

ユーザーガイド

Avigilon ACC™ ES Rugged 8ポートアプライアンス

VMA-RPA-RGD-8P2およびVMA-RPA-RGD-8P4

© 2021、Avigilon Corporation。All rights reserved. AVIGILON、AVIGILON ロゴ、AVIGILON コントロールセンター、ACC、およびAVIGILON APPEARANCE SEARCHは Avigilon Corporation の商標です。MAC、MacOS、FINDERおよびMACINTOSHはApple Inc.の登録商標です。FIREFOXはMozilla Foundationの登録商標です。Androidは、Google LLC の商標です。本書に記載されたその他の名称またはロゴは、該当する所有者の商標である可能性があります。本書で、商標の横に ™ および ® の記号がない場合でも、該当する商標の所有権を放棄してはおりませんので、予めご了承ください。Avigilon Corporation は、アメリカ合衆国およびその他の世界中にある管轄区域で発行された特許をもって、新技術を保護します (avigilon.com/patentsを参照)。書面で明示的に付与されない限り、Avigilon Corporation またはそのライセンサーの著作権、工業デザイン、商標、特許またはその他の知的財産権の使用は許可されません。

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

目次

はじめに	5
パッケージの内容	6
必要な工具	7
概要	8
前面からの図	8
背面からの図	9
システム要件	10
カメラのフレームレート	10
Web ブラウザ	10
サポート対象のネットワーク構成	11
ACC ES Rugged 8ポートアプライアンスの取り付け	12
ACC ES Rugged 8ポートアプライアンスを電源に接続する	15
初回のACC ES Rugged 8ポートアプライアンスの起動	16
サーバー管理 の使用	18
サーバー管理の開始と停止	18
PoEポートのステータスの表示	19
ACCサービスを管理する	21
ACC Client ウィがビデオをアーカイブできるようにする	21
サポートにサーバー ログとシステム ログを提供します	22
デバイス設定の管理	23
ACC ES Rugged 8ポートアプライアンス管理者パスワードを変更する	24
時間設定の管理	24
ストレージSSDの監視と切断	25
デバイスをカメラとACC Clientユーザーに接続する	26
PoE 電源予算の割り当て	27
サポートのためのデバイスログの提供	28
ACC Clientのインストール	29
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	30
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	30

Avigilonクラウド サービスへ接続する	30
ライセンスのアクティブ化	31
インターネット経由のアクティブ化	31
オフライン アクティベーション	31
ライセンスの非アクティブ化	32
ライセンスの再アクティブ化	34
外部電源の接続	35
LED インジケータ	37
PoE 電源への電力配分	40
証明書を管理する	41
Web 証明書を交換します	42
信頼できるCA証明書をアップロードする	43
ファームウェアをアップグレードする	45
ソフトウェアリセットボタンの使用	47
工場出荷時の設定への復元	49
ストレージSSDの交換	51
トラブルシューティング	55
Webブラウザからサーバー管理ページにアクセスする	55
デバイスを検出できません	55
ネットワーク構成	56
システムヘルスの監視	56
詳細情報	57

はじめに

Avigilon ACC ES Rugged 8ポートアプライアンスは、サーバー側のビデオ分析を組み込んだネットワークビデオ録画のためのオールインワンソリューションで、過酷な環境や遠隔地での設置と使用のために頑丈に構築されています。アプライアンスには次の機能があります。

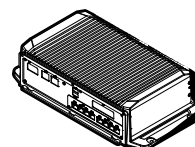
- IP カメラを接続し、電力を供給する PoE スイッチ。
- Avigilon コントロールセンター サーバー ソフトウェアを実行するための内蔵サーバー。
- 接続された非分析カメラで分類された対象物検出を可能にするビデオ分析エンジン。

このガイドでは、さまざまな場所にアプライアンスを設置する方法、固有の電力要件、およびアプライアンスの電源を入れた後にシステムを構成する方法について説明します。

パッケージの内容

ACCESRugged8ポートアプライアンスパッケージに次のものが同梱されていることを確認してください：

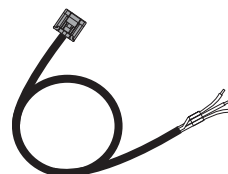
ACC ES Rugged 8ポートアプライアンス



フロントパネルキー



電源ケーブル（ユーザー指定の9-32VDC 100W（最小）電源に接続するため）



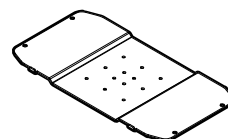
デジタル入出力ケーブル



DINブラケット



DINブラケットの取り付けプレート



DINレール#1のラベルが付いたビニール袋の取り付けプレートにDINブラケットを取り付けるための4本の皿頭ネジ



DINレール#2というラベルが付いたビニール袋のプレートにACC ES Rugged 8ポートアプライアンスを取り付けるための4本の円形ヘッドネジ



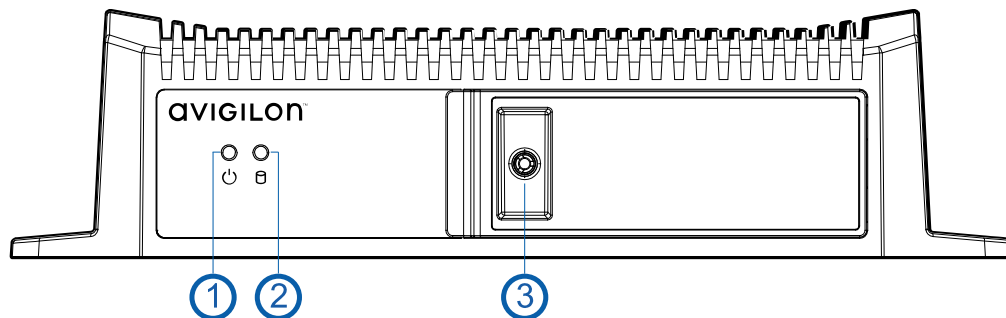
重要：UL 62368-1に準拠するには、ACC ES Rugged 8ポートアプライアンスが外部電源アダプターから給電され、Tmaが70Cのときの使用に適したUL規格の電源アダプターである必要があります。これは、出力がES1（またはSELV）を満たし、定格は9-32Vdc、最小100Wです。詳細についてはAvigilonに連絡してください。

必要な工具

ACC ES Rugged 8ポートアプライアンスとDINブラケットを取り付けプレートに取り付けるのに必要なのは、プラス#2ドライバーだけです。

概要

前面からの図



1. 電源LEDインジケータ
2. ディスクアクティビティLEDインジケータ

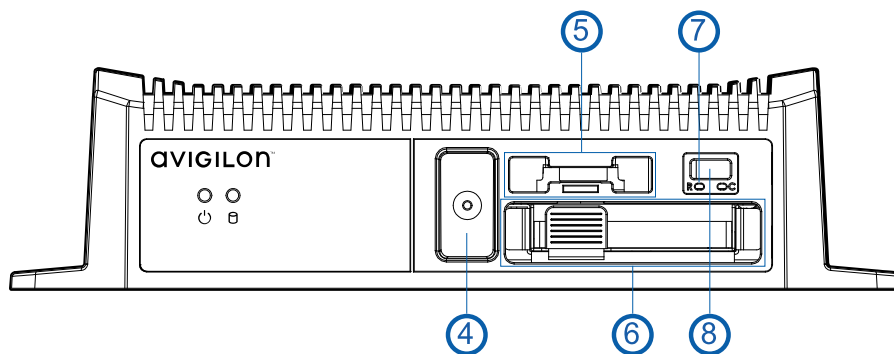
参照してください「LED インジケータ」 (37ページ)

3. ロック (ロック位置)

上記のように、フロントパネルは通常、内部コンポーネントへのアクセスを保護および防止するためにロックされています。

4. ロック (ロック解除位置)

以下のように、キーを使用してフロントパネルのロックを解除し、フロントパネルを開いて内部コンポーネントにアクセスします。



5. CMOSバッテリーホルダー

ホルダーのバッテリーからの電力により、アプライアンスの内部の日時設定、およびBIOS設定がCMOSメモリに保持されます。アプライアンスの時刻と日付の設定が信頼できなくなった場合、バッテリーの交換が必要ですが、これが許可されているのは訓練を受けた技術者のみです。



バッテリー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。使用済みバッテリーは、メーカーの指示に従って廃棄してください

6. SSDトレイ

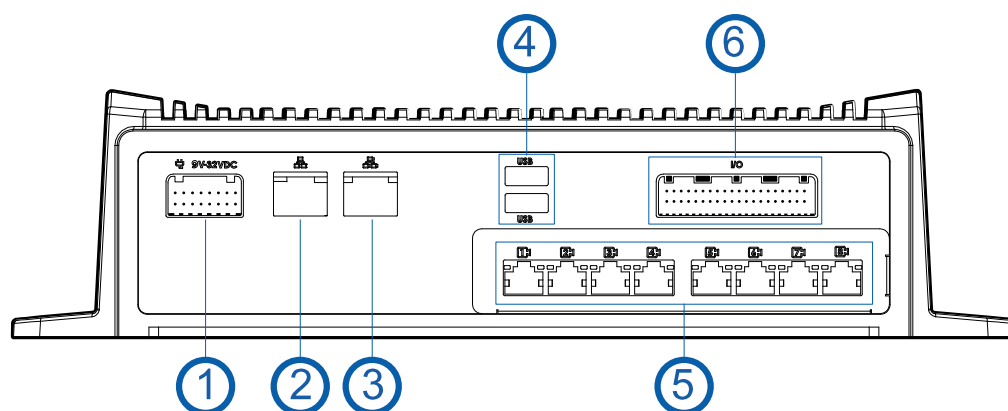
トレイをスライドさせて出し入れし、ストレージSSDにアクセスします。「ストレージSSDの交換」（51ページ）を参照してください。

7. 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ます。

8. USB 3.0 ポート

背面からの図



1. 電源コネクタ

2. 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 インターフェ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。

3. カメラ ネットワーク アップリンクポート

1GbEイーサネット接続を受け入れ、他のPoEスイッチおよびカメラにリンクします。

4. USB 2.0 ポート

5. 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。スイッチは合計60ワットの電力を提供でき、すべてのPoEポートで共有されます。

6. I/O コネクタ

外部入出力装置に接続します。2つのケーブル端には、デジタル入力とデジタル出力のラベルが付いています。詳細については、「「外部電源の接続」（35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

ACCESRugged8ポートアプライアンス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。

ACCES Rugged 8ポートアプライアンスの取り付け

ACCES Rugged 8ポートアプライアンスは、どの方向でも重量を支えることができるほぼすべての平面に、または4つの方向のいずれかでDINレールに取り付けることができます。付属の取り付けプレートとDINレールブラケットとネジを使用してDINレールに取り付ける場合以外、アプライアンスを取り付ける面に適したネジとアンカー、またはナットとボルトを用意する必要があります。

ヒント：アプライアンスの電源を完全にオンにしてカメラを接続し、録画を開始する前に、アプライアンスを任意の表面またはDINレールに取り付けます。アプライアンスを取り付ける前に設定する場合、設定が完了してアプライアンスを取り付ける前に、アプライアンスの電源を切り、すべてのケーブルを取り外すことをお勧めします。

アプライアンスを平面に取り付けるには：

アプライアンスの基部には、各コーナーに取り付け穴がついており、アプライアンスをあらゆる角度または方向でどの平面にも取り付けすることができます：

1. 電源およびケーブルコネクタに最もアクセスしやすいように、背面パネルを方向に向けてアプライアンスを配置します。
2. 表面のネジ穴の位置に印を付けます。
3. アンカー用の穴を開け、アンカーを壁に挿入します。木ネジ、コンクリートネジ、石工ネジを使用する場合は、必要に応じて穴を開けます。
4. 指定した留め具を使用して、アプライアンスを表面に取り付けます。

DINレールブラケットと取り付けプレートをアプライアンスに取り付けるには：

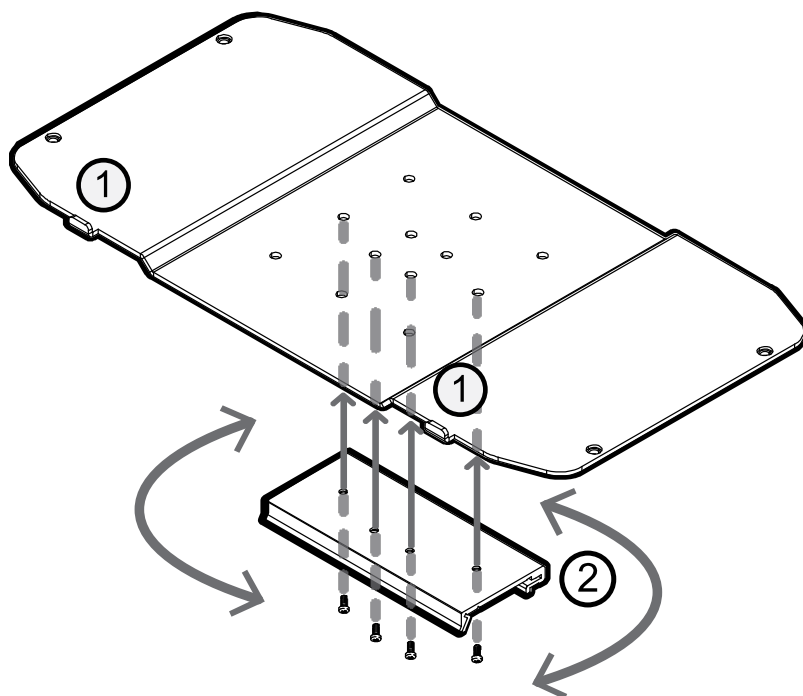
取り付けプレート、ブラケット、およびブラケットをプレートに取り付けるためのネジが付属しています。DINレールブラケットは、湾曲した部分を上にしてDINレールに固定されます。ACCES Rugged 8ポートアプライアンスの背面には、取り付けプレートの対応するスロットに適合する金属タブがあります。

ブラケットは、4つの位置のいずれかで取り付けプレートに取り付けることができます。これにより、さまざまな位置でアプライアンスをレールに取り付ける選択肢が生まれ、前面パネルと背面パネルに最適にアクセスできるようになります：

- 前面または背面を上または下に向ける
- 前面または背面が右または左向き

ヒント : ACC ES Rugged 8ポートアプライアンスをDINレールに取り付ける場合、取り付けプレートに対するブラケットの正しい方向を決定し、取り付けプレートをアプライアンスに取り付ける前に、取り付けプレートにブラケットを取り付けます。これにより、アプライアンスを最適な位置に設置できます。

1. 取り付けプレートで、DINレールブラケットを取り付ける位置を決定します。
2. DINレールブラケットを、取り付けプレート上の事前にドリルで開けられたネジ穴に正しい方向で合わせ、**DINレール#1**というラベルが付いたビニール袋に入った4本の皿頭ネジを使用して取り付けます。アプライアンスの背面にあるタブは、ブラケットの片側のスロットにのみはまります。

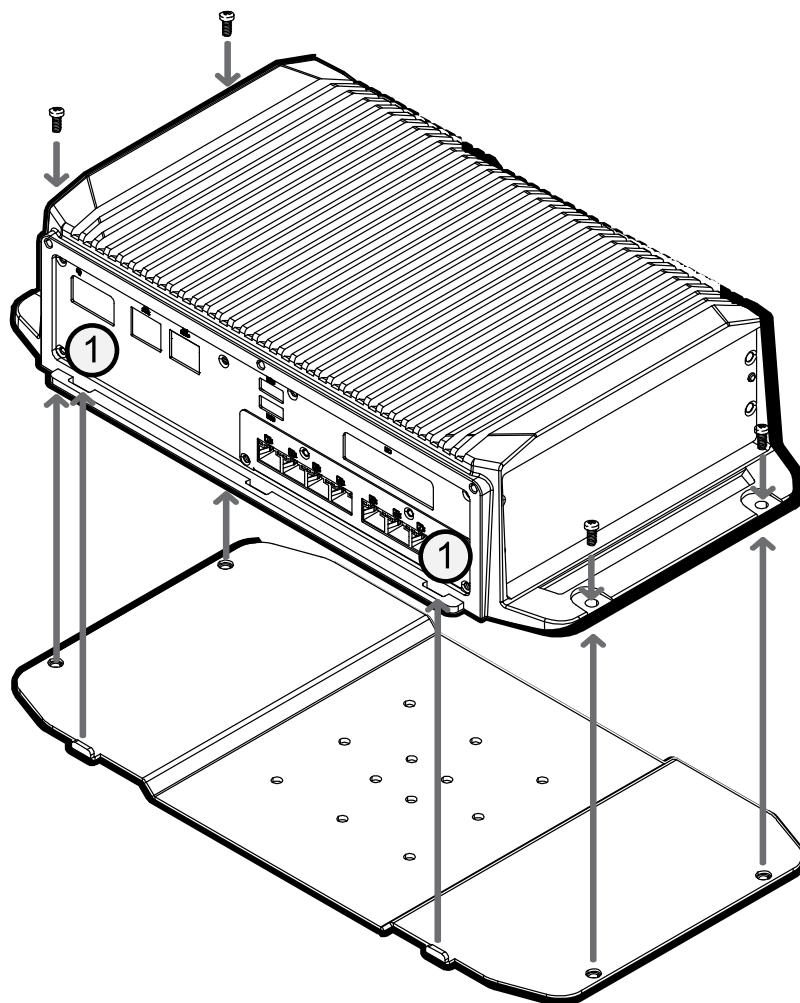


①アプライアンスの後部のスロットに収まる取付プレートのタブを示します。

KDIN取付ブラケットの上縁を示します。

例の方向では、アプライアンスの前面が上を向くようにアプライアンスを取り付けブラケットに配置しています。

3. 以下に示すように、**DIN rail#2** というラベルの付いたビニール袋に入った4本の丸頭ネジを使用し、DINレールブラケットの前後を正しい向きにして、アプライアンスを取り付けプレートに取り付けます。



① アプライアンスの背面のロットが取り付けプレートのどのタブに適合するかを示します。

4. フロントパネルのLEDインジケータが見え、背面パネルの接続にアクセスできるように、取り付けプレートのDINレールブラケットを正しく揃えてアプライアンスをDINレールにクリップします。

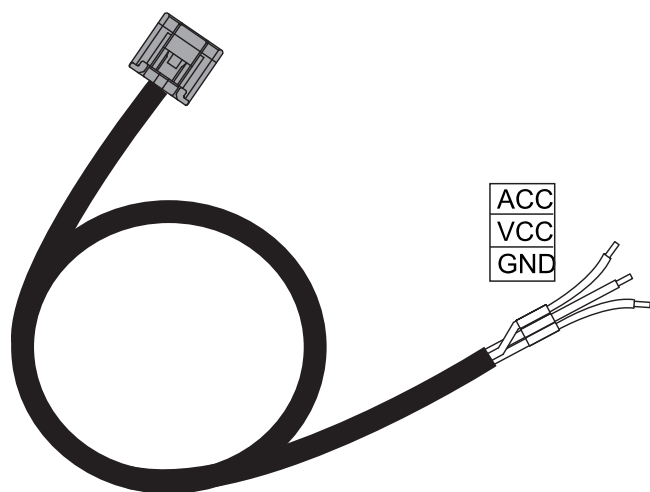


注意 — デバイスは指示に従って取り付けてください。指示に従わない場合、問題が生じても保証の対象になりません。

ACC ES Rugged 8ポートアプライアンスを電源に接続する

ACC ES Rugged 8ポートアプライアンスは、付属の電源ケーブルを使用して、適切な9~32ボルトのDC 100W（最小）電源から給電できます。

付属の電源ケーブルには、アプライアンスの背面にある電源コネクタに差し込む一端のコネクタと、ACC（アクセサリ）、VCC、およびGNDのラベルが付いた末尾の3本のワイヤがあります。



常時電源接続（非スイッチド）を行うには、ACCとVCCの両方のワイヤを電源のプラス側に接続します。アース線を電源のアース側に接続します。

スイッチされた電源信号（車両の車両アクセサリ信号など）に接続するには、ACCワイヤを使用します。ACCワイヤが電源のプラス側に接続されると、システムがオンになります。ACCワイヤが電源のプラス側から切断されると、システムは低電力スタンバイモードになります。

初回のACC ES Rugged 8ポートアプライアンスの起動

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. 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。
3. 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—最初の画面で**Advanced (高度)** をクリックして、2番目の画面で **Proceed to <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—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。
4. 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。
5. 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ドパネルが表示されます。
6. 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」(23ページ)を参照してください。

7. 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」（26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」（18ページ）を参照してください。

サーバー管理 の使用



ACC ES Rugged 8ポートアプライアンスは、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-RGD-8Px-<シリアル番号>」 という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」 (55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ACCK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 一定 PoE デバイスがポートに接続され、正常に動作しています。
色 出力

高出 PoE +がオンになっています。

力

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 Rugged 8ポートアプライアンスをリセットします	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 Rugged 8ポートアプライアンスからビデオをアーカイブできるようにします。「ACC Client ウィがビデオをアーカイブできるようにする」（21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 Rugged 8ポートアプライアンス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 ウィ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 Rugged 8ポートアプライアンス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 」(24ページ)を参照してください。
ACC ES Rugged 8ポートアプライアンス管理者のパスワードを変更します。	パスワード	「ACC ES Rugged 8ポートアプライアンス管理者パスワードを変更する」(24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」(45ページ)を参照してください。
ACC ES Rugged 8ポートアプライアンス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」(41ページ)を参照してください。

ACCES Rugged 8ポートアプライアンス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 — 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。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」（49ページ）を参照してください。

時間設定の管理

ACC ES Rugged 8ポートアプライアンス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 Rugged 8ポートアプライアンスのポート123に接続して、NTPサーバーとして使用できます。

選択：

- **DHCP**—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**—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SSDの監視と切断

ストレージのパネルでは、ACC ES Rugged 8ポートアプライアンス次のことができます：

- ストレージ容量と交換可能なストレージソリッドステートドライブ(SSD)のステータスを表示します。
- 障害が発生した場合、ストレージSSDのステータスを [オフライン] に設定してからアプライアンスから取り外して交換します。

重要 : ストレージSSDは、同じ容量のSSD (VMA-RPA-8P2モデルの場合は2TB、VMA-RPA-8P4モデルの場合は4TB) と交換する必要があります。

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
SSD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。 SSDが次の場合： <ul style="list-style-type: none">• 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。
SSDを取り出します。	[] をクリックします。 取り出し または キャンセル プロンプトが表示されます。ステータスが オフライン に変わり、  が  に変わり、すべてのサービスが停止したことが示されます。これでSSDを交換できます。詳細については、「ストレージSSDの交換」(51ページ)を参照してください。

ストレージのパネルでは、AI NVR次のことができます：

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」（11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	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。 <ul style="list-style-type: none">• 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	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

タスク

操作


法を設定します。 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」（40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。

- **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。

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。

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をクリックします。

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 Rugged 8ポートアプライアンスを展開したら、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」（34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/](https://www.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。

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」（31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が、ダウンロードされない場合、プロンプトが表示された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。

ライセンスの非アクティブ化

メモ : ライセンスは限られた回数だけ非アクティブにすることができます。以前に非アクティブ化したライセンスをアクティブ化しているときにエラーが発生した場合は、これが原因である可能性があります。解決策について Avigilon テクニカル サポートまでお問い合わせください。

個々のライセンスを非アクティブ化し、別のサイトでアクティブにすることができます。たとえばサーバーハードウェアをアップグレードしている場合、古いサーバーのライセンスを非アクティブ化して、同じライセンスを新しいサーバーでアクティブ化することができます。

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. 非アクティブ化したいライセンスを選択します。
4. [ライセンスの削除...]をクリックします。
5. ライセンスを記録するには、[クリップボードにコピー]をクリックしてテキストファイルに貼り付けます。

インターネット アクセスがある場合、

- [今すぐアクティベート停止]をクリックします。

インターネットへのアクセスがない場合、

メモ : licensing.avigilon.com アカウントが必要です。アクセスについては、組織の技術担当者にお問い合わせください。

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。
ライセンスが非アクティブになります。
3. .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。
 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が、ダウンロードされない場合、プロンプトが表示された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。



これで、新しいサイトでライセンスを再度アクティブ化することができます。

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化...]をクリックします。

インターネット アクセスがある場合、

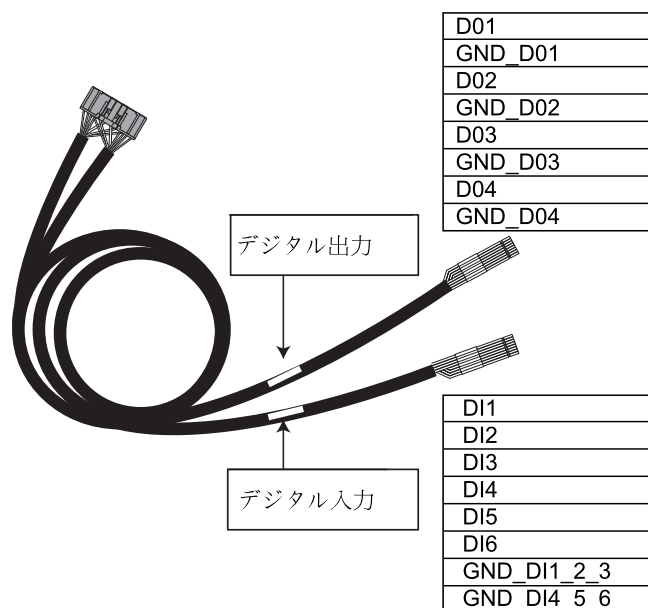
1. [ライセンスの再アクティブ化...]をクリックします。
2. **OK** をクリックして、変更を確認します。

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が、ダウンロードされない場合、プロンプトが表示された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。

外部電源の接続

外部デバイスは、アプライアンスの背面にあるデジタルI/Oコネクタに挿入されたデジタルI/Oケーブルを使用してACC ES Rugged 8ポートアプライアンスに接続されます。8つのラベル付き入力ワイヤーと8つのラベル付き出力ワイヤーの詳細を以下に示します。




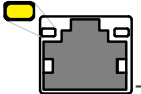


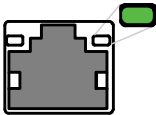

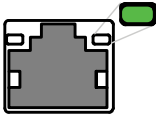
ピン	機能	説明
DI1	入力 1	アラーム入力 - アクティブロー入力。アクティブ化するには、入力をアースピン（GND）に接続します。非アクティブ化するには、切断された状態のままにします。
DI2	入力 2	
DI3	入力 3	
DI4	入力 4	
DI5	IN5	
DI6	IN6	
GND_DI1_2_3	入力1、2、3の接地ピン	
GND_DI4_5_6	入力4、5、6の接地ピン	

ピン	機能	説明
D01	出力 1	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。非アクティブなときは、端子が接続されていません。
GND_D01		
D02	出力 2	メモ：接点は通常開いています。
GND_D02		
D03	出力 3	最大負荷は 48 V、0.3 Aです。
GND_D03		
D04	出力 4	
GND_D04		

LED インジケータ

以下の一覧に、ACC ES Rugged 8ポートアプライアンスのLEDの意味を説明します。

	アイコン	LEDの状態	説明	
フロント LED		赤	デバイスの電源が入り、稼働中です	
		黄色	ストレージドライブの動作	
バック LED		左	オン： ポートはPoE電力を供給しています	
			黄色	オフ： ポートはPoE電力を供給していません
			点滅： ポートはPoE電力を供給していま	

アイコン	LEDの状態	説明
		せんが、PoE カメラが接続されています
	<p data-bbox="818 537 846 567">右</p>  <p data-bbox="818 743 870 772">緑色</p>	<p data-bbox="1338 537 1425 772">オン：ネットワークリンクが存在します</p> <p data-bbox="1338 806 1425 1087">オフ：ネットワークリンクが存在しません</p> <p data-bbox="1338 1121 1425 1440">点滅：ネットワークアクティビティが存在します</p>
<p data-bbox="331 1478 441 1675">企業 & カメラ アプリリンクポート</p> 	<p data-bbox="818 1478 846 1507">右</p>  <p data-bbox="818 1684 870 1713">緑色</p>	<p data-bbox="1338 1478 1425 1713">オン：ネットワークリンクが存在します</p> <p data-bbox="1338 1747 1425 1820">オフ：ネットワーク</p>

アイコン	LEDの状態	説明
		ワーク リンク が存在 しません 点滅： ネット ワーク アク ティビ ティが 存在し ます

PoE 電源への電力配分

Avigilon ACC ES Rugged 8ポートアプライアンス 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ます。PoE ポートはそれぞれ標準の PoE デバイスに 16 W、PoE+ デバイスに 30 W を出力することができます。これは通常、の式デバイスが標準 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。

$$\text{電力配分} = \text{<カメラの消費電力>} + \text{<想定されるケーブルの電力損失>}$$

例：次の4台のカメラをACC ES Rugged 8ポートアプライアンスに接続する場合：

$$\text{HD ドーム型カメラ 2 台} \quad (9 \text{ W} + 2.5 \text{ W}) \times 2 = 23 \text{ W}$$

$$\text{HD PTZ カメラ 1 台} \quad 25.5 \text{ W} + 4.5 \text{ W} = 30 \text{ W}$$

$$\text{HD マイクロドーム 1 台} \quad 4 \text{ W} + 2.5 \text{ W} = 6.5 \text{ W}$$

$$\text{合計} = 59.5 \text{ W}$$

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 PoE スイッチ全体がシャットダウンすることがあります。

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、[TheDebianProject](#)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 Rugged 8ポートアプライアンス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 Rugged 8ポートアプライアンスのファームウェア、
 - 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 Rugged 8ポートアプライアンスに接続された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 Rugged 8ポートアプライアンス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。

ソフトウェア リセットボタンの使用

ACC ES Rugged 8ポートアプライアンスでシステムエラーが発生し、それを電源から切断したり、アプライアンスの電源を入れ直したりできない場合は、アプライアンスの電源が入っている状態でリセットボタンを使用して再起動します。

メモ：リセット機能はカメラの接続もリセットするため、リセット中にすべての記録映像が失われます。リセット中、アプライアンスは録画しません。ただし、記録映像は失われません。

リセットボタンはACCESRugged8ポートアプライアンスの前面にあるロックされたパネルの背後にあります：

アプライアンスをリセットするには：

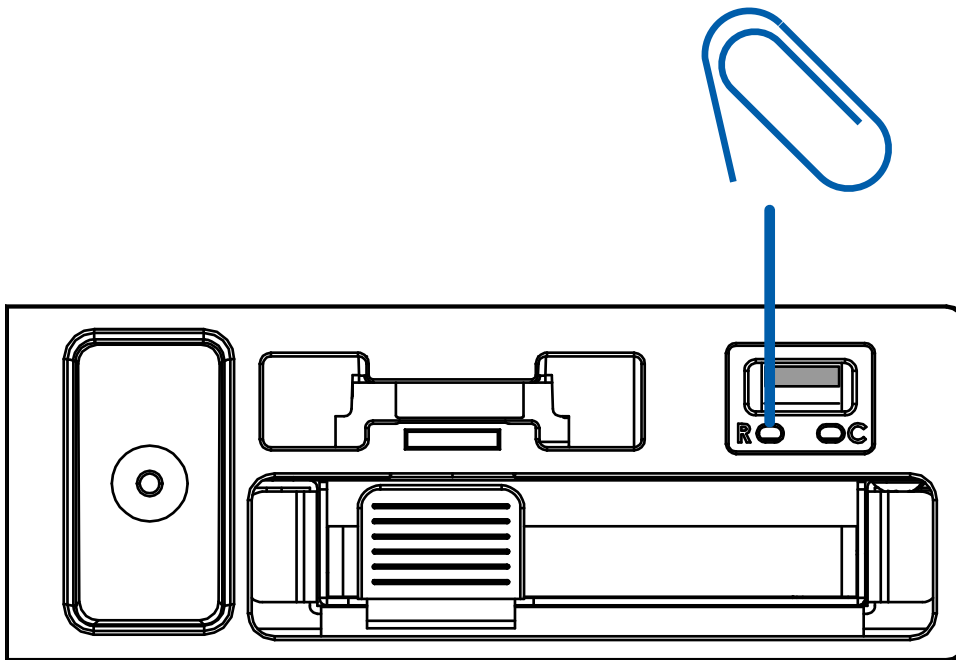
1. 提供されたキーを使用して、フロントパネルのロックを解除して開きます。

ヒント：キーを反時計回りに180度回して、フロントパネルのロックを解除します。フロントパネルが下がり、ストラップでアプライアンスに取り付けられます。


2. アプライアンスのリセットスイッチを見つけたら、まっすぐに伸ばしたペーパークリップなどの工具を使用して、リセットスイッチをゆっくりと押して離します。



過剰な力をかけないでください。工具を奥に押し込めすぎると、アプライアンスが損傷し、保証が無効になります。



3. アプライアンスが完全に再起動し、記録が再開したことを確認します：

- a. [サーバー管理ページ] サインイン ページにアクセスしてログインします。詳細については「サーバー管理の開始と停止」（18ページ）をご覧ください。
- b. Webインターフェースの起動ページのストレージパネルで、ステータスが  であることを確認します。

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、ACC ES Rugged 8ポートアプライアンス を工場出荷時の設定に復元することができます。復元プロセスを完了するには、USBメモリドライブが必要です。

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を含め、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。

アプライアンスがマージされたサイトまたは親子サイトファミリー構成の一部である場合は、ACC Client ソフトウェアで実行すべき追加のステップがあります。これは、この手順で指定されています。

1. USBメモリドライブを準備します。これは、次の条件を満たす必要があります：
 - a. FAT32フォーマットである。
 - b. `factory_restore`という名前で、拡張子のない任意のサイズのファイルを含みます。
2. USBメモリドライブをいずれかのUSBポートに挿入します。
3. アプライアンスがマージされたサイトまたは親子サイトファミリー構成の一部である場合：
 - a. リセットを行う前に、サイトから削除してください。
 - b. アプライアンスがマージされたサイトの一部でない場合は、ライセンスを非アクティブペー
トします。
4. ACC ES Rugged 8ポートアプライアンスの電源を入れ直します。次のことができます：
 - アプライアンスのプラグを抜き、再度差し込みます。
 - アプライアンスをリセットします（「ソフトウェアリセットボタンの使用」（47ページ）を参照）。
 - Webユーザーインターフェイスのデバイスパネルからアプライアンスを再起動します（「デバイス設定の管理」（23ページ）を参照）。
5. 電源が再びオンになり、`factory_restore`ファイルが検出されるとすぐに、現在の設定とデータが削除され、工場出荷時のファームウェアイメージが復元されてACC ES Rugged 8ポートアプライアンスが再起動されます。
6. ACC ES Rugged 8ポートアプライアンスが再起動したら、Webユーザーインターフェイスを起動して、工場出荷時のデフォルト設定に復元されていることを確認します。

7. USBメモリドライブを取り外します。

重要：工場出荷時のデフォルト設定に復元した後、USBメモリドライブを取り外さなかった場合、復元プロセスが再実行されます。

8. 必要に応じて、アプライアンスのファームウェアをアップグレードします。
9. アプライアンスがサイトクラスまたは親子サイトファミリー構成の一部である場合：
 - a. WebUIにアクセスし、Web UIを介して正しいIPアドレスを再入力します。ACC 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。
 - b. アプライアンスがマージされたサイトの一部でない場合は、ライセンスをアクティベートします。
 - c. アプライアンスをサイトまたはサイトファミリーにマージまたは接続します。

ストレージSSDの交換

失敗したか、まだ機能している ACC ES Rugged 8ポートアプライアンス のストレージSSDを交換できます。アプライアンスの電源を切らずに取り外して交換できます。アプライアンスのロックされたフロントパネルの後ろのトレイにあります。トレイはアプライアンスからスライドさせて出し入れします。

重要：ストレージSSDは、同じ容量のSSD（VMA-RPA-8P2モデルの場合は2TB、VMA-RPA-8P4モデルの場合は4TB）と交換する必要があります。

ACC ソフトウェアのシステム設定（ACC パスワードとカメラ接続の設定を含む）、さらに自己学習ビデオ解析ルール、記録ライセンス、および記録映像はすべて、ACC ES Rugged 8ポートアプライアンスのリムーバブルストレージSSDに保存されます。ストレージSSDに障害が発生した場合、このデータは障害が発生したドライブから取得できません。

Web UI管理者パスワード、アプライアンスIPアドレス、およびNTP構成設定はSSDに保存されませんが、失われることはありません。

ヒント：ストレージSSDを交換する必要がある場合は復元できるように構成した後、アプライアンスのシステム設定の定期的バックアップを開始します。

交換するのが故障したSSDでも機能しているSSDでも、ある程度のダウンタイムが必要です。SSDが取り出し状態になるとすぐに、すべての記録が停止し、以前の設定のバックアップが復元された後、またはACC ES Rugged 8ポートアプライアンス が新しくインストールされたかのように再構成され、ACC と記録のライセンスが再アクティブ化された後にのみ開始できます。

SSDを交換する前に、ACC ES Rugged 8ポートアプライアンス に追加された記録ライセンスを非アクティブ化します。「ライセンスの非アクティブ化」（32ページ）を参照してください。

SSDが交換された後：

- ライセンスを再アクティブしてください。「ライセンスの再アクティブ化」（34ページ）を参照してください。
- サイト設定のバックアップからACCシステム設定を復元します。


ヒント：アプライアンスのファームウェアの新しいバージョンが利用可能な場合は、アプライアンスのファームウェアをアップグレードする前にシステム設定を復元することをお勧めします。




- ある場合、最新バージョンのファームウェアにアップグレードします
- ビデオ録画とビデオ分析ルールは、新しくインストールされたアプライアンスと同様に、最初からやり直します。

ストレージSSDを交換するには、次の手順を使用します：

1. ACC ES Rugged 8ポートアプライアンスに関連付けられているすべてのライセンスを非アクティブ化します。サイトライセンスの非アクティブ化詳細については、ACC ヘルプまたはAvigilon ACC Client ユーザーガイドを参照してください。
2. SSDの取り出しステータスを開始します：

重要： SSDを物理的に接続解除してアプライアンスから取り外す前に、Webインターフェース起動ページのストレージパネルで取り出し状態を開始する必要があります。

- a. サーバー管理ページにログインします。詳細については、「「サーバー管理の開始と停止」(18ページ)」を参照してください。
- b. ナビゲーションバー上の**ストレージ**をクリックします。詳細については、「「ストレージSSDの監視と切断」(25ページ)」を参照してください。
- c. Webインタフェースの起動ページのストレージパネルで、をクリックします。

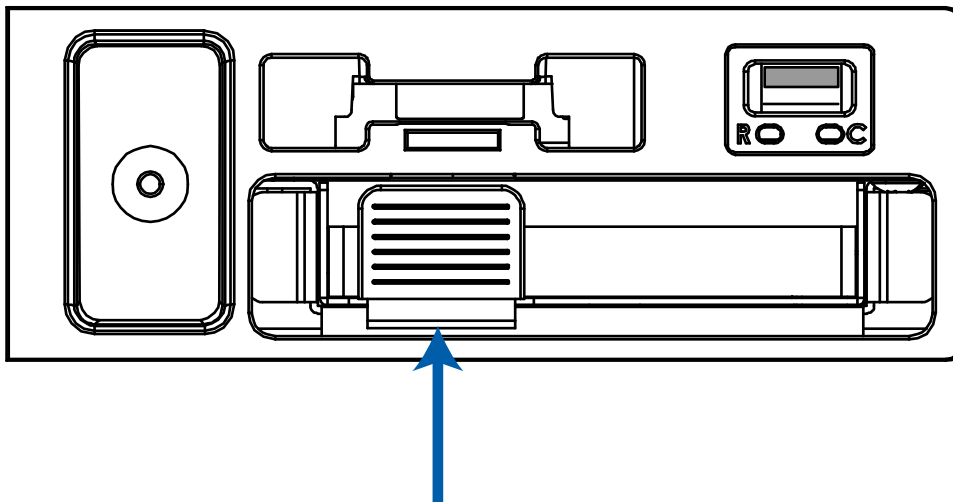
ステータスがに変わり、がに変わり、すべてのサービスが停止したことが示されます。

メモ： 機能しているストレージSSDが取り出されると、アプライアンス上のすべての記録およびソフトウェアサービスが停止します。同じストレージSSDがアプライアンスに再挿入された場合、ソフトウェアサービス再起動後に、記録が再開されます。

3. 提供されたキーを使用して、フロントパネルのロックを解除して開きます。


ヒント： キーを反時計回りに180度回して、フロントパネルのロックを解除します。フロントパネルが下がり、ストラップでアプライアンスに取り付けられます。

4. SSDトレイの青いプルタブを見つけます。



5. SSDの取り外し：

- a. 人差し指を青いタブの後ろに置き、少し力を加えてトレイをアプライアンスから引き出します。トレイを開くと、SSDがアプライアンスから物理的に接続解除されます。



重要：ステータスが  に変わるまで約10秒待ってから続行します。これは、アプライアンスがSSDの取り外しを検出したことを示すものです。

- b. トレイをスライド式引き出しから持ち上げます。
- c. トレイにSSDを取り付けている4本のネジを外します。それらを安全に保管して、交換用SSDを再接続します。
- d. トレイからSSDを取り外します。

Webインターフェースの起動ページのストレージパネルのSSDのステータスは  のままです。

6. SSDの挿入：

- a. トレイにSSDを置きます。
- b. 交換用SSDをトレイに取り付けます。
元のSSDを取り外した後に保管していた4本のネジを使用します。
- c. スライド式引き出しにトレイを入れます。
- d. かすかなカチッと音がするまで内側に青色のタブを押してください。これは、SSDが物理的にアプライアンスに接続されたことを示します。

Webインターフェースの起動ページの変更のストレージパネルのSSDのステータスが、 に変わります。SSDが物理的に再接続されると、ステータスが  に変わります。

7. ACC システム設定の最新のバックアップを復元するか、新しくインストールした時と同様、ACC ES Rugged 8ポートアプライアンスを構成します。ACCシステム設定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。
8. ある場合、アプライアンスファームウェアの最新バージョンをインストールします。詳細については、「「ファームウェアをアップグレードする」 (45ページ) 」を参照してください。
9. ACC ES Rugged 8ポートアプライアンスに使用されているすべてのライセンスを再アクティブ化します。サイトライセンスのアクティベーションの詳細についてはACC ヘルプまたは*Avigilon ACC Client ユーザーガイド*を参照してください。

重要：ライセンスを再アクティブ化できない場合は、[avigilon.com/contact](https://www.avigilon.com/contact) から Avigilon テクニカルサポートにお問い合わせください。

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-RGD-8Px-<シリアル番号>」という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—最初の画面で**Advanced (高度)** をクリックして、2番目の画面で **Proceed to <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—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ド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があります。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。
- ファイルエクスプローラー (Windows) またはFinder (Apple) の使用
「VMA-RPA-RGD-8Px-<シリアル番号>」という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-RGD-8Px-<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-RGD-8Px-<シリアル番号>](https://VMA-RPA-RGD-8Px-<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 Rugged 8ポートアプライアンスが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 Rugged 8ポートアプライアンス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」(26ページ) 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。

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。