

D-Link Central Wi-Fi Manager/CWM-100

WLAN Management System

ユーザマニュアル



安全にお使いいただくために

本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。また、必ず本書をよくお読みいただき、内容をご理解いただいた上で、記載事項にしたがってご使用ください。

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用前にご確認ください。
<http://www.dlink-jp.com/>

目次

はじめに	5
本マニュアルの対象者	6
表記規則について	6
第 1 章 本製品のご利用にあたって	7
概要	7
動作環境	7
サポートするアクセスポイント	7
第 2 章 初期設定ガイド	8
インストールと初期設定	8
Central Wi-Fi Manager のインストール	8
AP モジュールのインストール	12
CWM サーバの起動	13
Central Wi-Fi Manager の起動とログイン	14
AP モジュールの確認	15
サイト / ネットワークの作成、SSID 設定	15
新しい AP の追加 (AP installation utility for CWM)	18
設定の適用	22
AP への設定適用 (コンフィグアップロード)	22
キャプティブポータルとユーザ認証	23
キャプティブポータル設定	23
ローカルデータベース認証	24
パスコード認証	25
帯域最適化	29
帯域最適化設定	29
リモート AP の追加	30
ネットワーク機器設定	30
サイト / ネットワークの作成 (リモート AP)	30
ネットワークプロファイルのエクスポート / インポート (リモート AP)	31
Wi-Fi 設定変更	33
第 3 章 Home (ホーム)	34
Dashboard (ダッシュボード)	34
Site (サイト)	35
Device View (デバイスビュータブ)	35
Topology View (トポロジビュータブ)	36
第 4 章 Configuration (コンフィグレーション)	37
Site (サイト)	37
サイト一覧	37
サイト作成	38
サイトの表示について	38
Network (ネットワーク)	39
ネットワーク一覧	39
ネットワーク作成	40
Network の設定 / 編集	41
SSID	41
SSID 作成 / 編集	41
VLAN	60
Bandwidth Optimization (帯域最適化)	62
RF optimization (無線周波数最適化)	63
Schedule (スケジュール)	64
Device Settings (デバイス設定)	65
Performance (パフォーマンス設定)	66
WLAN Partition (無線 LAN パーティション)	68
Wireless Resource (無線リソース)	69
SSL certificate (SSL 認証)	70
Upload Configuration (コンフィグアップロード)	71
Firmware Upgrade (ファームウェア更新)	72
Undefined AP (未定義 AP)	73

第 5 章 System (システム)	74
Settings (システム設定)	74
General タブ (一般設定)	74
Module タブ (モジュール設定)	75
Database タブ (データベース設定)	76
SMTP (SMTP 設定)	77
Payment (Payment 設定)	78
User Manager (ユーザ管理)	79
ユーザアカウント作成	79
第 6 章 Monitor (モニタ)	80
Report (レポート)	80
Association (関連機器)	80
Security (セキュリティ)	83
Channel (チャネル)	85
Rogue AP (不正アクセスポイント)	86
SysLog (シスログ)	90
Captive portal log (キャプティブポータルログ)	90
Monitor (監視)	91
Monitor Manager (モニタ管理)	91
Monitor List (モニタリスト)	92
Event (イベント)	94
Type (各種イベント)	94
Condition (コンディション)	100
【付録 A】 フロントデスクユーザアカウントの作成	103
【付録 B】 キャプティブポータルログインページのカスタマイズ	109

はじめに

本ユーザマニュアルは、本製品のインストールおよび操作方法を例題と共に記述しています。

第1章 [本製品のご使用にあたって](#)

- 製品の概要とその機能について説明します。本製品の動作環境、サポートするアクセスポイントについて説明します。

第2章 [初期設定ガイド](#)

- 本製品のインストール、基本的な機能とその設定について説明します。

第3章 [Home（ホーム）](#)

- 本項目では「Central Wi-Fi Manager」の項目「Home」の説明をします。

第4章 [Configuration（コンフィグレーション）](#)

- 本項目では「Central Wi-Fi Manager」の項目「Configuration」の説明をします。

第5章 [System（システム）](#)

- 本項目では「Central Wi-Fi Manager」の項目「System」の説明をします。

第6章 [Monitor（モニタ）](#)

- 本項目では「Central Wi-Fi Manager」の項目「Monitor」の説明をします。

【付録A】 [フロントデスクユーザアカウントの作成](#)

- フロントデスクユーザアカウントの作成、設定について説明しています。

【付録B】 [キャプティブポータルログインページのカスタマイズ](#)

- キャプティブポータルログインページのカスタマイズについて説明しています。

本マニュアルの対象者

本マニュアルは、本製品の操作方法についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者、システム管理者、または IT 技術者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体・記号についての表記規則を表します。

表 1 字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に " (13 ページ) をご参照ください。

第1章 本製品のご利用にあたって

- 概要
- 動作環境
- サポートするアクセスポイント

概要

「Central Wi-Fi Manager」は D-Link 無線アクセスポイント管理用の最新ソフトウェアツール（無償）です。ネットワーク上にあるアクセスポイントの監視や管理を一元的に行うことができます。「Central Wi-Fi Manager」により、既存ネットワークで発生する無線トラフィックの様々なボトルネックを、シンプルに解消することができます。

注意 CWM では一部の特殊文字 ("&\) はサポート対象外となります。

動作環境

本製品の動作には、以下の条件以上の環境が必要です。

ハードウェア要件(1000AP/100AP 管理時)		
管理 AP 数	1000AP 管理時	100AP 管理時
データベース	PostgreSQL v9.1.0	PostgreSQL v9.1.0
CPU	Intel Core i5 3.2GHz	Intel Core i3 3.5GHz
メモリ	4GB DDR3	2GB DDR2
ハードディスク容量	2TB 以上	1TB 以上
グラフィックボード	DirectX 11 1GB	DirectX 11 1GB
ソフトウェア要件		
管理 AP 数	1000AP 管理時	100AP 管理時
OS	Windows Server 2008 R2 SP2 (64bit) Windows Server 2012 R2 (64bit)	Windows7 Pro/Ultimate/Enterprise Edition (32bit/64bit) Windows10 Pro (32bit/64bit) Windows Server 2008 R2 SP2 (64bit) Windows Server 2012 R2 (64bit)

サポートするアクセスポイント

本製品は、以下のアクセスポイントに対応しています。

アクセスポイント名	対応ハードウェアバージョン	対応ファームウェアバージョン
DAP-2610	A1	R1.01xx
DAP-2660	A1	R1.15xx
DAP-3662	A1	R1.05xx

注意 最新のバージョンまたは各アクセスポイントの対応モジュールについては、弊社ホームページで各製品のファームウェア情報をご確認ください。

第 2 章 初期設定ガイド

- インストールと初期設定
- 設定の適用
- キャプティブポータルとユーザ認証
- 帯域最適化
- リモート AP の追加
- Wi-Fi 設定変更

インストールと初期設定

「Central Wi-Fi Manager」は D-Link 無線アクセスポイント管理用の最新ソフトウェアツール（無償）です。ネットワーク上にあるアクセスポイントの監視や管理を一元的に行うことができます。「Central Wi-Fi Manager」により、既存ネットワークで発生する無線トラフィックの様々なボトルネックを、シンプルに解消することができます。

Central Wi-Fi Manager のインストール

取得した「Central Wi-Fi Manager」のアプリケーションファイルを起動します。使用言語を選択する次の画面が表示されます。

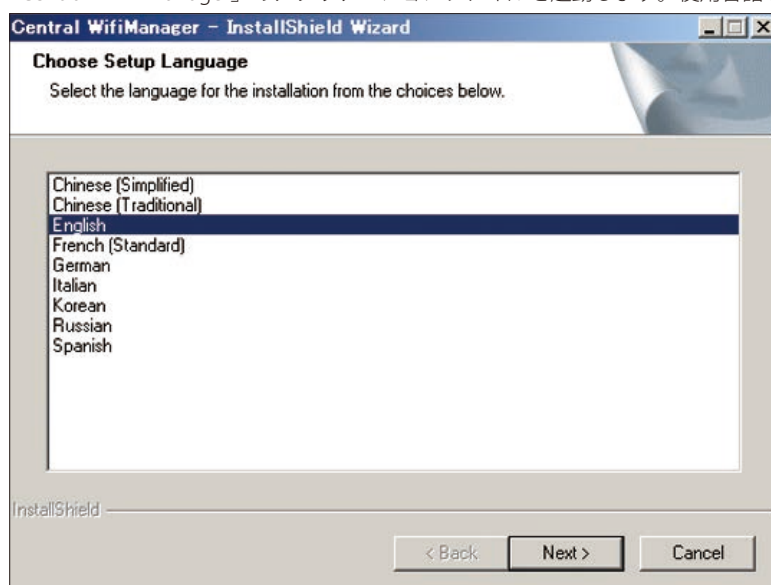


図 2-1 使用言語の選択

「Next」をクリックし、インストールプロセスを開始します。「Cancel」をクリックするとインストールを中止します。

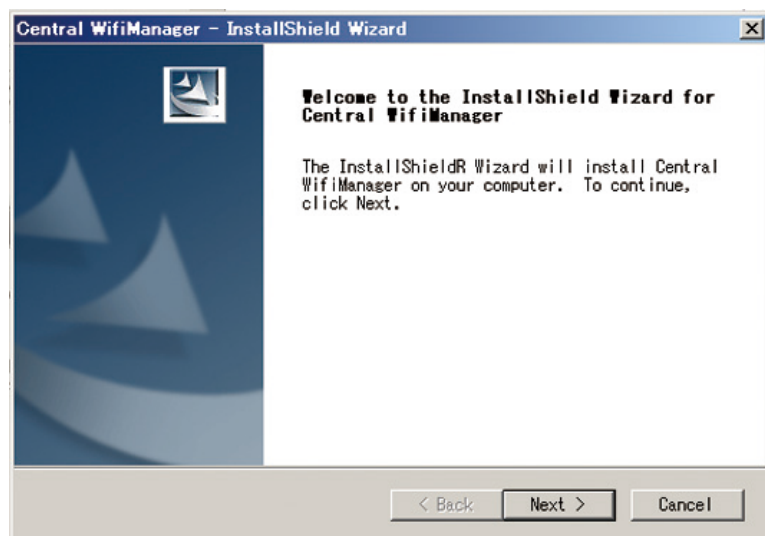


図 2-2 Central Wi-Fi Manager の起動

以下の画面では、ソフトウェアがインストールされるディレクトリパスが表示されます。アプリケーションを異なるディレクトリやドライブにインストールする場合は、「Browse」（参照）をクリックし、別のディレクトリパスを指定してください。

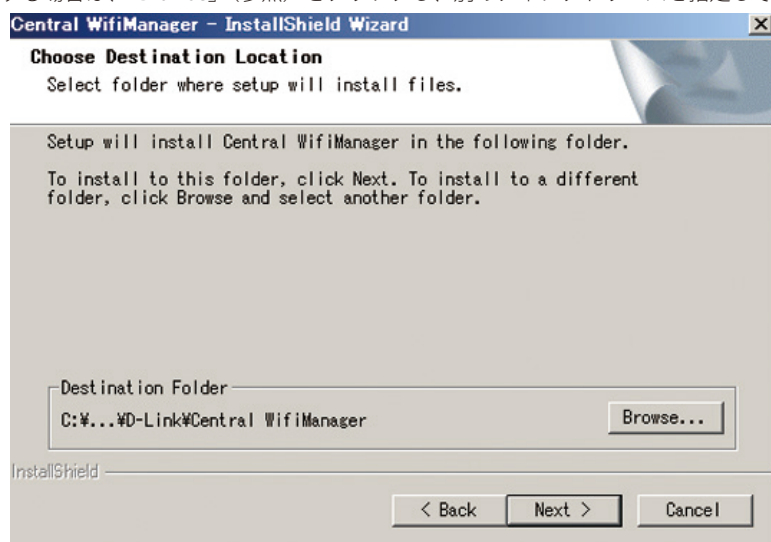


図 2-3 インストール箇所の指定

「Back」をクリックして前の手順へ戻ることも可能です。「Cancel」をクリックするとインストールを中止します。

以下の画面では「Manager Port」「Listen Port」「Service Port」のポート番号を変更することができます。これらのポート番号は複数のアクセスポイント接続で使用され、本設定でのみ構成することができます。インストール後に変更することはできません。コンピュータ上でこれらのポートを使用しない場合は、初期設定（デフォルト値）のままにします。

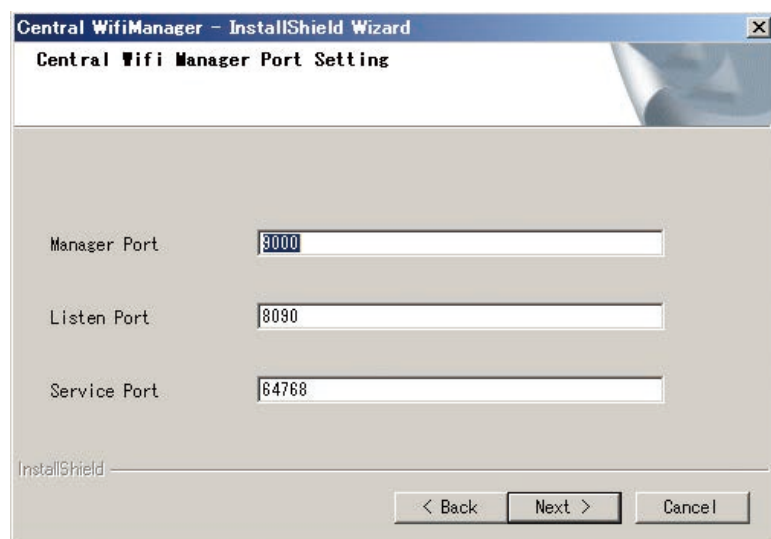


図 2-4 Port Settings

前の画面に戻るには「Back」、次の画面に進むには「Next」をクリックします。インストールを中断しウィザードを終了するには、「Cancel」をクリックします。

以下の画面では「Apache Server Service Port」を指定します。

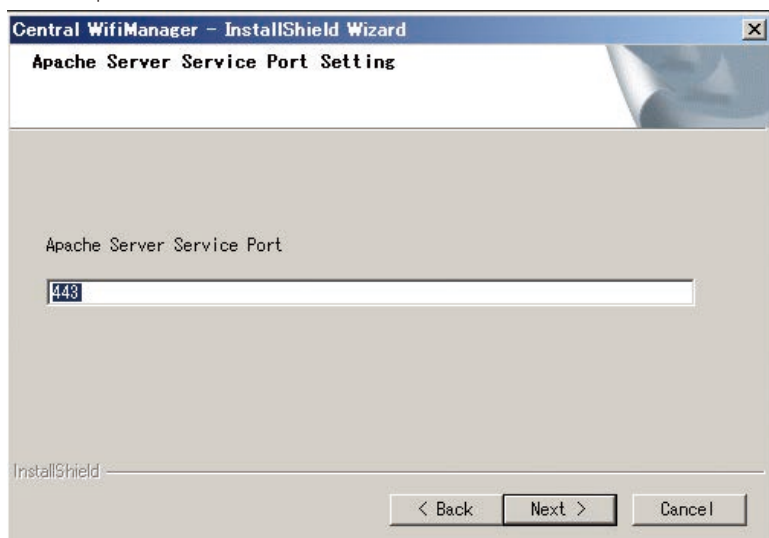


図 2-5 Apache Server Service Port Setting

以下の画面では、「Central Wi-Fi Manager Server」に Central Wi-Fi Manager の IP アドレスを入力します。通常はインストールで使用する PC の IP アドレスです。この IP アドレスは後で変更することが可能です。

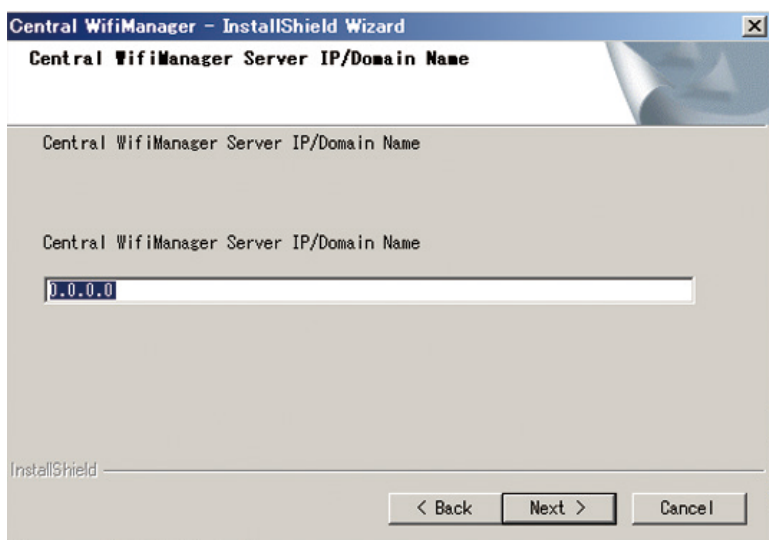


図 2-6 Server IP

前の画面に戻るには「Back」、次の画面に進むには「Next」をクリックします。
インストールを中断しウィザードを終了するには、「Cancel」をクリックします。

以下の画面では、本アプリケーションで利用する PostgreSQL データベースのパスワードを入力します。「Password」と「Retype password」には同じパスワードを入力してください。このパスワードは後で変更することができません。

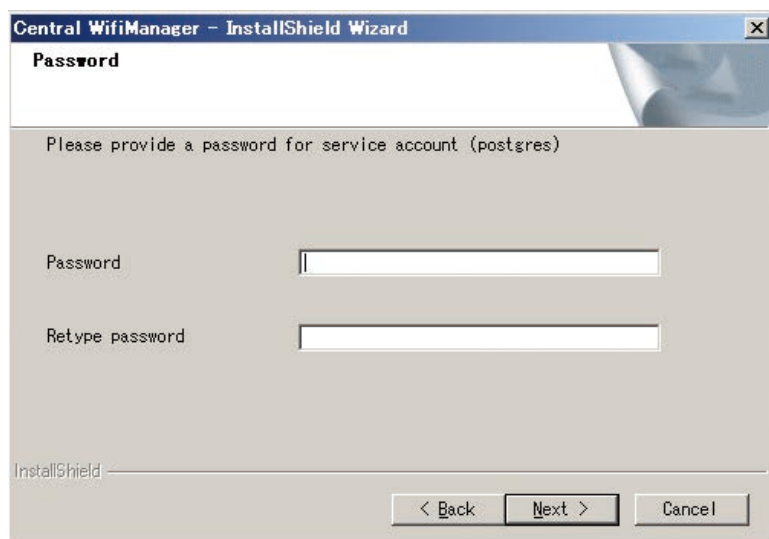


図 2-7 Password

前の画面に戻るには「Back」、次の画面に進むには「Next」をクリックします。インストールを中断しウィザードを終了するには、「Cancel」をクリックします。

本アプリケーションのインストールには、コンピュータ上に Microsoft Visual C++ 2008 Redistributable（再頒布可能パッケージ）がインストールされている必要があります。再頒布可能パッケージが見つからない場合、必要な再頒布可能パッケージをインストールするようにオプションが提示されます。再頒布可能パッケージが存在する場合、この手順はスキップされます。

Apache HTTP サーバアプリケーションは、コンピュータのファイアウォールによってブロックされる場合があります。Windows のデフォルトのファイアウォールが設定されている場合、セキュリティ警告メッセージが表示されます。「Allow Access」（アクセス許可）をクリックし、本アプリケーションのネットワーク通信を許可してください。以下の画面では、Central Wi-Fi Manager のインストールとは別に、本アプリケーションで利用されるアクセスポイント毎に異なるモジュールのインストールが必要となる旨のメッセージが表示されます。この内容は次項で説明します。

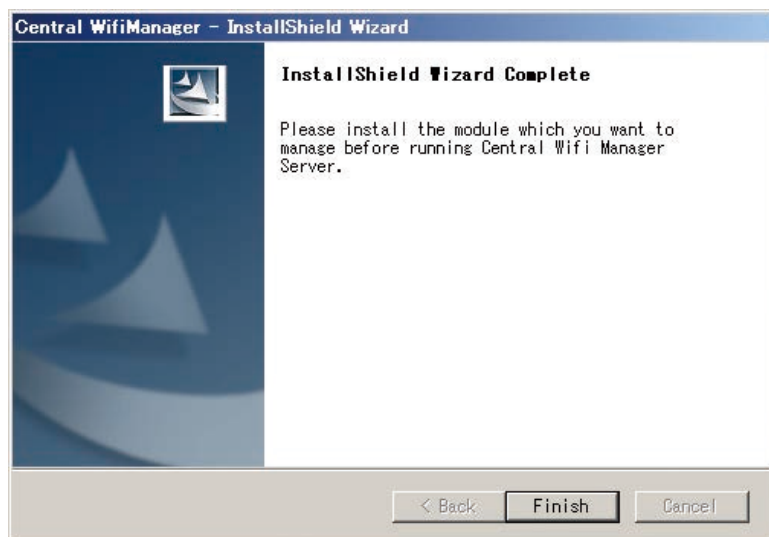


図 2-8 Finish

「Finish」をクリックし、インストールウィザードを終了します。

インストールが完了すると、「Central Wi-Fi Manager Server」と「Central Wi-Fi Manager」と呼ばれる2つのアプリケーションがPC上にインストールされます。

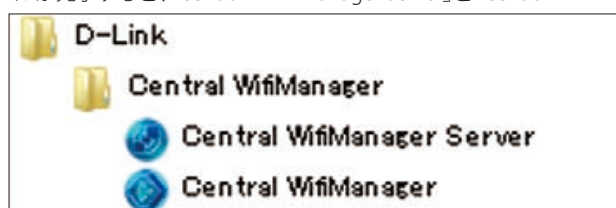


図 2-9 Central Wi-Fi Manager Files

AP モジュールのインストール

D-Link Central Wi-Fi Manager で使用する各アクセスポイントに対し、追加の管理モジュールをインストールする必要があります。本節では、D-Link Central Wi-Fi Manager で使用される、「DAP-2690」用のアクセスポイント管理モジュール（AP モジュール）をインストールする手順について説明します。Central Wi-Fi Manager サーバが既に実行中の場合は、「AP モジュール」をインストールする前に停止して閉じてください。

AP モジュールを実行すると、ウェルカムメッセージが表示され、コンピュータ上に管理モジュールがインストールされる旨のメッセージを表示します。

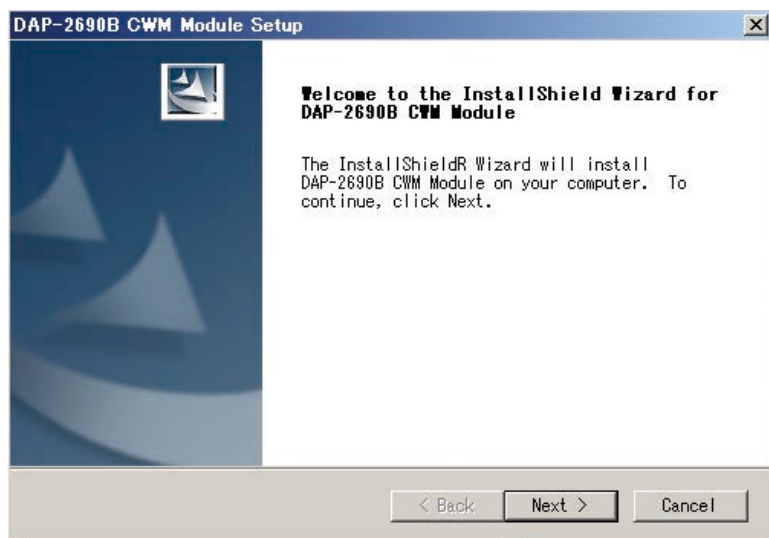


図 2-10 Install Access Point Module

「Next」をクリックして次に進みます。インストールを中断しウィザードを終了するには、「Cancel」をクリックします。AP モジュールが正常にインストールされると、以下の画面が表示されます。

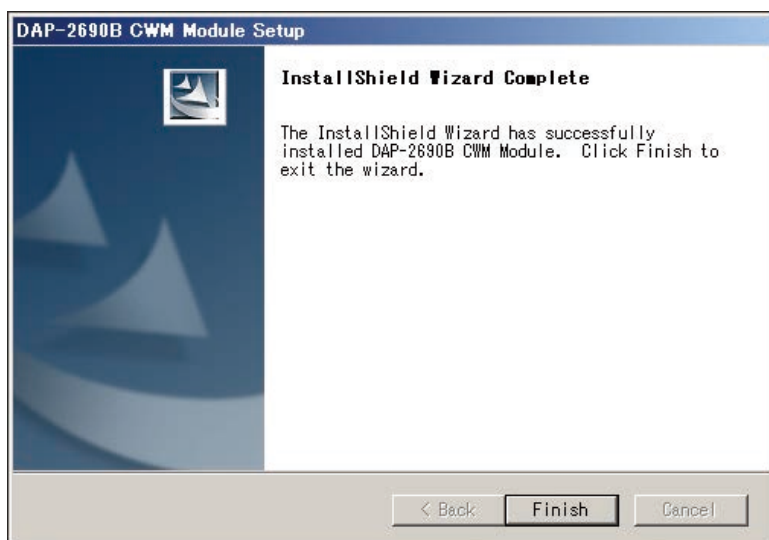


図 2-11 Install Access Point Module_Finish

「Finish」をクリックし、インストールを終了します。

CWM サーバの起動

本節では、Central Wi-Fi Manager Server アプリケーションについて説明します。インストールが完了すると、本アプリケーションが利用できるようになります。



Central WifiManager Server オプションをクリックし、サーバアプリケーションを開きます。

Central Wi-Fi Manager Server アプリケーションが実行されると、サーバアプリケーションの管理コンソール画面が表示されます。

メニューバーでは、「Server」と「Help」の2つのオプションが利用可能です。「Server」メニューからアプリケーションを「Start」（開始）、「Stop」（停止）、「Exit」（終了）することができます。もしくは、「Server」メニューオプションの下にある開始・停止アイコンを利用することもできます。「Help」メニューのオプションでは、「About」オプションをクリックしてアプリケーションの名前、バージョン、著作権の詳細を表示することができます。「Setting」セクションでは、「Automatically open configuration window when Windows start up（Windows 起動時に自動的に設定画面を開く）」と「Automatically start server when configuration window is open（設定画面が開いたときに自動的にサーバを起動する）」を選択することができます。「▶」アイコンをクリックし、サーバを起動します。

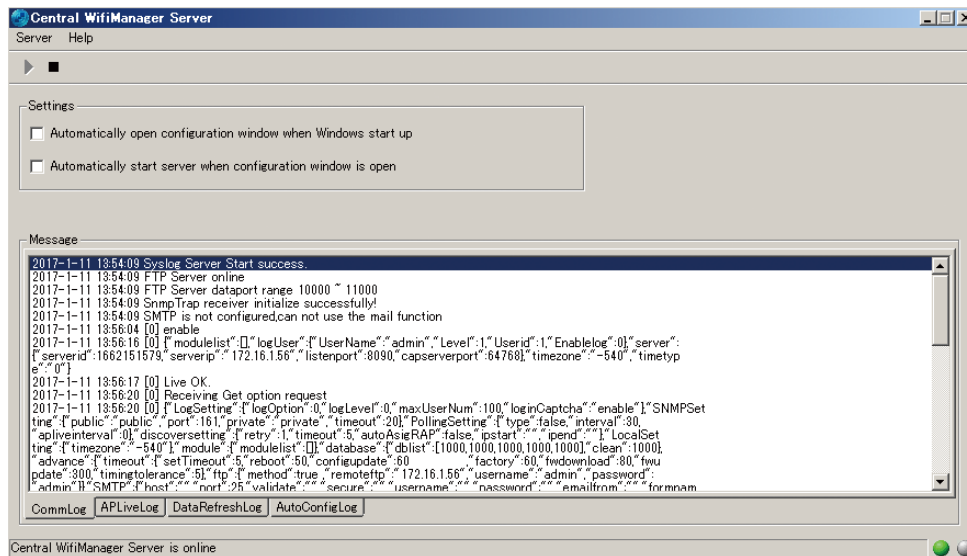


図 2-12 CWM Management Console

画面右上の閉じるアイコン（）をクリックすると、アプリケーションが終了し、画面が閉じます。サーバはバックグラウンドで実行されません。

最小化アイコン（）をクリックすると、画面は閉じますがバックグラウンドでサーバアプリケーションが実行されたままとなります。

サーバが起動し実行状態になると、画面右下の左側の丸いアイコン（）が緑色に表示されます。サーバが実行されていない時は、画面右下の右側の丸いアイコン（）が赤色に表示されます。

「Message」セクションの下タブを選択すると、「システム」「FTP 通信」「ライブアクセスポイント」「データ伝送」「自動構成に関するログエントリ」を見ることができます。

Central Wi-Fi Manager の起動とログイン

本項目では「Central Wi-Fi Manager」のクライアントアプリケーションの起動とログインについて説明します。インストールが完了すると、次のアプリケーションが有効となります。本章以降、起動後の「Central Wi-Fi Manager」の各項目について説明していきます。



図 2-13 アプリケーション選択（Windows 項目）

「Central Wi-Fi Manager」オプションをクリックしてクライアントアプリケーションを開きます。

「Central Wi-Fi Manager」では「Central Wi-Fi Manager Server」の接続に安全な HTTPS を使用します。まず Web ブラウザを開き、同じ PC 自体の IP アドレスに接続するローカルな方法である「localhost」に接続します。



図 2-14 Localhost 画面

リモートコンピュータからは、Web ブラウザにインストールされたサーバアプリケーションを持つコンピュータの IP アドレスを入力することにより「Central Wi-Fi Manager Server」に接続できるため、リモートコンピュータにソフトウェアをインストールする必要はありません。リモートコンピュータの上の Web ブラウザ (Internet Explorer または Google Chrome を推奨) を開き、Web ブラウザのアドレスバーに、例えば「https://192.168.10.1」または「https://domain-name.com」（192.168.10.1 または domain-name.com は IP アドレスまたは CWM サーバが稼働しているコンピュータのドメイン名）を入力し「ENTER」をクリックし CWM 管理インターフェースに入ります。

注意 「Central Wi-Fi Manager Server」への接続は、安全な HTTPS を使用します。

Web ブラウザを開きサーバへの接続した後、ログイン画面が表示されます。ログインユーザ名とパスワード、「CAPTCHA」を入力し、「Login」をクリックして「Central Wi-Fi Manager Configuration」に入ります。

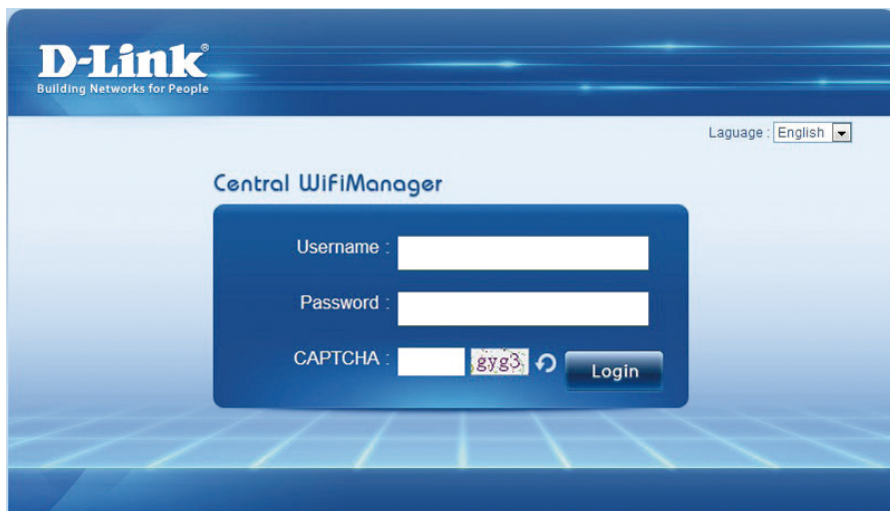


図 2-15 ログイン画面

注意 ユーザ名とパスワードの初期値はどちらも「admin」です。

注意 CWM では一部の特殊文字 ("&" "\") はサポート対象外となります。

初期値の言語は英語で、イタリア語、フランス語、スペイン語、ドイツ語、韓国語、ロシア語、繁体字中国語、簡体字中国語の使用が可能です。

リモートでのログイン

リモートコンピュータの Web ブラウザから、サーバアプリケーションがインストールされているコンピュータの IP アドレスもしくはドメイン名を入力して、「Central Wi-Fi Manager サーバ」へ接続することも可能です。リモートコンピュータにソフトウェアをインストールする必要はありません。リモートコンピュータ上で Web ブラウザを開き（Internet Explorer や Google Chrome が推奨されます）、Web ブラウザのアドレスバーに、「https://192.168.10.1」もしくは「https://domain-name.com」など（CWM サーバが実行されているコンピュータの IP アドレスもしくはドメイン名）を入力の上、Enter キーを押下し、CWM の管理インタフェースに接続します。

AP モジュールの確認

D-Link Central Wi-Fi Manager にログインした後、画面上部の「System」をクリック、「**System > Settings**」になっていることを確認し、ページ上部中央の「Module」タブオプションを選択して以下の画面を開きます。

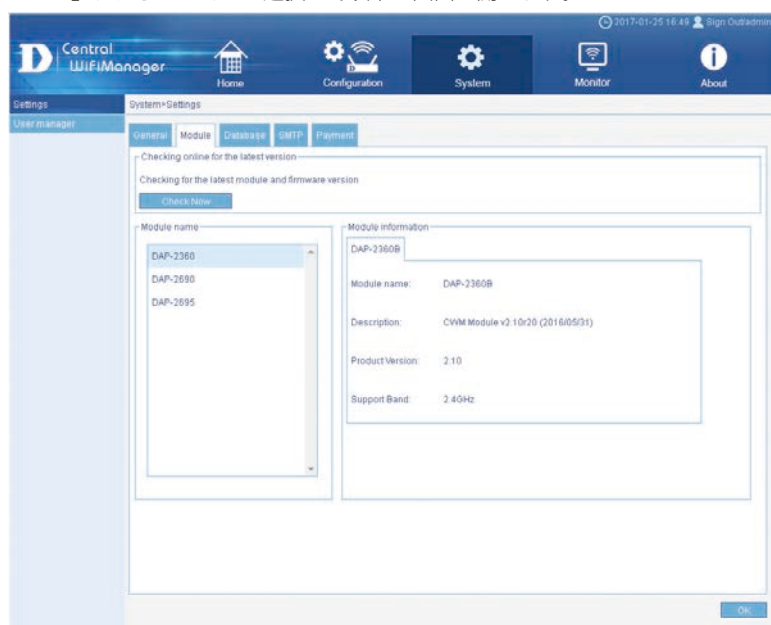


図 2-16 Update AP Module

「Module」タブでは、「Module Name」セクションにアクセスポイントの一覧が表示されます。Central Wi-Fi Manager サーバ管理下のアクセスポイントについて、すべての異なるモデル毎に、管理者による実行モジュールファイルのインストールが必要となります。

ネットワーク上にアクセスポイントが複数存在する場合、アクセスポイントの種類別にモジュールをインストールする必要があります。アクセスポイントのインストールモジュールとファームウェアバージョンを最新の状態に保つためには、弊社のホームページでファームウェアの最新情報をご確認いただき、必要に応じてアップグレードを行ってください。

サイト / ネットワークの作成、SSID 設定

新しいサイト（Site）を作成するには、「Configuration」を選択し、 ボタンをクリックします。マルチテナント用に複数のサイトを作成することができます。

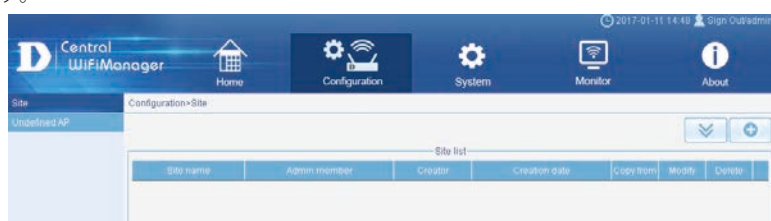


図 2-17 New Site

新しいネットワーク（Network）作成するには、新しく作成したサイトを選択し、 ボタンをクリックします。各サイトに対し、複数のネットワークを作成することができます。

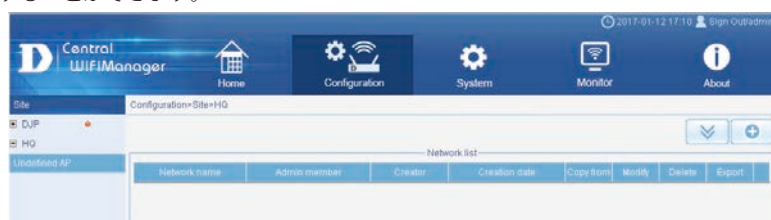


図 2-18 New Network

第2章 初期設定ガイド

新しいネットワークを作成した後、作成したネットワークを選択します。追加の情報が表示されます。各ネットワークに対し、「SSID」、「VLAN」、「Bandwidth Optimization」、「RF Optimization」、「Device Settings」などの追加の設定を行うことができます。

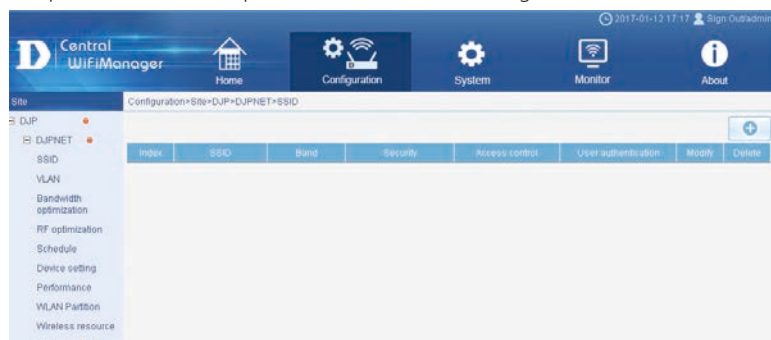


図 2-19 Network Configuration Options

新しく 5GHz の「SSID」を作成するには、新しく作成したネットワークを選択し、 ボタンをクリックします。表示される「Wireless settings」「Access control」「User authentication」などの各設定項目を指定します。設定を適用するには「Save」をクリックします。

The screenshot shows the 'New SSID (5G)' configuration page. The breadcrumb trail is 'Configuration > Site > DUP > DUPNET > SSID'. The page is divided into several sections: 'Basic settings' (Wireless settings, WPA settings), 'Access control', and 'User authentication'. The 'Wireless settings' section includes fields for Band (5G), Index (Primary), SSID, Character set (UTF-8), SSID broadcast (Enable), WMM (Wi-Fi Multimedia) (Enable), and Security (Open System). The 'WPA settings' section includes fields for Encryption (Disable), Key size (64 Bits), Key type (HEX), Key index (1), and Key value. The 'Access control' section includes a MAC address field, an 'Add' button, an 'Action' dropdown (Disable), and an 'Upload MAC address list' button. Below this is a table with columns for 'No.', 'MAC address', and 'Delete'. The 'User authentication' section includes an 'Authentication type' dropdown (Disable). At the bottom right, there are 'Save' and 'Back' buttons.

図 2-20 New SSID (5G)



CWM では一部の特殊文字 ("&" "\") はサポート対象外となります。

新しく 2.4GHz の「SSID」を作成するには、新しく作成したネットワークを選択し、 ボタンをクリックします。表示される「Wireless settings」「Access control」「User authentication」などの各設定項目を指定します。設定を適用するには「Save」をクリックします。

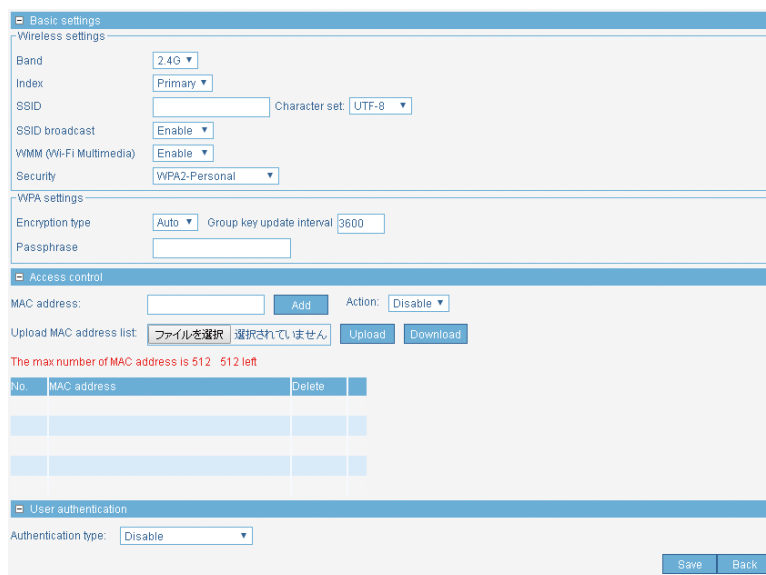
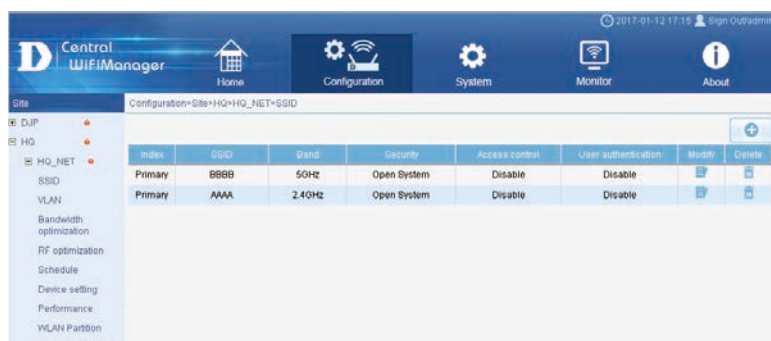


図 2-21 New SSID (2.4G)



Index	SSID	Band	Security	Access control	User authentication	Modify	Delete
Primary	BBBB	5GHz	Open System	Disable	Disable		
Primary	AAAA	2.4GHz	Open System	Disable	Disable		

図 2-22 Network' s SSID List

ここまでの設定は、ネットワークのアクセスポイントにアップロードされていない状態であるため、「Network」と「Site」の名前の右に赤い丸アイコン  が表示されます。

CWM に新しいアクセスポイントを追加する場合、まず、CWM の「AP installation utility for CWM」(AP installation utility for CWM) を実行する必要があります。CWM とアクセスポイントとの最初の同期 (CWM サーバの IP アドレスと認証情報) を行うためです。アクセスポイントが CWM に同期されると、CWM の「Uploading Configuration」オプションを利用して、リモートのアクセスポイントに対し、設定の新規構成や修正情報をプッシュすることが可能になります。

注意 以後、作成した固有のサイトは **(Site)**、ネットワークは **(Network)** と表記します。

次項では、これらのオプションについて詳細を説明します。

新しい AP の追加 (AP installation utility for CWM)

ネットワークプロファイルのエクスポート

CWM に新しいアクセスポイントを追加するには、「AP installation utility for CWM」というツールを使用します。「AP installation utility for CWM」は CWM からダウンロードすることが可能です。「AP installation utility for CWM」の起動前にまず CWM からネットワークプロファイルをエクスポートし、エクスポートファイルにはコントローラの認証キーと IP アドレスが含まれています。「Configuration」で作成したサイトを選択し、「Export」アイコンをクリックしてネットワークプロファイルをコンピュータ上にエクスポートします。



図 2-23 Export Network Profile

「Access Address」を確認するには、**System > General > Connection Settings** から「Access Address」欄を再確認してください。

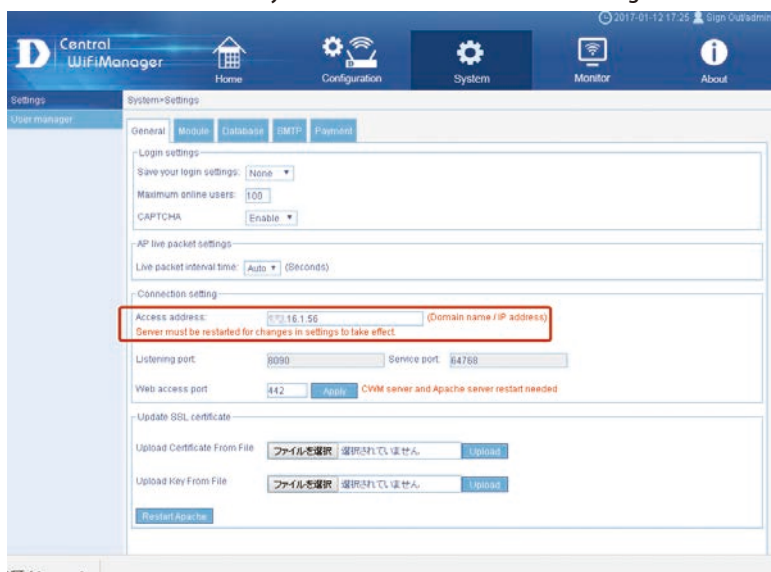


図 2-24 Modify Access Address

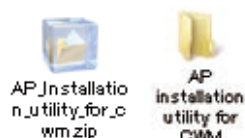
AP installation utility for CWM のインストール

AP installation utility for CWM のダウンロード、インストールを行うには **Configuration > (Site)** で「」をクリックします。



図 2-25 AP installation utility for CWM のダウンロード

「AP_Installation_utility_for_cwm.zip」がダウンロードされます。解凍すると「AP installation utility for CWM」フォルダが表示されます。



AP installation utility for CWM のダウンロードフォルダ内の「AP installation utility for CWM.exe」を実行します。



図 2-26 AP installation utility for CWM.exe の実行

AP installation utility for CWM が起動します。

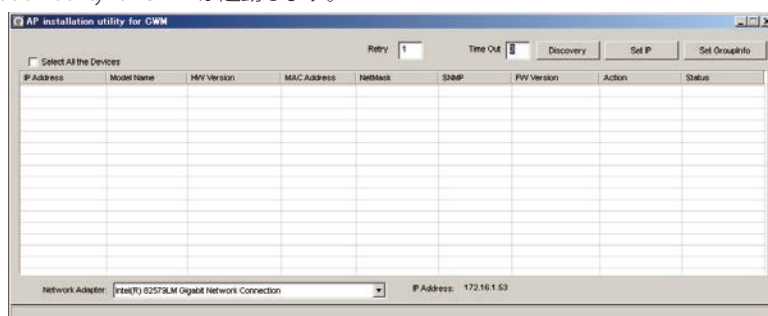


図 2-27 AP installation utility for CWM

プロファイルの検出とインポート

「AP installation utility for CWM」は、D-Link Central Wi-Fi Manager (CWM) に付加機能を提供する追加ユーティリティです。このユーティリティを使用して、設定 IP 範囲に関係なくローカル（レイヤ 2）ネットワークの新しい D-Link アクセスポイントをスキャンし、その後、CWM で使用するための事前設定を行うことができます。このユーティリティは別のセグメントに存在するアクセスポイントを見つけることはできません。このユーティリティを実行するコンピュータ上に、エクスポートされたネットワークプロファイルが準備できていることを確認してください。

AP installation utility for CWM を開くと、以下の画面が表示されます。「Discovery」ボタンをクリックし、イーサネットケーブルでネットワークに繋がっている D-Link アクセスポイントをスキャンします。

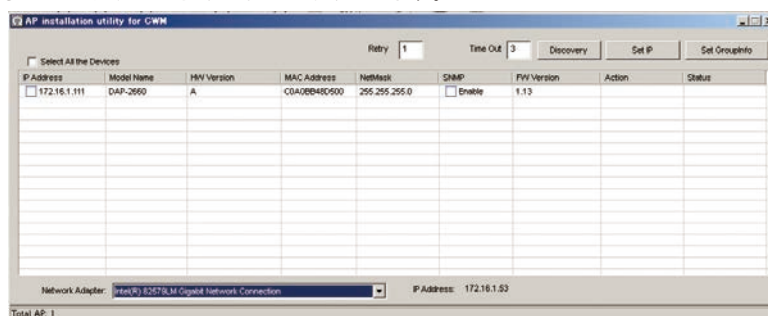


図 2-28 AP installation utility for CWM (起動)

「Discovery」ボタンをクリックすると、LAN（レイヤ 2）のスキャンが始まり、ネットワークに繋がっている D-Link アクセスポイントを検出します。

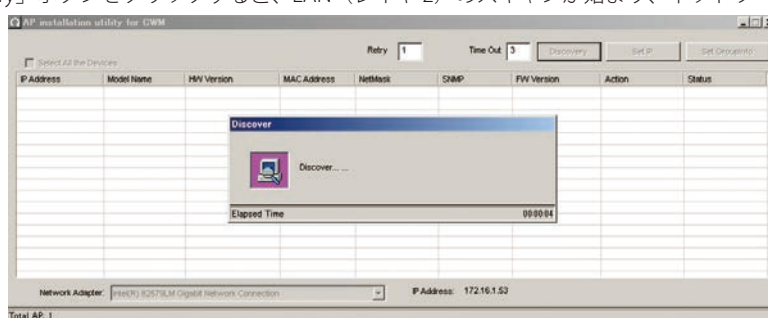


図 2-29 AP installation utility for CWM (Discovery)

第2章 初期設定ガイド

アクセスポイントが検出されると、検出結果が一覧に表示され、構成を変更することができるようになります。

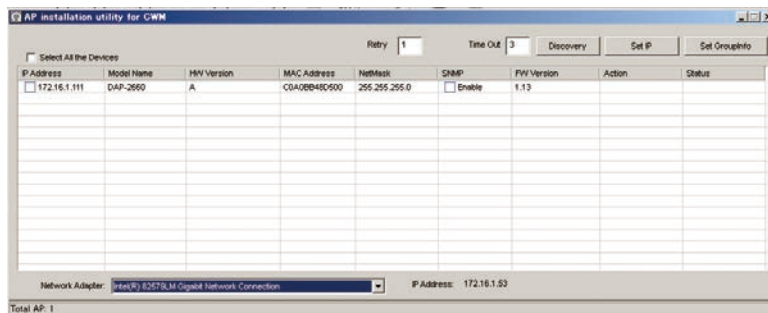
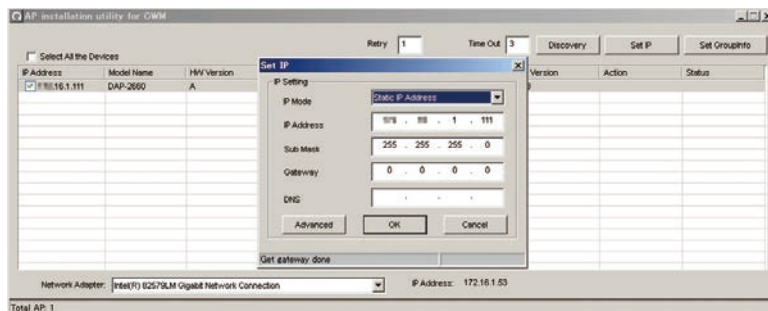


図 2-30 AP installation utility for CWM (検出)

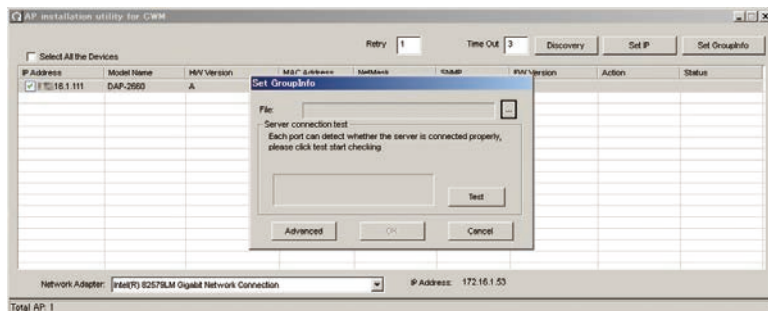
新しく検出されたアクセスポイントの IP アドレスを変更するには、該当のアクセスポイントを選択し、「Set IP」ボタンをクリックします。「新しい IP アドレス」「サブネットマスク」「ゲートウェイアドレス」「プライマリ DNS アドレス」を入力します。「OK」ボタンをクリックすると、変更が適用されます。



☒ 2-31 AP installation utility for CWM (Set IP)

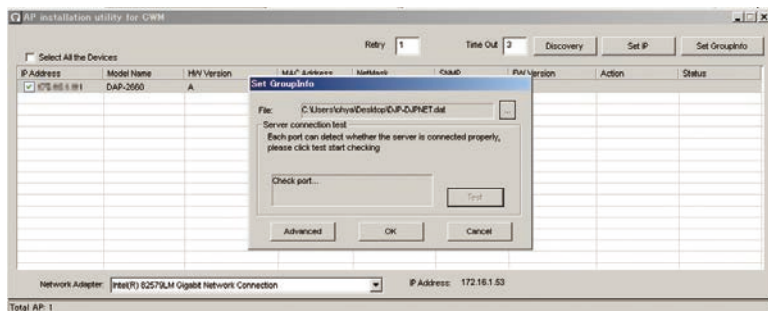
IP アドレスを設定し「OK」をクリックした後、アクセスポイントの構成で新しい IP アドレスが適用されます。その間、再起動されるまでしばらく待機する必要があります。「Status」パラメータでは、IP アドレスの変更およびアクセスポイント再起動の進捗状況が表示されます。

本ユーティリティを利用して、ネットワークデータファイルをアクセスポイントに直接アップロードし、アクセスポイントが所属するネットワークを識別するためのグループ情報を設定することもできます。ネットワークデータファイルをアップロードするには、「Set GroupInfo」ボタンをクリックします。「Set GroupInfo」ボタンをクリックした後、「...」ボタンをクリックしてコンピュータ上に保存されたネットワークデータファイルを指定し、アップロードすることが可能です。



☒ 2-32 AP installation utility for CWM (Set Groupinfo)

アップロードするデータファイルが有効なネットワークデータファイルであるかどうかを確認するには、「Test」ボタンをクリックします。「Test」ボタンをクリックします。ネットワークデータファイルが有効であることが正常に確認されると、「Check port....OK」のメッセージが表示されます。アップロードを開始するには、「OK」ボタンをクリックします。



☒ 2-33 AP installation utility for CWM_Test OK

「OK」ボタンをクリックすると、ネットワークデータファイルがアップロードされます。アクセスポイントはデータファイルの設定に従って構成され、その後再起動されます。「Status」パラメータに構成の進捗状況が表示されます。

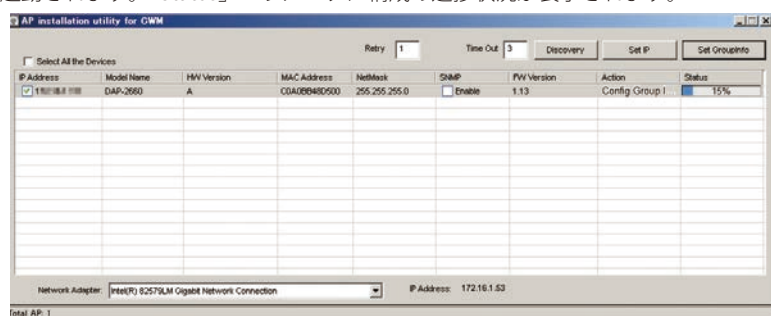


図 2-34 AP installation utility for CWM (Uploading)

アクセスポイントリスト

各アクセスポイントがどのサイトに接続されているかを確認するには、**Home > (Site)**を選択します。オンライン状態のアクセスポイントは、「Status」項目に青いアイコン（)が表示され、オフライン状態のアクセスポイントはグレーのアイコン（)が表示されます。

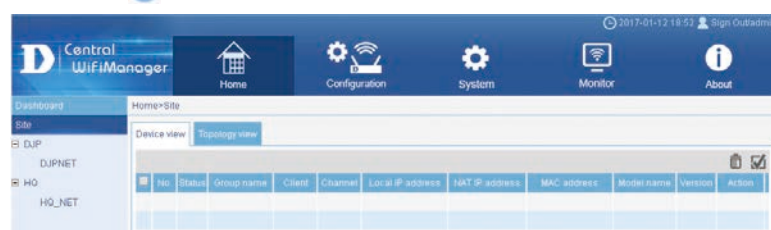


図 2-35 Access Points List

表示される各アクセスポイントの情報は、「No.」「Status」「Group name」「Client」「Channel」「Local IP address」「NAT IP address」「MAC address」「Model name」「Version」「Action」です。

設定の適用

AP への設定適用（コンフィグアップロード）

ネットワーク上の既存のアクセスポイントに新しい設定内容（Configuration）をアップロードするには、**Configuration > (Site) > (Network)** でアップロードするネットワークを選択し、左側の「Uploading Configuration」オプションを選択します。

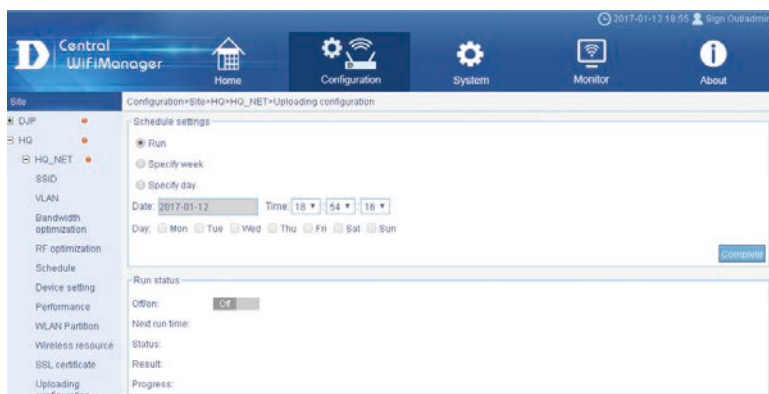


図 2-36 Uploading Configuration

「Complete」ボタンをクリックすると既存のアクセスポイントに新しい設定を適用します。

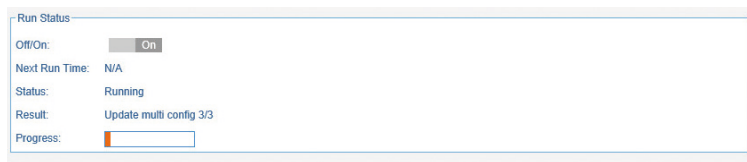


図 2-37 Uploading Configuration (Progress)

「Uploading Configuration」ページでは、ネットワーク上の既存アクセスポイントに対し、すぐに新しい構成を適用するか、定期的なコンフィグレーションの適用をスケジューリング（Schedule settings）するかを決めることができます。

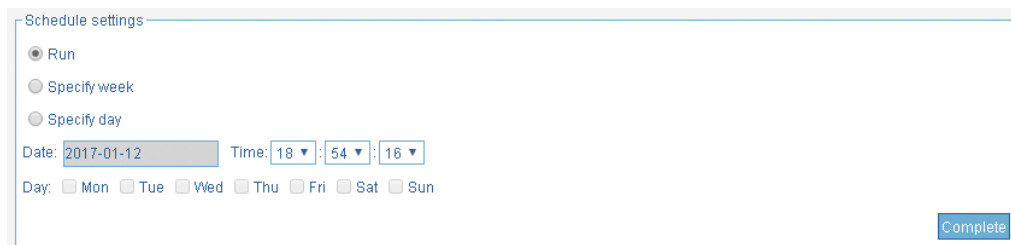


図 2-38 Uploading Configuration (Schedule)

キャプティブポータルとユーザ認証

キャプティブポータルでは、ゲストユーザに対し無線アクセスを提供することができます。本機能は、エンタープライズや大学、病院といった環境でよく利用されます。このシナリオにおける目的は以下の通りです。

- ・ キャプティブポータルについての理解
- ・ ローカルデータベース認証とパスコード認証の設定方法

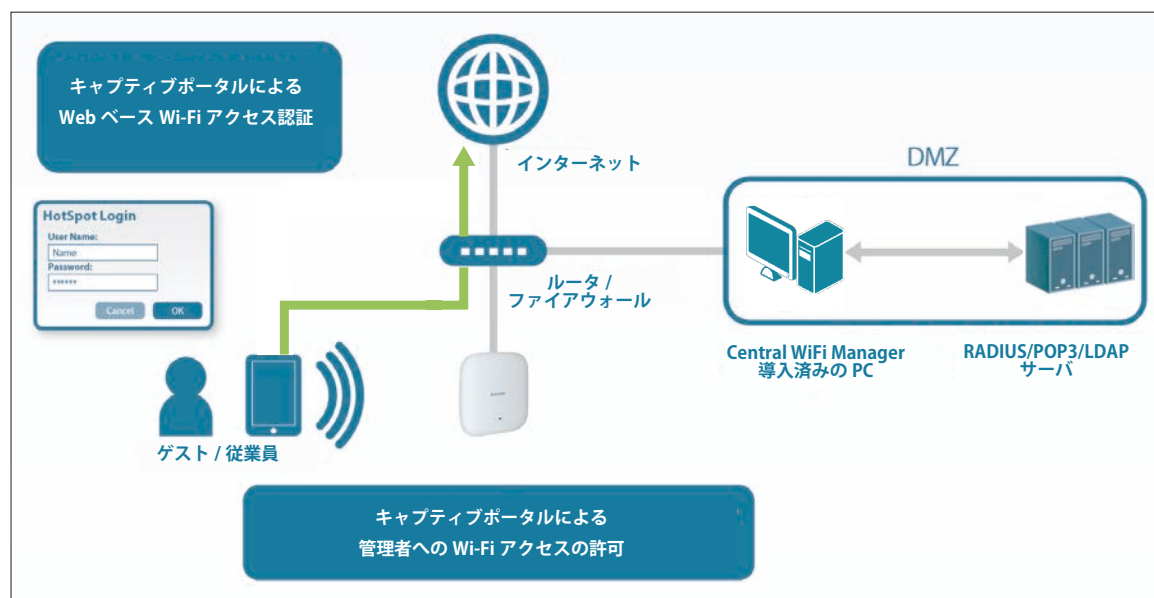


図 2-39 キャプティブポータル

キャプティブポータルの構成手順の概要は以下の通りです。

1. キャプティブポータルを設定します。
2. ローカルデータベース認証を設定します。
3. パスコード認証を設定します。
4. フロントデスクアカウント作成します。
5. フロントデスクアカウントをサイトネットワークへ追加します。
6. ゲストへパスワードを発行します。

キャプティブポータル設定

キャプティブポータル構成を設定するには、**Configuration > (Site) > (Network)** を選択し、設定する SSID を指定します。SSID の「Modify」で「User authentication」の「Authentication type」から認証方法を指定すると、「Web Redirection」オプションを指定する事が可能になります。Web サイトのリダイレクトを有効化し、リダイレクトさせる Web サイト (www.google.com) (例) を入力します。「Splash page customization」で Web ページのテンプレートを選択しアップロードすることも可能です。詳しくは「第 4 章 Configuration (コンフィグレーション)」の「Create SSID (SSID 作成)」を参照ください。「Save」ボタンをクリックし、変更を適用します。



図 2-40 Captive Portal Settings

注意 SSID の設定で「WPA-Enterprise」を選択し、設定する RADIUS サーバの IP アドレスと「Captive Portal」の IP インタフェースの設定画面で設定する DNS の IP アドレスが同じ場合、および「管理 VLAN」と「Captive Portal」の IP インタフェースの設定画面での VLAN が異なる場合には、「Captive Portal」は動作しません。

ローカルデータベース認証

本節では、新しいゲスト SSID を作成し、ローカルデータベース認証に使用するように設定します。新しい SSID を作成するには、**Configuration > (Site) > (Network)** を選択し、左側から「SSID」（初期値）を指定します。

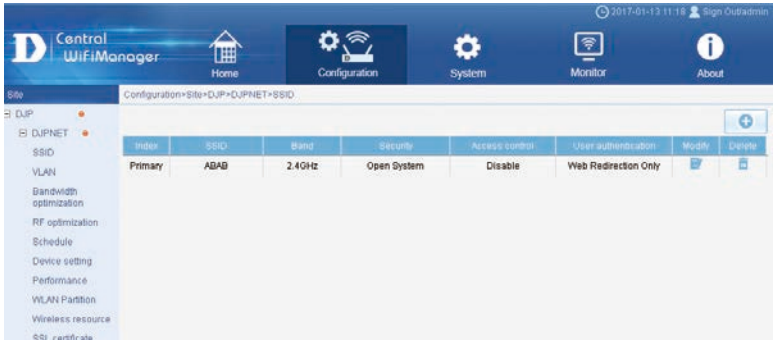


図 2-41 SSID（Configuration>Site>Network）

新しく 2.4GHz のゲスト「SSID」を作成するには、既存の Network を選択し、 ボタンをクリックします。「Basic settings」で「Band」（2.4G）、「Index」 「Character set」などを選択、SSID 名を入力し、「Security」で無線セキュリティを設定します。設定を適用するには「Save」をクリックします。

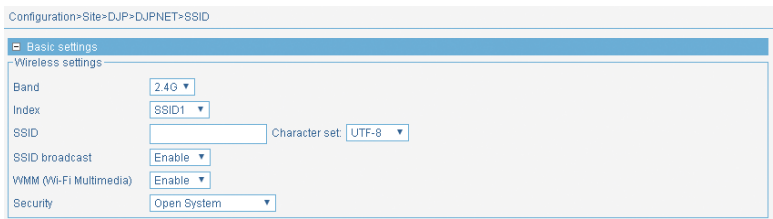


図 2-42 Configure SSID

「User Authentication」セクションで、「Username/Password」を選択します。ゲストユーザがイントラネットにアクセスすることを制限するためには、「IP filter settings」で IP 範囲を入力します。

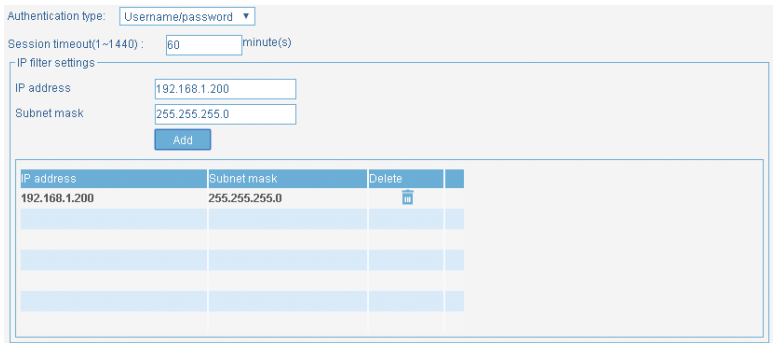


図 2-43 Configuration Guest SSID User Authentication ①

SSID の「IP Interface Settings」を設定し、新しいゲストアカウントの「Username」と「Password」を入力します。「Add」ボタンをクリックしてテーブルに新しいゲストユーザアカウントを追加します。「Save」ボタンをクリックし、変更を適用します。

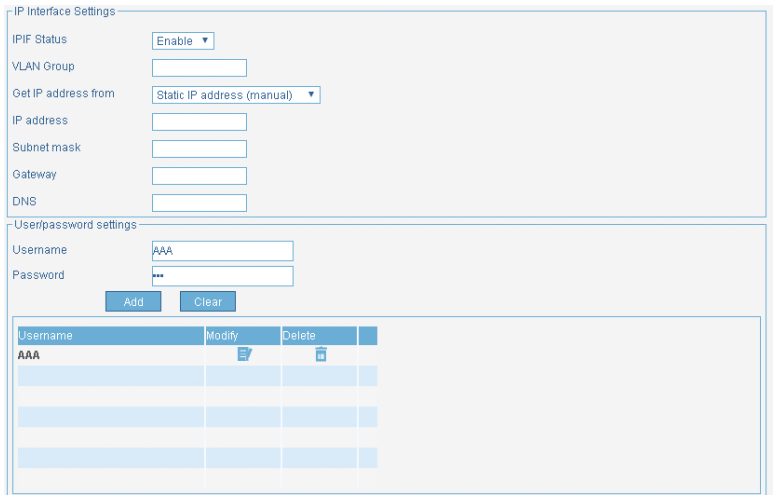


図 2-44 Configuration Guest SSID User Authentication ②

Configuration > (Site) > (Network) を選択し、左側のメニューより「Uploading Configuration」オプションを選択します。「Run」オプションを選択し、「Complete」ボタンをクリックしてネットワークのアクセスポイントに変更された設定をアップロードします。

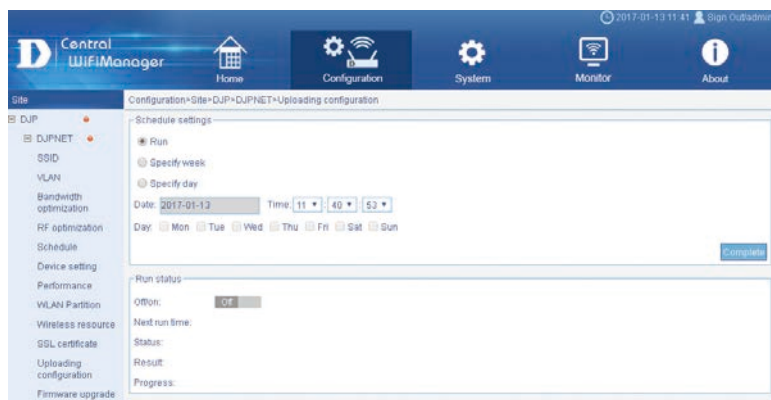


図 2-45 Uploading Configuration

パスコード認証

SSID パスコード認証

本項では、新しいゲスト SSID を作成し、パスコード認証を使用するように設定します。新しい SSID を作成するには、**Configuration > (Site) > (Network)** を選択します。

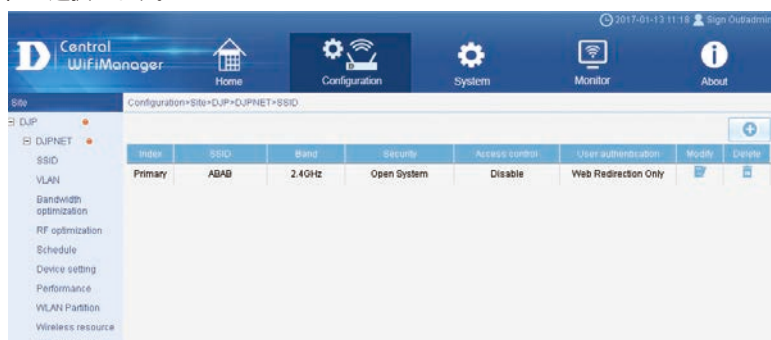


図 2-46 Create Guest SSID_Passcode

新しく 2.4GHz のゲスト「SSID」を作成するには、既存の「Network」を選択し、 ボタンをクリックします。「Band」(2.4G)、「Index」を選択し、SSID 名を入力し、無線セキュリティを設定します。設定を適用するには「Save」をクリックします。

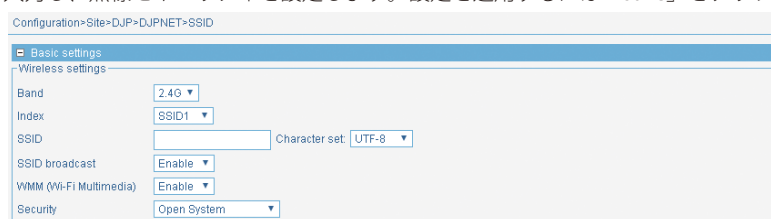


図 2-47 Configure SSID

「User Authentication」セクションで「Passcode」を選択します。「Save」ボタンをクリックし、変更を適用します。

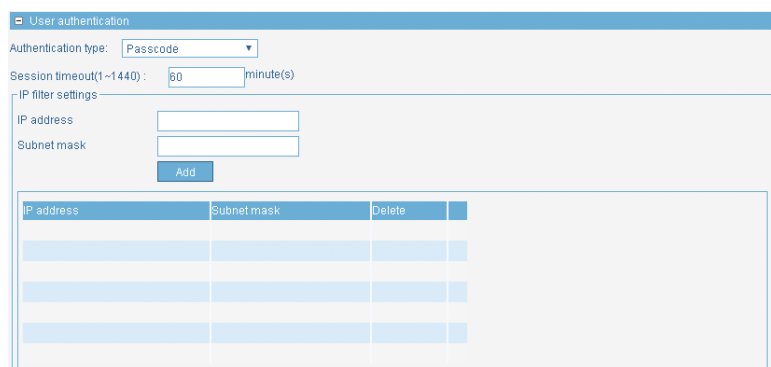


図 2-48 User Authentication_Passcode

フロントデスクアカウント作成

次に新しいフロントデスク（Front Desk）ユーザアカウントを作成します。**System > User Manager** を選択し、 ボタンをクリックします。

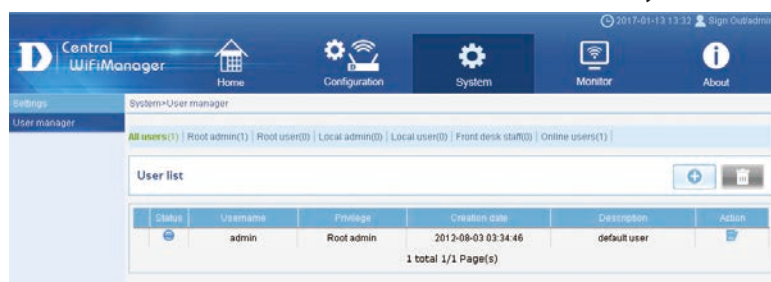


図 2-49 User Manager

新しいアカウントとして「Username」と「Passcode」を入力します。「Privilege」に「Front Desk Dtaff」オプションを選択し、「E-Mail」アドレスを入力します。「OK」ボタンをクリックし、新しいユーザアカウントを作成します。

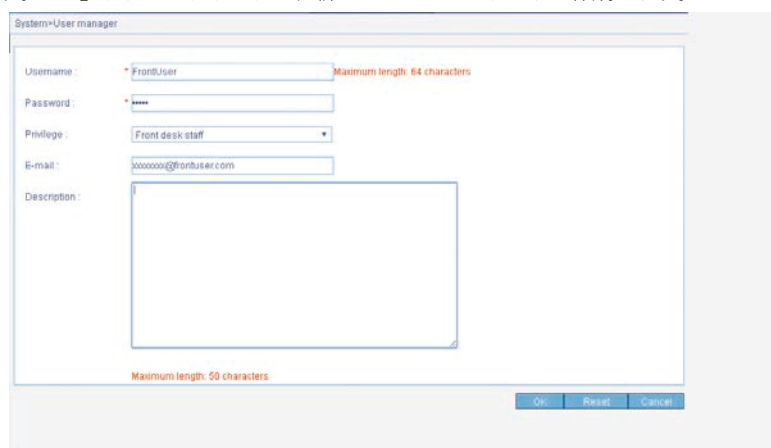


図 2-50 Create New Front Desk Account

注意 CWM では一部の特殊文字 ("&\) はサポート対象外となります。

フロントデスクアカウントのサイト / ネットワークへの追加

フロントデスクアカウントをサイトへ追加するには、**Configuration > (Site)** を選択し、追加するサイトの「Modify」アイコン をクリックします。



図 2-51 Add Front Desk Account to Site ①

「」をクリックした後、フロントデスクアカウントを選択し、「>>」ボタンをクリックして「Selected」テーブルに追加します。「OK」ボタンをクリックし、変更を適用します。

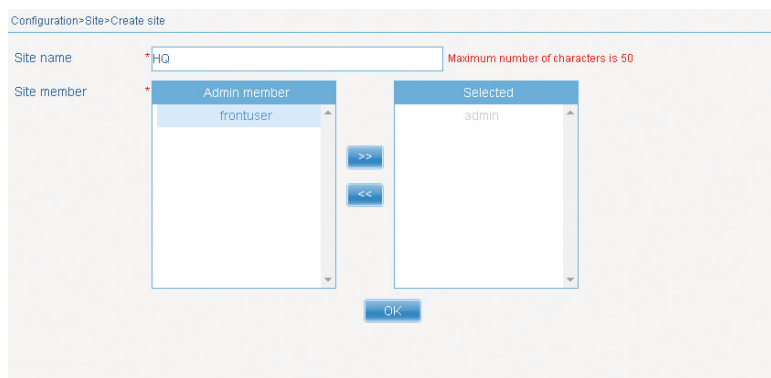


図 2-52 Add Front Desk Account to Site ②

次にフロントデスクアカウントをネットワークへ追加するには **Configuration > (Site) > (Network)** を選択し、追加するネットワークの「Modify」アイコンをクリックします。

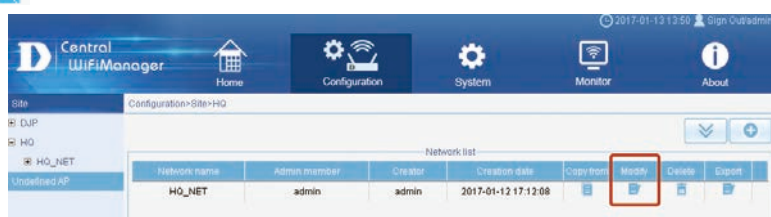


図 2-53 Add Front Desk Account to Network ①

編集アイコンをクリックした後、フロントデスクアカウントを選択し、「>>」ボタンをクリックして「Selected」テーブルに追加します。「OK」ボタンをクリックし、変更を適用します。

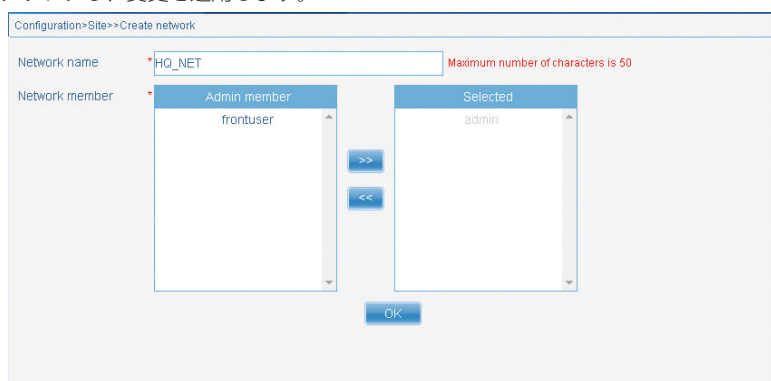


図 2-54 Add Front Desk Account to Network ②

ゲストへのパスコード発行

次に作成したフロントデスクアカウントのパスコード（Passcode）を発行します。まず一旦 CWM をサインアウトし、フロントデスクアカウントのユーザ名とパスワードを使用して再度ログインします。ログイン後、「Passcode settings」で「SSID」「Passcode quantity」「Duration」「Hours」「Last active day」「User limit」の情報を入力し、「Generate」ボタンをクリックします。



図 2-55 Generate Passcode

「View」ページにフロントデスクアカウントのパスコード一覧が表示されます。

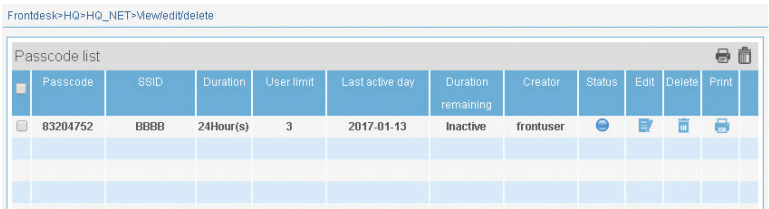


図 2-56 Display Passcodes

管理者の場合、CWM に管理者としてログインし直すことでパスコード一覧を確認することができます。管理者としてパスコード一覧を確認するには、**Configuration > (Site) > (Network) > (SSID)** を選択します。「Modify」アイコンをクリックすると、「User Authentication」セクションにパスコード一覧が表示されます。

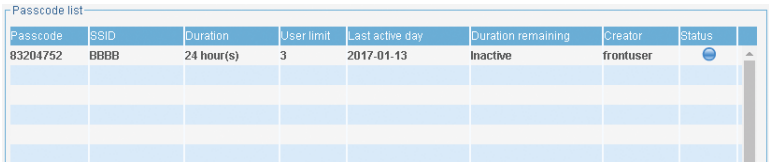


図 2-57 Display Passcodes_Administrator Account

Configuration > (Site) > (Network) を選択し、左側のメニューより「Uploading Configuration」オプションを選択します。「Run」オプションを選択し、「Complete」ボタンをクリックしてネットワークのアクセスポイントに変更された設定をアップロードします。

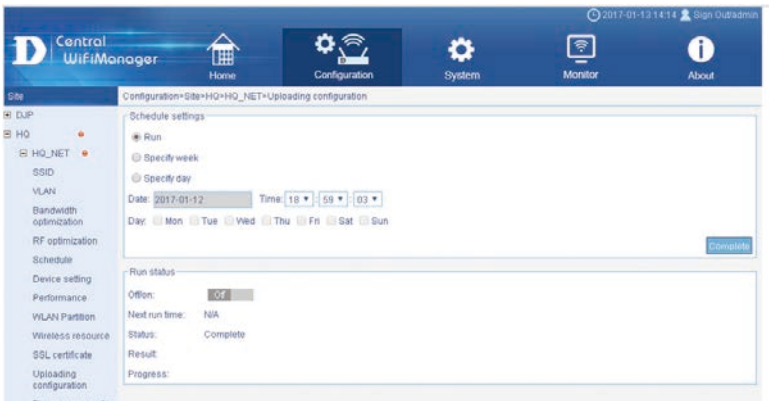


図 2-58 Uploading Configuration

帯域最適化

Bandwidth Optimization（帯域最適化）を行うことで、管理者が無線帯域の使用を制御することができます。「Downlink Bandwidth」と「Uplink Bandwidth」オプションにより、アクセスポイント合計の帯域を制限します。CWM で利用することができる帯域最適化ルールについての詳細は、「第4章 Configuration（コンフィグレーション）」の「Bandwidth Optimization（帯域最適化）」を参照して下さい。

帯域最適化設定

帯域最適化設定を行うには、**Configuration > (Site) > (Network) > Bandwidth Optimization** を指定します。

これはすべてのアクセスポイントに対する帯域設定となります。「Enable Bandwidth Optimization」にて「Enable」を選択、「Downlink Bandwidth」と「Uplink Bandwidth」を指定します。「Add bandwidth optimization rule」の「Rule Type」オプションを指定、「(Allocate maximum Bandwidth for each station)（各ステーションに対し最大の帯域制御を割り当てる）推奨」、「Band」、「SSID」を選択します。「Downlink Speed」と「Uplink Speed」を入力します。「Add」ボタンをクリックし、新しいルールを作成後「Save」ボタンをクリックして変更を適用します。

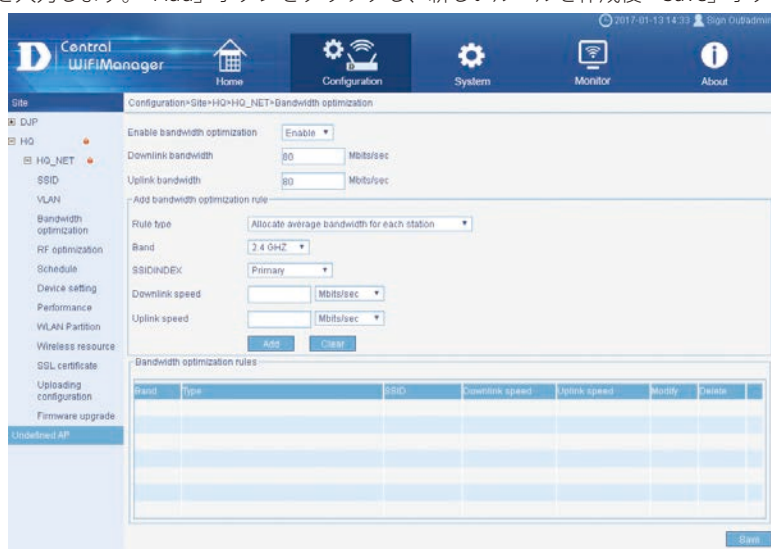


図 2-59 Bandwidth Optimization Settings

Configuration > (Site) > (Network) を選択し、左側のメニューより「Uploading Configuration」オプションを選択します。「Run」オプションを選択し、「Complete」ボタンをクリックしてネットワークのアクセスポイントに変更された設定をアップロードします。

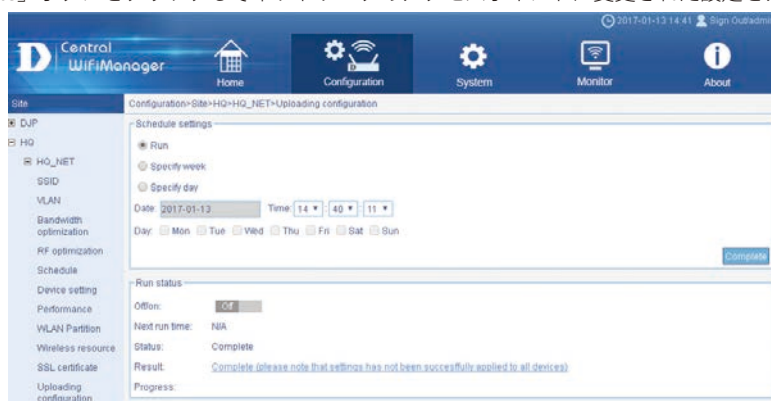


図 2-60 Uploading Configuration

リモート AP の追加

CWM は、サイト間 VPN で配置された、リモートのアクセスポイントを管理することができます。
構成手順の概要は以下の通りです。

1. Network Device 構成を設定します。
2. 各拠点に新しいサイトとネットワークを作成します。
3. ネットワークプロファイルをエクスポートし、リモートアクセスポイントにインポートします。

ネットワーク機器設定

リモートのアクセスポイントが CWM サーバにアクセスできるように、CWM サーバが配置されているサイトのファイアウォールでは以下のポート番号が開かれている必要があります。

- UDP 161 (SNMP port)
- UDP 162 (SNMP trap port)
- UDP 514 (Syslog port)
- UDP 8090 (Listen port)
- UDP 64768 (Service port)
- TCP 9000, Enable ftp-ALG (Manager port)
- TCP 443 (HTTPS, Management port)

また、CWM サーバがプライベート IP アドレスを使用している場合、ファイアウォールにおいて、グローバル IP アドレスとプライベート IP アドレスがマッピングされていなければなりません。

リモートサイトでは、以下のポートも開かれている必要があります。

- UDP 161 (SNMP port)
- UDP 162 (SNMP trap port)
- UDP 514 (Syslog port)
- UDP 8090 (Listen port)
- UDP 64768 (Service port)
- TCP 9000, Enable ftp-ALG (Manager port)

サイト / ネットワークの作成 (リモート AP)

新しいサイトを作成するには、「Configuration」を選択し、 ボタンをクリックします。
「Site name」「Site member」を指定し、「OK」でサイトを作成します。

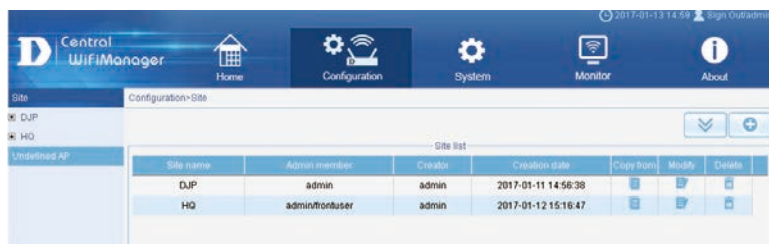


図 2-61 Create New Site

新しいネットワークを作成するには、新しく作成したサイトを選択し、 ボタンをクリックします。

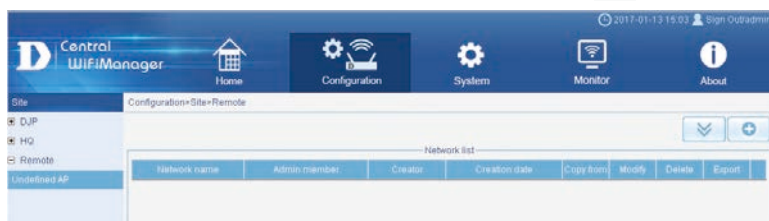


図 2-62 Create New Site_Branch_A

注意

CWM では一部の特殊文字 ("&" "\") はサポート対象外となります。

ネットワークプロファイルのエクスポート / インポート（リモート AP）

ネットワークプロファイルをエクスポートするには、**Configuration > (Site)** を選択し、作成したネットワークの「Export」アイコンをクリックし、コンピュータ上にネットワークプロファイルをエクスポートします。エクスポートしたプロファイルファイルは、リモートサイトのインストーラで利用します。

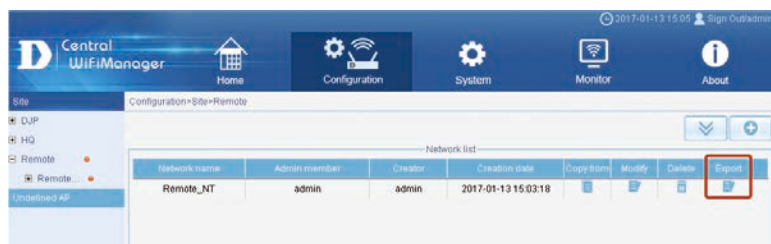


図 2-63 Export Network Profile

リモートサイトにおいてアクセスポイントを構成するコンピュータが、エクスポートされたプロファイルファイルを利用可能であることを確認してください。次に「AP installation utility for CWM」を実行します。

AP installation utility for CWM を開くと、以下の画面が表示されます。「Discovery」ボタンをクリックし、イーサネットケーブルでネットワークに繋がっている D-Link アクセスポイントをスキャンします。

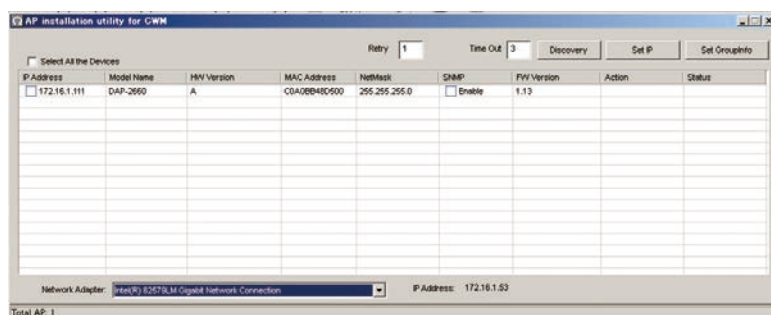


図 2-64 AP installation utility for CWM（起動）

「Discovery」ボタンをクリックすると、LAN（レイヤ 2）のスキャンが始まり、ネットワークに繋がっている D-Link アクセスポイントを検出します。

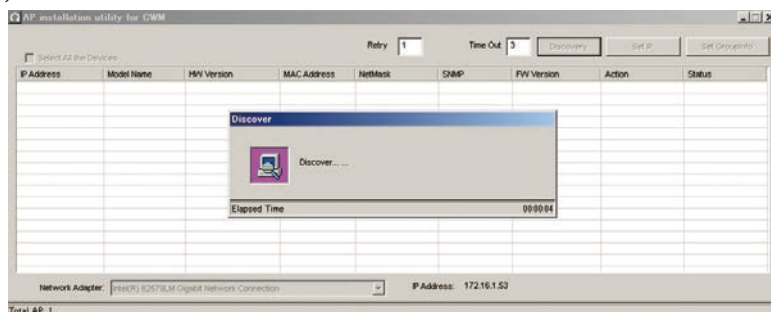


図 2-65 AP installation utility for CWM（Discover）

アクセスポイントが検出されると、検出結果が一覧に表示され、構成を変更できるようになります。

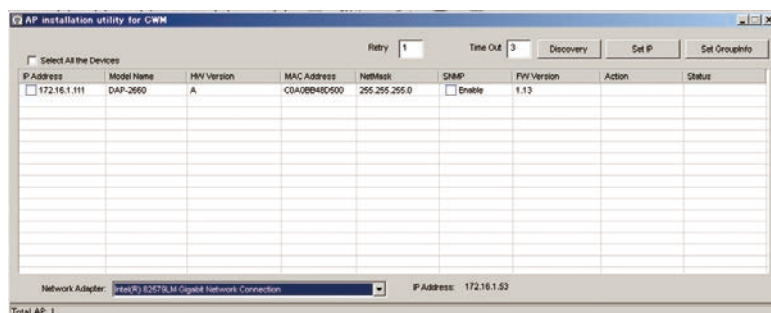


図 2-66 AP installation utility for CWM（検出）

第2章 初期設定ガイド

新しく検出されたアクセスポイントの IP アドレスを変更するには、該当のアクセスポイントを選択し、「Set IP」 ボタンをクリックします。「新しい IP アドレス」「サブネットマスク」「ゲートウェイアドレス」「プライマリ DNS アドレス」を入力します。「OK」 ボタンをクリックすると、変更が適用されます。

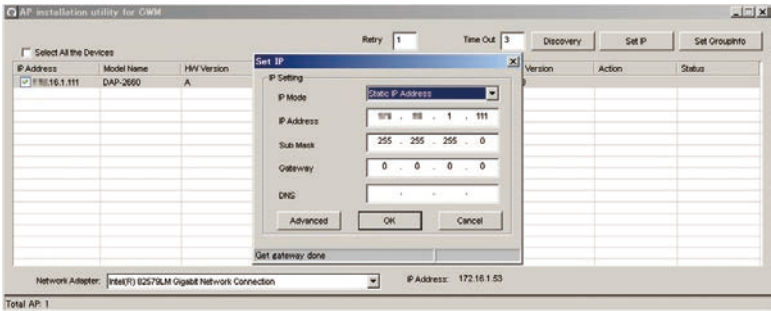


図 2-67 AP installation utility for CWM (Set IP)

IP アドレスを設定し「OK」をクリックした後、アクセスポイントの構成で新しい IP アドレスが適用されます。その間、再起動されるまでしばらく待機する必要があります。「Status」パラメータでは、IP アドレスの変更およびアクセスポイント再起動の進捗状況が表示されます。

本ユーティリティを利用して、ネットワークデータファイルをアクセスポイントに直接アップロードし、アクセスポイントが所属するネットワークを識別するためのグループ情報を設定することもできます。ネットワークデータファイルをアップロードするには、「Set GroupInfo」 ボタンをクリックします。「Set GroupInfo」 ボタンをクリックした後、「...」 ボタンをクリックしてコンピュータ上に保存されたネットワークデータファイルを指定し、アップロードすることが可能です。

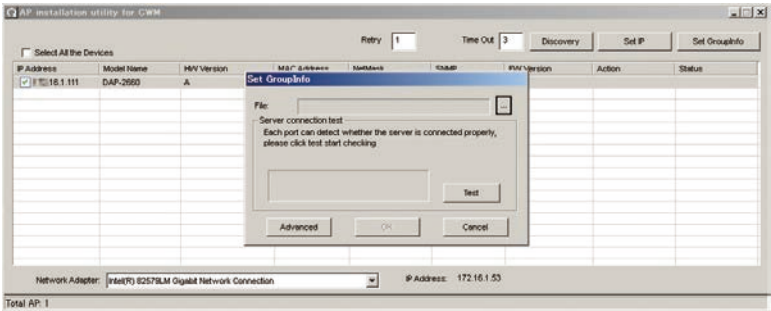


図 2-68 AP installation utility for CWM (Set Groupinfo)

アップロードするデータファイルが有効なネットワークデータファイルであるかどうかを確認するには、「Test」 ボタンをクリックします。「Test」 ボタンをクリックします。ネットワークデータファイルが有効であることが正常に確認されると、「Check port....OK」のメッセージが表示されます。アップロードを開始するには、「OK」 ボタンをクリックします。

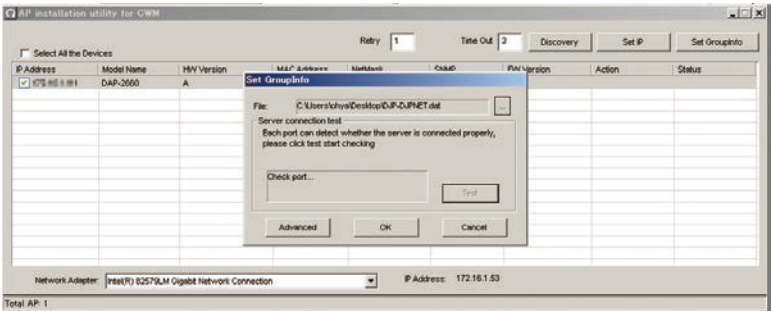


図 2-69 AP installation utility for CWM_Test OK

「OK」ボタンをクリックすると、ネットワークデータファイルがアップロードされます。アクセスポイントはデータファイルの設定に従って構成され、その後再起動されます。「Status」パラメータに構成の進捗状況が表示されます。

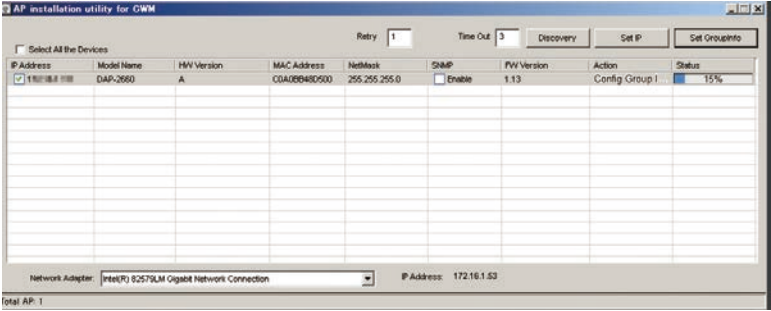


図 2-70 AP installation utility for CWM (Uploading)

Wi-Fi 設定変更

作成したネットワークの無線モードの詳細設定を行います。

Configuration > Site (サイト名) > Network (ネットワーク名) の左パネルのオプションから「Performance」を選択し、「2.4GHz」「5GHz」の設定を行うことができます。設定した内容は選択したネットワーク上の有効な全てのアクセスポイントに適用されます。

「Performance」をクリックすると、以下のページを表示されます。「2.4GHz」「5GHz」をタブで選択し、「Wireless」で無線帯を有効 / 無効に、「Wireless Mode」で無線モードの設定を行います。

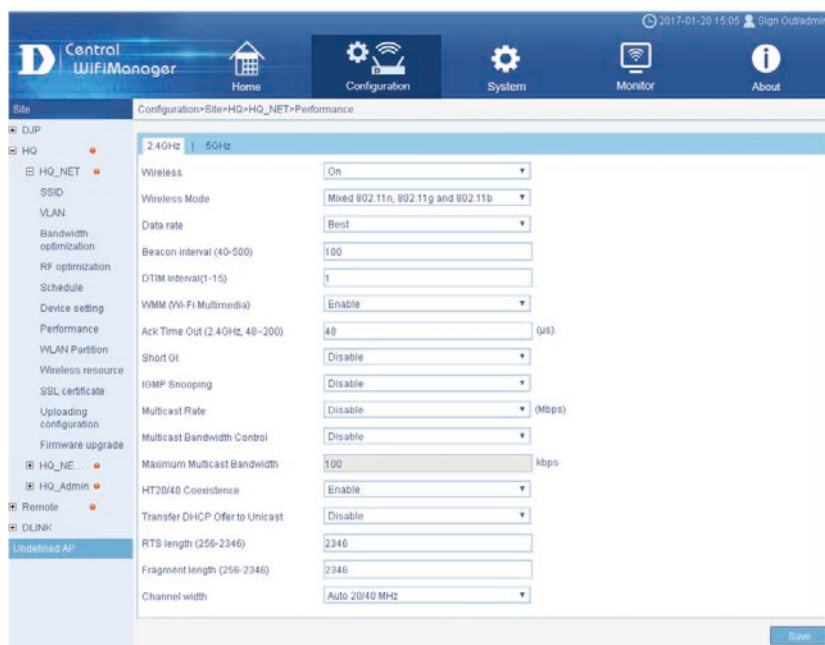


図 2-71 Performance (2.4GHz)

「Data Rate」や「Beacon Interval」の設定を各帯域で行い、「Save」ボタンをクリックすると変更を保存します。

ネットワークに設定した変更事項は **Configuration > (Site) > (Network) > Uploading Configuration** で各 AP にアップロードし適用します。

注意 詳しくは「第 4 章 Configuration (コンフィグレーション)」の「Performance (パフォーマンス設定)」を参照してください。

第 3 章 Home (ホーム)

本項目では「Central Wi-Fi Manager」の項目「Home」の説明をします。

Dashboard (ダッシュボード)

サーバへのログインに成功した後、「Dashboard」ページが有効になります。本項目では接続中のアクセスポイントの概要や無線クライアント一覧が表示されます。

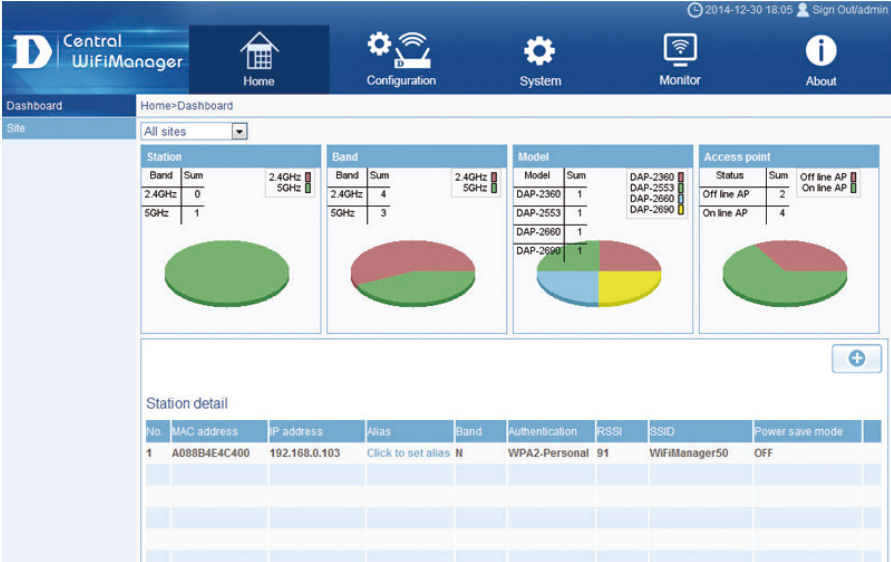


図 3-1 ダッシュボード

「サイト」を設定後、サイトリストはドロップダウンメニューでの選択が有効になります。ドロップダウンメニュー下は4つのブロックで構成され、使用状況を視覚的に示す円グラフが各ブロックに表示されます。

ブロック	詳細
Station	このネットワークのアクセスポイントに接続された無線クライアント数がサポートされた無線周波数ごとに表示されます。
Band	このネットワークのアクセスポイントにホストされた無線周波数帯域がサポートされた周波数帯域ごとに表示されます。
Model	このネットワークのアクセスポイント数がプロダクトコードごとに表示されます。
Access Point	オンラインとオフラインのアクセスポイント数がステータスごとに表示されます。

「Station Detail」リストには、接続された無線クライアントの一覧が基本情報と共に表示されます。

Site (サイト)

「Site」では、設定されたサイトの情報が表示されます。

Device View (デバイスビュータブ)

本項目では、「Site」内の「Device View」タブについて説明します。
「Device View」タブでは、作成した「Site」に関連するアクセスポイントの一覧が表示されます。表のコラムにはアクセスポイントについての詳細が表示されます。特定のアクセスポイントについてのより詳細な情報を見るには、そのアクセスポイントの IP アドレスをクリックします。

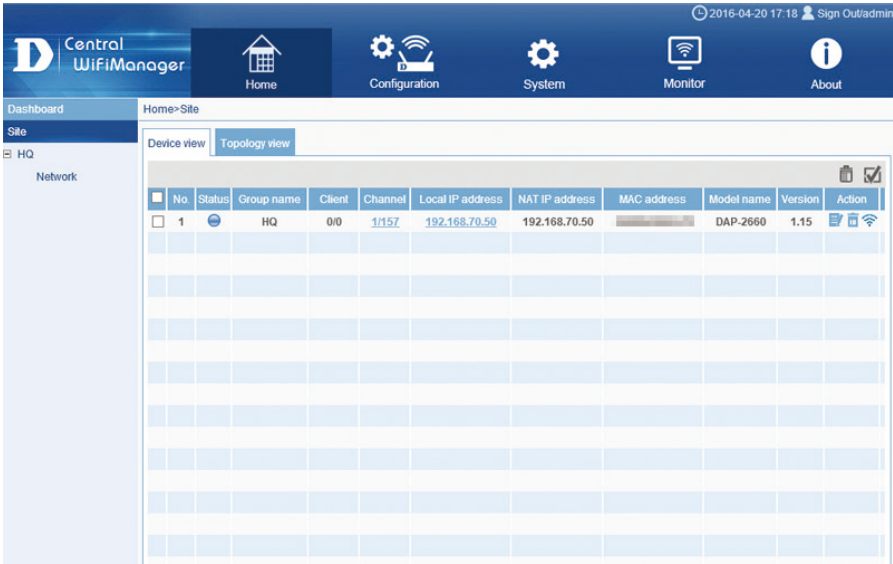


図 3-2 デバイスビュータブ

以下の項目があります。

アイコン	詳細
	クリックすると、このネットワークから全てのアクセスポイントを削除します。
	クリックして、表示するネットワーク情報の項目を指定します。
	クリックすると、該当のアクセスポイントを手動で再起動します。
	クリックすると、該当のアクセスポイントをネットワークから削除します。
	クリックすると、該当のアクセスポイントの送信出力の設定をします。

アイコンをクリックすると、アクセスポイントの送信出力の設定をするダイアログが表示されます。

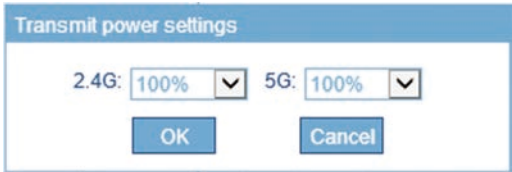


図 3-3 送信出力の調整

「2.4G」と「5G」の送信出力について設定します。「OK」を押して適用、「Cancel」で設定を中止します。

サイトの設定についての詳細は「第 2 章初期設定ガイド」「サイト / ネットワークの作成、SSID 設定」を参照してください。例では、サイト名「Headquarters」を作成し、このサイト内にネットワーク名「Server-Room」を作成します。ネットワークの作成または設定についての詳細は「第 2 章初期設定ガイド」「サイト / ネットワークの作成、SSID 設定」を参照してください。

Topology View (トポロジビュータブ)

本項目では、「Site」内の「Topology View」タブについて説明します。
「Topology View」タブでは、指定されたサイトに接続されたすべてのデバイスが視覚的に表示されます。



図 3-4 トポロジビュータブ

以下の項目があります。

項目	説明
Add Topology	上部のビューエリアの右にある「+」アイコンです。アイコンをクリックするとカスタムトポロジを追加します。
Edit Topology	上部のビューエリアの右にある「i」アイコンです。アイコンをクリックすると新しく追加したトポロジの名前を編集します。
Delete Topology	トポロジタブの右にある「x」アイコンです。アイコンをクリックすると作成したカスタムトポロジを削除します。初期値としてある「all」トポロジは、削除できません。
Map Size	トポロジビューのマップサイズは編集します。テキストボックスのビューに「width」（幅）と「height」（高さ）を入力し、「Submit」をクリックして変更を適用します。有効な値は 800 ～ 8000 です。
	Cursor：アイテムを個別に選択するオプションです。
	Guide：トポロジのガイドを表示にします。
	Add Device：アクセスポイントをトポロジに追加します。
	Add Background：トポロジのバックグラウンド画像をカスタマイズできます。お手持ちの画像をアップロードします。「JPG」「JPEG」「GIF」「PNG」のフォーマットが有効です。
	Pen：デバイスから他のデバイスへ手動で接続ラインを引きます。接続ラインを引くと、有線または無線のどちらかとして指定されます。線の色と太さはカスタマイズ可能です。
	Drag：シンプルセレクト機能を有効にして、オブジェクトとトポロジの背景を移動します。
	Save：トポロジを保存します。
	PC (Null)：Central Wi-Fi Manager Server がインストールされている管理 PC を示します。
	Access Points：サイトのあるアクセスポイントと相互の接続関係を示します。アクセスポイントのアイコン上でダブルクリックをすると、アクセスポイントの詳細情報が表示されます。

注意 CWM では一部の特殊文字 ("&" "\") はサポート対象外となります。

第 4 章 Configuration (コンフィグレーション)

本項目では「Central Wi-Fi Manager」の項目「Configuration」の説明をします。
「Configuration」では主に「Central Wi-Fi Manager」の「Site」「Network」の設定を行います。

Site (サイト)

「Site」では、サイトの作成、設定を行います。

本項目では、ネットワーク上の無線デバイスのロケーションに関するロジカルな「サイト」と「ネットワーク」の表示、作成、設定ができます。本 CWM アプリケーションを使用することにより、これらのサイトの無線デバイスは CWM にて一律に管理されます。

既に設定されているサイトとネットワークは、左パネルの「Site」オプション下に表示され、「Site」オプションをクリックすると、作成されたサイトの一覧がメインページに表示されます。

サイト一覧

左側の「Site」をクリックすると作成済みの「サイト一覧」が表示されます。

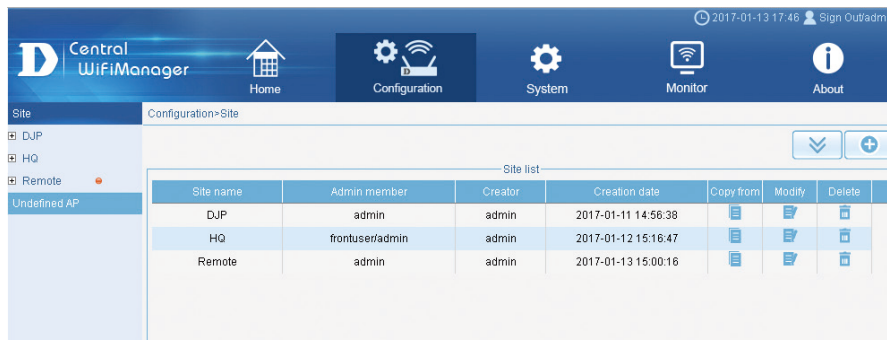


図 4-1 作成済みサイト一覧 (Configuration)

以下の項目があります。

	クリックすると、新しくサイトを作成します。
	クリックすると、「AP installation utility for CWM」(AP インストールツール)をダウンロードします。
 Copy From	クリックすると、別のサイトの「Configuration」(設定内容)を本サイトにコピーします。
 Modify	クリックすると、既存のサイトを編集します。
 Delete	クリックすると、既存のサイトを削除します。

注意 CWM では一部の特殊文字 ("&") はサポート対象外となります。

サイト作成

 をクリックすると、以下のサイト作成ページが表示されます。本項目ではサイトの作成と各サイトにメンバアカウントを割り当てます。

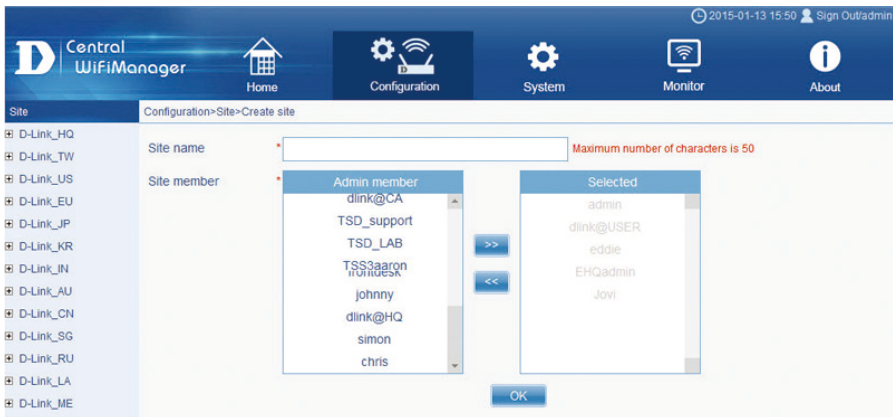


図 4-2 サイト作成

以下の項目があります。

項目	説明
Site name	新しいサイト名（最大 50 文字）を入力します。
Site member	左枠からサイトに追加するメンバアカウントを選択し、「>>」をクリックして右枠の「Selected」リストに追加します。「Selected」リストからメンバアカウントを削除するには、削除するメンバアカウントを選択して、「<<」をクリックします。

「OK」ボタンをクリックすると、新しいサイトが作成されます。

新しいサイトを作成するとサイト一覧に表示されます。

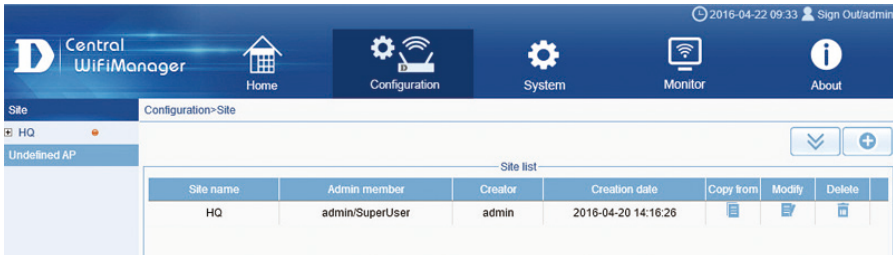


図 4-3 サイトリスト

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

サイトの表示について

左パネルのサイト一覧の「サイト名」をクリックすると、該当サイトについてのメインページ（サイト内のネットワーク一覧）が表示されます。



図 4-4 サイト表示

Network (ネットワーク)

「Network」では、ネットワークの作成、設定を行います。

本項目では、「サイト」内に作成するネットワークの表示、作成、設定について説明します。

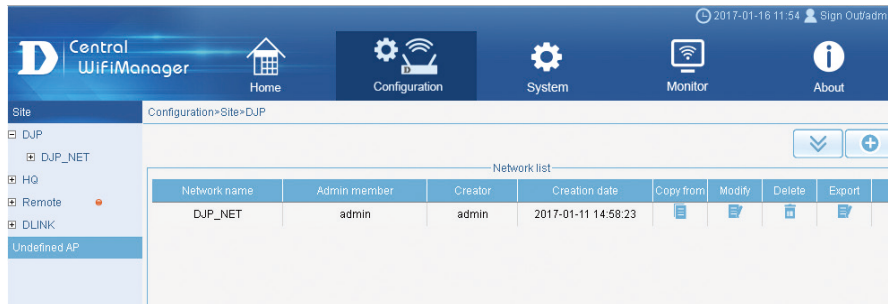


図 4-5 ネットワーク一覧 (Configuration > Site (サイト名))

注意 CWM では一部の特殊文字 ("&\) はサポート対象外となります。

ネットワーク一覧

左パネルの「サイト名」をクリックするとサイト内に作成した「ネットワーク一覧」が表示されます。

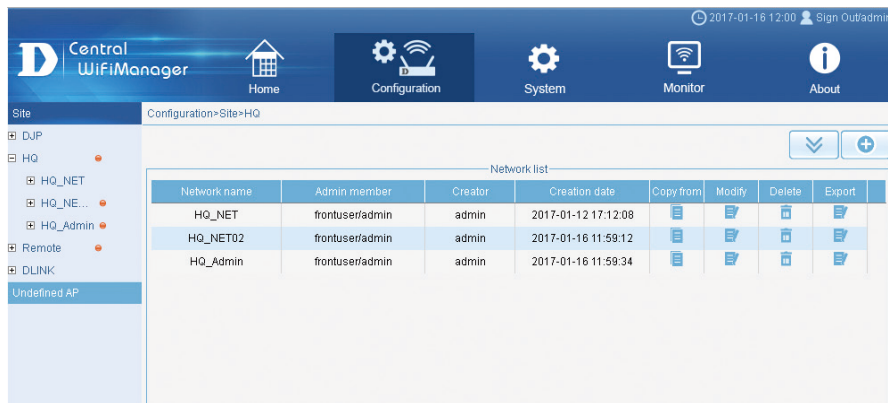


図 4-1 作成済みネットワーク一覧 (Configuration)

以下の項目があります。

	クリックすると、サイト内に新しくネットワークを作成します。
	クリックすると、「AP installation utility for CWM」(AP インストールツール) をダウンロードします。
	クリックすると、別のネットワークの「Configuration」(設定内容) を本ネットワークにコピーします。
	クリックすると、既存のネットワークを編集します。
	クリックすると、既存のネットワークを削除します。
	クリックすると、該当ネットワークの設定内容を Dat ファイルでをエクスポートします。

注意 CWM では一部の特殊文字 ("&\) はサポート対象外となります。

ネットワーク作成

左パネルにある作成した「サイト名」をクリックすると、当該のサイト内に作成された「ネットワーク」のリストが表示されます。

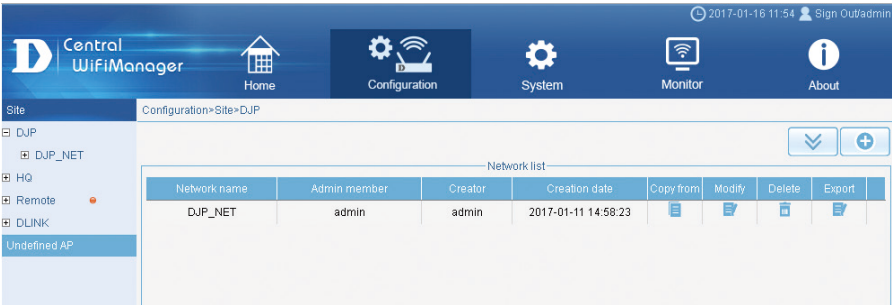


図 4-2 ネットワークリスト

 をクリックすると、新しいネットワークを追加・作成します。下記の画面が表示されます。

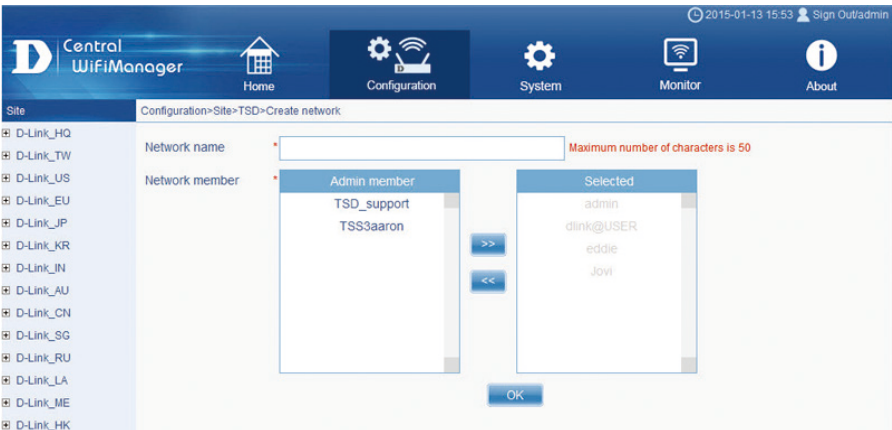


図 4-3 ネットワーク追加

この項目では、ネットワークの作成とそれぞれのネットワークにメンバアカウントを割り当てます。
以下の項目があります。

項目	説明
Network name	新しいネットワーク名（最大 50 文字）を入力します。
Network member	左枠からネットワークに追加するメンバアカウントを選択し、「>>」をクリックして右枠の「Selected」リストに追加します。「Selected」リストからメンバアカウントを削除するには、削除するメンバアカウントを選択して、「<<」をクリックします。

「OK」ボタンをクリックすると、新しいネットワークが作成されます。

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

Network の設定 / 編集

ネットワークを作成すると、左パネルの追加オプションが有効になります。これらのオプションは、「SSID」「VLAN」「Bandwidth Optimization」「RF Optimization」「Schedule」「Device settings」「Performance」「WLAN Partition」「Wireless resource」「SSL certificate」「Uploading Configuration」「Firmware Upgrade」を含み各項目に対して設定を行うことが可能です。

左パネルでネットワーク名をクリックすると、手動で設定可能なページが有効になり、設定した内容は選択したネットワーク上の有効な全てのアクセスポイントに適用されます。

注意 Configuration > Site (サイト名) > Network (ネットワーク名) でネットワーク選択時に最初に表示される画面は「SSID」の項目です。

SSID

本項目「SSID」では、作成したネットワークの無線ネットワークプロファイル「SSID」の作成、設定を行います。

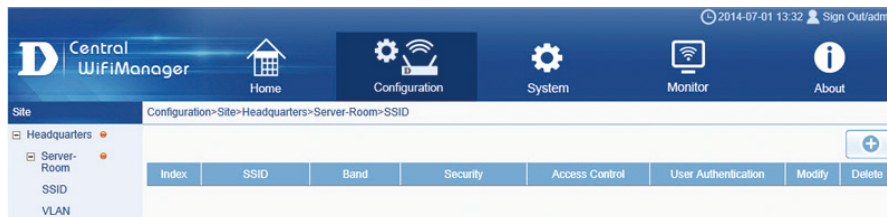


図 4-4 SSID (Configuration)

 をクリックすると、新しい SSID を追加します。

SSID 作成 / 編集

新しい SSID を追加すると、以下の画面が表示されます。既存の SSID の編集 (Modify) においても同様の項目が表示されます。

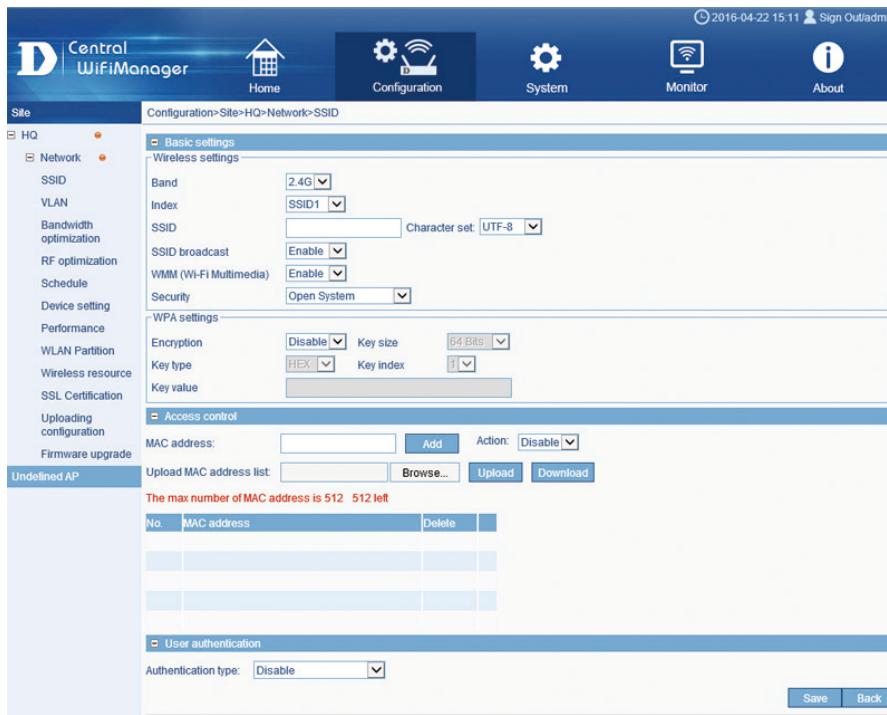


図 4-5 SSID 作成 / 編集

注意 CWM では一部の特殊文字 ("&") はサポート対象外となります。

Basic Settings（基本設定）

「Basic Settings」では、以下のパラメータが設定可能です。

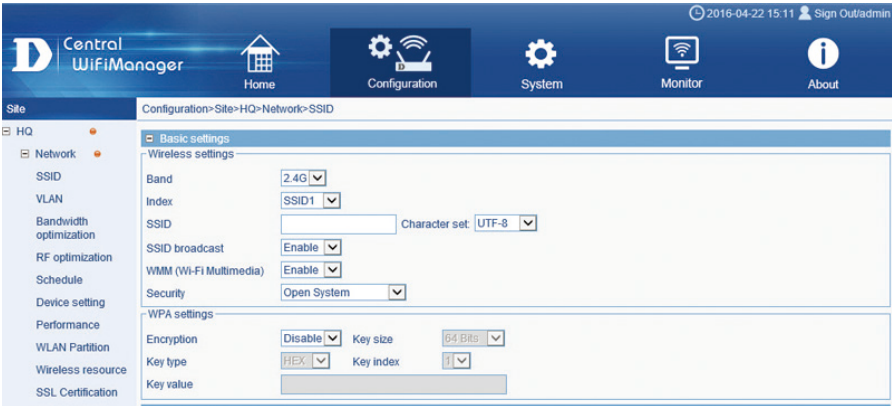


図 4-6 SSID 作成（Basic Settings）

以下の項目があります。

項目	説明
Band	このネットワークで使用する無線周波数帯域（2.4G または 5G）を選択します。
Index	ネットワークで使用する SSID インデックス「Primary」「SSID1 ～ SSID7」を選択します。
SSID	SSID 名を入力します。「Character set」で文字コードのコードセットを行います。
SSID Broadcast	無線 SSID の可視性を有効または無効にします。
WMM (Wi-Fi Multimedia)	WMM 機能を有効または無効にします。
Security	無線ネットワークで使用する無線セキュリティ「Open System」「Shared Key」「WPA-Personal」「WPA-Enterprise」「WPA2-Personal」「WPA2-Enterprise」「WPA-Auto-Personal」「WPA-Auto-Enterprise」から選択します。

ここでは、本アプリケーションで管理されるネットワークに有効な無線セキュリティオプションについて説明します。

Open System 選択時（Security）

無線セキュリティの方法として WEP「Open System」オプションを選択すると、以下のパラメータの設定が有効になります。

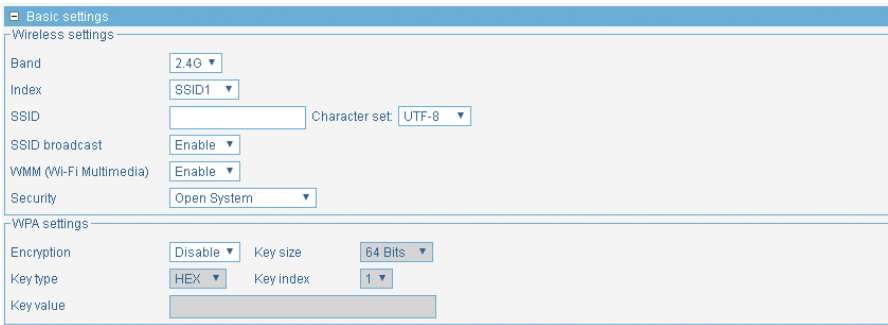


図 4-7 Open System（Security）

以下の項目があります。

項目	説明
Encryption	「WPA settings」でネットワークの WEP オープンシステムの暗号方式（有効または無効）を選択します。
Key Size	WEP キーサイズ (64Bits、128 Bit) を選択します。
Key Type	WEP キータイプ (HEX または ASCII) を選択します。
Key Index	4 つのインデックス (1-4) の内どのキーを使用するかを選択します。
Key Value	選択に基づき open system WEP 暗号キーを指定します。

Shared Key 選択時 (Security)

無線セキュリティの方法として WEP 「Shared Key」 オプションを選択すると、以下のパラメータの設定が有効になります。

図 4-8 Shared Key (Security)

以下の項目があります。

項目	説明
Encryption	ネットワークの WEP Shared Key の暗号方式（有効または無効）を選択します。
Key Size	WEP キーサイズ (64Bits、128 Bits、256 Bits) を選択します。
Key Type	WEP キータイプ（HEX または ASCII）を選択します。
Key Index	4 つのインデックス (First、Second、Third、Fourth) の内どのキーを使用するかを選択します。
Key Value	選択に基づき open system WEP 暗号キーを選択します。

WPA-Personal / WPA2-Personal / WPA-Auto-Personal 選択時 (Security)

無線セキュリティの方法として「WPA-Personal」「WPA2-Personal」「WPA-Auto-Personal」オプションを選択すると、以下のパラメータの設定が有効になります。

図 4-9 WPA-Personal (Security)

以下の項目があります。

項目	説明
Encryption Type	WPA の暗号タイプ（Auto、AES、TKIP）を選択します。
Group Key Update Interval	WPA グループキーの更新間隔値を入力します。初期値：3600
Passphrase	パスフレーズを入力します。

WPA-Enterprise / WPA2-Enterprise / WPA-Auto-Enterprise 選択時 (Security)

無線セキュリティの方法として「WPA-Enterprise」「WPA2-Enterprise」「WPA-Auto-Enterprise」オプションを選択すると、以下のパラメータの設定が有効になります。

Basic settings

Wireless settings

Band

2.4G

Index

SSID5

SSID

AAAA

Character set

UTF-8

SSID broadcast

Enable

WMM (Wi-Fi Multimedia)

Enable

Security

WPA-Enterprise

WPA settings

Encryption type

Auto

Group key update interval

3600

Primary RADIUS server settings

RADIUS server

Port

1812

RADIUS secret

Backup RADIUS server settings (optional)

RADIUS server

Port

1812

RADIUS secret

Primary accounting server settings

Accounting mode

Disable

Accounting server

Accounting port

1813

Accounting secret

Backup accounting server settings (optional)

Accounting server

Accounting port

1813

Accounting secret

図 4-10 WPA-Enterprise (Security)

以下の項目があります。

項目	説明
Encryption Type	WPA の暗号タイプ (Auto、AES、TKIP) を選択します。
Group Key Update Interval	WPA グループキーの更新間隔値を入力します。初期値：3600
Primary RADIUS server settings / Backup RADIUS server settings (optional)	
RADIUS Server	RADIUS サーバの IP アドレスを入力します。
Port	RADIUS サーバのポート番号を入力します。初期値：1812
RADIUS Secret	RADIUS のパスフレーズを入力します。
Primary accounting server settings / Backup accounting server settings (optional)	
Accounting mode	Accounting mode を有効 / 無効に指定します。
Accounting Server	Accounting サーバの IP アドレスを入力します。
Accounting Port	Accounting サーバのポート番号を入力します。初期値：1813
Accounting Secret	Accounting mode のパスフレーズを入力します。

注意

SSID の設定で「WPA-Enterprise」を選択し、設定する RADIUS サーバの IP アドレスと「Captive Portal」の IP インタフェースの設定画面で設定する DNS の IP アドレスが同じ場合、および「管理 VLAN」と「Captive Portal」の IP インタフェースの設定画面での VLAN が異なる場合には、「Captive Portal」は動作しません。

Access Control (アクセスコントロール)

「Access Control」では、ネットワークへのアクセスを承認または拒否するデバイスの MAC アドレスを指定することにより、ネットワークへのアクセスの可否をネットワークデバイスに設定することができます。

図 4-11 Access Control

以下の項目があります。

項目	説明
MAC Address	設定するネットワークデバイスの MAC アドレスを入力し「Add」でリストに追加します。
Action	ネットワークデバイスに適用するアクション (Disable (無効)、Accept (許可)、Reject (拒否)) を選択します。

「Upload」をクリックすると「.txt」で作成した MAC アドレスのリストをアップロードします。

「Download」をクリックすると登録した MAC アドレスの一覧を「.txt」のリストとしてダウンロードします。

設定したエントリの一覧は表に表示されます。「ゴミ箱」のアイコンをクリックすると指定のエントリを削除します。

User Authentication (ユーザ認証)

「User Authentication」では、ネットワーク上のアクセスポイントに接続するすべての無線クライアントに適用する認証方式を設定します。

図 4-12 User Authentication

以下の項目があります。

項目	説明
Authentication Type	ネットワーク上の無線クライアントに適用する認証タイプ (Disable、Web Redirection Only、Username/password、Remote RADIUS、LDAP、POP3、Passcode) を選択します。認証タイプとして無効 (Disable) を選択した場合は、本機能は無効となります。

Web Redirection Only 選択時 (Authentication Type)

「Authentication Type」として「Web Redirection Only」を選択した場合、ネットワーク上の各無線クライアントに適用するリダイレクション Web サイト URL を設定することができます。

図 4-13 Web Redirection Only

IP Interface Settings (Web Redirection) には以下の項目があります。

項目	説明
IPIF Status	IP インタフェースを有効 / 無効に指定します。
VLAN Group	VLAN グループ名を指定します。
Get IP From	IP アドレスの取得方法について「Static IP (Manual)」「Dynamic IP (DHCP)」から指定します。
IP Address	IP インタフェースの IP アドレスを入力します。
Subnet Mask	IP インタフェースのサブネットマスクを入力します。

Gateway	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの DNS アドレスを入力します。
Web redirection	チェックを入れ Web サイトリダイレクション機能を有効にします。
Website	HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。

「Save」ボタンをクリックすると、変更を適用します。「Back」ボタンをクリックすると、変更を破棄してメインページに戻ります。

Username/Password 選択時 (Authentication Type)

「Authentication Type」として「Username/password」を選択した場合、ネットワーク上の各無線クライアントにローカル認証を適用できます。ローカル認証では、認証プロセスのために外部サーバを必要としません。認証は制限されたサブネット、ユーザ名に基づいて適用され、パスワード認証は作成されたアカウントとそれらが属するグループに基づいて適用されます。



図 4-14 Username/password

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分

IP filter settings

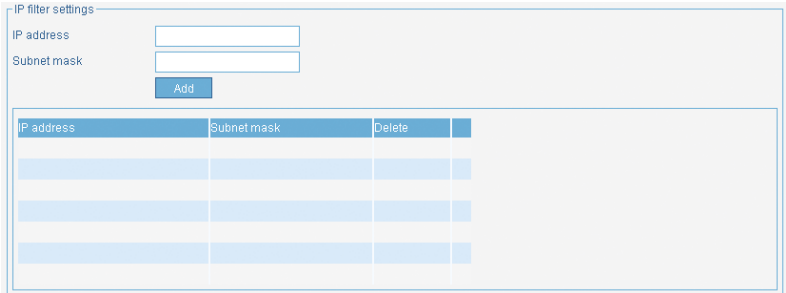


図 4-15 IP filter settings

「IP filter settings」には以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分
IP Address	IP アドレスまたは IP フィルタ規則で使用するネットワークのアドレスを入力します。例：192.168.70.66 などの IP アドレス、または 192.168.70.0 などのネットワークアドレス。この IP アドレスまたはネットワークはネットワーク上の無線クライアントにアクセスできません。
Subnet Mask	フィルタする IP アドレスまたはネットワークアドレスのサブネットマスクを入力します。例：255.255.255.0

「Add」ボタンをクリックすると、新しい IP フィルタ規則を追加します。🗑️のアイコンをクリックすると指定のエントリを削除します。

IP Interface Settings

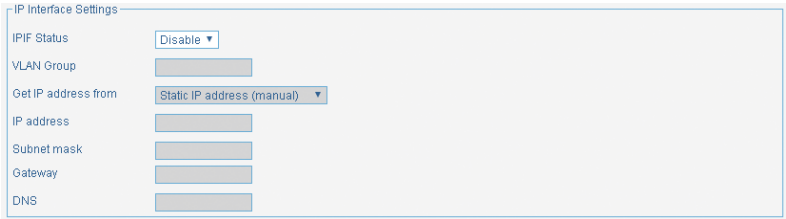


図 4-16 IP Interface Settings

「IP Interface Settings」には以下の項目があります。

項目	説明
IPIF Status	IP インタフェースを有効 / 無効に指定します。
VLAN Group	VLAN グループ名を指定します。
Get IP From	IP アドレスの取得方法について「Static IP (Manual)」「Dynamic IP (DHCP)」から指定します。

IP Address	IP インタフェースの IP アドレスを入力します。
Subnet Mask	IP インタフェースのサブネットマスクを入力します。
Gateway	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの DNS アドレスを入力します。

User/password settings

The screenshot shows a web interface for 'User/password settings'. It includes input fields for 'Username' and 'Password', followed by 'Add' and 'Clear' buttons. Below these is a table with three columns: 'Username', 'Modify', and 'Delete'. The table currently contains three empty rows.

図 4-17 User/password settings

「User/password settings」には以下の項目があります。

項目	説明
Username	使用する無線クライアントのユーザ名を入力します。
Password	使用する無線クライアントのパスワードを入力します。

「Add」ボタンをクリックすると、新しいユーザアカウントを追加します。

「Clear」ボタンをクリックすると、フィールドに入力した情報をクリアします。

アイコンをクリックすると、既存のアカウントを修正します。 アイコンをクリックすると、既存のユーザアカウントを削除します。

Web redirection

The screenshot shows a web interface for 'Web redirection'. It features a checkbox labeled 'Web redirection' which is checked. Below it is a 'Website' field with a dropdown menu currently set to 'http://' and an empty text input box for the URL.

図 4-18 Web redirection

「Web redirection」には以下の項目があります。

項目	説明
Web redirection	チェックを入れ Web サイトリダイレクション機能を有効にします。
Website	HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。

Splash page customization

The screenshot shows a web interface for 'Splash page customization'. It includes a 'Choose template' dropdown menu set to 'pages_default'. To the right are four buttons: 'Preview', 'Upload login file', 'Delete the template', and 'Download template'.

図 4-19 Splash page customization

「Splash page customization」には以下の項目があります。

項目	説明
Choose template	使用するログインページのスタイルを選択します。

スタイルを選択した後、「Preview」ボタンをクリックすると選択したスタイルをプレビューします。

「Upload login file」ボタンをクリックすると、新しいスタイルをアップロードします。

「Delete the style」リンクをクリックすると、選択したスタイルを削除します。

「Download Template」リンクをクリックすると、スタイルテンプレートをダウンロードします。

Enable white list

図 4-20 Enable white list

「Enable white list」には以下の項目があります。

項目	説明
Enable White List	ホワイトリスト機能を有効にします。ネットワークデバイスの MAC アドレスを指定することにより、ネットワークへの接続を許可するネットワークデバイスを設定します。
MAC Address	ネットワークへの接続を許可するネットワークデバイスの MAC アドレスを入力します。「Add」をクリックすると、MAC アドレスをホワイトリスト表に追加します。
Upload White List File	ホワイトリストファイルをアップロードするには、「Browse」をクリックしてホワイトリストファイルを指定し、コンピュータに保存後「Upload」をクリックします。

「Save」ボタンをクリックすると、変更を適用します。「Back」ボタンをクリックすると、変更を破棄してメインページに戻ります。

Remote RADIUS (Authentication Type)

「Authentication Type」として「Remote RADIUS」を選択した場合、このネットワーク上のアクセスポイントをネットワークにインストールされた追加の RADIUS サーバと通信し認証メッセージをリレーする認証デバイスとして機能するように設定することができます。

図 4-21 Remote RADIUS

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分

IP filter settings

図 4-22 IP filter settings

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分
IP Address	IP アドレスまたは IP フィルタ規則で使用するネットワークのアドレスを入力します。例：192.168.70.66 などの IP アドレス、または 192.168.70.0 などのネットワークアドレス この IP アドレスまたはネットワークはネットワーク上の無線クライアントにアクセスできません。
Subnet Mask	フィルタする IP アドレスまたはネットワークアドレスのサブネットマスクを入力します。例：255.255.255.0

「Add」ボタンをクリックすると、新しい IP フィルタ規則を追加します。🗑️ アイコンをクリックすると、既存のエントリを削除します。

IP Interface Settings

IP Interface Settings

IPIF Status: Disable ▼

VLAN Group: []

Get IP address from: Static IP address (manual) ▼

IP address: []

Subnet mask: []

Gateway: []

DNS: []

図 4-23 IP Interface Settings

「IP Interface Settings」には以下の項目があります。

項目	説明
IPIF Status	IP インタフェースを有効 / 無効に指定します。
VLAN Group	VLAN グループ名を指定します。
Get IP From	IP アドレスの取得方法について「Static IP (Manual)」「Dynamic IP (DHCP)」から指定します。
IP Address	IP インタフェースの IP アドレスを入力します。
Subnet Mask	IP インタフェースのサブネットマスクを入力します。
Gateway	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの DNS アドレスを入力します。

Remote RADIUS Settings

Remote RADIUS settings

RADIUS server settings

RADIUS server: [] RADIUS port: 1812 (1~65535)

RADIUS secret: []

Remote RADIUS type: SPAP ▼

Secondary RADIUS server settings

RADIUS server: [] RADIUS port: 1812 (1~65535)

RADIUS secret: []

Remote RADIUS type: SPAP ▼

Third RADIUS server settings

RADIUS server: [] RADIUS port: 1812 (1~65535)

RADIUS secret: []

Remote RADIUS type: SPAP ▼

図 4-24 Remote RADIUS Settings

以下の項目があります。

項目	説明
RADIUS Server	Primary、Secondary、または Third の RADIUS サーバの IP アドレスを入力します。
RADIUS Port	Primary、Secondary、または Third の RADIUS サーバのポート番号を入力します。初期値：1812
RADIUS Secret	Primary、Secondary、または Third の RADIUS サーバの暗号を入力します。
Remote RADIUS type	Primary、Secondary、または Third の RADIUS サーバタイプ (SPAP、MSCHAPv2) を入力します。

Web redirection

Web redirection ☒

Website: http:// []

図 4-25 Web redirection

「Web redirection」には以下の項目があります。

項目	説明
Web redirection	チェックを入れ Web サイトリダイレクション機能を有効にします。
Website	HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。

Splash page customization



図 4-26 Splash page customization

「Splash page customization」には以下の項目があります。

項目	説明
Choose template	使用するログインページのスタイルを選択します。

スタイルを選択した後、「Preview」ボタンをクリックすると選択したスタイルをプレビューします。
「Upload login file」ボタンをクリックすると、新しいスタイルをアップロードします。
「Delete the style」リンクをクリックすると、選択したスタイルを削除します。
「Download Template」リンクをクリックすると、スタイルテンプレートをダウンロードします。

Enable white list

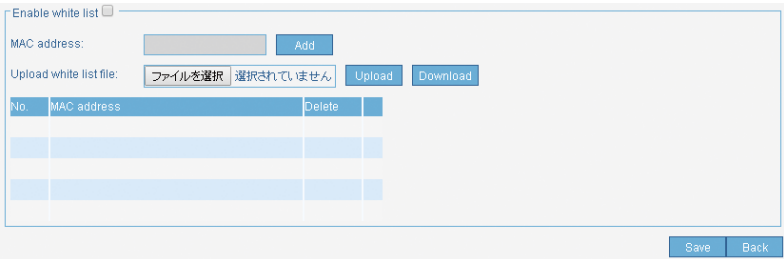


図 4-27 Enable white list

「Enable white list」には以下の項目があります。

項目	説明
Enable White List	ホワイトリスト機能を有効にします。ネットワークデバイスの MAC アドレスを指定することにより、ネットワークへの接続を許可するネットワークデバイスを設定します。
MAC Address	ネットワークへの接続を許可するネットワークデバイスの MAC アドレスを入力します。「Add」をクリックすると、MAC アドレスをホワイトリスト表に追加します。
Upload White List File	ホワイトリストファイルをアップロードするには、「Browse」をクリックしてホワイトリストファイルを指定し、コンピュータに保存後「Upload」をクリックします。

「Save」ボタンをクリックすると、変更を適用します。「Back」ボタンをクリックすると、変更を破棄してメインページに戻ります。

LDAP 選択時 (Authentication Type)

「Authentication Type」として「LDAP」を選択した場合、ネットワークのユーザ認証を処理するために追加の LDAP サーバを使用するアクセスポイントを設定することができます。



図 4-28 LDAP

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分

IP filter settings

IP filter settings

IP address

Subnet mask

IP address	Subnet mask	Delete

図 4-29 IP filter settings

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分
IP Address	IP アドレスまたは IP フィルタ規則で使用するネットワークのアドレスを入力します。例：192.168.70.66 などの IP アドレス、または 192.168.70.0 などのネットワークアドレス この IP アドレスまたはネットワークはネットワーク上の無線クライアントにアクセスできません。
Subnet Mask	フィルタする IP アドレスまたはネットワークアドレスのサブネットマスクを入力します。例：255.255.255.0

「Add」ボタンをクリックすると、新しい IP フィルタ規則を追加します。  アイコンをクリックすると、既存のエントリを削除します。

IP Interface Settings

IP Interface Settings

IPIF Status

VLAN Group

Get IP address from

IP address

Subnet mask

Gateway

DNS

図 4-30 IP Interface Settings

「IP Interface Settings」には以下の項目があります。

項目	説明
IPIF Status	IP インタフェースを有効 / 無効に指定します。
VLAN Group	VLAN グループ名を指定します。
Get IP From	IP アドレスの取得方法について「Static IP (Manual)」「Dynamic IP (DHCP)」から指定します。
IP Address	IP インタフェースの IP アドレスを入力します。
Subnet Mask	IP インタフェースのサブネットマスクを入力します。
Gateway	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの DNS アドレスを入力します。

LDAP Settings

LDAP settings

Server

Port

Authentication mode

Username

Password

Base DN (ou=,dc=)

Account attribute (ex.cn)

Identity ☐ Auto copy

図 4-31 LDAP Settings

以下の項目があります。

項目	説明
Server	LDAP サーバの IP アドレスを入力します。
Port	使用する LDAP サーバのポート番号を入力します。
Authenticate Mode	使用する認証モード（「Simple」、「TLS」）を選択します。
Username	LDAP データベースにアクセス並びに検索可能な管理者のユーザ名を入力します。

Password	LDAP データベースにアクセス並びに検索可能な管理者のパスワードを入力します。
Base DN	LDAP データベースのベースドメイン名を入力します。例：「cn=users」、「dc=test」、「dc=com」は、無線クライアントがドメイン「test.com」の「users」グループのメンバであることを意味します。
Account Attribute	アカウントの属性を入力します。例：「cn」は、Windows サーバで使用されることを意味します。
Identity	管理者名を入力します。例：「cn=Administrator」、「cn=users」、「dc=test」、「dc=com」

Web redirection

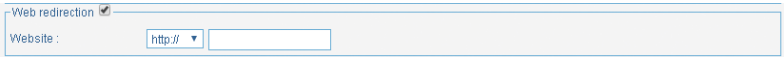


図 4-32 Web redirection

「Web redirection」には以下の項目があります。

項目	説明
Web redirection	チェックを入れ Web サイトリダイレクション機能を有効にします。
Website	HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。

Splash page customization

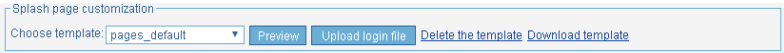


図 4-33 Splash page customization

「Splash page customization」には以下の項目があります。

項目	説明
Choose template	使用するログインページのスタイルを選択します。

スタイルを選択した後、「Preview」ボタンをクリックすると選択したスタイルをプレビューします。

「Upload login file」ボタンをクリックすると、新しいスタイルをアップロードします。

「Delete the style」リンクをクリックすると、選択したスタイルを削除します。

「Download Template」リンクをクリックすると、スタイルテンプレートをダウンロードします。

Enable white list

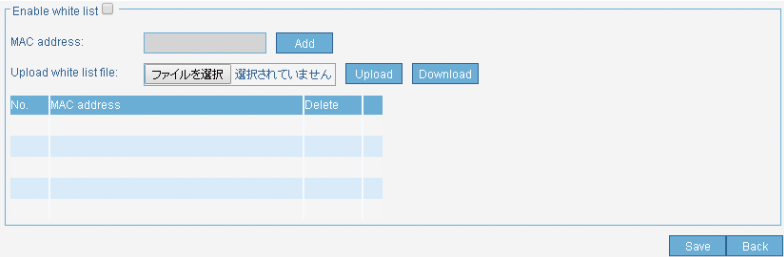


図 4-34 Enable white list

「Enable white list」には以下の項目があります。

項目	説明
Enable White List	ホワイトリスト機能を有効にします。ネットワークデバイスの MAC アドレスを指定することにより、ネットワークへの接続を許可するネットワークデバイスを設定します。
MAC Address	ネットワークへの接続を許可するネットワークデバイスの MAC アドレスを入力します。「Add」をクリックすると、MAC アドレスをホワイトリスト表に追加します。
Upload White List File	ホワイトリストファイルをアップロードするには、「Browse」をクリックしてホワイトリストファイルを指定し、コンピュータに保存後「Upload」をクリックします。

「Save」ボタンをクリックすると、変更を適用します。「Back」ボタンをクリックすると、変更を破棄してメインページに戻ります。

POP3 選択時 (Authentication Type)

「Authentication Type」として「POP3」を選択した場合、ネットワークのユーザ認証を処理するために追加の POP3 サーバを使用するアクセスポイントを設定することができます。

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分

IP filter settings

図 4-36 IP filter settings

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分
IP Address	IP アドレスまたは IP フィルタ規則で使用するネットワークのアドレスを入力します。例：192.168.70.66 などの IP アドレス、または 192.168.70.0 などのネットワークアドレス この IP アドレスまたはネットワークはネットワーク上の無線クライアントにアクセスできません。
Subnet Mask	フィルタする IP アドレスまたはネットワークアドレスのサブネットマスクを入力します。例：255.255.255.0

「Add」ボタンをクリックすると、新しい IP フィルタ規則を追加します。🗑️ アイコンをクリックすると、既存のエントリを削除します。

IP Interface Settings

図 4-37 IP Interface Settings

「IP Interface Settings」には以下の項目があります。

項目	説明
IPIF Status	IP インタフェースを有効 / 無効に指定します。
VLAN Group	VLAN グループ名を指定します。
Get IP From	IP アドレスの取得方法について「Static IP (Manual)」「Dynamic IP (DHCP)」から指定します。
IP Address	IP インタフェースの IP アドレスを入力します。
Subnet Mask	IP インタフェースのサブネットマスクを入力します。
Gateway	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの DNS アドレスを入力します。

POP3 Settings

POP3 settings

Server

Port:

110

(1~65535)

Connection type

None

図 4-38 POP3 Settings

以下の項目があります。

項目	説明
Server	POP3 サーバの IP アドレスを入力します。
Port	使用する POP3 サーバのポート番号を入力します。初期値：110 SSL/TLS 接続タイプの初期値は 995
Connection Type	POP3 接続タイプ（None、SSL/TLS）を選択します。

Web redirection

Web redirection ☒

Website :

http://

図 4-39 Web redirection

「Web redirection」には以下の項目があります。

項目	説明
Web redirection	チェックを入れ Web サイトリダイレクション機能を有効にします。
Website	HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。

Splash page customization

Splash page customization

Choose template:

pages_default

Preview

Upload login file

Delete the template

Download template

図 4-40 Splash page customization

「Splash page customization」には以下の項目があります。

項目	説明
Choose template	使用するログインページのスタイルを選択します。

スタイルを選択した後、「Preview」ボタンをクリックすると選択したスタイルをプレビューします。
「Upload login file」ボタンをクリックすると、新しいスタイルをアップロードします。
「Delete the style」リンクをクリックすると、選択したスタイルを削除します。
「Download Template」リンクをクリックすると、スタイルテンプレートをダウンロードします。

Enable white list

Enable white list ☐

MAC address:

Add

Upload white list file:

ファイルを選択

選択されていません

Upload

Download

No.	MAC address	Delete

Save

Back

図 4-41 Enable white list

「Enable white list」には以下の項目があります。

項目	説明
Enable White List	ホワイトリスト機能を有効にします。ネットワークデバイスの MAC アドレスを指定することにより、ネットワークへの接続を許可するネットワークデバイスを設定します。
MAC Address	ネットワークへの接続を許可するネットワークデバイスの MAC アドレスを入力します。「Add」をクリックすると、MAC アドレスをホワイトリスト表に追加します。
Upload White List File	ホワイトリストファイルをアップロードするには、「Browse」をクリックしてホワイトリストファイルを指定し、コンピュータに保存後「Upload」をクリックします。

「Save」ボタンをクリックすると、変更を適用します。「Back」ボタンをクリックすると、変更を破棄してメインページに戻ります。

Passcode 選択時 (Authentication Type)

「Authentication Type」として「Passcode」を選択した場合、以下のセクションの確認と設定ができます。

図 4-42 Passcode

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分

IP filter settings

図 4-43 IP filter settings

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分
IP Address	IP アドレスまたは IP フィルタ規則で使用するネットワークのアドレスを入力します。例：192.168.70.66 などの IP アドレス、または 192.168.70.0 などのネットワークアドレス この IP アドレスまたはネットワークはネットワーク上の無線クライアントにアクセスできません。
Subnet Mask	フィルタする IP アドレスまたはネットワークアドレスのサブネットマスクを入力します。例：255.255.255.0

「Add」ボタンをクリックすると、新しい IP フィルタ規則を追加します。🗑️ アイコンをクリックすると、既存のエントリを削除します。

IP Interface Settings

図 4-44 IP Interface Settings

「IP Interface Settings」には以下の項目があります。

項目	説明
IPIF Status	IP インタフェースを有効 / 無効に指定します。
VLAN Group	VLAN グループ名を指定します。
Get IP From	IP アドレスの取得方法について「Static IP (Manual)」「Dynamic IP (DHCP)」から指定します。
IP Address	IP インタフェースの IP アドレスを入力します。
Subnet Mask	IP インタフェースのサブネットマスクを入力します。
Gateway	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの DNS アドレスを入力します。

Passcode List

Passcode list								
Passcode	SSID	Duration	User limit	Last active day	Duration remaining	Creator	Status	

図 4-45 Passcode list

設定したパスコードのリストが表示されます。

Web redirection

Web redirection ☒

Website:

http://

図 4-46 Web redirection

「Web redirection」には以下の項目があります。

項目	説明
Web redirection	チェックを入れ Web サイトリダイレクション機能を有効にします。
Website	HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。

Splash page customization

Splash page customization

Choose template:

pages_default

Preview

Upload login file

Delete the template

Download template

図 4-47 Splash page customization

「Splash page customization」には以下の項目があります。

項目	説明
Choose template	使用するログインページのスタイルを選択します。

スタイルを選択した後、「Preview」ボタンをクリックすると選択したスタイルをプレビューします。
「Upload login file」ボタンをクリックすると、新しいスタイルをアップロードします。
「Delete the style」リンクをクリックすると、選択したスタイルを削除します。
「Download Template」リンクをクリックすると、スタイルテンプレートをダウンロードします。

Enable white list

Enable white list ☐

MAC address:

Add

Upload white list file:

ファイルを選択

選択されていません

Upload

Download

No.	MAC address	Delete

Save

Back

図 4-48 Enable white list

「Enable white list」には以下の項目があります。

項目	説明
Enable White List	ホワイトリスト機能を有効にします。ネットワークデバイスの MAC アドレスを指定することにより、ネットワークへの接続を許可するネットワークデバイスを設定します。
MAC Address	ネットワークへの接続を許可するネットワークデバイスの MAC アドレスを入力します。「Add」をクリックすると、MAC アドレスをホワイトリスト表に追加します。
Upload White List File	ホワイトリストファイルをアップロードするには、「Browse」をクリックしてホワイトリストファイルを指定し、コンピュータに保存後「Upload」をクリックします。

「Save」ボタンをクリックすると、変更を適用します。「Back」ボタンをクリックすると、変更を破棄してメインページに戻ります。

External Captive Portal 選択時 (Authentication Type)

「Authentication Type」として「External Captive Portal」を選択した場合、以下のセクションの確認と設定ができます。

図 4-49 External Captive Portal

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分

IP filter settings

図 4-50 IP filter settings

以下の項目があります。

項目	説明
Session timeout	セッションのタイムアウト値（1 ～ 1440 分）を入力します。初期値：60 分
IP Address	IP アドレスまたは IP フィルタ規則で使用するネットワークのアドレスを入力します。例：192.168.70.66 などの IP アドレス、または 192.168.70.0 などのネットワークアドレス この IP アドレスまたはネットワークはネットワーク上の無線クライアントにアクセスできません。
Subnet Mask	フィルタする IP アドレスまたはネットワークアドレスのサブネットマスクを入力します。例：255.255.255.0

「Add」ボタンをクリックすると、新しい IP フィルタ規則を追加します。🗑️ アイコンをクリックすると、既存のエントリを削除します。

IP Interface Settings

図 4-51 IP Interface Settings

「IP Interface Settings」には以下の項目があります。

項目	説明
IPIF Status	IP インタフェースを有効 / 無効に指定します。
VLAN Group	VLAN グループ名を指定します。
Get IP From	IP アドレスの取得方法について「Static IP (Manual)」「Dynamic IP (DHCP)」から指定します。
IP Address	IP インタフェースの IP アドレスを入力します。
Subnet Mask	IP インタフェースのサブネットマスクを入力します。
Gateway	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの DNS アドレスを入力します。

注意 SSID の設定で「WPA-Enterprise」を選択し、設定する RADIUS サーバの IP アドレスと「Captive Portal」の IP インタフェースの設定画面で設定する DNS の IP アドレスが同じ場合、および「管理 VLAN」と「Captive Portal」の IP インタフェースの設定画面での VLAN が異なる場合には、「Captive Portal」は動作しません。

External Captive Portal

External Captive Portal Server address: http://

Web redirection ☒

Website : http://

図 4-52 External Captive Portal Server address / Web redirection

「External Captive Portal Server address / Web redirection」には以下の項目があります。

項目	説明
External Captive Portal Server address	外部キャプティブポータルサーバアドレスを入力します。 HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。
Web redirection	チェックを入れ Web サイトリダイレクション機能を有効にします。
Website	HTTP または HTTPS のどちらかを選択します。http:// または https:// のどちらかを選択した後、空欄に Web サイトの URL を入力します。

Enable white list

Enable white list ☐

MAC address: Add

Upload white list file: ファイルを選択 選択されていません Upload Download

No.	MAC address	Delete

Save Back

図 4-53 Enable white list

「Enable white list」には以下の項目があります。

項目	説明
Enable White List	ホワイトリスト機能を有効にします。ネットワークデバイスの MAC アドレスを指定することにより、ネットワークへの接続を許可するネットワークデバイスを設定します。
MAC Address	ネットワークへの接続を許可するネットワークデバイスの MAC アドレスを入力します。「Add」をクリックすると、MAC アドレスをホワイトリスト表に追加します。
Upload White List File	ホワイトリストファイルをアップロードするには、「Browse」をクリックしてホワイトリストファイルを指定し、コンピュータに保存後「Upload」をクリックします。

「Save」ボタンをクリックすると、変更を適用します。「Back」ボタンをクリックすると、変更を破棄してメインページに戻ります。

作成した SSID が表示されます。

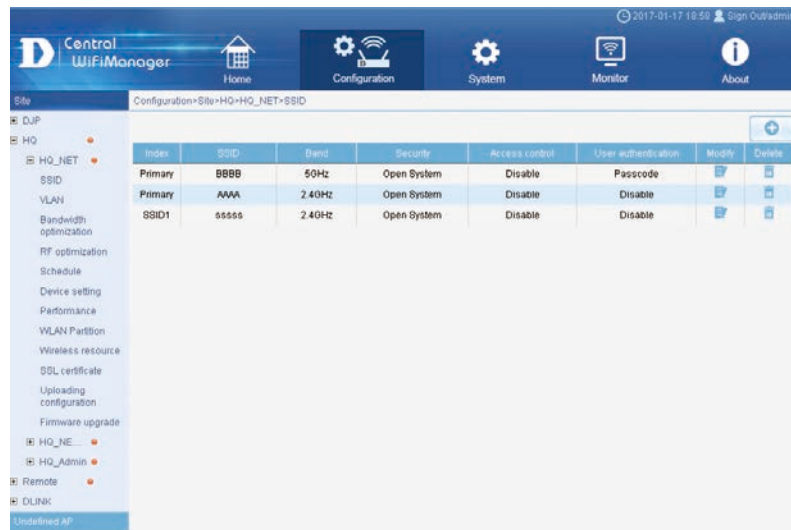


図 4-54 SSID

- アイコンをクリックすると、新しい SSID を追加します。
- アイコンをクリックすると、既存の SSID 修正します。
- アイコンをクリックすると、既存の SSID を削除します。

VLAN

本項目「VLAN」では、作成したネットワークへの「VLAN」の作成、設定を行います。

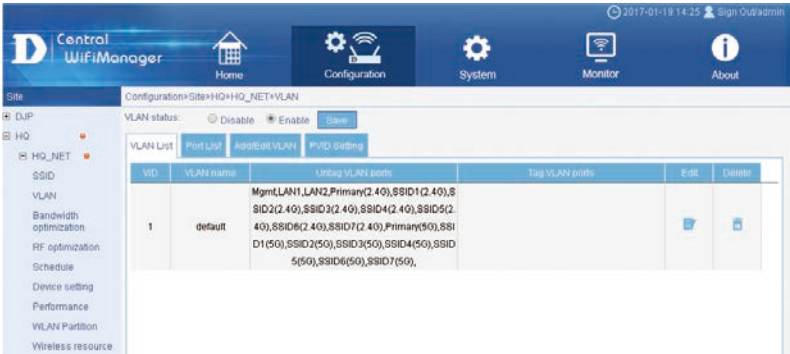


図 4-55 VLAN

タブの設定の前に、以下のパラメータが設定可能です。
以下の項目があります。

項目	説明
VLAN Status	VLAN の「Enable」（有効）または「Disable」（無効）を選択します。

「Save」ボタンをクリックすると変更を適用します。

「VLAN Status」を有効にした後、ネットワークのアクセスポイントで管理された仮想 LAN（VLAN）を作成、確認、設定ができます。

VLAN List タブ

「VLAN List」タブには作成した VLAN の一覧が表示されます。

VLAN List	Port List	Add/Edit VLAN	PVID Setting
VID	VLAN name	Untag VLAN ports	Tag VLAN po
1	default	Mgmt,LAN1,LAN2,Primary(2.4G),SSID1(2.4G),SSID2(2.4G),SSID3(2.4G),SSID4(2.4G),SSID5(2.4G),SSID6(2.4G),SSID7(2.4G),Primary(5G),SSID1(5G),SSID2(5G),SSID3(5G),SSID4(5G),SSID5(5G),SSID6(5G),SSID7(5G),	

図 4-56 VLAN List

「Edit」ボタンをクリックすると、既存の VLAN を修正します。詳細は「Add/Edit」タブを参照。
「Delete」ボタンをクリックすると、既存の VLAN を削除します。

Port List タブ

「Port List」タブには、ネットワーク上のアクセスポイントにおいて有効なすべてのポートが表示されます。

Configuration>Site>HQ>HQ_NET>VLAN			
VLAN status: ☐ Disable ☒ Enable Save			
VLAN List	Port List	Add/Edit VLAN	PVID Setting
Port name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN1		1	1
LAN2		1	1
Primary(2.4G)		1	1
Primary(5G)		1	1

図 4-57 Port List

「Port Name」エントリの隣の列には、ポートが属する VLAN の VLAN ID 番号が表示されます。
番号の列には、VLAN のタグ付けされたメンバ「Tag VID」またはタグなしメンバ「Untag VID」かを示します。
最後の列には、特定のポートの「PVID」番号が表示されます。

Add/Edit VLAN タブ

「Add/Edit VLAN」タブでは、新しい VLAN の作成と VLAN 上の各ポートへポートメンバを割り当てることができます。「Modify」アイコンをクリックすると、「VLAN List」タブにおいて既存の VLAN を修正するためにこのタブはリダイレクトされます。

図 4-58 Add/Edit VLAN

以下の項目があります。

項目	説明
VLAN ID (VID)	VLAN ID を入力します。
VLAN Name	VLAN 名を入力します。
Port	このコラムの各ポートのメンバシップオプションを選択します。ネットワーク上の VLAN のポートは、タグなしメンバ (Untag) タグ付きメンバ (Tag)、非メンバ (Not Member) のいずれかを設定できます。
Select All	クリックすると表上のすべてのポートを「Untag」、「Tag」、「Not Member」のいずれかに変更します。
Mgmt	アクセスポイントの管理ポートです。
LAN1 ~ LAN2	アクセスポイントの LAN ポートです。アクセスポイントが 1 つの LAN ポートしか持たない場合、LAN1 となります。
Primary	ネットワーク上のアクセスポイントのプライマリ WLAN SSID です。
SSID1 ~ SSID7	ネットワーク上のアクセスポイントのセカンダリ WLAN SSID です。

「Save」ボタンをクリックすると、変更を適用します。

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

PVID Setting タブ

「PVID Setting」タブでは、ネットワーク上のアクセスポイントと無線クライアントのポート VLAN 識別子 (PVID) の確認と設定ができます。

図 4-59 PVID Setting

以下の項目があります。

項目	説明
PVID Auto Assign Status	PVID の自動割り当てステータス機能を「Enable」(有効) または「Disable」(無効) にします。
Mgmt	アクセスポイントの管理ポートです。
LAN1 ~ LAN2	アクセスポイントの LAN ポートです。アクセスポイントが 1 つの LAN ポートしか持たない場合、LAN1 となります。
Primary	ネットワーク上のアクセスポイントのプライマリ WLAN SSID です。
SSID1 ~ SSID7	ネットワーク上のアクセスポイントのセカンダリ WLAN SSID です。

「Save」ボタンをクリックすると、変更を適用します。

Bandwidth Optimization（帯域最適化）

「Bandwidth Optimization」をクリックすると、以下のページが有効になります。本項目では、ネットワークのアクセスポイントの帯域幅の確認と設定ができます。

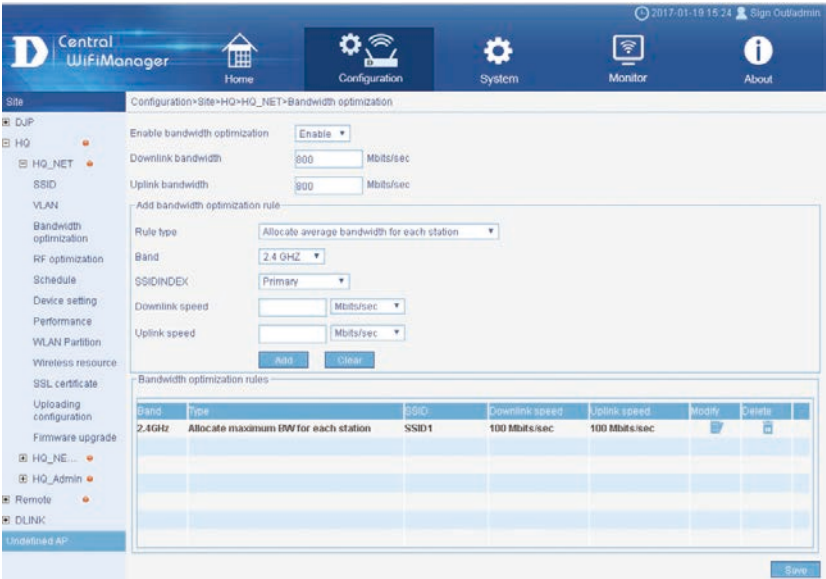


図 4-60 Bandwidth Optimization

以下の項目があります。

項目	説明
Enable Bandwidth Optimization	帯域最適化機能を「Enable」（有効）または「Disable」（無効）にします。
Downlink Bandwidth	ネットワーク上のアクセスポイントのダウンリンク帯域幅スピードの合計を Mbits/ 秒で入力します。
Uplink Bandwidth	ネットワーク上のアクセスポイントのアップリンク帯域幅スピードの合計を Mbits/ 秒で入力します。
Add bandwidth optimization rule	
Rule Type	作成または修正する規則のタイプを選択します。 「Allocate average BW for each station」 AP は各クライアントに平均帯域幅を分配します。 「Allocate maximum BW for each station」 接続された各クライアントに最大帯域幅を指定します。今後のクライアントのための準備特定帯域幅 「Allocate different BW for 11a/b/g/n station」 802.11b/g/n、802.11a/n クライアントのウェイトは「10%/20%/70%」、「20%/80%」。AP は 802.11a/b/g/n クライアントに異なる帯域幅を分配します。 「Allocate specific BW for SSID」：すべてのクライアントは合計帯域幅を共有します。
Band	規則で使用する無線周波数帯域（2.4Ghz または 5GHz）を選択します。
SSIDINDEX	使用する SSID（Primary、SSID1 ～ SSID7）を選択します。
Downlink Speed	各ステーションまたは特定の SSID に割り当てられるダウンリンクスピード値（Mbits/ 秒または Kbits/ 秒）を入力します。
Uplink Speed	各ステーションまたは特定の SSID に割り当てられるアップリンクスピード値（Mbits/ 秒または Kbits/ 秒）を入力します。

「Add」ボタンをクリックすると、「Bandwidth Optimization Rules」の一覧に新しい規則を追加します。

「Clear」ボタンをクリックすると、フィールドに入力したすべての情報をクリアします。

「Save」ボタンをクリックすると、変更を適用します。

 アイコンをクリックすると、既存のエントリを修正します。

 アイコンをクリックすると、既存のエントリを削除します。

RF optimization (無線周波数最適化)

「RF」をクリックすると以下の項目が表示されます。本項目では、ネットワーク上のアクセスポイントで使用する高周波 (RF) の確認と最適化ができます。

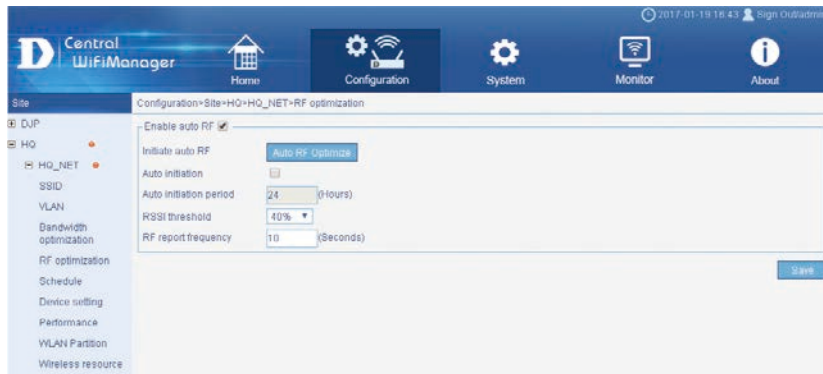


図 4-61 RF

以下の項目があります。

項目	説明
Enable Auto RF	RF 最適化機能を有効にします。
Init Auto RF	「Auto RF Optimize」ボタンをクリックすると手動で自動 RF 最適化機能を開始します。AP は自動的に最適なチャネルを選択します。
Auto initiation	入力した期間に基づき定期的に RF 最適化を行います。開始期間終了後、AP は自動的に最適なチャネルを選択します。
Auto initiation period	「Auto initiation」オプションを有効にした後、自動開始期間値を時間で入力します。
RSSI Threshold	ネットワークの RSSI しきい値を選択します。値は 10% ～ 100% で 10%刻みで増加します。AP はチャネルまたは電力を調整し、スキャン後、指定したしきい値以下の RSSI でネットワークの AP を検出します。
RF Report Frequency	RF レポートが生成される周波数値を秒で入力します。AP はチャネルまたは電力を指定した周波数で調整します。

「Save」ボタンをクリックすると、変更を適用します。

Schedule（スケジュール）

「Schedule」をクリックすると以下の項目が表示されます。本項目では、ネットワーク上のスケジュールを設定、表示します。

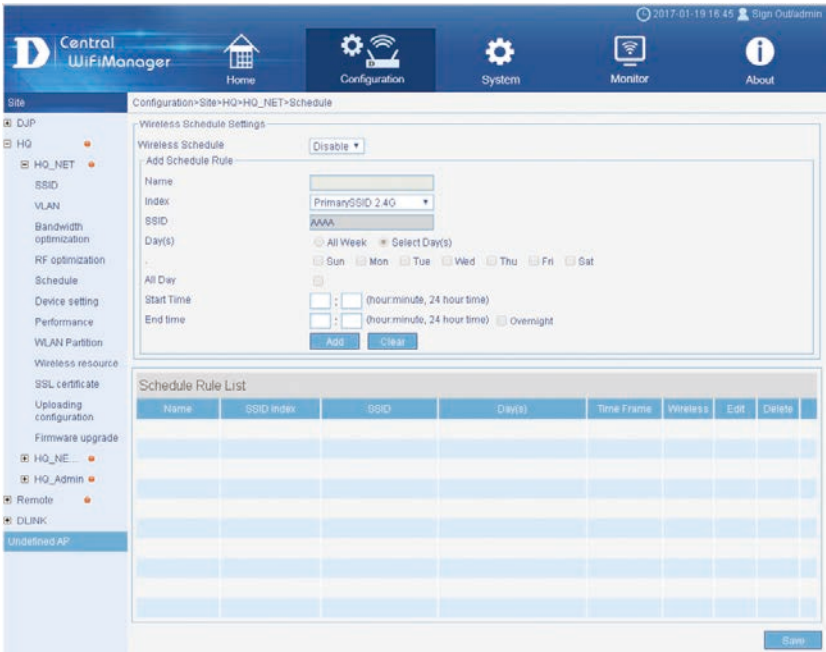


図 4-62 Schedule

以下の項目があります。

項目	説明
Wireless Schedule	スケジュール機能を有効 / 無効に指定します。
Name	スケジュール名を入力します。
Index	スケジュールのルールが適用される SSID を指定します。
Day(s)	スケジュールが有効になる日にちを指定します。 「All Week」 - 一週間通してスケジュールのルールを有効にします。 「Select Day(s)」 - スケジュールのルールが適用される曜日を指定します。
All Day	一日中ルールを有効にします。
Start Time	スケジュールルールが有効になる開始時間を指定します。 指定欄に「時」 / 「分」を入力します。
End Time	スケジュールルールが有効になる終了時間を指定します。 指定欄に「時」 / 「分」を入力します。 「Overnight」を指定すると夜中の間もずっとスケジュールルールは有効になります。

「Save」ボタンをクリックすると、変更を適用します。

 アイコンをクリックすると、既存のエントリを修正します。  アイコンをクリックすると、既存のエントリを削除します。

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

Device Settings (デバイス設定)

「Device Settings」をクリックすると、以下のページが有効になります。本項目ではネットワーク上のアクセスポイントのログインとアクセシビリティの確認と設定ができます。また、いくつかの高度な無線設定は 2.4GHz と 5GHz の両方の周波数帯に対して設定することができます。

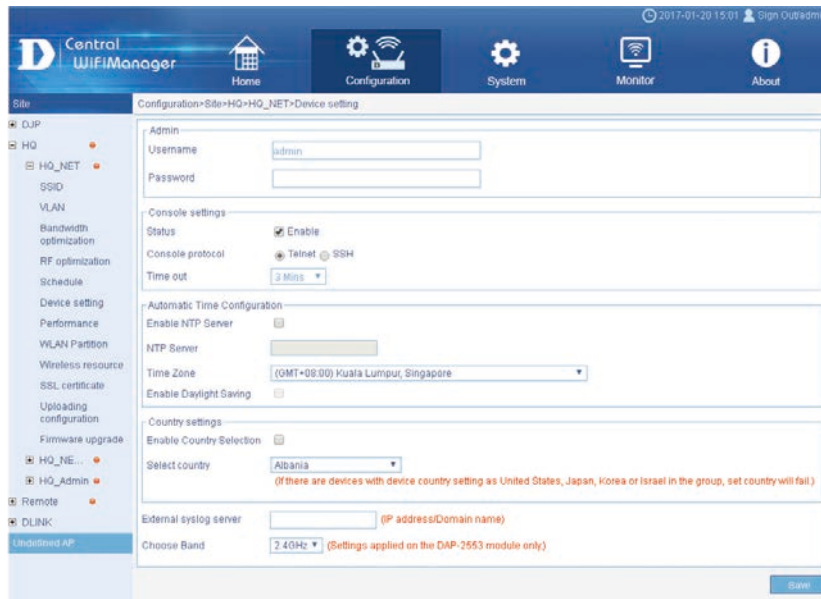


図 4-63 Device Settings

以下の項目があります。

項目	説明
Username	ネットワーク上のすべてのアクセスポイントに適用されているユーザ名を表示します。
Password	ネットワーク上のすべてのアクセスポイントに適用されるパスワードを入力します。
Status	ネットワーク上のすべてのアクセスポイントのコンソールポートの接続性を有効にします。
Console Protocol	ネットワーク上のすべてのアクセスポイントで使用されるコンソールポート (Telnet / SSH) を選択します。
Time Out	アクティブコンソールセッションのタイムアウト値 (1 分、3 分、5 分、10 分、15 分、Never) を選択します。
Enable NTP Server	NTP サーバを有効 / 無効に指定します。
NTP Server	NTP サーバの IP アドレスまたはドメイン名を入力します。
Time Zone	使用するタイムゾーンを指定します。
Enable Daylight Saving	Daylight Saving (サマータイム) を有効にします。
Enable Country Selection	ネットワークの存在する国の指定を有効にします。
Select country	ネットワークの存在する国を指定します。
External syslog server	外部 Syslog サーバの IP アドレスまたはドメイン名を入力します。
Choose Band	AP の無線帯を選択します。「2.4GHz」「5GHz」から指定します。

「Save」ボタンをクリックすると、変更を適用します。

注意 CWM では一部の特殊文字 ("&") はサポート対象外となります。

Performance（パフォーマンス設定）

「Performance」をクリックすると、以下のページが有効になります。本項目では、ネットワーク上のアクセスポイントの無線パフォーマンスについて設定します。

2.4GHz 帯

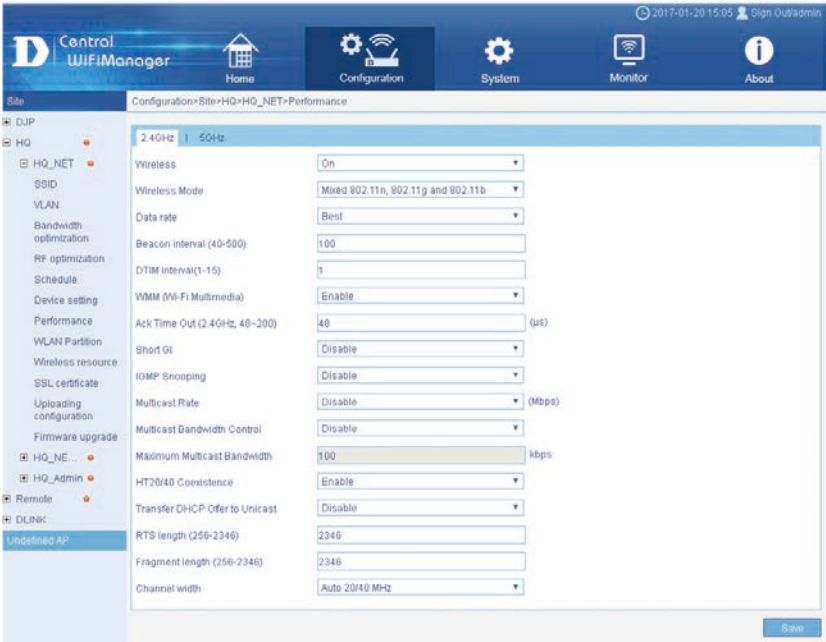


図 4-64 Performance（2.4GHz）

以下の項目があります。

項目	説明
Wireless	ネットワークの無線帯を「On」または「Off」で選択します。
Wireless Mode	無線モードを指定します。 「Mixed 802.11n, 802.11g and 802.11b」「Mixed 802.11g and 802.11b」「802.11n Only」から指定します。
Data Rate	無線データレート「Mixed 802.11g and 802.11b」を選択後、最適なレートを決定します。
Beacon Interval	ビーコン間隔値（40 ～ 500）を入力します。初期値：100
DTIM Interval	DTIM 値（1 ～ 15）を入力します。初期値：1
WMM (Wi-Fi Multimedia)	WMM (Wi-Fi Multimedia) を有効 / 無効に指定します。
ACK Timeout	ACK タイムアウト値を指定します。48 から 200（ μs ）で指定します。初期値は「48」（ μs ）です。
Short GI	ショート GI を有効 / 無効にします。
IGMP Snooping	IGMP スヌーピングを有効 / 無効にします。
Multicast Rate	マルチキャストレートを指定します。
Multicast Bandwidth Control	マルチキャスト帯域制御を有効 / 無効にします。
Maximum Multicast Bandwidth	最大マルチキャスト帯域幅を入力します。初期値では「100kbps」
HT20/40 Coexistence	「HT20/40 coexistence」を有効 / 無効に指定します。
Transfer DHCP Offer to Unicast	ユニキャストへ DHCP のオファー送信を有効 / 無効にします。
RTS Length	RTS 長値（256 ～ 2346）を入力します。初期値：2346
Fragment Length	フラグメント長値（256 ～ 2346）を入力します。初期値：2346
Channel Width	ネットワークで使用するチャンネル幅を指定します。「20 MHz」「Auto 20/40 MHz」から指定します。

「Save」ボタンをクリックすると、変更を適用します。

5GHz 帯

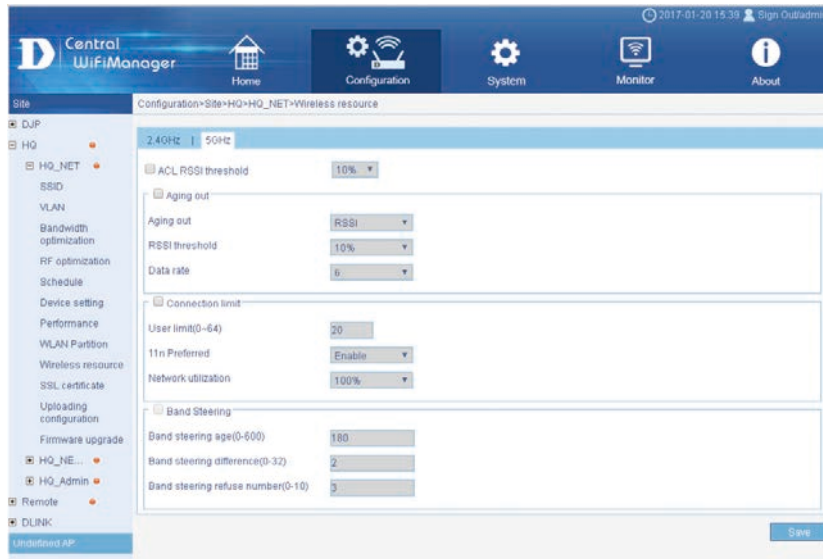


図 4-65 Performance (5GHz)

以下の項目があります。

項目	説明
Wireless	ネットワークの無線帯を「On」または「Off」で選択します。
Wireless Mode	無線モードを指定します。 「Mixed 802.11n, 802.11a」「802.11a Only」「802.11n Only」「Mixed 802.11ac」から指定します。
Data Rate	無線データレート「802.11a Only」を選択した場合、最適なレートを決定します。
Beacon Interval	ビーコン間隔値（40 ～ 500）を入力します。初期値：100
DTIM Interval	DTIM 値（1 ～ 15）を入力します。初期値：1
WMM (Wi-Fi Multimedia)	WMM (Wi-Fi Multimedia) を有効 / 無効に指定します。
ACK Timeout	ACK タイムアウト値を指定します。25 から 200（ μ s）で指定します。初期値は「48」（ μ s）です。
Short GI	ショート GI を有効 / 無効にします。
IGMP Snooping	IGMP スヌーピングを有効 / 無効にします。
Multicast Rate	マルチキャストレートを指定します。
Multicast Bandwidth Control	マルチキャスト帯域制御を有効 / 無効にします。
Maximum Multicast Bandwidth	最大マルチキャスト帯域幅を入力します。初期値では「100kbps」
HT20/40 Coexistence	「HT20/40 coexistence」を有効 / 無効に指定します。
Transfer DHCP Offer to Unicast	ユニキャストへ DHCP のオファー送信を有効 / 無効にします。
RTS Length	RTS 長値（256 ～ 2346）を入力します。初期値：2346
Fragment Length	フラグメント長値（256 ～ 2346）を入力します。初期値：2346
Channel Width	ネットワークで使用するチャンネル幅を指定します。「20 MHz」「Auto 20/40 MHz」から指定します。

「Save」ボタンをクリックすると、変更を適用します。

WLAN Partition (無線 LAN パーティション)

「WLAN Partition」をクリックすると、以下のページが有効になります。本項目では、ネットワーク上の無線パーティションについて設定します。

2.4GHz 帯

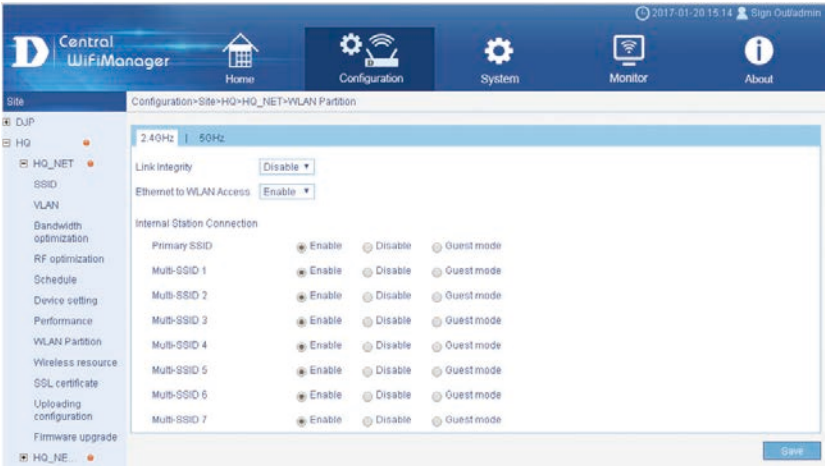


図 4-66 WLAN Partition (2.4GHz)

以下の項目があります。

項目	説明
Link Integrity	「Link Integrity」(リンクインティグリティ) 機能を有効 / 無効にします。
Ethernet to WLAN Access	「Ethernet to WLAN」 機能を有効 / 無効にします。
Primary SSID	本 WLAN パーティションのプライマリ SSID のメンバシップを有効 / 無効にします。 「Guest Mode」を指定すると本 WLAN パーティションにゲストとしてのアクセスを許可します。
Multi-SSID 1 to 7	本 WLAN パーティションの指定のマルチ SSID のメンバシップを有効 / 無効にします。 「Guest Mode」を指定すると本 WLAN パーティションにゲストとしてのアクセスを許可します。

「Save」ボタンをクリックすると、変更を適用します。

5GHz 帯

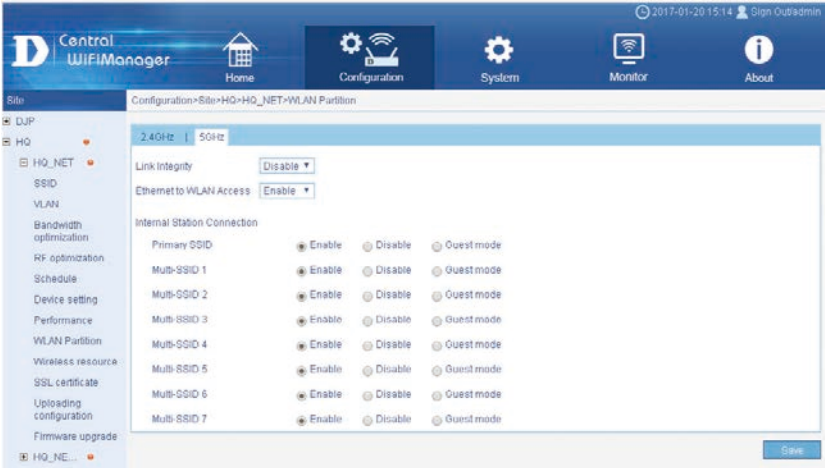


図 4-67 WLAN Partition (5GHz)

以下の項目があります。

項目	説明
Link Integrity	「Link Integrity」(リンクインティグリティ) 機能を有効 / 無効にします。
Ethernet to WLAN Access	「Ethernet to WLAN」 機能を有効 / 無効に指定します。
Primary SSID	本 WLAN パーティションのプライマリ SSID のメンバシップを有効 / 無効にします。 「Guest Mode」を指定すると本 WLAN パーティションにゲストとしてのアクセスを許可します。
Multi-SSID 1 to 7	本 WLAN パーティションの指定のマルチ SSID のメンバシップを有効 / 無効にします。 「Guest Mode」を指定すると本 WLAN パーティションにゲストとしてのアクセスを許可します。

「Save」ボタンをクリックすると、変更を適用します。

Wireless Resource (無線リソース)

「Wireless Resource」をクリックすると、以下のページが有効になります。本項目では、ネットワーク上の無線リソースについて設定します。

2.4GHz 帯

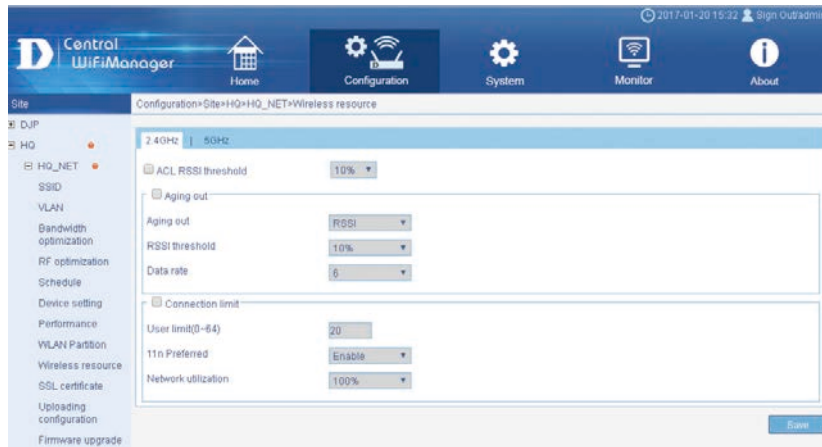


図 4-68 Wireless Resource (2.4GHz)

以下の項目があります。

項目	説明
ACL RSSI Threshold	「ACL RSSI」のしきい値を指定します。「10-100%」の間で指定可能です。
Aging Out	「Aging Out」を有効にしてモードを選択します。「RSSI」「Data Rate」から指定可能です。
RSSI Threshold	上記で「RSSI」を指定した場合、「RSSI」のしきい値を指定します。「10 - 100%」の間で指定可能です。
Data Rate	上記で「Data Rate」を指定した場合、「Data Rate」接続リミットを指定します。「6 - 54Mbps」の間で指定可能です。
Connection Limit	接続制限を有効にします。
User Limit	ユーザ接続制限数を指定します。0 から 64 ユーザで指定可能です。初期値は 20 です。
11n Preferred	「802.11n」を優先的に使用する場合有効にします。
Network Utilization	ネットワーク使用率を指定します。「0 - 100%」の間で指定可能です。初期値は 100% です。

「Save」ボタンをクリックすると、変更を適用します。

5GHz 帯

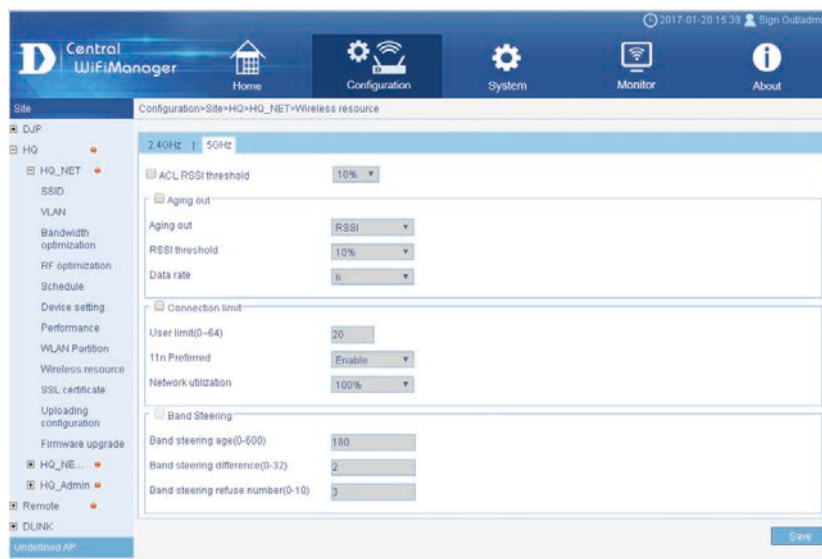


図 4-69 Wireless Resource (5GHz)

以下の項目があります。

項目	説明
ACL RSSI Threshold	「ACL RSSI」のしきい値を指定します。「10-100%」の間で指定可能です。
Aging Out	「Aging Out」を有効にしてモードを選択します。「RSSI」「Data Rate」から指定可能です。

RSSI Threshold	上記で「RSSI」を指定した場合、「RSSI」のしきい値を指定します。「10 - 100%」の間で指定可能です。
Data Rate	上記で「Data Rate」を指定した場合、「Data Rate」接続リミットを指定します。 「6 - 54Mbps」の間で指定可能です。
Connection Limit	接続制限を有効にします。
User Limit	ユーザ接続制限数を指定します。0 から 64 ユーザで指定可能です。初期値は 20 です。
11n Preferred	「802.11n」を優先的に使用する場合有効にします。
Network Utilization	ネットワーク使用率を指定します。「0 - 100%」の間で指定可能です。初期値は 100% です。
Band Steering Age	バンドステアリングエイジ値 (0 ～ 600) を入力します。初期値：180
Band Steering Difference	バンドステアリング差値 (0 ～ 32) を入力します。初期値：2
Band Steering Refuse Number	バンドステアリング拒否値 (0 ～ 10) を入力します。初期値：3

「Save」ボタンをクリックすると、変更を適用します。

SSL certificate (SSL 認証)

「SSL certificate」をクリックすると、以下のページが有効になります。本項目では、ネットワークで使用する SSL 認証について設定します。



図 4-70 SSL certificate

以下の項目があります。

項目	説明
Upload Certificate From File	「Browse」をクリックし、アップロードする SSL 認証ファイルを参照します。
Upload Key From File	「Browse」をクリックし、アップロードする SSL 鍵ファイルを参照します。

「Upload」をクリックし認証ファイルアップロードを実行します。その後「Status」「Result」「Progress」の内容が表示されます。

Upload Configuration (コンフィグアップロード)

「Uploading Configuration」をクリックすると、以下のページが有効になります。本項目では、コンフィグレーションファイルをアップロードするスケジュールを指定、または手動でネットワークのアクセスポイントにコンフィグレーションファイルをアップロードする設定を行います。

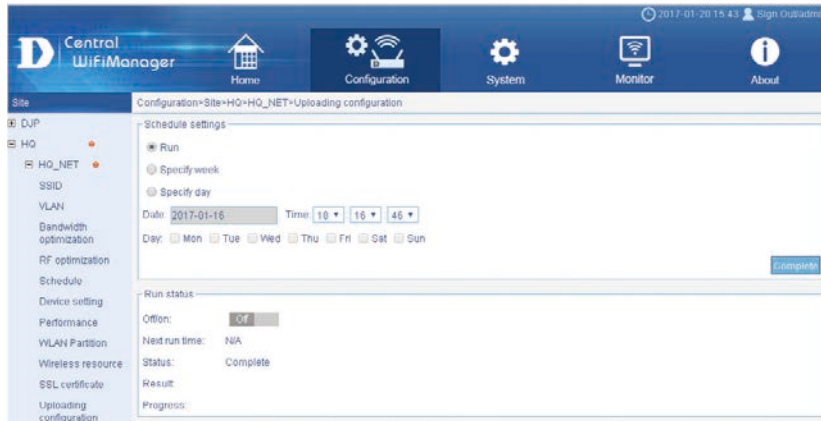


図 4-71 Upload Configuration

「Schedule Settings」セクションでは、以下のパラメータが設定可能です。

項目	説明
Run	ネットワーク上のすべてのアクセスポイントにコンフィグレーションファイルを手動でアップロードします。「Complete」をクリックするとアップロードを開始します。
Specify Time	スケジュールされた時刻にコンフィグレーションファイルをアップロードします。このオプションは、毎週指定した時刻にコンフィグレーションファイルを継続的にアップロードします。
Specify Date	スケジュールされた日にコンフィグレーションファイルをアップロードします。このオプションは、指定した日時にコンフィグレーションファイルを一度アップロードします。
Date	「Specify Date」オプションを選択した後、コンフィグレーションファイルをアップロードする日付けを指定します。
Time	「Specify Time」または「Specify Date」オプションを選択した後、コンフィグレーションファイルをアップロードする時刻を指定します。
Day	「Specify Time」オプションを選択した後、コンフィグレーションファイルをアップロードする曜日を指定します。

「Complete」ボタンをクリックすると、変更を適用、または手動でアップロードを開始します。

「Run Status」セクションでは、以下のパラメータが設定可能です。

項目	説明
Off/On	「On」の場合はスケジュールされたコンフィグレーションのアップロードを有効にし、「Off」の場合はスケジュールされたアップロードを無効にします。スケジュールを再定義する場合は、このオプションを「Off」にする必要があります。

最初にアップロードを行った後、次のアップロードが行われる際「Next Run Time」フィールドが表示されます。すべてのアップロードを行った後、レビューのために「Result」ハイパーリンクが有効となります。

Firmware Upgrade (ファームウェア更新)

「Firmware Upgrade」をクリックすると、以下のページが有効になります。本項目では、ファームウェアファイルをアップロードするスケジュールを指定、または手動でネットワークのアクセスポイントにファームウェアファイルをアップロードする設定を行います。

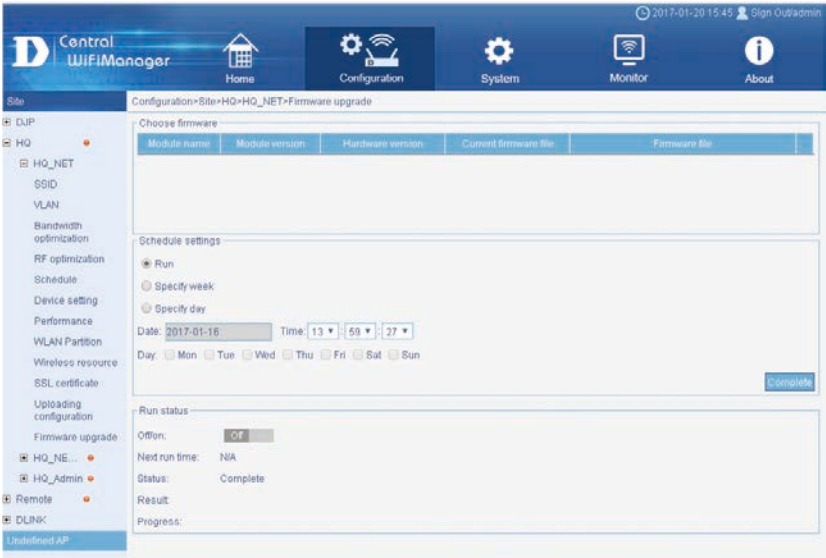


図 4-72 Firmware Upgrade

「Choose Firmware」セクションでは、以下のパラメータが設定可能です。

項目	説明
Firmware File	ネットワーク上のすべてのアクセスポイントに対し、手動または設定されたスケジュールに基づきアップロードするファームウェアファイルを指定できます。「Browse」をクリックしてコンピュータに保存されたファームウェアを指定します。

「Schedule Settings」セクションでは、以下のパラメータが設定可能です。

項目	説明
Run	ネットワーク上の特定したすべてのアクセスポイントにファームウェアを手動でアップロードします。「Complete」をクリックするとアップロードを開始します。
Specify Time	スケジュールされた時刻にファームウェアをアップロードします。このオプションは、毎週指定した時刻にファームウェアを継続的にアップロードします。
Specify Date	スケジュールされた日にファームウェアをアップロードします。このオプションは、指定した日時に一度ファームウェアをアップロードします。
Date	「Specify Date」オプションを選択した後、ファームウェアをアップロードする日付けを指定します。
Time	「Specify Time」または「Specify Date」オプションを選択した後、ファームウェアをアップロードする時刻を指定します。
Day	「Specify Time」オプションを選択した後、ファームウェアをアップロードする曜日を指定します。

「Complete」ボタンをクリックすると、変更を適用、または手動でアップロードを開始します。

「Run Status」セクションでは、以下のパラメータが設定可能です。

項目	説明
Off/On	「On」の場合はスケジュールされたファームウェアのアップロードを有効にし、「Off」の場合はスケジュールされたアップロードを無効にします。スケジュールを再定義する場合は、このオプションを「Off」にする必要があります。

最初にアップロードを行った後、次のアップロードが行われる際「Next Run Time」フィールドが表示されます。すべてのアップロードを行った後、レビューのために「Result」ハイパーリンクが有効となります。

Undefined AP (未定義 AP)

「Undefined AP」をクリックすると、以下のページが有効になります。本項目では、ネットワークに属していないアクセスポイントの一覧を確認することができます。

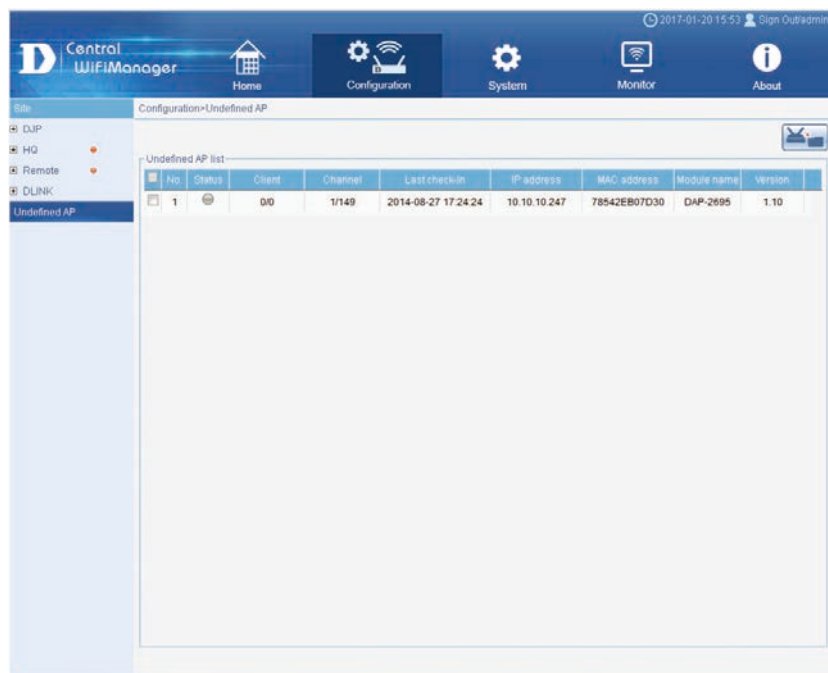


図 4-73 Undefined AP

このリストにあるアクセスポイントをネットワークに追加するには、エントリ横のチェックボックスを選択して右上部にある  アイコンをクリックします。追加するために選択可能な有効なネットワークの一覧が表示されます。

第 5 章 System（システム）

本項目では「Central Wi-Fi Manager」の項目「System」の説明をします。「System」では主に「Central Wi-Fi Manager」のシステム機能に関する設定を行うことが可能です。

Settings（システム設定）

インタフェース上部の「System」と左パネルの「Settings」をクリックした後、本項目の設定と確認が可能になります。本項目には「General」「Module」「Database」「Advance」「SMTP」の5つのタブがあります。

General タブ（一般設定）

「General」タブでは、以下のパラメータの設定が可能です。

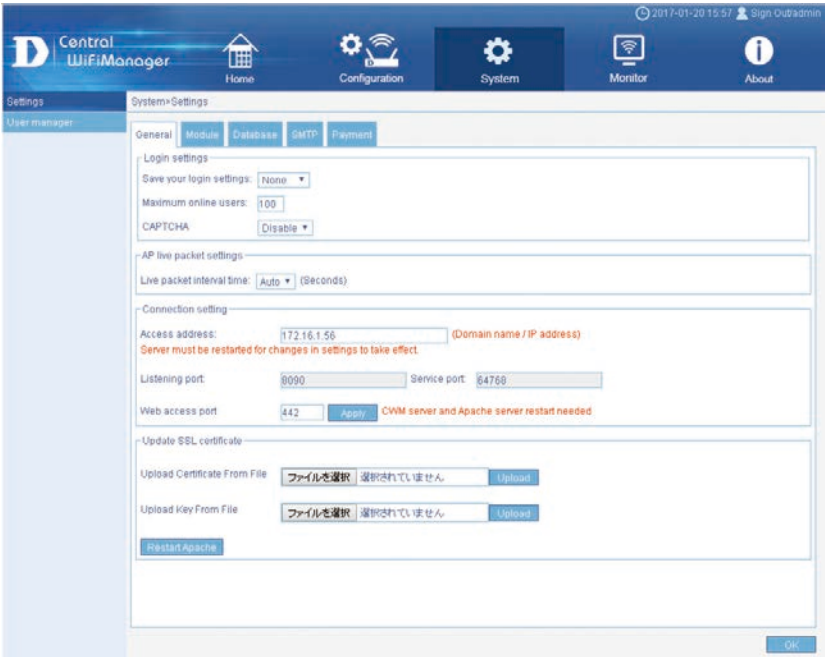


図 5-1 General

以下の項目があります。

項目	説明
Login Settings	
Save Your Login Settings	「Login Settings」セクションでは、ログインセッションを記憶させるかさせないかを選択します。「None」オプションを選択すると、ユーザは毎回即座にインターフェース（Web UI）にログインします。「1 week」オプションを選択すると、ユーザセッションは一週間開かれます。手動でログアウトを行わない限り、この間、ユーザは最初のログイン後再びログインを要求されることはありません。
Maximum online users	「Login Settings」セクションでは、同時に管理インターフェースにアクセスを許可するユーザの最大数（1 ～ 10）を入力します。初期値：5
CAPTCHA	CAPTCHA を有効 / 無効にします。
AP live packet settings	
Live packet interval time	「AP live packet settings」セッションでは、ライブパケットの時間間隔（Auto、2、5、10、20、30）を選択します。
Connection settings	
Access Address	CWM アプリケーションの IP アドレスを入力します。
Listen Port	CWM アプリケーションのリッスンポート番号を入力します。初期値：8090
Service Port	CWM アプリケーションのサーバのポート番号を入力します。初期値：64768
Web access port	CWM アプリケーションの Web アクセスのポート番号を入力します。初期値：443
Update SSL Certification	
Upload Certificate From File	「Browse」をクリックし、アップロードする SSL 認証ファイルを参照します。 「Upload」をクリックしアップロードを開始します。
Upload Key From File	「Browse」をクリックし、アップロードする SSL 鍵ファイルを参照します。 「Upload」をクリックしアップロードを開始します。

「Restart Apache」をクリックすると CWM をホストする Apache サーバを再起動します。

「Apply」ボタンをクリックすると変更を適用します。

Module タブ (モジュール設定)

「Module」タブでは、アクセスポイントモジュールの一覧が「Module Name」セクションに表示されます。
CWM サーバアプリケーションにより管理されるアクセスポイントのすべての異なるモデルにおいて、管理者は指定のアクセスポイントに実行可能なモジュールファイルをインストールする必要があります。アクセスポイントの各タイプごとに 1 つインストールすることが可能です。

注意 すべてのアクセスポイントのモジュールファイルはアプリケーションで対応され、D-Link の Web サイトからダウンロードすることができます。

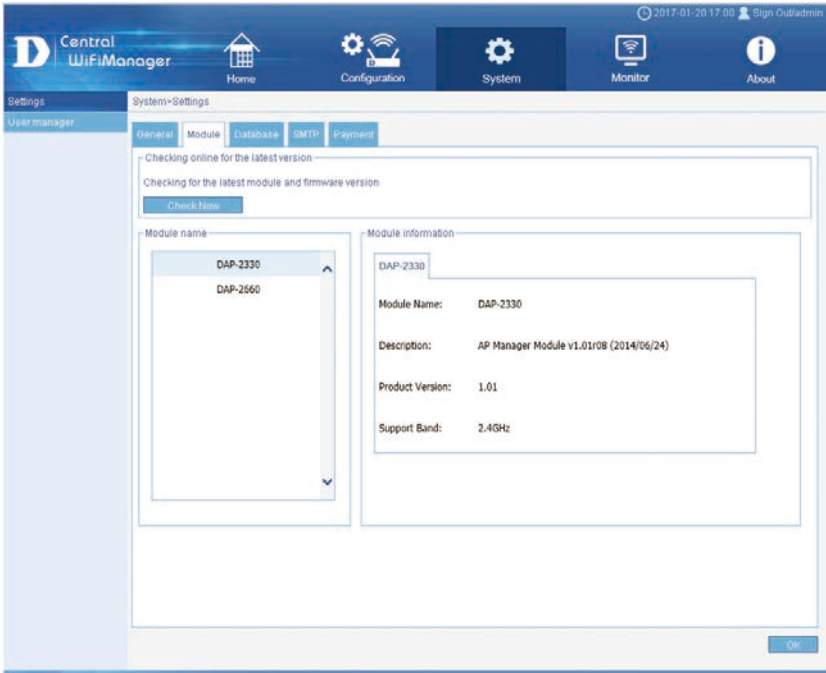


図 5-2 Module タブ

インストールされたアクセスポイントモジュールに関する詳細は「Module Information」を参照します。
インストールしたモジュールを保持してファームウェアのバージョンを更新するには「Check Now」ボタンをクリックします。
「OK」ボタンをクリックすると変更を適用します。

「Check Now」ボタンをクリックすると、以下のページが有効になります。本項目ではアプリケーションはインストールされたアクセスポイントモジュールが更新されたかどうかを確認します。

Online Check Version					
	Model Name	HW	Version	Result	Download
	DAP-2330	A	1.01		
	DAP-2660	A	1.05		

図 5-3 Check Now

Database タブ（データベース設定）

「Database」タブをクリックすると以下のページが表示されます。このページでは、アプリケーションのデータベース情報のバックアップ、復元とそのスケジュールを確認、設定することができます。「Database」タブでは、「General」と「Backup」の2つのサブタブがあります。それぞれのタブで、以下のパラメータの設定が可能です。

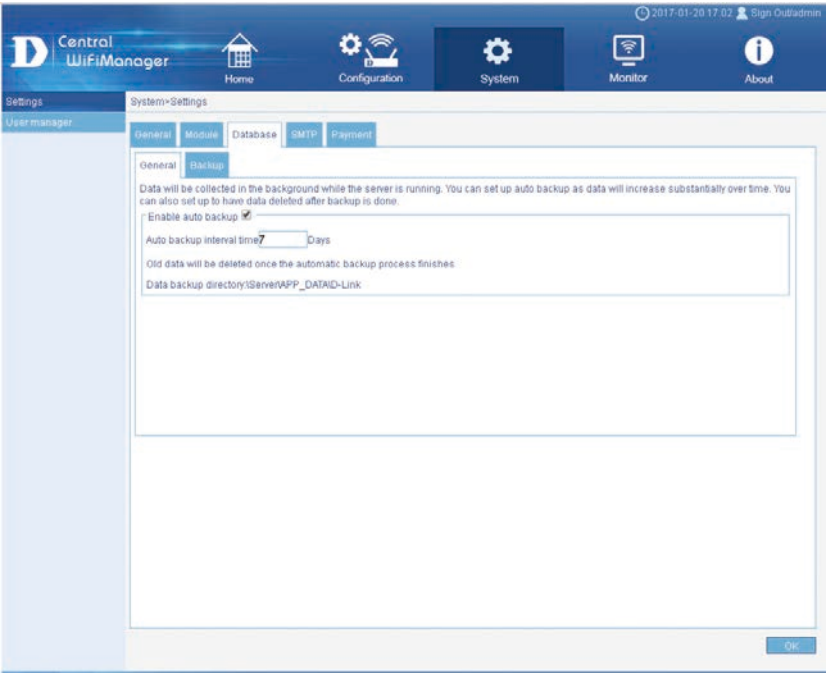


図 5-4 Database（General タブ）

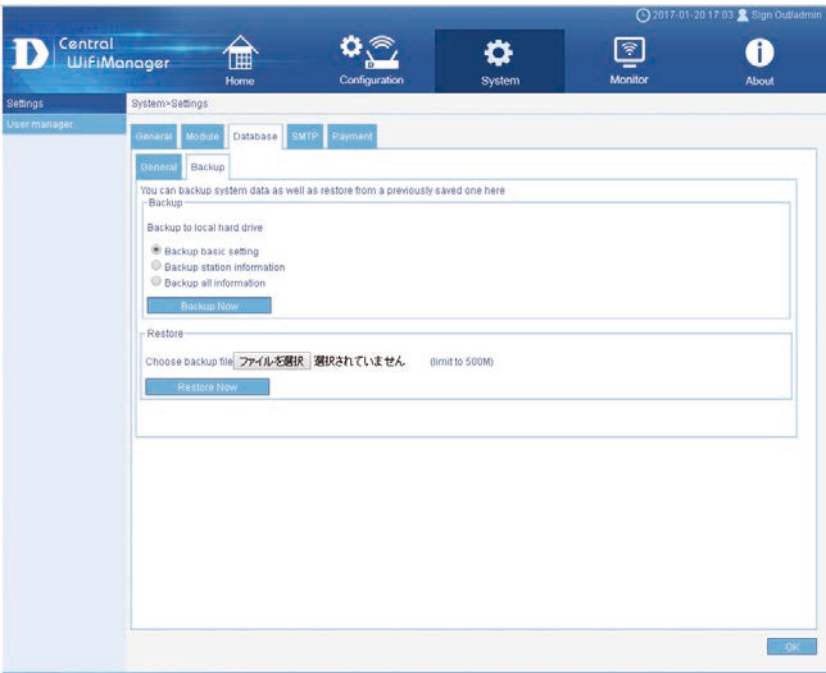


図 5-5 Database（Backup タブ）

以下の項目があります。

項目	説明
General タブ	
Enable auto backup	アプリケーションの自動バックアップ機能を有効にします。
Auto backup interval time	自動バックアップの時間帯を日付単位で入力します。 「Old data will be deleted once the automatic backup process finishes」オプションを選択して、保留日数値を入力すると、新しいデータベースのバックアップが正常に行われた後、古いデータベースのバックアップ情報を破棄します。初期値は7日です。
Data backup directory	この欄にはバックアップディレクトリのパスが参考として表示されます。

Backup タブ	
Backup	手動でシステムデータをインタフェースに接続しているコンピュータにバックアップします。 - Backup basic settings - 基本的なシステム設定のバックアップをします。 - Backup station information - 無線ステーション情報のバックアップをします。 - Backup all information - 全ての情報に関してバックアップします。 「Backup Now」をクリックすると手動バックアップを行います。バックアップファイルは SQL のファイル拡張子付きの PostgreSQL ファイルです。
Restore	バックアップしたファイルを使用して手動でアプリケーションに設定を復元します。「Browse/ ファイルを選択」をクリックして、前回バックアップした SQL ファイルを指定し、「Restore Now」をクリックして復元を開始します。

「OK」 ボタンをクリックすると変更を適用します。

SMTP (SMTP 設定)

「SMTP」タブをクリックすると以下のページが表示されます。このページでは、「Simple Mail Transfer Protocol」(SMTP) の設定の確認、設定ができます。

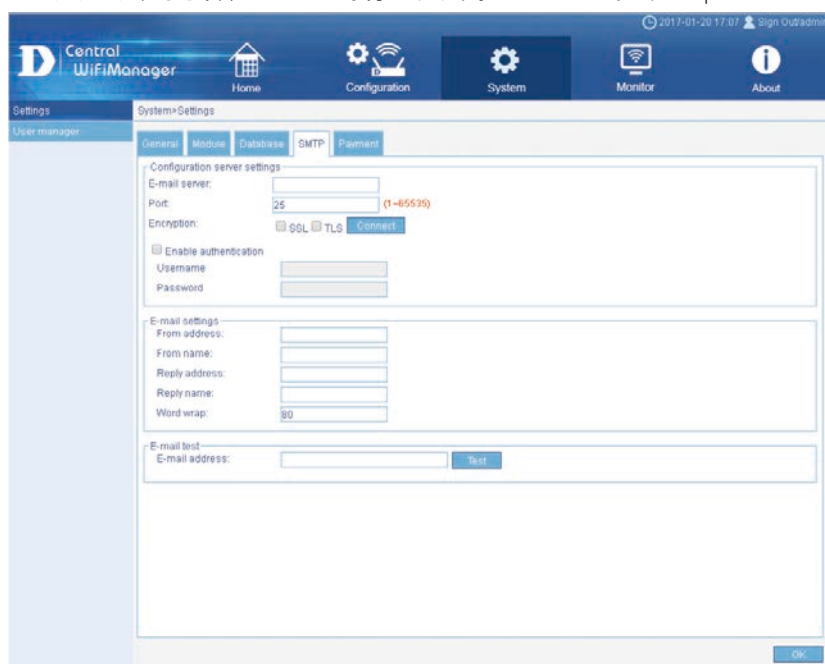


図 5-6 SMTP

以下の項目があります。

項目	説明
Configure Server Settings	
E-Mail Server	SMTP サーバの IP アドレス、またはドメイン名を入力します。
Port	SMTP サーバのポート番号を入力します。初期値：25
Encryption	必要に応じて SMTP 接続の暗号化方法 (SSL または TLS) を選択します。メールサーバ設定が正しいかどうかを確認するには「Connect」をクリックします。
Enable authentication	SMTP サーバが認証を必要とする場合、メールを送信します。
Username	認証有効後、SMTP ユーザアカウントのユーザ名を入力します。
Password	認証有効後、SMTP ユーザアカウントのパスワードを入力します。
E-Mail Settings	
From address	受信者が送信者を認識できるよう、送信者の E メールアドレスを入力します。
From name	送信者名を入力します。
Reply address	受信者の E メールアドレスを入力します。
Reply name	受信者名を入力します。
Word wrap	ワードラップ値を入力します。初期値：80
E- Mail Test	
Mailbox address	受信者の E メールアドレスがアクティブかどうかを確認します。受信者の E メールアドレスを入力し「Test」をクリックします。

「OK」 ボタンをクリックすると変更を適用します。

注意 CWM では一部の特殊文字 ("&") はサポート対象外となります。

Payment (Payment 設定)

「Payment」タブをクリックすると以下のページが表示されます。このページでは「Paypal」による支払いの設定が行われます。

注意 本項目は日本ではサポート対象外となります。

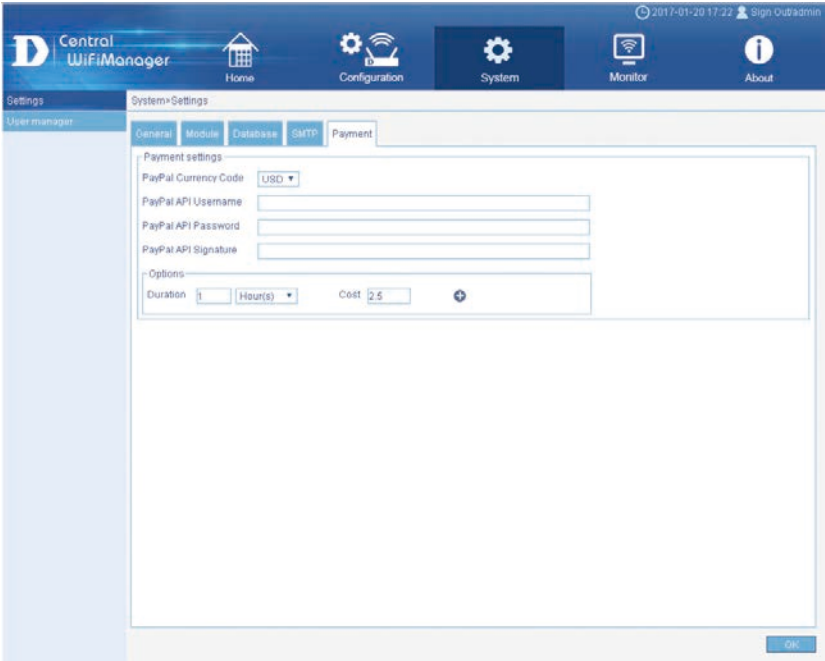


図 5-7 Payment

以下の項目があります。

項目	説明
PayPal Currency Code	PayPal の通貨コードです。
PayPal API Username	PayPal API のユーザ名です。
PayPal API Password	PayPal API のパスワードです。
PayPal API Signature	PayPal API のシグニチャです。
Duration	有効期間を指定します。
Cost	有効期間にかかるコストを指定します。

「OK」ボタンをクリックすると変更を適用します。

注意 本項目は日本ではサポート対象外となります。

User Manager (ユーザ管理)

上部パネルの「System」と左パネルの「User Manager」をクリックした後、次のページが表示されます。このページでは、ユーザアカウントの確認、作成、設定ができます。CWM サーバアプリケーションにアクセスするために作成可能な 5 種類のユーザアカウント（「Root Admin」「Root User」「Local Admin」「Local User」「Front Desk Staff」）があります。

「User List」セクションには、ユーザアカウントの一覧が表示されます。

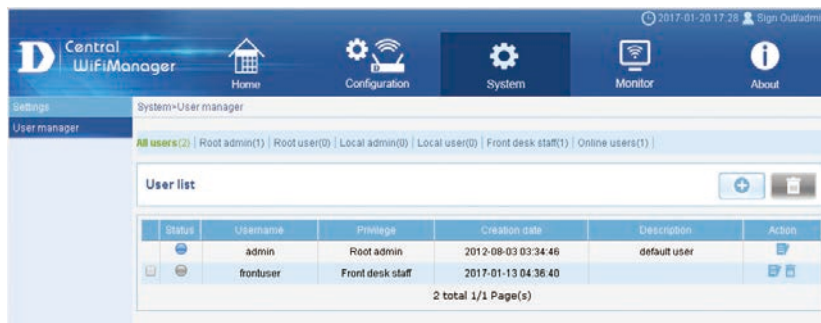


図 5-8 User Manager

-  アイコンをクリックすると、新しいアカウントを追加します。
-  アイコンをクリックすると、既存のアカウント修正します。
-  アイコンをクリックすると、既存のアカウントを削除します。

ユーザアカウント作成

-  アイコンをクリックすると、以下のページが有効になります。このページでは、以下のパラメータの設定が可能です。

図 5-9 Create User Account

以下の項目があります。

項目	説明
Username	新しいユーザアカウントのユーザ名（4～64文字以内）を入力します。
Password	新しいユーザアカウントのパスワード（4～64文字以内）を入力します。
Privilege	ユーザアカウントの特権レベル（「Root Admin」「Root User」「Local Admin」「Local User」「Front Desk Staff」）を選択します。
E-mail	ユーザアカウントに伴う E メールアドレスを入力します。
Description	ユーザアカウントの詳細な説明を入力します。

「OK」ボタンをクリックすると、ユーザアカウントを作成します。

「Reset」ボタンをクリックすると、このフォームのフィールドに入力した情報をクリアします。

「Cancel」ボタンをクリックすると、変更を破棄してメインページに戻ります。

注意 CWM では一部の特殊文字 ("&\) はサポート対象外となります。

第 6 章 Monitor (モニタ)

本項目では「Central Wi-Fi Manager」の「Monitor」の説明をします。「Monitor」では主に「Central Wi-Fi Manager」の管理している無線クライアントについての表示、確認を行います。

Report (レポート)

Association (関連機器)

上部パネルの「Monitor」と左パネルの「Association」をクリックすると、以下のページが表示されます。本項目では、すべてのアクセスポイントとアプリケーションにより管理される無線クライアントのレポートを確認することができます。3つの関連レポートは、「By Access Point」、「By Wireless Station」、「By Station Number」により生成されます。

By Access Point タブ (関連アクセスポイント)

本項目では、「By Access Point」により生成されたレポートについて説明します。このレポートは、1つ目のドロップダウンメニューの「Group Type」(サイト)を選択することにより絞り込まれ、次に2つ目のドロップダウンメニューのネットワークを選択し表示内容の条件を指定します。

 ボタンをクリックするとレポートを更新します。

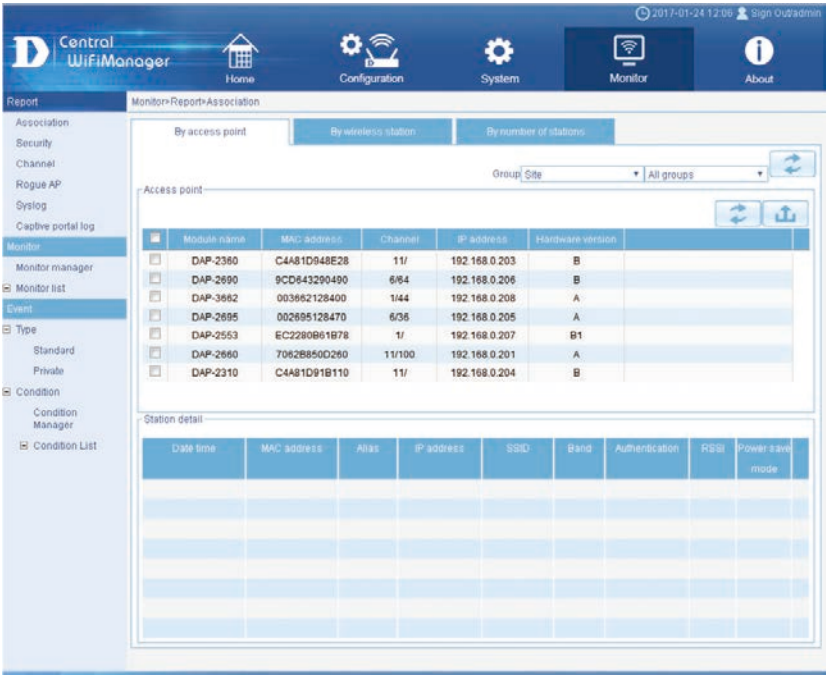


図 6-1 By Access Point

「Access Point」リストでは、アプリケーションにより管理されたアクセスポイントの一覧が表示されます。各アクセスポイントの「Module Name」、「MAC Address」、「Channel」、「IP Address」、「HW Version」などの情報が表示されます。

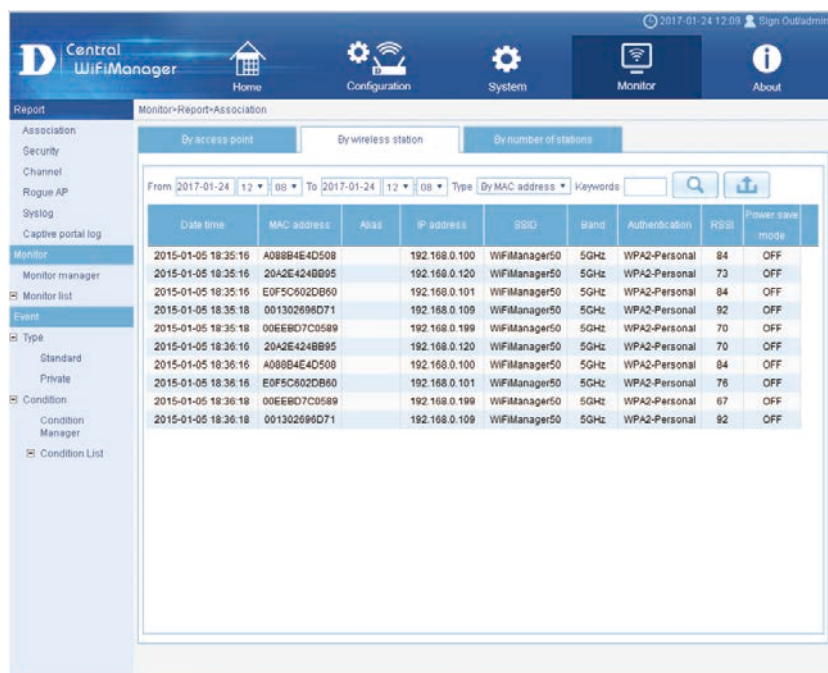
「Station Detail」リストでは、アプリケーションにより管理されたアクセスポイントに接続された無線クライアントの一覧が表示されます。各無線クライアントの「Module Name」、「MAC Address」、「Channel」、「IP Address」、「HW Version」などの情報が表示されます。

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

By Wireless Station タブ (関連ワイヤレスステーション)

本項目では、「By Wireless Station」により生成されたレポートについて説明します。このレポートは、「From/To」で期間を選択することにより絞り込むことが可能で、「Type」として「By MAC Address」または「By Alias」の選択、更に追加として「Key Words」を条件に加えることも可能です。

 ボタンをクリックするとレポートを更新します。



Date time	MAC address	Alias	IP address	SSID	Band	Authentication	RSSI	Power save mode
2015-01-05 18:35:16	A08B94E4D508		192.168.0.100	WiFiManager50	5GHz	WPA2-Personal	84	OFF
2015-01-05 18:35:16	20A2E424B895		192.168.0.120	WiFiManager50	5GHz	WPA2-Personal	73	OFF
2015-01-05 18:35:16	E0F5C602DB90		192.168.0.101	WiFiManager50	5GHz	WPA2-Personal	84	OFF
2015-01-05 18:35:18	001302696D71		192.168.0.109	WiFiManager50	5GHz	WPA2-Personal	92	OFF
2015-01-05 18:35:18	00EE6D7C0589		192.168.0.199	WiFiManager50	5GHz	WPA2-Personal	70	OFF
2015-01-05 18:36:16	20A2E424B895		192.168.0.120	WiFiManager50	5GHz	WPA2-Personal	70	OFF
2015-01-05 18:36:16	A08B94E4D508		192.168.0.100	WiFiManager50	5GHz	WPA2-Personal	84	OFF
2015-01-05 18:36:16	E0F5C602DB90		192.168.0.101	WiFiManager50	5GHz	WPA2-Personal	76	OFF
2015-01-05 18:36:18	00EE6D7C0589		192.168.0.199	WiFiManager50	5GHz	WPA2-Personal	67	OFF
2015-01-05 18:36:18	001302696D71		192.168.0.109	WiFiManager50	5GHz	WPA2-Personal	82	OFF

図 6-2 By Wireless Station

このリストには、アクセスポイントに接続されアプリケーションにより管理される無線クライアントの一覧が表示されます。各無線クライアントの「Date/Time」、「MAC Address」、「Alias」、「IP Address」、「SSID」、「Band」、「Authentication」、「RSSI」、「Power Save Mode」などの情報が表示されます。

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

By Station Number タブ (関連ステーション番号)

このページでは、「By Station Number」により生成されたレポートについて説明します。このレポートは「From/To」で期間を選択することにより絞り込むことが可能で、1つ目のドロップダウンメニューの「Group Type」(サイト)を選択することにより絞り込まれ、次に2つ目のドロップダウンメニューのネットワークを選択し表示内容の条件を指定します。  ボタンをクリックするとレポートを更新します。

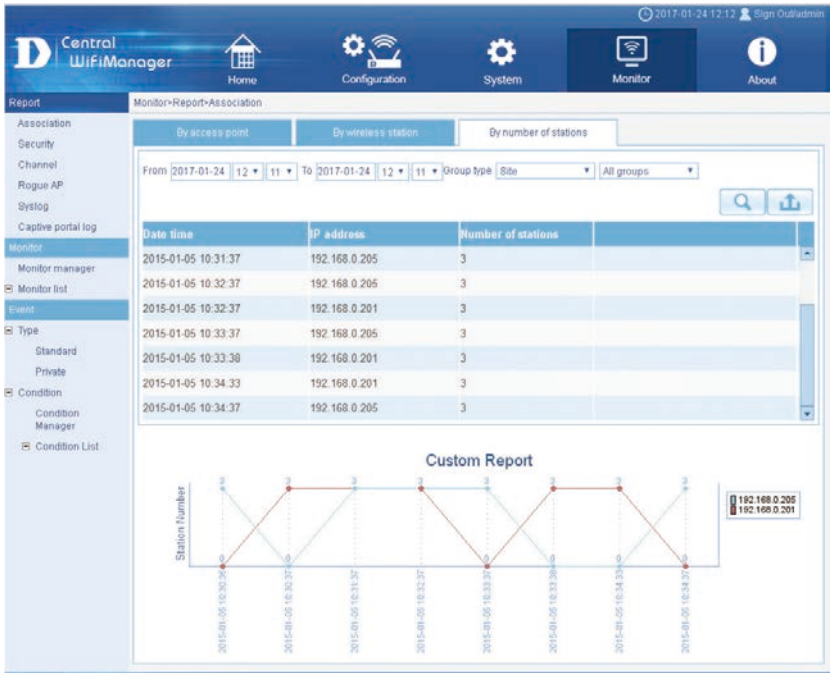


図 6-3 By Station Number

リストには、ステーション番号によりアクセスポイントの一覧が表示され、アプリケーションで管理されるアクセスポイントに接続されたアクティブ無線クライアント接続が表示されます。
各無線クライアントの「Date/Time」、「IP Address」、「Station' s Number」などの情報が表示されます。
折れ線グラフでは、「Station Number」のグラフ表示は時間とともに IP アドレスごとに表示されます。
 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。
このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

Security (セキュリティ)

上部パネルの「Monitor」と左パネルの「Security」をクリックすると、以下のページが表示されます。本項目では、アプリケーションで管理されるすべてのアクセスポイントの無線セキュリティ設定のレポートを確認することができます。セキュリティレポートは、「Chart」または「List」で表示されます。

Chart (AP セキュリティレベルチャート)

本項目では、「Chart」レポートについて説明します。「Chart」レポートには、アプリケーションで管理されるアクセスポイント上のすべての有効なセキュリティレベルが表示されます。このレポートは、1 つ目のドロップダウンメニューの「Group Type」(サイト) を選択することにより絞り込まれ、次に 2 つ目のドロップダウンメニューのネットワークを選択し表示内容の条件を指定します。

 ボタンをクリックするとレポートを更新します。

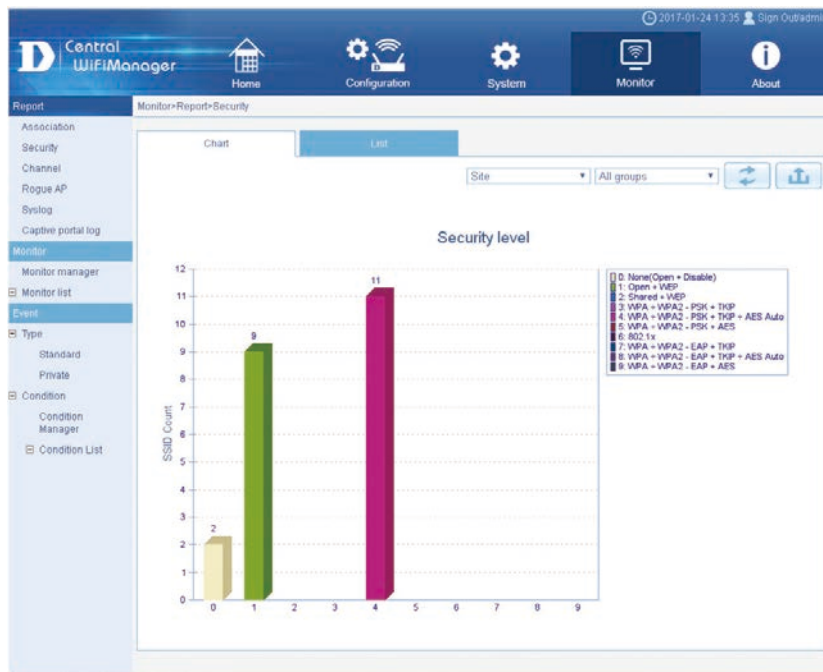


図 6-4 Chart

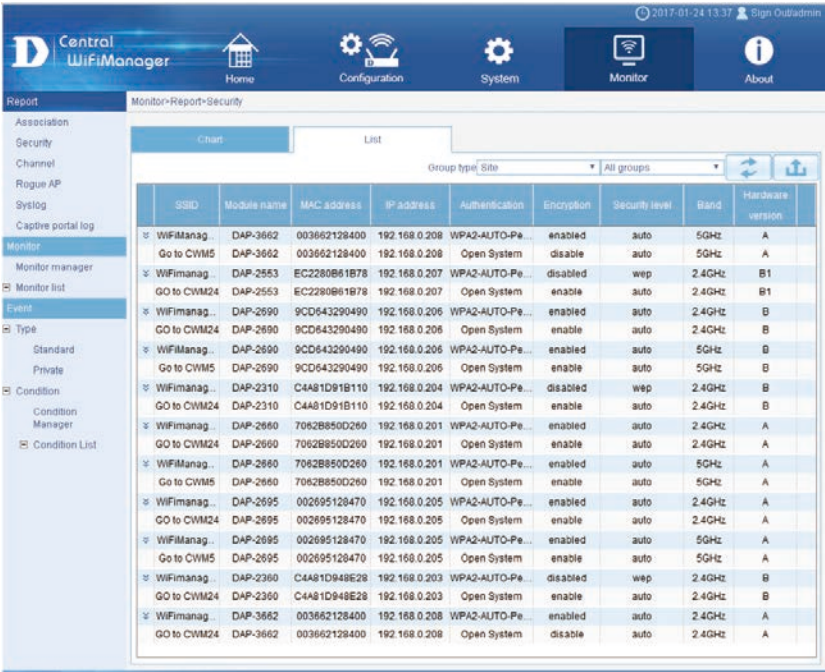
このレポートはネットワーク上のアクセスポイントによりホストされる SSID の有効数をカウントし、どのセキュリティレベルで設定されているかを査定し、チャートにセキュリティレベルごとにグラフ表示します。

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

List (SSID リスト)

本項目では、「List」レポートについて説明します。「List」レポートには、アプリケーションで管理されるアクセスポイントによりホストされるすべての有効な SSID が表示されます。このレポートは、1 つ目のドロップダウンメニューの「Group Type」(サイト) を選択することにより絞り込まれ、次に 2 つ目のドロップダウンメニューのネットワークを選択し表示内容の条件を指定します。

 ボタンをクリックするとレポートを更新します。



SSID	Module name	MAC address	IP address	Authentication	Encryption	Security level	Band	Hardware version
WiFiManag...	DAP-3662	003662128400	192.168.0.208	WPA2-AUTO-Pe...	enabled	auto	5GHz	A
Go to CWM5	DAP-3662	003662128400	192.168.0.208	Open System	disable	auto	5GHz	A
WiFiManag...	DAP-2553	EC2280B61B78	192.168.0.207	WPA2-AUTO-Pe...	disabled	wep	2.4GHz	B1
Go to CWM24	DAP-2553	EC2280B61B78	192.168.0.207	Open System	enable	auto	2.4GHz	B1
WiFiManag...	DAP-2690	9CD643290490	192.168.0.206	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	B
Go to CWM24	DAP-2690	9CD643290490	192.168.0.206	Open System	enable	auto	2.4GHz	B
WiFiManag...	DAP-2690	9CD643290490	192.168.0.206	WPA2-AUTO-Pe...	enabled	auto	5GHz	B
Go to CWM5	DAP-2690	9CD643290490	192.168.0.206	Open System	enable	auto	5GHz	B
WiFiManag...	DAP-2310	C4A81D91B110	192.168.0.204	WPA2-AUTO-Pe...	disabled	wep	2.4GHz	B
Go to CWM24	DAP-2310	C4A81D91B110	192.168.0.204	Open System	enable	auto	2.4GHz	B
WiFiManag...	DAP-2660	7062B8500260	192.168.0.201	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	A
Go to CWM24	DAP-2660	7062B8500260	192.168.0.201	Open System	enable	auto	2.4GHz	A
WiFiManag...	DAP-2660	7062B8500260	192.168.0.201	WPA2-AUTO-Pe...	enabled	auto	5GHz	A
Go to CWM5	DAP-2660	7062B8500260	192.168.0.201	Open System	enable	auto	5GHz	A
WiFiManag...	DAP-2695	002695128470	192.168.0.205	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	A
Go to CWM24	DAP-2695	002695128470	192.168.0.205	Open System	enable	auto	2.4GHz	A
WiFiManag...	DAP-2695	002695128470	192.168.0.205	WPA2-AUTO-Pe...	enabled	auto	5GHz	A
Go to CWM5	DAP-2695	002695128470	192.168.0.205	Open System	enable	auto	5GHz	A
WiFiManag...	DAP-2360	C4A81D948E28	192.168.0.203	WPA2-AUTO-Pe...	disabled	wep	2.4GHz	B
Go to CWM24	DAP-2360	C4A81D948E28	192.168.0.203	Open System	enable	auto	2.4GHz	B
WiFiManag...	DAP-3662	003662128400	192.168.0.208	WPA2-AUTO-Pe...	enabled	auto	2.4GHz	A
Go to CWM24	DAP-3662	003662128400	192.168.0.208	Open System	disable	auto	2.4GHz	A

図 6-5 List

各 SSID の「SSID」、「Module Name」、「MAC Address」、「IP Address」、「Authentication」、「Encryption」、「Security Level」、「Band」、「HW Version」などの情報が表示されます。

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

Channel (チャネル)

上部パネルの「Monitor」と左パネルの「Channel」をクリックすると、以下のページが表示されます。本項目では、周波数帯域ごとの無線チャネル使用のチャートレポートを確認することができます。

このレポートは、1つ目のドロップダウンメニューの「Group Type」(サイト) を選択することにより絞り込まれ、次に2つ目のドロップダウンメニューのネットワークを選択し表示内容の条件を指定します。

 ボタンをクリックするとレポートを更新します。

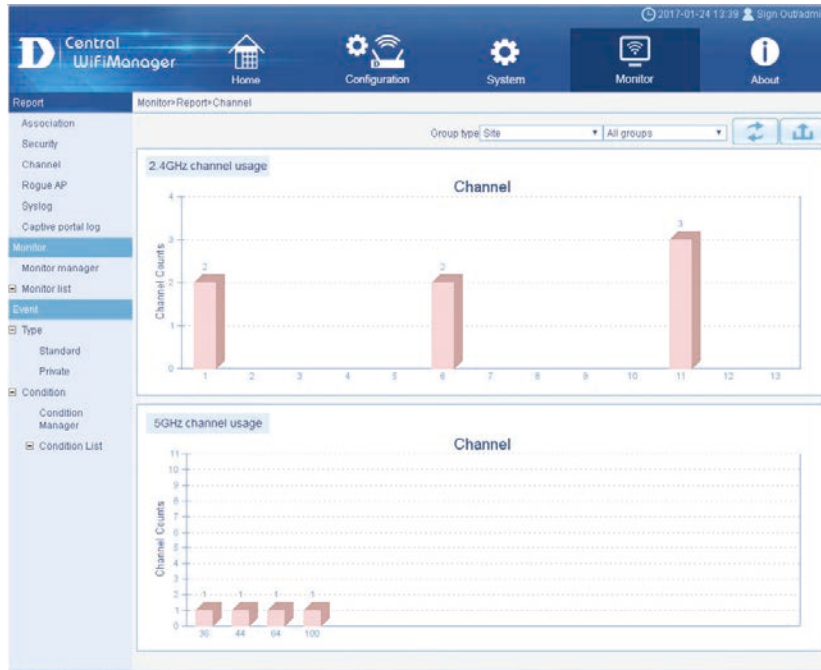


図 6-6 Channel

最初のチャートレポートでは、2.4GHz 無線周波数帯域のチャネル番号カウントを、2 番目のチャートレポートでは、5GHz 無線周波数帯域のチャネル番号カウントを確認することができます。

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

Rogue AP（不正アクセスポイント）

上部パネルの「Monitor」と左パネルの「Rogue AP」をクリックすると、以下のページが表示されます。このページでは「new」「rogue」「valid」「neighborhood」に関するアクセスポイントを確認することができます。本項目は、ネットワークのアクセスポイントをスキャンし、カテゴリーごとに分類することを目的としています。

New AP（新規アクセスポイント）

「New AP」タブでは、その環境上の新しいアクセスポイントの一覧を確認することができます。ここに表示されるアクセスポイントは、ネットワーク上のアクセスポイントにより検出され、新しいアクセスポイントとして分類されます。

 ボタンをクリックすると、ネットワークに接続されたアクセスポイントの範囲内で分類されていないアクセスポイントのスキャンします。

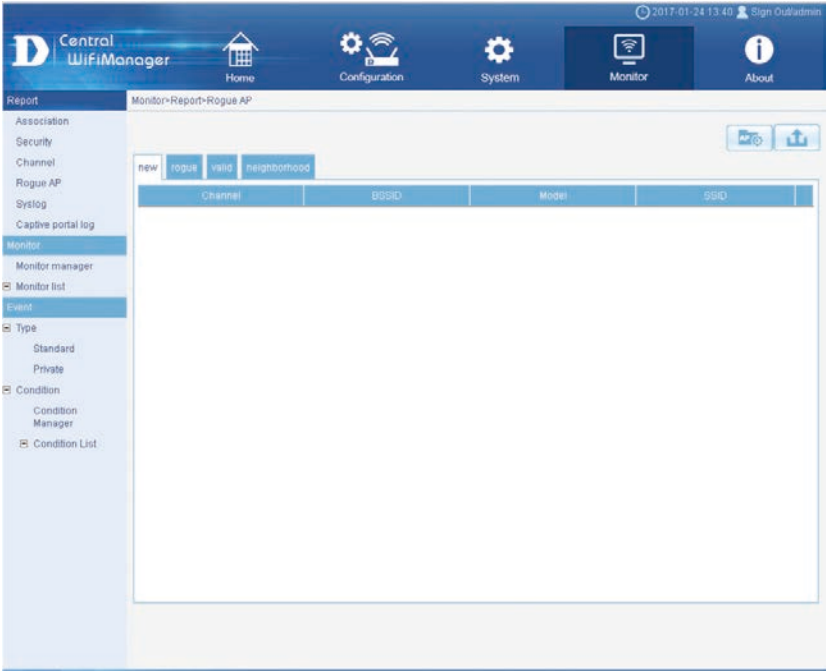


図 6-7 New AP

最初のチャートレポートでは、2.4GHz 無線周波数帯域のチャンネル番号カウントを、2 番目のチャートレポートでは、5GHz 無線周波数帯域のチャンネル番号カウントを確認することができます。

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

 をクリックすると、以下のページが有効になります。本項目では、ネットワークに接続されたアクセスポイントの範囲内で分類されていないアクセスポイントのスキャンを開始します。

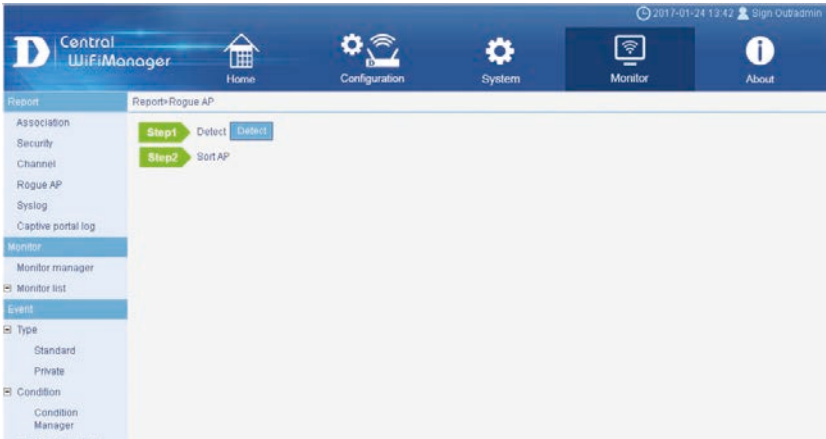


図 6-8 New AP (Detect)

「Detect」ボタンをクリックするとスキャンを開始し、以下のページが表示されます。このページはスキャンに使用するネットワーク上のアクセスポイントを選択することができます。

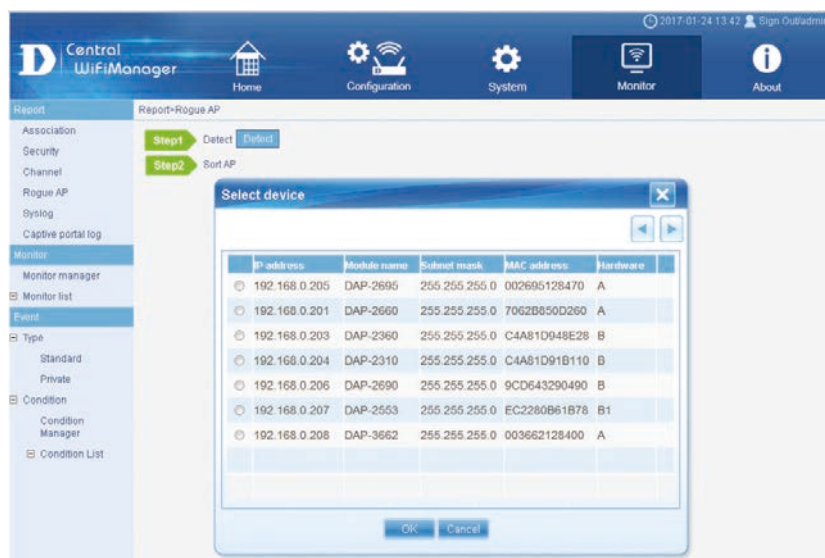


図 6-9 New AP (Detected)

アクセスポイントを選択し「OK」ボタンをクリックするとスキャンを開始します。
「Cancel」ボタンをクリックすると、スキャンをキャンセルしてメインページに戻ります。

「OK」ボタンをクリックしてスキャンを完了すると、以下のページが有効になります。本項目では、前項で選択したネットワーク上のアクセスポイントの無線範囲内にある分類されていないアクセスポイントが表示されます。

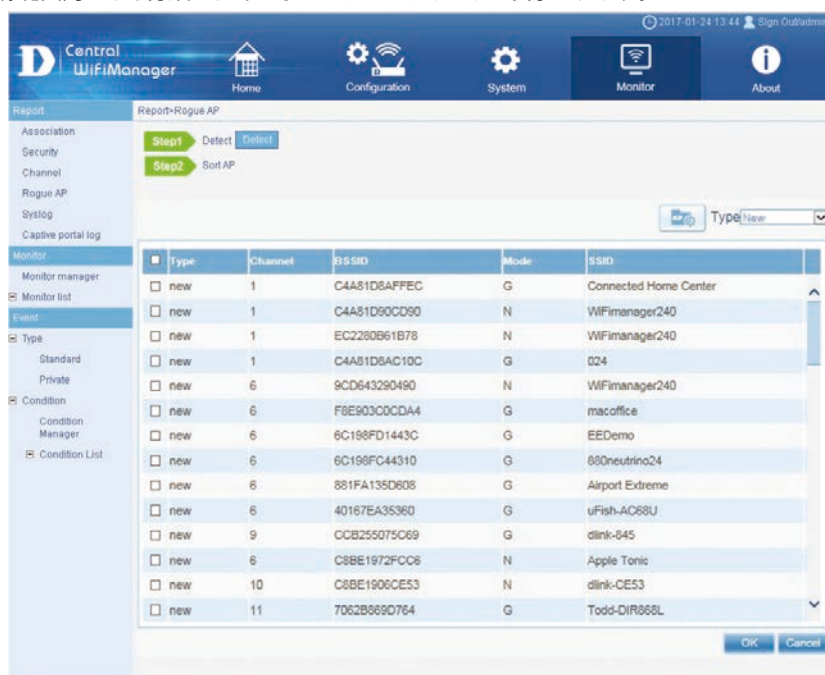


図 6-10 New AP (AP Detected)

このリストのアクセスポイントを分類するには、エントリの横のチェックボックスを選択して  ボタンをクリックし、リストから分類カテゴリ（「New」「Rogue」「Neighborhood」「Valid」）を選択します。

リストの表示エントリをフィルタして特定のカテゴリのみを表示するには、ドロップダウンメニューから「Type」オプション（「All」「New」「Rogue」「Neighborhood」「Valid」）を選択します。

アクセスポイントを選択し「OK」ボタンをクリックすると選択したアクセスポイントを目的のカテゴリに分類します。

「Cancel」ボタンをクリックすると、工程をキャンセルしてメインページに戻ります。

Rogue AP (不正アクセスポイント)

「Rogue AP」タブでは、ネットワークのアクセスポイントにより検出され、rogue アクセスポイントとして分類されたその環境のアクセスポイントの一覧を確認することができます。

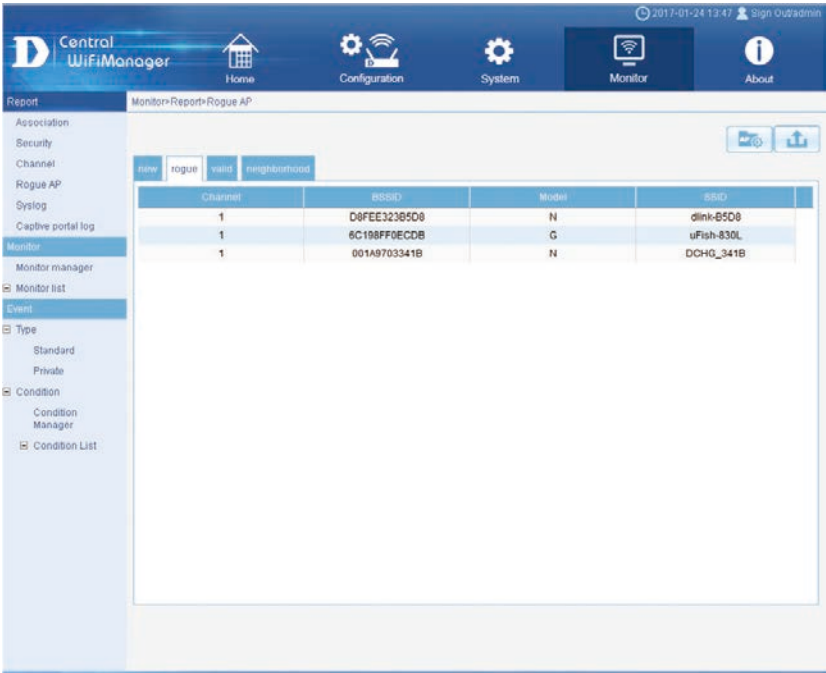


図 6-11 Rogue AP

- ボタンをクリックすると、ネットワークに接続されたアクセスポイントの範囲内で分類されていないアクセスポイントをスキャンします。
- ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

Valid AP (有効なアクセスポイント)

「Valid AP」タブでは、ネットワークのアクセスポイントにより検出された環境上にあり、有効なアクセスポイントとして分類されたアクセスポイントの一覧を確認することができます。

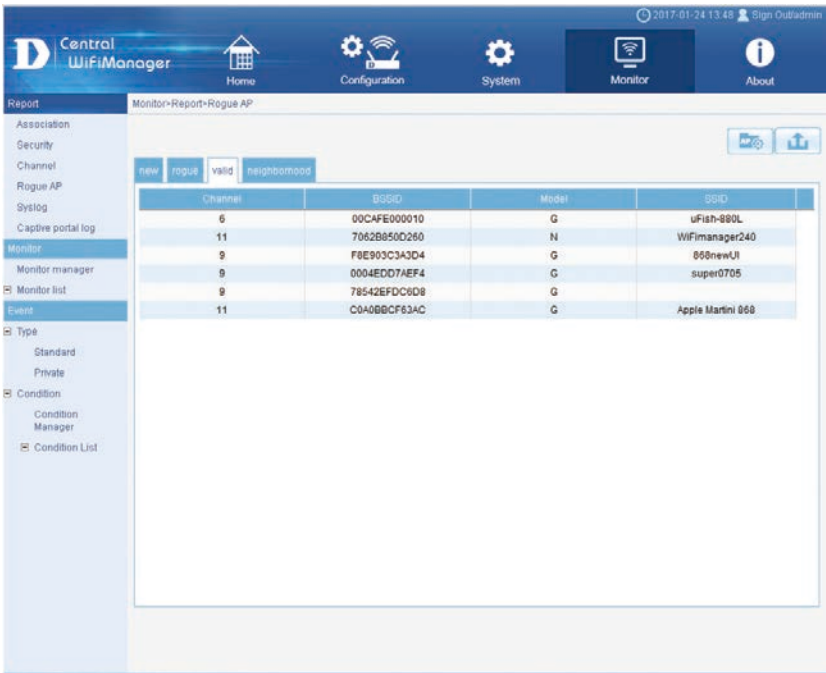


図 6-12 Valid AP

- ボタンをクリックすると、ネットワークに接続されたアクセスポイントの範囲内で分類されていないアクセスポイントをスキャンします。
- ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

Neighborhood (隣接のアクセスポイント)

「Neighborhood」タブでは、ネットワークのアクセスポイントにより検出された環境上にあり、隣接アクセスポイントとして分類されたその環境のアクセスポイントの一覧を確認することができます。

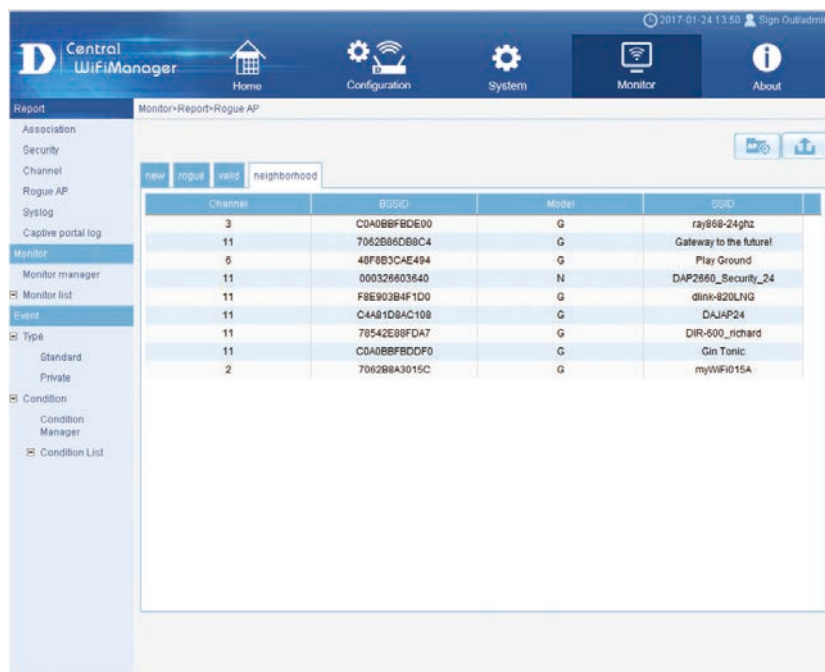


図 6-13 Neighborhood

 ボタンをクリックすると、ネットワークに接続されたアクセスポイントの範囲内で分類されていないアクセスポイントをスキャンします。

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。
このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

SysLog (シスログ)

上部パネルの「Monitor」と左パネルの「SysLog」をクリックすると、以下のページが表示されます。本項目では、ネットワークと CWM サーバアプリケーションで発生したイベントにより生成されたシステムログエントリを確認することができます。

Facility	Priority	Time stamp	Sender	Description
0	6	2014-08-12 17:04:21	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G-Association Success STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:14:26	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G-4-way handshake start STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:14:26	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G-4-way handshake success STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:14:49	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G-Association Success STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:14:49	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G-4-way handshake start STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:14:49	118.167.25.94	[00:26:95:12:84:70] [Wireless] 5G-4-way handshake success STA A0:88:B4:E4:D5:08
0	6	2014-08-12 17:32:05	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G-Association Success STA 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:33	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G-Association Success STA 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:39	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G-4-way handshake start STA A 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:39	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G-Association Success STA 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:40	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G-4-way handshake start STA A 84:7A:88:6C:48:18
0	6	2014-08-12 17:36:41	36.225.38.83	[00:26:95:12:84:70] [Wireless] 5G-4-way handshake start STA A 84:7A:88:6C:48:18

図 6-14 SysLog

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

Captive portal log (キャプティブポータルログ)

上部パネルの「Monitor」と左パネルの「Captive portal log」をクリックすると、以下のページが表示されます。本項目では、キャプティブポータルで発生したイベントにより生成されたログエントリを確認することができます。

Time stamp	AP Mac	Station Mac	Authentication	Action
------------	--------	-------------	----------------	--------

図 6-15 Captive portal log

 ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

Monitor (監視)

Monitor Manager (モニタ管理)

上部パネルの「Monitor」と左パネルの「Monitor Manager」をクリックすると、以下のページが表示されます。このページでは特定のデバイスで発生したイベントの詳細を監視する「監視ウォッチドッグ」の確認、作成、設定をします。

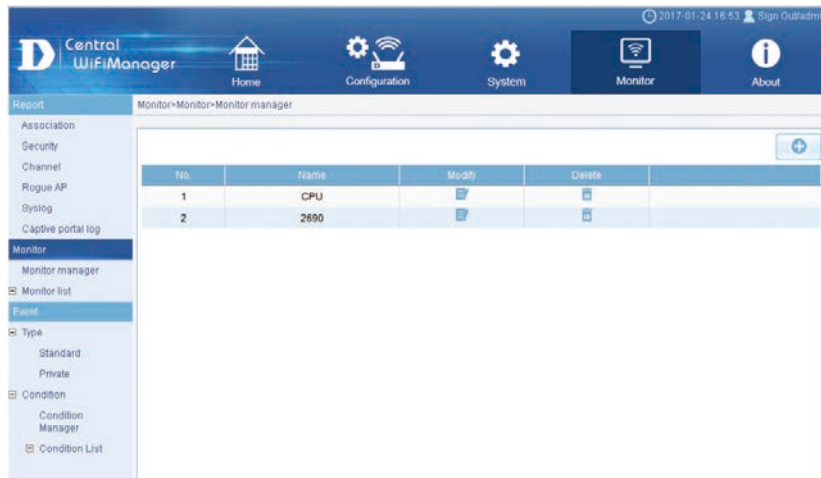


図 6-16 Monitor Manager

このページでは監視管理ウォッチドッグエントリの一覧が表示されています。

-  アイコンをクリックすると、新しい監視管理エントリを追加します。
-  アイコンをクリックすると、既存の監視管理エントリを修正します。
-  アイコンをクリックすると、既存の監視管理エントリを削除します。

モニタプロファイル作成

-  アイコンをクリックすると、以下のページが有効になります。このページでは監視管理ウォッチドッグの作成、そして設定ができます。

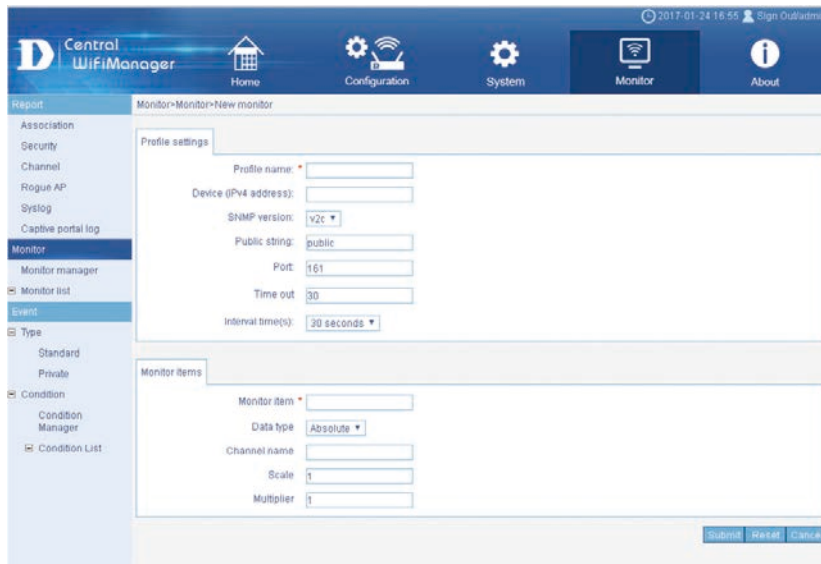


図 6-17 Create Profile

「Profile Settings」セクションでは、以下のパラメータが設定可能です。

項目	説明
Profile Name	プロファイル名を入力します。この名前はリストのエントリの識別に使用されます。
Device (IPv4 Address)	テキストボックスをクリックしてネットワークに関連するアクセスポイントの一覧を確認します。エントリを選択して「OK」をクリックし、フィールドに追加します。
SNMP version	このフィールドはエントリで使用される SNMP バージョンを表示します。初期値：SNMPv2c
Public string	パブリック SNMP の文字列名を入力します。初期値：public
Port	SNMP エージェントがリクエストメッセージを受信するために使用するポート番号を入力します。
Time out	メッセージのタイムアウト値を入力します。初期値：30
Interval Time(s)	時間間隔値を入力します。初期値：30 秒

「Monitor Items」 セクションでは、以下のパラメータが設定可能です。

項目	説明
Monitor Item	テキストボックスをクリックして有効な監視アイテムの一覧を確認します。 リストから監視アイテム（「TransmittedByte-2.4G」「ReceivedByte-2.4G」「TransmittedByte-5G」「ReceivedByte-5G」「CPU Utilization」）を選択します。
Data Type	データタイプ（「Absolute」（絶対）「Relative」（相対））を選択します。
Channel Name	チャンネル名を入力します。
Scale	スケール値を入力します。
Multiplier	乗算値を入力します。

「Submit」 ボタンをクリックすると変更を許可します。
「Reset」 ボタンをクリックすると入力した情報をクリアします。
「Cancel」 ボタンをクリックすると、変更を破棄しメインページに戻ります。

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

Monitor List (モニタリスト)

上部パネルの「Monitor」と左パネルの「Monitor List」をクリックすると、以下のページが表示されます。本項目では、前項目で作成した監視管理ウォッチドッグイベントのグラフチャートの確認ができます。作成されたイベント一覧は、左パネルの監視リスト下に表示されます。
ここでは例として監視管理イベント「Access-Point-1」を作成します。

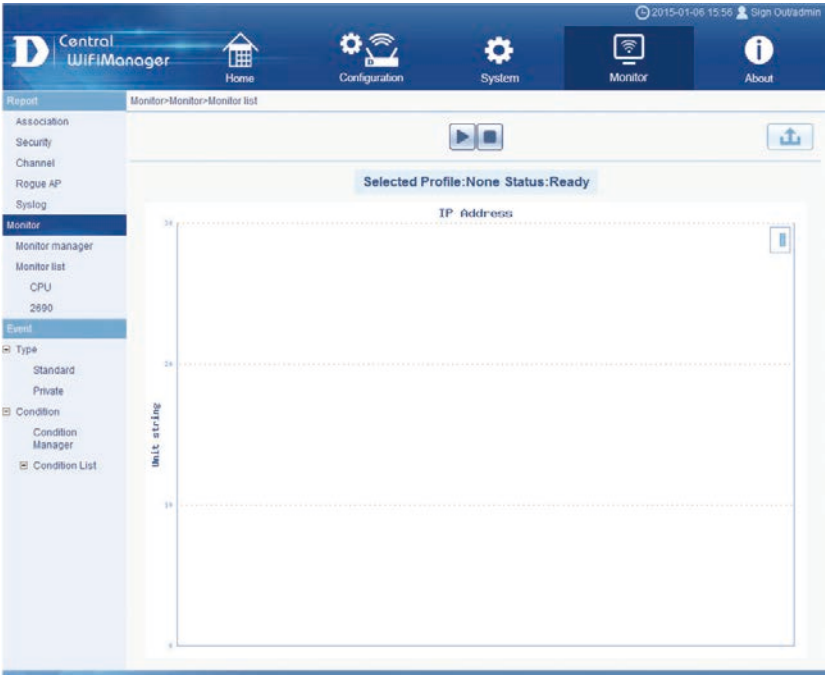


図 6-18 Monitor List

このページでは監視管理ウォッチドッグエントリの一覧が表示されています。

- ボタンをクリックすると、新しい監視イベントが稼働します。
- ボタンをクリックすると、監視イベントが停止します。
- ボタンをクリックすると、これらのリストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。
エクスポートは、「PNG」形式のファイルに対応します。
- ボタンをクリックすると監視管理イベントは稼働し、リアルタイムでの更新がチャートに表示されます。

このチャートでは「192.168.70.50」の IP アドレスを持つアクセスポイントの 2.4GHz 周波数帯の伝送されたデータを SNMPv2 とパブリック文字列を

使用して 30 秒間隔で監視します。

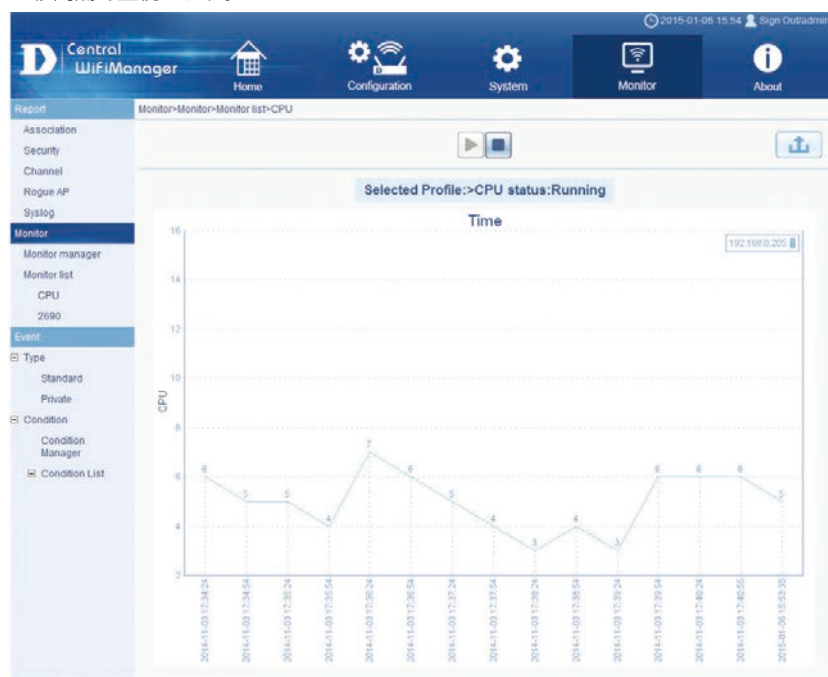


図 6-19 Monitor List (Real Time)

 ボタンをクリックすると、本チャートをこのインターフェースにアクセスしているコンピュータにエクスポートします。エクスポートは、「PNG」形式のファイルに対応します。

Event (イベント)

Type (各種イベント)

Standard (通常イベント)

上部パネルの「Monitor」と左パネルの **Event > Type > Standard** の順にクリックすると、以下のページが表示されます。
本項目では、「Event & Notice Settings」の設定に基づき生成された通常 (Standard) イベントタイプメッセージを確認することができます。
表示するイベントは、選択した基準のフィルタリングに基づくイベント、または発生したすべてのイベントで選択できます。

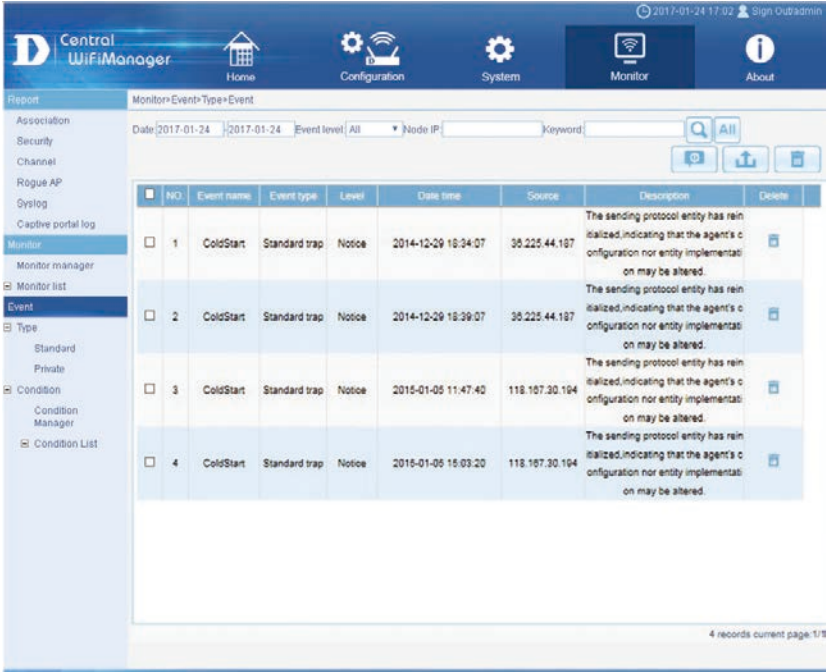


図 6-20 Standard

リストに表示するイベントをフィルタすると、以下のパラメータが設定可能になります。

項目	説明
Date	1 つ目のテキストボックスをクリックしてオプションから開始日を選択します。同様に、2 つ目のテキストボックスに終了日を選択します。
Event Level	ドロップダウンリストからイベントレベル (「all」 (すべて) 「critic」 (クリティック) 「error」 (エラー) 「warning」 (警告) 「notice」 (通知)) を選択します。
Node IP	ノードの IP アドレスを入力します。
Keyword	特定のキーワードを含むイベントのみを表示するには、テキストボックスにキーワードを入力します。

- ボタンをクリックすると、入力した基準に基づくエントリのみを表示します。
- ボタンをクリックすると、発生したすべてのスタンダードイベントを表示します。
- ボタンをクリックすると、新しいスタンダードイベントと通知を作成します。
- ボタンをクリックすると、リストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。
- 大きい ボタンをクリックすると、イベントリストからすべてのエントリを破棄します。
- 指定エントリの横にある小さな ボタンをクリックすると、イベントリストからそのエントリのみを破棄します。

Event タブ

 ボタンをクリックすると、以下のページが有効になります。このページではスタンダード SNMP イベントと、ネットワークでそのタイプのイベントが発生したとき「Standard」ページのメッセージ表示に使用される通知設定を設定することができます。

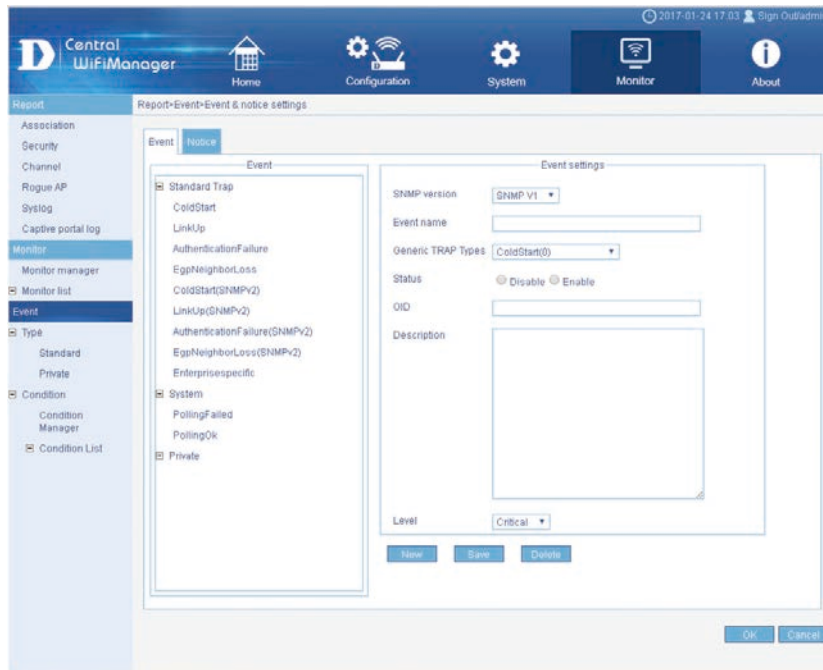


図 6-21 Event

「Event」タブでは、以下のパラメータが設定可能です。

項目	説明
Event	既存のスタンダードタブを修正するには、このセクションを選択します。既存トラップを選択後、パラメータは修正のために自動的に「Event Settings」セクションに入ります。新しいトラップを作成する場合は、このセクションではどのイベントも選択しません。
SNMP Version	トラップに使用する SNMP バージョン (SNMPv1、SNMPv2c) を選択します。既存トラップを修正中、このフィールドは変更できません。
Event Name	イベント名を入力します。この名前は、リストのイベントの識別に使用されます。
Generic TRAP Types	新しいトラップに使用するジェネリックトラップ (Coldstart(0) (コールドスタート)、WarmStart(1) (ウォームスタート)、LinkDown(2) (リンクダウン)、LinkUp(3) (リンクアップ)、AuthenticationFailure(4) (認証失敗)、EgpNeighborLoss(5) (隣接装置ダウン)、EnterpriseSpecific(6) (エンタープライズ指定)) を選択します。既存トラップを修正中、このフィールドは変更できません。
Status	指定トラップについて Enable (有効) または Disable (無効) を選択します。
OID	トラップのオブジェクト識別子 (OID) 番号を入力します。既存トラップを修正中、このフィールドは変更できません。
Description	トラップの概要を入力します。
Level	トラップのレベル (Critical (重大)、Error (エラー)、Warning (警告)、Notice (通知)) を選択します。

「New」ボタンをクリックすると、入新しいトラップを作成します。

「Save」ボタンをクリックすると、変更を適用します。

「Delete」ボタンをクリックすると、選択したトラップを削除します。

「OK」ボタンをクリックすると、変更を適用します。

「Cancel」ボタンをクリックすると、変更を破棄してメインページに戻ります。

注意 CWM では一部の特殊文字 ("&" "\") はサポート対象外となります。

Notice タブ

「Notice」タブでは、スタンダードトラップイベントが特定の警告レベルにより生成された際、通知機能を有効にすることができます。

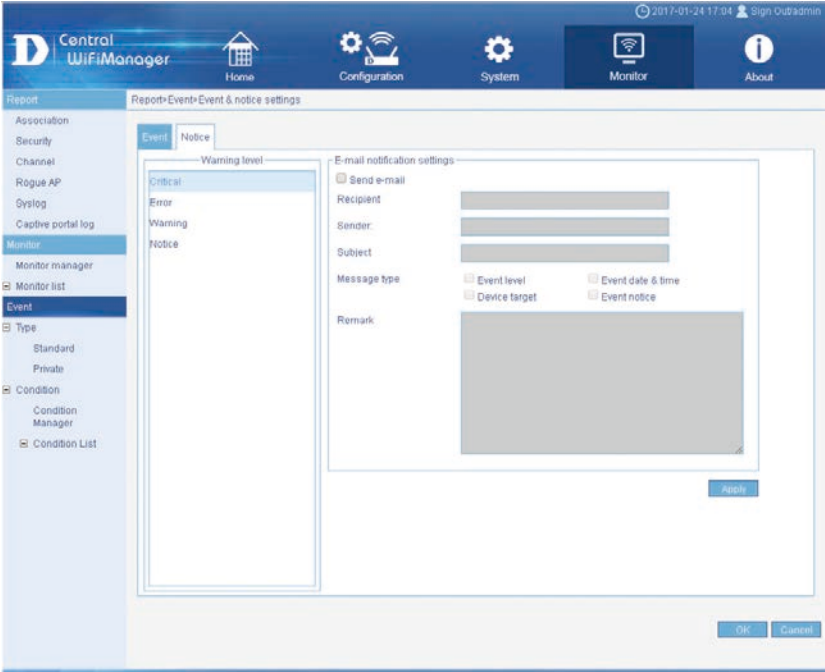


図 6-22 Notice

「Notice」タブでは、以下のパラメータが設定可能です。

項目	説明
Warning Level	警告レベル（Critical（重大）、error（エラー）、warning（警告）、notice（通知））を選択します。
Send E-Mail	警告レベルを選択後、オプションで選択した警告レベルの E メール通知機能を有効にします。
Recipient	受信者の E メールアドレスを入力します。
Sender	送信者の E メールアドレスを入力します。
Subject	Eメールの件名（Subject）を指定します。
Message Type	メッセージタイプ（Event Level、Event Date/Time、Device Target、Event Notice）を選択します。
Remark	メッセージのリマークを入力します。

- 「Apply」ボタンをクリックすると、変更を適用します。
- 「OK」ボタンをクリックすると、変更を適用します。
- 「Cancel」ボタンをクリックすると、変更を破棄してメインページに戻ります。

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

Private (プライベートイベント)

上部パネルの「Monitor」と左パネルの **Event > Type > Private** の順にクリックすると、以下のページが表示されます。本項目では、「Event & Notice Settings」の設定に基づき生成されたプライベートイベントタイプメッセージを確認することができます。

特定デバイスのみで発生するプライベートイベントは、CWM サーバアプリケーションにより管理されます。これらのイベントは、製品固有のものです。このリストでは、表示するイベントを選択した基準のフィルタリングに基づくイベント、または発生したすべてのイベントで選択することができます。

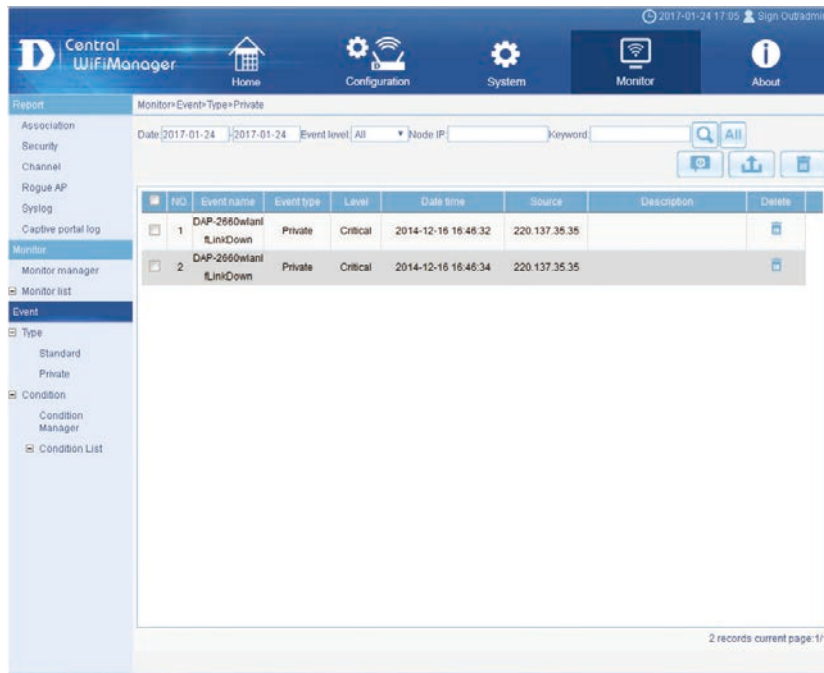


図 6-23 Private

リストに表示するイベントをフィルタすると、以下のパラメータが設定可能になります。

項目	説明
Date	1つ目のテキストボックスをクリックしてオプションから開始日を選択します。同様に、2つ目のテキストボックスに終了日を選択します。
Event Level	ドロップダウンリストからイベントレベル（「All」（すべて）「critic」（クリティック）「error」（エラー）「warning」（警告）「notice」（通知））を選択します。
Node IP	ノードの IP アドレスを入力します。
Keyword	特定のキーワードを含むイベントのみを表示するには、テキストボックスにキーワードを入力します。

 ボタンをクリックすると、入力した基準に基づくエントリのみを表示します。

 ボタンをクリックすると、発生したすべてのスタンダードイベントを表示します。

 ボタンをクリックすると、新しいスタンダードイベントと通知を作成します。

 ボタンをクリックすると、リストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。

大きい  ボタンをクリックすると、イベントリストからすべてのエントリを破棄します。

指定エントリの横にある小さな  ボタンをクリックすると、イベントリストからそのエントリのみを破棄します。

Event タブ

 ボタンをクリックすると、以下のページが有効になります。このページではプライベート SNMP イベントと、ネットワークでそのタイプのイベントが発生したとき「Private」ページのメッセージ表示に使用される通知設定を設定することができます。

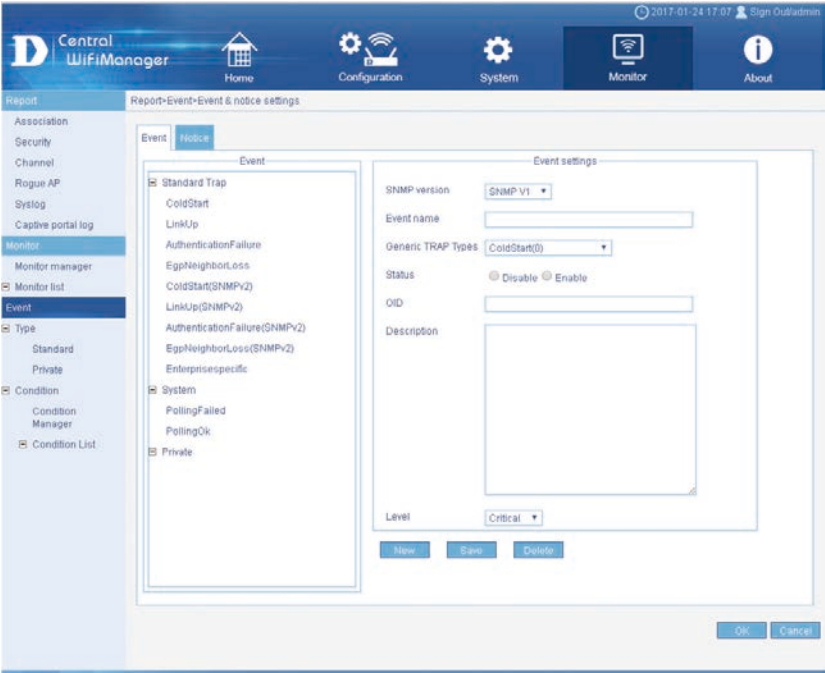


図 6-24 Event (Private)

「Event」タブでは、以下のパラメータが設定可能です。

項目	説明
Event	既存のスタンダードタブを修正するには、このセクションを選択します。既存トラップを選択後、パラメータは修正のために自動的に「Event Settings」セクションに入ります。新しいトラップを作成する場合は、このセクションではどのイベントも選択しません。
SNMP Version	トラップに使用する SNMP バージョン (SNMPv1、SNMPv2c) を選択します。既存トラップを修正中、このフィールドは変更できません。
Event Name	イベント名を入力します。この名前は、リストのイベントの識別に使用されます。
Generic TRAP Types	新しいトラップに使用するジェネリックトラップ (Coldstart(0) (コールドスタート)、WarmStart(1) (ウォームスタート)、LinkDown(2) (リンクダウン)、LinkUp(3) (リンクアップ)、AuthenticationFailure(4) (認証失敗)、EgpNeighborLoss(5) (隣接装置ダウン)、EnterpriseSpecific(6) (エンタープライズ指定)) を選択します。既存トラップを修正中、このフィールドは変更できません。
Status	指定トラップについて Enable (有効) または Disable (無効) を選択します。
OID	トラップのオブジェクト識別子 (OID) 番号を入力します。既存トラップを修正中、このフィールドは変更できません。
Description	トラップの詳細を入力します。
Level	トラップのレベル (Critical (重大)、Error (エラー)、Warning (警告)、Notice (通知)) を選択します。

- 「New」ボタンをクリックすると、入新しいトラップを作成します。
- 「Save」ボタンをクリックすると、変更を適用します。
- 「Delete」ボタンをクリックすると、選択したトラップを削除します。
- 「OK」ボタンをクリックすると、変更を適用します。
- 「Cancel」ボタンをクリックすると、変更を破棄してメインページに戻ります。

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

Notice タブ

「Notice」タブでは、プライベートトラップイベントが特定の警告レベルにより発生した際、通知機能を有効にすることができます。

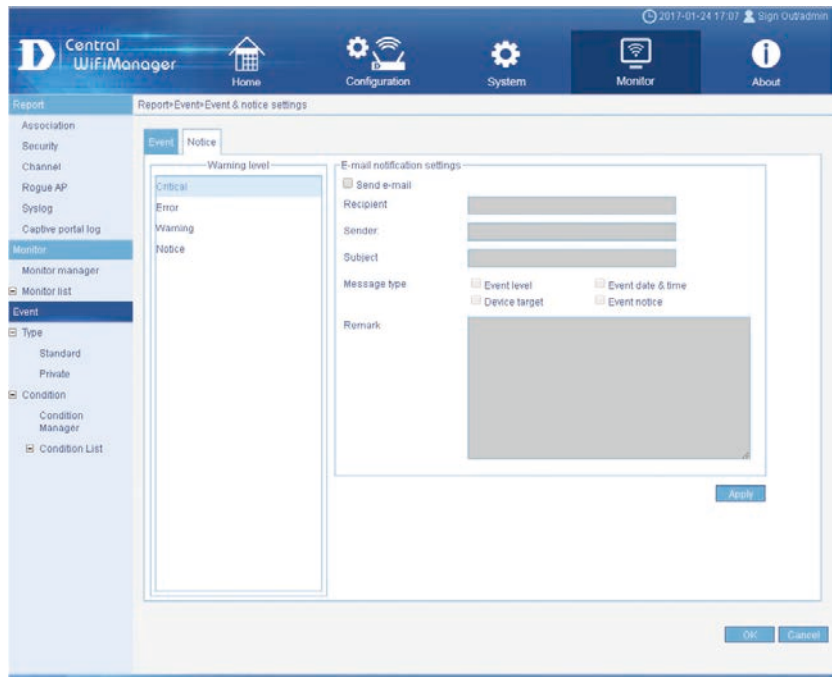


図 6-25 Notice (Private)

「Notice」タブでは、以下のパラメータが設定可能です。

項目	説明
Warning Level	警告レベル（Critical（重大）、error（エラー）、warning（警告）、notice（通知））を選択します。
Send E-Mail	警告レベルを選択後、オプションで選択した警告レベルの E メール通知機能を有効にします。
Recipient	受信者の E メールアドレスを入力します。
Sender	送信者の E メールアドレスを入力します。
Subject	Eメールの件名（Subject）を指定します。
Message Type/	メッセージタイプ（Event Level、Event Date/Time、Device Target、Event Notice）を選択します。
Remark	メッセージのリマークを入力します。

- 「Apply」ボタンをクリックすると、変更を適用します。
- 「OK」ボタンをクリックすると、変更を適用します。
- 「Cancel」ボタンをクリックすると、変更を破棄してメインページに戻ります。

注意 CWM では一部の特殊文字 ("&\") はサポート対象外となります。

Condition (コンディション)

Condition Manager (コンディション管理)

上部パネルの「Monitor」と左パネルの **Event > Condition > Condition Manager** の順にクリックすると、以下のページが表示されます。本項目では、管理プロファイルの確認、作成、設定をすることができます。
既存するコンディション管理プロファイルがリストに表示されます。

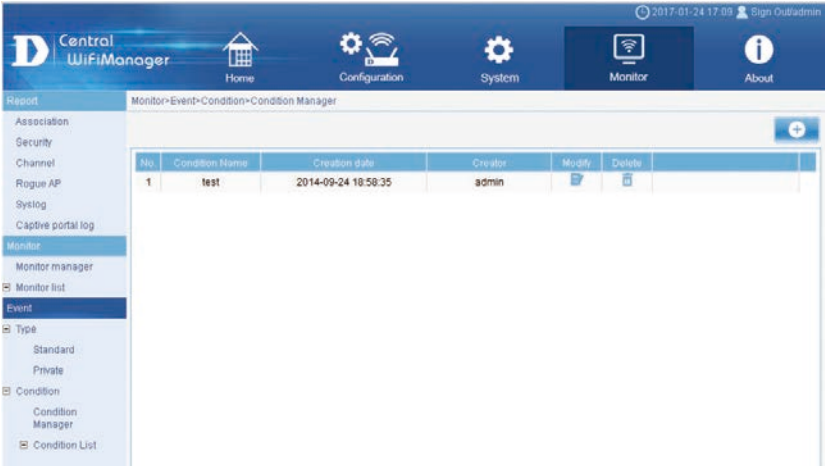


図 6-26 Condition Manager

- アイコンをクリックすると、新しいコンディション管理プロファイルを追加します。
- アイコンをクリックすると、既存のコンディション管理プロファイルを修正します。
- アイコンをクリックすると、既存のコンディション管理プロファイルを削除します。

コンディション作成

- アイコンをクリックすると、以下のページが表示されます。本項目では、新しいコンディション管理プロファイルを作成します。

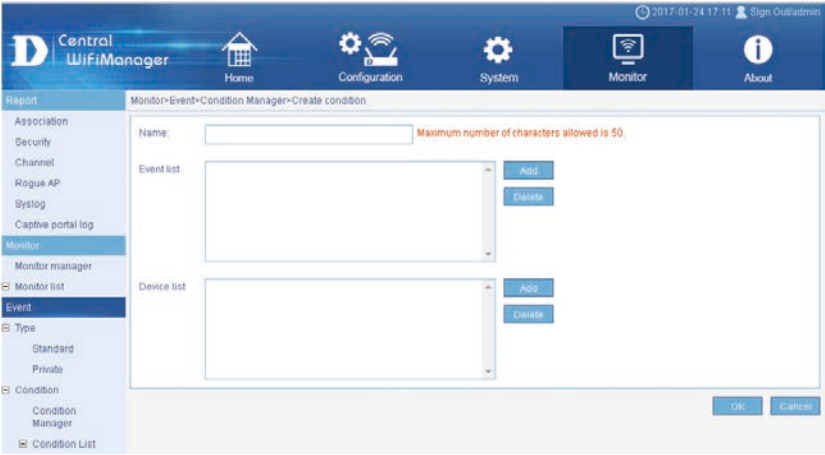


図 6-27 Create Condition

以下のパラメータが設定可能です。

項目	説明
Name	コンディション管理プロファイル名を入力します。
Event List	イベントをイベントリストに追加するには、「Add」ボタンをクリックします。イベントリストからイベントを破棄するには、破棄するイベントを選択して「Delete」ボタンをクリックします。
Device List	デバイスをデバイスリストに追加するには、「Add」ボタンをクリックします。デバイスリストからデバイスを破棄するには、破棄するデバイスを選択して「Delete」ボタンをクリックします。

「OK」ボタンをクリックすると、変更を適用します。
「Cancel」ボタンをクリックすると、変更を破棄してメインページに戻ります。

注意 CWM では一部の特殊文字 ("&"\) はサポート対象外となります。

「Event List」パラメータの横の「Add」ボタンをクリックすると、以下のウィンドウが表示されます。

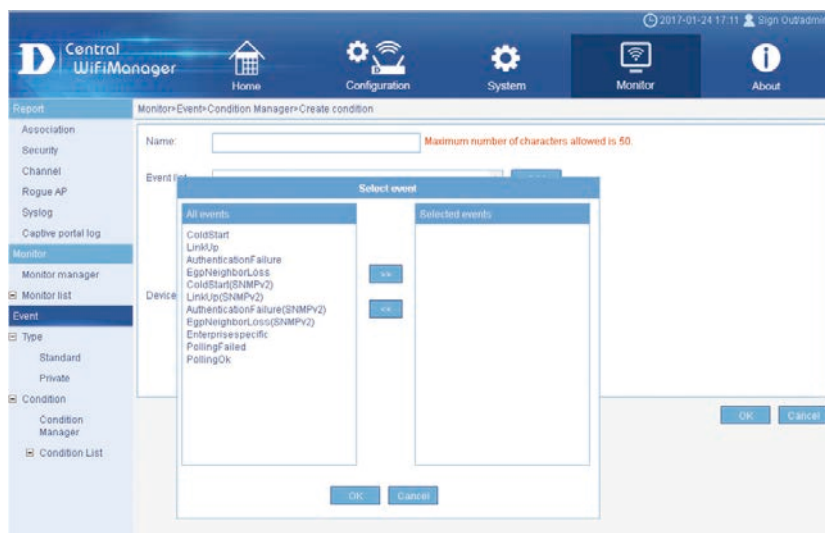


図 6-28 Create Condition (Add/Event List)

「All Event」セクションでは、すべての有効なトラップイベントが表示されます。

これらのイベントの1つまたはそれ以上を使用するには、対象を選択し「>>」ボタンをクリックして「Selected Event」セクションに追加します。

選択したイベントの1つまたはそれ以上を「Selected Events」セクションから破棄するには、対象を選択し「<<」ボタンをクリックします。

「OK」ボタンをクリックすると、選択を適用します。

「Cancel」ボタンをクリックすると、選択を破棄してメインページに戻ります。

「Device List」パラメータ横の「Add」ボタンをクリックすると、以下のウィンドウが表示されます。

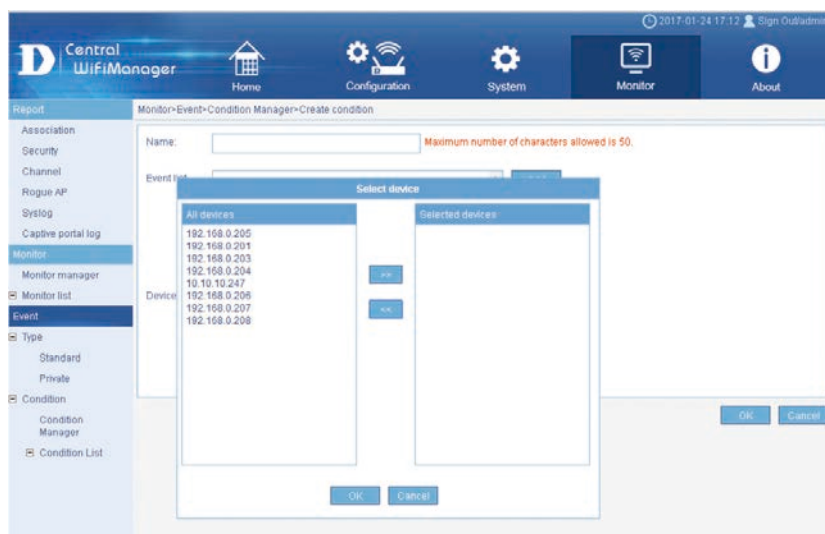


図 6-29 Create Condition (Add/Device List)

「All Event」セクションでは、すべての有効なトラップイベントが表示されます。

これらのイベントの1つまたはそれ以上を使用するには、対象を選択し「>>」ボタンをクリックして「Selected Event」セクションに追加します。

選択したイベントの1つまたはそれ以上を「Selected Devices」セクションから破棄するには、対象を選択し「<<」ボタンをクリックします。

「OK」ボタンをクリックすると、選択を適用します。

「Cancel」ボタンをクリックすると、選択を破棄してメインページに戻ります。

Condition List (コンディションリスト)

前セクションでウォッチ管理プロファイルをクリックした後、それらのプロファイルは左パネルの「Condition List」 オプションセクションに対し有効になります。ここでは例としてネットワークの無線リンク上のアクセスポイントがダウンしたときにイベントを生成するコンディション管理プロファイル「WiFi-Link-Down」を作成しています。

上部パネルの「Monitor」と左パネルの「Event」>「Condition」>「Condition List」>「WiFi-Link-Down」の順にクリックすると、以下のページが表示されます。本項目では、ウォッチ管理プロファイルの設定に基づき生成されたウォッチリストメッセージを確認することができます。

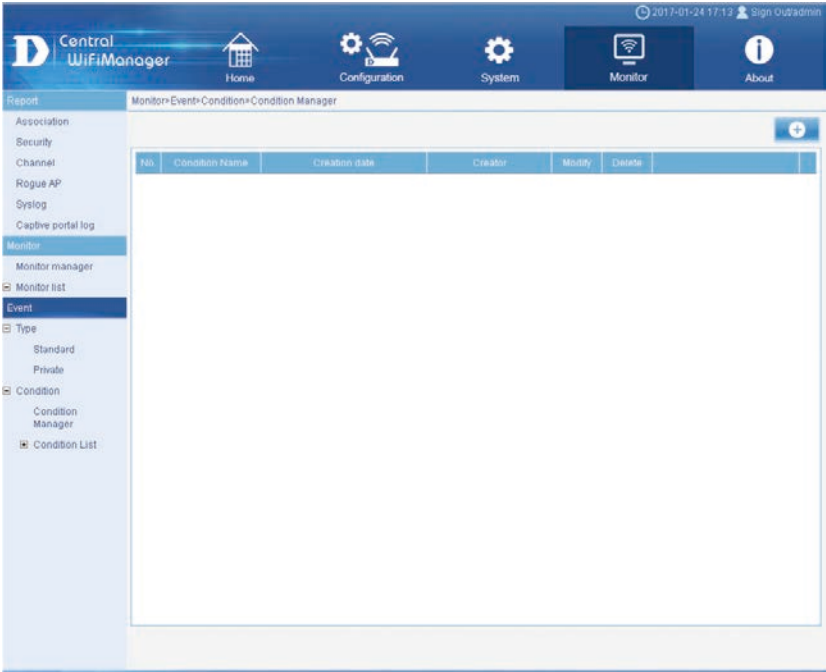


図 6-30 Condition List

リストに表示するイベントをフィルタすると、以下のパラメータが設定可能になります。

項目	説明
Date	1 つ目のテキストボックスをクリックしてオプションから開始日を選択します。同様に、2 つ目のテキストボックスに終了日を選択します。
Event Level	ドロップダウンリストからイベントレベル（「all」（すべて）「critic」（クリティック）「error」（エラー）「warning」（警告）「notice」（通知））を選択します。
Node IP	ノードの IP アドレスを入力します。
Keyword	特定のキーワードを含むイベントのみを表示するには、テキストボックスにキーワードを入力します。

-  ボタンをクリックすると、入力した基準に基づくエントリのみを表示します。
-  ボタンをクリックすると、発生したすべてのプライベートイベントを表示します。
-  ボタンをクリックすると、新しいプライベートイベントと通知を作成します。
-  ボタンをクリックすると、リストに表示された内容をこのインターフェースにアクセスしているコンピュータにエクスポートします。このエクスポートは、「TXT」、「PDF」、「Excel」形式のファイルに対応します。
- 大きい  ボタンをクリックすると、イベントリストからすべてのエントリを破棄します。
- 指定エントリの横にある小さな  ボタンをクリックすと、イベントリストからそのエントリのみを破棄します。

【付録 A】 フロントデスクユーザアカウントの作成

フロントデスクユーザアカウントは、無線ネットワークの使用を制限時間内のみ許可されたゲストのためのアカウントになります。

ここではフロントデスクスタッフアカウントの作成方法と、ゲストパスワードの生成方法について説明します。

「front desk staff」アカウントを設定するには、管理アカウントでCWM サーバアプリケーションに入る必要があります。上部メニューの「System」と左メニューの「User Manager」で操作してください。  ボタンをクリックし新しいユーザアカウントを作成します。

 ボタンをクリックすると以下のページとパラメータが有効になります。

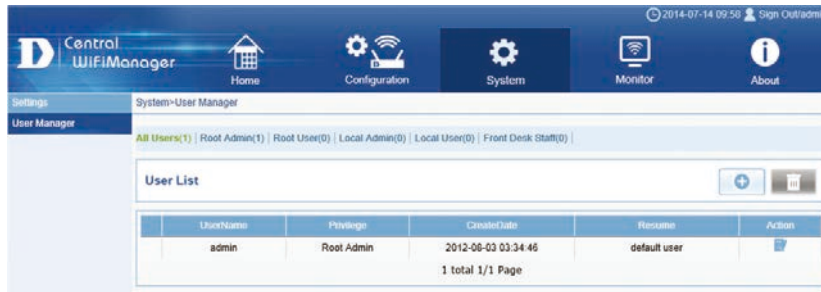


図 7-1 front desk staff

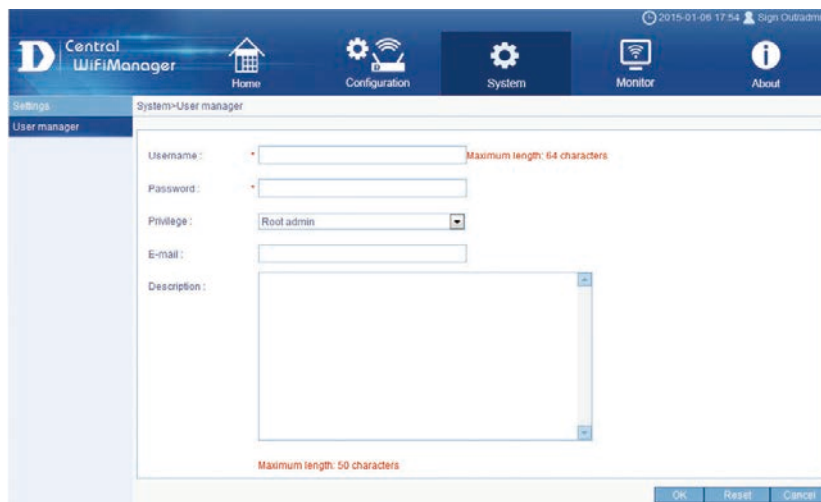


図 7-2 User Manager

以下の項目があります。

項目	説明
Username	フロントデスクスタッフアカウントのユーザ名を入力します。
Password	フロントデスクスタッフアカウントのパスワードを入力します。
Privilege	「Front Desk Staff」のオプションを選択します。
E-mail	フロントデスクスタッフのEメールアドレスを入力します。
Description/	このアカウントについての追加情報を入力します。

「OK」ボタンをクリックすると、新しいアカウントを作成します。

「Reset」ボタンをクリックすると、このフィールドに入力した情報をクリアします。

注意 CWM では一部の特殊文字 ("&" "\") はサポート対象外となります。

【付録A】 フロントデスクユーザアカウントの作成

フロントデスクスタッフアカウントの追加に成功すると、ユーザ管理リストに表示されます。

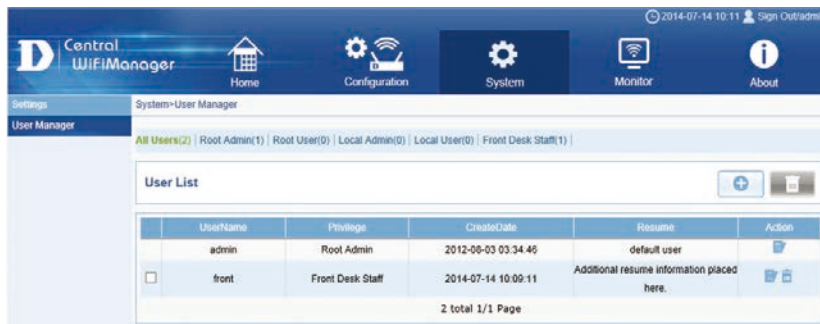


図 7-3 User Manager Table

次にゲスト無線ネットワークにユーザ認証のパスコードを設定します。上部メニューの「Configuration」を操作し、左メニューでネットワークを選択します。例では、ゲストネットワークは「Headquarters」サイトの「Server-Room」ネットワーク内に配置しています。



図 7-4 SSID (SR-Guest)

この例では、ゲストネットワークの SSID は「SR-Guest」です。

「SR-Guest」エントリの ボタンをクリックしてパスコードユーザ認証を有効にします。

ボタンをクリックすると、以下のページが有効になり、SSID「SR-Guest」のパラメータを修正することができます。

「User Authentication」セクションで、「Passcode as the Authentication Type」を選択、「Save」ボタンをクリックすると変更が適用されます。

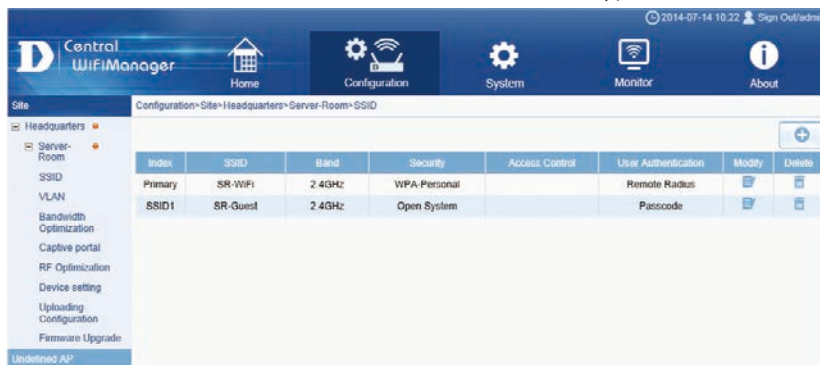


図 7-5 SR-Guest (Passcode)

SSID のユーザ認証のパスコード設定に成功すると、「User Authentication」エントリコラムには「SR-Guest」エントリの「Passcode」が表示されます。

ネットワークのアクセスポイントは、関連するアクセスポイントの設定が更新されるまでこれらの新しい変更を認識しません。関連するアクセスポイントの設定を手動で更新するには、上部メニューの「Configuration」と、左メニューのネットワークリンクを操作してください。この例でのネットワークは「Server-Room」です。

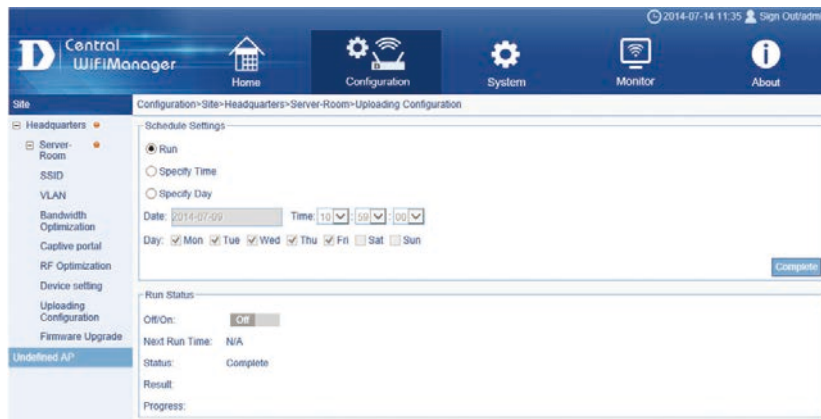


図 7-6 Schedule Setting

左メニューの「Upload Configuration」オプションを選択します。「Schedule Settings」セクションで、「Run」オプションを選択し、「Complete」ボタンをクリックします。

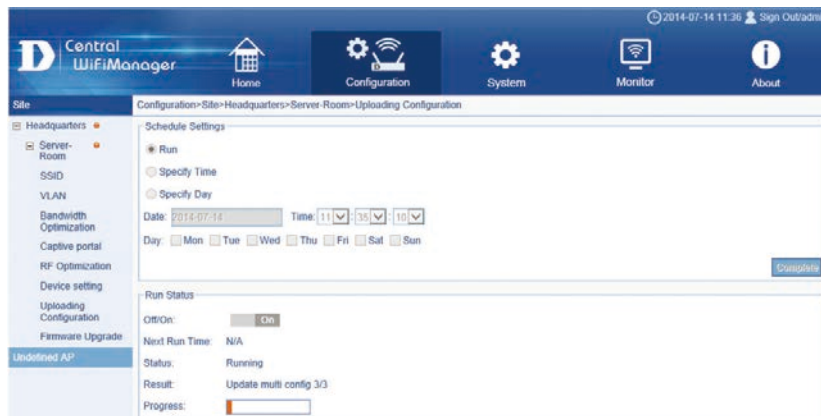


図 7-7 Run Status

設定は「Run Status」セクションに表示されるように関連するアクセスポイントにアップロードされます。コンフィグレーションファイルがアクセスポイントにアップロードされると、「Run Status」セクションの「Status」オプションが「Complete」となります。

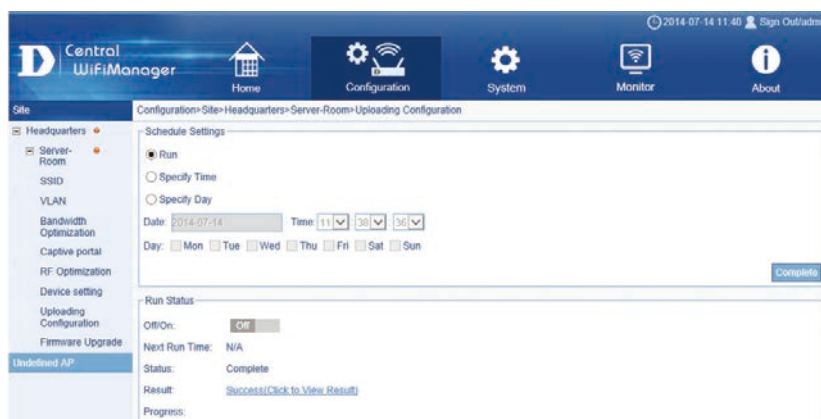


図 7-8 Run Status (Complete)

【付録A】 フロントデスクユーザアカウントの作成

次に、新しいフロントデスクスタッフユーザアカウントをサイトのネットワークメンバリストに追加します。上部メニューの「Configuration」を操作し、左メニューで関連サイトを選択します。この例でのサイト名は「Headquarters」です。

すべてのネットワークは「Network List」リストに表示されます。この例でのネットワークは「Server-Room」です。エントリ横の  をクリックするとネットワークを修正します。

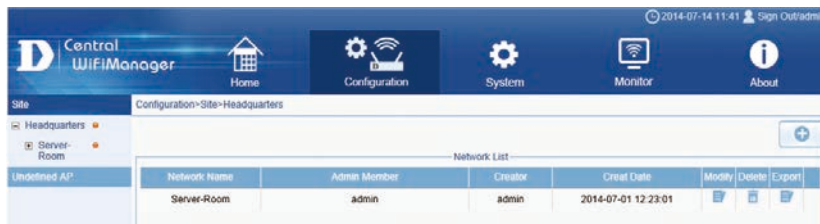


図 7-9 Network List (Server-Room)

 ボタンをクリックすると、次のページが有効になります。フロントデスクスタッフユーザアカウントは有効になり、選択して「>>」をクリックし、「Selected」コラムに移動することによりこのネットワークに追加可能となります。

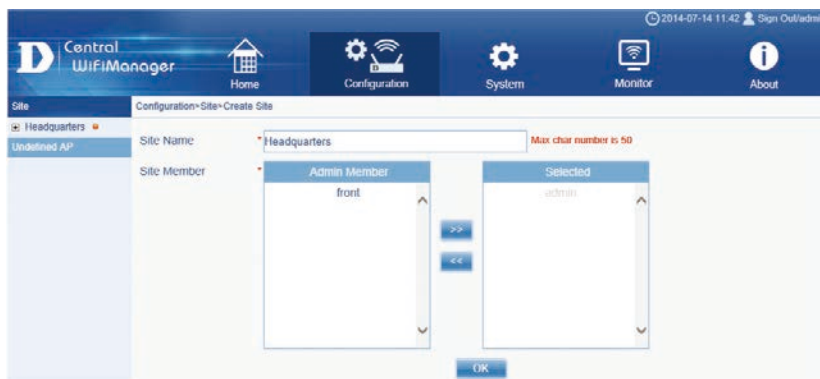


図 7-10 Selected

「OK」ボタンをクリックすると変更を適用します。

この後、ネットワークのアクセスポイントにコンフィギュレーションファイルを再びアップロードします。手順については前の項を参照してください。

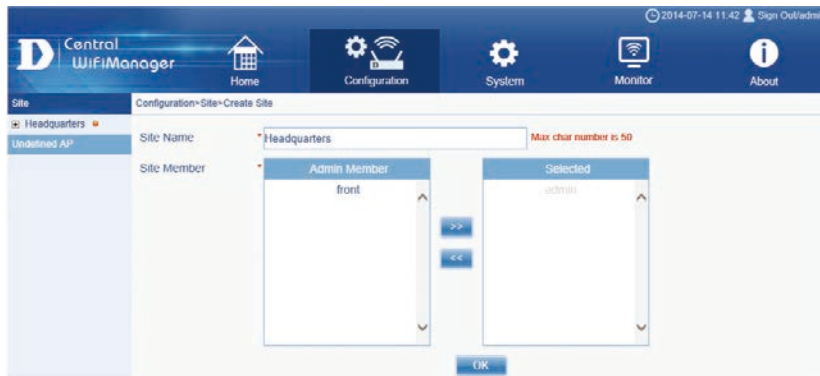


図 7-11 Uploads

管理アカウントからログアウトし、フロントデスクスタッフアカウントに戻ります。

フロントデスクアカウント名とパスワードを入力し、「Login」 ボタンをクリックしてフロントデスクアカウントとしてログインします。

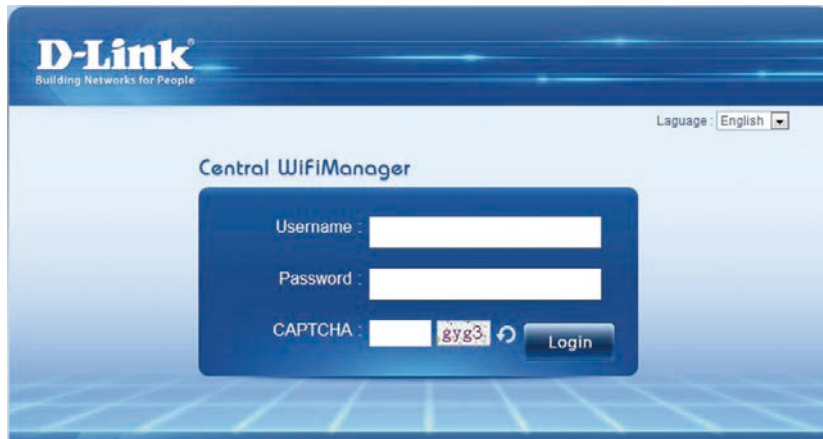


図 7-12 Login

フロントデスクアカウントでのログインに成功すると、以下のページが有効になります。ここではフロントデスクユーザのパスコードを生成します。



図 7-13 Passcode Settings

以下の項目があります。

項目	説明
SSID	生成したパスコードを使用して一時的に無線ネットワークにアクセスするために使用するネットワーク SSID が表示されます。
Security Key	パスコードは手動で入力可能です。空欄にした場合システムがランダムにパスコードを生成します。「Display Security Key」 オプションを選択すると、このフィールドに入力した文字を表示することができます。
Pass Code Quantity	生成されたパスコードの数を入力します。通常、生成されるパスコードは 1 つです。
Duration	無線接続の持続期間を入力します。
Last Active Day	このコードを使用した最後のアクティブ日を選択します。
Device Limit	デバイスの制限値を入力します。値は、このパスコードを使用できるアクティブユーザの最大数です。

「Generate」 ボタンをクリックすると、新しいパスコードを生成します。

左メニューの「View/Edit/Delete」 オプションをクリックすると、生成されたパスコードの一覧を確認することができます。フロントデスクスタッフがアクティブとパッシブな接続を監視するために有用な「Duration Remaining」と「Status」 フィールドが表示されます。

-  アイコンをクリックすると、既存のエントリを修正します。
-  アイコンをクリックすると、既存エントリを削除します。

	Passcode	SSID	Duration	User limit	Last active date	Duration remaining	Creator	Status	Edit	Delete
D-Link_TW	54597967	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk			
D-Link_US	68956522	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk			
D-Link_EU	25176003	GO to CWM24	10 hour(s)	5	15-01-30	0	frontdesk			
D-Link_KR	01291468	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk			
D-Link_IN	23160099	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk			
D-Link_AU	61721043	GO to CWM24	10 hour(s)	5	15-01-30	0	frontdesk			
D-Link_CN	85314185	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk			
D-Link_JG	55182153	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk			
	54581108	GO to CWM24	10 hour(s)	5	15-01-30	not active	frontdesk			

図 7-14 Passcode List

パスコードはフロントデスクスタッフによりフロントデスクユーザに与えられます。

新しいパスコードを生成するには、フロントデスクスタッフは「Central Wi-Fi Manager Server」アプリケーションにログインし、フロントデスクユーザアカウントの詳細により、関連する「パスコード情報」を入力します。次に「Generate」をクリックしてフロントデスクユーザに付与するコードを取得します。「パスコード情報」は指定の「Duration」の時間に基づき、有効期限が切れると破棄されます。

フロントデスクユーザは有効な無線ネットワークに接続し、Web ブラウザを使用しネットワークやインターネットへの接続をしようとする際、パスコードの入力を求められます。フロントデスクスタッフにより供給された正しいコードを入力すると、フロントデスクユーザはパスコードの持続時間中、ネットワークやインターネットへの接続が可能となります。

図 7-15 entering passcode

【付録 B】 キャプティブポータルログインページのカスタマイズ

「キャプティブポータルログインページ」のカスタマイズには、カスタマイズのための3つの「スタイリングオプション」があり、以下の手順に従ってのカスタマイズが可能です。各スタイリングオプションは異なるUIスタイルを示し、該当のWebページのソースファイルを編集します。以下は、各スタイリングオプションを変更するための編集可能なファイルの概要です。

- ・「Pages_default」：ログインページに「テキスト」と「画像」を表示します。
- ・「Pages_license」：ログインページに「テキスト」と「画像」に加え「独自のロゴ画像」を表示します。
- ・「Pages_headerpic」：ログインページに「テキスト」と「画像」に加え「独自のロゴ画像」と「ヘッダー画像」を表示します。

「画像」は既存の画像を、「テキスト」は既存の「text.js」ファイルを置き換えることによりカスタマイズされます。

ソースファイルの入手

ソースファイルは、「Configuration」メニュー下の「SSID」ページから入手することができます。

「Splash page customization」で、ドロップダウンメニューからスタイルを選択し、「Download Template」をクリックすると、ソースファイルをダウンロードします。

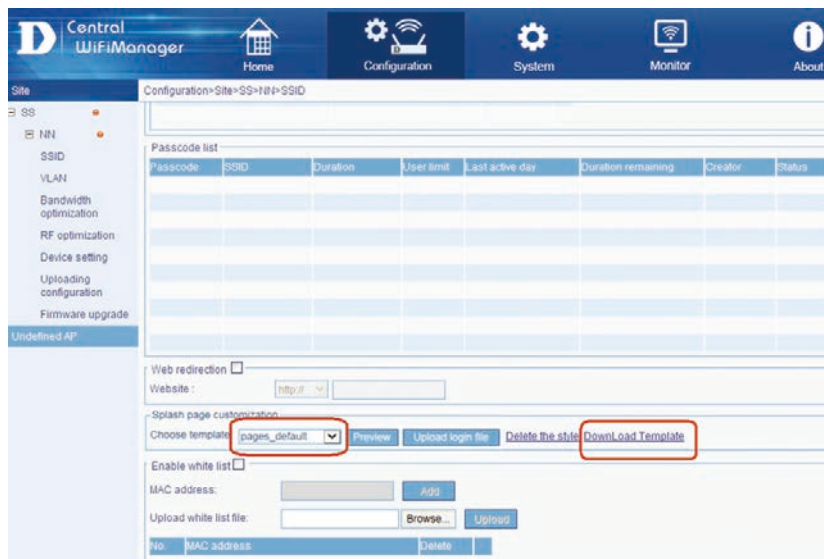


図 7-16 source file

ダウンロードするソースファイルは、ドロップダウンメニューから選択したファイル名と同じである必要があります。ダウンロードしたファイルは、拡張子「.tar」（例：Pages_default.tar）付の圧縮ファイルとなります。ファイルの解凍には対応した解凍ツールを使用してください。ソースファイルは解凍したフォルダに配置する必要があります。

各スタイリングソースファイルの内容とイラスト

「Pages_default」：bg.png、login_box.png、login_login.png、text.js

- ・ カスタマイズは「png」形式の画像ファイルを使用し、同じファイル名を使用してください。
- ・ text.js ファイルに入力するテキストは UTF-8 エンコーディング形式を使用してください。



図 7-17 Pages_default

【付録B】 キャプティブポータルログインページのカスタマイズ

「Pages_license」: bg.png、bott.png、logo.png、text.js

- ・ カスタマイズは「png」形式の画像ファイルを使用し、同じファイル名を使用してください。
- ・ text.js ファイルに入力するテキストは UTF-8 エンコーディング形式を使用してください。



図 7-18 Pages_license

「Pages_headerpic」: bg.png、bg_top.png、bott.png、logo.png、text.js

- ・ カスタマイズは、「png」形式の画像ファイルを使用し、同じファイル名を使用してください。
- ・ text.js ファイルに入力するテキストは UTF-8 エンコーディング形式を使用してください。

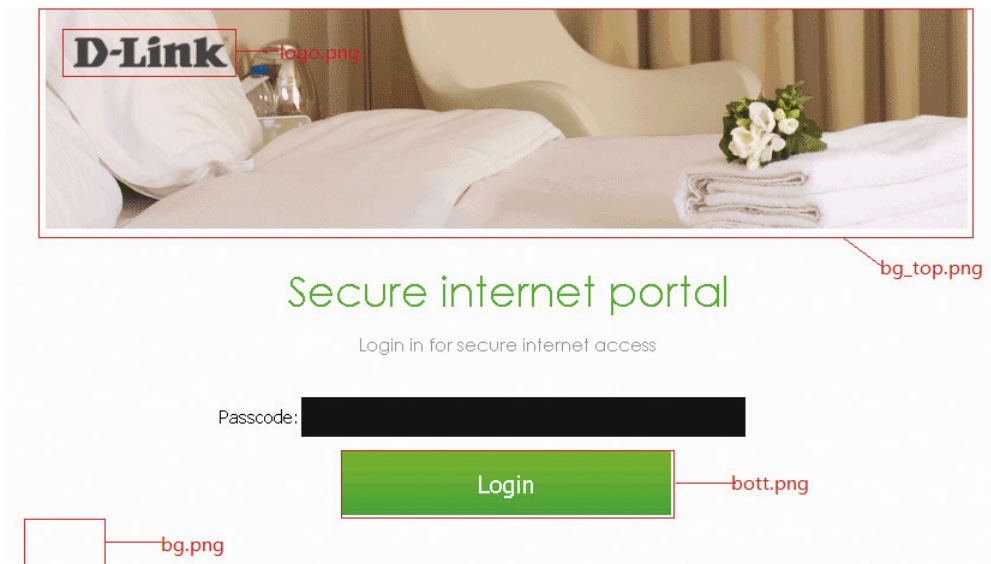


図 7-19 Pages_headerpic

the text.js ファイルテキストの編集

テキストエディタソフトで text.js ファイルを開きます。ファイルにある以下のパラメータの “=” の後の値を変更してログインページに表示するテキストをカスタマイズします。

```
var username=" Username" ;
var password=" Password" ;
var login=" Login" ;
var license_notice=" Logging in indicates you have read and accepted the license" ;
var license_link=" Use Policy" ;
```

カスタマイズ後のソースファイルのアップデート

解凍したソースファイルを編集後、「tar」形式にファイルを圧縮してから CWM にアップロードします。
 以下は圧縮ソフト「7-zip」を使用した圧縮ファイルの例です。

1. 解凍したすべてのソースファイルを選択して右クリックします。ドロップダウンメニューから「7-Zip」>>「Add to archive」の順に選択します。

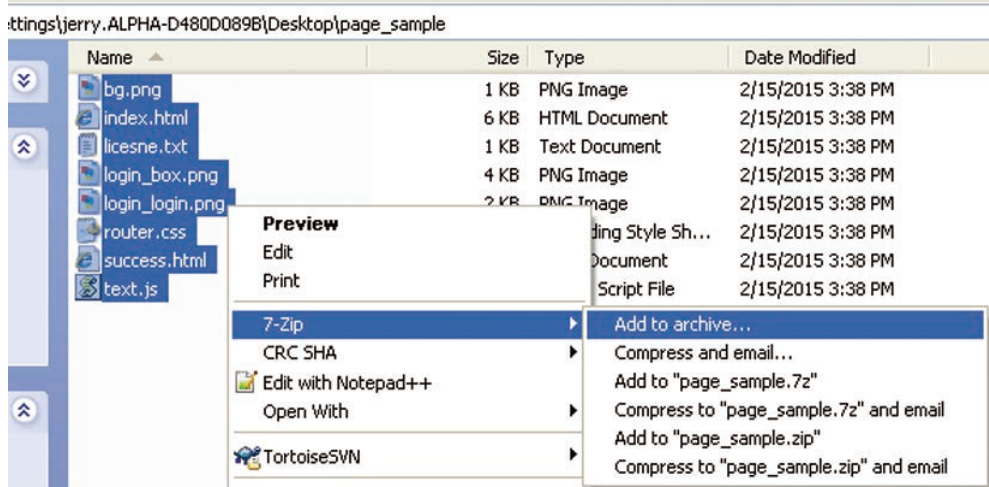


図 7-20 7zip

2. ダイアログでドロップダウンメニューからアーカイブフォーマットとして「tar」を選択して「OK」をクリックします。（圧縮ファイルは 448KB 以下である必要があります。所定サイズを超えるファイルはアップロードの失敗の原因となる可能性があります。）

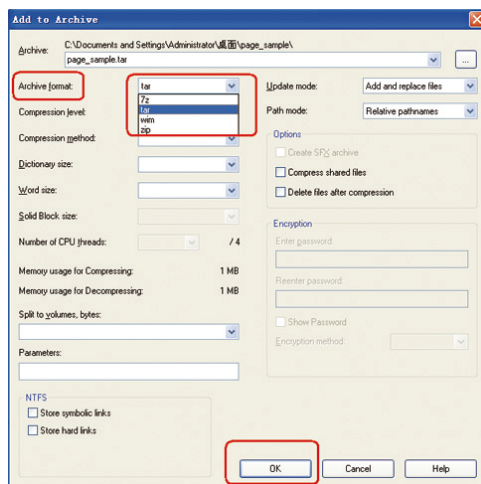


図 7-21 archive

3. CWM Web 管理 UI で、**Configuratio** > **SSID** の順に選択します。「Splash page customization」下の「Upload login file」をクリックします。新しいスタイルプロファイルの追加を許可するダイアログが表示されます。任意の名前を入力し「Browse」をクリックするとソースファイルのアップロードを許可する別のダイアログが開きます。

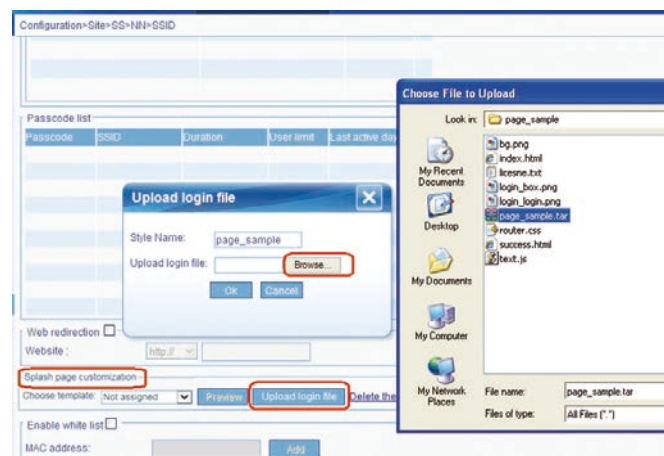


図 7-22 Upload login file

【付録B】 キャプティブポータルログインページのカスタマイズ

4. ソースファイルのアップロードに成功すると、ドロップダウンメニュー上で新しいスタイルが選択可能となり、キャプティブポータルログインページのカスタマイズ設定を完了します。

Splash page customization

Choose style: page_sample ▼ Preview Upload login file Delete the style DownLoad Template

Enable white list ☐ Style1 Style2 Style3 page_sample Add

MAC address:

Upload white list file: Browse... Upload

図 7-23 new style



CWM では一部の特殊文字 ("&" "\") はサポート対象外となります。