

Cisco Business Wireless Access Point(BAP)での簡易ネットワーク管理プロトコルの設定

目的

このドキュメントの目的は、Cisco Business Wireless(CBW)Access Point(AP)で簡易ネットワーク管理プロトコル(SNMP)設定を設定する方法を示すことです。

該当するデバイス | ソフトウェアバージョン

- 140AC ([データシート](#)) | 10.0.1.0 ([最新版をダウンロード](#))
- 145AC ([データシート](#)) | 10.0.1.0 ([最新版をダウンロード](#))
- 240AC ([データシート](#)) | 10.0.1.0 ([最新のダウンロード](#))

概要

CBW APは、パフォーマンス、アクセス性、高密度ネットワークを実現する最新の802.11ac Wave 2標準をサポートします。業界最高レベルのパフォーマンスを実現し、安全性と信頼性の高いワイヤレス接続を実現し、堅牢でモバイルなエンドユーザエクスペリエンスを実現します。

SNMPは、ネットワーク内のすべてのデバイスから情報を収集し、これらのデバイスを設定および管理するために使用される一般的なネットワーク管理プロトコルです。マスターAP Webインターフェイスを使用して、SNMP v2cとSNMP v3の両方のアクセスモードを設定できます。SNMPv2cは、SNMPv2のコミュニティストリングベースの管理フレームワークです。コミュニティストリングは、クリアテキストで送信されるパスワードのタイプです。SNMP v3機能は、ネットワーク上のデータパケットを認証および暗号化することで、デバイスへのセキュアなアクセスを提供します。

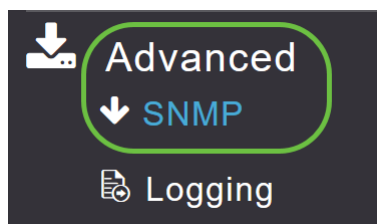
マスターAPには、次のSNMPアクセスモードを設定できます。

- SNMP v2cのみ
- SNMP v3のみ
- SNMP v2cとSNMP v3の両方
- SNMP v2cとSNMP v3のどちらでもない

SNMPの設定

手順 1

[Advanced] > [SNMP]を選択します。



手順 2

MIBブラウザを使用して設定を照会するSNMPサービスオプションを有効にします。

SNMP

↓ Service Disabled

Service ?

SNMP Access V2C V3

Read Only Community public

Read-Write Community *****

Apply

手順 3

SNMPセットアップウィンドウで、SNMPアクセスの横にある適切なチェックボックスを選択し、目的のSNMPモードを有効にします。

デフォルトのモードはv2cです（または、デフォルトでは、SNMPアクセスモードの両方または両方が選択されていません）。

選択したSNMPアクセスモードが有効になっている。

SNMP



Service

Disabled

Service ?

SNMP Access **V2C** **V3**

Read Only Community

Read-Write Community

Apply

手順 4

[読み取り専用コミュニティ]フィールドに、目的のコミュニティ名を入力します。デフォルト名はpublicです。

SNMP



Service

Disabled

Service ?

SNMP Access **V2C** **V3**

Read Only Community

Read-Write Community

Apply

手順 5

[読み取り/書き込みコミュニティ]フィールドに、目的のコミュニティ名を入力します。デフォルト名はprivateです。

SNMP



Service

Disabled

Service ?

SNMP Access **V2C** **V3**

Read Only Community

Read-Write Community

Apply

手順 6

[Apply] をクリックします。

SNMP



Service

Disabled

Service ?

SNMP Access **V2C** **V3**

Read Only Community

Read-Write Community

Apply

ステップ7

SNMPトラップレシーバを設定するには、「**Add New SNMP Trap Receiver**」をクリックします。このツールは、ネットワークデバイスから送信されたSNMPトラップを受信、ログ記録、および表示します。デフォルト設定は「無効」です。

SNMP Trap Receivers

⊕ Add New SNMP Trap Receiver

Action	Receiver Name	IP Address	Status	SNMPv3
--------	---------------	------------	--------	--------

手順 8

[Add SNMP Trap Receiver] ウィンドウで、次の項目を設定します。

- レシーバ名
- 接続先のサーバのIPアドレス
- ステータス
- SNMPv3を有効にするオプション

[Apply] をクリックします。

Add SNMP Trap Receiver ×

Receiver Name ①

IP Address ②

Status ③

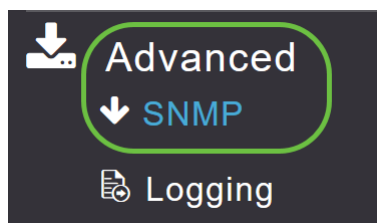
SNMPv3 ④

⑤

SNMPv3ユーザの追加

手順 1

[Advanced] > [SNMP]を選択します。



手順 2

[SNMPのセットアップ] ウィンドウの[SNMPv3ユーザー]セクションで、[新しいSNMPv3ユーザーの追加]ボタンをクリックします。

SNMP V3 Users

⊕Add New SNMP V3 User

Action	User Name	Access Mode	Authentication protocol	Privacy Protocol
--------	-----------	-------------	-------------------------	------------------

手順 3

[Add SNMP v3 User]ウィンドウで、次の詳細を入力します。

- *User Name* : 新しいSNMPv3ユーザのユーザ名を入力します。
- *アクセスモード* : ドロップダウンリストから、必要なモードの1つを選択します。読み取り専用または読み取り/書き込み。既定値は[読み取り専用]です。
- *認証プロトコル*: [認証プロトコル]ドロップダウンリストから、次のいずれかのオプションを選択します。HMAC-MD5、HMAC-SHA、またはNone。デフォルトの認証プロトコルは**HMAC-SHA**です。
- *Authentication Password* : 目的の認証パスワードを入力します。パスワードの最小長は12 ~ 31文字です。
- *Confirm Authentication Password* : 上記で指定した認証パスワードを確認します。[パスワードの表示(Show Password)]チェックボックスをオンにすると、[認証パスワード(Authentication Password)]フィールドと[認証パスワードの確認(Confirm Authentication Password)]フィールドのエントリが表示され、文字が一致するかどうかを確認できます。
- *プライバシープロトコル* : ドロップダウンリストから、次のいずれかのオプションを選択します。CBC-DES、CFB-AES-128、またはNone。デフォルトのプライバシープロトコルは**CFB-AES-128**。
- *Privacy Password* : 目的のプライバシーパスワードを入力します。パスワードの最小長は12 ~ 31文字です。
- *Confirm Privacy Password* : 上記で指定したプライバシーパスワードを確認します。[Show Password]チェックボックスをオンにすると、[Privacy Password]フィールドと[Confirm Privacy Password]フィールドのエントリが表示され、文字が一致するかどうかを確認できます。

Add SNMP V3 User



User Name *

Access Mode

Authentication protocol

Authentication Password

Confirm Authentication Password

Show Password

Privacy Protocol

Privacy Password

Confirm Privacy Password

Show Password

手順 4

[Apply]をクリックし、新しいSNMPv3ユーザを作成します。

Add SNMP V3 User

User Name *

Access Mode

Authentication protocol

Authentication Password

Confirm Authentication Password

Show Password

Privacy Protocol

Privacy Password

Confirm Privacy Password

Show Password

新しく追加されたSNMPv3ユーザが、[SNMP Setup]ウィンドウの[SNMP V3 Users]テーブルに表示されます。

SNMP V3 Users

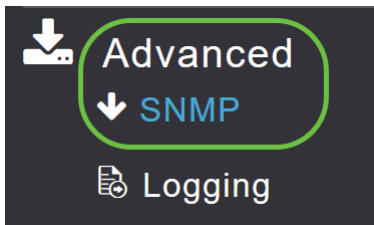
Action	User Name	Access Mode	Authentication protocol	Privacy Protocol
<input checked="" type="checkbox"/>	Test	Read Only(Default)	HMAC-SHA(Default)	CFB-AES-128(Default)
<input checked="" type="checkbox"/>	ciscoA2	Read Only(Default)	HMAC-SHA(Default)	CFB-AES-128(Default)

最大7人のSNMPv3ユーザを追加できます。

SNMPv3ユーザの削除


手順 1

[Advanced] > [SNMP]を選択します。



手順 2

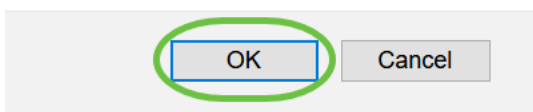
SNMP Setupで、削除するSNMPv3ユーザを含む行のXアイコンをクリックします。

Action	User Name	Access Mode	Authentication protocol	Privacy Protocol
	Test	Read Only(Default)	HMAC-SHA(Default)	CFB-AES-128(Default)

手順 3

アクションを確認するポップアップウィンドウが表示されます。[OK] をクリックします。

Are you sure? You want to delete this User.



SNMPv3 Usersテーブルが更新され、削除されたエントリがテーブルから削除されます。

結論

準備は万端！これで、CBW APでSNMPが正常に設定されました。詳細については、次の記事を参照して、ネットワークを簡単に管理してください。

[よく寄せられる質問 \(FAQ\)](#) [Firmware Upgrade RLAN アプリケーションのプロファイリング](#) [クライアントプロファイリング](#) [マスターAPツール Umbrella WLANユーザ](#) [Logging](#) [トラフィックシェーピング](#) [Rogues](#) [干渉源](#) [構成管理](#) [ポート設定](#) [メッシュモード](#)