SNMP

この章では、ネットワークデバイスを管理する方法を提供する Simple Network Management Protocol（SNMP）機能について説明します。ここで説明する内容は、次のとおりです。

- エンジン ID （1 ページ）
- SNMP ビュー （3 ページ）
- SNMP グループ （4 ページ）
- SNMP ユーザー （5 ページ）
- SNMP コミュニティ （7 ページ）
- トラップの設定 （9 ページ）
- 通知受信者SNMPv1、2 （10 ページ）
- 通知受信者SNMPv3 （12 ページ）
- 通知フィルタ （13 ページ）

エンジン ID

エンジン ID は、それらを一意に識別するために SNMPv3 エンティティによって使用されます。SNMPエージェントは、正規のSNMPエンジンと見なされます。つまり、エージェントが着信メッセージ（Get、GetNext、GetBulk、Set）に応答して、マネージャにトラップ メッセージを送信します。エージェントのローカル情報は、メッセージ内のフィールドにカプセル化されます。

各SNMPエージェントは、SNMPv3メッセージ交換で使用されるローカル情報を保持します。デフォルトの SNMP エンジン ID は、エンタープライズ番号とデフォルトの MAC アドレスで構成されます。このエンジン ID は、ネットワーク内の 2 台のデバイスが同じエンジン ID を持つことがないように、管理ドメインで一意である必要があります。

ローカル情報は読み取り専用の 4 つの MIB 変数に保存されます（snmpEngineId、snmpEngineBoots、snmpEngineTime、および snmpEngineMaxMessageSize）。

⚠

注意 エンジン ID を変更すると、設定されているすべてのユーザーが消去されます。

SNMP エンジン ID を設定するには、次の手順を実行します。

手順

ステップ 1 [SNMP] > [Engine ID] をクリックします。

ステップ 2 [Local Engine ID] に次のどちらを使用するかを選択します。

- デフォルトを使用（Use Default）：デバイスによって生成されたエンジン ID を使用することを選択します。デフォルトのエンジン ID は、デバイスの MAC アドレスを基にして生成されています。
- なし（None）：エンジン ID は使用されません。
- ユーザ定義（User Defined）：ローカル デバイスのエンジン ID を入力します。フィールド値は 16 進数文字列（範囲：10 ～ 64）です。16 進数文字列の各バイトは、2 桁の 16 進数で表されます。

  リモートのエンジン ID テーブルでは、すべてのリモート エンジン ID とその IP アドレスが表示されます。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

リモートエンジン ID テーブルは、エンジンの IP アドレスとエンジン ID の間のマッピングを示します。

エンジン ID の IP アドレスを追加するには：

ステップ 4 [Add] をクリックします。次のフィールドに入力します。

- サーバ定義（Server Definition）：IP アドレスまたは名前によってエンジン ID サーバを指定するかどうかを選択します。
- [IP バージョン]：サポートする IP 形式を選択します。
- [IPv6 Address Type]：IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能なグローバル ユニキャスト IPv6 タイプになります。
- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイス（IPv6 アドレス タイプとしてリンク ローカルが選択されている場合）を選択します。
- サーバ IP アドレス/名前（Server IP Address/Name）：IP アドレスまたはログ サーバのドメイン名を入力します。
- [Engine ID]：エンジン ID を入力します。

ステップ 5 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

SNMP ビュー

ビューは、MIB サブツリーの集合のためのユーザ定義のラベルです。各サブツリー ID は、関連するサブツリーのルートのオブジェクト ID（OID）によって定義されます。目的のサブツリーのルートを指定するには、既知の名前を使用するか、または、OID を入力します。ビューページでは、SNMP ビューの作成および編集が有効です。デフォルトのビュー（Default および DefaultSuper）を変更することはできません。

ビューは、グループにアタッチすることも、基本アクセスモードを使用するコミュニティにアタッチする（SNMP グループ （4 ページ）を使用）こともできます。

SNMP ビューを設定するには、次の手順を実行します。

手順

ステップ 1 [SNMP] > [Views] をクリックします。

ステップ 2 [Add] をクリックし、新しいビューを定義します。

ステップ 3 パラメータを入力します。

- [View Name]：0 ～ 30 文字でビューの名前を入力します。
- オブジェクト ID サブツリー（Object ID Subtree）：選択した SNMP ビューに含まれるか除外される MIB ツリー内のノードを選択します。オブジェクトを選択するオプションは次のとおりです。
  - リストから選択（Select from list）：MIB ツリーを移動できるようになります。
  - ユーザ定義（User Defined）：[Select from list] オプションで提供されていない OID を入力します。

ステップ 4 [Include in view] を選択または選択解除します。これを選択すると、選択した MIB はビューに含まれ、そうでないものは除外されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 ビューの設定を確認するには、[Filter: View Name] リストからユーザ定義のビューを選択します。

- デフォルト（Default）：読み取りおよび読み取り/書き込みビューのデフォルトの SNMP ビューです。
- DefaultSuper：管理者ビューのデフォルトの SNMP ビューです。

SNMP グループ

SNMPv1 および SNMPv2 では、コミュニティストリングは、SNMP フレームとともに送信されます。コミュニティストリングは、SNMP エージェントにアクセスするためのパスワードとして機能します。ただし、フレームもコミュニティストリングも暗号化されません。したがって、SNMPv1 と SNMPv2 は安全ではありません。

SNMPv3 では、次のセキュリティ メカニズムを設定することができます。

- 認証（Authentication）：デバイスは SNMP ユーザが承認済みシステム管理者であることを確認します。これは、フレームごとに実行されます
- プライバシー（Privacy）：SNMP フレームは暗号化されたデータを伝送できます。

したがって、SNMPv3 では、3 つのレベルのセキュリティがあります。

- セキュリティなし（認証なし、プライバシーなし）
- 認証（認証あり、プライバシーなし）
- 認証およびプライバシー

SNMPv3 では、各ユーザが読み取りまたは書き込みできるコンテンツと、ユーザが受信する通知を制御する手段を提供します。グループは、読み取り/書き込み権限とセキュリティのレベルを定義します。グループは、SNMP ユーザーまたはコミュニティに関連付けられている場合に機能します。

（注） グループにデフォルト以外のビューを関連付けるには、まずSNMP ビュー （3 ページ）でビューを作成します。

SNMP グループを作成するには、次の手順を実行します。

手順

ステップ 1 [SNMP] > [Groups] をクリックします。

このページには、既存の SNMP グループおよびセキュリティ レベルが含まれています。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [Group Name]：新しいグループ名を入力します。
- セキュリティ モデル（Security Model）：グループ、SNMPv1、v2、v3 にアタッチされる SNMP バージョンを選択します。

さまざまなセキュリティ レベルの、3 つのタイプのビューを定義できます。セキュリティレベルごとに、以下のフィールドを入力して、読み取り、書き込み、通知用のビューを選択します。

- 有効化（Enable）：セキュリティ レベルを有効にするには、このフィールドを選択します。
- セキュリティ レベル（Security Level）：グループにアタッチするセキュリティ レベルを定義します。SNMPv1 および SNMPv2 は、認証もプライバシーもサポートしません。SNMPv3 を選択する場合、次のいずれかを選択します。
  - 認証なし、プライバシーなし（No Authentication and No Privacy）：認証とプライバシーのどちらのセキュリティ レベルもグループに割り当てられません。
  - [Authentication and No Privacy]：SNMP メッセージが認証され、SNMP メッセージの送信元が保証されますが、メッセージは暗号化されません。
  - 認証およびプライバシー（Authentication and Privacy）：SNMP メッセージを認証し、それらを暗号化します。
- ビュー（View）：選択すると、ビューに読み取り、書き込み、通知アクセスが関連付けられます。グループのアクセス権限は、グループに読み取り、書き込み、および通知アクセスがある MIB ツリーの範囲を制限します。
  - 読み取り（Read）：管理アクセスは、選択したビューの読み取り専用です。そうでない場合、このグループに関連付けられているユーザまたはコミュニティが、SNMP 自体を制御するものを除くすべての MIB を読み取ることができます。
  - [Write]：選択したビューに対する管理アクセス権限は、書き込みです。そうでない場合、このグループに関連付けられているユーザまたはコミュニティが、SNMP 自体を制御するものを除くすべての MIB を書き込むことができます。
  - 通知（Notify）：選択したビューに含まれるものにトラップの使用可能な内容が制限されます。それ以外の場合、トラップの内容は制限されません。これは、SNMPv3 でのみ選択できます。

ステップ 4 [Apply] をクリックします。SNMP グループは実行コンフィギュレーション ファイルに保存されます。

SNMP ユーザー

SNMPユーザは、ログイン クレデンシャル（ユーザ名、パスワード、および認証方式）と、グループおよびエンジン ID との関連付けによって動作するコンテキストおよび範囲によって定義されます。設定されたユーザーには、そのグループの属性が設定され、関連付けられたビュー内でアクセス権限が設定されます。

SNMPv3 ユーザを作成するには、まず次が存在しなければなりません。

- エンジン ID をデバイスで最初に設定する必要があります。これは、エンジン ID （1 ページ）で設定します。

- SNMPv3 グループが使用可能でなければなりません。SNMPv3 グループは、SNMP グループ （4 ページ）で定義します。

SNMP ユーザを表示し、新規で定義するには：

手順

ステップ 1 [SNMP] > [Users] をクリックします。

このページには、既存のユーザが表示されます。このページのフィールドは、次のフィールドを除いて [Add] ページで説明されています。

- IP アドレス（IP Address）：エンジンの IP アドレスを表示します。

ステップ 2 [Add] をクリックします。

このページは、SNMP ユーザに SNMP アクセス制御権限を割り当てるための情報を提供します。

ステップ 3 パラメータを入力します。

- [User Name]：ユーザーの名前を入力します。
- エンジン ID（Engine ID）：ユーザを接続するローカルまたはリモート SNMP エンティティを選択します。ローカル SNMP エンジン ID を変更または削除すると、SNMPv3 ユーザ データベースが削除されます。通知メッセージを受信して情報をリクエストするには、ローカルおよびリモート ユーザの両方を定義する必要があります。
  - ローカル（Local）：ユーザはローカルのデバイスに接続されます。
  - リモート IP アドレス（Remote IP Address）：ユーザはローカルのデバイスだけでなく、別の SNMP エンティティに接続されます。リモートエンジン ID が定義されている場合、リモートデバイスはインフォームメッセージを受信できますが、情報を要求することはできません。
- グループ名（Group Name）：SNMP ユーザが所属する SNMP グループを選択します。SNMP グループは、[Add Group] ページで定義されます。

  （注）
  削除されたグループに属しているユーザーは残りますが、アクティブではありません。

- [Authentication Method]：認証方式を選択します。認証方式は、割り当てられたグループ名に応じて異なります。グループの認証が不要な場合、ユーザーは認証を設定できません。次のオプションがあります。
  - [None]：ユーザー認証は使用されません。
  - [SHA]：SHA-1（セキュア ハッシュ アルゴリズム）認証方式でキーを生成するために使用されるパスワード。
  - [SHA224]：SHA-224（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 128 ビットに切り捨てたキーを生成するために使用されるパスワード。

- [SHA256]：SHA-256（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 192 ビットに切り捨てたキーを生成するために使用されるパスワード。
- [SHA384]：SHA-384（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 256 ビットに切り捨てたキーを生成するために使用されるパスワード。
- [SHA512]：SHA-512（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 384 ビットに切り捨てたキーを生成するために使用されるパスワード。

- [Authentication Password]：パスワードおよび認証方式を使用して認証を行う場合は、ローカルユーザーパスワードを [Encrypted] または [Plaintext] のいずれかに入力します。ローカルユーザーパスワードはローカルデータベースと比較され、最大 32 文字の ASCII 文字を含めることができます。
- プライバシー方式（Privacy Method）：次のいずれかのオプションを選択できます。
  - [None]：プライバシーパスワードは暗号化されません。
  - [AES]：プライバシーパスワードは AES に従って暗号化されます。
- [Privacy Password]：AES プライバシー方式を選択した場合は、16 バイト（AES 暗号キー）が必要です。このフィールドは、ちょうど 32 文字の 16 進数でなければなりません。暗号化モードまたはプレーンテキストモードを使用するオプションがあります。

ステップ 4 [Apply] をクリックして設定を保存します。

SNMP コミュニティ

SNMPv1 および SNMPv2 のアクセス権限は、[Communities] ページでコミュニティを定義することによって管理されます。コミュニティ名とは、SNMP 管理ステーションとデバイスの間で共有されるパスワードの一種です。SNMP 管理ステーションの認証に使用されます。

SNMPv3 はコミュニティではなくユーザと連携するため、コミュニティは SNMPv1 および v2 でのみ定義されます。ユーザは、アクセス権が割り当てられているグループに属します。[Communities] ページは、コミュニティにアクセス権を直接（基本モード）またはグループを通じて（拡張モード）関連付けます。

- 基本モード：コミュニティのアクセス権限は、読み取り専用、読み取り/書き込み、SNMP 管理者のいずれかに設定できます。また、SNMP ユーザー （5 ページ）で定義されたビューを選択することで、コミュニティへのアクセスを、特定の MIB オブジェクトのみに制限できます。
- 拡張モード：コミュニティのアクセス権限は、SNMP グループ （4 ページ）で定義されたグループによって定義されます。特定のセキュリティ モデルを持つグループを設定できます。グループのアクセス権限は、読み取り、書き込み、および通知です。

SNMP コミュニティを定義するには、次の手順を実行します。

手順

ステップ 1 [SNMP] > [Communities] をクリックします。

ステップ 2 [Add] をクリックして、新しい SNMP コミュニティを定義および設定します。

ステップ 3 次のフィールドを設定します。

SNMP Management Station	次のオプションのいずれかを選択します。 • [All]：すべての IP デバイスが SNMP コミュニティにアクセスできることを示します。 • [User Defined]：SNMP コミュニティにアクセスできる管理ステーションの IP アドレスを入力します。
IP Version	[IPv4] または [IPv6] を選択します。
IPv6 Address Type	サポートされる IPv6 アドレスタイプを選択します（IPv6 が使用される場合）。次のオプションがあります。 • [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	IPv6 アドレスタイプがリンクローカルの場合、 IPv6 アドレスを VLAN または ISATAP 経由で受信するかを選択します。
IP Address	SNMP 管理ステーションの IP アドレスを入力します。
Community String	デバイスに対する管理ステーションの認証に使用するコミュニティ名を入力します。

Basic	このコミュニティタイプでは、どのグループにも接続できません。選択できるのはコミュニティ アクセス レベル（読み取り専用、読み取り/書き込み、またはSNMP管理）のみであり、必要に応じて、特定のビューではさらに制限します。デフォルトでは、MIB 全体に適用されます。これを選択した場合、次のフィールドに入力します。 • [Access Mode]：コミュニティのアクセス権を選択します。次のオプションがあります。 [Read Only]：管理アクセスは読み取り専用に制限されます。コミュニティに変更を加えることはできません。 [Read Write]：管理アクセスは読み取り/書き込みです。デバイス構成に変更を行うことはできますが、コミュニティにはできません。 [SNMP Admin]：ユーザーは、すべてのデバイス設定オプションにアクセスし、コミュニティを変更できます。SNMP管理は、SNMP MIBを除くすべてのMIBの読み取り/書き込みに相当します。SNMP管理は、SNMP MIBへのアクセスに必要です。 • [View Name]：SNMP ビューを選択します（アクセスが付与される MIB サブツリーの集合）。
Advanced	選択したコミュニティに対してこのタイプを選択します。 • [Group Name]：アクセス権を決定する SNMP グループを選択します。

ステップ 4 [Apply] をクリックします。SNMP コミュニティが定義され、実行コンフィギュレーションが更新されます。

トラップの設定

[Trap Settings] ページでは、デバイスから SNMP 通知を送信するかどうか、およびどのケースで送信するかを設定することができます。

トラップ設定を定義するには、次の手順を実行します。

手順

ステップ 1 [SNMP] > [Trap Settings] をクリックします。

ステップ 2 デバイスから SNMP 通知を送信できるように指定するには、[SNMP Notifications] で [Enable] を選択します。

ステップ 3 SNMP 認証失敗時の通知を有効にするには、[Authentication Notifications] で [Enable] を選択します。

ステップ 4 [Apply] をクリックします。SNMP トラップ設定は、実行コンフィギュレーション ファイルに書き込まれます。

通知受信者SNMPv1、2

通知の受信者は、SNMP通知の宛先、および各宛先に送信するSNMP通知の種類（トラップまたはインフォーム要求）を設定できます。SNMP通知とはデバイスからSNMP管理ステーションに送信されるメッセージであり、リンク アップ/ダウンなど、特定のイベントが発生したことを示します。

特定の通知をフィルタリングすることもできます。フィルタ処理を行うには、通知フィルタ（13 ページ）でフィルタを作成し、そのフィルタを SNMP 通知受信者に関連付けます。通知フィルタを使用すると、これから送信される通知の OID に基づいて、管理ステーションに送信される SNMP 通知のタイプをフィルタリングすることができます。

SNMPv1,2 で受信者を定義するには：

手順

ステップ 1 [SNMP] > [Notification Recipients SNMPv1,2] をクリックします。

このページには、SNMPv1,2 の受信者が表示されます。

ステップ 2 次のフィールドに入力します。

- [Informs IPv4 Source Interface]：ドロップダウンから、IPv4 SNMP サーバーとの通信に使用するトラップメッセージ内で送信元 IPv4 アドレスとして使用するオプション（[Auto] または [VLAN1]）を選択します。
- [Traps IPv4 Source Interface]：ドロップダウンから、IPv4 SNMP サーバーとの通信に使用するトラップメッセージ内で送信元 IPv4 アドレスとして使用するオプション（[Auto] または [VLAN1]）を選択します。
- [Informs IPv6 Source Interface]：ドロップダウンから、IPv6 SNMP サーバーとの通信に使用する通知メッセージ内で送信元 IPv6 アドレスとして使用するオプション（[Auto] または [VLAN1]）を選択します。
- [Traps IPv6 Source Interface]：ドロップダウンから、IPv6 SNMP サーバーとの通信に使用するトラップメッセージ内で送信元 IPv6 アドレスとして使用するオプション（[Auto] または [VLAN1]）を選択します。

（注）
自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

- [Server Definition]：リモート ログ サーバーを IP アドレスで指定するか、名前で指定するかを選択します。
- [IP Version]：IPv4 または IPv6 を選択します。
- [IPv6 Address Type]：リンク ローカルまたはグローバルのいずれかを選択します。
  - [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [Global]：IPv6アドレスは、他のネットワークからも認識かつアクセス可能なグローバルユニキャスト IPv6 タイプになります。
- [Link Local Interface]：IPv6 アドレスタイプがリンクローカルの場合、 IPv6 アドレスを VLAN または ISATAP 経由で受信するかを選択します。
- [Recipient IP Address/Name]：トラップが送信される場所の IP アドレスまたはサーバ名を入力します。
- [UDP Port]：受信者のデバイスで通知のために使用する UDP ポートを入力します。
- [Notification Type]：トラップまたは通知のどちらを送信するかを選択します。両方が必要な場合は、2 名の受信者を作成する必要があります。
- [Timeout]：デバイスがインフォーム要求を再送信するまでの待機時間を秒数で入力します。
- [Retries]：デバイスがインフォーム要求を再送信する回数を入力します。
- [Community String]：プルダウン メニューから、トラップ マネージャのコミュニティストリングを選択します。コミュニティストリング名は、SNMP コミュニティ （7 ページ）にリストされた名前から生成されます。
- [Notification Version]：トラップの SNMP バージョンを選択します。SNMPv1 または SNMPv2 のいずれかをトラップのバージョンとして使用できますが、一度に有効にできるのは 1 つのバージョンのみです。
- [Notification Filter]：選択すると、管理ステーションに送信される SNMP 通知タイプのフィルタリングが有効になります。フィルタは通知フィルタ （13 ページ）で作成されます。
- [Filter Name]：トラップに含める情報を定義した SNMP フィルタ（通知フィルタ （13 ページ）で定義）を選択します。

ステップ 5 [Apply] をクリックします。SNMP 通知の受信者設定は、実行コンフィギュレーション ファイルに書き込まれます。

通知受信者SNMPv3

SNMPv3 で受信者を定義するには：

手順

ステップ 1 [SNMP] > [Notification Recipients SNMPv3] をクリックします。

ステップ 2 次の設定を行います。

- [Informs IPv4 Source Interface]：ドロップダウンリストから、IPv4 SNMP サーバーとの通信に使用する通知メッセージ内で、IPv4アドレスを送信元IPv4アドレスとして使用する送信元インターフェイスを選択します。
- [Traps IPv4 Source Interface]：ドロップダウンリストから、トラップメッセージ内で、IPv4 アドレスを送信元アドレスとして使用する送信元インターフェイスを選択します。
- [Informs IPv6 Source Interface]：ドロップダウンリストから、IPv4 SNMP サーバーとの通信に使用する通知メッセージ内で、IPv6アドレスを送信元IPv4アドレスとして使用する送信元インターフェイスを選択します。
- [Traps IPv6 Source Interface]：ドロップダウンリストから、トラップメッセージ内で、IPv6 アドレスを送信元アドレスとして使用する送信元インターフェイスを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

- [Server Definition]：リモート ログ サーバーを IP アドレスで指定するか、名前で指定するかを選択します。
- [IP Version]：IPv4 または IPv6 を選択します。
- [IPv6 Address Type]：IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [Global]：IPv6アドレスは、他のネットワークからも認識かつアクセス可能なグローバルユニキャスト IPv6 タイプになります。
- [Link Local Interface]：プルダウン リストからリンク ローカル インターフェイスを選択します（IPv6 アドレス タイプにリンク ローカルが選択されている場合）。
- [Recipient IP Address/Name]：トラップが送信される場所の IP アドレスまたはサーバ名を入力します。

- [UDP Port]：受信者のデバイスで通知のために使用する UDP ポートを入力します。
- [Notification Type]：トラップまたは通知のどちらを送信するかを選択します。両方が必要な場合は、2名の受信者を作成する必要があります。
- [Timeout]：デバイスがインフォームまたはトラップを再送するまでに待機する時間（秒数）を入力します。タイムアウト：範囲 1 ～ 300、デフォルト 15
- [Retries]：デバイスがインフォーム要求を再送信する回数を入力します。再試行回数：範囲 0 ～ 255、デフォルト 3
- [User Name]：ドロップダウン リストから、SNMP 通知を送信するユーザを選択します。通知を受け取るには、そのユーザーがページで定義されていて、そのエンジン ID がリモートである必要があります。
- [Security Level]：パケットに適用する認証のレベルを選択します。

  （注）
  このセキュリティ レベルは、どのユーザ名を選択したかによって異なります。このユーザ名が「認証なし」として設定された場合、セキュリティ レベルは「認証なし」のみとなります。ただし、[User Name] に [Authentication and Privacy] 権限が割り当てられている場合、[Security Leve] は [No Authentication]、[Authentication Only]、または [Authentication and Privacy] のいずれかになります。

  次のオプションがあります。

  - [No Authentication]：パケットは認証または暗号化されていないことを示します。
  - [Authentication]：パケットは認証されているが、暗号化されていないことを示します。
  - [Privacy]：パケットは認証および暗号化されていることを示します。

- [Notification Filter]：選択すると、管理ステーションに送信される SNMP 通知タイプのフィルタリングが有効になります。
- [Filter Name]：トラップに含まれる情報を定義する SNMP フィルタを選択します。

ステップ 5 [Apply] をクリックします。SNMP 通知の受信者設定は、実行コンフィギュレーション ファイルに書き込まれます。

通知フィルタ

[Notification Filter] ページでは、SNMP 通知フィルタと、チェック対象のオブジェクト ID（OID）を設定することができます。通知フィルタを使用すると、これから送信される通知の OID に基づいて、管理ステーションに送信される SNMP 通知のタイプをフィルタリングすることができます。

通知フィルタを定義する手順は次のとおりです。

手順

ステップ 1 [SNMP] > [Notification Filter] をクリックします。

[Notification Filter] テーブルには、各フィルタの通知情報があります。テーブルでは、フィルタ名でフィルタ通知のエントリをフィルタリングできます。[Object Identifier Tree Filter] には、設定された各フィルタの現在のステータスが表示されます。

ステップ 2 [Add] をクリックして通知フィルタを追加するか、[Edit] をクリックして既存の通知フィルタを編集します。

ステップ 3 次のパラメータを入力または変更します。

- フィルタ名（Filter Name）：0 ～ 30 文字で名前を入力します。
- オブジェクト ID サブツリー（Object ID Subtree）：選択した SNMP フィルタに含まれるか除外される MIB ツリー内のノードを選択します。オブジェクトを選択するオプションは次のとおりです。
  - [Select from List]：MIB ツリー内を探索できます。上向き矢印を押すと選択したノードの親と兄弟のレベルに移動します。下向き矢印を押すと選択したノードの子のレベルまで下がります。1 つのノードからその兄弟に渡すには、ビューのノードをクリックします。兄弟をビューに移動するには、スクロール バーを使用します。
  - [Object ID]：[Include in filter] オプションが選択されている場合にこのオプションを選択すると、入力したオブジェクト ID がビューに表示されます。

ステップ 4 [Include in filter] を選択または選択解除します。これを選択すると、選択した MIB はフィルタに含まれ、そうでないものは除外されます。

ステップ 5 [Apply] をクリックします。SNMP ビューが定義され、実行コンフィギュレーションが更新されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。