。

  Advanced System Health機能パッケージのサブスクリプションが必要です。これは、サイトレベルのアップグレードを迅速かつ効率的に完了するため、Avigilon推奨の方法です。Avigilon クラウド サービス
  に付属のヘルプファイルにあるサイトのサーバーをアップグレードする手順を参照してください。
- 同じサイトで同時にすべてのACC ES Analytics Applianceに接続されたACC Clientからのリモートサイトアップグレードを使用できます。ACCクライアントに付属のヘルプファイルにあるサイトのサーバーをアップグレードする手順を参照してください。
- サーバー管理ページは、次の手順を使用して使用できます。

サーバー管理ページを使ってファームウェアをアップグレードまたは再インストールする前に、ファームウェア（`.fp`）ファイルの最新バージョンをAvigilon **サポートコミュニティ**からダウンロードします。

インターネットに接続されたワークステーションから：

1. **support.avigilon.com**に移動して、適切なACC ES Analytics Applianceファームウェアを検索します。

   > **メモ：**ファームウェアをダウンロードするには、アカウントを持っているか、アカウントを作成し、コミュニティにログインしなければなりません。

2. ファイルをサーバー管理ページにアクセスできる場所に保存します。

サーバー管理ページからファームウェアをアップグレードするには：

1. デバイスパネルに移動します。

   必要に応じ、スクロールして ファームウェアのアップグレードペインを表示します。

2. ファームウェアのアップグレードペインで、**'.fp' ファイルをここにドロップするか、クリックしてアップロードします**をクリックして、ファームウェアパッケージ（.fp）ファイルが保存された場所に移動します。

3. **OK** をクリックして続行を確認します。アップロードの進行状況インジケーターが表示されます。ファイルがアップロードされ、確認されるまで待ちます。

   重要：進行中のファームウェアのアップロードするは、アップロードおよび確認段階でのみキャンセルできます。ファイルがアップロードされる前に、**アップロードのキャンセル**をクリックしてください。

   ファイルが確認されると、ファームウェアのアップグレードが自動的に開始されます。デバイスは、アップグレード中に数回再起動します。デバイスが再起動している間にWeb UI の通信が失われましたメッセージが表示されます。この手順には数分かかります。デバイスが再起動すると、サーバー管理ページへの接続がWebブラウザに復元されます。

   メモ：アップロード段階またはアップグレードプロセス中にエラーが生じた場合や、ファームウェアが破損した場合は、ファイルを削除するように促されます。

リセット ボタンの使用

リセットボタンはアプライアンスの正面にあります。システムステータスLEDの左側にある、ラベルのない小さい○がこのボタンです。詳細については、「「前面からの図」（2ページ）」を参照してください。

リセットボタンには2 つの機能があります。

- システムの再起動 ― アプライアンスでシステムエラーが発生した場合、強制的に再起動させることができます。
- 工場出荷時の設定への復元 ―ACC ソフトウェアが期待したとおりに機能しなくなった場合に、アプライアンスを工場出荷時の設定にリセットすることができます。構成設定と収録されているデータはすべて削除されます。

メモ：リセットボタンを使用する場合、アプライアンスに電源が投入されている必要があります。

システムの再起動

アプライアンスでシステム エラーが生じてWebインターフェイスにアクセスできなくなった場合、物理的なアプライアンスからシステムを再起動して問題の解決を試みることができます。

- 引き伸ばしたペーパークリップなどを使って、リセット ボタンをそっと押し、離します。

注意 ― 過度な力を適用しないこと。工具を奥に押し込めすぎると、レコーダーが損傷し、保証が無効になることがあります。

重要：リセット ボタンを長押ししすぎないでください。長押ししすぎると工場出荷時の設定に復元されてしまいます。

工場出荷時の設定への復元

ACC サーバー ソフトウェアが期待したとおりに機能しなくなったり、管理者パスワードを思い出せなくなったりした場合に、アプライアンスを工場出荷時の設定にリセットすることができます。

メモ：工場出荷時の設定に復元すると、インストールしたカスタム証明書の含め、すべての構成設定と記録映像が削除されます。工場出荷時のデフォルト設定が復元された後、機能上の問題が発生する前からの、最新のシステムバックアップを復元できます。カスタム証明書をリロードして、ACCサーバーソフトウェアを最新のリリースの更新が必要となる場合もあります。

1. 引き伸ばしたペーパークリップなどを使って、リセットボタンを軽く押し続けます。

   注意 ー 過度な力を適用しないこと。工具を奥に押し込めすぎると、レコーダーが損傷し、保証が無効になることがあります。

2. LED がオレンジで点滅するようになるまで、ボタンを押すのをやめないでください。

詳細情報

その他の製品ドキュメント、ソフトウェアとファームウェアのアップグレードについては、
support.avigilon.com をご覧ください。

テクニカルサポート

Avigilonテクニカル サポートには、**support.avigilon.com/contactsupport** から連絡してください。

限定的保証

この製品のAvigilon 保証条件は、**avigilon.com/warranty** に規定されています。