AirWorks AWK-3131A ユーザーマニュアル

第7.1版,2019年6月

www.moxa.com/product



© 2019 Moxa Inc. All rights reserved.

AirWorks AWK-3131A ユーザーマニュアル

本書に記載されているソフトウェアはライセンス契約のもとに提供されており、同契約条件に従ってのみ使用できます。

著作権に関する注意事項

© 2019 Moxa Inc. All rights reserved.

商標

MOXA ロゴは、Moxa Inc.の登録商標です。 本書に記載されるその他すべての商標および登録商標は、それぞれのメーカーに帰属します。

免責事項

本書の情報は予告なしに変更されることがあり、Moxaの確約を表明するものではありません。

Moxa は本書を、明示または暗黙を問わず、その特定の目的を含む(ただし必ずしもそれに限定されない)あらゆる種類の保証なく「現状のまま」 提供します。Moxa は、本書、または本書に記載されている製品および / またはプログラムを随時改善および / または変更する権利を留保しま す。

本書に記載されている情報は、正確かつ信頼できるものであることが意図されていますが、Moxa はその使用、またはその使用から生じる可能性がある第三者の権利に対するいかなる侵害に対しても一切責任を負いません。

本書には意図しない技術的または印刷上の誤りが含まれる場合があります。かかる誤りを訂正するために、本書の情報には定期的に変更が行われ、これらの変更は改訂版に組み込まれます。

製品新	ቆታ	•••••
概要	<u>i</u>	
梱包	1品確認リスト	
製品	の特長	
機能	:設計	
	ーー・ / / / / / / / / / / / / / / / / / /	
	モリンク	
	フレフト ケノー (ニングロールキ)	
	うしー (テンダル田力)	•••••
はじめ	אורוווי איז איז איז איז איז איז איז איז איז אי	
最紅	1のインストールと設定	
ふん		
世记		•••••
懱肫	シブイト イツノ	•••••
Web ⊐	レンノール設定	
Web	ブラウザによる設定	
Ove	niew(概要)	
Gen	view(版文) aval Satun(其太設宁)	
Gen	fai Setup(金本成だ)	
	System Information(システム情報).	•••••
	Interface On/Off(インターフェイスオン/オフ)	• • • • • • • • • • • •
	Network Settings(ネットワーク設定)	
	System Time(システム時間)	1
Wire	/less LAN Setup (無線 LAN 設定)	1
	Operation Mode (動作于一下)	
	Porio WI AN Setup (其本 WI AN 設定)	1
	Dasic WLAN Setup (空本 WLAN 設定)	⊥۱
	WLAN Security Settings(WLAN セイユリティ設定)	1 ~
	Advanced WLAN Settings(詳細 WLAN 設定)	Z
	WLAN Certificate Settings (WLAN 証明書設定) (EAP-TLS の Client (クライアント)/Client-router (クライアント-ルータ))/ Sla
	(スレーブ)モードのみ)	2
Adva	anced Setup(詳細設定)	2
	Jsing Virtual AN (仮想 AN の使用)	
		3
	DHCP Server (DHCP $\neg - \Lambda$) (AP/ $\partial \neg 1$ $r \rightarrow - \nu - \gamma - \nu - \nu$	3
	Packet Filters(ハケットノイルタ)	د
	RSTP Settings(RSTP 設定)(マスタまたはスレーブモードのみ)	3
	Static Route(静的ルート)(クライアント-ルータモードのみ)	3
	NAT Settings/Port Forwarding(NAT 設定/ポートフォワーディ ング)(クライアントールータモードのみ)	3
	SNMP Agent(SNMP エージェント)	4
	Link Fault Pass-through (リンクフォルトパススルー)(クライ アント/スレーブモードのみ)	4
امم	and Notifications (ログと通知)	2
LUga	· and Notifications (ー) こ (ロイ)	۲ /
	System Logs(SA) ALI)	
	Syslog	
	E-mail Notifications (Eメール通知)	4
	リレー	4
	Trap(トラップ)	4
Stat	us(ステータス)	
	Wireless I AN Status (無線 I AN ステータス)	4
	$A_{\text{rescaled}} = 0 (instable integration of the integration of t$	
	Associated Client List(関連的)られにジフィアンドリスト) (AP/マスタモートのみ)	
	DHCP Client List (DHCP $\overline{\mathcal{O}}$ \overline	5
	System Logs(システムログ)	5
	Relay Status(リレーステータス)	5
	DI and Power Status(DI および電源ステータス)	5
	AeroLink Protection Status(AeroLink Protection のステータス)(クライアント/スレーブモードのみ)	5
	System Status $(227/27-42)$	5
	System Status (2π) , 2π , (2π)	
1.		
7.		····· .
	Console Settings(コンソール設定)	5
	Ping(ビンク)	5
	Firmware Upgrade(ファームウェアの更新)	5
	Configuration Import and Export(設定のインポート/エクスポート)	5
	Load Factory Default(初期値のロード)	5
	Account Settings (アカウント設定)	
	Noooung Counge () カラント 政定/	с
	ハヘノートの変更	5
		_
	Misc. Settings(詳細設定)	5
	Misc. Settings(詳細設定) Troubleshooting(トラブルシューティング)	5 5
Save	Misc. Settings(詳細設定) Troubleshooting(トラブルシューティング) © Configuration(設定の保存)	5 5 6
Save	Misc. Settings(詳細設定) Troubleshooting(トラブルシューティング) e Configuration(設定の保存) art(再記動)	5 5 6

目 次

4.	ソフトウェアのインストールと設定	1
	概要	2
	Wireless Search Utility	2
	Wireless Search Utility のインストール	2
	Wireless Search Utility の設定	5
5.	その他のコンソールアクセス	1
	RS-232 コンソール設定 (115200, なし, 8, 1, VT100)	2
	Telnet コンソールと SSH コンソールによる設定	3
	HTTPS/SSL 対応 Web ブラウザによる設定	4
	Telnet およびブラウザによるアクセスの無効化	5
Α.	参照	1
	AeroLink Protection	2
	ビーコン	3
	DTIM	3
	フラグメント	
	RTS しきい値	3
		4
		4
	RSTP と STP の違い	4
в.	補足情報	1
	ファームウェアの復元	2
	適合宣言	3
	干渉に関する FCC (米連邦通信委員会)の注意事項	3
	RED(Radio equipment directive)適合宣言	4

AWK-3131A 産業用 a/b/g/n 高速無線アクセスポイント製品は、モバイル装置を使って TCP/IP ネットワークに接続する有線接続が 難しいアプリケーションにとって、理想的な無線ソリューションです。AWK-3131A は−25~60℃の気温で動作し、どれほど過酷な産業 環境でも十分な耐久性を発揮します。

この章の内容は以下のとおりです:

- □ 概要
- □ 梱包品確認リストエラー!参照元が見つかりません。
- □ 製品の特長
- □ 機能設計

>LED インジケータ
 >電子ブザー
 >リセットボタン
 >リレー(デジタル出力)

概要

AWK-3131Aは802.11nに準拠し、優れた速度、範囲、信頼性によって帯域幅の消費が最も多い用途にも対応します。802.11n規格は、 空間多重 MIMO(Multi-In、Multi-Out)、20 および 40 MHz チャンネル、デュアルバンド(2.4 GHz および 5 GHz)などの複数のテクノロ ジーを採用して高速な無線通信を実現しながら、引き続きレガシー802.11a/b/g デバイスともこれまで通り通信できます。

AWK-3131A は、標準モデルで-25~60℃の気温で動作し、どれほど過酷な産業環境でも十分な耐久性を発揮します。AWK は、DIN レールマウントまたは分電箱を使用して簡単に設置でき、広範な動作温度範囲、LED インジケータ付きの IP30 準拠のケース、および DIN レールマウントを備えているため、あらゆる種類の産業用無線用途に便利で信頼できるソリューションです。

梱包品確認リスト

MoxaのAWK-3131Aには次のアイテムが同梱されています。

- AWK-3131A 無線 AP/クライアント1 台
- 2.4/5 GHz アンテナ2本:ANT-EDB-ARM-0202
- DIN レールキット
- プラスチック製 RJ45 保護キャップ2個
- ケーブルホルダ(ネジ1本付き)
- クイックインストールガイド(印刷物)
- 保証書

メモ 標準モデルのAWK-3131Aには上記のアイテムが同梱されていますが、カスタムバージョンでは梱包品の内容が異なることがあります。

製品の特長

- IEEE 802.11a/b/g/n 対応
- 高度な無線セキュリティ
 - ▶ 64 ビットおよび 128 ビット WEP/WPA/WPA2
 - ▶ SSID 隠蔽/IEEE 802.1X/RADIUS
 - ▶ パケットアクセス制御およびフィルタリング機能
- STP/RSTP によるシステムネットワークの冗長化への対応
- 長距離通信への対応(5 GHz チャンネルのみ)
- 迅速なハンドオーバを可能にするTurbo Roaming(クライアントモード)
- ABC-01 による設定のインポート/エクスポート
- RS-232 コンソール管理
- 2DI+1DO でオンサイトの監視および警告に対応
- -40~75℃の広範な動作温度範囲(-T モデル)
- 冗長な 12~48 VDC 電源入力または IEEE 802.3af パワーオーバーイーサネット
- DIN レール
- 耐久性に優れた IP30 準拠の金属ケースを採用

メモ Moxa の製品の最新の仕様は https://www.moxa.com にあります。



・ AWK-3131A は携帯型モバイルデバイスではありません。人体から 20cm 以上離して使用してください。

AWK-3131A は一般的使用を目的として設計されてはいません。安全のため、AWK-3131A の取り付けと無線ネットワーク構築は、資格のある専門業者に依頼してください。

特許 <u>http://www.moxa.com/doc/operations/Moxa_Patent_Marking.pdf</u>

機能設計

LED インジケータ

AWK-3131A のフロントパネル上の LED を見れば、無線の現在のステータスや設定をすばやく簡単に確認できます。

「FAULT」(フォルト)LED はシステムエラーとユーザー設定イベントを示します。AWK-3131A が DHCP サーバから IP アドレスを取得で きないと、「FAULT」(フォルト)の LED が 0.5 秒間隔で点滅します。「SIGNAL」(信号)の LED は信号強度を示し、「Client」(クライアント) モードでのみ動作します。



以下の表は、LED 表示とそれに対応する無線設定の要約です。詳細は、第3章の「基本 WLAN 設定」に関するセクションに記載されています。

LED	色	状態	説明
		フロント パネル LED	のインジケーター(システム)
DWD1	4 3	点灯	電源入力1 から電力が供給されています。
PWRI	称來	消灯	電源入力1 から電力が供給されていません。
DWDO	4 7	点灯	電源入力2 から電力が供給されています。
PWRZ	称來	消灯	電源入力2 から電力が供給されていません。
	-L 1 - 3 ⁻ 3	点灯	電力はPoE で供給されています。
POE	オレンシ	消灯	電力はPoE で供給されていません。
		上灯	システムが起動中か、システム設定エラーまたはリレーイベントが発
		見と	生しました。
		点滅	
FAULT	±	(0.5 秒間隔の 短い点	DHCP サーバからIP アドレスを取得できません。
(フォルト)	小	滅)	
		点滅	
		(1 秒間隔の 長い点滅)	
		消灯	エラー状態はありません。
		点灯	システムの起動が完了し、システムは動作中です。
		点滅	
	緑	(0.5 秒間隔の 短い点	AeroLink Protection は有効で、現在「バックアップ」状態です。
STATE		滅)	
		点滅	 デバイスの場所が毎線ユーティリティで特定されました(間隔・1 秒)
		(1 秒間隔の 長い点滅)	
	赤	点灯	システムは起動中です。
SIGNAL		点灯	 Wi-Fi 信号レベル(クライアント/スレーブ/クライアント-ルータモード
(信号)	緑	消灯	のみ)
(5個の LED)			
		点灯	WLAN 機能がクライアント/スレーブ/クライアント-ルータモードになっ
			ており、AP とのリンクを催立しました。
	緑	点滅	WLAN データ通信はクライアント/スレーフ/クライアント-ルータモード
WLAN		消灯	WLAN かクライアント/スレーフ/クライアントールーダモートになってい
			ないか、AP とのリンクを催立していません。
		点灯	
	オレンジ	点滅	WLAN テータ通信がAP/マスタモートです。
		消灯	WLAN か使用されていないか、適切に動作していません。
	4 7	点灯	LAN ホートの1000 Mbps リンクか アクティフ です。
	禄	点滅	アータを1000 Mbps で送信しています。
LAN		消灯	LAN ホートの1000 Mbps リンクか非アクティフです。
		点灯	LAN ホートの10/100 Mbps リンクが アクティフ です。
	オレンジ	点滅	テータを10/100 Mbps で送信しています。
		消灯	LAN ボートの10/100 Mbps リンクが 非アクティブ です。



注意

「STATE」(状態)(緑)、「FAULT」(フォルト)、「WLAN」の各LED が同時に点灯して1 秒間隔で点滅する場合は、システムが起動に 失敗したことを意味します。これは、ファームウェア更新中の予期しないシャットダウンといった不適切な操作や制御不可能な問題 に起因します。ファームウェアの復元方法については、付録B の「ファームウェアの復元」を参照してください。

電子ブザー

システムが使用可能になると、短いビープ音が2回鳴ります。

リセットボタン

「RESET」(リセット)ボタンは AWK-3131A の上面パネルにあります。クリップをまっすぐに伸ばしたものなど、先の細いものを使って 「RESET」(リセット)ボタンを押すと、AWK-3131A を再起動したり、工場既定設定にリセットしたりすることができます。

- システム再起動:「RESET」(リセット)ボタンを押して5秒以内に放します。
- 工場既定値へのリセット:「STATE」(状態)の LED が緑に点滅し始めるまで「RESET」(リセット)ボタンを5 秒以上押します。ボタンを放すとAWK-3131A がリセットされます。



リレー(デジタル出力)

以下に示すように、AWK-3131Aの上部パネルには、2つの端子ブロック接点から構成されるリレー出力が1つあります。これらのリ レー接点は、システム障害とユーザー設定イベントを送信するのに使用されます。

ユーザー設定イベントがトリガされると、リレー接点に接続された2本の配線が開回路を形成します。ユーザー設定イベントが発生していない場合は、リレー回路は閉じたままです。安全上の理由から、AWK-3131Aの電源が入っていないときには、リレー回路は開いたままになっています。

AWK-3131A	$\sigma \eta \nu$ -	-ステ-	-970	り要約

電源ステータス	Event	Relay
オフ	-	開
オン	あり	開
	なし	ショート



この章では、Moxa の AirWorks AWK-3131A を初めてインストールする方法、無線ネットワークをすばやく設定する方法、接続に問題 がないかどうかをテストする方法について説明します。3 番目のセクションで説明する機能ガイドマップを使用すれば、必要な機能を 簡単に見つけられます。

この章の内容は以下のとおりです:

- □ 最初のインストールと設定
- ロ 通信テスト
- ロ 機能ガイドマップ

最初のインストールと設定

AWK-3131A をインストールする前に、梱包品確認リストに記されているアイテムがすべて箱に入っていることを確認してください。また、イーサネットポートを備えたノートパソコンまたは PC にアクセスする必要もあります。AWK-3131A は、デバイスと最初に接続する ときに必要なデフォルトの IP アドレスを備えています。

- ステップ1:電源を選択します。
 AWK-3131A には、DC 電源入力または PoE(パワーオーバーイーサネット)から電力を供給できます。AWK-3131A はユーザーが 選択したどの電源でも使用できます。
- ステップ 2: AWK-3131A をノートパソコンまたは PC に接続します。
 AWK-3131A は MDI/MDI-X オートセンシングに対応しているので、ストレートケーブルまたはクロスオーバーケーブルを使って AWK-3131A をコンピュータに接続できます。接続が確立されると、AWK-3131A の LAN ポートの LED インジケータが点灯します。
- ステップ3: コンピュータのIPアドレスを設定します。
 AWK-3131Aと同じサブネット内のIPアドレスを選択します。AWK-3131AのデフォルトのIPアドレスは192.168.127.253で、サブネットマスクは255.255.255.255.0なので、コンピュータのIPアドレスは192.168.127.xxxに設定します。
- メモ 「Maintenance」(メンテナンス)・「Load Factory Default」(工場既定のロード)を選択して、「Submit」(送信)ボタンをクリックすると、 AWK-3131Aは工場既定設定にリセットされ、IPアドレスも192.168.127.253にリセットされます。
 - ステップ4: Webベースのネットワークマネージャを使ってAWK-3131Aを設定します。
 お使いのコンピュータのWebブラウザを開いて、アドレスの欄にhttp://192.168.127.253と入力すると、Webベースのネットワークマネージャのホームページにアクセスできます。ホームページが開く前に、下図のようにユーザー名とパスワードを入力する必要があります。最初の設定時は、デフォルトのユーザー名とパスワードを入力してから、「Login」(ログイン)ボタンをクリックしてください:

_	ΜΟΧΛ°	
		MOXA AWK-3131A-US Username : admin Password : •••• Login
	goahead WEBSERVER	

メモ デフォルトのユーザー名とパスワードは以下のとおりです:		
	ユーザー名:	admin
	パスワード:	moxa (ファームウェアバージョン 1.4 以降)
		root (ファームウェアバージョン 1.3 まで)
	安全のため、デフォルトのパスワ	ードは必ず変更することをお勧めします。パスワードを変更するには、「Maintenance」(メンテナン
	ス)・「Password」(パスワード)を追	択し、画面の指示に従います。
	Overview (Warning: C This screen displays curr	nange the default password to ensure a higher level of security.) ent active settings
	System Information	
	Model name	AWK-3131A-US
	Device name	AWK-3131A_0000

メモ

「Submit」(送信)をクリックして変更を適用すると、Webページが更新されて、以下のようにページに「(Updated)」(更新済み)と表示 され、Webページの右上にメッセージが点滅表示されます:

		** Click Restart to activate new settings! **		
	WWW.IIIOXB.COM	W Total Solution for Industrial Wireless Networking		
Main Menu Overview	System Information (Updated)			
変更を有効にするには、設定変更後に「Restart」(再起動)をクリックして「Save and Restart」(保存して再起動)をクリックします。				

変更を有効にするには、設定変更後に「Restart」(冉起動)をクリックして「Save and Restart」(保存して冉起動)をクリックします AWK-3131Aの再起動プロセスが完了するまで約30秒かかります。

- ステップ5: AWK-3131Aの動作モードを選択します。
 デフォルトでは、AWK-3131Aの動作モードはAPに設定されています。「Wireless LAN Setup」(無線LAN設定)・「WLAN」・「Basic WLAN Setup」(基本WLAN設定)でクライアントモードに変更できます。AWK-3131Aの動作を設定する方法についての詳細は、第 3章に記載されています。
- ステップ6:通信をテストします。
 以下の各セクションでは、ネットワーク接続が確立されていることを確認する2種類のテスト方法について説明します。

通信テスト

AWK-3131A のインストール後、サンプルのテストを実行して、AWK-3131A と無線接続が正常に機能しているかどうか確認できます。 以降、2 種類のテスト方法について説明していきます。AWK-3131A を 1 台だけ使用している場合は最初の方法を、複数の AWK-3131A を使用している場合は 2 番目の方法を採用してください。

単一の AWK-3131A をテストする方法

AWK-3131A を 1 台だけ使用している場合は、WLAN カードを備えた 2 台目のノートパソコンが必要です。WLAN カードを設定して AWK-3131A(メモ: デフォルトの SSID は **MOXA**)に接続し、AWK-3131A に接続している 1 台目のノートパソコン(A)と同じサブネット になるように、2 台目のノートパソコン(B)の IP アドレスを変更します。

WLAN カードの設定後、AWK-3131A との無線接続を確立して、ノートパソコン B の DOS ウィンドウを開きます。 プロンプトに対して以下を入力します。

ping 〈ノートパソコン Aの IPアドレス〉

入力後、「Enter」を押します(下図参照)。「Reply from IP address ...」という応答があれば、通信に問題はありません。「Request timed out.」という応答は通信できないことを意味します。その場合は接続が正しいかどうか設定を再確認してください。



複数の AWK-3131A をテストする方法

AWK-3131Aを複数台使用している場合は、1 台目のノートパソコン(A)に加えて、イーサネットポートを備えた2 台目のノートパソコン (B)が必要です。ノートパソコン A に接続された1 台目の AWK-3131A のデフォルト設定を使って、ノートパソコン B に接続されている 2 台目または3 台目の AWK-3131A をクライアントモードに変更してから、各ノートパソコンと AWK-3131A を正しく設定します。



テスト環境の設定後、ノートパソコンBのDOSウィンドウを開きます。プロンプトに対して以下を入力します。 ping <ノートパソコン Aの IPアドレス>

入力後、「Enter」を押します。「Reply from IP address ...」という応答があれば、通信に問題はありません。「Request timed out」という 応答は通信できないことを意味します。その場合は接続が正しいかどうか設定を再確認してください。

機能ガイドマップ





管理機能はツリーに分類され、Web ベース管理コンソールの左側のフィールドに表示されます。このガイドで必要な機能を効率的に見つけることができます。

3

Web コンソール設定

この章では、Web ベースのコンソールの設定についてあらゆる面を説明します。Moxa の使いやすい管理機能は AWK-3131A の 設定だけでなく、無線ネットワークの確立とメンテナンスにも役立ちます。

この章の内容は以下のとおりです。

- Web ブラウザによる設定
- □ Overview(概要)
- □ Quick Setup(簡易設定)
- □ General Setup(基本設定)
 - ≫ System Information(システム情報)
 - » Interface On/Off(インターフェイスオン/オフ)
 - ≫ Network Settings(ネットワーク設定)
 - ≫ System Time(システム時間)
- □ Wireless LAN Setup(無線 LAN 設定)
 - \gg AeroMag
 - ≫ Operation Mode(動作モード)
 - ≫ Basic WLAN Setup(基本 WLAN 設定)
 - ≫ WLAN Security Settings(WLAN セキュリティ設定)
 - ≫ Advanced WLAN Settings(詳細 WLAN 設定)
 - ≫ WLAN Certificate Settings (WLAN 証明書設定)(EAP-TLS の Client(クライアント)/Client-router(クライアント-ルータ)

/Slave (スレーブ)モードのみ)

- □ Advanced Setup(詳細設定)
 - ≫ Using Virtual LAN(仮想 LAN の使用)
 - ≫ 仮想 LAN を設定する
 - ≫ DHCP Server(DHCP サーバ) (AP/クライアント-ルータモードのみ)
 - ≫ Packet Filters(パケットフィルタ)
 - ≫ RSTP Settings(RSTP 設定)(マスタまたはスレーブモードのみ)
 - ≫ Static Route(静的ルート)(クライアント-ルータモードのみ)
 - ≫ NAT Settings/Port Forwarding(NAT 設定/ポートフォワーディ ング)(クライアント-ルータモードのみ)
 - » SNMP Agent(SNMP エージェント)
 - ≫ Link Fault Pass-through (リンクフォルトパススルー)(クライ アント/スレーブモードのみ)
- Logs and Notifications(ログと通知)
 - ≫ System Logs(システムログ)
 - \gg Syslog
 - ≫ E-mail Notifications(Eメール通知)
 - ≫ リレー
 - ≫ Trap(トラップ)
- □ Status(ステータス)
 - ≫ Wireless LAN Status(無線 LAN ステータス)
 - ≫ Associated Client List(関連付けられたクライアントリスト) (AP/マスタモードのみ)
 - ≫ DHCP Client List(DHCP クライアントリスト)(AP モードのみ)
 - ≫ System Logs(システムログ)
 - ≫ Relay Status(リレーステータス)
 - ≫ DI and Power Status(DI および電源ステータス)
 - ≫ AeroLink Protection Status (AeroLink Protection のステータス) (クライアント/スレーブモードのみ)

- ≫ System Status(システムステータス)
- ≫ Network Status(ネットワークステータス)
- メンテナンス
 - ≫ Console Settings(コンソール設定)
 - ≫ Ping(ピング)
 - ≫ Firmware Upgrade(ファームウェアの更新)
 - ≫ Configuration Import and Export(設定のインポート/エクスポート)
 - ≫ Load Factory Default(工場既定値)
 - ≫ Account Settings(アカウント設定)
 - ≫ パスワードの変更
 - ≫ Misc. Settings(その他の設定)
 - » Troubleshooting(トラブルシューティング)
 - ≫ Save Configuration(設定の保存)
 - ≫ Restart(再起動)
 - ≫ Logout(ログアウト)

Web ブラウザによる設定

Moxa AWK-3131A の Web ブラウザのインターフェイスは、AWK-3131A の設定を変更したり、内蔵の監視およびネットワーク管理 機能にアクセスしたりするのに便利です。推奨 Web ブラウザは、JVM(Java Virtual Machine)がイ ンストールされた Microsoft® Internet Explorer 7.0 以上です。

✓モ AWK-3131A と同じ LAN に接続されている PC ホストから AWK-3131A の管理機能や監視機能を使用するには、PC ホストと AWK-3131A が同じ論理サブネットに属している必要があります。同様に、AWK-3131A が他の VLAN 設定用に設定されている場 合、PC ホストが管理 VLAN に属していることを確認する必要があります。 Moxa AWK-3131A のデフォルトの IP は 192.168.127.253 です。

AWK-3131AのWeb ベースコンソール管理インターフェイスにアクセスするには、以下の手順に従います。.

1. Web ブラウザ(つまり Internet Explorer)を開き、アドレスの欄に AWK-3131A の IP アドレスを入力します。「Enter」を押して 接続を確立します.

🎒 ab	🗿 about:blank - Microsoft Internet Explorer 📃 🔍							
Eile	<u>E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help			1
\bigcirc	Back 🔻	$\mathbf{\Theta}$	- 💌 🕻	1) 🔎 Search	K Favorites	<i></i> 😥	. 🎍 »
A <u>d</u> dre	ess 🗌	http://	192.168.127	.253			💌 🔁 Go	b Links »
								<u>^</u>

2. Web コンソールのログインページが開きます。パスワード(デフォルトのユーザー名は admin、デフォルトの パスワードは moxa) を入力し、「Login」(ログイン)をクリックして続行します.

_	ΜΟΧΛ°	
		MOXA AWK-3131A-US Username : admin Password : ••••
	webserver	Login

 Web ページをコンピュータにダウンロードするのに少し時間がかかる場合があります。お使いの AWK-3131A の モデル名と IP アドレスが両方とも Web ページのタイトルバーに表示されていることに注意してください。この 情報は複数の AWK-3131A をそれぞれ識別するのに役立ちます。

もしも誤ったユーザー名やパスワードが入力されるとワーニングメッセージが表示されます。システムはユーザーアカウントを 「Maintenance → Account Settings」のページで設定された設定をベースにして見ています。デフォルトのリトライ回数は5回でデ フォルトのロックアウト時間は 600 秒です。

いったんアカウントがロックされると、ユーザーはロックアウト期間が終わるまで再試行を待つことになります。

Invalid username or password	Invalid username or password	Username ;admin Password : Login	
	Invalid username or password	This account is locked. Username :admin Password : Login	

4. ブラウザの左脇にあるメニューツリーを使って AWK-3131A 機能を開きます。



以下のセクションで、AWK-3131Aの各管理機能を詳細に説明します。簡単な概要は第3章の「機能マップ」のセクションに記載されています。

メモ AWK-3131A のモデル名は AWK-3131A-XX と表示されます。この XX は国コードです。国コードは AWK-3131A のバージョンと 使用する周波数を示しています。以下の図では、例として AWK-3131A-US を使用しています。(お使いのコンピュータの画面に表 示される国コードとモデル名は、これらの例とは異なる場合があります。

Overview(概要)

「Overview」(概要)のページには、AWK-3131A の現在のステータスが要約して表示されます。情報は、「System Information」(システム情報)、「Device Information」(デバイス情報)、「802.11 Information」(802.11 情報)の各グループに分類されています。

Home A Main Menu	Overview (Warning: Change the d	default password to ensure a higher level of secur	ity.)		
💼 Overview	This screen displays current active se	ettings			
🗉 🧰 General Setup	System Information				
🗉 🧰 Wireless LAN Setup	Model name	AWK-3131A-US			
🗉 🧰 Advanced Setup	Device name	AWK-3131A_7286			
🗉 🧰 Logs and Notifications	Serial number	7286			
E Status	System uptime	0 days 00h:01m:51s			
	Firmware version	1.6 Build 17091517			
	Device Information				
	Device MAC address	00:90:E8:62:BB:89			
Restart	IP address	192.168.127.253			
Logout	Subnet mask	255.255.255.0			
	Gateway				
	802.11 Information				
	Country code	US			
	Operation mode	AP			
	Channel	6			
	RF type	B/G/N Mixed			
	Channel width	N/A			
	SSID	MOXA			

「SSID」のリンク(MOXA)をクリックすると、以下の図のように 802.11 の詳細情報が表示されます。

Wireless LAN Status

🖉 Auto Update		
Show status of	WLAN (SSID: MOXA) V	

802.11 Information	
Operation mode	AP
Channel	6
Channel width	N/A
RF type	B/G/N Mixed
SSID	MOXA
MAC	06:90:E8:11:22:33
Security mode	OPEN
Current BSSID	N/A
Signal strength	N/A
Signal strength	-108 dBm
Noise floor	-108 dBm
SNR	N/A
Transmission Information	
Rate	Auto
Power	20 dBm
Outgoing Packets	
Total sent	0
Packets with errors	0
Packets dropped	9154
Incoming Packets	
Total received	0
Packets with errors	0
Packets dropped	0

メモ

「802.11 Information」(802.11 情報)に表示される内容は、動作モードによって異なります。例えば、「Current BSSID」(現在の BSSID)、「Signal strength」(信号強度)、「SNR」は、動作モードがクライアント/クライアントールータ/スレーブモードの場合にしか表示 されません

General Setup(基本設定)

「General Setup」(基本設定)のグループには、管理者が AWK-3131A のメンテナンスと管理に最もよく使用する 一般的な設定が含まれています。

System Information(システム情報)

「System Information」(システム情報)の項目、特に「Device name」(デバイス名)と「Device description 」(デバイスの説明)は、 「Overview」(概要)のページ、SNMP 情報、および警告メールに表示されたり、含まれたりします。「System Information」(システム情報)の項目を設定すれば、ネットワークに接続されている個々の AWK-3131A を識別するのが容易になります。

System Information		
Device name	AWK-3131A_0000	
Device location		
Device description		
Device contact information		
Login Message		
Login authentication failure message	Invalid username or password	

Submit

Device name(デバイス名)

設定	説明	工場既定値
最大 31 文字	このオプションは、個別の AWK-3131A の役割や用途をそれぞれ指 定す	モデル名_<デバイス
	るのに便利です。	MAC の最後の 3 バイト>

Device location (デバイスの場所)

設定	説明	工場既定値
最大 31 文字	個々の AWK-3131A の場所を指定します	なし

Device description(デバイスの説明)

設定	説明	工場既定値
最大 31 文字	この欄は AWK-3131A のより詳しい記述を記録するのに使います。	なし

Device contact information (デバイス連絡情報)

設定	説明	工場既定値
最大 31 文字	題発生時の連絡先の情報を提供します。このスペースにはこの	なし
	AWK-3131A のメンテナンス担当者の連絡情報を記録します。	

Login Message (ログインメッセージ)

設定	説明	工場既定値
最大 31 文字	ログインした時に全てのユーザーに表示するメッセージを入力します。	空白

Login authentication failure message (ログイン認証失敗メッセージ)

設定	説明	工場既定値
最大 31 文字	無効なユーザー名やパスワードでログインしたユーザーに表示する、ログイ	なし
	ン認証が失敗したメッセージを入力します。	

Interface On/Off(インターフェイスオン/オフ)

Interface On/Off

LAN	🖲 Enable 🔍 Disable	
Submit		

Network Settings(ネットワーク設定)

「Network Settings」(ネットワーク設定)の設定パネルでは、通常の TCP/IP ネットワークパラメータを変更でき ます。ただし、クライ アントールータ動作モードが追加されたため、このパネルではネットワークパラメータのセット が 2 種類提供されるようになりました。 その両方のタイプの設定について、以下で説明します。

AP/クライアント/マスタ/スレーブ動作モードでのネットワーク設定

Network Settings

IP address assignment IP address Subnet mask	Static ▼ DHCP +3.104 Static 255.255.252.0
Gateway	192.168.43.254
Primary DNS server	192.168.50.41
Secondary DNS server	192.168.50.42

Submit

IP address assignment(IP アドレスの割り当て

設定	説明	工場既定値
DHCP	AWK-3131AのIPアドレスはネットワークの DHCPサーバによって自動的に	Static(静的)
	割り当てられます	
Static(静的)	AWK-3131A の IP アドレスを手動で設定します	

IP address (IP アドレス)

設定	説明	工場既定値
AWK-3131A の IP アドレス	TCP/IP ネットワーク上の AWK-3131A を識別します。	192.168.127.253

Subnet mask(サブネットマスク)

設定	説明	工場既定値
AWK-3131A のサブネットマ	AWK-3131A が接続しているネットワークの種類を識別します。 (例: クラ	255.255.255.0
スク	ス B のネットワークでは 255.255.0.0、クラス C のネッ トワークでは	
	255.255.255.0)	

Gateway(ゲートウェイ)

設定	説明	工場既定値
AWK-3131A のデフォルトゲ	LAN を外部のネットワークに接続しているルータの IP アドレス	なし
ートウェイ		

Primary/ Secondary DNS server(プライマリ / セカンダリ DNS サーバ)

設定	説明	工場既定値
プライマリ/セカンダリ DNS	ネットワークで使用される DNS サーバの IP アドレス。DNS サーバの IP ア	なし
サーバの IP アドレス	ドレスを入力すると、ブラウザのアドレスの欄に IP アドレスではなく、	
	AWK-3131A の URL(例: http://ap11.abc.com)を入力できるようになりま	
	す。プライマリ DNS サーバが接続に失敗する と、セカンダリ DNS サーバが	
	使用されます。	

クライアントールータ動作モードでのネットワーク設定

Network Settings

WLAN (Default Route)	
IP address assignment	Static 🔻
IP address	192.168.128.253
Subnet mask	255.255.255.0
Gateway	
Primary DNS server	
Secondary DNS server	
LAN	
IP address	192.168.127.254
Subnet mask	255.255.255.0

Submit

WLAN IP address assignment (WLAN IP アドレスの割り当て)

設定	説明	工場既定値
DHCP	AWK-3131A WLAN インターフェイスの IP アドレスはネットワークの DHCP	Static(静的)
	サーバによって自動的に割り当てられます	
Static(静的)	AWK-3131A WLAN インターフェイスの IP アドレスを手動で設定 します。	

WLAN IP address (WLAN IP アドレス)

設定	説明	工場既定値
AWK-3131A WLAN イ ンタ	TCP/IP ネットワーク上での AWK-3131A の WLAN インターフェイスの IP アド	192.168.128.253
ーフェイスの IP アドレス	レスを識別します。	

WLAN subnet mask(WLAN サブネットマスク)

設定	説明	工場既定値
AWK-3131A WLAN インター	AWK-3131A の WLAN インターフェイスが接続されているネットワークの種	255.255.255.0
フェイスの IP アドレス	類を識別します(例: クラス B のネットワークでは 255.255.0.0、クラス C のネ	
	ットワークでは 255.255.255.0)	

WLAN gateway(WLAN ゲートウェイ)

設定	説明	工場既定値
AWK-3131A WLAN インタ	WLAN を外部のネットワークに接続しているルータの IP アドレスです。	なし
ーフェイスのデフォルトゲー		
トウェイ		

Primary/Secondary DNS server

設定	説明	工場既定値
プライマリ/セカンダリ DNS	ネットワークで使用される DNS サーバの IP アドレス。DNS サーバの IP アド	なし
サーバの IP アドレス	レスを入力すると、ブラウザのアドレスの欄に IP アドレスではなく、	
	AWK-3131A の URL(例:http://ap11.abc.com)を入力できるようになりま	
	す。プライマリ DNS サーバが接続に失敗すると、セカンダリ DNS サーバが	
	使用されます。	

LAN IP address (LAN IP アドレス)

設定	説明	工場既定値
AWK-3131A LAN インターフ	TCP/IP ネットワーク上での AWK-3131A の LAN インターフェイ スの IP アド	192.168.127.254
ェイスの IP アドレス	レスを識別します.	

LAN subnet mask(LAN サブネットマスク)

設定	説明	工場既定値
AWK-3131A LAN イン ター	AWK-3131AのLAN インターフェイスが接続されているネットワー クの種類	255.255.255.0
フェイスのサブネッ トマスク	を識別します(例: クラス B のネットワークでは 255.255.0.0、 クラス C のネッ	
	トワークでは 255.255.255.0)	

System Time(システム時間)

AWK-3131A は NTP サーバからの情報やユーザー指定の日付/時刻情報に基づく時間補正機能を備えています。「Logs and Notifications」(ログや 通知)などの機能では、メッセージにリアルタイム情報を追加できます。

	Date (YYYY/MM/DD) Time (HH:MM:SS)		
Current local time	Set Time		
Time protocol	SNTP		
Time zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 🔻		
Daylight saving time	Enable		
Time server 1	time.nist.gov		
Time server 2			
	600 (600~9999 seconds)		

「Current local time 」(現在のローカル時間)には、この Web ページを開いたときの AWK-3131A のシステム時 刻が表示されま す。「Set Time」(時間設定)ボタンをクリックすると、更新した日付と時刻のパラメータを有効に できます。変更が完了すると、 「(Updated)」(更新済み)という文字列が表示されます。「Save and Restart」(保存して再起動)を実行しなくても、ローカルシステム 時刻が即座に有効になります。 ★モ AWK-3131A はリアルタイムクロック(RTC)を内蔵しています。初期設定後や長期シャットダウン後、特にネットワークに NTP サーバにアクセスするイーサネット接続がない場合や LAN 上に NTP サーバがない場合には、AWK3131A の「Current local time」(現在のローカル時間)を更新することを強くお勧めします

Current local time(現在のローカル時間)

設定	説明	工場既定値
ユーザーが指定可能な時	日付と時刻のパラメータを使えばローカル時間を設定でき、設定した ロー	なし
間	カル時間は即座に有効になります。	
	24 時間形式を使用します : yyyy/mm/dd hh: mm: ss	

Time zone (タイムゾーン)

設定	説明	工場既定値
ユーザー選択可能な時間	時間帯を設定すると、GMT(グリニッジ標準時)からローカル時間に変換で	GMT(グリニッジ標準時)
帯	きるようになります。	



注意

時間帯を変更すると、「Current local time」(現在のローカル時間)が自動的に調整されます。「Current local time」(現在のローカル 時間)を設定する前に、「Time zone」(時間帯)を設定してください。

Daylight saving time(夏時間)

設定 説明

「Daylight saving time」(夏時間)を使用すると、以下のパラメータが表示されます。

- 「Starts at」(開始日): 夏時間が始まる日付。
- 「Stops at」(終了日): 夏時間が終わる日付。
- 「Time offset」(タイムオフセット):時計を何時間進めるかを指定します。

Time server 1/2(タイムサーバ 1/2)

設定	説明	工場既定値
1/2 台目のタイムサー バ	NTP タイムサーバの IP またはドメインアドレス。1 台目の NTP サーバ	time.nist.gov
の IP/名前	が切断されると、2 台目の NTP サーバが使用されます。	

Time sync interval(時間同期間隔)

設定	説明	工場既定値
NTP サーバの同期間隔	このパラメータは NTP サーバが時刻を同期する間隔を指定します。	600 (秒)
(600~9999 秒)		

Wireless LAN Setup(無線 LAN 設定)

AWK-3131A には無線動作モードのセットが 2 組あります。ポイントツーマルチポイント通信用の AP/クライアン トモードと透過的 なポイントツーポイント通信用のマスタ/スレーブモードです。この 2 種類の動作モードの主な違いは、クライアント/スレーブ無線機 での MAC アドレスの変換です。

AP/クライアント: 802.11 規格の限界を克服するために、IP ブリッジング機構が使用されます。この場合、クライアント無線機に接続 されたデバイスの MAC アドレスは、クライアントの MAC アドレスで置き換えられます。AP/クライアントモードでは、MAC 認証シス テムまたは MAC(レイヤ 2)ベースの通信が使用されている場合に通信の問題が発生する可能性があります。その場合は、ネット ワークの動作モードをマスタ/スレーブモードに変更する必要があります。

マスタ/スレーブ: パケットがスレーブ無線を通過したときにデバイスの MAC アドレスを変更せずに維持できるトラン スペアレントなポイントツーポイントプロトコルです。有線システムに代わる、安心して使用できる無線ソリュ ーションをお探しの場合は、マスタ/スレ ーブを使用してください。.

クライアントールータ: 標準的なクライアントモードの 1 つのバリエーションです。WLAN の動作はクライアントモードと同じですが、 WLAN サブネットと LAN サブネットを分離するためにルータの動作が追加されました。これにより、ネットワークプランナは、クライア

工場既定値

ント無線機の背後でプライベート IP アドレスを割り当てることができます。「Static Route」(静的ルート)、「NAT」、「Port Forwarding」 (ポートフォワーディング)の各機能の詳 細は、「Advanced Setup」(高度な設定)に関するセクションに記載されています。

スニファー: 無線トラフィックを簡単に分析できる手段をお客様に提供するために、AWK-3131A では Wireshark パ ケットスニファー ソフトウェアと動作する「Sniffer」(スニファー)モードをサポートしています。

Operation Mode(動作モード)

AWK-3131A は、AP、クライアント、クライアント-ルータ、マスタ、スレーブ、スニファーという 6 種類の動作モー ドに対応しています。 各モードは無線ネットワークにおいてそれぞれ異なる役割を果たします。

Wireless enable	🖲 Enable 🔘 Disable	O Disable	
Operation mode	AP 🔻		
	AP		
Submit	Client Client-Router Master Slave Sniffer		

Wireless enable (無線の使用)

設定	説明	工場既定値
Enable(使用する)/Disable	RF (無線周波数)モジュールは手動でオンとオフを切り替えられます	Enable(使用する)
(使用しない)		

Operation mode (動作モード)

設定	説明	工場既定値
AP	AWK-3131A は無線アクセスポイントの役割を果たします	AP
Client(クライアント)	AWK-3131A は無線クライアントの役割を果たします	
Client-Router	AWK-3131A は、無線クライアントの役割を果たしますが、WLAN インター	
(クライアントルータ)	フェイスと LAN インターフェイスを 2 つのサブネットに分けるルータ機能を含	
	んでいます。	
Master(マスタ)	AWK-3131A は無線マスタの役割を果たします	
Slave(スレーブ)	AWK-3131A は無線スレーブの役割を果たします	
Sniffer(スニファー)	デバイスをリモート Wireshark インターフェイスに切り替え、802.11 パケット	
	をキャプチャして分析します。.	

スニファーモードの手順:

- 1. AWK-3131A で動作モードをスニファーモードに設定してから、デバイスを保存して再起動します。
- 2. Wireshark(v1.12.0 以上)がインストールされているラップトップに、AWK-3131A をイーサネットを介して接続します。
- 3. AWK-3131A の IP アドレスを入力してリモートインターフェイスを追加します。

メモ 動的ブリッジングを使用する方が便利ですが、クライアントでは、無線インターフェイス(WLAN)とイーサネットイ ンターフェイス(LAN) との間で通信できるパケットが IP ベースのものだけになり、その他の種類のトラフィック(IPX や AppleTalk など)は送信できないという制限があります。

Interface Management	📕 Wireshark: Remote I 💶 🔳 💌	
Pipes Local Interfaces Remote Interfaces Remote Interfaces Host	Host: 192.168.127.253	•
<u>A</u> dd <u>D</u> elete	Apply	Close

Wireshark の詳しい使用方法については次の Web ページをご覧ください。

https://www.wireshark.org/docs/wsug_html_chunked/ChCapInterfaceRemoteSection.html

4. Wireshark を使って 802.11 無線パケットのキャプチャを開始します。

Basic WLAN Setup(基本 WLAN 設定)

「Basic WLAN Setup」(基本 WLAN 設定)パネルでは、SSID の追加と編集ができます。SSID は無線ネットワークデバイスが無線接 続の構築や維持に使用する一意のIDです。1 つのネットワークまたはサブネットワーク上の複数のアクセスポイントに同じSSIDを使 用できます。AWK では最大 9 つの SSID を使用でき、各 SSID を個別に設定できます。すべての SSID を同時に使用可能です。つま り、クライアントデバイスは任意の SSID を使ってアクセスポイントと接続できるのです。

Basic WLAN Setup (Multiple SSID)

Status	SSID	Operation Mode	Action
Active	MOXA	АР	Edit

Add SSID

「Add SSID」(SSID の追加)をクリックすると、SSID を追加できます。.

Basic WLAN Setup (Multiple SSID)

Status	SSID	Operation Mode	Action
Active	MOXA	АР	Edit
Inactive		АР	Save Cancel
Add SSID			

「Edit」(編集)をクリックすると、各 SSID にそれぞれ異なる設定を割り当てることができます。設定パネルの表示は以下のとおりで す。

0

Basic WLAN Setup

Operation mode	AP
RF type	B/G/N Mixed 🔻
Channel	6 🔻
Channel width	20 MHz 🔻
SSID	MOXA
SSID broadcast	Enable Disable
AeroLink AP	Enable Isable
Management frame encryption	Enable Disable
Management frame encryption password	•••••

Submit

メモ 「Client](クライアント)、「Client-Router」(クライアントールータ)、または「Slave」(スレーブ)モードに切り替えると、「Basic WLAN Setup」(基本 WLAN 設定)パネルの「Site Survey」(サイト調査)ボタンが使用可能になります。「Site Survey」(サイト調査)ボタンを クリックすると、下図のように、使用可能な AP に関する情報が表示されます。エンティティの SSID をクリックすると、「Basic WLAN Setup」(基本 WLAN 設定)ページの「SSID」欄にその SSID の値を移入できます。「Refresh」(更新)ボタンをクリックすると、再検 索して表を更新できます。

Basic WLAN Setup

Operation mode	Client-Router	
кг цре	D/G/N Plixed	
Channel width	20 MHz 🔻	
SSID	MOXA	Site Survey
Proxy ARP	🖲 Enable 🔍 Disable	

Submit

Site Survey

No.	SSID	MAC Address	Channel	Mode	Signal/Noise Floor
1	MHQ-NB	FC:F5:28:CB:5D:AB	1	BSS/WPA2/Enterprise	••000 (-96dBm/-111dBm)
2	MHQ-Mobile	FE:F0:28:CB:5D:AB	1	BSS/WPA2/Enterprise	∎000 (-96dBm/-111dBm)
3	MHQ-NB	FC:F5:28:CB:5D:93	1	BSS/WPA2/Enterprise	∎000 (-96dBm/-111dBm)
5	MHQ-Mobile	FE:F0:28:CB:5D:93	1	BSS/WPA2/Enterprise	∎0000 (-97dBm/-111dBm)
6	51_FRED	06:90:E8:00:07:96	1	BSS/WPA2/PSK	∎0000 (-108dBm/-111dBm)
7	MHQ-NB	FC:F5:28:CB:39:02	1	BSS/WPA2/Enterprise	∎0000 (-108dBm/-111dBm)
9	MHQ-Mobile	FE:F0:28:CB:39:02	1	BSS/WPA2/Enterprise	∎0000 (-103dBm/-111dBm)
10	MHQ-NB	FC:F5:28:CB:5D:99	6	BSS/WPA2/Enterprise	∎0000 (-104dBm/-111dBm)
11	MHQ-Mobile	FE:F0:28:CB:5D:99	6	BSS/WPA2/Enterprise	∎0000 (-105dBm/-111dBm)
13	MHQ-NB	FC:F5:28:CB:5D:90	6	BSS/WPA2/Enterprise	••000 (-91dBm/-111dBm)
14	MHQ-Mobile	FE:F0:28:CB:5D:90	6	BSS/WPA2/Enterprise	∎000 (-90dBm/-111dBm)
15	MHQ-NB	FC:F5:28:CB:5D:3F	6	BSS/WPA2/Enterprise	••000 (-83dBm/-111dBm)
17	MHQ-Mobile	FE:F0:28:CB:5D:3F	6	BSS/WPA2/Enterprise	••000 (-85dBm/-111dBm)
18	MHQ-NB	FC:F5:28:CB:5D:8D	6	BSS/WPA2/Enterprise	∎0000 (-104dBm/-111dBm)

RF type(RF タイプ)

設定	説明	工場既定値
2.4 GHz		
В	IEEE 802.11b 規格にのみ対応	B/G/N Mixed
G	IEEE 802.11g 規格にのみ対応	(B/G/N 混在)
B/G Mixed(B/G 混在)	IEEE 802.11b/g 規格に対応。ただし、802.11b クライアントがネットワーク上	1
	にある場合は 802.11g が減速する可能性があります	
G/N Mixed(G/N 混在)	IEEE 802.11g/n 規格に対応。ただし、802.11g クライアントがネットワーク上	1
	にある場合は 802.11n が減速する可能性があります	
B/G/N Mixed(B/G/N 混在)	IEEE 802.11b/g/n 規格に対応。ただし、802.11b クライアントがネットワーク	
	上にある場合は 802.11g/n が減速する可能性があります	
N Only(N のみ)	2.4 GHz IEEE 802.11n 規格にのみ対応	
(2.4 GHz)		
5 GHz		
A	IEEE 802.11a 規格にのみ対応	
A/N Mixed(A/N 混在)	IEEE 802.11a/n 規格に対応。ただし、802.11a クライアントがネットワーク上	
	にある場合は 802.11n が減速する可能性があります	
N Only(N のみ)	5GHz IEEE 802.11n 規格にのみ対応	
(5 GHz)		

Channel (チャンネル)(AP モードのみ)

設定	説明	工場既定値
使用可能なチャンネルは	このオプションは、AWK-3131A が無線 AP の役割を果たしている場 合に	6(B/G/N 混在モードの
RF タイプによって異なりま	のみ調整可能です。無線クライアントとして動作している AWK3131A は、	場合)
す	関連付けられているアクセスポイントのチャンネルを使用します	

Channel width (チャンネル幅)(11N RF タイプのみ)

設定	説明	工場既定値
20 MHz	チャンネル幅を選択します。どのオプションを使用するべきか判断で きない	20 MHz
20/40 MHz	場合は、「20/40 MHz」(自動)を選択してください	

Channel bonding(チャンネルボンディング)

「Channel bonding」(チャンネルボンディング)はチャンネル幅が 20/40MHzに設定されている時に AP によって使われているチャンネルを示します。

SSID

設定	説明	工場既定値
最大 31 文字	クライアントと AP が相互に通信するには、クライアントの SSID と AP の	MOXA
	SSID が同じでなければなりません。	
	注:SSID には次の文字は使えません `'´' ;&	

SSID broadcast (for AP mode only)

設定	説明	工場既定値
Enable(使用する)/Disable	SSID がブロードキャスト可能かどうかを指定します.	Enable(使用する)
(使用しない)		



重要!

SSID ブロードキャスト機能が使わない設定の時、APとクライアントはDFS チャンネルの接続を確立することができません。クライアントはDFS チャンネルの受動スキャンしか許されていないからです。これらのチャンネルへのアクティブスキャンは禁止されています。

AeroLink AP

設定	説明	工場既定値
Enable(使用する)/Disable	クライアント側の Aerolink 保護に数ミリ秒の復帰時間で起動をかけるため、	Disable(使用しない)
(使用しない)	Aerolink AP が AP 側のイーサネット通信をモニタできるようにします。	
	注: AeroLink 保護は同時にクライアント側で許可する必要があります	

Management Frame Encryption(マネジメントフレーム暗号化)

設定	説明	工場既定値
Enable(使用する)/Disable	この機能を使用するとセキュリティが向上します。マネジメントフレーム暗号	Disable(使用しない)
(使用しない)	化は、互いに接続する2つのデバイス間でユーザーが指定のパスワードを	
	設定することができます。	

メモ AeroMag は Management Frame Encryption をサポートしていません

WLAN Security Settings(WLAN セキュリティ設定)

AWK-3131A は、**Open**(オープン)、**WEP**(Wired Equivalent Privacy)、**WPA**(Wi-Fi Protected Access)、 **WPA2** の 4 種類の標準的 な無線セキュリティモードに対応しています。AWK-3131A では、 セキュリティモード と WPA タイプ を選択することで、数種類のセ キュリティモードを使用できます。

- Open(オープン): 認証なし、データ暗号化なし。
- WEP:静的 WEP(Wired Equivalent Privacy)キーを手動で設定する必要があります。
- WPA/WPA2-Personal: WPA/WPA2-PSK としても知られています。「Passphrase 」(パスフレーズ)の欄には、実際の送信 パケット暗号化と受信パケット復号化に使用するキーを生成するためのマスタキーとして TKIP または AES エンジンが使用する PSK(Pre-Shared Key)を指定する必要があります。
- WPA/WPA2-Enterprise: WPA/WPA2-EAP(Extensible Authentication Protocol)とも呼ばれます。WPA/WPA2-Enterprise では デバイスベースの認証だけでなく、IEEE 802.1X によるユーザーベースの認証 も使用できます。AWK-3131A は EAP-TLS、 EAP-TTLS、EAP-PEAP の 3 種類の EAP 方式に対応しています。
- WPA-WPA2 mixed: AWK は同時に WPA/WPA2 をサポートしています。AWK は WPA と WPA2 を使う両方の Wi-Fi クライアントを 認証することが出来ます。

WLAN Security Settings

SSID	MOXA
Security mode	Open 🔻
	Open
Submit	WEP
	WPA
	WPA2
	WPA-WPA2 mixed

設定	説明	工場既定値
Open(オープン)	認証なし。	Open(オープン)
WEP	静的 WEP が使われます。	
WPA	WPA が使われます。	
WPA2	IEEE 802.11i を"TKIP/AES + 802.1X"でサポートします。	
WPA-WPA2 mix	AWKに接続するWPA と WPA2の両方のクライアントを同時に認証します。	

Security mode (セキュリティモード)

Open(オープン)

セキュリティ上の理由から、セキュリティモードを Open(オープン)システムにセットしてはいけません。なぜなら認証とデータ暗号化が オープンシステムモードでは行われないからです。

WEP (レガシーモードのみ)

メモ

Moxa はレガシー目的でのみ WEP セキュリティモードを含んでいます。WEP はとても安全ではなく Wi-Fi アライアンスとしては全く非 推奨と考えられます。どのような事情があっても WEP の利用は推奨できません。

IEEE 802.11 規格によれば、WEP は認証 およびデータの暗号化を使用して機密性を 保持できます。「Shared」(または「Shared Key」)認証はWEP 認証とデータの暗号化 の両方が必要とされる場合に使用されま す。通常、「Open」(または「Open System」) 認証はWEP によるデータの暗号化が認証 と共に実行される場合に使用されます。

WLAN Security Settings

SSID	MOXA
Security mode	WEP V
Authentication type	Open 🔻
Key type	HEX 🔻
Key length	64 bits 🔻
Key index	1 🔻
WEP key 1	
WEP key 2	
WEP key 3	
WEP key 4	
Submit	

セキュリティモードとしてWEPを使用する場合は、キー(いわゆるWEPシード)の長さを 64/128 ビットに指定できます。これは実際に は24ビットの初期化ベクトルを伴う40/104ビットのシークレットキーです。AWK-3131A では、**キーインデックス**と共に使用するために 選択できる4組のWEPキー設定に対応しています。選択したキー設定はAP側から無線クライアント側へのトラフィックを暗号化する 送信キーとして使用するキーを指定します。4つのWEPキーはすべて、無線クライアント側から AP 側へのトラフィックを復号化す る 受信キーとして使用されます。

WEP キーは、HEX と ASCII の 2 つの**キータイプ**を使用できます。各 ASCII 文字は 8 ビットなので、40 ビット(ま たは 64 ビット)の WEP キーは 5 文字、104 ビット(または 128 ビット)のキーは 13 文字になります。16 進数で は、各文字が 4 ビットなので、40 ビッ トのキーは 10 文字の 16 進数 128 ビットのキーは 26 文字の 16 進数となり ます。

Authentication type (認証タイプ)

設定	説明	工場既定値
Open(オープン)	データ暗号化は有効ですが、認証はありません。	Open(オープン)
Shared(共有)	データの暗号化と認証の両方が使用されます。	

Key type (キータイプ)

設定	説明	工場既定値
HEX	16 進数形式で WEP キーを指定	HEX
ASCII	ASCII 形式で WEP キーを指定	

Key length(キー長)

設定	説明	工場既定値
64 bits(64 ビット)	初期化ベクトル 24 ビットの 40 ビットシークレットキーを使用	64 bits
128 bits(128 ビット)	初期化ベクトル 24 ビットの 104 ビットシークレットキーを使用	

Key index(キーインデックス)

設定	説明	工場既定値
1-4	使用する WEP キーを指定	Open(オープン)

WEP key 1-4(WEP キー 1-4)

設定	説明	工場既定値
ASCII 形式:	RC4 暗号化エンジンの WEP シードとして使用できる文字列	None(なし)
64 ビット:5 文字		
128 ビット:13 文字 HEX:		
64 ビット:10 文字(16 進		
数)		
128 ビット:26 文字(16 進		
数)		

WPA/WPA2-Personal

WPA(Wi-Fi Protected Access)と WPA2 は WEP の大幅に改善された暗号化方式です。WPA は 802.11i draft 3 に 基づくセキュ リティ規格で、WPA2 は 802.11i の承認済みバージョンに基づいています。初期化ベクトルは、WEP の 2 倍の 48 ビットで送信、 暗号化、および強化されます。本当のセッションを保護するために、キーは定期的に変更さ れます。

AES 暗号化は WPA2 規格だけに含まれますが、一部の無線 AP やクライアントの WPA セキュリティモードでも広く使 用できます。 AWK-3131A は互換性を確保するために、WPA および WPA2 の AES アルゴリズムにも対応しています。

WPA/WPA-PSK(Pre-Shared Key)としても知られる Personal バージョンの WPA/WPA2 は、無線通信の機密性を高める暗号化の ための手軽な手段を提供します。パスフレーズは WLAN 接続の暗号化方式(または暗号タイプ)のベースとして使用されます。パス フレーズは、できるだけ長い複雑なものでなければなりません。パスフレーズの ASCII 文字の数は最小8文字、最大63文字です。 安全のため、このパスフレーズは部外者に公表せず、定期的に変更してください。

WLAN Security Settings

SSID	MOXA
Security mode	WPA T
WPA type	Personal 🔻
Encryption method	AES T
EAPOL version	1 •
Passphrase	•••••
Key renewal	3600 (60~86400 seconds)

Submit

WPA type(WAP タイプ)

設定	説明	工場既定値
Personal(個人)	PSK(Pre-Shared Key)対応の WPA と WPA2 を提供します	Personal(個人)
Enterprise(法人)	WPA と WPA2 の法人レベルのセキュリティを提供します	

Encryption method(暗号化方式)

設定	説明	工場既定値
TKIP**	TKIP(Temporal Key Integrity Protocol)を使用します	AES
AES	AES(Advance Encryption System)を使用します	
Mixed*(混在)	TKIP ブロードキャストキーと TKIP+AES ユニキャストキーを一部のレガシ	
	ーAP クライアントに提供します。このオプションはあまり使用されません	

** このオプションは 802.11a/b/g 規格でのみ使用できます

* このオプションは AP/マスタのレガシーモードでのみ使用でき、AES 対応クライアントでは使用できません.

Passphrase (パスフレーズ)

設定	説明	工場既定値
8~63 文字	暗号化および復号化用のキーを生成するためのマスタキー	なし

Key renewal (for AP/Master mode only)

設定	説明	工場既定値
60~86400 秒	グループキーを更新する間隔を指定します	3600(秒)
(1 分~1 日)		

メモ

「key renewal」(キー更新)の値は、暗号化キーを変更する頻度を無線 AP に指示します。通常、この「key renewal」(キー更新)の 値を短く設定して暗号化キーが頻繁に変更されるようにすると、セキュリティレベルは高くなります。デフ ォルト値は 360 秒(6 分) です。回線があまり混み合っていない場合は、更新間隔を長くすることもできます。

WPA/WPA2-Enterprise (AP/マスタモード)

「*WPA type*」(WPA タイプ)を「Enterprise」(法人)に設定すると、802.1X によって使用されるフレームワーク認証プロトコルである EAP(Extensible Authentication Protocol)を使ったネットワーク認証が可能になります。これらの Enterprise(法人)レベルのセキュリ ティモードでは、WPA/WPA2 で IEEE 802.1X 機能が有効な場合、バックエンドの RADIUS(Remote Authentication Dial-In User Service)サーバが必要です。IEEE 802.1X プロトコルにより、大規模ネットワークで効率的な接続認証を実行することが可能になりま す。キーやパスフレーズの交換は必要ありません。

WLAN Security Settings

SSID	MOXA
Security mode	WPA 🔻
WPA type	Enterprise 🔻
Encryption method	AES V
EAPOL version	1 🔻
Primary RADIUS server IP	
Primary RADIUS server port	1812
Primary RADIUS shared key	
Secondary RADIUS server IP	
Secondary RADIUS server port	1812
Secondary RADIUS shared key	
Key renewal	3600 (60~86400 seconds)

Submit

WPA type (WAP タイプ)

設定	説明	工場既定値
Personal(個人)	PSK(Pre-Shared Key)対応の WPA と WPA2 を提供します	Personal(個人)
Enterprise(法人)	WPA と WPA2 の法人レベルのセキュリティを提供します	

Encryption method(暗号化方式)

設定	説明	工場既定値
TKIP**	TKIP(Temporal Key Integrity Protocol)を使用します	AES
AES	AES(Advance Encryption System)を使用します	
Mixed*	TKIP ブロードキャストキーと TKIP+AES ユニキャストキーを一部のレガシ	
	ーAP クライアントに提供します。このオプションはあま り使用されません。	

** このオプションは 802.11a/b/g 規格でのみ使用できます

*このオプションは AP/マスタのレガシーモードでのみ使用でき、AES 対応クライアントでは使用できません.

Primary/Secondary RADIUS server IP(プライマリ/セカンダリ RADIUS サーバ IP)

設定	説明	工場既定値
RADIUS サーバの IP アドレ	EAP 用の代用 RADIUS サーバを指定します。	なし
ス		

Primary/Secondary RADIUS port (プライマリ/セカンダリ RADIUS ポート)

設定	説明	工場既定値
ポート番号	代理 RADIUS サーバのポート番号を指定します。	1812

Primary/ Secondary RADIUS shared key(プライマリ/セカンダリ RADIUS 共有キー)

設定	説明	工場既定値
最大 31 文字	AP と RADIUS サーバの共有シークレットキー	なし

Key renewal(キー更新)

設定	説明	工場既定値
60 分~ 86400 秒	グループキーを更新する間隔を指定します	3600 (秒)
(1 分~1 年)		

WPA/WPA2-Enterprise (クライアント/クライアントールータ/スレーブモード)

クライアントとして使用する場合、AWK-3131A はAP側のWPA/WPA-Enterprise 設定に応じて、EAP-TLS、EAP-TTLS、EAP-PEAP の 3 種類の EAP 方式(または EAP プロトコル)に対応できます。

WLAN Security Settings

SSID Security mode	MOXA WPA2 V
WPA type	Enterprise 🔻
Encryption method	TKIP 🔻
EAPOL version	1 🔻
EAP protocol	TLS 🔻
Certificate issued to	TLS
Certificate issued by	TTLS
Certificate expiration date	PEAP

Submit

Encryption method(暗号化方式)

設定	説明	工場既定値
TKIP**	TKIP(Temporal Key Integrity Protocol)を使用します	ТКІР
AES	AES(Advance Encryption System)を使用します	

** このオプションは 802.11a/b/g 規格でのみ使用できます.

EAP protocol

設定	説明	工場既定値
TLS	TLS(Transport Layer Security)プロトコルを指定	TLS
TTLS	TTLS(Tunneled Transport Layer Security)を指定	
PEAP	PEAP(Protected Extensible Authentication Protocol、別名 Protected	
	EAP)を指定	

クライアント側で WPA/WPA2-Enterpise 設定として EAP プロトコルを選択する前に、AP 側でシステムが同プロトコ ルに対応してい るかどうかをネットワーク管理者に確認してください。上記の3種類の一般的な EAP プロトコルについて、以下の各セクションで詳しく 説明していきます

EAP-TLS

TLS は SSL(Secure Socket Layer)の後継規格で、分散ネットワーク上で信頼できる通信チャンネルを確立できま す。TLS は証明 書交換による相互認証に対応しています。EAP-TLS も安全に使用できます。確認のためにデジタル証 明書を認証サーバに送信 する必要がありますが、認証サーバも証明書を提供しなければなりません。

「Basic WLAN Setup」(基本 WLAN 設定)→「WLAN Certificate Settings」(WLAN 証明書設定)を使用すれば、クライアント側で WLAN 証明書をインポートして EAP-TLS を使用できます。
WLAN Security Settings

SSID	MOXA
Security mode	WPA2 🔻
WPA type	Enterprise 🔻
Encryption method	TKIP 🔻
EAPOL version	1 🔻
EAP protocol	TLS 🔻
Certificate issued to	
Certificate issued by	
Certificate expiration date	

Submit

使用できる場合は、「Current Status 」(現在のステータス)で現在の証明書のステータスを確認できます.

- 「Certificate issued to」(証明書の発行先): 証明書のユーザー
- 「Certificate issued by」(証明書の発行元): 証明書の発行者
- 「Certificate expiration date」(証明書の有効期限): 証明書が期限切れとなる日付

EAP-TTLS

通常、平行する認証システムを作成するよりも、Windows ドメイン、Active Directory、LDAP ディレクトリ、 Kerberos レルムといった 既存の認証システムを再利用するほうがはるかに容易です。したがって、いわゆる「レガシ 一認証方式」に対応するためには TTLS (Tunneled TLS)や PEAP(Protected EAP)が使用されます

TTLS と PEAP の機能は同じです。最初に、両者は EAP-TLS のような TLS トンネルを構築して、認証サーバ上のデジタル証明書で ネットワークが信頼できるかどうかを検証します。このステップでは次のステップ(つまり「内部」認証)を保護するトンネルが確立され るため、「外部」認証と呼ばれることがあります。次に、ネットワークに対してユーザーを認証する古い認証プロトコルを暗号化するた めに、TLS トンネルが使用されます。

上記からわかるように、外部認証でも簡略化された形のデジタル証明書が必要です。必要とされるのは、小規模な証明書発行機関 が作成できる少数の証明書のみです。TTLS や PEAP では証明書の数を削減できるため、EAP-TLS よりもはるかに一般的に使 用されています。

AWK-3131A は PAP、CHAP、MS-CHAP、MS-CHAP-V2 などを含む一部の非暗号型 EAP 方式に対応していま す。これらの EAP 方式を無線ネットワークで直接使用することはお勧めできませんが、TTLS や PEAP による内部認証方式としては役立つかも しれません

内部認証と外部認証は TTLS およ び PEAP で明確なユーザー名を使 用できるので、外部認証では匿名の ユーザー名を使用しておいて、本当 のユーザー名は暗号化されたチャン ネルを使用した場合にのみ 表示さ れるようにすることができます。すべ てのクライアントソ フトウェアが匿名 での変更に対応しているわけではな いことに注意してください。TTLS や PEAP によって ID を隠せるようにす る前に、この点をネットワーク管理者 に確認してください。

WLAN Security Settings

SSID	MOXA
Security mode	WPA2 V
WPA type	Enterprise 🔻
Encryption method	TKIP V
EAPOL version	1 🔻
EAP protocol	TTLS V
TTLS inner authentication	MS-CHAP-V2 V
Anonymous name	PAP CHAP MS_CLIAP
user name	
Password	MS-CHAP-V2

Submit

TTL inner authentication(TTL 内部認証)

設定	説明	工場既定値
PAP	PAP(Password Authentication Protocol)を使用	MS-CHAP-V2
CHAP	CHAP(Challenge Handshake Authentication Protocol)を使用	
MS-CHAP	Microsoft CHAP を使用	
MS-CHAP-V2	Microsoft CHAP バージョン 2 を使用	

Anonymous(匿名)

設定	説明	工場既定値
最大 31 文字	外部認証に使用される明確な名前	なし

User name (ユーザー名)と Password(パスワード)

設定	説明	工場既定値
	内部認証で使用されるユーザー名とパスワード	なし

PEAP

TLS と PEAP の内部認証手順に はいくつか違いがあります。TTLS は暗号化されたチャンネルを使って 属性値ペア(AVP)を交換しますが、 PEAP は暗号化されたチャ ンネル を使ってトンネル内で2番目の EAP 交換を開始します。AWK-3131A は内部認証の EAP 方式としてのみ MS-CHAP-V2 に対応しています。

WLAN Security Settings

SSID	MOXA
Security mode	WPA2 🔻
WPA type	Enterprise 🔻
Encryption method	TKIP V
EAPOL version	1 🔻
EAP protocol	PEAP V
Inner EAP protocol	MS-CHAP-V2 🔻
Anonymous name	MS-CHAP-V2
User name	
Password	

Submit

Inner EAP protocol(内部 EAP プロトコル)

設定	説明	工場既定値
MS-CHAP-V2	Microsoft CHAP バージョン 2 を使用	MS-CHAP-V2

Anonymous(匿名)

設定	説明	工場既定値
最大 31 文字	外部認証に使用される明確な名前	なし

User name (ユーザー名)と Password (パスワード)

設定	説明	工場既定値
-	内部認証で使用されるユーザー名とパスワード	なし

Advanced WLAN Settings(詳細 WLAN 設定)

このセクションでは、無線ネットワークの設定に役立つ詳細な無線関連パラメータについて詳しく説明します。

Advanced WLAN Settings

Township land and a	A
Transmission rate	Auto •
Minimum transmission rate	0 (0 to 64Mbps, 0 to disable)
Multicast rate	6M •
Maximum transmission power	20 dBm 🔻
Beacon interval	100 (40 to 1000ms)
DTIM interval	1 (1 to 15)
Inactive timeout	60 (1 to 240 second)
Fragmentation threshold	2346 (256 to 2346)
RTS threshold	2346 (32 to 2346)
Antenna	Both T
WMM	Enable 🔻
Turbo Roaming	Enable
AeroLink Protection	Disable 🔻
MAC clone	Disable 🔻

Submit

Transmission rate(伝送速度)

設定	説明	工場既定値
Auto(自動)	AWK-3131A はデータ速度を自動的に感知して調整します。	Auto(自動)
使用可能な速度	使用するデータ速度をユーザーが手動で選択できますが、RF タイプが	
	G/N 混在、B/G/N 混在、または A/N 混在の場合には選択できません。	

Minimum transmission rate(最小伝送速度)

設定	説明	工場既定値
0 ~64 Mbps	最小通信速度を設定すれば、AWK-3131A が信号の弱い無線リンクと 通	0(使用しない)
(使用しない場合は0に設	信しなくなり、無線の全体的パフォーマンスが維持されて、無線周 波数の	
定)	使用が最適化されます。	

Multicast rate (マルチキャストレート)

設定	説明	工場既定値
使用可能な速度	ブロードキャストおよびマルチキャストパケットの伝送のために、無線機べ	6M
	ースで固定マルチキャストレートを設定できます。このパ ラメータは、無線	
	メディアでマルチキャストビデオストリーミン グが行われる場合に有用です	
	(設定されたレートを無線クライアント が処理できる場合)。	

Maximum Transmission power(最大伝送送信出力)

設定	説明	工場既定値
使用可能な出力	大出力電力をマスクするための電力をユーザーが手動で選択できま す。	20 dBm
	送信速度が異なると最大出力電力も異なる場合があるため、製品 データ	
	シートを確認してください。802.11bg の場合、選択可能な出力は 0~20	
	です。	

Beacon interval(ビーコン間隔)(AP/マスタモードのみ)

設定	説明	工場既定値
ビーコン間隔	ビーコンの周波数間隔を指定します。	100 (ms)
(40~1000 ms)		

Inactive timeout (非アクティブタイムアウト)(AP モードのみ)

設定	説明	工場既定値
8 ~240 秒	アクセスポイントがクライアントにアライブパケットを送信し始 めるまでの時	60 (秒)
	間	

DTIM interval(DTIM 間隔)(AP/マスタモードのみ)

設定	説明	工場既定値
データビーコンレート	AWK-3131A が DTIM(Delivery Traffic Indication Message)を 送信する頻	1
(1~15)	度を示します。	

Fragmentation threshold(フラグメント化しきい値)

設定	説明	工場既定値
フラグメント長	別の新しいパケットを分割して作成する前のデータパケットの最大 サイズ	2346
(256~2346)	を指定します。	

RTS threshold(RTS しきい値)

設定	説明	工場既定値
RTS/CTS しきい値 (256~	パケットのサイズがそれ以上大きくなったらアクセスポイントが通 信効率を	2346
2346)	確保するために送受信を調整することになる最大サイズを指 定します。	

メモ 上記の各設定の詳細については、付録 A の関連用語集が参考になります。上記の各パラメータを正しく設定すれば、無線ネットワークのパフォーマンスを向上させることができます。

Transmission distance(伝送距離)		
設定	説明	工場既定値
伝送距離または最大範囲	2 台の AWK デバイス間の伝送距離または最大範囲を指定します。こ のパ	500
(500 ~ 11,000 m)	ラメータは特に長距離通信の場合に、正しく設定する必要があり ます。	

メモ AP とクライアントの両方で同じ「Transmission distance」(伝送距離)パラメータが設定されていることを確認してください。このパラ メータが 500 を超える場合、長距離伝送に対応した最適なアルゴリズムが使用されます(5GHZ のチャネルのみ)

Antenna(アンテナ)

設定	説明	工場既定値
A/B/Auto(自動)	出力アンテナポートを指定します。「Antenna」(アンテナ)を「Auto」(自動)	Auto(自動)
	に設定すると、802.11n 対応 2x2 MIMO 通信と、802.11a/b/g 対応レガシ	
	ーモードの 2T2R*通信を使用できます。	

*メモ: スループットが 2 倍になる 802.11n の複数空間データストリーム(2x2 MIMO)とは異なり、2T2R は同じデータを両方のアン テナポートから送受信します。

WMM

設定	説明	工場既定値
Enable(使用する)/Disable	WMM は WLAN トラフィックの QoS 規格です。WMM 対応の無線 クライア	Enable(使用する)
(使用しない)	ントで WMM を有効にすると、音声とビデオのデータが優先されます。	
	メモ: 802.11n モードでは WMM が常に有効になっています。	

Turbo Roaming (クライアントモードのみ)

設定	説明	工場既定値
Enable(使用する)	Disable(使用しない)	Disable(使用しない)
/Disable(使用しない)	MoxaのTurbo Roaming は AWK-3131A がクライアントとして一群の APの	
	間でローミングする場合に、迅速なハンドオーバーを可能にします。	

「Turbo Roaming」を使用すると、以下のパラメータが表示されます。

 Roaming threshold: 」(ローミングしきい値):新しい AP 候補をいつ探し始めるかを指定します。現在の接続品質(SNR または 信号強度)がここで指定したしきい値より低くなると、AWK がバックグラウンドスキャン を開始して、ネクストホップ候補を探しま す。

下の表に、異なる RF タイプごとのデフォルトのしきい値のリストを示します。

RF タイプ	RSSI	信号強度
レガシー 2.4G	30	-65
レガシー 5G	30	-65
N-モ ー ド 2.4G	40	-55
N-モード 5G	40	-50

- メモ AWK がバックグラウンドスキャンを実行している間は、無線のパフォーマンスが通常より3分の1低下します。
 - 「Roaming difference」(ローミングの差分): ローミングを実行するべきかどうかを決定します。バッ クグラウンドスキャンがトリガ された後、ローミングが実行されるのは、AP 候補が現在の接続より高い接続品質(つまりローミングの差分)を提供する場合 だけです。複数のアクセスポイントがその基準を満たす場合は、接続品質が最高のアクセスポイントがローミング先として選択さ れます。
 - 「Scan channels」(チャンネル検索):通信チャンネルとローミングチャンネルを事前定義します。
 - 「AP alive check」(AP アライブ確認): AeroLink Protection がより迅速に WLAN の切断に対応できるようにします。
- メモ この機能を有効にすると、トラフィックがないときに AWK-3131A が 10ミリ秒間隔でアライブ確認パケットを送信する ようになります。小さなアライブ確認パケットを高頻度で送信すると、同じチャンネルを使用する他の無線通信に影響する可能性があるため、この機能は指定した無線チャンネルを完全に制御できる場合にのみ使用してください。
 - 「AP candidate threshold」(AP 候補しきい値):「AP alive check」(AP アライブ確認)機能が現在のアクセスポイントを使用不能 であるとした後で周囲のアクセスポイントが接続先の AP 候補として認定されるためには、そのアクセスポイントの接続品質 (SNR/信号強度)が十分に高くなければなりません。

Turbo Roaming RF type	 Enable B/G/N Mixed
Roaming threshold	SNR 30 dB (5 ~ 40)
	Signal Strength -75 dBm (-100 ~ -35)
Roaming difference	7 (5 ~ 20)
Scan channels	6 •
	Not Scanning 🔻
	Not Scanning 🔻
AP alive check	Enable 🔻
AP candidate threshold	SNR 20 dB (5 ~ 40)
	Signal Strength -85 dBm (-100 ~ -35)

メモ

製品の文書に掲載されている Turbo Roaming の回復時間(<150 ms)は、試験結果の平均値です。 それは最適化された条件下で行 われており、AP 間は干渉のない 20MHz の RF チャネルを使い、WPA2-PSK セキュリティと既定値の Turbo Roaming パラメータを使 っています。クライアントは 100Kbps のトラフィック負荷のある3-チャネルのローミングで設定されます。しかしながら、いくつかの要素 が組み合わさるとローミングクライアントの AF 回復時間に影響が出ます。例えば以下の項目が挙げられます。

- サイトの RF 干渉
- クライアントのデバイスの移動速度
- アプリケーションのトラフィックのスループット
- 設定された Turbo Roaming のパラメータ。例えばローミングのしきい値、ローミングの差分、AP 候補のしきい値等。.

従って、デバイスの適用に先立ってサイトサーベイ(現地調査)をお勧めします。クライアントと AP の両方にとって理想的なパラメータ 設定を評価することでアプリケーションに対して最適な適用プランを立てることができます。

AeroLink Protection(クライアントモードのみ)

設定	説明	工場既定値
Enable(使用する)/ Disable	AeroLink Protection を有効にして、同じ LAN ネットワーク上の無 線クラ	Disable(使用しない)
(使用しない)	イアントが自動的に互いとネゴシエートし、冗長な無線通信を構成できるよ	
	うにします。詳細については、「Status」(ステータス)→「AeroLink	
	Protection Status」(AeroLink Protection のステータス)を参照してください。	

AeroLink Protection を使用すると、以下のパラメータが表示されます。

AeroLink Protection	Enable 🔻
AP alive check	Disable 🔻
AeroLink SNR/Signal Strength detection	Enable
AeroLink threshold	SNR 40 (5 to 40)
	Signal Strength -55 dBm (-100 to -35)
AeroLink difference	7 (5 to 20)

- 「AP alive check」(AP アライブ確認):「Enable」(使用する)を選択すると AeroLink Protection が WLAN 切断により早く反応する ようになります。
- 「AeroLink SNR/Signal Strength detection」(AeroLink SNR/信号強度検出): SNR/信号強度しきい値を基準に AeroLink の応答 を許可します。
- 「AeroLink threshold」(AeroLink しきい値): 冗長な無線デバイスをいつ探し始めるかを決定します。もしも現在の接続品質(SNR か信号強度)が指定のしきい値より低い場合、クライアントは他の適切な無線デバイスを探し始めます。
- AeroLink difference (AeroLink 差分): クライアントがいつ他の通信パスへ切り替えるかを決定します。 冗長な無線デバイスを探 した後、 冗長な無線でデバイスに切り替えるのは候補が現在の接続よりも良い(AeroLink 差分)接続品質を提供できる時だけで す。

メモ

この機能を有効にすると、トラフィックがないときに AWK-3131A が 10 ミリ秒間隔でアライブ確認パケットを送信する ようになりま す。小さなアライブ確認パケットを高頻度で送信すると、同じチャンネルを使用する他の無線通信に影響する可能性があるため、この 機能は指定した無線チャンネルを完全に制御できる場合にのみ使用してください。 MAC clone (MAC クローン)(クライアントモードのみ)

MAC clone MAC clone method

MAC clone static MAC

Enable 🔻 Static 🔻

(ex: 00:90:E8:00:00:01)

設定	説明	工場既定値
MAC clone	この特長を使用するとAWK クライアントに装置の MAC アドレスをコピーする	Disable
(MAC クローン)	のを許可します。これにより MAC センシティブなネットワーク(MAC をベース	(使用しない)
	にした通信または MAC 認証によるネットワーク)における IP ブリッジの動作	
	の制限を克服することができます。	
MAC clone method	• Auto(自動): AWK クライアントは AWK に接続するデバイスが1つだけ	Auto(自動)
(MAC クローンメソッド)	の時 LAN に接続するデバイスの MAC アドレスをコピーします。	
	• Static (スタティック:静的):AWK クラインアントは LAN に接続する複数	
	のデバイスに使われる MAC アドレスをシェアします。これは AWK に	
	LAN を介して複数のデバイスが接続することを許可し、そのうちの1つ	
	だけが MAC アドレスを割り当てられる必要があります。	
MAC clone static address	AWK デバイスに接続する、コピーされるべきスタティックな MAC アドレスを	-
(MAC クローンスタティック	指定します。	
アドレス)		

WLAN Certificate Settings (WLAN 証明書設定)

(EAP-TLS の Client(クライアント)/Client-router(クライアント-ルータ)/

Slave (スレーブ)モードのみ)

EAP-TLSが使われる時、末端のクライアントにはWPA/WPA2-エンタープライズをサポートするためにWLAN 証明書が必要になりま す。AWK-3131A は **PKCS #12** をサポートします。それは「*Personal Information Exchange Syntax Standard」*(個人情報交換文法標 準)として知られており、パスワードベースのシンメトリックなキーで保護されたパブリックキーの証明を伴うもので、プライベートキー を保存するために、一般的に使われれるファイルフォーマットを定義する証明書フォーマットです。

WLAN Certificate Settings

Certificate private password		
Select certificate/key file	Browse	

Submit	
Status	
Certificate issued to	
Certificate issued by	
Certificate expiration date	

Current status(現在の状況)は、AWK-3131A にインポートされている、現在の WLAN の証明書の情報を表示します。証明書が有効でなければなにも表示されません。

Certificate issued to(証明書の利用者): 証明書の利用者を示します。

Certificate issued by(証明書発行者):証明書を発行した人を示します。

Certificate expiration date(証明書失効日):証明書が失効する日を表示します。

Import WLAN Certificate (WLAN 証明書のインポート)という次のステップを順に行うと新しい WLAN 証明書をインポートすることが出来ます。

「Certificate private password」(プライベートパスワードの証明書)欄に対応するパスワード(またはキー)を入力し「Submit」(提出)をクリックしてパスワードをセットする。

- 2. パスワードが「Certificate private password」欄に表示される。ブラウザの「*Select certificate/key file*」(証明書/キーのファイルを 選択する)のボタンをクリックして証明書ファイルを選択する。
- 「Upload Certificate File」(証明書ファイルをアップロードする)をクリックして証明書ファイルをインポートする。インポートが成功したら、「*Current Certificate*」(現在の証明書)にアップロードした情報が確認できる。もしも失敗したら、ステップ1にもどってパスワードを正しく設定し証明書ファイルのインポートをもう一度行う必要があるかもしれない。

Certificate private password	
Submit	
Step 2:	
Select certificate/key file	Browse

✓モ WLAN 証明書は AWK-3131A がリブートした後も残ります。たとえ失効しても「Current Certificate」で見ることができます。

Advanced Setup(詳細設定)

AWK-3131A およびワイヤレスネットワークシステムの機能を向上させるために、いくつかの高度な機能を利用できます。 VLAN は、レ イヤー2 ネットワークのブロードキャストドメインに接続されているかのようにグループ化されたクライアントとホストの集合です。

DHCP サーバーは、ワイヤレスクライアントを効率的に展開するのに役立ちます。 パケットフィルタは、ファイアウォールなどのセキュ リティメカニズムをさまざまなネットワークレイヤーに提供します。さらに、AWK-3131A は STP / RSTP プロトコルをサポートしてネット ワーク全体の信頼性を高め、SNMP サポートによりネットワーク管理を容易にすることができます。

Using Virtual LAN (仮想 LAN の使用)

仮想 LAN(VLAN)を AWK シリーズでセットアップすると、物理的なセグメントとは対照的に、LAN を論理的なセグメントに分割すること で効率が向上します。一般的に VLAN の方が管理しやすいです。

仮想 LAN(VLAN)のコンセプト

VLAN って何?

仮想 LAN は、VLAN と一般的に知られていますが、物理的な配置とは関係なしに、同じブロードキャストドメインにつながっているか のように通信する仕様を共通セットに持つホストグループです。 VLAN は同じ物理 LAN と同じ特性を持ちますが、末端の端末が同じ ネットワークスイッチ上になくても一緒のグループになれます。 デバイスの物理的な再配置をすることなしにソフトウェアでネットワーク の再設定が行えます。

VLAN はアクセスポイント信号が届く範囲で広がります。クライアントは SSID や VLAN アサインメントを介して無線のサブネットワーク にセグメント付けることができます。 クライアントはアサインされた SSID/VLAN をサポートするよう設定された AP に接続することでネ ットワークにアクセスできます。

VLAN の利点

VLANs は便利で効率的で簡単にネットワークを管理するために次のように使われます。

- 追加、移動、変更を単一のコンタクト先から管理できます
- 監視グループを定義できます
- 不必要な宛先へのブロードキャストやマルチキャスト通信のトラフィックを軽減します
- ネットワークパフォーマンスを改善し遅延を減らします
- セキュリティが向上します
- 安全なネットワークにより、メンバー自身の VLAN のリソースを抑制できます。
- セキュリティを妥協することなくクライアントはローミングできます。

VLAN ワークグループとトラフィックマネジメント

AP は、ネットワークネーム(SSID)をベースにクライアントを VLAN にアサインします。AP は、無線インターフェイスごとに最大 9 つの SSID をサポートでき、SSID ごとに設定可能な一意の VLAN を使用できます。AP は、送信または受信されたパケットをネットワーク名 に関連付けられた VLAN と照合します。VLAN が受信したトラフィックは、同じ VLAN に関連付けられた無線インターフェイスでのみ送 信されます。これにより、無線 LAN 上の不要なトラフィックが排除され、帯域幅が節約され、スループットが最大化されます。

無線トラフィック管理の強化に加えて、VLAN 対応 AP は、無線ユーザーのワークグループへの簡単な割り当てをサポートします。 典 型的なシナリオでは、各ユーザーVLAN は部門ワークグループを表します。たとえば、1 つの VLAN をマーケティング部門に使用し、 もう1 つの VLAN を人事部門に使用できます。

このシナリオでは、AP は受け入れたすべてのパケットを VLAN に割り当てます。各パケットは、受信した無線クライアントに応じて、 マーケティングまたは人事として識別されます。AP は、有線バックボーンでネットワークスイッチに送信されるパケットに、識別子付き の VLAN ヘッダーまたは「タグ」を挿入します。

最後に、マーケティング部門からプリンタやサーバーなどの適切 な企業リソースにパケットをルーティングするようにスイッチを構 成します。人事部からのパケットは、インターネットへのアクセス のみを許可するゲートウェイに制限できます。人事部のメンバ ーは、電子メールを送受信してインターネットにアクセスできま すが、ローカル企業ネットワーク上のサーバまたはホストにアク セスすることはできません。



仮想 LAN を設定する

VLAN 設定

AWK の VLAN を設定するには、VLAN 設定ページを使用してポートを設定します。

VLAN Settings

Management VLAN ID:	1		
Port	PVID	VLAN Tagged (Use commas to separate VLAN tags)	
LAN	1		
MOXA (WLAN 1)	1		
Submit			

Management VLAN ID(マネジメント VLAN ID)

設定	説明	工場既定値
VLAN ID	AWK のマネジメント VLAN を設定します。	1
範囲:1 [~] 4094		

Port(ポート)

型式	説明	基幹ポート
LAN	このポートは AWK の LAN ポートです	Yes(はい)
WLAN	これは特定の SSID の無線ポートです。このフィールドは生成された SSID を	
	参照します。もしより多くの SSID が作られたら新しい役割が追加されます。	

Port PVID

設定	説明	工場既定値
VLAN ID	ポートに接続するデバイスのポートの VLAN ID を設定します。 ポートは	1
(1~4094)	LAN ポートまたは WLAN ポートにすることができます。	

VLAN Tagged

設定	説明	工場既定値
コンマで分割された VLAN	どの LAN がこの特定の LAN と通信するのかを規定します。	(なし)
ID のリスト。各 VLAN ID は		
1~4094 _°		

メモ VLAN 機能により、無線クライアントは AP を管理できます。 VLAN 管理 ID が VLAN ID と一致する場合、その VLAN のメンバーであ る無線クライアントは AP 管理アクセスを持ちます。

注意: VLAN 管理 ID が設定され、AP の VLAN ID の 1 つと同等になると、そのユーザーVLAN のすべてのメンバーが AP への管理 アクセス権を持ちます。 VLAN メンバーシップを AP への正当なアクセスを持つ人々に制限するように注意してください。

DHCP Server(DHCP サーバ) (AP/クライアント-ルータモードのみ)

DHCP(Dynamic Host Configuration Protocol)は、管理者が、永久 IP アドレスを割り当てるのではなく、IP アドレスをユーザーにー 定期間「リース」することによって、一時的な IP アドレスをネットワークコンピュータに割り当てられるようにするネットワークプロトコ ルです。

AWK-3131A は簡略型 DHCP サーバとして機能するので、クライアント側からの DHCP 要求に応えて、無線クライアントに IP アドレスを容易に割り当てることができます。このページで設定した IP 関連のパラメータはクライアントにも送信されます。

特定のクライアントの MAC アドレスを入力すれば、そのクライアントに静的 IP アドレスを割り当てることができま す。AWK-3131A は最大 16 のエンティティを含む「Static DHCP mapping」(静的 DHCP マッピング)リストを 提供します。設定をアクティブにするに は、各エンティティの「Active」(アクティブ)チェックボックスをチェック してください。

IP 割り当てのステータスは、「Status」(ステータス)→「DHCP Client List」(DHCP クライアントリスト)の下で確認できます。

DHCP Server (For AP/Client-Router mode only)

DHCP server	Disable 🔻
Default gateway	
Subnet mask	
Primary DNS server	
Secondary DNS server	
Starting IP address	
Maximum number of users	
Client lease time	14400 (2 to 14400 minutes)

Static DHCP Mapping

No.	Active	IP Address	MAC Address
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

Submit

DHCP server (DHCP サーバ)

設定	説明	工場既定値
Enable(使用する)	AWK-3131A を DHCP サーバとして使用します。	Disable(使用しない)
Disable(使用しない)	DHCP サーバ機能を使用しません。	

Default gateway (デフォルトゲートウェイ)

設定	説明	工場既定値
デフォルトゲートウェ イの	外部ネットワークに接続するルータの IP アドレス	なし
IP アドレス		

Subnet mask (サブネットマスク)

設定	説明	工場既定値
サブネットマスク	サブネットワークの種類を識別します(例: クラス В のネットワー クでは	なし
	255.255.0.0、クラス C のネットワークでは 255.255.255.0)	

Primary/ Secondary DNS server (プライマリ /セカンダリ DNS サーバ)

設定	説明	工場既定値
プライマリ/セカンダリ DNS	ネットワークで使用される DNS サーバの IP アドレス。DNS サーバの IP	なし
サーバの IP アドレス	アドレスを入力すると、URL を使用できるようになります。プライマリ DNS	
	サーバが接続に失敗すると、セカンダリ DNS サーバが使用されます。	

Start IP address(スタート IP アドレス)

設定	説明	工場既定値
IP address(IP アドレス)	AWK-3131A が割り当て可能な最初の IP アドレスを表示します。	なし

Maximum number of users (ユーザーの最大数)

設定	説明	工場既定値
1~128	同時に割り当て可能な IP アドレスの数を指定します。	なし

Client lease time(クライアントリース時間)

設定	説明	工場既定値
2~14400 分	IP アドレスを割り当てるリース時間。リース時間に達すると、IP ア ドレス	14400 分
	の有効期限が切れます。	(10 日)

Packet Filters(パケットフィルタ)

AWK-3131A には LAN および WLAN インターフェイスを経由する、**P ベース**パケットの様々なフィルタが含まれ ています。それらのフィルタをファイアウォールとして設定すれば、ネットワークのセキュリティを強化できます。

MAC Filters (MAC フィルタ)

AWK-3131A の MAC フィルタは特定の MAC アドレスを持つ IP ベースのパケットを承認または排除できるポリシー ベースのフィ ルタです。AWK-3131A では、フィルタリングポリシーに MAC アドレスを設定するためのエンティテ ィが 32 ロ用意されています。設 定をアクティブにするには、各エンティティの「Active」(アクティブ)チェックボ ックスをチェックしてください。

MAC Filters			
MAC filters fun Policy	ction	Disable ▼ Drop ▼	
No.	Active	Name	MAC Address
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			

Submit

MAC filters (MAC フィルタ)

設定	説明	工場既定値
Enable(使用する)	MAC フィルタを使用します	Disable(使用しない)
Disable(使用しない)	MAC を使用しません	

Policy(ポリシー)

設定	説明	工場既定値
Accept(許可)	リストアップされたエンティティからのパケットのみ許可します	Drop(拒否)
Drop(拒否)	リストアップされたエンティティからのパケットをすべて拒否します	

注意

フィルタ機能を使用する場合は、以下に注意してください。 「Drop」(拒否)+「リスト内のエンティティを 1 つもアクティブ化しない」 = すべてのパケットを許可する 「Accept」(許可)+「リスト内のエンティティを 1 つもアクティブ化しない」 = すべてのパケットを拒否する

IP Protocol Filters (IP プロトコルフィルタ)

AWK-3131A の IP プロトコルフィルタは、特定の IP プロトコルと送信元/送信先 IP アドレスを持つ IP ベースのパケ ットを承認 または排除できるポリシーベースのフィルタです。

AWK-3131A では、フィルタリングポリシーに IP プロトコルとソース/デスティネーション IP アドレスを設定するためのエンティティが 8 つ用意されています。使用可能な IP プロトコルは、「All」(すべて)、「ICMP」、「TCP」、「UDP」の 4 つです。「Source IP」(ソース IP) と「Destination IP」(デスティネーション IP)のいずれかを指定する必要があります。 IP アドレスとネットマスクを組み合わせて、許可 または拒否する特定の IP アドレスや IP アドレスの範囲を指定できます。例えば、「IP アドレス 192.168.1.1 とネットマスク 255.255.255.255」は単一の IP アドレス 192.168.1.1 を表します。「IP アドレス 192.168.1.1 とネットマスク 255.255.255.0」は 192.168.1.1 から 192.168.1.255 までの IP アドレスの範囲を表します。設定をアクティブにするには、各エンティ ティの「Active」(ア クティブ)チェックボックスをチェックしてください。

IP Protocol Filt	ers					
IP protocol filt Policy	ers function		Disable V Drop V			
No.	Active	Protocol	Source IP	Source Netmask	Destination IP	Destination Netmask
1		All 🔻				
2		All 🔻				
3		All 🔻				
4		All 🔻				
5		All 🔻				
6		All 🔻				
7		All 🔻				
8		All 🔻				
9		All 🔻				
10		All 🔻				
11		All 🔻				
12		All 🔻				
13		All 🔻				
14		All 🔻				
15		All 🔻				
16		All 🔻				
17		All 🔻				
18		All 🔻				
19		All 🔻				
20		All V				
21		All 🔻				
22		All 🔻				
23		All V				
24		All V				
25		AII				
20		All Y				
27		All •				
28						
29		All T				
30						
31						
32		All				

Submit

IP protocol filters (IP プロトコルフィルタ)

設定	説明	工場既定値
Enable(使用する)	IP プロトコルフィルタを使用します	Disable(使用しない)
Disable(使用しない)	IP プロトコルフィルタを使用しません	

Policy(ポリシー)

設定	説明	工場既定値
Accept(許可)	リストアップされたエンティティからのパケットのみ許可します	Drop(拒否)
Drop(拒否)	リストアップされたエンティティからのパケットをすべて拒否します	



注意

フィルタ機能を使用する場合は、以下に注意してください。 「**Drop**」(拒否)+「リスト内のエンティティを1つもアクティブ化しない」 = すべてのパケットを許可する。 「**Accept**」(許可)+「リスト内のエンティティを 1 つもアクティブ化<mark>しない</mark>」 = すべてのパケットを拒否する

TCP/UDP Port Filters (TCP/UDP ポートフィルタ)

AWK-3131A の TCP/UDP ポートフィルタは特定のソースポートまたはデスティネーションポートを持つ TCP/UDP ベースのパケットを承認または排除できるポリシーベースのフィルタです。

AWK-3131A では、指定したプロトコルのソース/デスティネーションポートの範囲を設定するためのエンティティが 8 つ用意されてい ます。TCP または UDP プロトコルの選択に加え、ソースポート、デスティネーションポー ト、またはその両方を設定できます。1 つ のポートを指定する場合は、終了ポートは空白のままにしておくことができ ます。ただし、終了ポートが開始ポートを上回ることはで きません。

「Application name」(アプリケーション名)は対応するエンティティを記述する最大 31 文字の文字列です。設定をアクティブにするには、 各エンティティの「Active」(アクティブ)チェックボックスをチェックしてください。

TCP/UDP Port F	ICP/UDP Port Filters				
TCP/UDP port f Policy	ilters function		Disable ▼ Drop ▼		
No.	Active	Source Port	Destination Port	Protocol	Application Name
1		~	~	TCP V	
2		~	~	TCP V	
3		~	~	TCP V	
4		~	~	TCP V	
5		~	~	TCP V	
6		~	~	TCP V	
7		~	~	TCP V	
8		~	~	TCP V	
9		~	~	TCP V	
10		~	~	TCP V	
11		~	~	TCP V	
12		~	~	TCP V	
13		~	~	TCP V	
14		~	~	TCP V	
15		~	~	TCP V	
16		~	~	TCP V	
17		~	~	TCP V	
18		~	~	TCP •	
19		~	~	TCP V	
20		~	~	TCP V	
21		~	~	TCP V	
22		~	~	TCP V	
23		~	~	TCP V	
24		~	~	TCP V	
25		~	~	TCP V	
26		~	~	TCP V	
27		~	~	TCP V	
28		~	~	TCP V	
29		~	~	TCP V	
30		~	~	TCP V	
31		~	~	TCP V	
32		~	~	TCP V	

Submit

TCP/UDP port filters(TCP/UDP ポートフィルタ)

設定	説明	工場既定値
Enable(使用する)	TCP/UDP ポートフィルタを使用します	Disable(使用しない)
Disable(使用しない)	TCP/UDP ポートフィルタを使用しません	

Policy(ポリシー)

設定	説明	工場既定値
Accept(許可)	リストアップされたエンティティからのパケットのみ許可します	Drop(拒否)
Drop(拒否)	リストアップされたエンティティからのパケットをすべて拒否します	



注意

フィルタ機能を使用する場合は、以下に注意してください。 「**Drop**」(拒否)+「リスト内のエンティティを 1 つもアクティブ化<mark>しない</mark>」 = すべてのパケットを許可する 「**Accept**」(許可)+「リスト内のエンティティを 1 つもアクティブ化<mark>しない</mark>」 = すべてのパケットを拒否する

RSTP Settings(RSTP 設定)(マスタまたはスレーブモードのみ)

AWK-3131A は、IEEE 802.1D(スパニングツリープロトコル(STP))と IEEE 802.1w(ラピッド STP)規格に対応しています。 STP/RSTP は、予想外のパスのルーピングを解消するだけでなく、有線/無線パスが誤って切断された場合にバックアップパスにより回復できます。このフェイルオーバー機能はネットワークの信頼性と可用性の向 上に役立ちます。 AWK-3131A の STP/RSTP 機能はデフォルトでは無効になっています。完全な効果を発揮させるには、ネットワークに接続したすべ ての AWK-3131A で RSTP/STP を有効にする必要があります。AWK-3131A が、ネットワークスイッチ機器ではなくデバイス(PLC、 RTU など)に接続しているスレーブの役割を果たす場合、STP/RSTP を有効にする必要はありません。有効にすると、不要なネゴ シエーションが発生する場合があるためです。AWK-3131A はマスタまたはスレーブモードでのみ STP/RSTP に対応します。

以下のそれぞれの図は、設定可能なスパニングツリープロトコルパラメータを示しています。各パラメータの詳しい説明は図の下にあります。

RSTP Settings (WLAN is only for Master/Slave only)						
Bridge priority	32768 🔻					
Hello time	2 (1~10	2 (1~10 seconds)				
Forwarding delay	15 (4~30	seconds)				
Max age	20 (6~40	seconds)				
No	Enable RSTP	Port Priority	Port Cost	🗆 Edge Port		
1 LAN		128 🔻	20000			
2 WLAN : Master		128 🔻	200000			
Submit						

メモ

ファームウェアバージョン 1.6 における STP/RSTP のリカバリー時間は、約 25[~]35 秒です。

RSTP status(RSTP ステータス)

この欄は、STP/RSTP を有効にしている場合にのみ表示されます。この AWK-3131A がスパニングツリーのルート であるかどうか が示されます(ルートは自動的に決定されます。

Bridge priority(ブリッジ優先度)

設定	説明	工場既定値
ユーザーが選択する数値	選択する数字が小さいほど、ブリッジ優先度が高くなります。ブリッ ジ優先	32768
	度が高いほど、スパニングツリートポロジのルートに設定 される確率が高く	
	なります	

Hello time (ハロー時間)

設定	説明	工場既定値
ユーザーが入力する数値	スパニングツリートポロジのルートは、定期的にネットワーク内 の他のデバ	2 (秒)
(1~10 秒	イスに対して「ハロー」メッセージを送信し、トポロジに 問題がないかどうか	
	を確認します。「Hello time」(ハロー時間)は ルートがハローメッセージを送	
	信する頻度を示します。	

Forwarding delay(フォワーディング遅延)

設定	説明	工場既定値
ユーザーが入力する数値	このデバイスがトポロジを変更すべきかどうかを確認するまでに待機 する	15 (秒)
(4~30 秒)	時間を指定します	

Max. age (最大エイジ)

設定	説明	工場既定値
ユーザーが入力する数値	ルートではないデバイスが、「Max. age」(最大エイジ)に設定されている時間	20 (秒)
(6~40 秒)	が経過してもルートから「ハロー」メッセージを受信しなかった場合、このデ	
	バイスは自分自身をルートとして再設定します。ネットワーク上の複数のデ	
	バイスがルートとして検出されると、それらのデバイスが再ネゴシエートし	
	て、新しいスパニングツリ ートポロジを構成します。	

Enable RSTP (RSTP を使用する)

設定	説明	工場既定値
Enable(使用する)/ Disable	スパニングツリートポロジのノードとしてポートを使用するかど うかを指定し	使用しない(チェックな
(使用しない)	ます。	し

Port priority(ポート優先度)

設定	説明	工場既定値
ユーザーが選択する数値	入力する数値が小さいほど、スパニングツリートポロジ内のノー ドとしての	128
	このポートの優先度が上がります。	

Port cost (ポートコスト)

設定	説明	工場既定値
Enable(使用する)/ Disable	入力する数値が大きいほど、このポートはスパニングツリートポ ロジのノー	2000000
(使用しない)	ドとしてより不適格になります。	

Edge port (エッジポート)

設定	説明	工場既定値
チェックあり/なし	BPDU が通過しないと予想されるポートをエッジポートに設定します。	チェックなし(AP ポート
		を除く)

メモ

ネットワーク装置とは対照的に、非 STP/RSTP サブネットワークまたはエンドデバイス(PLC や RTU など)に接続 されているポ ートをエッジポートに指定することをお勧めします。これにより、STP/RSTP プロトコルの不必要な待 機やネゴシエーションを防ぎ、 システムの初期化を加速できます。エッジポートは BPDU を受信すると、STP/RSTP ポートとして機能して、ネゴシエーションを開 始できます。 エッジポートの設定はポートで STP/RSTP を無効にすることとは異なります。STP/RSTP を無効にすると、ポート は STP/RSTP の BPDU をまったく処理しません。

Port Status (ポートステータス)

「Port Status」(ポートステータス)は、スパニングツリーにおけるこのポートの現在のステータスが表示されます。通常の伝送には 「Forwarding」(転送)を使用し、伝送をブロックするには「Blocking」(ブロック)を使用します。

Static Route(静的ルート)(クライアント-ルータモードのみ)

「Static Route」(静的ルート)ページは、AWK-3131A の静的ルーティングテーブルの設定に使用されます。

Static Route (For Client-Router mode only)

No.	Active	Destination	Netmask	Gateway	Metric	Interface
1						LAN 🔻
2						LAN 🔻
3						LAN 🔻
4						LAN 🔻
5						LAN 🔻
6						LAN 🔻
7						LAN T
8						LAN 🔻
9						LAN 🔻
10						LAN 🔻
11						LAN 🔻
12						LAN 🔻
13						LAN 🔻
14						LAN 🔻
15						LAN T
16						LAN V

Submit

Active (アクティブ)

このチェックボックスをチェックすると、静的ルーティングが有効になります。

Destination(送信先)

送信先の IP アドレスを指定します。

Netmask(ネットマスク)

この IP アドレスのサブネットマスクを指定します。

Gateway(ゲートウェイ)

LAN を外部ネットワークに接続しているルータの IP アドレスを指定します。

Metric (メトリック)

隣接するネットワークにアクセスするための「コスト」を指定します。

Interface (インターフェイス)

このルーティングルールのネットワークインターフェイスを指定します。

NAT Settings/Port Forwarding(NAT 設定/ポートフォワーディ ング)(クライアント

-ルータモードのみ)

クライアントールータ動作モードを促進するために、AWK-3131A では NAT (Network Address Translation)と Port Forwarding がサポートされています。この機能はプライベート IP から外部 IP (WAN IP)に送出される通信を変換します。

NAT/Port Forwarding (For Client-Router mode only)

NAT Settings

NAT mode

Disable 🗸

Disable 🗸

Port Forwarding Settings

Port forwarding

設定	説明	工場既定値
NAT mode(NAT モード)	有効 (N-1 NAT または 1-1 NAT)または NAT モードを無効にします。	Disable
		(使わない)
Port Forwarding	ポートフォワーディング機能を有効または無効にします。	Disable
(ポートフォワーディング)		(使わない)

N-1 NAT



1-1 NAT



WAN IP	転送される外部 IP を指定します。
LAN IP	「転送先」LAN IP を指定します。

Port Forwarding (ポートフォワーディング)



設定	説明
Active (アクティブ)	このチェックボックスをチェックして、ポートフォワーディングルールを有効にします。
Protocol(プロトコル)	通信プロトコルを指定します。
WAN Port(WAN ポート)	転送される外部ポートを指定します。
LAN IP	「転送先」LAN IP を指定します。
LAN Port(LAN ポート)	「転送先」LAN ポートを指定します。

通信を始める時に外部デバイスを許可するため、外部ポート(WAN ポート)と内部 IP/ポートコンボ(LAN IP/LAN ポート)との間の静的なマップを定義し、外部デバイスがこのデバイスとの接続を開始できるようにします。

SNMP Agent(SNMP エージェント)

AWK-3131A は SNMP V1/V2c/V3 に対応しています。SNMP V1 と SNMP V2c は認証にコミュニティストリング の照合を使用し ます。すなわち、SNMP サーバはコミュニティストリング「 public/private 」(デフォルト値)を使用して読み取り専用権限または読み取 り/書き込み権限ですべてのオブジェクトにアクセスします。MD5 または SHA 認証レベルを選択する必要がある SNMP V3 は最も安 全なプロトコルです。データ暗号化を有効にしてデータのセキュリティを強化することもできます。

AWK-3131A がサポートする SNMP セキュリティモードとセキュリティレベルは下表のとおりです。SNMP のエージェントとマネージャとの通信で使用されるセキュリティのモードとレベルを選択してください。

プロトコル	UI web ページで	認証の種類	データ暗号化	方式
バージョン	の設定			
SNMP	V1, V2c	コミュニティストリング	なし	認証にコミュニティストリングの照合を使用します。
V1, V2c	Read			
	Community			
	(V1,V2c リード⊐			
	ミュニティ)			
	V1, V2c	コミュニティストリング	なし	認証にコミュニティストリングの照合を使用します。
	Write/Read			
	Community			
	(V1,V2cリード/ラ			
	イトコミュニティ)			
SNMP V3	No-Auth	なし	なし	admin または user アカウントを使用してオブジェ クト
	(認証なし)			にアクセスします
	MD5 または	MD5 または SHA に	なし	HMAC-MDSアルゴリズムまたは HMAC-SHAアル ゴリ
	SHA	基づく認証		ズムに基づく認証を提供します。8 文字のパス ワード
				が認証の最低要件です。
	MD5 または	MD5 または SHA に	データ暗号化キ	HMAC-MDSアルゴリズムまたは HMAC-SHAアル ゴリ
	SHA	基づく認証	—	ズムに基づく認証とデータ暗号化キーを提供します。8
				文字のパスワードとデータ暗号キーが、認 証と暗号化
				の最低要件です。

以下のパラメータは「SNMP Agent」(SNMP エージェント)ページで設定できます。各パラメータの詳しい説明は 図の下にあります。

Ch	 n		0.00	
-	Р.	АП		
_	 •			

SNMP agent	Disable T
Remote management	Disable 🔻
Read community	public
Write commnuity	private
SNMP agent version	V1, V2c •
Admin authentication type	No Auth 🔻
Authentication username	admin 🔻
Admin encryption method	Disable 🔻
Private key	
Private MIB information	
Device object ID	enterprise.8691.15.33

Submit

SNMP agent (SNMP エージェント)

設定	説明	工場既定値
Enable(使用する)	SNMP エージェントを使用します	Disable
Disable(使用しない)	SNMP エージェントを使用しません	(使用しない)

Remote management(リモート管理)

|--|

Enable(使用する)	SNMP エージェントを介したリモート管理を許可します。	Disable
Disable(使用しない)	SNMP エージェントを介したリモート管理を許可しません。	(使用しない)

Read community (リードコミュニティ)(V1, V2c)

設定	説明	工場既定値
V1, V2c リードコミュニティ	最大 31 文字のコミュニティストリングの照合を認証に使用しま す。すなわ	Public
	ち、SNMP エージェントはこのコミュニティストリング を使用して読み取り専	
	用権限ですべてのオブジェクトにアクセスでき ます。	

Write community (ライトコミュニティ)(V1, V2c)

設定	説明	工場既定値
V1, V2c リード/ライトコミュ	最大 31 文字のコミュニティストリングの照合を認証に使用しま す。すなわ	private
ニティ	ち、SNMP エージェントはこのコミュニティストリング を使用して読み取り/	
	書き込み権限ですべてのオブジェクトにアクセ スできます	

SNMP agent version (SNMP エージェントのパージョン)

設定	説明	工場既定値
V1, V2c, V3, または	スイッチの管理に使用する SNMP プロトコルのバージョンを指定します。	V1, V2c
V1, V2c, または		
V3 only(V3 のみ)		

Admin auth type(管理者認証の種類)(V1, V2c, V3, および V3 のみ)

設定	説明	工場既定値
No Auth (認証なし)	admin アカウントを使用してオブジェクトにアクセスします。認証は ありませ	No Auth
	κ	(認証なし)
MD5	HMAC-MD5 アルゴリズムに基づく認証を提供します。8 文字のパス ワー	
	ドが認証の最低要件です。	
SHA	HMAC-SHA アルゴリズムに基づく認証を提供します。 8 文字のパスワ	
	ードが認証の最低要件です。	

認証用ユーザーネーム:認証タイプが MD5/SHA の場合、SNMP 認証アカウント設定として8つの可能なアカウントの中で1つのみ 設定できます。

Admin private key(管理者プライベートキー) (V1, V2c, V3, および V3 のみ)

設定	説明	工場既定値
Disable(使用しない)	データ暗号化なし	Disable
DES	DES ベースのデータ暗号化	(使用しない)
AES	AES ベースのデータ暗号化	

Private key(プライベートキー)

データ暗号化キーはデータ暗号化の最低要件です(最大 63 文字)。

Private MIB Information Device Object ID (プライベート MIB 情報デバイスオブジェクト ID)

AWK-3131A の企業値を示す固定値で、OID とも呼ばれます。変更できません。

Link Fault Pass-through (リンクフォルトパススルー) (クライ アント/スレーブモー

ドのみ)

この機能は、イーサネットポートのリンクが切断した場合に、無線接続が強制的に切断されることを意味します。イ ーサネットリンク が回復すると、AWK は AP への接続を試みます。

無線が切断すると、AWKのイーサネットポートは自動ネゴシエーションを再開しますが、リンク切断状態は続きます。無線接続が回復 すると、AWK はイーサネットリンクの回復を試みます。

システムログには、元のリンク接続/切断イベントに加えて、リンクフォルトパススルーのイベントも記録されます。

Link Fault Pass-Through (For Client/Slave mode only)

Link Fault Pass-Through

🔍 Enable 🔍 Disable

Submit

Link Fault Pass-Through(リンクフォルトパススルー)

設定	説明	工場既定値
Enable(使用する)	リンクフォルトパススルーを使用します	Disable
Disable(使用しない)	リンクフォルトパススルーを使用しません	(使用しない)

Logs and Notifications(ログと通知)

産業用デバイスはシステムのエンドポイントに配置されることが多いため、ネットワーク内の他の場所で何が起きて いるかを常に認 識できるわけではありません。したがって、無線 AP やクライアントなどを含むこれらのデバイスは、 リアルタイムの警告メッセージ をシステムの保守担当者に提供する機能を備えている必要があります。これにより、た とえシステム管理者が制御室を長期間離れ ていても、例外が発生した場合にはデバイスのステータスが直ちに管理者に 通知されるようにできます。

AWK-3131A は、これらのイベントを記録するだけでなく、SNMP トラップ、E メール、リレー出力など、エンジニア に自動警告する様 々な方式に対応しています。また 2 つのデジタル入力に対応し、センサーをシステムに統合して E メ ールやリレー出力による警 告を自動的に発生させます。

System Logs(システムログ)

System Log Event Types (システムログイベントタイプ)

グループ分けされたイベントの詳細情報を以下の表に示します。「Enable logging」(ログを使用する)ボックスを チェックすると、その グループのイベントが有効になります。デフォルトではすべて有効になっています(チェックが 付いています)。システムイベントのロ グは、「Status」(ステータス)→「System Logs」(システムロ グ)を選択すると表示されます。

System Log Event Types

Event Type En	nable Logging
System-related events	Active
Network-related events	Active
Configuration-related events	Active
Power events	Active
DI events	Active

Submit

System-related events(システム関連イ ベント)	以下の場合にイベントをトリガ
System warm start	設定(IP アドレス、サブネットマスクなど)を変更したときなど、 AWK-3131A を
(システムのウォームスタート)	再起動した場合
システムのコールドスタート	電源オフから AWK-3131A を再起動した場合
ウオッチドッグトリガー再起動	ウオッチドッグにより AWK-3131A を再起動した場合
Network-related events(ネットワーク 関連イベン	以下の場合にイベントをトリガ
Network-related events(ネットワーク 関連イベント)	以下の場合にイベントをトリガ
Network-related events(ネットワーク 関連イベント) LAN リンク接続	以下の場合にイベントをトリガ LAN ポートがデバイスまたはネットワークに接続された場合
Network-related events(ネットワーク 関連イベント) LAN リンク接続 LAN リンク切断	以下の場合にイベントをトリガ LAN ポートがデバイスまたはネットワークに接続された場合 ケーブルが外れていたり、相手のデバイスがシャットダウンしたりし て、ポート

	-
クライアントの接続/解除 (AP/マスタモード	無線クライアントが接続、あるいは切断された場合
WLAN の AP への接続(クライアント/スレーブモ	AWK-3131A が AP に接続した場合
- F)	
WLAN の切断(クライアント/スレーブモード)	AWK-3131A と AP が切断した場合
RSTP 変更	RSTP のトポロジーが変わった場合
RSTP 新ルートブリッジ ID	RSTP のルートブリッジ ID が変わった場合
以前の AP から現在の AP へのクライアントローミ	信号強度が以前の AP より現在の AP の方がある値以上大きくなって旧 AP か
ング (クライアント/スレーブモード)	ら現在の AP にクライアントが変わる場合
IP アドレスの競合	AWK-3131A が同じサブネットにつながる別のデバイスと同じ IP アドレスを持つ
	場合
WLAN / LAN がアップしたのでリンク障害パススル	WLAN/LAN リンクがアップして Link fault pass-through (LFPT)が LAN/WLAN
—LAN / WLAN が接続された	機能を有効にした場合
WLAN / LAN がダウンしたのでリンク障害パスス	WLAN/LAN リンクがダウンして Link fault pass-through (LFPT) が
ルーLAN / WLAN が接続断された	LAN/WLAN 機能を無効にした場合
DFS 周波数越えのチャンネル可用性チェック	チャンネル可用性チェック(channel availability check (CAC))が始まった時(チャ
(AP/マスターモード)	ンネル[channel] 、周波数[frequency] GHz で 60 秒/)
	チャンネル可用性チェック(channel availability check (CAC))タスクが完了した
	時(チャンネル [channel]、周波数[frequency] GHz./)
	レーダ信号が検出された時 [channel]、[frequency] GHz)
AeroLink protection (エアロリンクプロテクション)	AeroLink protection 状態が変わった時
状態	AeroLink 状態: Initialize (init)/Discovery/Idle/Negotiation (nego) Back
	up/Active/Changed/Undefined (undef)
	AeroLink detection メソッド: SNR/信号強度/切断
Config-related events(設定関連イベント)	以下の場合にイベントをトリガ
設定変更	設定項目が変更された場合
Web コンソールを介した設定ファイルのイン ポー	設定ファイルが AWK-3131A にインポートされた場合
+	
コンソール認証エラー	不正なパスワードが入力された場合
ファームウェア更新完了	AWK-3131A のファームウェアが更新された場合
ABC-01 から設定をロード	ABC-01 からの設定のロードが成功した場合/エラーの場合
ABC-01 に設定を保存	ABC-01 への設定の保存が成功した場合/エラーの場合
ABC-01 エラー	AWK-3131A がコンソールポートから ABC-01 を検出できない場合
設定をデフォルトにリセット	設定を工場既定値に戻す場合
Power events(電源イベント)	以下の場合にイベントをトリガ
電源 1/2 変位(オン→オフ)	AWK -3131A の電源が PWR1/2 でオフになった場合
PoE 変位(オン→オフ)	AWK -3131A の電源が PoE でオフになった場合
電源 1/2 変位(オフ→オン)	PWR1/2 を介して AWK -3131A の電源がオンになった場合
PoE 変位(オフ→オン)	PoE を介して AWK-3131A の電源がオンになった場合

Syslog

この機能は Syslog サーバのイベントログを提供します。最大 3 つまでの Syslog サーバと Syslog サーバの UDP ポ 一ト番号を 設定できます。イベントが発生すると、そのイベントが Syslog UDP パケットとして指定の Syslog サーバ に送信されます。.

Syslog Event Types (Syslog イベントタイプ)

グループ分けされたイベントの詳細情報を以下の表に示します。「Enable logging」(ログを使用する)ボックスを チェックすると、その グループのイベントが有効になります。デフォルトではすべて有効になっています(チェックが 付いています)。各イベントグループの 詳細は、3-31 ページの「System Log Event Types(システムログイ ベントタイプ)」の表に掲載されています。 Syslog Event Types

Event Type	Enable Logging
System-related events	✓ Active
Network-related events	✓ Active
Configuration-related events	✓ Active
Power events	✓ Active
DI events	Active
RSSI report events	Active

Submit

Syslog Server Settings

You can configure the parameters for your Syslog servers in this page.

Syslog port	514	
Syslog server 3		
Syslog port	514	
Syslog server 2		
Syslog port	514	
Syslog server 1		

Submit

Syslog server 1/2/3

設定	説明	工場既定値
IP address(IP アドレス)	1/2/3 台目の Syslog サーバの IP アドレスを入力します	なし

Syslog port

設定	説明	工場既定値
ポートの送信先 (1~	対応する Syslog サーバの UDP ポートを入力します	514
65535)		

NOTE RSSI report events(RSSI レポートイベント)(クライアントモードのみ)はサイト調査段階に適しており、RSSI を表として描くために特別なユーティリティを必要とします。ただし、この機能を使用するとトラフィック負荷が増大するため、通常はこの機能を「disable」(使用しない)に設定することをお勧めします。

E-mail Notifications (Eメール通知)

Notification Event Types(通知イベントタイプ)

イベント項目を有効にするには、その項目の「Active」(アクティブ)ボックスをチェックします。デフォルトではす べて無効になっていま す(チェックが付いていません)。各イベント項目の詳細はシステムログセクションにあります。

Notification Event Types

Event Type	Enable Notification
Cold start	Active
Warm start	C Active
Power 1 transition (On>Off)	C Active
Power 1 transition (Off>On)	C Active
Power 2 transition (On>Off)	C Active
Power 2 transition (Off>On)	C Active
PoE transition (On>Off)	C Active
PoE transition (Off>On)	C Active
Configuration changed	C Active
Console authentication failure	C Active
DI 1 transition (On>Off)	C Active
DI 1 transition (Off>On)	C Active
DI 2 transition (On>Off)	Active
DI 2 transition (Off>On)	C Active
LAN link on	C Active
LAN link off	C Active

Submit

E-mail Conver Cottings

E-mail Server Settings(Eメールサーバ設定)

AWK-3131A から警告メールを受信するメールアドレスを最大4つまで設定できます。以下のパラメータは、「E-mail Server Settings」 (Eメールサーバ設定)ページで設定できます。また、「Send Test Mail」(テストメールの送信)ボタンを使用すれば、メールサーバや Eメールアドレスが正常に機能しているかどうかをテストできます。これらのパラメータの詳しい説明は図の下にあります。

E-man server settings	
Mail server (SMTP)	
User name	
Password	
From e-mail address	
To e-mail address 1	
To e-mail address 2	
To e-mail address 3	
To e-mail address 4	
Submit Send Test Mail	

メモ	

AWK-3131A は、ファームウェア V1.6 では Google や Yahoo SMTP サーバーサービスをサポートしていません。

Mail server (SMTP)(メールサーバ) (SMTP)

Setting	説明	工場既定値
IP address(IP アドレス)	E メールサーバの IP アドレス。	なし

User name (ユーザー名)と Password (パスワード)

設定	説明	工場既定値
	SMTP サーバで使用されるユーザー名とパスワード	なし

From e-mail address(送信者 Eメールアドレス)

設定	説明	工場既定値
最大 63 文字	警告メールの「From」(送信者)フィールドに表示される管理者の E メールア	なし
	ドレスを入力します。	

To E-mail address 1/2/3/4 (受信者 Eメールアドレス 1/2/3/4)

設定	説明	工場既定値
最大 63 文字	受信者の E メールアドレスを入力します。	なし

リレー

AWK-3131A の上部パネルには、2 つの端子ブロック接点から構成されているリレー出力が1つあります。これらのリレー接点は、ユ ーザー設定イベントやシステムエラーを示すために使用されます。

ユーザー設定イベントがトリガされると、リレー接点に接続された2本の配線が開回路を形成します。ユーザー設定イベントが発生 していない場合は、リレー回路は閉じたままです。安全上の理由から、AWK-3131Aの電源が入っていないときには、リレー回路は 開いたままになっています。

Relay Event Types(リレーイベントタイプ)

イベント項目を有効にするには、その項目の「Active」(アクティブ)ボックスをチェックします。デフォルトではすべて無効になっています(チェックが付いていません)。各イベント項目の詳細はシステムログセクションにあります。

Relay Event Types

Event Type	Enable Notification
Power 1 transition (On>Off)	Active
Power 2 transition (On>Off)	C Active
DI 1 transition (On>Off)	C Active
DI 1 transition (Off>On)	C Active
DI 2 transition (On>Off)	C Active
DI 2 transition (Off>On)	C Active
LAN link on	Active
LAN link off	Active

Submit

Trap(トラップ)

トラップは管理ステーションに異常な状態を知らせるために使用できます。このトラップでトリガされる通知により、ネットワークの効率 を向上させることができます。

管理ステーションは通常、大量のオブジェクトを備えた多数のデバイスを管理するので、すべてのデバイス上のすべてのオブジェクト に対してクエリのためにポーリングまたは要求の送信を行うことは、管理ステーションにとって大きな負担になります。管理対象デバ イスのエージェントがメッセージ(つまりトラップ)を送信してイベントを管理ステー ションに通知するほうが効率的です。

Trap Event Types(トラップイベントの種類)

Trap Event Types

Event Type	Enable Notification
Cold start	Active
Warm start	Active
Power 1 transition (On>Off)	Active
Power 1 transition (Off>On)	Active
Power 2 transition (On>Off)	Active
Power 2 transition (Off>On)	Active
PoE transition (On>Off)	Active
PoE transition (Off>On)	Active
Configuration changed	Active
Console authentication failure	Active
DI 1 transition (On>Off)	Active
DI 1 transition (Off>On)	Active
DI 2 transition (On>Off)	Active
DI 2 transition (Off>On)	Active
LAN link on	Active
LAN link off	Active

Submit

SNMP Trap Receiver Settings (SMTP トラップ受信者設定)

SNMP トラップは、SMIv1 MIB (SNMPv1)と SMIv2 MIB (SNMPv2c)で定義されます。 この 2 つの形式は基本的に同等で、相互に変換 可能です。Web ページを使って SNMP トラップ受信者のパラメータを設定できます。

SNMP Trap Receiver Settings	
1st trap version	V1 V
1st trap server IP/name	V1
1st trap community	alert
2nd trap version	V1 V
2nd trap server IP/name	
2nd trap community	alert

Submit

1st / 2nd trap version

設定	説明	工場既定値
V1	SNMPv1 で定義される SMTP トラップ	V1
V2	SNMPv2 で定義される SMTP トラップ	

1st / 2nd trap server IP/name

設定	説明	工場既定値
IP アドレスまたはホスト名	ネットワークで使用されるトラップサーバの IP アドレスまたは名前を入力し	None
	ます。	

1st / 2nd trap community

設定	説明	工場既定値
最大 31 文字	最大 31 文字のコミュニティストリングの照合を認証に使用します	Alert(警報)

Status(ステータス)

Wireless LAN Status (無線 LAN ステータス)

「Wireless LAN Status」(無線 LAN ステータス)ページには、動作モードやチャンネルなどの「802.11 Information」(802.11 情報)関連 パラメータのステータスが表示されます。「Auto Update」(自動更新)ボックスをチェックすると、ステータスが5秒ごとに更新されま す。

「802.11 Information」(802.11 情報)の一部の値は、選択した動作モードによっては表示されない場合があります。たとえば AP モード では、「Current BSSID」(現在の BSSID)、「Signal strength」(信号強度)、および「SNR」(信号雑音比)パラメータは使用できません。

このページで絶えず更新される「Signal strength」(信号強度)、「Noise floor」(ノイズフロア)、「SNR」(信号雑音比)などの情報は、ク ライアントモードの AWK-3131A の信号強度を監視するのに便利です。

Wireless LAN Status

🗹 Auto Update

Show status of WLAN (SSID: MOXA) V

802.11 Information	
Operation mode	AP
Channel	6
Channel width	N/A
RF type	B/G/N Mixed
SSID	MOXA
MAC	06:90:E8:11:22:33
Security mode	OPEN
Current BSSID	06:90:E8:11:22:33
Signal strength	N/A
Signal strength	-95 dBm
Noise floor	-95 dBm
SNR	N/A
Transmission Information	
Rate	Auto
Power	20 dBm
Outgoing Packets	
Total sent	2298
Packets with errors	0
Packets dropped	46662
Incoming Packets	
Total received	1391
Packets with errors	0
Packets dropped	0

Associated Client List(関連付けられたクライアントリスト) (AP/マスタモードのみ)

「Associated Client List」(関連付けられたクライアントリスト)には、特定の AWK-3131A に現在関連付けられている すべてのクライ アントが表示されます。このページには、次のようなネットワークの診断に役立つ情報が表示されます。

「MAC Address」(MAC アドレス): 関連付けられているクライアントの MAC アドレスが表示されます。この AP/ マスタで DHCP サーバが有効になっている場合は、IP アドレスも表示されます。

「Connection Duration」(接続時間): クライアントがどれだけの時間この AP/マスタに接続されているかが表示 されます。

「SNR」: 関連付けられたクライアントの信号雑音比(SN 比)が表示されます。この情報は特に、全体的な無線パフ ォーマンスを低下させる可能性がある信号の弱いクライアントを特定するのに役立ちます。

「Tx(Bytes/Pkts)」(Tx(パイト数/パケット数)): クライアントが関連付けられた後の AP からクライアント へのトラフィックが記録されます。

「Rx(Bytes/Pkts)」(Rx(パイト数/パケット数)): クライアントが関連付けられた後のクライアントから AP へのトラフィックが記録され ます。

Associat	ed Client List						
Show clie	ents for WLAN (SSID: u) V						
No.	MAC Address	Connection Duration	SNR	Signal Strength	Tx (Bytes)	Tx (Pkts)	Rx (Bytes)
1	00:90:e8:00:05:6e (192.168.127.254)	1 days 01h:12m:38s	53	-40	545091	631	59966
Refresh							

DHCP Client List(DHCP クライアントリスト)(AP モードのみ)

「DHCP Client List」(DHCP クライアントリスト)には、IP の割り当てを必要とし、IP の割り当てに成功したす べてのクライアントが表示されます。「Refresh」(更新)ボタンをクリックすると、リストを更新できます。

DHCP Client List

	MAC	IP
1.	01:5C:96:9D:29:77:71	192.168.41.229
2.	01:30:10:B3:72:72:7F	192.168.41.142
3.	01:9C:4E:36:A6:98:08	192.168.41.216
4.	01:B4:CE:F6:4E:CB:3C	192.168.41.146
5.	01:90:B6:86:75:A5:28	192.168.41.184
6.	01:8C:70:5A:49:FF:58	192.168.41.127
7.	01:68:09:27:CD:41:43	192.168.41.143
8.	01:5C:C5:D4:75:50:7B	192.168.41.140
9.	01:84:3A:4B:39:B7:5C	192.168.41.181
10.	01:A4:C3:61:03:F0:E2	192.168.41.137
11.	* 192.168.41.226	
12.	01:80:86:F2:B2:65:1F	192.168.41.222
13.	01:34:4D:F7:3A:23:FB	192.168.41.122
14.	01:30:75:12:A7:15:0E	192.168.41.139
15.	01:EC:85:2F:88:B3:6A	192.168.41.213
16.	01:30:75:12:F2:59:F9	192.168.41.125
17.	01:78:6C:1C:BF:51:0E	192.168.41.144
18.	01:AC:81:12:59:66:2F	192.168.41.156

Select All Refresh

「Select all」(すべて選択)ボタンを押すと、リストのすべての内容を選択して編集できます.



System Logs(システムログ)

トリガされたイベントはシステムログに記録されます。「Export Log」(ログのエクスポート)をクリックする と、使用可能なビューアにロ グの内容をエクスポートできます。「Clear Log」(ログのクリア)ボタンを使うとログ の内容をクリアでき、「Refresh」(更新)ボタンを使う とログを更新できます。

System Logs

_		
(9	33) 2015/05/28,04h:12m:54s System warm start, restarted by console	*
(9	34) 2015/05/28,04h:19m:19s LAN link off	
(9	35) 2015/05/28,04h:19m:21s LAN link on	
(9	36) 2015/05/28,07h:45m:59s Configuration changed	
(9	37) 2015/05/28,07h:46m:23s Power 1 transition (Off -> On)	
(9	38) 2015/05/28,07h:46m:29s LAN link on	
(9	39) 2015/05/28,07h:46m:34s System warm start, restarted by console	
(9	00) 2015/05/28,08h:14m:07s LAN link off	
(9	91) 2015/05/28,08h:14m:09s LAN link on	
(9	92) 2015/05/28,08h:21m:55s Configuration changed	
(9	03) 2015/05/28,08h:22m:20s Power 1 transition (Off -> On)	
(9	04) 2015/05/28,08h:22m:26s WLAN disconnected, connect time(0sec), (reason 0)	
(9	95) 2015/05/28,08h:22m:26s LAN link on	
(9	06) 2015/05/28,08h:22m:29s System warm start, restarted by console	
(9	07) 2015/05/28,08h:24m:24s Configuration changed	
(9	98) 2015/05/28,08h:24m:49s Power 1 transition (Off -> On)	
(9	99) 2015/05/28,08h:24m:55s LAN link on	
(10	00) 2015/05/28,08h:24m:59s System warm start, restarted by console	-
		Ŧ
		-//
=		

Export Log Clear Log Refresh

Relay Status (リレーステータス)

ユーザー設定可能なイベントのステータスは、「Relay Status」(リレーステータス)の下に表示されます。「Auto refresh」(自動更新) ボックスをチェックすると、ステータスが 5 秒ごとに更新されます。

イベントがトリガされると、このリストに記録されます。システム管理者は、イベントを確認して処理を終えたら、「Acknowledge Event」 (イベント確認)をクリックできます。

Relay Status

🗹 Auto Update	
Relay Status	
Power 1 transition (On>Off)	 Acknowledge Event
Power 2 transition (On>Off)	 Acknowledge Event
DI 1 transition (On>Off)	 Acknowledge Event
DI 1 transition (Off>On)	 Acknowledge Event
DI 2 transition (On>Off)	 Acknowledge Event
DI 2 transition (Off>On)	 Acknowledge Event
LAN link on	 Acknowledge Event
LAN link off	 Acknowledge Event

DI and Power Status (DI および電源ステータス)

この Web ページには、電源入力とデジタル入力のステータスが表示されます。「Auto refresh」(自動更新)ボッ クスをチェックすると、 ステータスが 5 秒ごとに更新されます。

DI and Power Status

🗹 Auto Update				
Input Status	On / Off			
Power 1 status	On			
Power 2 status	Off			
PoE status	Off			
DI 1 status	Off			
DI 2 status	Off			

AeroLink Protection Status (AeroLink Protection のステータス) (クライアント/スレーブモードのみ)

「Advanced WLAN Setup」(高度WLANセットアップ)パネルでエアロリンク保護を有効にすると、エアロリンク保護の現在の状態が簡易診断のために表示されます。

AeroLink Protection Status

🗹 Auto Update	
AeroLink Protection Status	
Current state	N/A (Init/Discover/Idle/Nego/Backup/Active/Change)
Detection method	N/A (SNR/Signal Strength/Disconnection)

AeroLink Protection グループのメンバーのステータスは、以下の7つのいずれかになります。

- 「Initiation State(Init)」(開始状態(Init)): AeroLink Protection Protocol を開始します。
- 「Discovering State」(検出状態 (Discover)): これからネゴシエーションする他の AeroLink Protection メンバーを検出します。
- 「Idle State(Idle)」(アイドル状態(Idle)): 内部プロトコルのチェックポイント
- 「Negotiation State (Nego)」(ネゴシエーション状態(Nego)): 他の AeroLink Protection メンバーと ネゴシエーションし、アクティブノードを選出します。
- 「Backup State(Backup)」(バックアップ状態(Backup)): ネゴシエーション後、このノードがバック アップノードとして割り当てられます。代わりにすべてのトラフィックはアクティブノードを通過します。
- **メモ**ノードがバックアップ状態になると、「STATE」(状態) LED が点滅します。
 - 「Active State(Active)」(アクティブ状態(Active)): ネゴシエーション後、このノードがアクティブ ノードとして割り当てられるため、 トラフィックはこのノードを通過します。
 - 「Role Change State(Change)」(役割変更状態(Change)): アクティブノードが WLAN を介してデ ータを送信できなくなると、 「Change」状態に変化し、バックアップノードからアクティブノードの再ネゴシ エーションをトリガします。

エアロリンク保護機能は以下の検出方法の1つに適用できます。

- SNR(信号雑音比): 関連クライアントの Signal-Noise Ratio (SNR)をチェックする
- Signal Strength(信号強度): 関連クライアントの信号強度をチェックする
- Disconnection(切断): 切断を検出する

System Status (システムステータス)

システムステータスのセクションには、現在のデバイスのメモリと CPU の使用率のステータスが表示されます。

Web コンソール設定

メモ CPU に負荷がかかりすぎると、ウォッチドッグによりトリガされるシステムの再起動が起きる可能性があります。ファイヤーウォール ルール(IP/MAC/プロトコルフィルタ)やトラフィック PPS(パケット数/秒)が多いと、CPU 使用率が上昇します。

System	System Status			
Memor	y Info			
Total	(kB)	126724		
Used	(kB)	48604		
Free	(kB)	78120		
CPU Info				
Usage	(%)	4.33		

Refresh

Network Status(ネットワークステータス)

ネットワークステータスのセクションには、デバイスの ARP、ブリッジステータス、LLDP、RSTP、ルーティングテーブ ルに関するネッ トワークステータスが表示されます。

ARP Table (ARP テーブル)

ARP(Address Resolution Protocol)テーブルには、デバイスの現在のアドレスマッピング(IP から MAC への)が表示されます。

ARP Table		
IP Address	MAC Address	
192.168.127.18	F0:DE:F1:DD:A1:ED	

Refresh

Bridge Status (ブリッジステータス)

デバイスのネットワークブリッジの現在のステータスが表示されます。このセクションに表示される各インターフェイスおよび対応する MAC アドレスは、流入トラフィックのエントリポイントです。

Brid	ge St	tatus
------	-------	-------

Interface	MAC Address
LAN	00:90:E8:22:B1:D9
ath01	00:90:E8:4E:9A:79
LAN	F0:DE:F1:DD:A1:ED

Refresh

LLDP Status (LLDP ステータス)

LLDP (Link Layer Discovery Protocol)を通じて収集された隣接するデバイスに関する情報が表示されます。

Interface		Neighbor Information						
Interface	System Name	ID	IP	Port	Port Description			
LAN	AWK-3121_13496	00:90:E8:22:B1:D9 (MAC)	192.168.127.253	7 (LOCAL)	LAN			
WLAN	AWK-3121_0777	00:90:E8:4E:9A:79 (MAC)	192.168.127.252	10 (LOCAL)	WLAN			

メモ

AWK-3131A の LLDP 機能は、IEEE 802.3 をサポートしていません。

Routing Table(ルーティングテーブル)

現在のデバイスのルーティング情報が表示されます。

Routing Table			
Destination	Gateway	Mask	Interface
192.168.127.0	*	255.255.255.0	*
default	192.168.127.251	0.0.0.0	*
Refresh			

RSTP Status (RSTP ステータス)

設定されたスパニングツリープロトコルパラメータを表示します。

RSTP Status					
RSTP status					
Bridge priority	3276	58			
Hello time	2 seconds				
Forwarding delay	y 15 seconds				
Max age	20 s	econds			
No	Enable RSTP	Port Priority	Port Cost	Edge Port	Status

メンテナンス

メンテナンス機能として、AWK-3131Aと有線/無線ネットワークを管理するためのツールが管理者に提供されています。

Console Settings(コンソール設定)

HTTP、HTTPS、Telnet、SSH 接続のコンソールへのアクセス許可を有効または無効にできます。安全のために、2 つの 安全なコン ソール、HTTPS と SSH へのアクセスのみを許可するようお勧めします。

Console Settings				
Auto logout period	10 (1 to 60 minutes)			
Accessible Interfaces				
Interface	нттр	HTTPS	Telnet	
Enable services				
Ethernet		v	v	
WLAN				
* If you disable all access portals, you will not be able to remotely access this device * If you disable HTTPS, some Moxa service features will be disabled.	3.			
Accessible Net List				
Accessible Net List	🔍 Enable 🖲 Disable			
Submit				

Ping(ピング)

「Ping」(ピング)は有線または無線ネットワークの整合性の診断に役立ちます。「Destination」(送信先)の欄に ノードの IP アドレスを 入力すれば、ping コマンドを使って、ノードの存在を確認して、アクセスパスが有効かどうか を検出できます。

Ping		
Destination	192.168.41.233	
Ping		
ノードとアクセスパスが有効な場合は	は、すべてのパケットが損失なく問題なく送信されたことが表示され	ます。
有効ではない場合、以下の図のよう	に、一部または全部のパケットが失われることがあります。	
Ping		
Destination		
Ping		
PING 192.168.41.233 (192.)	168.41.233): 56 data bytes	
64 bytes from 192.168.41.23	33: seq=1 ttl=64 time=0.548 ms	
64 bytes from 192.168.41.23	33: seq=2 ttl=64 time=0.565 ms	
04 bytes from 192.108.41.23	55: seq=5 tu=04 time=0.507 ms	
192.168.41.233 ping stat	istics	
4 packets transmitted, 4 pack round-trip min/avg/max = 0	(ets received, 0% packet loss 1.548/0.594/0.696 ms	

Firmware Upgrade(ファームウェアの更新)

AWK-3131A のファームウェアを更新することで、付加価値の高い機能を追加できます。最新のファームウェアは Moxa のダウンロ ードセンターから入手できます。

ファームウェアの更新を実行する前に、AWK-3131A がオフラインになっていることを確認してください。「Browse」(参照)ボタンをク リックしてファームウェアのイメージファイルを指定し、「Firmware Upgrade and Restart」(ファームウェアを更新して再起動する)をクリ ックすると、ファームウェアの更新が開始します。進捗バーが 100%に達すると、AWK-3131A が自動的に再起動します。

ファームウェアの更新中は、AWK-3131A の他の機能は使用できません。

Firmware Upgrade			
Select firmware file		Browse	
Firmware Upgrade and Restart]		

注意 ファームウェアを更新する時は電源が安定していることを確認してください。予期しない電源断は故障の原因になります。

ファームウェア更新は現在のローミング設定を変える可能性があります。リブート後にデバイスのローミング設定をチェックしてください。

Configuration Import and Export(設定のインポート/エクスポート)

「Configuration Import & Export」(設定のインポート/エクスポート)を使えば、AWK-3131A の設定を簡単に バックアップまたは復元 できます。 「Configuration Import」(設定のインポート)セクションで「Browse」(参照)をクリックし、設定ファイルを指定して「Import Configuration」 (設定をインポート)ボタンをクリックすると、設定のインポートが開始されます。

Configuration Import & Export	
Configuration Import	
Select configuration file	Select file

Import Configuration

「Configuration Export」(設定のエクスポート)セクションで「Export Configuration」(設定をエクスポート)ボタンをクリックして、ローカ ルのストレージメディアに設定ファイルを保存します。設定ファイルはテキストファイルなので、一般的なテキスト編集ツールで表示し たり編集することができます。

Configuration Export

Export Configuration

「Config Import Export」(設定のインポートエクスポート)を使えば、ABC-01の設定もバックアップしたりリストアしたりできます。

ABC-01 Import

Import Configuration

ABC-01 Export

Export Configuration

「SNMP MIB File EXPORT」(SNMP MIB ファイルのエクスポート)を使えば、SNMP MIB ファイルも利用できます。

SNMP MIB File Export

Export MIB

設定を AWK にダウンロードするには、以下の手順に従います。

1. AWK の電源を切ります。

2. ABC-01 を AWK の RS-232 コンソールに接続します。

3. AWK の電源を入れます。

- 4. AWK が起動プロセス中にABC-01 を検出し、自動的にABC-01から AWK へ設定をダウンロードします。設定のダウ ンロードが 完了し、その設定の形式が正しい場合、AWK は短いビープ音を3回鳴らし、起動プロセスを続行します。
- 5. AWK の起動が正常に完了すると、通常どおりビープ音が 2 回鳴り、AWK が使用可能であることを示す LED が緑一色に点灯します。

Load Factory Default(初期値のロード)

この機能を使えば、AWK-3131A をリセットしたり、設定をすべて初期値に戻すことができます。AWK-3131A の 上部パネルのリセッ トボタンを押してハードウェアをリセットすることもできます。

Load Factory Default

Reset to Factory Default

Click "System Reset" to reset all settings, including the console password, to the factory default values.

The system will be restarted immediately.

System Reset

Account Settings(アカウント設定)

リモートサイトにあるデバイスがハッカーから安全であることを確実にするために、初めてデバイスを設定する時には高強度のパスワ ードを推奨します。

Password Policy

Minimum password length	4	(4 - 16 characters)
Password strength check	Disable	•
Password validity	90	(0 - 365 days, 0 is disable)
Password retry count	5	(0 - 10, 0 is disable)
Lockout time	600	(60 - 3600 seconds)

Account List

No.	Active	Account Name	User Level	HTTP/HTTPS	Telnet/SSH /Console	Moxa Services	Diagnostics	Action
1	v	admin	Admin 👻					Edit Delete
2			Admin 💌					Edit Delete
3			Admin User					Edit Delete
4			Admin 🔻					Edit Delete
5			Admin 👻					Edit Delete
6			Admin 🔻				V	Edit Delete
7			Admin 👻					Edit Delete
8			Admin 👻		\checkmark			Edit Delete

* Only characters allowed in the Account Name are alphabets, numerals, at sign (@), period (.), and underscore(_).

Field	説明	Default 設定
Minimum password	デフォルトの設定では、パスワード長は4文字~16文字の間です。セキュリテ	4
length	ィを改善するため、初めてデバイスを設定する時に最小パスワード長を少なくと	
(最小パスワード長)	も8文字にすることを推奨します。	
Password strength	パスワード強度チェックオプションを有効にすると、ユーザーは高強度のパスワ	使用しない
check	ードの選択を必ず求められます。	
(パスワード強度チェッ	注意:詳細は次の「パスワード変更」のセクションを見てください。	
ク)		
Password validity	パスワードを変更しなければならなくなるまでの日数。 パスワードはハッカー	90 日
(パスワード有効性)	から保護するために定期的に更新されるべきです。	
Password retry count	ログイン中にユーザーが誤ったパスワードを入力して、デバイスのログイン機	5
(パスワードリトライ回	能がロックされるまでの連続回数。	
数)		
Lockout time	n回連続して失敗したログインの試行後、デバイスのログイン機能がロックされ	600 秒
(ロックアウト時間)	る秒数。ここで、n はパスワードの再試行回数です。	

新しいユーザーアカウントの登録や既存のアカウントを編集するには、「Edit」をクリックします。

以下の項目が設定できます。
Account Settings

Active	Enable 🔻	
User level	Admin 👻	
Account name	admin	(A-Z, a-z, 0-9, '@', '.', and '_')
New Password	••••	
Confirm Password		
 Your password must follow the password policy. The minimum password length is 4 characters. 		
Accessible Access Portal		

HTTP/HTTPS	Enable	Disable
Telnet/SSH/Console	Enable	Disable
Moxa Service	Enable	Disable
Diagnostic	Enable	Oisable

Field	説明	Default 設定
Active	ユーザーアカウントを有効にするには「Enable」を選択します	Disable(使用しない)
(アクティブ)		
User level	Administrator(アドミニストレータ:管理者):ユーザーに Web UI へのアクセスを	Admin(管理者)
(ユーザーレベル)	許可したり、デバイスの設定を変更したり、デバイスへのインポート/エクスポートの機能を使ったりします。 User(ユーザー): ユーザーに Web UI へのアクセスを許可しますが、ユーザー はデバイスの設定やデバイスのインポート/エクスポートの機能を使うことはで きません。	
Account name (アカウント名)	アカウントのユーザー名	Admin(管理者)
New Password (新パスワード)	デバイスにログインするために使われるパスワードです。	Moxa
Confirm Password (パスワード確認)	パスワードを再入力します。新パスワードとパスワードの確認入力が合わない 場合、パスワードを再度入力することが求められます。	N/A(対象外)

パスワードの変更

「Change Password」(パスワードの変更)機能を使って既存ユーザーのパスワードを変更できます。最初に現在のパスワードを入力し、それから新しいパスワードを「New password」(新パスワード)と「Confirm password」(パスワードの確認)の入力欄に入力します。

NOTE ネットワークの安全を高いレベルに維持するために、デフォルトのパスワード (moxa)は使用しないでください。また、全てのユーザのパスワードは定期的 に変更してください。

Change Password				
Current password	••••			
New password				
Confirm password				

• Your password must follow the password policy.

The minimum password length is 4 characters.

- NOTE 「Password-strength test」(パスワード強度テスト)オプションを使用すると、以下のパスワードポリシーに従ったパスワードを使うこと を促されます。
 - パスワードは少なくとも1文字は数字を含む必要があります。
 0.1.2.…9.
 - パスワードは大文字と小文字の両方を含む必要があります。
 A, B, …, Z, a, b, …, z.
 - パスワードには次の特殊文字を少なくとも1つ使う必要があります。
 [^]!@#\$%^-_:..<) []}
 - 次の特殊文字はパスワードには使えません。
 `' " | : &
 - ファームウェアのバージョン 1.4 から後は、デフォルトのパスワードは「moxa」です。以前の全てのファームウェアのバージョン(1.3 まで)では、デフォルトのパスワードは「root」です。

Always Enable O Disable Factory Reset Function after 60 Seconds.

Misc. Settings(詳細設定)

AWK-3131Aを使いこなす追加の設定がこのページでお使いいただけます。

Misc. Settings

Reset button

Submit

Reset button (リセットボタン)

設定	説明	工場既定値
Always Enable	AWK-3131A のリセットボタンが通常通り使えます。	Always enable
(いつも使う)		(いつも使う)
Disable the Factory Reset	AWK-3131A をリセットしてデフォルトの工場設定にする機能が、	
Function after 60 Seconds	AWK-3131A の再起動終了後 60 秒で効かなくなります。	
(60 秒後に工場リセット機能		
を使わなくする		
)		

Troubleshooting(トラブルシューティング)

この機能を使用すると、現在のシステムのステータスをすばやく取得して、Moxaのエンジニアに診断情報を提供できます。現在の デバイス情報をエクスポートするには、「Export」(エクスポート)をクリックします。

Troubleshooting

Export current device information

Export

Wi-Fi Mirror Port(Wi-Fi ミラーポート)

Wi-Fiミラーポートは、Wi-Fiスニファーをシステム運用環境にセットアップすることが簡単でない場合、現在のチャネル上にあるネット ワークの Wi-Fi 通信のふるまいを知るのに役立ちます。 **Wi-Fi Mirror Port**

Capture Wi-Fi Frames

Remote Capture

	(1~180s)	Capture
Enable	Disable	

Wi-Fi ミラーポートをセットアップするには、Wireshark ツールがインストールされたコンピュータが必要です。これを使って AWK デバイ スにイーサネット経由で接続します。

メモ	Wi−Fi ミラーポートは情報収集に便利です。しかし Wi−Fi ミラーポートを使うと DFS 機能は適め、通常使用時は Wi−Fi ミラーポート機能を使わない設定をお勧めします。	切に動作しないかも	しれません。このた
	Wi-Fiミラーポートをセットアップして短時間のモニタリングを行うには次のことを行って下さし	۱,	
	 「Capture Wi-Fi Frames」ボックスに期間を入力します 1秒~180秒の範囲で値を入れることが出来ます 「Capture」をクリック WEB 上でタイムアウトを待ちます Web ブラウザからレポートをダウンロードすることができます 		
	Wi-Fiミラーホートをセットアップして長時間のモニタリンクを行っては次のことを行って下さい	١ ₀	
	1. 「Wi-Fi Mirror Port」ヘーシー、C「Remote Capture」オフションを「Enable」に変更。 2. お使いのコンピュータ上で Wireshark ツールを起動、「Capture」で「Options」を選択。 3. Wireshark の「Input」タブにて、「 Manage Interfaces」をクリック		
	Wireshark · Capture Interfaces		? ×
	Input Output Options	Traffic	
	> Realtek LISB NIC: Local Ethernet		_
	 Microsoft: Bluetooth Network Connection VMware Virtual Ethernet Adapter: VMware Network Adapter VMnet1 Microsoft: Wi-Fi VMware Virtual Ethernet Adapter: VMware Network Adapter VMnet8 Intel(R) Ethernet Connection I219-V: Public Ethernet 		
	< ☑ Enable promiscuous mode on all interfaces	Manage Inte	> erfaces
	Capture filter for selected interfaces:	▼ Comp	ile BPFs

4. 「Remote Interfaces」をクリックして新しいインターフェイスを追加

- 5. AWK デバイスの情報を入力
 - Port(ポート): 2002
 - Auth(認証) : Null authentication
 - Host(ホスト): 〈AWK IP〉
- 6. 「OK 」をクリック

AirWorks AWK-3131A UM

Local Inter	faces	Pipes	Remote Interfaces		
Show	Host /	Device	JRL		
	rpcap:	//[192.16	58.125.100]:2002/mon0		
+ -	Ľ.,			Rem	note Settings
		k daas nat	cours comoto cottingo		

7. 「Input」を選択 -->「Interface」 -->「rpcap://...:2002/mon0 」

Interfa	ce							Tra	affic		
> Re	altek USB N	IC: Local E	hernet					_			
> Mi	crosoft: Blu	etooth Net	work Co	nnectio	n						
VN	Aware Virtu	al Ethernet	Adapter	VMwa	re Netwo	rk Adap	ter VMne	t1			
Mi	crosoft: Wi	-Fi						_			
VN	Aware Virtu	al Ethernet	Adapter	VMwa	re Netwo	rk Adap	ter VMne	t8			
Int	el(R) Etherr	net Connec	tion 1219	-V: Pub	lic Ethern	net		_			
rp	cap://[192.1	68.125.100]:2002/n	ion0							
rp	cap://[192.1	68.125.100]:2002/n	ion0							
rp	cap://[192.1	68.125.100]:2002/n	ion0							
rp	cap://[192.1	68.125.100]:2002/n	ion0							>
Enabl	cap://[192.1 e promiscuo	68.125.100 us mode on]:2002/n all interfa	ion0 ces					Man	age Interfac	> :es
Enabl	e promiscuo filter for sele	68.125.100 us mode on ected interfa]:2002/n all interfa	ces Enter a	a capture f	filter			Man	age Interfac	> ces BPFs

高度なトラブルシューティングが必要な場合は、Moxa サービスセンターが暗号化されたスクリプトファイルを提供します。スクリプトフ ァイルは、システムに関する追加の詳細情報を取得します

スクリプトを実行するには、「Browse」(参照)を使ってスクリプトファイルを見つけて選択し、以下の詳細を入力してから「Run Script」 (スクリプトを実行)をクリックします。

Troubleshooting	
Current device info	Export
Diagnostics	
Diagnostic script	Browse
Export diagnostic results	● to a file ○ to a TFTP server
TFTP sever IP	
Diagnostic script name	N/A
Last start time	N/A
Last end time	N/A
Diagnostic status	
Diagnostic result	N/A
Run Script Stop Script	

設定	説明
Diagnostic script	「Browse」(参照)ボタンを使って Moxa 診断スクリプトファイルを選択します。
(診断スクリプト)	
Export diagnostic	エクスポート先を以下から選択します。
results	-「to a file」(ファイルへ)
(診断結果のエクスポー	- 「to a TFTP server」(TFTP サーバへ)
F)	
TFTP server IP	TFTP オプションを選択した場合、TFTP サーバの IP アドレスを指定します。
(TFTP サーバの IP)	
Diagnostic script name	スクリプトファイルの名前が表示されます。
(診断スクリプト名)	
Last start time	最後に実行したスクリプトの開始時刻が表示されます。
(最後の開始時間)	
Last end time	最後に実行したスクリプトの終了時刻が表示されます。
(最後の終了時間)	
Diagnostic status	システム診断の進捗状況が表示されます。
(診断ステータス)	
Diagnostic result	システム診断の結果が表示されます。
(診断結果)	 エクスポート失と て[to o flo)(ファイルへ)オプションを深切すると シス テムログが暗号化されてファ
	イルニタムネオートルとして、Wannes(シアール・シオンションを送水すると、システムロンが唱うにそれてシア
	イルに体行されより。ログンノイルの取入りイスは「MD」により。ログンノイルのワイスが「MD」により。
	ノノ イル奴がう 凹と起えると、取り口レンナイルが削除されより。

Save Configuration (設定の保存)

AWK-3131A が設定の変更を揮発性および不揮発性メモリに保存するしくみは以下の図のとおりです。AWK-3131A を シャットダ ウンまたは再起動すると、揮発性メモリに保持されているデータはすべて消えます。AWK-3131A はフラッシュメモリに保存されてい る設定を使用して起動と初期化を行うので、AWK-3131A を再起動 する前に、新しい設定をすべてフラッシュメモリに保存する必 要があります。

したがって「Save Configuration」(設定の保存)機能または「Restart」(再起動)機能のどちらも実行しない場合、新しい変更は機能 しません。



左側のメニューボックスの「Save Configuration」(設定の保存)をクリックすると、以下の画面が表示されます。この時点でフラッシュ メモリの設定を更新する場合は、「Save」(保存)をクリックします。あるいは、他の機能を実行して、設定の保存を後回しにすること もできます。ただし、設定を保存するまでの間、新しい設定変更は不揮発性メモリ内に保持されます。

Save Configuration

After you submit configuration changes, you must save the changes and restart the system to make the changes take effect. Click **Save** to save configuration changes in the system memory. Click **Restart** to activate configuration changes and display the active settings in the web console.

Save

Network Settings After Reboot

Network Info	
LAN IP address	192.168.43.104
LAN subnet mask	255.255.252.0
LAN gateway	192.168.43.254

Restart(再起動)

設定の変更を実行すると、画面の右上で文字列が点滅表示します。すべての変更を行った後、左側のメニューボックスの 「Restart」(再起動)機能をクリックします。2 つの異なる画面のいずれかが表示されます。

最近設定を変更して、まだ保存していない場合は、2 つのオプションが表示されます。ここで「Restart」(再起動)ボタ ンをクリックす ると、AWK-3131A が直接再起動し、設定の変更はすべて無視されます。「Save and Restart」(保存 して再起動する)ボタンをクリ ックすると、すべての設定の変更が適用されてから、AWK-3131A が再起動します。

Restart

!!! Warning !!!

Click "Restart" to discard configuration changes and restart the system.

Click "Save and Restart" to save configuration changes and restart the system.

Restart Save and Restart

Network Settings After Reboot

Network Info	
LAN IP address	192.168.43.104
LAN subnet mask	255.255.252.0
LAN gateway	192.168.43.254

設定を変更せずに、またはすべての変更を保存してから「Restart」(再起動)機能を実行した場合、画面には「Restart」(再起動) ボタンしか表示されません。

Restart

!!! Warning !!!

The system will restart immediately after you click "Restart". All Ethernet connections will be disconnected.

Restart

Network Settings After Reboot

Network Info		
LAN IP address	192.168.43.104	
LAN subnet mask	255.255.252.0	
LAN gateway	192.168.43.254	

システムの再起動中は、AWK-3131A の機能はすべて実行できません。

Logout(ログアウト)

「Logout」(ログアウト)は、現在の HTTP または HTTPS セッションを切断して「Login」(ログイン)ページに戻 るのに役立ちます。 安全のため、ログアウトしてからコンソールマネージャを終了するようにお勧めします。

Logout

Click Logout to log out of the web console.

Logout

4

ソフトウェアのインストールと設定

この章の内容は以下のとおりです:

- □ 概要エラー!参照元が見つかりません。
- Wireless Search Utility
 - ▶ Wireless Search Utility のインストール
 - ▶ Wireless Search Utility の設定

概要

Wireless Search Utility は Moxa の Web サイト(www.moxa.com) からダウンロードできます。

Wireless Search Utility

Wireless Search Utility のインストール

Wireless Search Utility をダウンロードしたら、セットアッププログラムのファイルを実行してインストールを開始します。

1. 「Welcome」(歓迎)の画面が開いたら「Next」(次へ)をクリックしてインストールを続行します。



2. 「Next」(次へ)をクリックしてプログラムファイルをデフォルトのディレクトリにインストールするか、「Browse」(参照)をクリックして 別の場所を選択します。

📴 Setup - Wireless Search Utility
Select Destination Location Where should Wireless Search Utility be installed?
Setup will install Wireless Search Utility into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\Moxa\Wireless\Wireless Search Utility Browse
At least 3.2 MB of free disk space is required.
< Back Next > Cancel

3. 「Next」(次へ)をクリックしてプログラムのショートカットファイルをデフォルトのディレクトリに作成するか、「Browse」(参照)をクリックして別の場所を選択します。

😼 Setup - Wireless Search Utility 📃 🔍 🔀
Select Start Menu Folder Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Moxa\Wireless\Wireless Search Utility Browse
< Back Next > Cancel

4. 「Next」(次へ)をクリックして付加的なタスクを選択します。

🔂 Setup - Wireless Search Utility	
Select Additional Tasks Which additional tasks should be performed?	3
Select the additional tasks you would like Setup to perform while installing Wireless Search Utility, then dick Next.	
Additional icons:	
Create a desktop icon	
Create a Quick Launch icon	
< Back Next > Cancel	

5. 「Next」(次へ)をクリックして、インストールを続行します。インストーラがインストールオプションのサマリを表示します。

📴 Setup - Wireless Search Utility	X
Ready to Install Setup is now ready to begin installing Wireless Search Utility on your computer.	
Click Install to continue with the installation, or click Back if you want to review or change any settings.	
Destination location: C:\Program Files (x86)\Moxa\Wireless\Wireless Search Utility	*
Start Menu folder: Moxa\Wireless\Wireless Search Utility	
	Ŧ
٠	
< Back Install C	ancel

6. 「Install」(インストール)をクリックすると、インストールの実行が始まります。セットアップウィンドウにインストールの進捗状況が 表示されます。インストールの設定を変更するには、「Back」(戻る)をクリックして前の画面に戻ってください。 7. 「Finish」(完了)をクリックすると、Wireless Search Utilityのインストールが完了します。



Wireless Search Utility の設定

お使いのコンピュータと同じ LAN に接続されているすべての AWK-3131A AP を特定するには、ブロードキャスト検索機能が使用され ます。AWK-3131A を特定すると、その IP アドレスを変更できるようになります。ブロードキャスト検索機能は IP アドレスではなく、TCP パケットで検索するので、AWK-3131A が AP とクライアントのどちらに設定されているかは問題ではありません。いずれの場合も、ホ ストと同じサブネットに属しているかどうかに関わらず、LAN に接続されている AP とクライアントが特定されます。

Wireless Search Utilityプログラムを起動します。「Login」(ログイン)ページで「Device Search only」(デバイス検索のみ)オプションを選択すると、デバイスが検索され、各デバイスの設定が表示されます。「Device management」(デバイス管理)オプションを選択すると、IPの割り当て、ファームウェアの更新、デバイスの特定ができます。

Search Utility - Login	×
Wireless Sea	arch Utility
Device Search Only	
C Device Management	
Password:	
	V OK X Cancel

2. Wireless Search Utilityを開いて、「Search」(検索)アイコンをクリックします。

沟 Wirel	less Search Utili	ty				- 0 X
<u> </u>	dit F <u>u</u> nction T <u>o</u>	ols <u>H</u> elp				
<u>S</u> ear	ch Sear <u>c</u> h Ex	- 🔏 Locate	₩eb <u>I</u> elnet	Assign IP Unic) ick	
No	Model name	IP address	Device MAC address	Subnet mask	Firmware version	д
Search					ŗ	

3. 「Searching」(検索)ウィンドウに検索の進捗状況が表示されます。検索が完了すると、特定されたすべてのAWKが「Wireless Search Utility」(無線検索ユーティリティ)ウィンドウに表示されます。

🞾 Wire	less Search Utility	1000	-				
<u> </u>	<u>E</u> dit F <u>u</u> nction T <u>o</u> ols	<u>H</u> elp					
Sear	rch Sear <u>c</u> h Ex T	Locate Web	Telnet Assign IP	Linlock			
No	Model name	IP address	Device MAC address	Subnet mask	Firmwar	Overview	д
£1	AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0	1.12 Bu	System Info Device Info	802. 4 🕨
2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	1.1 Buil	Model name	AVUK.2121.
9 .3	AWK-3121-JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0	1.13 Bu	moder name	AWIK-5121-
						Device name	AWK-3121
						Device location	
						Device description	
						Serial No.	13496
						System up time	0 days 05h:
						Firmware version	1.12 Build 1
•		III			F.		

4. 「Locate」(場所の特定)をクリックすると、選択したデバイスがビープ音を発生します。

😡 Wireless Search Utility	a second and the second	-				X
<u>File Edit Function Tools</u>	<u>H</u> elp					
Search Search Ex *	Locate Web	Telnet Assign IP	E Unlock			
No Model name	IP address	Device MAC address	Subnet mask	Firmwar	Overview	д
📲 1 AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0	1.12 Bu	System Info Device Info 8	302. 💶 🕨
2 AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	1.1 Buil		LUK OT OT
📲 3 🛛 AWK-3121-JP	192.168.127.252	00-90-E8-4E-96-79	255 255 255 0	113BL	Model name A	WK-3121-
	Locate			<u>~</u>	Device name A	WK-3121
	Locatin Mod IP: MAD Net	g lel: AWK-3121-EU 192.168.127.253 C: 00:90:E8:22:B1:D9 mask: 255.255.255.0			Device description Serial No. 1: System up time 0 Firmware version 1.	3496 days 05h: .12 Build 1

- 5. 検索ユーティリティのアイコン設定を使用する前に、AWKのロックが解除されていることを確認してください。パスワードがデフォ ルトに設定されている場合、AWKはロックを自動的に解除します。それ以外の場合は、新しいパスワードを手動で入力する必要 があります。
- 6. 「Tools」(ツール)・「Login Options」(ログインオプション)と進むと、他のAWKの管理やロック解除ができます。

🞾 Wire	less Search Utility	/					
<u> </u>	Edit F <u>u</u> nction T <u>o</u> ol	ls <u>H</u> elp					
	rch Sear <u>c</u> h	Utility Login Options Login Options	Telnet Assign IP	D nlock			
No	Model name	<u>A</u> dvanced Options	vice MAC address	Subnet mask	Firmwar	Overview	д
61	AWK-3121-E	<u>C</u> ustomize List View	0:E8:22:B1:D9	255.255.255.0	1.12 Bu	System Info Device Info	802. 🔸 🕨
6 2 6 3	AWK-3131A-EU AWK-3121-JP	192.168.127.251 192.168.127.252	00:90:E8:4C:38:A1 00:90:E8:4E:9A:79	255.255.255.0 255.255.255.0	1.1 Buil 1.13 Bu	Model name	AWK-3121-
						Device name	AWK-3121_
						Device location	
						Device description	
						Serial No.	13496
						System up time	0 days 05h:
						Firmware version	1.12 Build 1
•		III					
							11.

 スクロールダウンリストを使って、管理したいAWK のMAC アドレスを選択して「Add」(追加)をクリックします。AWK デバイスの パスワードを入力し、「OK」をクリックして保存します。検索ページに戻って、AWK を再度検索すると、そのAWK のロックが自動 的に解除されることを確認できます。

注意						
安全のため、Wirele	ss Search Utility の)デフォルトのロ	グインパスワー	ードを変更する	あようお勧めしま	す。
Login Options	2 . 2	-			×	
Found device(s):	192.168.127.252 - 00	0:90:E8:4E:9A:79	· [Add		
Last IP	Device MAC address	Username	Password			
Default	×	admin	root			
192.168.127.253	00:90:E8:22:B1:D9	admin	root			
192 169 127 252	00:90:E8:4E:9A:79	admin	root			

ハイライト表示された AWK の設定を変更するには:

1. 「Web」アイコンをクリックして、Web コンソールを開きます。Web コンソールでは、すべての設定を変更できます。Web コンソー ルの詳しい使用方法については、第3章のWeb コンソールの使用方法に関する説明を参照してください。

💫 Wire	less Search Utility						
<u> </u>	<u>F</u> ile <u>E</u> dit F <u>u</u> nction T <u>o</u> ols <u>H</u> elp						
≦ <u>S</u> ear	ch Sear <u>c</u> h Ex T	Locate	Telnet Assign IP	D nlock			
No	Model name	IP address	Device MAC address	Subnet mask	Firmwar	Overview	Д
£1	AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0	1.12 Bu	System Info Device Info	802. 4 🕨
a 2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	1.1 Buil	M	AV-01-01
6 3	AWK-3121-JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0	1.13 Bu	Model name /	AWK-3121-
						Device name /	AWK-3121_
						Device location	
						Device description	
						Codel No.	10400
						Serial No.	13496
						System up time	0 days 05h:
						Firmware version	1.12 Build 1
-							
•		III			۰.		
Web							11.

2. telnet を使って AWK を設定する場合は、「Telnet」をクリックします。

💫 Wire	less Search Utility					_ X
<u>File</u>	dit Function Tools	<u>H</u> elp				
<u>S</u> ear	ch Sear <u>c</u> h Ex T	Locate Web	Telnet Assign IP	 <u>U</u> nlock		
No	Model name	IP address	Device MAC address	Subnet mask	Overview	д
f 1	AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0	System Info Device Info	802.11 Info
2 2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	Model name	AUR 2121 EU
- 3	AWK-3121 JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0	Model name	AWK-3121-EU
					Device name	AWK-3121_13496
					Device location	
					Device description	
					Serial No.	13496
					System up time	0 days 05h:22m:01s
					Firmware version	1 12 Build 15120319
1						
Tabat				•		
leinet						11.

3. 「Assign IP」(IP の割り当て)をクリックすると、IP 設定を変更できます。

😥 Wireless Search Utility		×
<u>File E</u> dit F <u>u</u> nction T <u>o</u> ols <u>H</u> elp		
<u>S</u> earch Search Ex Locate	web Telnet Assign IP Unlock	
No Model name IP address	Device MAC address Subnet mask Overview	Д
⁶ 1 AWK-3121-EU 192.168.1 ⁶ 2 AWK-3131A-EU 192.168.1 ⁶ 3 AWK-3121 JP 192.168.1	Assign IP Configuration Static AwK-3121-EU IP configuration \$192.168.127.253 AwK-3121_11496 AwK-3121_11496 IP address 192.168.127.253 Image: Configuration of the second arrow	
<		

以下では、3つの高度なオプション、「Search」(検索)、「Connection」(接続)、および「Miscellaneous」(その他)について説明します:

Search(検索)

- Retry count (再試行回数)(デフォルト=5): 自動的に再検索の回数を指定します。
- Retry interval (再試行間隔)(ms): 再検索する間隔。

Advanced Options	X
Search Connection Misc.	
Retry count: 5	
Retry interval (ms): 1000	
Multicast retry count 3	
	V OK X Cancel

Connection(接続)

- Connection timeout (secs)(接続タイムアウト)(秒):このオプションを使用すると、「Default Login」(デフォルトログイン)、「Locate」 (場所の特定)、「Assign IP」(IP の割り当て)、「Upload Firmware」(ファームウェアのアップロード)、「Unlock」(ロック解除)が完了 するまでの待機時間を設定できます。
- Upgrade timeout (secs)(アップグレードタイムアウト)(秒):このオプションを使用すると、ファームウェアのアップグレード中に接続が切断されるまでの待機時間を設定できます。このオプションは、ファームウェアがフラッシュに書き込まれるまでの待機時間を設定するのに使用できます。

Advanced Options	X
Search Connection Misc.	
Connection timeout (sec): 10	
Upgrade timeout (sec): 500	
Protocol timeout (msec): 200	
	V OK X Cancel

Misc.(その他)

Search on start(スタート時に検索): Wireless Search Utility へのログイン後にデバイスの検索が開始されるようにする場合は、この ボックスをチェックしてください。

Advanced Options	X
Search Connection Misc.	
Search on start	
	V OK X Cancel

その他のコンソールアクセス

この章では AWK-3131A に初めてアクセスする方法について説明します。AWK-3131A にアクセスするには、HTTP によ るアクセ スに加えて、シリアルコンソール、Telnet コンソール、SSH コンソール、HTTPS コンソールという4 つの方法 があります。シリアル コンソールによる接続では、短いシリアルケーブルを使って AWK-3131A とPC の COM ポート を接続する必要があります。この方 法は、AWK-3131A のIP アドレスがわからない場合でも使用できます。その他のコン ソールは、イーサネット LAN やインターネット から AWK-3131A にアクセスするのに使用できます。

この章の内容は以下のとおりです。

- □ RS-232 コンソール設定(115200, なし, 8, 1, VT100)
- □ Telnet コンソールと SSH コンソールによる設定 Telnet コンソールと SSH コンソールによる設定
- □ HTTPS/SSL 対応 Web ブラウザによる設定
- □ Telnet およびブラウザによるアクセスの無効化

RS-232 コンソール設定(115200, なし, 8, 1, VT100)

シリアルコンソールによる接続では、短いシリアルケーブルを使って AWK-3131A と PC の COM ポートを接続する必要があります。 この方法は、AWK-3131A の IP アドレスがわからない場合でも使用できます。LAN ケーブルが切断した場合や LAN でブロードキャス トストームが発生した場合など、イーサネット LAN か AWK-3131A にアクセスできない場合にも、シリアルコンソール設定を使用する と便利です。



注意

逆電圧保護がサポートされている場合でも、逆電圧(例: -48VDC)で AWK-3131A に電力が提供されている場合は RS-232 コンソ ールマネージャを使用しないでください。逆電圧で RS-232 コンソールを接続する必要がある場合 は、Moxa の TCC-82 アイソレ ータを使用してください。

NOTE Moxa の Web サイトから無料でダウンロードできる「Moxa PComm (Lite)」Terminal Emulator を使用す ることをお勧めします。

PComm ターミナルエミュレータを起動する前に、RJ45-DB9 メス(または RJ45-DB25 メス)ケーブルを使って AWK-3131A の RS-232 コンソールポートと PC の COM ポート(通常は COM1 または COM2(システムの設定による))を接続してください。PComm タ ーミナルエミュレータのインストール後、以下の手順に従って RS-232 コンソールユーティリティにアクセスします。

- 1. Windows のデスクトップから、「スタート」メニューを開いて、「PComm(Lite)」グループの「PComm Terminal Emulator」(PComm ターミナルエミュレータ)を起動します。
- 2. 「Port Manager」(ポートマネージャ)の下の「Open」(開く)を選択して、新しい接続を開きます。



「Property」(プロパティ)ウィンドウの「Communication Parameter」(通信パラメータ)ページが開きます。コンソール接続用の適切な COM ポートを選択し、「Baud Rate」(ボーレート)、「Data Bits」(データビット)、「Parity」(パリティ)、「Stop Bits」(ストップビット)をそれぞれ 115200、8、None(なし)、1 に 設定します。「Terminal」(ターミナル)タブをクリックして、「Terminal Type」(ターミナルタイプ)を VT100(または ANSI)に設定します。「OK」をクリックして続行します。

Property	Property 🗙
Communication Parameter Terninal File Transfer Capturing COM Options Ports : <u>"COM1 · ·</u> Baud Rate : 115200 · · Data Bits : 8 · · Parity : None · · Stop Bits : 1 · ·	Communication Parameter Terninal File Transfer Capturing Terminal Type : VT100 ANSI WT100 Dumb Terminal Option : Dumb Terminal Transmit Local Echo Send 'Enter' Key As: CR-LF
Flow Control T RTS/CTS T X0N/X0FF C X0XFF C X0XFF C X0XFF C X0XFF C X0XFF C X0XF	Receive CR Translation : No Changed I

4. コンソールのログイン画面が表示されます。ログイン名(デフォルト: admin)とパスワード(新しいパスワードが設定されていない 場合のデフォルト: root)を使って、RS-232 コンソールにログインします。 1.1

👪 COM4,115200,None,8,1,ANSI	
AWK-3131-US DTR AWK-3131_0002 login: admin RTS Password:	<
State: OPEN CTS DSR RI DCD Ready	/

5. AWK-3131A のデバイス情報とメインメニューが表示されます。画面の指示に従って、実行する管理オプションを選択してくださ

👪 c	OM4,115200,None,8,1,ANSI	×
DTR	Model Name : AWK-3131-US LAN MAC Address : 00:90:E8:00:00:F9 Serial No : 2 Firmware Version : 1.0 Build 10120801 	
	(5) Restart (q) Quit Key in your selection:	•
State:	OPEN CTS DSR RI DCC Ready	

メモ

PComm Terminal Emulator ウィンドウの外観を変更する場合は、「**Edit**」(編集)→「Font」(フォント)を選択して、希望する書式オプシ ョンを選択します。



注意

RS-232 ケーブルを外したり、「DTR」をトリガした場合は、ネットワークのセキュリティを確保するために、切断イベントが発生してログ アウトが強制的に実行されます。操作を再開するには、再びログインする必要があります。

Telnet コンソールと SSH コンソールによる設定

Telnet や SSH クライアントを使用して、AWK-3131A にアクセスし、ネットワークからコンソールを管理できます。 AWK-3131A と同じ LAN に接続されている PC ホストからネットワークを介して AWK-3131A の機能にアクセスするには、PC ホストと AWK-3131A が同じ論理サブネットに属している必要があります。それを確認するには、PC ホストの IP アドレスとサブネットマスクをチェックします。

★モ AWK-3131A のデフォルト IP アドレスは 192.168.127.253 で、デフォルトのサブネットマスクは 255.255.255.0 です(クラス C ネットワ ーク)。これらの値が正しく設定されていない場合は、PC ホストのネットワーク設定を確認して、IP アドレスを 192.168.127.xxx に、サ ブネットマスクを 255.255.255.0 に変更してください。

Telnet や SSH クライアントからコンソールユーティリティにアクセスするには、以下のステップを実行します。

1. Windows のデスクトップから「スタート」→「ファイル名を指定して実行」を実行し、Telnet を使用して Windows の「ファイル名を指 定して実行」ウィンドウから AWK-3131A の IP アドレスにアクセスします (MS-DOS プロンプトから telnet コマンドを発行することも できます)。

Run	? ×
<u>;</u>	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	telnet 192.168.127.253
	OK Cancel <u>B</u> rowse

 SSHクライアント(例: PuTTY)を使用する場合、クライアントプログラム(例: putty.exe)を実行してから、AWK-5232 のIP アドレス を入力して、SSH 接続ポートに 22 を指定します。

į	RuTTY Configuration		×
	Category:		
	⊡-Session	Basic options for your PuTTY sessi	ion
	Logging	C Specify the destination you want to connect to	
	- Keyboard	Host Name (or IP address)	<u>P</u> ort
	Bell	192.168.127.253	22
	Features ⊡- Window Appearance	Connection type: ○ <u>R</u> aw ○ <u>T</u> elnet ○ Rlog <u>i</u> n ● <u>S</u> SH	🔿 Serial

3. コンソールのログイン画面が表示されます。ログインと管理については、前述の「RS-232 コンソール設定」を参照し てください。

HTTPS/SSL 対応 Web ブラウザによる設定

AWK-3131A は HTTP アクセスの安全を確保するために、すべての HTTP トラフィックの HTTPS/SSL 暗号化に対応しています。 HTTPS/SSL を使用して AWK-3131A の Web ブラウザインターフェイスにアクセスにするには、以下の手順を実行します。

1. Web ブラウザを開いて、アドレスの欄に「https://<AWK-3131AのIPアドレス>」を入力します。「Enter」を押して接続を確立します。

Attps://192.168.127.253/home.asp - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🗘 Back 🔹 🔿 🖉 😰 🖓 🔞 Search 🕋 Favorites 🛞 Media 🧐 🛃 🚽 🎒 🗹 🚍	
Address 🛃 https://192.168.127.253/home.asp	

2. セキュリティ証明書が信頼されていない会社から発行されたことをユーザーに警告する警告メッセージが表示されます。

Security	Alert		
£	Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.		
	The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.		
	The security certificate date is valid.		
	The security certificate has a valid name matching the name of the page you are trying to view.		
	Do you want to proceed?		
	Yes View Certificate		

3. 「Yes」(はい)を選択して Moxa IW 発行の証明書を承認してから、HTTPS/SSL によって安全が確保された AWK-3131A の Web ブラウザインターフェイスに入ります。(URL のプロトコルは https と表示されます。) 続いて、ウィンドウ左側のメニューツ リーを使えば、目的の機能のページを開いて AWK-3131A の各機能にアク セスできます。



Telnet およびブラウザによるアクセスの無効化

AWK-3131A を公共のネットワークに接続するけれど、その管理機能をネットワークから使用したくない場合は、 Telnet コンソール と Web 設定の機能を両方ともオフにすることをお勧めします。以下の図のように、「Maintenance」(メンテナンス)→「Console Settings」(コンソール設定)を実行して、それらの機能を無効 にします。.

Console Settings				
HTTP console	Enable Oisable			
HTTPS console	Enable Oisable			
Telnet console	🖲 Enable 🔍 Disable			
SSH console	🖲 Enable 🔍 Disable			

Submit



この付録では、無線関連技術について詳しく説明します。これらの情報は、AWK-3131Aの管理と、産業用無線ネットワークの効率的なプランニングに役立ちます。

この付録の内容は以下のとおりです。

- AeroLink Protection
- ロビーコン
- DTIM
- ロ フラグメント
- □ RTS しきい値
- □ STP と RSTP
 - ➢ STP/RSTP の概念の概念
 - ▶ RSTP と STP の違い

AeroLink Protection

海底油田用プラットフォーム間の通信や列車−地上間通信などの産業用用途において、信頼性の高い無線ブリッジは、システムのダ ウンタイムを最小限に抑え、システムの可用性を最大限に高めるために欠かせません。Moxaの AeroLink Protection は、2 つのネッ トワーク間に高い信頼性の無線ブリッジを提供し、ネットワークレベルの冗長性を形成します。

1. 通信フェイルオーバー: AeroLink Protection のメンバーは互いにネゴシエートして、データ通信のアクティブノードを自動的に選 出します。アクティブノードがそのアクセスポイントへのデータ送信ができなくなると、別のパスで通信を再開するように他のバッ クアップノードに通知します。



2. 周波数干渉フェイルオーバー: この概念は以前のモデルに類似しています。通信の周波数に干渉が発生し、アクティブ な周波 数でデータを伝送できなくなった場合、別のバックアップ周波数で通信を再開します。



3. デバイスフェイルオーバー: AeroLink Protection は、通信と周波数の障害に対処した後、単一障害点のない無線ネットワーク を提供するためにデバイスのステータスもチェックします。アクティブノードに電源の障害が発生した場合、バックアップノードは、 無線通信を自動的に再開します。



- 4. スケーラブル: AeroLink Protection は、ユーザーがバックアップノード数を増やして上記の障害すべてからの完全な無線冗長性 を実現できるように、スケーラブルなバックアップパスを可能にするように設計されています。
- 高速回復: 冗長な無線ネットワークを維持するだけでなく、障害発生時にも通信を中断させないことも重要です。 AeroLink Protection は、300 ms ですべての障害から通信を回復するように設計されています。 AeroLink Protection グループのメンバーのステータスは、以下の7 つのいずれかになります。

- 「Initiation State(Init)」(開始状態(Init)): AeroLink Protection Protocol を開始します。
- 「Discovering State (Discover)」(検出状態(Discover)): これからネゴシエーションする他の AeroLink Protection メンバーを検 出します。
- 「Idle State(Idle)」(アイドル状態(Idle)):内部プロトコルのチェックポイント
- 「Negotiation State (Nego)」(ネゴシエーション状態(Nego)):他の AeroLink Protection メンバーとネゴシエーションし、アクティブ ノードを選出します。
- 「Backup State(Backup)」(バックアップ状態(Backup)): ネゴシエーション後、このノードがバックアップノードとして割り当てられ ます。代わりにすべてのトラフィックはアクティブノードを通過します。

メモ ノードがバックアップ状態になると、「STATE」(状態)の LED が点滅します。

- 「Active State(Active)」(アクティブ状態(Active)): ネゴシエーション後、このノードがアクティブノードとして割り当てられるため、 トラフィックはこのノードを通過します。
- 「Role Change State(Change)」(役割変更状態(Change)): アクティブノードが WLAN を介してデー タを送信できなくなると、 「Change」状態に変化し、バックアップノードからアクティブノードの再ネゴシエーションをトリガします。

AeroLink Protection 機能は次の3つの検出方法のうちの1つを適用します。

- SNR: 関連するクライアントの信号雑音比 (SNR)の状態
- 信号強度: 関連するクライアントの信号強度の状態
- 切断

ビーコン

ビーコンは、ネットワークを常に同期させておくために AP がブロードキャストするパケットです。ビーコンには、無線 LAN サービス エリア、AP のアドレス、ブロードキャストのデスティネーションアドレス、タイムスタンプ、DTIM(Delivery Traffic Indicator Map)、TIM (Traffic Indicator Message)が含まれます。ビーコン間隔は、AP の周波数間隔のことです。

DTIM

DTIM(Delivery Traffic Indication Map)はビーコンフレームに含まれており、AP によってバッファされたブロードキャストおよびマルチ キャストフレームがまもなく配信されることを示します。設定を下げるとネットワーク効率が上がりますが、PC が電力を節約するスリー プモードに入ることを妨げます。設定を上げると、PC がスリープモードに 入れるようになり、電力を節約できます。

フラグメント

設定を下げると、パケットのサイズが小さくなり、作成される単位通信あたりのパケット数が多くなります。この値を下げてパケットの エラー率が上がった場合は再度上げることができますが、ネットワーク全体のパフォーマンスが低下する可能性があります。この値 の変更は最小限にとどめることをお勧めします。

RTS しきい値

RTS しきい値(256-2346)- パケットがそのサイズを超えるとアクセスポイントが効率的な通信を確保するために送受信の調整を行 うパケットサイズを指定します。この値はデフォルト設定の 2.346 のままにしておいてください。スムーズなデータフローが得られない 場合は変更できますが、変更は最小限にとどめるようお勧めします。

STP と RSTP

STP/RSTP の概念

スパニングツリープロトコル(STP)は、ネットワークのリンク障害を削減し、ループから保護するために設計されました。複雑な構造の ネットワークでは、ネットワーク内の偶然のループによってブロードキャストストームが引き起こされる傾向があります。STP プロトコ ルは IEEE 802.1D 規格、1998 Edition ブリッジ仕様の一部です。

ラピッドスパニングツリープロトコル (RSTP)は、IEEE 802.1w-2001 規格で定義されたスパニングツリーアルゴリズムおよびプロトコ ルを実装します。RSTP は以下のメリットがあります。

- ブリッジされたネットワークのトポロジが STP に比べてはるかに迅速に決定されます。
- RSTP は STP と下位互換なので、導入が比較的容易です。例えば、次のとおりです。
 - ▶ この形式のパケットが受信されると、デフォルトで 802.1D スタイルの BPDU が送信されます。
 - STP(802.1D)と RSTP(802.1w)は、同じ AWK-3131A の LAN ポートと WLAN ポート(AP と WDS1~ WDS8)で動作できます。

AWK-3131A がレガシースイッチなどの古い機器に接続されている場合、この機能は特に有用です。

RSTP と STP の違い

RSTP は STP と似ていますが、各ブリッジが隣接するブリッジへのリンクを有効にするときにループの形成を防ぐ措置をとったことを 確認できる付加的な情報が BPDU に含まれている点が異なります。ポイントツーポイントリンクで接続された隣接するブリッジどうし は、ネットワーク内の他のすべてのブリッジが変化に対応できたかどうかを確認するまで待たなくても、リンクを有効にできます。 RSTP の主なメリットは、設定がネットワークワイドではなく、ローカルで決定されるため、RSTP が自動設定を実行して STP よりも速く リンクを復元できることです。 この付録では、本製品に関する付加的な情報を提供します。また、Moxaのテクニカルサポートとの連絡方法についても説明します。 この付録の内容は以下のとおりです:

- ロ ファームウェアの復元
- 口 適合宣言
 - ▶ エラー!参照元が見つかりません。
- □ RED(Radio equipment directive)適合宣言

ファームウェアの復元

「FAULT」(フォルト)、「Signal Strength」(信号強度)、「WLAN」の LED がすべて同時に点灯し、1 秒間隔で点滅する場合、システムが 起動に失敗したことを意味します。これは、誤った操作やファームウェア更新中の予期しないシャットダウンなどの制御不可能な問題 に起因します。AWK-3131A は、管理者が上記の障害を解決して、システムの操作再開を支援するように設計されています。以下の 指示に従ってファームウェアを復元できます:

AWK-3131Aの ES-232 コンソールに 115200bps および N-8-1 で接続します。ターミナルエミュレータに以下のメッセージが1秒ごとに表示されます。

please set-up TFTP server 192.168.127.1 contains awk3131a.rom for firmware recovery. please set-up TFTP server 192.168.127.1 contains awk3131a.rom for firmware recovery. please set-up TFTP server 192.168.127.1 contains awk3131a.rom for firmware recovery. please set-up TFTP server 192.168.127.1 contains awk3131a.rom for firmware recovery. please set-up TFTP server 192.168.127.1 contains awk3131a.rom for firmware recovery. please set-up TFTP server 192.168.127.1 contains awk3131a.rom for firmware recovery.

Take the following steps for the firmware recovery:

- 1. ラップトップのIPアドレスを「192.168.127.1」に変更します。
- 2. ラップトップでTFTPサーバをセットアップします。
- 3. MoxaのWebサイトからAWK-3131Aのファームウェアをダウンロードします。
- 4. ファームウェアのファイル名を「awk3131a.rom」に変更します。
- 5. AWK-3131AのRJ45イーサネットポートに接続します。

設定が正しければ、端末ターミナルエミュレータに以下のメッセージが表示され、ファームウェア復元プロセスが完了すると AWK-3131A が再起動します。

適合宣言

干渉に関する FCC (米連邦通信委員会)の注意事項

本装置は FCC 規則 Part15 に従うクラス B のデジタルデバイスに関する制限に適合していることがテストにより確認されています。こ れらの制限は装置を住居環境で使用した場合に有害な干渉の発生を適度に防止することを目的としています。本装置は無線周波エ ネルギーを発生、使用、および放出しており、指示に従って設置または使用しない場合は、無線通信に有害な干渉を引き起こすこと があります。ただし、特定の設置によって干渉が発生しないという保証はありません。本装置によってラジオまたはテレビの受信に有 害な干渉が発生した場合は(装置の ON/OFF によって確認できます)、以下の対策を試して干渉を是正してください:

- 受信アンテナの向きまたは場所を変える。
- 本装置と受信機の距離を離す。
- 受信機とは回路が異なるコンセントに本装置を接続する。
- 販売店やラジオ/テレビの専門技術者に問い合わせる。

FCC からの警告: 適合性を確実に維持するために、例えば、コンピュータや周辺機器に接続する場合はシールドインターフェイスケ ーブルのみを使用してください。製造元が明確に承認していない変更または改造を行うと、本装置を操作するユーザーの権利が無 効になることがあります。この送信機は、他のアンテナや送信機と一緒に配置したり使用してはなりません。

電磁波放出に関する FCC からの注意事項

本装置は制御不能な環境を対象に設定されたFCCの電磁者放出制限に適合しています。本装置はラジエターや人体から20 cm以 上離して設置または使用してください。

本装置は FCC 規則 Part 15 に適合しています。動作は以下の 2 つの条件に従う必要があります。(1)本装置によって、有害な干渉 が発生することはない。(2)本装置は、不適切な動作を引き起こる可能性のある干渉も含め、すべての干渉に対応できなければなら ない。

U-NII 装置は 5.15~5.25 GHz 帯域内で、同ーチャンネルの MSS 動作に有害な干渉をもたらす可能性を削減するために、使用を屋内に制限されます。

RED(Radio equipment directive) 適合宣言

Moxa は、AWK-3131AA 装置が指令 2014/53/Euの基本要件および他の該当条件に適合していることを宣言します。

5150~5350 MHz の周波数範囲は屋内での使用に限定されています。この範囲内での屋外操作は禁じられています。

安全性

本装置は、本装置を設置し使用するユーザーの安全を最大限に配慮して設計されていますが、電気装置を取り扱うときには感電や 静電気の危険に細心の注意を払う必要があります。したがって、本装置およびコンピュータの製造元のガイドラインはすべて、常に 装置の安全な使用を確保できなければなりません。

使用が想定されていない EU 諸国

なし。