

SmartPSS Lite ユーザーマニュアル








はじめに

一般

本書は、SmartPSS Lite（以下、「ソフトウェア」と呼ぶ）の機能と操作を紹介します。本ソフトウェアのご使用前によくお読みになり、将来の参照用に本書を大切に保管してください。

安全上の指示

以下の警告表示が本書内に示される場合があります。

警告表示	意味
 危険	死亡事故や深刻な怪我の可能性のある重大な危険を示します。
 警告	軽度や中程度の怪我を負う受傷事故が発生する可能性がある危険を示します。
 注意	物損、データ損失、性能の低下、予期しない結果を招く可能性のあるリスクを示します。
 ヒント	問題解決や時間節約のための方法を示します。
 注記	追加情報を示します。

改訂履歴

Version	Revision Content	Release Time
V1.0.4	Updated the event linkage and database settings.	January 2024
V1.0.3	<ul style="list-style-type: none">Updated the system settings function.	April 2023
V1.0.2	<ul style="list-style-type: none">Updated basic setting function.Updated adding device function.Updated device configuration function.	December 2022
V1.0.1	<ul style="list-style-type: none">Updated home page.Updated data management function.Updated backup and restore function.	August 2022
V1.0.0	First release.	April 2022

プライバシー保護に関する通知

本デバイスのユーザーまたはデータ管理者として、顔、指紋、ナンバープレートなど他人の個人データを収集する場合があります。お客様は、現地のプライバシー保護の法規制を遵守し、他者の正当な権利と利益を保護するために、次のような措置を講じる必要があります。監視区

域の存在を知らせ、必要な連絡先情報を提供するために、明確で目に見える識別情報を提供します。

マニュアルについて

- 本書は参考資料です。本書と製品には若干の差異が見られる場合があります。
- 本書に従わない方法で操作したことにより生じた損害については、当社は責任を負いかねます。
- マニュアルは該当の管轄地域における最新の法規制に基づき更新されます。詳しくは、紙版の取扱説明書か、CD-ROMをご利用ください。あるいは、QRコード読み取りか、公式HPをご覧ください。本書は参考資料です。電子版と紙版では、若干の差異が見られる場合があります。
- 全てのデザインやソフトウェアは、書面による予告なしに変更されることがあります。製品の更新により、実際の製品とマニュアルとの間に差異が生じる場合があります。必要に応じてカスタマーサービスに連絡し、最新のプログラムと補足説明書を入手して下さい。
- 機能、操作、技術データの説明には、印刷上の誤りや逸脱がある場合があります。いかなる疑義または論争がある場合は、当社が最終的な解釈の権利を有するものとします。
- マニュアル（PDF形式）を開くことができない場合は、リーダーソフトウェアをアップグレードするか、他のPDFリーダーソフトをお試しください。
- 本書に記載されている商標、登録商標、会社名は、それぞれの所有者に帰属します。
- デバイスの使用中に問題が発生した場合は、当社のウェブサイトを確認するか、販売代理店またはカスタマーサービスへお問い合わせください。
- 本書の内容については、万全を期して作成しましたが、万一不明な点や誤りなどお気づきの点がありましたら、ご連絡ください。また、いかなる不確実性または論争がある場合は、当社が最終的な解釈の権利を有するものとします。

目 次

はじめに	1
1 概要	1
2 インストールとログイン	2
2.1 インストール	2
2.2 初期化	2
2.3 ログイン	4
2.4 パスワードの再設定	5
2.5 フィードバック	5
3 ホームページ	7
4 システム設定	9
4.1 基本設定	9
4.2 モニタリング設定	10
4.3 デバイス設定	12
4.4 イベント設定	12
4.5 ローカルパス	13
4.6 データ管理	14
4.7 勤怠管理設定	16
4.8 ビデオ通話設定	17
4.9 バックアップと復元	19
4.10 データベース設定	20
5 デバイスの管理	21
5.1 デバイスの追加	21
5.1.1 自動検索によるデバイスの追加	21
5.1.2 手動によるデバイスの追加	22
5.1.3 デバイスの一括インポート	25
5.2 デバイスの削除	25
5.3 デバイスのエクスポート	26
5.4 デバイスの編集	27
5.4.1 デバイス情報の編集	27
5.4.2 初期化	27
5.4.3 IPアドレスの変更	30
5.4.4 デバイス設定	31
5.4.5 アラーム設定	34
6 ログの検索	36
7 イベント設定	37
8 イベントセンター	40
8.1 ページの紹介	40
8.2 ライブビュービデオの設定	41
付録1 サイバーセキュリティに関する推奨事項	44

1 概要

SmartPSS Liteは中小規模のソリューション向けに開発されたクライアントソフトウェアです。必要に応じて様々なソリューションをダウンロードすることができます。本書では一般的な機能と操作を紹介します。

2 インストールとログイン

2.1 インストール

技術サポートに連絡するかToolBoxをダウンロードしてSmartPSS Liteを入手してください。

- SmartPSS Liteのソフトウェアパッケージを入手する場合は、ページの説明に従いソフトウェアをインストールし、実行してください。
- ToolBoxによりソフトウェアを入手する場合は、ページの説明に従い SmartPSS Liteを実行してください。

2.2 初期化

初めてログインするときに、ログイン用のパスワードの設定や、ログイン用のパスワードの設定など、Smart PSS Lite を初期化します

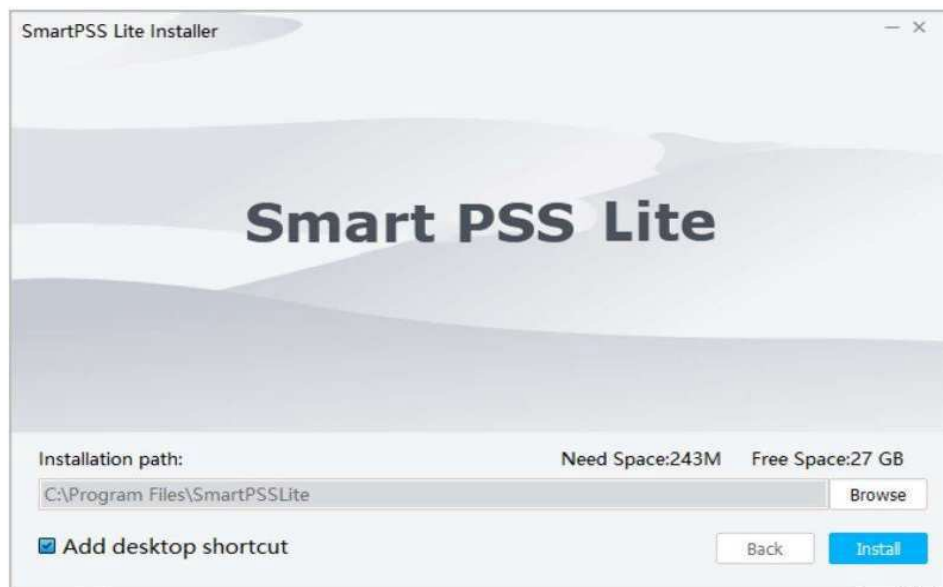
パスワードをリセットするためのセキュリティ上の質問。

手順 1 SmartPSSLite.exe をダブルクリックするか、または ToolBox のソフトウェア アイコンの横にある Open をクリックします。

手順 2 ドロップダウン リストから言語を選択し、[I have read and agree the software] を選択します
同意して、次へをクリックします。

手順 3 [参照] をクリックしてインストールパスを選択し、[インストール] をクリックします。

図2-1 インストールパスの選択



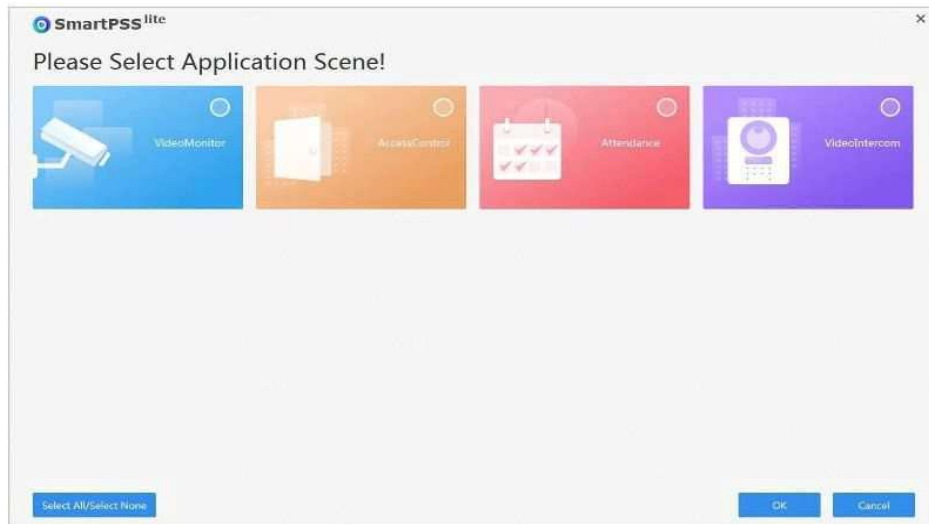
手順 4 [Finish] をクリックしてインストールを完了します。



[Run Smart PSS Lite] を選択して、Smart PSS Lite を起動します。

手順 5 追加するアプリケーション シーンを選択し、[OK] をクリックします。

図2-2 アプリケーションシーンの選択



ステップ6 「同意して続行」をクリックし、ソフトウェア使用許諾契約と製品プライバシーポリシーに同意します。
ステップ7 初期化ページでパスワードを設定し、[次へ]をクリックします。

図2-3 パスワードの設定



表 2-1 初期化パラメータ

パラメータ	説明
パスワード	パスワードには空白でない8～32文字で入力し、大文字、小文字、数字、特殊文字（'";:&を除く）のうち2種類以上の文字を含める必要があります。
パスワードの強度	推測やブルートフォースアタックに対するパスワードの有効性が表示されます。緑は強力なパスワード、赤は強度に欠けるパスワードを意味します。パスワード強度のプロンプトに従い、セキュリティレベルが高いパスワードを設定します。
パスワードの確認	再度パスワードを入力し、パスワードを確認します。
登録後の自動ログイン	SmartPSS Liteが初期化後に自動的にログインするように、 登録後に自動ログイン （Auto Login after Registration）を有効化します。それ以外の場合は、ログインページが表示されます。

ステップ7: セキュリティ質問を設定し、**終了**（Finish）をクリックします。

図2-4 セキュリティの質問を設定する

The screenshot shows a window titled 'Initialization' with a close button (X) in the top right corner. Inside the window, there are two tabs: '1.Password Setting' (active) and '2.Password Protection'. Below the tabs, there is a message: 'Please set security questions!'. This is followed by three sets of questions and answers. Each set consists of a 'Question' label, a dropdown menu, and an 'Answer' text box. The questions are: 'Question 1: What is your favorite children's book?', 'Question 2: What was the first name of your first boss?', and 'Question 3: What is the name of your favorite fruit?'. At the bottom right of the window, there is a blue button labeled 'Finish'.

2.3 ログイン

手順

手順 1 SmartPSSLite.exe をダブルクリックするか、または ToolBox のソフトウェア アイコンの横にある Open をクリックします。

手順 2 ユーザ名とパスワードを入力し、「Login」をクリックします。
コンピュータ上で複数のネットワークが使用可能な場合は、その中から1つを選択できます

図 2-5 ログイン

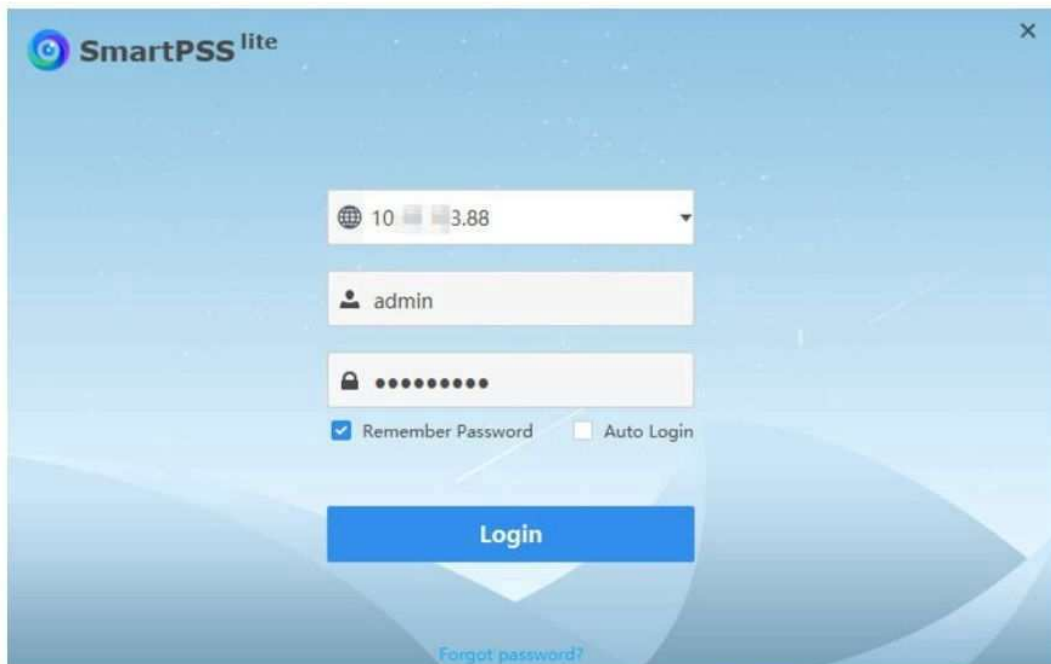


表 2-2 ログインのパラメータ

パラメータ	説明
パスワードを保存	次回ログイン時にパスワードを入力する必要が無いように、 パスワードを保存 (Remember Password) を有効化します。
自動ログイン	次回同じユーザーアカウントを使用する時にSmartPSS Liteが自動的にログインするように、 自動ログイン (Auto Login) を有効化します。
パスワードをお忘れですか？	パスワードを忘れた時に パスワードをお忘れですか？ (Forgot password?) をクリックし、セキュリティ質問によりパスワードを再設定します。

2.4 パスワードの再設定

セキュリティの質問に回答することでパスワードを再設定することができます。

ステップ1: SmartPSSLite.exeをダブルクリックするかToolBoxのソフトウェアアイコンの隣の**開く (Open)** をクリックします。

ステップ2: ログインページで**パスワードをお忘れですか？** (Forgot password?) をクリックします。

ステップ3: セキュリティ質問に回答し、**次へ (Next)** をクリックします。

ステップ4: ページの説明に従い、パスワードを再設定します。

2.5 フィードバック

報告がある場合は、ページの右上にある > **フィードバック (Feedback)** を選択して提案(言葉)を入力し、写真と添付ファイルをアップロードして、**送信 (Submit)** をクリックします。

図2-6 フィードバック

Feedback

×

Problem type: Attendance Solution ▼

Do you have any suggestions or questions to tell us?

You can enter up to 200 characters

Contact type: Email ▼

Add Picture

Add Affix

☐ Device info(system version, processor, memory, free disk space)

☐ Resource warning(CPU consumption, memory usage)

Submit

3 ホームページ

ホームページは9つの部分から構成されます。

図 3-1 ホームページ

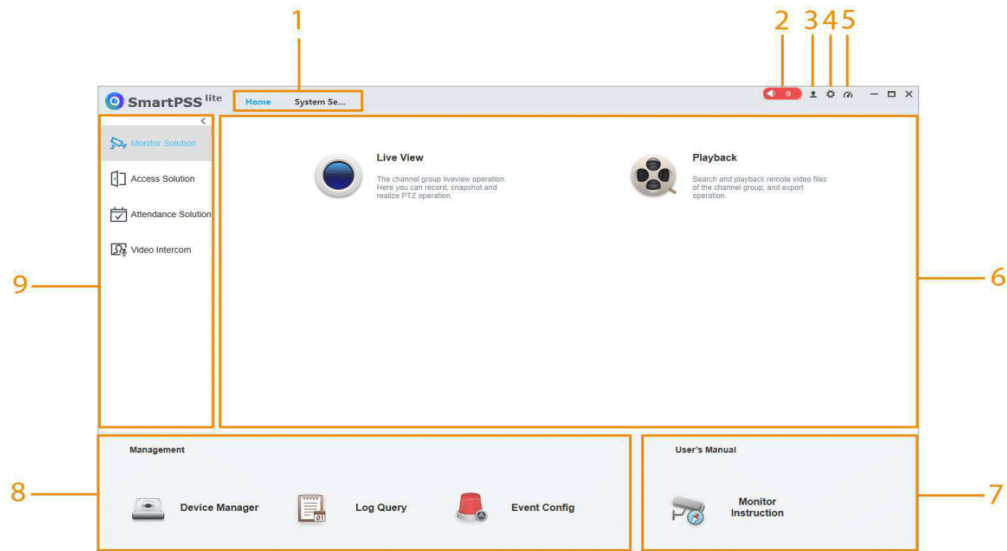










表 3-1 ホームページのパラメータ

番号	パラメータ	説明
1	機能タブ	デフォルトでホームページが表示されます。 初めて機能をクリックする時は、機能タブがここに追加されます。
2	アラーム音	 または  をクリックすると、アラーム音がオンまたはオフになります。アイコンの数字は、報告されたが未処理のアラームイベントの数を意味します。番号をクリックして イベントセンター (Event Center) を開き、アラームイベントの詳細を表示します。詳細については、「8 イベントセンター」を参照してください。

番号	パラメータ	説明
3	ユーザー	<ul style="list-style-type: none"> •  をクリックし、アカウント (User Manager) を選択し、役割/ユーザーの追加、役割/ユーザーの削除、権限の設定などのユーザーの管理を実行します。 •  をクリックし、ロックスクリーン (Lock Screen) を選択し、画面をロックします。ロック解除したい時には、ログインアカウントのパスワードを入力します。 •  をクリックし、ユーザー切り替え (Switch User) を選択し、ログインページに戻ります。新規アカウントでログインできます。 •  をクリックし、ヘルプマニュアル (Help Manual) を選択し、取扱説明書を入手します。 •  をクリックし、製品について (About) を選択すると、システムのバージョン、日付、オープンソースステートメント (Open source Statement)、ソフトウェアライセンス規約 (Software license agreement) が表示されます。 <p>検索および問題の解決のために、デバッグログがローカルパスに自動的に保存されるようにデバッグログを開く (Open Debugging Log) を有効化します。</p>
4	システム	基本設定やモニタリング設定などを設定します。詳細については、「4 システム設定」を参照してください。
5	システムステータス	 をクリックして、CPUとRAMの使用率のステータスを表示します。CPUの使用率が高い場合は、アイコンが赤になります。
6	機能モジュール	機能アイコンをクリックして、機能ページへ移動します。
7	ユーザーマニュアル	アイコンをクリックして、対応するソリューションのユーザーマニュアルを取得します。
8	管理	<ul style="list-style-type: none"> • デバイス (Device Manager): デバイスの追加、デバイスのリモート設定、IPアドレスの変更などを行うことができます。 • ログ (Log Query): ソフトウェアとデバイスのログ情報を検索したり、エクスポートすることができます。 • イベント設定 (Event Config): アラーム連動アクションを設定します。
9	ソリューションモジュール	必要なソリューションを選択します。 > または < をクリックして、ソリューションを表示または非表示にします。

4 システム設定

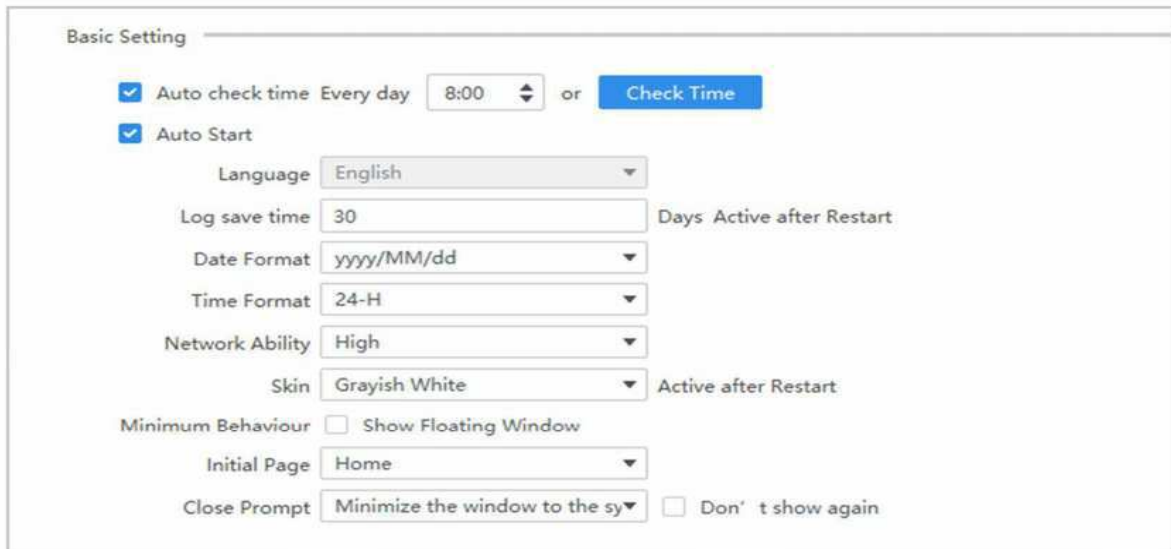
4.1 基本設定

ソフトウェアの時間、言語、スキンなどの機能を設定します。

ステップ1:  > システム (System Config) > 基本設定 (Basic setting) を選択します。

ステップ2: 基本設定パラメータを設定します。

図4-1 基本設定



Basic Setting

☒ Auto check time Every day 8:00 or

☒ Auto Start

Language English

Log save time 30 Days Active after Restart

Date Format yyyy/MM/dd

Time Format 24-H

Network Ability High

Skin Grayish White Active after Restart


Minimum Behaviour ☐ Show Floating Window

Initial Page Home

Close Prompt Minimize the window to the sy ☐ Don't show again

表 4-1 基本設定パラメータの説明

パラメーター	説明
オートチェック時間	設定時刻にデバイスが自動的に時間をチェックするように 毎日時間を自動チェック (Auto Check Time Everyday) を有効化し 時間をチェック (Check Time) を設定します。
自動スタート	コンピュータの電源を入れると、ソフトウェアが自動的に起動します。
言語	再起動後アクティブになる言語を表示します。
ログ保存時間	ログの保存期間を設定し、当日から設定された時間までのログが保存されます。この機能は、再起動後にアクティブになります。例えば、保存期間を30として設定すると、過去30日間のログが保存されます。
日付形式	年/月/日の表示形式を選択します。

パラメーター	説明
時間形式	時間の表示形式を選択します。
ネットワーク機能	ご利用のネットワーク状態に基づいてネットワークの能力を選択します。例えば、ネットワークの状態が高速である場合は 高 (High) を選択することを推奨します。
スキン	再起動後アクティブになるスキンを選択します。デフォルト設定は灰白色です。
最小動作	浮動ウィンドを表示 (Show Floating Window) を選択すると、ソフトウェアが最小化された後に、トリガーされたアラームイベント数を入力するようプロンプト  が表示されます。
初期ページ	ソフトウェアの起動時にデフォルトで開く機能タブを選択します。 新規と最後のページを復元 (Resume last page) から選択できます。
プロンプトを閉じる	ソフトウェアを閉じた時に、プロンプトを自動的にポップアップ表示するか設定できます。。プロンプトが不要な場合は、 今後表示しない (Don't show again) にチェックを入れてください。

ステップ3: **適用** (Apply) をクリックします。

4.2 モニタリング設定

デフォルトのシステムタイプ、インスタントリプレイ時間、ローカル録画時間などの機能を設定します。

ステップ1:  > **システム設定** (System Config) > **モニタリング設定** (Monitor setting) を選択します。

ステップ2: モニタリング設定パラメータを設定します。

図 4-2 モニタリング設定

Monitor Setting

Default Stream Type

Self-adaptive Stream Type

Instantly replay time

5Minutes

Local Record Time

30

Minutes

Default Device Tree

Device Tree(By Device)

Active after Restart

Decode Type

Soft Decode

☐ Resume Last Preview
 ☒ Show IVS Rule
 ☐ Save Device Tree Selection

表 4-2 モニタリング設定パラメータの説明

パラメータ	説明
デフォルトのストリームタイプ	リアルタイムのデフォルトストリームタイプを選択します。 自適応ストリーム (Self-adaptive Stream Type)、 サブストリーム (Sub Stream)、 メインストリーム (Main Stream) から選択できます。
インスタント再生時間	インスタント再生時間を選択します。 この値が5分の場合、その前の5分間が再生されます。
ローカル記録時間	ローカル記録時間を選択します。この値が30分に設定されている場合、システムはビデオを30分間録画し、自動的にコンピュータのデフォルトパスにこのビデオを保存します。デフォルトパスは¥Data¥User¥Recordです。
デフォルトデバイスツリー	<ul style="list-style-type: none"> デバイスツリー (デバイス別): デバイスをノードとして表示します。 領域ツリー (チャンネル別): チャンネルをノードとして表示します。
デコードタイプ	<ul style="list-style-type: none"> ソフトデコード (Soft Decode): グラフィックカードでビデオをデコードします。 ハードウェアデコード (Hardware Decode): CPUでデコードします。
最後のプレビューを再開	この機能を有効にすると、ソフトウェアの再起動後に、ソフトウェアは、自動的に最後のプレビューを開きます。
IVSルールを表示します	この機能を有効にすると、モニタリング画面にIVSルールが表示されます。
デバイスツリー選択の保存	デバイスをデバイス ツリー内で選択したままにしておき、別のデバイス検索を実行します。

ステップ 3適用 [Apply] をクリックします。

4.3 デバイス設定

[System Settings] > [Device Settings] を選択し、[Auto Login to device (Take Effect)] をクリックします。
[Restart]（再起動後）をクリックすると、起動時にプラットフォームに自動的にログインします。

4.4 イベント設定


アラーム音を設定し、メールの送信者と受信者をリンクします。
ステップ1:  > システム設定 (System Config) > イベント (Event) を選択します。
ステップ2: イベント設定パラメータを設定します。

図 4-3 イベント設定

Event

☒ Loop


☐ Global Wav


Channel Event ▾

Video Loss ▾

Wav File Path

./Data/System/Sound/en/video lost.wav





☒ SMTP

SMTP Server

Port 25

User Name

Password

Sender

Receiver

Encrypt Mode None ▾

Interval Time 10 (s)

Test

+

表 4-3 イベント設定パラメータの説明

パラメータ	説明
ループプレイ	この機能を有効にした場合、イベントが発生するとアラーム音がループします。

パラメータ	説明
グローバルWav	<ul style="list-style-type: none"> ● グローバルWav (Global Wav) を選択し、Wavファイルパス (Wav File Path) でサウンドファイルを指定します。対応するイベントがトリガーされた後でサウンドが再生されます。 ● グローバルWav (Global Wav) を選択せずに、ドロップダウンリストでイベントタイプとサウンドタイプを選択するか、Wavファイルパス (Wav File Path) でサウンドファイルを選択します。対応するイベントがトリガーされた後でサウンドが再生されます。
SMTP	<p>SMTP機能を有効にする。</p> <ol style="list-style-type: none"> 1. SMTP機能を有効にする。 2. SMTPサーバーのポート番号のIPを入力します。 3. 送信メールのユーザー名とパスワードを入力します。 4. 送信者と受信者のメールを入力します。 <p>最大5件まで入力可能です。</p> <ol style="list-style-type: none"> 5. 暗号化モードを選択し、間隔時間を入力します。 <p>設定した間隔で、自動的に電子メールで通知を送信します。</p> <p>設定した間隔で自動的に電子メールで通知を送信します。</p> <p>暗号化プロトコルは、ネットワーク上の送信中にデータを安全に保つために使用されます。</p> <p>ネットワークを介して送信されます。</p> <ol style="list-style-type: none"> 6. 電子メールテストをクリックすると、テスト電子メールを送信して、正常に機能するかどうかを確認できます。

ステップ3: **適用** (Apply) をクリックします。

4.5 ローカルパス

プラットフォームが収集した写真、ビデオ、その他のデータの保存パスを設定します。
手順

ステップ 1  をクリックし、システム設定 > ファイルパスを選択します。

ステップ2 ローカルパスを設定します。


図 4-4 ローカルパスを設定する



ステップ3 **適用** (Apply) をクリックします。

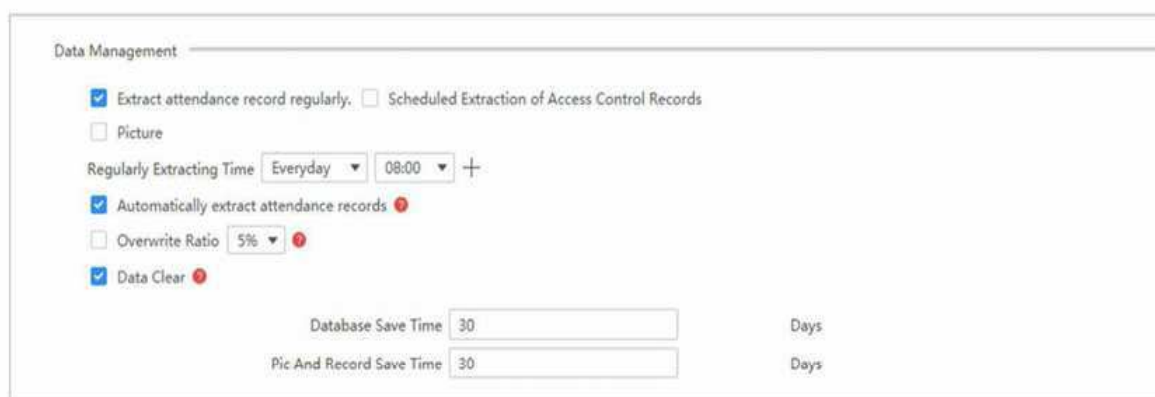
4.6 データ管理

デバイスから出勤データを定期的に抽出し、コンピューターに保存されているデータ、写真、ビデオを定期的に消去します。

ステップ1:  > **システム設定** (System Config) > **データ管理** (Data Management) を選択します。

ステップ2: データ管理パラメータを設定します。

図 4-5 データ管理



Data Management

☒ Extract attendance record regularly. ☐ Scheduled Extraction of Access Control Records

☐ Picture

Regularly Extracting Time: Everyday 08:00 +

☒ Automatically extract attendance records



☐ Overwrite Ratio: 5%

☒ Data Clear

Database Save Time: 30 Days

Pic And Record Save Time: 30 Days

表 4-4 データ管理パラメータの説明

パラメータ	説明
出勤記録を定期的抽出 します。	ソフトウェアは、設定された時間に応じて、勤怠とアクセス制御の記録と写真を自動的に抽出します。
アクセス制御レコード の定期抽出	 <ul style="list-style-type: none"> 勤怠デバイスでは勤怠データが直接抽出されます。アクセスコントローラーでは、事前にデバイスが勤怠ポイントとして設定され、次に勤怠データが抽出されます。詳細については、<i>SmartPSS Lite 勤怠ソリューションユーザーズマニュアル</i>を参照してください。 定期抽出時間 (Regularly Extracting Time) を毎日 (Everyday) に設定した場合、5個のタイムポイントを選択できます。 定期抽出時間 (Regularly Extracting Time) を毎週 (Every Week) に設定した場合、特定の曜日で特定のタイムポイントを選択できます。
勤怠記録を自動抽出	勤怠記録を自動抽出 (Auto extraction) 機能を有効にすると、ソフトウェアは、自動的に、勤怠記録またはアクセス制御記録を抽出します。
上書き率	上書き率 (Overwrite Ratio) 機能を有効にして、比率を設定します。 ディスクが一杯になると、システムは比率に応じて古い画像とビデオを自動的に上書きします。
データベース保存時間 写真と記録の保存時間	実際の要件に応じて、データベース、写真、ビデオの保存時間を設定します。ソフトウェアは保存期間が超過したデータと画像を自動的に消去します。消去は毎日00:00またはソフトウェアが起動する時刻に開始します。  このデータには温度監視データは含まれません。

ステップ3: **適用** (Apply) をクリックします。

4.7 勤怠管理設定

手順

ステップ 1 をクリックし、「システム設定 (System Settings) 」 >

「出席設定 (Attendance Setting) 」を選択します。

ステップ 2 勤怠設定を設定します。

図 4-6 勤怠設定

Attendance Setting

Report Time Format: min

☒ Sync Third-party Database: C:/Users/Public/SmartPSSLite/Data/User/ExternalDatabase/

☒ Attendance Summary SMTP Settings

SMTP Server:

Port: 25

Username:

Password:

Sender:

Receiver: +

Encryption Type: None

Email Test



☒ Send attendance summary regularly

Period: ☒ Month Passed ☐ Current Month

Time: Daily Summary Table Everyday Select time +

表 4-5 勤怠設定パラメータ

パラメータ	説 明
レポートの時間形式	勤怠レポートの時間形式を定義します。例えば、min に設定されている場合、レポートの勤怠時間は時間と分の形式で表示されます。

パラメータ	説 明
サードパーティデータベースの同期	定義されたファイルパスに勤怠データを同期させます。
勤怠サマリーSMTP設定	<p>指定した電子メールに勤怠サマリーを送信する。</p> <ol style="list-style-type: none"> 1. SMTP機能を有効にする。 2. SMTPサーバーのポート番号のIPを入力する。 3. 送信メールのユーザー名とパスワードを入力します。 4. 送信者と受信者のメールアドレスを入力します。 <p></p> <p>5通までのメールに対応。</p> <p>5. 暗号化モードを選択します。 システムは自動的に設定された間隔で電子メールに勤怠レポートを送信します。</p> <p></p> <p>暗号化プロトコルは、ネットワーク上でのデータ伝送中にネットワーク上での伝送中にデータを安全に保つために使用される。</p> <p>6. 電子メールのテスト]をクリックして、テスト電子メールを送信し、正常に機能するかどうかを確認することができます。</p>
出勤簿を定期的に送付	<ul style="list-style-type: none"> ● 期間 定義された頻度で勤怠サマリーを送信します。 毎月： 毎月送信します。 現在の月： 今月の出欠状況を送信します。 ● 当月： 今月の出欠サマリーを送信します。 時刻： 指定した時刻に出席集計を送信します。 毎日のサマリーテーブル： 日別集計表： 日別集計表の形式で勤怠集計を送信します。 月別サマリー 月別集計表： 月別集計表の形式で出欠状況を送信します。 月別サマリー表のフォーマットで送信します。

ステップ3 適用をクリック

4.8ビデオ通話設定

設定手順

Step 1 をクリックし、「システム設定」>「ビデオ通話」を選択します。

Step 2 出席の設定を行います。

図 4-7 ビデオ会議

Video Intercom

SIP Server Port 5080
Reset
Take Effect after Restart

Compound Organization ☒ Building ☒ Unit Take Effect after Restart

If you want to change the organization configuration for the compound, please clear the data in dial management first, and then clear the room number and compound organization in building management.

表 4-6 ビデオ インターコムのパラメータ


パラメータ	説 明
SIP サーバ ポート	プラットフォームが SIP サーバとして機能する場合は、SIP サーバのポートを入力します。
複合組織	<p>組織レベルを設定する。</p> <ul style="list-style-type: none"> ●建物：組織は建物のみが含まれます。 ●ユニット：組織には建物とユニットが含まれます。 <p> 設定は、プラットフォームが次の状態になった後に有効になります。</p> <p>再起動しました。組織のレベルを変更する場合は、 [Video Intercom] > [Intercom Con g] > [Dial] の順に選択します。</p> <p>そこから既存のデータを管理してクリアし、 Building Manager に移動して残りのデータをクリアします。</p>

ステップ 3 適用をクリック

4.9 バックアップと復元

バックアップおよび復元プラットフォームの構成。

手順

ステップ 1 をクリックし、[システム設定] > [バックアップと復元]を選択します。

ステップ 2 バックアップ パラメータを設定します。


Backup and Restore

Backup Path

C:/Users/Public/SmartPSSLite/Data/User/Backup

Manual Backup

☐ Auto Backup

 Back up all data

Reset


Take Effect after Restart

Backup Path of Platform Co...

C:/Users/Public/SmartPSSLite/Data/User/BackupPlatConfig

Manual Backup

☐ Auto Backup

 Only back up the platform configuration

Reset

Take Effect after Restart

表 4-7 パラメータの説明

パラメータ	説 明
Backup Path	バックアップファイルのパスを選択し、[適用]をクリックして変更を保存します。設定ファイルは定義されたファイルパスに保存されます。
Manual Backup	設定ファイルを設定したファイルパスに手動でバックアップする。
Auto Backup	自動バックアップ機能を有効にし、自動バックアップ時間を設定し、[適用]をクリックします。プラットフォームは自動的に設定されたファイルパスに設定されたファイルパスにバックアップされます。
復元	設定ファイルをプラットフォームにアップロードします。プラットフォームが再起動すると、コンフィギュレーションはプラットフォームに適用されます。再起動後にプラットフォームに適用される

ステップ 3 適用をクリック

4.10 データベース設定

サードパーティのデータベースを設定します。
サードパーティ製サーバーのデータベースは、自動的に本プラットフォームの出退勤記録と同期されかつ、プラットフォームとも同期されます。

手 順

- ステップ1 > ⚙️ をセレクトして、ThirdParties Database Congを選択します。
ステップ2 データベース設定の構成

図 4-9 データベースの設定

Database Settings

Attendance Database(tripartite)

Database Type MYSQL

Server IP

Server Port

Database Name

User Name

User Password

Connection Test

Enable Database ☐

表 4-8 パラメータの説明

Parameters	Description
Database Type	MYSQL.
Server IP	サーバーのIPアドレスとポート
Database Name	データベースの名前
User Name	データベースのユーザー名とパスワード
User Password	
Connection Test	接続が成功したかどうかをテストする

ステップ 3 データベース機能を有効にする

5 デバイスの管理

SmartPSS Liteではデバイスを追加することができます。SmartPSS Liteでデバイスを追加後、デバイスをリモートで設定し操作することができます。

5.1 デバイスの追加

様々な方法でデバイスを追加することができます。IPアドレスやネットワークセグメントなど、状況に応じて最適な方法を選択してください。

- 自動検索
- 手動による追加
- 一括インポート

5.1.1 自動検索によるデバイスの追加



- 同じネットワークセグメント内にデバイスを一括して追加したい場合、またはネットワークセグメントが明確であるがデバイスのIPアドレスが不明確である場合は、自動検索でデバイスを追加することを推奨します。
- デバイスを追加する際にはConfigToolとDSSを終了して下さい。終了していない場合、全てのデバイスを検索できない場合があります。

ステップ1: **デバイス** (Device Manager) ページ上で**自動検索** (Auto Search) をクリックします。

ステップ2: ネットワークセグメントの範囲を設定し、**検索** (Search) をクリックします。

検索済みのデバイスのリストが表示されます。



- **自動検索** (Auto Search) をクリックして検索結果を更新します。
- 必要なデバイスを1台クリックして**IPを変更** (Modify IP) をクリックし、IPアドレス、サブネットマスク、ゲートウェイを変更します。詳細については、「5.4.3 IPアドレスの変更」を参照してください。
- 初期化されていないデバイスを1台クリックし、**初期化** (Initialization) をクリックします。IPアドレス、サブマスク、ゲートウェイ、ログインパスワードをリセットすることができます。詳細については、「5.4.2 初期化」を参照してください。

図5-1 検索結果

The screenshot shows a window titled 'Auto Search' with a close button (X) in the top right corner. Inside the window, there are two tabs: 'Auto Search' (selected) and 'Initialization'. Below the tabs, there is a 'Device Segment' field with a dropdown menu and a 'Search' button. To the right of the 'Search' button, it says 'Search Device Number: 1'. Below this, there is a table with the following columns: 'No.', 'IP', 'Device Type', 'MAC Address', 'Port', and 'Initialization Status'. The table contains one row with the following data: '1', '10.10.10.10', 'DSS V8', '00:00:00:00:00:00', '443', and 'Initialized'. At the bottom right of the window, there are two buttons: 'Add' and 'Cancel'.

No.	IP	Device Type	MAC Address	Port	Initialization Status
1	10.10.10.10	DSS V8	00:00:00:00:00:00	443	Initialized

ステップ3: 必要なデバイスをクリックし、**追加** (Add) をクリックします。

ステップ4: ログインユーザー名とパスワードを入力し、**OK**をクリックして確認します。



- デバイスを追加した後も**自動検索** (Auto Search) ページは表示されています。さらに追加し続けるか、**キャンセル** (Cancel) をクリックして終了することができます。
- 追加した後、デバイスが自動的にログインします。ログインに成功した場合、ステータスがオンラインとして表示され、そうでない場合はオフラインになります。

5.1.2 手動によるデバイスの追加

特定のIPアドレスまたはドメイン名のあるデバイスを1台追加する必要がある場合は、デバイスを手動で追加することを推奨します。

ステップ1: **デバイス** (Device Manager) ページ上で**追加** (Add) を選択します。

ステップ2: デバイスパラメータを設定します。

- IPを使用してデバイスを追加します。

図 5-2 デバイスの手動追加

Add Device

Device Name:

*

Device

Method to add:

IP

IP:

*

Port:

*

37777

User Name:

*

admin

Password:

*

Add and Continue

Add

Cancel

表 5-1 IPパラメータの追加

パラメータ	説明
チャンネル名	容易に識別できるように、デバイスに、監視領域を含む名称を付けることをお勧めします。
登録モード	IP を選択します。
IP/ドメイン	デバイスのIPアドレスを入力します。
ポート	ポート番号を入力します。デフォルトのポート番号は37777です。実際のポート番号が優先されます。

パラメータ	説明
ユーザー名	ログインユーザー名を入力します。
パスワード	ログインパスワードを入力します。

- SNを使用してデバイスを追加します。

図 5-3 SNによるデバイスの追加

The screenshot shows a dialog box titled "Add Device" with a close button (X) in the top right corner. Inside the dialog, there are four input fields, each with a red asterisk indicating it is required: "Device Name:", "SN:", "User Name:", and "Password:". To the right of the "Device Name" field is a dropdown menu labeled "Method to add:" with the option "SN(For Device Support P2P)" selected. At the bottom of the dialog, there are three buttons: "Add and Continue" (blue), "Add" (blue), and "Cancel" (grey).

表 5-2 SNパラメータの追加

パラメータ	説明
登録モード	SN (デバイスサポートP2P用) (SN (For Device Support P2P)) を選択します。
SN	デバイスのシリアル番号を入力します。

ステップ3: **追加** (Add) をクリックしてデバイスを追加し、**デバイスの追加** (Add Device) ページを閉じるか、**追加して続行** (Add and Continue) をクリックしてデバイスを追加し、別のデバイスを容易に追加できる**デバイスの追加** (Add Device) ページを開いたままにします。

5.1.3 デバイスの一括インポート

デバイスを一括して追加する必要があるが同じネットワークセグメント上にない場合は、インポートしてデバイスを追加することを推奨します。デバイス情報を.xml形式のファイルとして編成し、ファイルをインポートします。



デバイス情報のテンプレートをエクスポートすることができます。デバイスを選択し、**エクスポート** (Export) をクリックします。

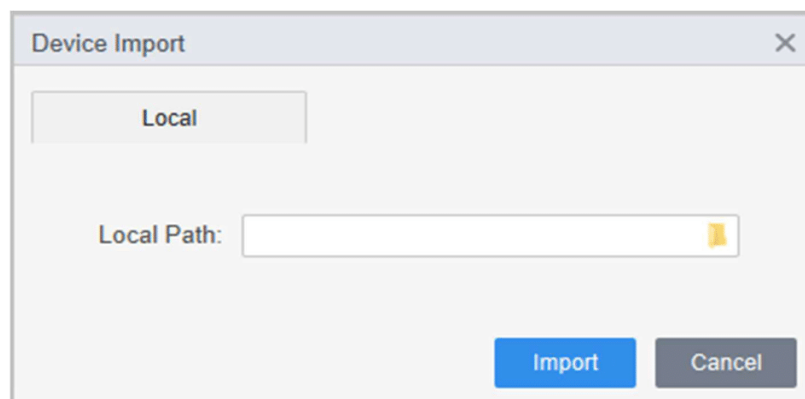
ステップ1: **デバイス**(Device Manager) > **インポート** (Import) をクリックします。

ステップ2: 情報ファイルを選択して、**インポート** (Import) をクリックします。




追加した後、デバイスが自動的にログインします。ログインに成功した場合、ステータスがオンラインとして表示され、そうでない場合はオフラインになります。

図 5-4 デバイス情報を.xmlフォーマットでインポートする



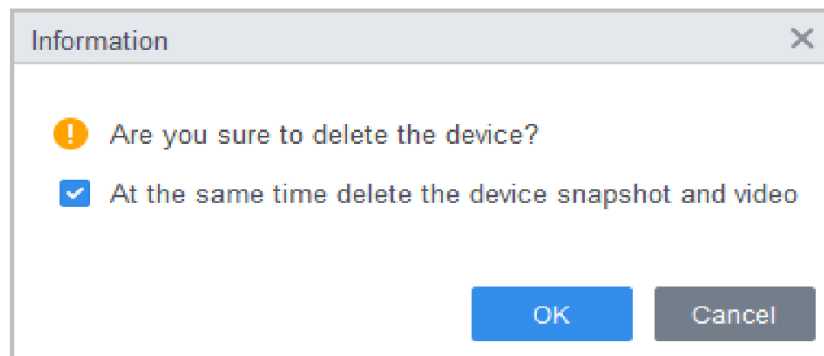
5.2 デバイスの削除

ステップ1: ホームページ上で**デバイス** (Device Manager) を選択します。

ステップ2: 不要になったデバイスを選択し、**削除** (Delete) またはデバイス右側のをクリックします。

ステップ3: (任意) それらのスナップショットとビデオが不要な場合は、**デバイスのスナップショットとビデオを同時に削除する** (At the same time delete the device snapshot and video) を選択します。それ以外の場合は選択しないでください。

図 5-5 デバイスを削除する



ステップ4: **OK**をクリックします。

5.3 デバイスのエクスポート

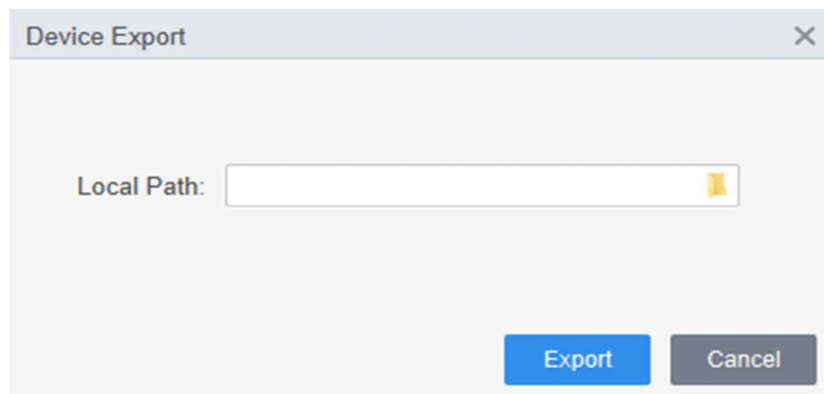
デバイス情報をローカルにエクスポートすることができます。

ステップ1: ホームページ上で**デバイス** (Device Manager) を選択します。

ステップ2: エクスポートしたいデバイスを選択し、**デバイス** (Device Manager) ページで**エクスポート** (Export) をクリックします。

ステップ3: エクスポートのローカルパスを選択し、**エクスポート** (Export) をクリックします。

図 5-6 デバイス情報をエクスポートする



5.4 デバイスの編集

5.4.1 デバイス情報の編集

追加したデバイスの名称、ログインユーザー名、パスワードなどの情報を変更することができます。

ステップ1: ホームページ上で**デバイス** (Device Manager) を選択します。

ステップ2: デバイスリスト内で、選択済みのデバイスの右側にある✎をクリックするか、デバイスをダブルクリックします。

ステップ3: デバイスの情報を編集します。

ステップ4: **保存** (Save) をクリックします。

5.4.2 初期化

コンピュータと同じネットワークセグメント内にあるデバイスの初期化だけに対応しています。

ステップ1: **デバイス** (Device Manager) > **自動検索** (Auto Search) をクリックします。

ステップ2: ネットワークセグメントの範囲を設定し、**検索** (Search) をクリックします。

図 5-7 デバイスリスト

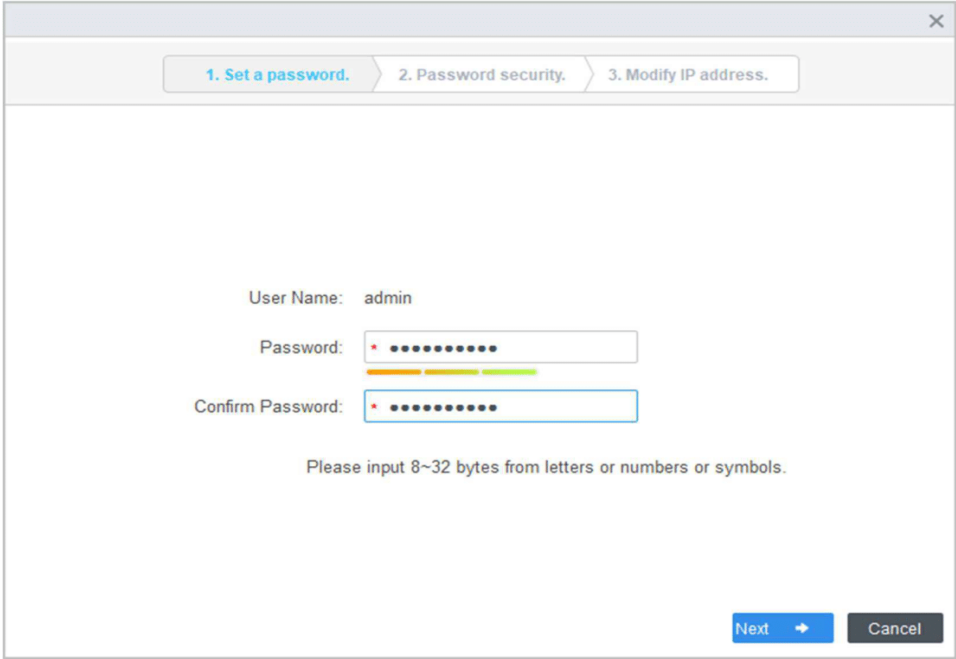
The screenshot shows a window titled "Auto Search" with a close button (X) in the top right corner. Inside the window, there are two tabs: "Auto Search" (selected) and "Modify IP". Below the tabs, there is a "Device Segment" field with a dropdown menu and a "Search" button. To the right of the "Search" button, it says "Search Device Number: 1". Below this, there is a table with the following columns: "No.", "IP", "Device Type", "MAC Address", "Port", and "Initialization Status". The table contains one row with the following data: "1", "10.10.10.10", "DSS V8", "00:00:00:00:00:00", "443", and "Uninitialized". At the bottom right of the window, there are two buttons: "Add" and "Cancel".

No.	IP	Device Type	MAC Address	Port	Initialization Status
1	10.10.10.10	DSS V8	00:00:00:00:00:00	443	Uninitialized

ステップ3: 初期化されていないデバイスをクリックし、**初期化** (Initialization) をクリックします。

ステップ4: パスワードを設定し、**次へ** (Next) をクリックします。

図 5-8 パスワードを設定する



The screenshot shows a web-based configuration window with a close button (X) in the top right corner. At the top, there is a progress bar with three steps: "1. Set a password." (highlighted in blue), "2. Password security.", and "3. Modify IP address.". The main content area contains the following fields and text:

- "User Name: admin" (text label)
- "Password:" followed by a text input field containing masked characters (dots) and a strength indicator bar below it with segments of red, yellow, and green.
- "Confirm Password:" followed by a text input field containing masked characters.
- A note below the fields: "Please input 8~32 bytes from letters or numbers or symbols."
- At the bottom right, there are two buttons: "Next" with a right-pointing arrow and "Cancel".

ステップ5: パスワード再設定のメールアドレスを入力します。

図 5-9 メールアドレスを予約する

The screenshot shows a window titled 'Bind Email Address'. At the top, there is a progress bar with three steps: '1. Set a password.', '2. Password security.' (which is highlighted in blue), and '3. Modify IP address.'. Below the progress bar, there is a radio button labeled 'Email' which is selected. Underneath, the text 'Bind Email Address:' is followed by a dropdown menu that currently shows 'Reset Password'. At the bottom right of the window, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

ステップ6: 新規IPアドレス、サブネットマスク、ゲートウェイを入力し、**終了** (Finish) をクリックします。入力しないと、それら3つのパラメータがデフォルト値になります。

図 5-10 IPアドレスを変更する

The screenshot shows a window titled 'Modify IP address'. At the top, there is a progress bar with three steps: '1. Set a password.', '2. Password security.', and '3. Modify IP address.' (which is highlighted in blue). Below the progress bar, there are three rows of input fields. The first row is labeled 'New IP:' and has four input boxes. The second row is labeled 'Subnet Mask:' and has four input boxes. The third row is labeled 'Gateway:' and has four input boxes. At the bottom right of the window, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

5.4.3 IPアドレスの変更

リモートデバイスを初期化した後、初期化したデバイスのIPアドレスを変更することができます。

ステップ1: **デバイス** (Device Manager) ページ上で**自動検索** (Auto Search) をクリックします。

ステップ2: ネットワークセグメントの範囲を設定し、**検索** (Search) をクリックします。

ステップ3: 必要なデバイスを選択し、**IPを変更** (Modify IP) をクリックします。

ステップ4: デバイスのIPアドレス、サブネットマスクおよびゲートウェイを変更し、**OK**をクリックします。1台のデバイスのIPを変更したり、デバイスのIPを一括して変更したりすることができます。



- 一括して変更をする場合、新規IPは最上位のデバイスに割り当てられ、他のIPアドレスの数字が上位から下位まで1つずつ増えます。たとえば、デバイスを2台選択し、新規IPを192.168.1.10として設定すると、リスト内の一番上のデバイスのIPアドレスは192.168.1.10に変更され、その次のデバイスは192.168.1.11に変更されます。
- 一括して変更をする場合、サブネットマスクとゲートウェイは選択されたすべてのデバイスに割り当てられます。

図 5-11 1台のデバイスのIPを変更する

図 5-12 デバイスのIPを一括で変更する



Batch modify the device IP

5 Devices have been selected!

Start IP: *

SubMask: *

Gateway: *

OK Cancel

ステップ5: ログインユーザー名とパスワードを入力し、**OK**をクリックして確認します。




5.4.4 デバイス設定

一部のアクセス管理デバイスでは、時間設定、ファームウェアのアップグレード、デバイスの再起動、従業員の抽出、勤怠記録の抽出などの設定を行うことができます。

手順


ステップ1: **デバイス**(Device Manager) を選択し、をクリックします。

図 5-13 デバイスを設定する

<input type="checkbox"/> No.	Name ▲	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
<input type="checkbox"/> 1			Access Standalone		37777	0/0/22	Online		  

ステップ2: デバイスパラメータを設定します。

- 時間設定



10.31.94.18

IP Address: 10.31.94.18 SN: 80000000000000000000000000000000

Software Version: 3.0.0.0.R Device Type: The 2 Generation

System

Time Update Restarted Local Alarm Linkage

Data

Extract Personnel Extract Attendance Records

図 5-14 デバイスのIPを一括で変更する

The image shows a 'Time Settings' window with the following fields and options:

- Date Format: yyyy-MM-dd
- Time Format: 24-H
- Time Zone: GMT+08:00
- System Time: 2022-04-14, 10:55:24, with a 'Sync PC' button.
- ☐ DST Enable
 - Start Time: [dropdown], Last Wee, Thursday, 00:00
 - End Time: [dropdown], Last Wee, Thursday, 00:00
- ☐ NTP
 - NTP Server: 255.255.255.255
 - Port: 65535 (1-65535)
 - Update Period: 65535 Min(0-65535)
- Buttons: Save, Cancel

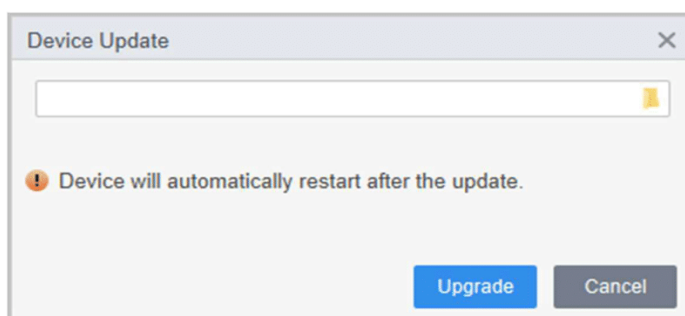
表 5-3 時間設定のパラメータ

パラメータ	説明
日付形式	日付表示形式。
時間形式	日付表示形式を設定。
タイムゾーン	タイムゾーンを設定。
システム時間	システム時間を設定します。 PC同期 (Sync PC) をクリックして、システム時間をPC時刻が同一になるように設定することもできます。
DST	必要に応じてDSTを有効化します。DSTの種類、開始時刻、終了時刻を設定します。

パラメータ	説明
NTP	システム時間がNTP時間と同一になるように同期する必要がある場合は、NTPサーバーを有効化します。サーバーアドレス、ポートおよび更新期間を入力します。

- ファームウェアのアップグレード
アップグレードファイル(.bin)を選択し、指示に従って操作します。

図 5-15 ファームウェアのアップグレード



- 再起動
クリックして、デバイスを再起動します。
- ローカルアラームのリンク
クリックしてアラームリンク情報を設定してから、**保存** (Save) をクリックします。

図 5-16 ローカルアラームのリンク

表 5-4 外部アラームのパラメータ

パラメータ	説明
アラーム入力	必要に応じてアラーム入力チャネル番号を選択します。
アラーム出力	必要に応じてアラーム出力チャネル番号を選択します。
出力遅延	設定した期間が経過すると、アラームが出力します。

パラメータ	説明
現在の設定を以下にコピー	必要に応じて現在の設定を他のデバイスにコピーすることができます。

- 人事情報を抽出する
必要な人員を選択し、デバイスからコンピュータに人事情報を抽出します。
- 勤怠記録を抽出する
手動で期間を設定し勤怠記録を抽出します。



抽出する前に、アクセスコントローラーを勤怠ポイントとして設定したことを確認してください。勤怠ポイントの設定の詳細については、*SmartPSS Lite_勤怠ソリューション_ユーザーマニュアル*をご覧ください。

関連操作

一部のデバイスでは、をクリックしてデバイスのWebクライアントに移動できます。

5.4.5 アラーム設定

ASC2202B-Dは、外部アラームデバイスに接続できます。**外部アラーム**（External Alarm）ページに移動し、パラメータを設定します。

図 5-17 外部アラーム

表 5-5 時間設定のパラメータ

パラメータ	説明
アラーム入力	必要に応じてアラーム入力チャンネル番号を選択します。
アラーム出力	必要に応じてアラーム出力チャンネル番号を選択します。
出力遅延	定義された期間が経過すると、アラームが遅れて発報します。
現在の設定を以下にコピー	必要に応じて現在の設定を他のデバイスにコピーすることができます。

6 ログの検索

アラームイベント、クライアントのログ、デバイスのログの問い合わせをすることができます。

ステップ1: **ログ** (Log Query) を選択します。

ステップ2: ログ種類とログ時刻を選択し、必要の場合はキーワードを入力します。

ステップ3: **検索** (Search) をクリックします。

ステップ4: (任意) **エクスポート** (Export) をクリックし、ログをローカルのデバイスにエクスポートします。

図 6-1 ログ検索

Log Type System Log	Export	No.	Time	User Name	Event Type	Device Name	Channel Name	Remarks
All		1	2020-04-30 19:04:03	2-2	User Login			
Time 04/30 00:00-04/30 23:59		2	2020-04-30 19:03:31	2-2	User Logout			
Key words:		3	2020-04-30 16:30:22	2-2	User Login			
Search		4	2020-04-30 16:30:06	1	User Login			
		5	2020-04-30 16:29:49	admin@1	User Login			
		6	2020-04-30 16:29:22	admin	User Logout			
		7	2020-04-30 16:22:51	admin	User Login			
		8	2020-04-30 16:21:47	admin	User Logout			
		9	2020-04-30 11:52:23	admin	User Login			
		10	2020-04-30 11:44:59	admin	User Logout			
		11	2020-04-30 11:33:08	admin	User Login			
		12	2020-04-30 09:49:06	admin	User Logout			
		13	2020-04-30 09:44:42	admin	User Login			


7 イベント設定

イベントを設定をすると、アラーム音やメール送信、アラームリンクなどのイベントリンクを設定することができます。

- アクセスコントローラ、カメラ、ストレージに接続されている外部アラームリンク（煙アラームなど）を設定します。
- デバイスによって対応するアラームリンクが異なるので、実際のページはデバイスごとに異なる場合があります。
- アクセスコントローライベントの連携を設定します。
 - ◇ アラームイベント
 - ◇ 異常イベント
 - ◇ 通常イベント

ステップ1: ホームページで**イベント設定** (Event Config) をクリックします。

ステップ2: 必要なデバイスを選択し、**アラームイベント** (Alarm Event) > **侵入イベント** (Intrusion Event) を選択します。

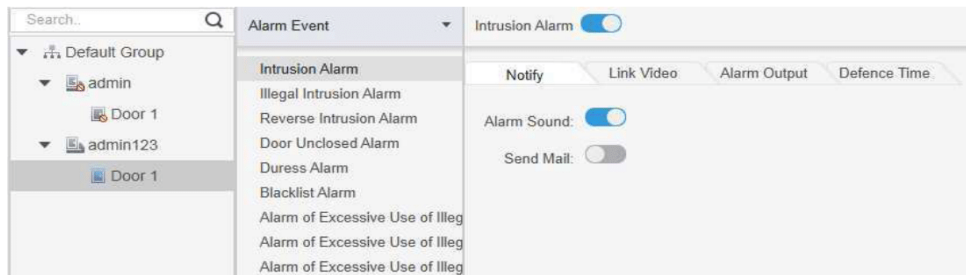
ステップ3: **侵入アラーム** (Intrusion Alarm) の右側にある  をクリックして機能を有効にします。

ステップ4: 侵入アラームのリンクアクションを設定します。

- アラーム音を有効にします。
- アラームメールを送信します。
 - 1) **メールの送信** (Send Mail) を有効にし、SMTPの設定を確定すると、自動的に**システム設定** (System Settings) ページに進みます。
 - 2) サーバーアドレス、ポート番号、暗号化モードなどのSMTPパラメータを設定します。

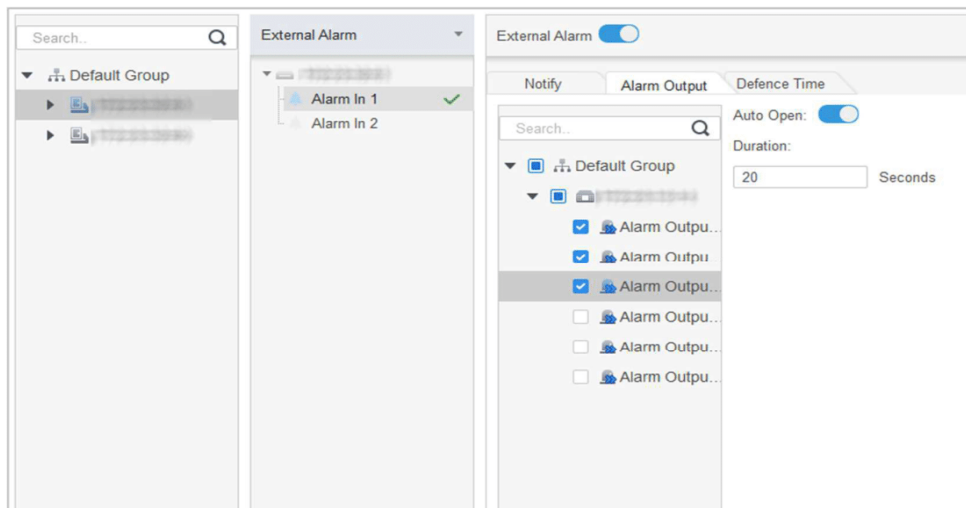
侵入イベントが発生すると、指定した受信者に自動的にアラームメールが送信されます。

図 7-1 侵入アラームの設定



- リンクビデオを設定します。
リンクビデオ (Link Video) をクリックし、必要に応じてビデオ レイアウトを選択します。侵入アラームがトリガーされると、自動的にページにビデオが表示されます。
- アラームI/Oを設定します。
 1. **アラーム出力** (Alarm Output) タブをクリックします。
 2. アラーム入力に対応するデバイスを選択し、アラーム入力チャンネルを選択し、**外部アラーム** (External Alarm) を有効にします。
 3. アラーム出力に対応するデバイスを選択し、アラーム出力ページを選択します。
 4. アラーム連動の**自動オープン** (Auto Open) を有効にします。
 5. 期間を設定します。

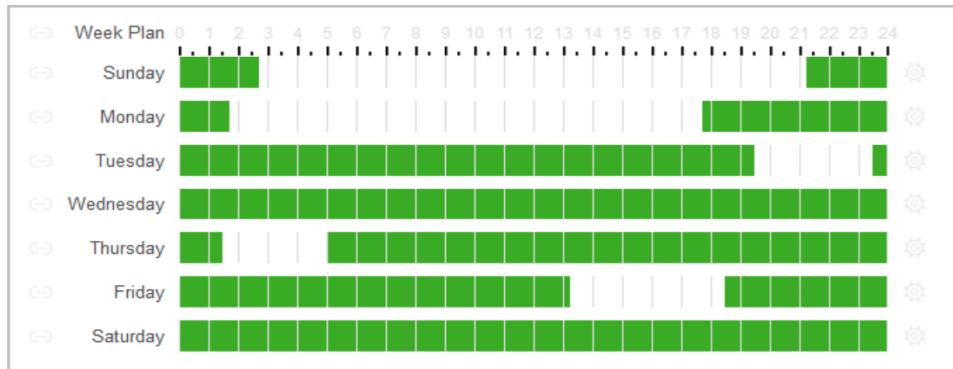
図 7-2 アラームリンクの設定



- 警戒期間を設定します。当該設定には、2つの方法があります。
 - ◇ 方法 1: カーソルを動かして期間を設定します。カーソルがペンシルに変化した場合、それをクリックすると期間がプラスになり、消しゴムに変化した場合、

それをクリックすると期間がマイナスになります。緑のエリアの期間は警戒中です。

図 7-3 警戒期間を設定する (方法1)




◇ 方法 2:  をクリックして期間を設定し、**OK**をクリックします。

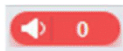
図 7-4 警戒期間を設定する (方法2)

ステップ5: (任意) **コピー先** (Copy To) をクリックして、適用するアクセスコントローラーを選択し、**OK**をクリックします。

ステップ6: **保存** (Save) をクリックします。

8 イベントセンター

リアルタイムでアラームイベントを表示して処理できます。ページの右上にある番号



をクリックすると、イベントセンターに進みます。

8.1 ページの紹介

図 8-1 イベントセンター

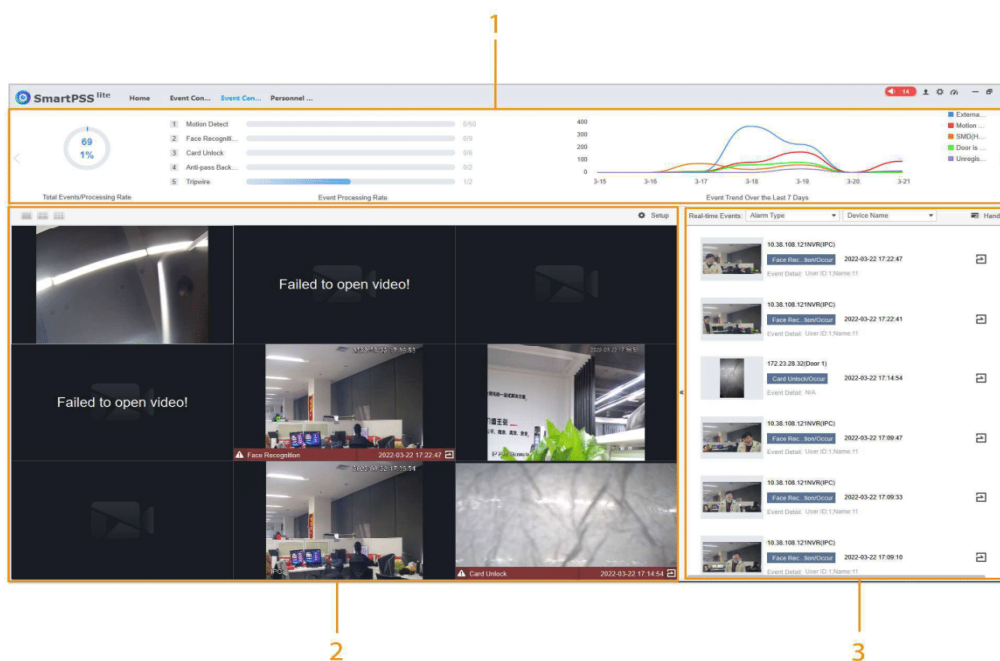







表8-1 イベントセンターパラメータの説明

番号	パラメータ	説明
1	イベント統計	<ul style="list-style-type: none"> • 合計イベント/処理速度 (Total Events/Processing Rate): 合計イベントと処理速度の円グラフを表示します。グラフをクリックすると、未処理のイベントの情報が表示されます。 • イベント処理率 (Event Processing Rate): 各種イベントタイプの処理率をリアルタイムで表示します。 • 過去7日間のイベント傾向 (Event Trend Over the Last 7 Days): 7日間 (今日を除く) の上位5つのイベントタイプのグラフを表示します。グラフにカーソルを合わせると、アラームイベントの指定数が表示されます。 <p>  をクリックすると、各アラームイベントの詳細が表示されます。</p>
2	ライブビュービデオ	設定されたチャンネルビデオをプレビューします。《 》をクリックしてプレビューページに移動します。
3	リアルタイムイベント	リアルタイムのアラームイベントを表示します。アラームのタイプやデバイスに応じて、イベント情報が検索できます。

8.2 ライブビュービデオの設定

ライブビュービデオチャンネルを設定し、チャンネルの画像、ビデオ、ビデオ通話をキャプチャします。

手順

ステップ1:    **イベントセンター** (Event Center) ページの画面番号をクリックして選択します。



1、4、9 画面分割のみをサポートします。

ステップ2: 画面を右クリックし、**ストリーム種別** (Stream Type) をクリックして、ライブビューしたいビデオチャンネルを選択します。

ステップ3: **セットアップ** (Setup) をクリックし、実際のニーズに応じて設定を選択します。

図 8-2 セットアップ

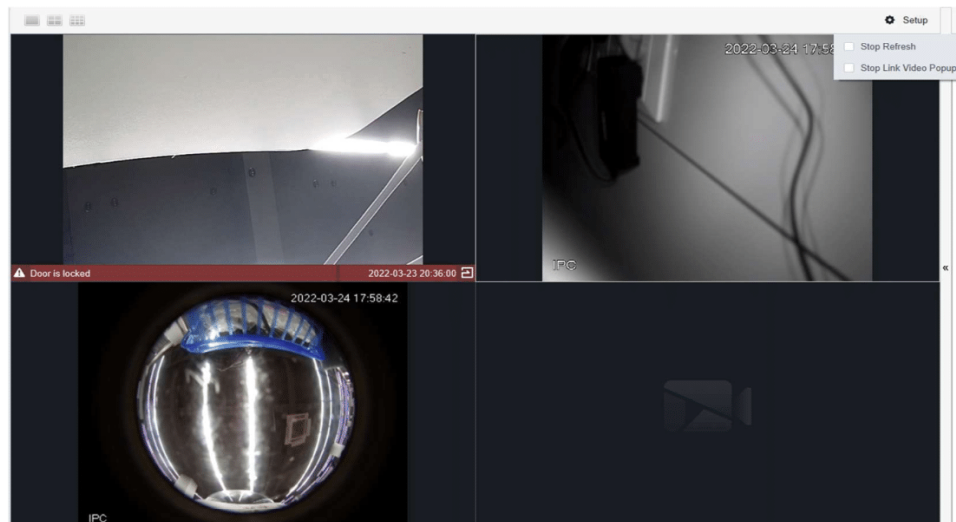


表 8-2 セットアップ












パラメータ	説明
リフレッシュ停止	リアルタイムアラームイベントの更新を停止します
リンクビデオポップアップ停止	イベントリンクビデオのポップアップを停止します。

関連操作

ライブビュービデオ操作。

画面にカーソルを合わせると、ウィンドウの右上にショートカットアイコンが表示されます。

表 8-3 ライブビュー操作パラメータの説明

アイコン	パラメータ	説明
	ローカル録画	このアイコンをクリックすると、現在の画面ウィンドウでビデオが録画されます。アイコンをもう一度クリックすると録画が停止し、ビデオがコンピュータに保存されます。デフォルトの保存パスは「.../Data/User/Record」です。ストレージパスは、  > システム (System Config) > ローカルパス (Local Path) > 録画パス (Record Path) で変更できます。
	訪問者の画像	コンピュータに、画像として、現在のビデオ画面のスナップショットが保存されます (一度に1回)。デフォルトの保存パスは「.../Data/User/Picture/Capture」です。ストレージパスは、  > システム (System Config) > ローカルパス (Local Path) > 画像パス (Pic Path) で変更できます。
	音声	このアイコンをクリックすると、カメラの音声が開閉します。
	音声通話	このアイコンをクリックすると、対応するカメラの音声通話が開閉します。
	インスタントリプレイ	アイコンをクリックすると、インスタントリプレイ機能が開閉します。ページの右上にある  > システム (System Config) > 基本設定 (Basic Setting) で、リプレイ時間を設定できます。  デバイスにビデオがなければ、インスタントリプレイ機能を有効にすることはできません。
	拡大	アイコンをクリックし、マウスホイールをスクロールして画面を拡大または縮小します。
	ビデオの終了	このアイコンをクリックするとビデオが閉じます。

付録 1 サイバーセキュリティに関する推奨

プラットフォームの基本的なサイバーセキュリティを確保するために必要な措置:

1. 強力なパスワードの使用

パスワードを設定するには、次の推奨事項を参照してください:

- 長さは 8 文字以下にする必要があります。
- 少なくとも 2 つのタイプの文字を含めます。文字タイプには大文字と小文字があります、数字と記号。
- アカウント名またはアカウント名を逆順に含めないでください。
- 123 や abc などの連続文字は使用しないでください。
- 111、aaa などの重複文字は使用しないでください。

2. セキュリティに関する質問への回答のカスタマイズ

.....セキュリティ質問の設定は、回答の違いを確認し、異なる回答を選択する必要があります

.....質問と異なる回答をカスタマイズする（すべての質問を設定することは禁止されています）

.....（同じ回答）は、セキュリティ問題が推測またはクラックされるリスクを軽減するためのものです。

.....プラットフォームのサイバーセキュリティを強化するための推奨措置:

1. アカウント バインディング IP/MAC をイネーブルにする

.....アカウント バインディング IP/MAC メカニズムをイネーブルにし

.....一般的に使用されるクライアントがある端末の IP/MAC を許可リストとして追加します

.....アクセスのセキュリティを向上させる。

2. 定期的にパスワードを変更する

.....推測やクラックのリスクを減らすために、定期的にパスワードを変更することをお勧めします。

3. アカウントロックメカニズムのオン

.....アカウントロック機能は工場出荷時にデフォルトで有効になっているため、この機能を維持することをお勧めします

.....アカウントのセキュリティを保護するためです。攻撃者が複数のパスワードに失敗した場合

.....を試みると、対応するアカウントと送信元 IP がロックされます。

4. 合理的なアカウントと権限の割り当て

.....ビジネスや管理のニーズに応じて、新規ユーザーを合理的に追加し、合理的に

.....それらに最低限の権限を割り当てます。

5. 重要でないサービスを閉鎖し、重要なサービスのオープンな形態を制限する

必要がない場合は、NetB をオフにすることをお勧めしますIOS（ポート 137、138、139）、SMB（ポート 445）、リモート デスクトップ（ポート 3389）および Windows でのその他のサービス、および Telnet（ポート 23）および SSH（ポート 22）Linux の場合。同時に、データベース ポートを Outside に対して閉じるか、または に対してだけ開くようにしますMySQL（ポート 3306）などの特定の IP アドレスを使用して、プラットフォームが直面するリスクを軽減します。

6. OS/サードパーティ製コンポーネントのパッチ適用

オペレーティング システムおよびサードパーティ コンポーネントのセキュリティ上の脆弱性を定期的に検出し、

.....シリアルパッチを時間内に適用することを推奨します。

7. セキュリティ 監査

● オンラインユーザーをチェック: オンラインユーザーを定期的にチェックして、確認することをお勧めします不正なユーザーがログインしています。

● プラットフォーム ログの表示:ログを表示することにより、次の操作を試行したときの IP 情報を取得できますプラットフォームにログインし、ログインしたユーザのキー操作情報を表示します。

8. 安全なネットワーク環境の確立

プラットフォームのセキュリティをより保護し、サイバーセキュリティリスクを低減するために推奨事項:

● 最小化の原則に従い、プラットフォームが外部マッピングするポートを制限します

ファイアウォールまたはルータ、およびサービスに必要なマップ ポートのみ

● 実際のネットワーク要件に基づいて、個別のネットワーク通信がない場合

.....2 つのサブネット間の要件を満たすには、VLAN、ゲートキーパーなどを使用することを推奨します

.....ネットワーク分離の効果を得るためにネットワークを分割する