CHAPTER 16

SNMP 監視の設定

この章では、SNMP トラップ、受信者、コミュニティ ストリングおよびグループの関連性、ユーザ セキュリティ モデル グループ、ユーザ アクセス権を設定する方法について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と WAE を総称する用語として「WAAS デバイス」を使用します。「WAE」は、WAE アプライアンスおよび WAE ネットワーク モジュール（NME-WAE デバイス ファミリ）を示します。

この章には、次の項があります。

SNMP について

Simple Network Management Protocol （SNMP; 簡易ネットワーク管理プロトコル）は、SNMP エージェントを介して WAAS デバイスを外部監視できる、相互運用可能な標準ベースのプロトコルです。

SNMP によって管理されるネットワークは、次のプライマリ コンポーネントから構成されます。

- **管理対象デバイス** —SNMP エージェントを持つネットワーク ノードで、管理対象ネットワークに常駐します。管理対象デバイスには、ルータ、アクセス サーバ、スイッチ、ブリッジ、ハブ、コンピュータ ホスト、およびプリンタが含まれます。WAAS ソフトウェアを実行する各 WAAS デバイスは、SNMP エージェントを持っています。
- **SNMP エージェント** — 管理対象デバイスに常駐するソフトウェア モジュールです。エージェントは、管理情報のうちローカルに関する知識を保持し、その情報を SNMP と互換可能な形式に変換します。SNMP エージェントは、MIB （Management Information Base; 管理情報ベース）からデータを収集します。MIB は、デバイス パラメータとネットワーク データに関する情報のリポジトリです。また、エージェントは、トラップ、つまり特定イベントの通知を管理システムに送信することもできます。
- **管理ステーション** — ASNMP ホストと呼ぶこともあります。管理ステーションは、SNMP を使用して SNMP エージェントに SNMP Get 要求を送信して、WAAS デバイスから情報を取得します。次に、管理対象デバイスは、管理情報を収集して保存し、SNMP を使用してこの情報を管理ステーションに提供します。

事前に、SNMP 管理アプリケーションが管理ステーションに配備されていないと、この SNMP 情報にはアクセスできません。この SNMP 管理ステーションは、SNMP を使用して SNMP Get 要求をデバイス エージェントに送信して WAAS デバイスから情報を取得するため、SNMP ホストと呼ばれています。

SNMP 通信プロセス

SNMP 管理ステーションと WAAS デバイスに存在する SNMP エージェントは、SNMP を使用して、次のように通信します。

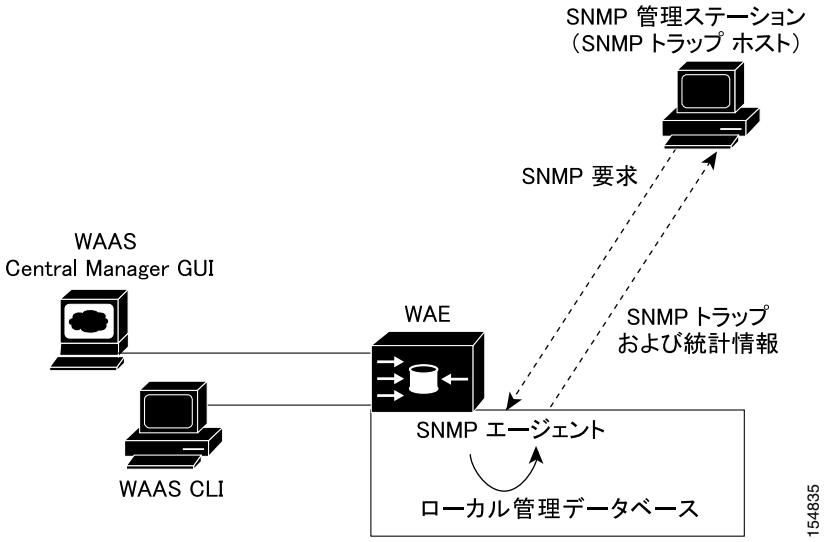
1. SNMP 管理ステーション（SNMP ホスト）は、SNMP を使用して WAAS デバイスに情報を要求します。
2. これらの SNMP 要求を受信すると、WAAS デバイス上の SNMP エージェントは、個々のデバイスに関する情報を保持しているテーブルにアクセスします。このテーブル、またはデータベースが、MIB と呼ばれます。

（注）　WAAS デバイス上の SNMP エージェントは、異常な状況でのみ SNMP ホストとの通信を開始します。つまり、ホストに送信する必要のあるトラップがある場合にホストとの通信を開始します。この項目の詳細については、16-8 ページの「SNMP トラップの有効化」を参照してください。

3. エージェントは、MIB 内で指定された情報を見つけると、SNMP を使用して、その情報を SNMP 管理ステーションに送信します。

図 16-1 に、個々の WAAS デバイス用のこれらの SNMP 操作を示します。

図 16-1　WAAS ネットワーク内の SNMP コンポーネント



サポートされている SNMP バージョン

WAAS ソフトウェアは、次の SNMP のバージョンをサポートします。

- **バージョン 1（SNMPv1）**—SNMP の初期の実装です。機能の完全な説明については、RFC 1157 を参照してください。
- **バージョン 2 （SNMPv2c）**—SNMP の 2 番目のリリースで、RFC 1902 に規定されています。データ タイプ、カウンタ サイズ、およびプロトコル動作が追加されています。
- **バージョン 3 （SNMPv3）**— 最新バージョンの SNMP で、RFC 2271 ～ RFC 2275 に規定されています。

WAAS ソフトウェアを実行する各 Cisco デバイスは、SNMP プロトコルを使用してデバイス設定と操作に関する情報を交換するために必要なソフトウェアを搭載しています。

SNMP セキュリティ モデルおよびセキュリティ レベル

SNMPv1 および SNMPv2c には、SNMP パケット トラフィックの機密性を保持するためのセキュリティ（つまり、認証またはプライバシー）機能がありません。その結果、ワイヤ上のパケットが検出され、SNMP コミュニティ ストリングが見破られてしまうことがあります。

SNMPv1 および SNMPv2c のセキュリティ上の欠点を解決するために、SNMPv3 では、ネットワークを経由するパケットを認証および暗号化することで、WAAS デバイスへの安全なアクセスを提供しています。WAAS ソフトウェアの SNMP エージェントは、SNMPv3 はもちろん、SNMPv1 と SNMPv2c もサポートします。

SNMPv3 で提供されるセキュリティ機能は、次のとおりです。

- **メッセージの完全性** — 伝送中にパケットが一切妨害されていないことを保証します。
- **認証** — 有効な送信元からのメッセージであるかどうかを判別します。
- **暗号化** — 不正な送信元によってパケットが認識されてしまうのを防ぐため、パケットの内容をスクランブルします。

SNMPv3 は、セキュリティ モデルだけでなく、セキュリティ レベルも備えています。セキュリティ モデルは、ユーザと、ユーザが所属するグループに対して設定される認証プロセスです。セキュリティ レベルは、セキュリティ モデルの中で許容されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットの処理時に使用されるセキュリティ プロセスが決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2c、および SNMPv3 の 3 つです。

表 16-1 は、セキュリティ モデルとセキュリティ レベルの組み合わせをまとめたものです。

表 16-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	プロセス
v1	noAuthNoPriv	コミュニティ ストリング	なし	ユーザ認証の照合にコミュニティ ストリングを使用します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	ユーザ認証の照合にコミュニティ ストリングを使用します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ認証の照合にユーザ名を使用します。
v3	AuthNoPriv	Message Digest 5 （MD5）または Secure Hash Algorithm （SHA）	なし	Hash-Based Message Authentication Code （HMAC; ハッシュベースのメッセージ認証コード）-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。
v3	AuthPriv	MD5 または SHA	あり	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。Cipher Block Chaining （CBC; 暗号ブロック連鎖）-Data Encryption Standard 56-bit （DES-56; データ暗号規格 56 ビット）に基づく、DES-56 暗号化（パケット認証）を提供します。

SNMPv3 エージェントは、次のモードで使用できます。

- noAuthNoPriv モード（パケットに対してオンになっているセキュリティ メカニズムはありません）
- AuthNoPriv モード（プライバシー アルゴリズム（DES-56）を使用して暗号化する必要がない、パケット用）
- AuthPriv モード（暗号化する必要があるパケット用。プライバシーを保持するには、パケットに対して認証を実行する必要があります）

SNMPv3 を使用すれば、ユーザは、データが改ざんされる恐れを抱くことなく、SNMP エージェントから管理情報を安全に収集できます。また、Content Engine の設定を変更する SNMP set パケットなどの機密情報は、ワイヤ上で内容が露呈するのを防ぐために、暗号化することができます。グループベースの管理モデルでは、さまざまなユーザが異なるアクセス特権で同じ SNMP エージェントにアクセスすることができます。

サポートされる MIB

この項では、WAAS がサポートしている Cisco 固有の MIB について説明します。MIB は、アルファベット順に掲載されています。サポートされている Cisco 固有の MIB は、次のとおりです。

- ACTONA-ACTASTOR-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONTENT-ENGINE-MIB

- CISCO-ENTITY-ASSET-MIB
- ENTITY-MIB
- EVENT-MIB
- HOST-RESOURCES-MIB
- MIB-II

ACTONA-ACTASTOR-MIB

この MIB は、ActaStor バージョン番号、ライセンス情報、インストール情報、および一般情報を含む WAAS 統計情報を提供します。

CISCO-CDP-MIB

この MIB は、ローカル インターフェイスの ifIndex 値を表示します。リピータ ポートに ifIndex 値が割り当てられていない 802.3 リピータの場合、この値はポート固有の値になり、リピータがサポートしている任意　ifIndex　より大きい。 この例では、特定のポートが　cdpInterfaceGroup　と cdpInterfacePort の対応する値によって示され、これらの値が RFC 1516 のグループ番号とポート番号の値に対応します。

CISCO-CONFIG-MAN-MIB

この MIB は、さまざまな位置に存在する設定データのモデルを表します。

- **running** — 動作中のシステムが使用している
- **terminal** — 接続しているハードウェア
- **local** — NVRAM またはフラッシュ メモリにローカルに保存される
- **remote** — ネットワーク上のサーバに保存される

この MIB は、特に設定に関係する操作だけを含みますが、一般的なファイル保存と転送には一部のシステム機能を使用できます。

CISCO-CONTENT-ENGINE-MIB

これは、シスコシステムズの MIB モジュールです。

CISCO-ENTITY-ASSET-MIB

この MIB は、ENTITY-MIB （RFC 2037）entPhysicalTable の資産情報項目を監視します。この MIB は、MIBentPhysicalTable に表示される関連するエンティティの注文可能製品番号、シリアル番号、ハードウェア リビジョン、製造番号およびリビジョン、ファームウェア ID およびリビジョン（存在する場合）およびソフトウェア ID およびリビジョン（存在する場合）を表示します。

このデータが使用できないエンティティは、この MIB に表示されません。この MIB の表はほとんど埋まっていないので、特定の時点で特定のエンティティに一部の変数が存在しない場合があります。たとえば、電源が入っていないモジュールを示す行は、ソフトウェア ID （ceAssetSoftwareID）とリビジョン（ceAssetSoftwareRevision）に値がない場合があります。同様に、電源モジュールは、表にファームウェアやソフトウェア情報が表示されません。

データに他の項目が埋め込まれている場合がありますが（シリアル番号の中の製造日付など）、すべてのデータ項目を 1 つの単位と見なします。項目を分解したり、項目を構文解析しないでください。文字列の等価および非等価演算だけを使用してください。

ENTITY-MIB

これは、1 つの SNMP エージェントがサポートする複数の論理エンティティを表すための MIB モジュールです。

EVENT-MIB

この MIB は、ネットワーク管理目的でイベント トリガーと処理を定義します。MIB は、RFC 2981 として公開されています。

HOST-RESOURCES-MIB

この MIB は、ホスト システムを管理します。「ホスト」という用語は、インターネットに接続している他の同様なコンピュータと通信する任意のコンピュータを示します。
HOST-RESOURCES-MIB は、通信サービスが主な機能であるデバイス（ターミナル サーバ、ルータ、ブリッジ、監視機器）に必ずしも適用されるわけではありません。この MIB は、すべてのインターネット ホスト（たとえば、パーソナル コンピュータや UNIX が稼動するシステム）に共通の属性を提供します。

MIB-II

MIB-II は、インターネット標準 MIB です。MIB-II は、RFC 1213 に規定され、TCP/IP に基づくインターネットのネットワーク管理プロトコル用です。

WAAS デバイスへの MIB ファイルのダウンロード

WAAS ソフトウェアを稼働する WAAS デバイスによってサポートされる MIB はすべて、MIB ファイルを次の Cisco FTP サイトからダウンロードできます。

ftp://ftp.cisco.com/pub/mibs/v2

各 MIB に定義されている MIB オブジェクトは、上記 FTP サイトの MIB ファイルに、一目でわかる形で記述されています。

WAAS デバイス上の SNMP エージェントの有効化

デフォルトでは、WAAS デバイス上の SNMP エージェントが無効になっており、SNMP コミュニティ ストリングは定義されていません。SNMP コミュニティ ストリングは、WAAS デバイス上の SNMP エージェントへアクセスするときに、認証用のパスワードとして使用されます。認証されるには、WAAS デバイスに送信された SNMP メッセージの Community Name フィールドが、WAAS デバイスに定義された SNMP コミュニティ ストリングに一致している必要があります。

デバイスに SNMP コミュニティ ストリングを定義すると、WAAS デバイス上の SNMP エージェントが有効になります。WAAS Central Manager GUI を使用すると、デバイスまたはデバイス グループに SNMP コミュニティ ストリングを定義できます。

SNMP 要求に SNMPv3 プロトコルが使用されている場合は、次のステップで、SNMP ユーザ アカウントを定義します。このアカウントは、SNMP を使用して WAAS デバイスにアクセスするために使用できます。WAAS デバイスで SNMPv 3 ユーザ アカウントを作成する方法の詳細については、16-17 ページの「SNMP ユーザの作成」を参照してください。

SNMP を設定するためのチェックリスト

表 16-2 で、WAAS デバイスまたはデバイス グループで SNMP 監視を有効にするためのプロセスについて説明します。

表 16-2　SNMP を設定するためのチェックリスト

作業	追加情報と手順
1. SNMP 監視の準備をする。	詳細については、16-8 ページの「SNMP 監視用の準備」を参照してください。
2. 有効にしたい SNMP トラップを選択する。	WAAS Central Manager は、WAAS デバイスまたはデバイス グループで有効にできるさまざまなトラップを提供しています。 詳細については、16-8 ページの「SNMP トラップの有効化」を参照してください。
3. SNMP トラップを受信する SNMP ホストを指定する。	WAAS デバイスまたはデバイス グループがトラップを送信する必要がある SNMP ホストを指定します。異なる WAAS デバイスが異なるホストへトラップを送信できるように、複数のホストを指定できます。 詳細については、16-11 ページの「SNMP ホストの指定」を参照してください。
4. SNMP コミュニティ ストリングを指定する。	外部ユーザが MIB の読み取りまたは書き込みを実行できるように、SNMP コミュニティ ストリングを指定します。 詳細については、16-12 ページの「SNMP コミュニティ ストリングの指定」を参照してください。
5. SNMP ビューを設定する。	SNMP グループを特定のビューに制限するには、グループに表示したい MIB サブツリーを指定するビューを作成する必要があります。 詳細については、16-14 ページの「SNMP ビューの作成」を参照してください。
6. SNMP グループを作成する。	任意の SNMP ユーザを作成する、またはグループが特定の MIB サブツリーを表示するように制限したい場合は、SNMP グループを設定する必要があります。 詳細については、16-15 ページの「SNMP グループの作成」を参照してください。
7. SNMP ユーザを作成する。	SNMP 要求に SNMPv3 プロトコルが使用されている場合は、SNMP を使用して WAAS デバイスにアクセスするために、少なくとも 1 つの SNMPv3 ユーザ アカウントを WAAS デバイスに定義する必要があります。 詳細については、16-17 ページの「SNMP ユーザの作成」を参照してください。
8. SNMP 連絡先設定を構成する。	詳細については、16-19 ページの「SNMP 連絡先設定の構成」を参照してください。

SNMP 監視用の準備

SNMP 監視用に WAAS ネットワークを設定する前に、次の準備作業を完了します。

- WAAS デバイスが SNMP トラップを送信するために使用する SNMP ホスト（管理ステーション）を設定します。
- すべての WAAS デバイスがトラップを同じホストへ送信するか、異なるホストへ送信するかを決定します。各 SNMP ホストの IP アドレスまたはホスト名を書き留めます。
- SNMP エージェントにアクセスするために使用するコミュニティ ストリングを入手します。
- グループ別にビューを制限できるように SNMP グループを作成するかどうかを決定します。

SNMP トラップの有効化

WAAS デバイスが SNMP トラップを送信できるようにするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。選択に応じて、[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP トラップを設定したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。[Device Home] ウィンドウが表示され、左側に [Contents] ペインが表示されます。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[General Settings]** を選択します。[SNMP General Settings] ウィンドウが表示されます（図 16-2 を参照してください）。表 16-3 で、このウィンドウのフィールドについて説明します。

図 16-2　[SNMP General Settings] ウィンドウ

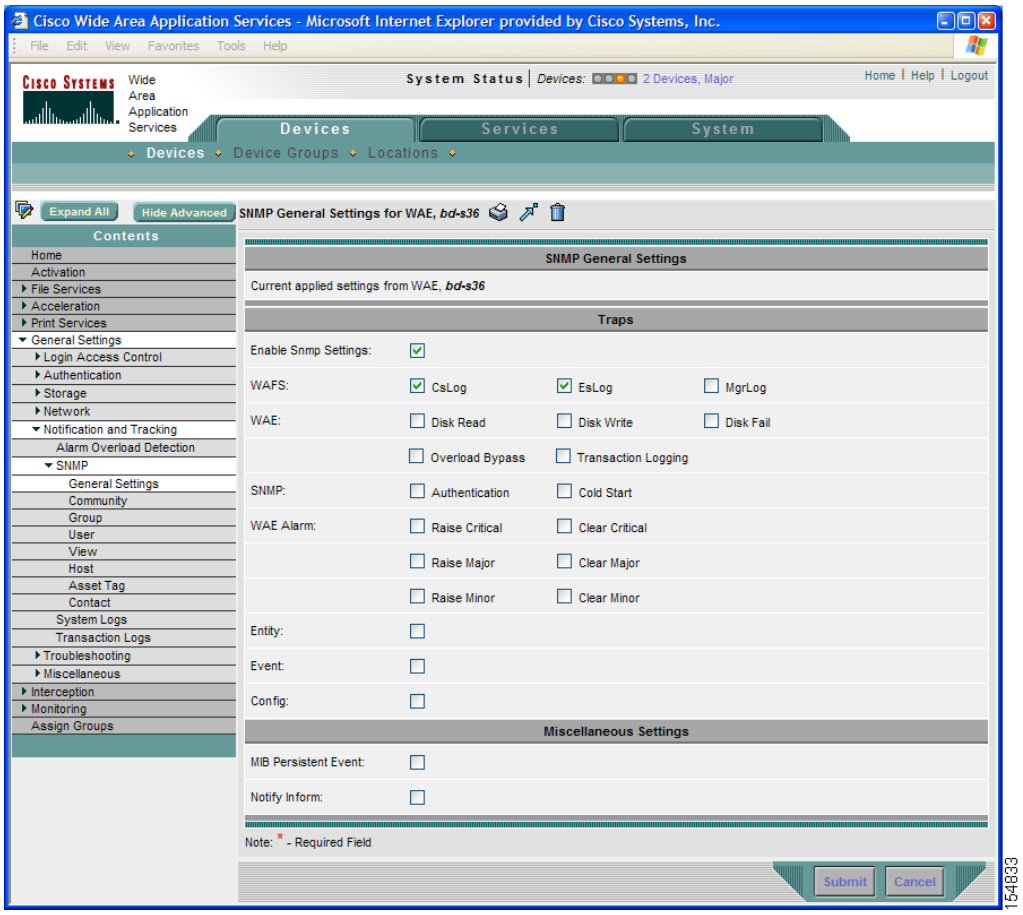


表 16-3　SNMP 一般設定

GUI パラメータ	機能
トラップ	
Snmp 設定を有効にします。	SNMP トラップを有効にします。
WAFS	SNMP WAFS トラップを有効にします。 • **CsLog** — コア サーバ エラー トラップを有効にします。 • **EsLog** — エッジ サーバ エラー トラップを有効にします。 • **MgrLog** — WAAS Central Manager エラー トラップを有効にします。
WAE	SNMP WAFS トラップを有効にします。 • **Disk Read** — ディスク読み取りエラー トラップを有効にします。 • **Disk Write** — ディスク書き込みエラー トラップを有効にします。 • **Disk Write** — ディスク障害エラー トラップを有効にします。 • **Overload Bypass** —WCCP 過負荷迂回エラー トラップを有効にします。 • **Transaction Logging** — トランザクション ログ書き込みエラー トラップを有効にします。

表 16-3　SNMP 一般設定 （続き）

GUI パラメータ	機能
SNMP	SNMP 固有トラップを有効にします。 • **Authentication** — 認証トラップを有効にします。 • **Cold Start** — コールド スタート トラップを有効にします。
WAE アラーム	SNMP アラーム トラップを有効にします。 • **Raise Critical** — 重度アラーム設定トラップを有効にします。 • **Clear Critical** — 重度アラーム消去トラップを有効にします。 • **Raise Major** — 中度アラーム設定トラップを有効にします。 • **Clear Major** — 中度アラーム消去トラップを有効にします。 • **Raise Minor** — 軽度アラーム設定トラップを有効にします。 • **Clear Minor** — 軽度アラーム消去トラップを有効にします。
エンティティ	SNMP エンティティ トラップを有効にします。
イベント	イベント MIB を有効にします。
設定	CiscoConfigManEvent エラー トラップを有効にします。
その他の設定	
MIB 永続イベント	SNMP Event MIB の永続性を有効にします。
Notify Inform	SNMP notify inform 要求を有効にします。inform 要求は、トラップより信頼性に優れていますが、ルータとネットワークのリソース使用量が増えます。 受信者がトラップを受信したときに受信確認を送信しないため、トラップの信頼性は低くなります。送信側は、トラップが受信されたかどうかを決定できません。ただし、inform 要求を受信する SNMP マネージャは、SNMP 応答でメッセージの受信を確認します。送信側が応答を受信しない場合、inform 要求を再び送信できます。したがって、inform 要求が意図した送信先に到達する可能性が高くなります。

ステップ 5　SNMP トラップを有効にするには、適切なチェック ボックスを選択します。

ステップ 6　**[Submit]** をクリックします。

デフォルトまたはデバイス グループ設定を適用した後でまだ保存されていない変更があると、現在の設定の横に、"Click Submit to Save" メッセージが赤い色で表示されます。また、**[Reset]** をクリックすると、すでに設定したウィンドウ設定に戻すことができます。[Reset] ボタンは、デフォルトまたはデバイス グループ設定を適用して現在のデバイス設定を変更し、まだ設定を送信していない場合だけ表示されます。

CLI から SNMP トラップを有効にするには、**snmp-server enable traps** グローバル設定コマンドを使用できます。**snmp trigger** EXEC コマンドを使用すると、特定の設定に関連するその他の MIB オブジェクトについて追加の SNMP トラップを定義できます。

SNMP ホストの指定

ホストは、作成順に表示されます。作成できる SNMP ホストの最大数は 4 です。

SNMP ホストを指定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP ホストを定義したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。[Device Home] ウィンドウまたは [Modifying Device Groups] ウィンドウが表示されます。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[Host]** を選択します。[SNMP Hosts] ウィンドウが表示されます。

ステップ 5　タスクバーで、**[Create New SNMP Host]** アイコンをクリックします。[Creating New SNMP Host] ウィンドウが表示されます。表 16-4 で、このウィンドウのフィールドについて説明します。

表 16-4　SNMP ホスト設定

GUI パラメータ	機能
トラップ ホスト	WAE から SNMP トラップ メッセージで送信される SNMP トラップ ホストのホスト名または IP アドレス。これは必須フィールドです。
コミュニティ / ユーザ	WAE から SNMP トラップ メッセージで送信される SNMP コミュニティまたはユーザの名前（最大 256 文字）。これは必須フィールドです。
認証	SNMP トラップ動作の受信者へ通知を送信するために使用するセキュリティ モデル。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。 • **[No-auth]** — セキュリティ メカニズムなしで通知を送信します。 • **[v2c]** — バージョン 2c セキュリティを使用して通知を送信します。 • **[v3-auth]** — SNMP バージョン 3 AuthNoPriv を使用して通知を送信します。 • **[v3-noauth]** — SNMP バージョン 3 NoAuthNoPriv を使用して通知を送信します。 • **[v3-priv]** — SNMP バージョン 3 AuthPriv を使用して通知を送信します。
再試行	inform 要求に許される再試行回数（1 ～ 10）。デフォルトは、2 回です。
タイムアウト	inform 要求のタイムアウト（1 ～ 1000 秒）。デフォルトは 15 秒です。

ステップ 6　SNMP トラップ ホストのホスト名または IP アドレス、SNMP コミュニティまたはユーザ名、通知を送信するためのセキュリティ モデル、および inform 要求の再試行回数とタイムアウトを入力します。

ステップ 7　**[Submit]** をクリックします。

CLI から SNMP ホストを指定するには、**snmp-server host** グローバル設定コマンドを使用できます。

SNMP コミュニティ ストリングの指定

SNMP コミュニティ ストリングは、WAAS デバイスに存在する SNMP エージェントにアクセスするために使用するパスワードです。コミュニティ ストリングには、2 つの種類があります。group と read-write です。コミュニティ ストリングは、SNMP メッセージのセキュリティを強化します。

コミュニティ ストリングは、作成順に表示されます。 作成できる SNMP コミュニティの最大数は 10 です。デフォルトでは、SNMP エージェントは無効で、コミュニティ ストリングは設定されていません。コミュニティ ストリングを設定すると、デフォルトですべてのエージェントへの読み取り専用アクセスが許可されます。

SNMP エージェントを有効にし、SNMP エージェントにアクセスできるコミュニティ ストリングを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP コミュニティ設定を構成したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。[Contents] ペインが左側に表示されます。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[Community]** を選択します。[SNMP Community Strings] ウィンドウが表示されます。

ステップ 5　タスクバーで、**[Create New SNMP Community String]** アイコンをクリックします。[Creating New SNMP Community String] ウィンドウが表示されます。表 16-5 で、このウィンドウのフィールドについて説明します。

表 16-5　SNMP コミュニティ設定

GUI パラメータ	機能
コミュニティ	WAE の SNMP エージェントにアクセスするときに認証用のパスワードとして使用するコミュニティ ストリング。認証されるには、WAE に送信された SNMP メッセージの "Community Name" フィールドが、ここで定義した SNMP コミュニティ ストリングに一致している必要があります。コミュニティ ストリングを入力すると、WAE 上の SNMP エージェントが有効になります。このフィールドには、最大 256 文字を入力できます。 これは必須フィールドです。

表 16-5　SNMP コミュニティ設定 （続き）

GUI パラメータ	機能
グループ名 /rw	コミュニティ ストリングが属するグループ。[Read/Write] オプションを使用すると、このコミュニティ ストリングに read または write グループを関連付けることができます。[Read/Write] オプションは、MIB サブツリーの一部へのアクセスだけを許可します。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。 • **[None]** — コミュニティ ストリングに関連付けるグループ名を指定したくない場合は、このオプションを選択します。このオプションを選択すると、[Group Name] フィールドは無効のままになります。 • **[Group]** — グループ名を指定したい場合は、このオプションを選択します。 • **[Read/Write]** — コミュニティ ストリングに関連付けられたグループへの読み取り / 書き込みアクセスを許可したい場合は、このオプションを選択します。このオプションを選択すると、[Group Name] フィールドは無効のままになります。 これは必須フィールドです。
グループ名	コミュニティ ストリングが属するグループの名前。このフィールドには、最大 256 文字を入力できます。このフィールドは、前のフィールドで [Group] オプションを選択した場合のみ使用できます。

ステップ 6　適切なフィールドに、コミュニティ ストリングを入力し、グループへの読み取り / 書き込みアクセスを許可するかどうかを選択し、グループ名を入力します。

ステップ 7　**[Submit]** をクリックします。

CLI からコミュニティ ストリングを設定するには、**snmp-server community** グローバル設定コマンドを使用できます。

SNMP ビューの作成

ユーザのグループを特定の MIB ツリーを表示するだけに制限するには、WAAS Central Manager GUI を使用して SNMP ビューを作成する必要があります。ビューを作成したら、後の項の説明に従って、このグループに属する SNMP グループと SNMP ユーザを作成する必要があります。

ビューは、作成順に表示されます。作成できるビューの最大数は 10 です。

バージョン 2 SNMP （SNMPv2）MIB ビューを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMPv2 ビューを作成したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[View]** を選択します。[SNMP Views] ウィンドウが表示されます。

ステップ 5　タスクバーで、**[Create New View]** アイコンをクリックします。[Creating New SNMP Host] ウィンドウが表示されます。表 16-6 で、このウィンドウのフィールドについて説明します。

表 16-6　SNMPv2 ビュー設定

GUI パラメータ	機能
名前	このファミリのビュー サブツリーの名前を表す文字列（最大 256 文字）。ファミリ名は、ENTITY-MIB のような有効な MIB 名である必要があります。これは必須フィールドです。
ファミリ	MIB のサブツリーを識別するオブジェクト ID （最大 256 文字）。これは必須フィールドです。
ビュータイプ	ビューから MIB ファミリを包含するか、除外するかを決定するビュー オプション。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。 • **[Included]** — MIB ファミリをビューに入れます。 • **[Excluded]** — MIB ファミリをビューから除外します。

ステップ 6　適切なフィールドに、ビュー名、ファミリ名、およびビューの種類を入力します。

ステップ 7　**[Submit]** をクリックします。

ステップ 8　後の項の説明に従って、このビューに割り当てる SNMP グループを作成します。

CLI から SNMP ビューを作成するには、**snmp-server view** グローバル設定コマンドを使用できます。

SNMP グループの作成

任意の SNMP ユーザを作成する、またはユーザのグループが特定の MIB サブツリーを表示するように制限したい場合は、SNMP グループを設定する必要があります。

グループは、作成順に表示されます。作成できる SNMP グループの最大数は 10 です。

ユーザ セキュリティ モデル グループを定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP グループを作成したい デバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。[Device Home] ウィンドウまたは [Modifying Device Group] ウィンドウが表示されます。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[Group]** を選択します。[SNMP Group Strings for WAE] ウィンドウが表示されます。

ステップ 5　タスクバーで、**[Create New SNMP Group String]** アイコンをクリックします。[Creating New SNMP Group String for WAE] ウィンドウが表示されます。表 16-7 で、このウィンドウのフィールドについて説明します。

表 16-7　SNMP グループ設定

GUI パラメータ	機能
名前	SNMP グループの名前。最大 256 文字を入力できます。これは必須フィールドです。
Sec モデル	グループ用のセキュリティ モデル。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。 • **[v1]** — バージョン 1 セキュリティ モデル（SNMP バージョン 1 [noAuthNoPriv]） • **[v2c]** — バージョン 2 セキュリティ モデル（SNMP バージョン 2 [noAuthNoPriv]） • **[v3-auth]** — ユーザ セキュリティ レベル SNMP バージョン 3 AuthNoPriv • **[v3-noauth]** — ユーザ セキュリティ レベル SNMP バージョン 3 noAuthNoPriv • **[v3-priv]** — ユーザ セキュリティ レベル SNMP バージョン 3 AuthPriv **（注）** SNMPv1 または SNMPv2c セキュリティ モデルにしたがって定義されたグループは、SNMP ユーザには関連付けないでください。それらは、コミュニティ ストリングだけに関連付ける必要があります。

表 16-7　SNMP グループ設定 （続き）

GUI パラメータ	機能
読み取りビュー	エージェントの内容を表示できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。グループのユーザに読み取りアクセスを提供するには、ビューを指定する必要があります。 SNMP ビューを作成する方法については、16-14 ページの「SNMP ビューの作成」を参照してください。
書き込みビュー	データを入力し、エージェントの内容を設定できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。 SNMP ビューを作成する方法については、16-14 ページの「SNMP ビューの作成」を参照してください。
通知ビュー	notify、inform、または trap を指定できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。 SNMP ビューを作成する方法については、16-14 ページの「SNMP ビューの作成」を参照してください。

ステップ 6　適切なフィールドに、SNMP グループ設定名、セキュリティ モデル、および読み取り、書き込み、および通知ビューの名前を入力します。

ステップ 7　**[Submit]** をクリックします。

ステップ 8　後の項の説明に従って、この新しいグループに属する SNMP ユーザを作成します。

CLI から SNMP グループを作成するには、**snmp-server group** グローバル設定コマンドを使用できます。

SNMP ユーザの作成

ユーザは、作成順に表示されます。作成できるユーザの最大数は 10 です。

SNMP エンジンにアクセスできるユーザを定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP ユーザを作成したい デバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[User]** を選択します。デバイスまたはデバイス グループ用の SNMP ユーザのリストが表示されます。

ステップ 5　タスクバーで、**[Create New SNMP User]** アイコンをクリックします。[Creating New SNMP User] ウィンドウが表示されます。表 16-8 で、このウィンドウのフィールドについて説明します。

表 16-8　SNMP ユーザ設定

GUI パラメータ	機能
名前	デバイスまたはデバイス グループにアクセスできるユーザ名を表す文字列（最大 256 文字）。これは必須フィールドです。
グループ	ユーザが属するグループの名前（最大 256 文字）。これは必須フィールドです。
リモート SNMP ID	リモート SNMP エンティティ用のグローバル固有識別情報。SNMPv3 メッセージを WAE へ送信するには、WAE にリモート SnmpID を持つ少なくとも 1 人のユーザを設定する必要があります。SnmpID は、オクテット文字列形式で入力する必要があります。
認証アルゴリズム	送信中の SNMP パケットの完全性を保証する認証アルゴリズム。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。 • **[No-auth]** — SNMP パケット用にセキュリティ メカニズムをオンにする必要がありません。 • **[MD5]** — ハッシュに基づくメッセージ認証コード MD5（HMAC-MD5）アルゴリズムに基づく認証を提供します。 • **[SHA]** — ハッシュに基づくメッセージ認証コード安全なハッシュ（HMAC-SHA）アルゴリズムに基づく認証を提供します。
認証パスワード	ユーザ認証（HMAC-MD5 または HMAC-SHA）パスワードを設定する文字列（最大 256 文字）。表示制限を超える場合、文字数が表示領域に合わせて調整されます。 認証アルゴリズム用に **no-auth** オプションを選択した場合、このフィールドはオプションです。そうでない場合は、このフィールドに値を入力する必要があります。
確認パスワード	確認用の認証パスワード。再入力するパスワードは、前のフィールドに入力したパスワードと同じである必要があります。

表 16-8　SNMP ユーザ設定 （続き）

GUI パラメータ	機能
私用パスワード	SNMP エージェントが SNMP ホストからパケットを受信できるようにする認証（HMAC-MD5 または HMAC-SHA）パラメータを設定する文字列（最大 256 文字）。表示制限を超える場合、文字数が表示領域に合わせて調整されます。
確認パスワード	確認用の私用パスワード。再入力するパスワードは、前のフィールドに入力したパスワードと同じである必要があります。

ステップ 6　適切なフィールドに、ユーザ名、ユーザが属するグループ、ユーザが属するリモート エンティティのエンジン ID、SNMP トラフィックの改ざんから保護するために使用する認証アルゴリズム、ユーザ認証パラメータ、およびパケット用の認証パラメータを入力します。

ステップ 7　**[Submit]** をクリックします。

CLI から SNMP ユーザを作成するには、**snmp-server user** グローバル設定コマンドを使用できます。

SNMP 資産タグ設定の構成

CISCO-ENTITY-ASSET-MIB に値を作成する SNMP 資産タグ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP 資産タグを定義したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。[Device Home] ウィンドウまたは [Modifying Device Groups] ウィンドウが表示されます。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[Asset Tag]** を選択します。[SNMP Asset Tag Settings] ウィンドウが表示されます。

ステップ 5　[Asset Tag Name] フィールドに、資産タグの名前を入力します。

ステップ 6　**[Submit]** をクリックします。

CLI から SNMP 資産タグ設定を構成するには、**asset tag** グローバル設定コマンドを使用できます。

SNMP 連絡先設定の構成

SNMP 連絡先設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices]**、**[Devices]** または **[Devices]**、**[Device Groups]** を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP 連絡先を設定したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。[Device Home] ウィンドウまたは [Modifying Device Groups] ウィンドウが表示されます。

ステップ 3　**[Show Advanced]** をクリックして、[Contents] ペインにすべてのメニュー項目を表示します。

ステップ 4　[Contents] ペインで、**[General Settings]**、**[Notification and Tracking]**、**[SNMP]**、**[Contact]** を選択します。[SNMP Contact Settings] ウィンドウが表示されます。

ステップ 5　提供されるフィールドに、連絡先の氏名と住所を入力します。

ステップ 6　**[Submit]** をクリックします。

CLI から SNMP 連絡先設定を構成するには、**snmp-server contact** グローバル設定コマンドを使用できます。