



## 通知の設定

このセクションでは、次の点について説明します。

- [通知の設定](#) (1 ページ)
- [通知グループ](#) (2 ページ)
- [通知基準](#) (3 ページ)
- [通知の種類](#) (4 ページ)
- [SNMP トラップ通知](#) (5 ページ)
- [SMTP サーバの設定](#) (13 ページ)
- [syslog 通知](#) (13 ページ)
- [特定のアラームに制限された通知](#) (15 ページ)

## 通知の設定

Cisco Prime Collaboration Assurance では、IP テレフォニー、TelePresence 環境、IP ファブリックで発生するイベントにตอบสนองし、イベントやアラーム情報が表示されます。

イベントやアラームは、アラームやイベントのブラウザなど、Cisco Prime Collaboration Assurance ダッシュボードで確認できます。また、他のホストの SNMP トラップ収集装置、syslog 収集装置、およびユーザにイベントに関する情報を転送するように通知を設定することもできます。

通知は、デバイスのコンポーネントではなく、デバイスのロールごとにイベントを監視します。サポートされているイベントとアラームの一覧については、「[Prime Collaboration でサポートされているアラームとイベント](#)」を参照してください。

各アラームに対して Cisco Prime Collaboration Assurance は、アラーム、デバイス、重大度、状態を通知が設定されたグループと比較し、一致する場合には通知を送信します。ユーザが設定したアラームセットと通知基準によって一致を決定することができます通知条件を設定する手順については、[デバイス通知グループの追加](#)を参照してください。

次の表には、重大度の値と、アラームの状態が時間の経過によってどのように変化するか示されています。



(注) 通知で送信するイベントの重大度は、Cisco Prime Collaboration Assurance のデフォルト値からユーザ定義の値に変更できます。

この表には、アラーム、イベントの重大度、ステータスが示されています。

表 1: アラームとイベントの重大度とステータス

イベント	アラーム
重大度	
<ul style="list-style-type: none"> <li>• クリティカル               <ul style="list-style-type: none"> <li>◦</li> </ul> </li> <li>• メジャー(Major)</li> <li>• マイナー(Minor)</li> <li>• 警告               <ul style="list-style-type: none"> <li>◦</li> </ul> </li> <li>• 情報：イベントがクリアされると、重大度は情報に変更されます。一部のイベントは、デフォルトで、重大度が [Informational] になっています。</li> </ul>	<ul style="list-style-type: none"> <li>• クリティカル (Critical)</li> <li>• メジャー</li> <li>• マイナー</li> <li>• 警告</li> <li>• クリア</li> </ul>
ステータス (Status)	
<ul style="list-style-type: none"> <li>• アクティブ - イベントはライブです。</li> <li>• クリア：イベントはアクティブではありません。</li> </ul>	<ul style="list-style-type: none"> <li>• 認識：ユーザは手動でアラームを認識させています。ユーザは、アクティブなイベントにだけ確認応答を実行できます。</li> <li>• クリア - アラームはアクティブではありません。</li> <li>• アクティブ - アラームはライブです。</li> <li>• User Cleared</li> </ul>

## 通知グループ

通知グループは、通知の生成と送信に関するユーザ定義のルールセットです。

次の表は、通知先グループの内容について説明しています。

表 2:通知グループ

項目	説明
通知基準	通知が生成される理由の名前付きのセット。
通知タイプ	送信する通知のタイプ。SNMP トラップ、電子メール、または syslog です。
通知の受信者	SNMP トラップ、syslog メッセージ、または電子メールアドレスをリスニングするシステムのホスト名とポート。
毎日の登録アクティビティ期間	Cisco Prime Collaboration Assurance が通知を送信するイベントを監視しているときに、このサブスクリプションを利用すべき時間です。

## 通知基準

通知基準は、通知を送信するための監視対象項目を定義したものです。通知基準は、デバイスまたは電話、および特定の重大度とステータスを持つイベントのユーザ定義のセットに名前を付けたものです。通知グループを設定するには、通知基準を指定する必要があります。

Cisco Prime Collaboration Assurance は、デバイス ベースの通知条件をサポートします。次の表には、デバイス ベースの通知条件が示されています。

表 3:通知基準

項目	説明
デバイス	モニタするデバイス、デバイス グループ、またはクラスタ。
アラーム セット	(オプション)。モニタする1つ以上のアラームグループ。 <a href="#">特定のアラームに制限された通知</a> を参照してください。
アラームの重大度とステータス	複数のアラーム重大度レベルおよびステータス。

また、通知名や、通知によって表示される、[特定のアラームに制限された通知](#)デバイス ベースイベントの重大度もカスタマイズできます。

## 通知の種類

Cisco Prime Collaboration Assurance は、SNMP トラップ、電子メール、syslog という 3 つのタイプの通知を提供します。通知グループを設定するときには、送信する 1 つ以上の通知タイプと、各タイプの通知の受信者を指定する必要があります。

次の表には、通知のタイプが示されています。

表 4:通知タイプ

タイプ	説明
SNMP トラップ通知	<p>Cisco Prime Collaboration Assurance は、アラームとイベントに関するトラップを生成し、トラップの受信者に通知を送信します。これらのトラップは、Cisco Prime Collaboration Assurance サーバによって生成されたイベントとアラームに基づきます。トラップメッセージの形式は、CISCO-EPM-NOTIFICATION-MIB で定義されています。</p> <p>SNMP トラップ通知の使用は、Cisco Prime Collaboration Assurance によって処理される前に、raw トラップを別のサーバに転送することではありません。</p> <p>(注) Cisco Prime Collaboration Assurance は、ポーリングと受信のため、SNMP バージョン 1 (SNMPv1) と SNMPv2 トラップをサポートします。Cisco Prime Collaboration Assurance は、トラップを SNMPv2 トラップとして転送します。ただし、Cisco Prime Collaboration Assurance では、SNMPv3 のトラップ処理はサポートしていません。</p> <p>MIB OID と、アラームやイベント用として Cisco Prime Collaboration Assurance によって割り当てられる適切な値とのマッピングの詳細については、<a href="#">SNMP トラップ通知</a>を参照してください。</p>

タイプ	説明
電子メール通知	<p>Cisco Prime Collaboration Assurance は、アラーム情報を含む電子メールメッセージを生成します。電子メールの登録を作成するときには、サブジェクト行だけを含めるか、電子メールメッセージ全体を含めるかを選択できます。</p> <p>(注) Cisco Prime Collaboration Assurance を Enterprise モードでインストールした場合は、件名で次のフォーマットを使用した電子メール通知を受け取ります。</p>
	<p><i>[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY.</i></p> <p>例： <i>[PC-ALERT-#CPCM-Ent-Cluster#]50.0.50.230:Gatekeeper Registration Failure:CRITICAL</i></p> <p>クラスタ名またはデバイス IP がない場合は、空白である場合があります。</p>
	<p>NAT 環境では、デバイスのプライベート IP アドレスも表示されます。</p> <p>Cisco Prime Collaboration Assurance を MSP モードでインストールした場合、デバイスが属しているカスタマーを参照することができます。</p>
Syslog 通知	<p>Cisco Prime Collaboration Assurance は、リモートシステムの syslog デーモンに転送可能なアラーム用の syslog メッセージを生成します。</p> <p>NAT 環境では、デバイスのプライベート IP アドレスも表示されます。</p> <p>Cisco Prime Collaboration Assurance を MSP モードでインストールした場合、デバイスが属しているカスタマーを参照することができます。</p> <p>Syslog メッセージのサンプルと説明については、<a href="#">syslog 通知</a>を参照してください。</p>

## SNMP トラップ通知

アラームまたはイベントが Cisco Prime Collaboration Assurance サーバで受信されると、そのサーバは CISCO-EPM-NOTIFICATION-MIB に定義されたトラップ形式に変換されます。他の MIB オブジェクトはサポートされていません。すべてのトラップレシーバは、同じトラップフォーマットの同じトラップを受信します。

CISCO-EPM-NOTIFICATION-MIB は、[Cisco.com](http://Cisco.com) からダウンロードできます。

次の表に、MIB OID とその対応値を、Cisco Prime Collaboration Assurance によってアラームのために割り当てられるものを示します。

表 5: CISCO-EPM-NOTIFICATION-MIB アラーム概要

トラップフィールド名	OID	タイプ	Prime Collaboration のアラーム	トラップ フォワーダの内容 (EPM MIB)
cenAlarmIndex	1.3.6.1.4.1.9.9.311.1.1.2.1.1	Unsigned32	-	MIB index
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdmin 文字列	-	この MIB のバージョンです。バージョン文字列は、メジャーバージョン.マイナーバージョンの形式です。  (注) 必ず 9.0 に設定します。
cenAlamTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	タイムスタンプ	タイムスタンプ	アラームがトリガーされた時刻です。
cenAlarmUpdated タイムスタンプ	1.3.6.1.4.1.9.9.311.1.1.2.1.4	タイムスタンプ	lastmodified のタイムスタンプ	アラームが最後に変更された時刻です。
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdmin 文字列	ID	Cisco Prime Collaboration Assurance によって生成された一意のアラーム ID です。
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32	lastcleartime	アラームがアクティブであるか (1)、クリアされたか (2) を示します。
cenAlarmStatus 定義	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdmin 文字列	lastcleartime	アラームに関する簡単な説明です。  • 1-Active • 2-Cleared
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	整数	-	アラーム タイプは直接 (2) です。
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32	カテゴリ	アラームのカテゴリ。整数値として表示されます。

cenAlarmCategory 定義	1.3.6.1.4.1.99.311.1.1.2.1.10	SnmpAdmin 文字列	カテゴリ	AlarmCategory を文字で 表したものです (番号、 説明) です。  <ul style="list-style-type: none"> <li>• 3,Endpoint : すべて のエンドポイントの ハードウェアア ラーム (ペリフェラ ルエラー) です。</li> <li>• 4,Network Devices : すべてのネットワー ク デバイスのハー ドウェアアラーム (インターフェイス エラー) です。</li> <li>• 5,Service Infrastructure : コー ルおよび会議制御 (Cisco Unified CM および VCS) 、管 理 (TMS) 、マル チポイントスイッ チ (CTMS) 、およ びマルチポイント コントロールユ ニット (TPS、 MCU) のアラーム。</li> <li>• 6,Conference : エン ドポイントのアラーム (会議の一部) 、 およびネットワーク のアラーム (ジッ ター、遅延、または ドロップ) 。</li> </ul>
cenAlarmServer AddressType	1.3.6.1.4.1.99.311.1.1.2.1.11	InetAddress タイプ	-	このトラップを生成して いるサーバが到達可能な インターネット アドレ スのタイプです。この値 は、IPv4 管理の場合は 1 に設定されます。
cenAlarmServer アドレス	1.3.6.1.4.1.99.311.1.1.2.1.12	InetAddress	-	Cisco Prime Collaboration Assurance IP アドレスで す。

cenAlarmManaged ObjectClass	1.3.6.1.4.1.99.311.1.1.2.1.13	SnmpAdmin 文字列	Source	、Cisco VCS などのソースのエンティティタイプです。
cenAlarmManaged ObjectAddressType	1.3.6.1.4.1.99.311.1.1.2.1.14	InetAddress タイプ	ソース	管理対象デバイスが到達可能なインターネットアドレスのタイプです。この値は、IPv4 管理の場合は 1 に設定されます。
cenAlarmManaged ObjectAddress	1.3.6.1.4.1.99.311.1.1.2.1.15	InetAddress	ソース	管理対象オブジェクトの IP アドレスです。
cenAlarmDescription	1.3.6.1.4.1.99.311.1.1.2.1.16	OctetString	説明	アラームの詳細です。
cenAlarmSeverity	1.3.6.1.4.1.99.311.1.1.2.1.17	Integer32	重大度	アラームの重大度を整数値で示します。有効な整数は、0-7 です。
cenAlarmSeverity 定義	1.3.6.1.4.1.99.311.1.1.2.1.18	OctetString	重大度	アラームの重大度を文字列で表したものの（番号、説明）です。  <ul style="list-style-type: none"> <li>• 0,critical</li> <li>• 1,major</li> <li>• 2,minor</li> <li>• 3,warning</li> <li>• 4,info</li> <li>• 5,normal</li> <li>• 6,unknown</li> <li>• 7,cleared</li> </ul>
cenAlarmTriageValue	1.3.6.1.4.1.99.311.1.1.2.1.19	Integer32	-	未使用です。
cenEventIDList	1.3.6.1.4.1.99.311.1.1.2.1.20	OctetString	-	このアラームの原因となったイベント ID のリストです。
cenUserMessage1	1.3.6.1.4.1.99.311.1.1.2.1.21	SnmpAdmin 文字列	isacknowledged	このアラームが認知されたかどうかを示します。



cenUserMessage2	1.3.6.1.4.1.99.311.1.1.2.1.22	SnmpAdmin 文字列	以前の重大 度	アラームの以前の重大度。例として、会議の実行中に「メジャー」アラームがトリガーされた場合を考えます。会議が完了すると、会議アラームが自動的にクリアされます。この会議におけるアラームの直前の重大度は「メジャー」であるため、この場合は [メジャー (Major)] と表示されます。
cenUserMessage3	1.3.6.1.4.1.99.311.1.1.2.1.23	SnmpAdmin 文字列	-	未使用です。
cenAlarmMode	1.3.6.1.4.1.99.311.1.1.2.1.24	整数	-	2 : アラート。このトラップは、アラーム通知であるかイベント通知であるかを示します。
cenPartitionNumber	1.3.6.1.4.1.99.311.1.1.2.1.25	Unsigned32	-	未使用です。
cenPartitionName	1.3.6.1.4.1.99.311.1.1.2.1.26	SnmpAdmin 文字列	-	未使用です。
cenCustomer ID	1.3.6.1.4.1.99.311.1.1.2.1.27	SnmpAdmin 文字列	ownerid	Enterprise モードでは、Cisco Prime Collaboration Assurance の通知ユーザインターフェイスに入力された顧客 ID の詳細が表示されます。  MSP モードでは、顧客名が表示されます。
cenCustomer 改定	1.3.6.1.4.1.99.311.1.1.2.1.28	SnmpAdmin 文字列	-	未使用です。

cenAlertID	136.14.1.99311.1.1.2.129	SnmpAdmin 文字列	id	Cisco Prime Collaboration Assurance によって割り当てられた一意のアラーム ID です。割り当てられているアラーム ID については、「 <a href="#">Cisco Prime Collaboration Assurance</a> でサポートされているアラームとイベント」の表を参照してください。
------------	--------------------------	------------------	----	--

次の表に、MIB OID とその対応値を、Cisco Prime Collaboration Assurance によってイベントのために割り当てられるものを示します。

表 6: CISCO-EPM-NOTIFICATION-MIB イベント概要

トラップフィールド名	OID	タイプ	Prime Collaboration イベント	トラップフォワーダの内容 (EPM MIB)
cenAlarmIndex	136.14.1.99311.1.1.2.11	Unsigned32	-	MIB index
cenAlarmVersion	136.14.1.99311.1.1.2.12	SnmpAdmin 文字列	-	この MIB のバージョンです。バージョン文字列は、メジャーバージョン.マイナーバージョンの形式です。 (注) 必ず 9.0 に設定します。
cenAlarmTimestamp	136.14.1.99311.1.1.2.13	タイムスタンプ	タイムスタンプ	イベントがトリガーされた時刻です。
cenAlarmUpdateTimestamp	136.14.1.99311.1.1.2.14	タイムスタンプ	-	未使用です。
cenAlarmInstanceID	136.14.1.99311.1.1.2.15	SnmpAdmin 文字列	ID	Cisco Prime Collaboration Assurance によって生成された一意のイベント ID です。
cenAlarmStatus	136.14.1.99311.1.1.2.16	Integer32	-	未使用です。
cenAlarmStatus 定義	136.14.1.99311.1.1.2.17	SnmpAdmin 文字列	-	未使用です。
cenAlarmType	136.14.1.99311.1.1.2.18	整数	-	イベントタイプは直接 (2) です。

cenAlarmCategory	136.14.199311.1.12.19	Integer32	カテゴリ	イベントのカテゴリです。整数値として表示されます。
cenAlarmCategory 定義	136.14.199311.1.12.10	SnmpAdmin 文字 列	カテゴリ	<p>AlarmCategory を文字で表したものです（番号、説明）です。</p> <ul style="list-style-type: none"> <li>• 3,Endpoint : すべてのエンドポイントのハードウェアイベント（ペリフェラルエラー）。</li> <li>• 4,Network Devices : すべてのネットワークデバイスのハードウェアイベント（インターフェイスエラー）。</li> <li>• 5,Service Infrastructure : コールおよび会議制御（Cisco Unified CM および VCS）、管理（TMS）、マルチポイントスイッチ（CTMS）、およびマルチポイントコントロールユニット（TPS、MCU）のイベント。</li> <li>• 6,Conference : エンドポイントのイベント（会議の一部）、およびネットワークのイベント（ジッター、遅延、またはドロップ）。</li> </ul>

cenAlarmServer AddressType	136.14.199311.1.121.11	InetAddress タイプ	-	このトラップを生成しているサーバが到達可能なインターネットアドレスのタイプです。この値は、IPv4 管理の場合は 1 に設定されます。
cenAlarmServer アドレス	136.14.199311.1.121.12	InetAddress	-	Prime Collaboration の IP アドレスです。
cenAlarmManaged ObjectClass	136.14.199311.1.121.13	SnmpAdmin 文字列	Source	CTS、Cisco VCS などのソースのエンティティタイプ。
cenAlarmManaged ObjectAddressType	136.14.199311.1.121.14	InetAddress タイプ	ソース	管理対象デバイスが到達可能なインターネットアドレスのタイプです。この値は、IPv4 管理の場合は 1 に設定されます。
cenAlarmManaged ObjectAddress	136.14.199311.1.121.15	InetAddress	ソース	管理対象オブジェクトの IP アドレスです。
cenAlarmDescription	136.14.199311.1.121.16	OctetString	説明	イベントの詳細です。
cenAlarmSeverity	136.14.199311.1.121.17	Integer32	重大度	イベントの重大度を整数値で示します。有効な整数は、0-7 です。
cenAlarmSeverity Definition	136.14.199311.1.121.18	OctetString	重大度	アラームの重大度を文字列で表したものの（番号、説明）です。  <ul style="list-style-type: none"> <li>• 0,critical</li> <li>• 1,major</li> <li>• 2,minor</li> <li>• 3,warning</li> <li>• 4,info</li> <li>• 5,normal</li> <li>• 6,unknown</li> <li>• 7,cleared</li> </ul>
cenAlarmTriageValue	136.14.199311.1.121.19	Integer32	-	未使用です。
cenEventIDList	136.14.199311.1.121.20	OctetString	-	未使用です。
cenUserMessage1	136.14.199311.1.121.21	SnmpAdmin 文字列	-	未使用です。

cenUserMessage2	136.14.1.99311.1.12.122	SnmpAdmin 文字列	-	未使用です。
cenUserMessage3	136.14.1.99311.1.12.123	SnmpAdmin 文字列	-	未使用です。
cenAlarmMode	136.14.1.99311.1.12.124	整数	-	3-event このトラップは、アラーム通知であるかイベント通知であるかを示します。
cenPartitionNumber	136.14.1.99311.1.12.125	Unsigned32	-	未使用です。
cenPartitionName	136.14.1.99311.1.12.126	SnmpAdmin 文字列	-	未使用です。
cenCustomer ID	136.14.1.99311.1.12.127	SnmpAdmin 文字列	-	未使用です。
cenCustomerRevision	136.14.1.99311.1.12.128	SnmpAdmin 文字列	-	未使用です。
cenAlertID	136.14.1.99311.1.12.129	SnmpAdmin 文字列	-	未使用です。

## SMTP サーバの設定

SMTP サーバ名と送信者 AAA 電子メールアドレスを、[アラームとイベントの電子メール設定 (E-mail Setup for Alarms & Events)] ページ ([アラームとレポートの管理 (Alarm & Report Administration)]、> [アラームとイベントの電子メール設定 (E-mail Setup for Alarms & Events)] で指定することで、アラームの電子メール通知を送受信するように SMTP サーバを設定することができます。[Sender AAA E-mail Address] フィールドの値は、多数のサーバがある場合に、電子メールを受信したサーバを特定するのに便利です。

## syslog 通知

syslog メッセージは 1,024 文字までに制限されています (見出しを含む)。この syslog の制限のため、syslog ベースのイベントの詳細には完全な情報が含まれない可能性があります。syslog メッセージがこの制限を超えた場合、syslog の送信側によって 1,024 文字に切り捨てられます。

Cisco Prime Collaboration Assurance server がアラームを送信する際に生成する syslog メッセージの例を、次に示します。

```
Local7.Emerg 10.78.110.27 Feb 19 14:42:49 pcollab-44798 pc798:%local7-0-ALARM:
14$Description=デバイスの温度または温度は通常の動作範囲外です。Out37 イベントが生成されると、通常は、ファン、電源、電源も表示されます。または温度イベン
ト::Status=1,active^Critical^Acknowledged=no^AlarmURL=https://10.78.110.27/emsam/index.html
#pageId=com_cisco_ifm_web_page_alarms&queryParams=Id%3D84837&forceLoad=true^Device Work
```

Center=  
 https://10.78.110.27/emsam/index.html#pageId=com\_cisco\_emsam\_page\_inventory&deviceId=3681728  
 ^CUSTOMER=customer2/CU44/2,324]。デフォルト アラーム名=Out324^Managed  
 Object=150.50.3.2^Managed Object Type=Router^MODE=2;アラーム  
 ID=84837^Component=150.50.3.2/8<000&<000>

次の表では、上記の例に基づいて syslog 通知パラメータを説明します。

表 7: syslog 通知の説明

パラメータ	説明
Local7.Emerg 10.78.110.27 Feb 19 14:42:49 pcollab-44798 pcollab-44798	Syslog が生成された Cisco Prime Collaboration Assurance サーバの IP アドレスとホスト名
%local7-0-ALARM	<ul style="list-style-type: none"> <li>• Syslog Facility データ : %local7</li> <li>• 重要度 : 0-深刻、1-重大、2-やや重大、および 3-警告</li> <li>• タイプはアラーム</li> </ul>
14	暦年
説明	アラームの説明
ステータス = 1、アクティブ	アラームのステータス : 1はアクティブ、2は解除済み
Severity	アラームの重大度
承認済み	アラームが受信確認されているかどうかを示します
AlarmURL	[アラーム (Alarm) ] ページを起動する URL
Inventory Management	[インベントリ管理 (Inventory Management) ] ページを起動する URL
CONFERENCE DIAGNOSTICS	conferencealarm の場合、[会議診断 (Conference Diagnostics) ] ページを起動する URL
カスタマー	通知の設定中に定義された顧客 ID
CUSTREV	通知の設定中に定義された顧客リビジョン
デフォルト アラーム名	アラーム名
管理対象オブジェクト	アラームが発生したデバイスの IP アドレスまたはホスト名
管理対象オブジェクトタイプ	デバイスタイプ (ルータ、エンドポイントなど)

パラメータ	説明
モード	Syslog メッセージがアラーム (2) であるかどうかを示します
アラーム ID (Alarm ID)	アラームの固有 ID
コンポーネント	アラームが発生したデバイス コンポーネント

## 特定のアラームに制限された通知

場合によっては、Cisco Prime Collaboration Assurance が監視する一部のアラームのみで、通知を送信する必要があります。目的のアラームは、通知基準を定義するときに、次のように設定することができます。

- デバイスベースの通知基準ごとに、1つのアラームセットを指定します。アラームセットは必要なだけ作成することができます。

アラームセットは、次の目的に使用できます。

- Cisco Prime Collaboration Assurance 通知が監視するアラーム数を制限します。アラームセットを使用しない場合、Cisco Prime Collaboration Assurance 通知はすべてのアラームを監視し、通知を送信するかどうか判断します。
- 異なる複数の宛先に送信する通知の集約。たとえば、次の各目的で個別のアラームセットを作成することができます。
  - 特定の個人または部署に送信される電子メール通知を特定のアラームに関するものだけにして、量を制限する。
  - 特定のアラームの発生をすべて syslog に書き込む。
  - 特定のアラームが発生した場合に SNMP トラップを送信する。

デバイスベースの通知基準を作成する場合は、基準の1つとして1つのアラームセットを含める必要があります。デフォルトのアラームセット「All」には、すべてのアラームが含まれています。

## アラームセットの追加

通知を設定できるアラームセットを作成できます。

アラームセットを追加および編集するには、次の手順を実行します。

**ステップ 1** 選択 [通知の設定 (Notification Setup)]。

**Cisco Prime Collaboration リリース 11.5 以降の場合**

移行方法 [アラームおよびレポート管理 (Alarm & Report Administration)] > [通知のセットアップ (Notification Setup)]

ステップ2 [カスタム通知 (Custom Notification)] をクリックして、詳細を入力します。

(注) 複数のアラームを持つアラームセットを作成する場合、複数の検索基準を使用する必要がある場合があります。このような状況では、[+]アイコンを使用して複数の検索基準を入力する [Advanced Filtering] オプションを使用し、[Match] に [Any] を選択する必要があります。[クイックフィルタ (Quick Filter)] オプションは、思うように動作しない場合があります。

(注) 既存のアラームセットにアラームを追加する場合は、フィルタリングによって元のアラームのセットが上書きされるのを避けるために、フィルタを使用してアラームを検索しないでください。

ステップ3 [追加 (Add)] をクリックし、必要な情報を指定します。

ステップ4 [保存 (Save)] をクリックして変更内容を保存します。

## デバイス通知グループの追加

デバイス通知先グループを追加および編集するには、次の手順を実行します。



(注) 既存の通知グループをテンプレートとして使用し、新しい通知グループを作成することもできます。

ステップ1 選択 [通知のセットアップ (Notification Setup)] [保証通知基準 (Assurance Notification Criteria)] を選択します。

**Cisco Prime Collaboration リリース 11.5 以降の場合**

選択 [アラームおよびレポート管理 (Alarm & Report Administration)] > [通知のセットアップ (Notification Setup)] [カスタム通知 (Custom Notification)] を選択します。

ステップ2 [Add] をクリックして、新しい基準を追加します。

ステップ3 [新しいデバイスベースの条件 (New Device-Based Criterion)] ウィザードで、[一般情報の定義 (Define General Information)] ページに次の情報を追加します。

展開モードに基づいて、ドメイン固有または顧客固有のデバイス通知先グループを作成できます。[新しいデバイスベースの条件 (New Device-Based Criterion)] ウィザードで、必要な詳細を入力し、[ドメインに関連付け (Associate to Domain)] ドロップダウンリストからドメインを選択するか、[顧客 (Customer)] ドロップダウンリストからドメインを選択します。

(注) スーパー管理者はすべてのドメインにアクセスでき、1つのドメインまたはすべてのドメインの通知グループを作成できます。

ステップ4 [Next] をクリックします。



[Select Devices/Device Groups] ペインが表示されます。

このチェックボックスをオンにすると、すべてのグループに追加された新しいデバイスが、自動的にそのグループの一部になり、Cisco Prime Collaboration Assurance にデバイスが追加または削除されると、通知基準からも追加または削除されます。このような動作は、該当のデバイスが属するデバイスグループが通知基準に含まれている場合に発生します。

通知基準に含まれるすべてのデバイスグループでデバイスのスタティックなリストを保持する場合は、オフにします。

**ステップ 5** [Add] をクリックします。

**ステップ 6** [デバイス/デバイスグループの選択 (Select Device/Device Groups)] ウィンドウで、[すべてのデバイスを含める (Include all Devices)] または [デバイスの選択 (Select Devices)] のラジオボタンをクリックします。

[すべてのデバイスを含める (Include all Devices)] オプションを選択した場合は、デバイスグループフォルダを展開して、1つまたは複数のデバイス、デバイスグループ、またはクラスタを選択します。

[デバイスの選択 (Select Devices)] オプションを選択した場合は、デバイスグループフォルダを展開し、1つまたは複数のデバイス、デバイスグループ、またはクラスタのチェックボックスをオンにします。

(注) クラスタレベルの電子メール通知を追加する場合は、[インフラストラクチャ (Infrastructure)] > [UCM クラスタ (UCM Clusters)] デバイスグループフォルダに一覧表示されているクラスタとクラスタ ID 内のすべてのノードのリストから、クラスタ ID を選択する必要があります。

デバイスグループを選択した場合、[最新情報をグループメンバーシップに含める (Include updates to the group membership)] チェックボックスをオンにした場合に限り、Cisco Prime Collaboration Assurance からデバイスが追加または削除された時に、通知基準最新の状態に保たれます。すべてのグループに追加された新しいデバイスは、自動的にそのグループの一部になります。

**ステップ 7** [Next (次へ)] をクリックします。

**ステップ 8** [通知先の設定 (Set up Destination)] ペインで、必要な情報を追加します。

**ステップ 9** [Next] をクリックします。

**ステップ 10** 概要情報を確認し、[Save] をクリックします。

デバイス通知グループを保存すると、[新しいデバイスベースの条件 (New Device-Based Criterion)] ウィザードで入力した詳細情報が、[Assurance通知基準 (Assurance Notification Criteria)] ページに表示されます。[顧客 (Customer)] 列に、通知先グループが所属する顧客が示されます。

## [一般情報 (General Information)] フィールドの説明

次の表で、[一般情報 (General Information)] ウィンドウのフィールドを説明します。

表 8: 一般的情報の追加

グラフィカルユーザインターフェイスの要素	説明
[Criterion Name] フィールド	通知基準の名前を入力します。
[Customer Identification] フィールド	適切な識別情報を入力します。このフィールドが空白のままの場合は、電子メール通知と syslog 通知では空白が表示されます。  SNMP トラップ通知では、次のように表示されます。  顧客ID: -
[Customer Revision] フィールド	適切な識別情報を入力します。このフィールドが空白のままの場合は、電子メール通知と syslog 通知では空白が表示されます。  SNMP トラップ通知では、次のように表示されます。  顧客リビジョン: *
[Alarm Set Type] リスト ボックス	次のいずれかを選択します。
[Alarm Severity] チェックボックス	オフのままにするか、次の 1 つまたは複数を選択します。  <ul style="list-style-type: none"> <li>• 深刻</li> <li>• やや重大</li> <li>• 比較的重大でない</li> <li>• 警告</li> </ul>
[Alarm Status] チェックボックス	オフのままにするか、次の 1 つまたは複数を選択します。  <ul style="list-style-type: none"> <li>• Active</li> <li>• Acknowledged</li> <li>• Cleared</li> <li>• User Cleared</li> </ul>

グラフィカルユーザインターフェースの要素	説明
OperationInterval	<p>通知グループが常にアクティブになるようにスケジュールするには、[Always] オプションボタンをクリックします。</p> <p>通知グループをアクティブにする時間帯を選択します。</p> <ul style="list-style-type: none"> <li>• [From: HH:MM] : 登録がアクティブになる時間および分を選択します。</li> <li>• [To: HH:MM] : 登録がアクティブな期間の最後の時間および分を選択します。</li> </ul> <p>デフォルトでは、これらの値は 00:00 から 00:00 までで、登録は24時間アクティブになっています。</p> <p>たとえば、あるシフトでは電子メール通知を送信し、別のシフトでは送信しないようにする場合にこのフィールドを使用します。</p>

## 通知先フィールドの説明を設定

次の表に、[通知先の設定 (Set up Destinations) ] ページのフィールドについて説明します。

表 9: 通知先の設定

グラフィカルユーザインターフェースの要素	説明
[Include Link to Notification Details] チェックボックス	<p>オンにすると、通知に URL が含まれます。ユーザはその URL を使用して、関連する詳細な情報を確認するためのページを Cisco Prime Collaboration Assurance で直接開くことができます。</p> <p>通知から URL を省略する場合はオフにします。</p>

グラフィカルユーザインターフェイスの要素	説明
[Subscription Type] オプション ボタン	<p>該当の登録に含める登録タイプを一度に1つずつ選択し、データを入力します。</p> <ul style="list-style-type: none"> <li>• [トラップ (Trap) ] : トラップサブスクリプションタイプのフィールドにデータを入力します。</li> <li>• [E-Mail] : [E-Mail Subscription Type] フィールドにデータを入力します。</li> <li>• [Syslog (Syslog) ] : Syslog サブスクリプションタイプのフィールドにデータを入力します。</li> </ul> <p>Cisco Prime Collaboration Assurance では、[サブスクリプション: 概要 (Subscription: Summary) ] ページの [完了 (Finish) ] をクリックするまで、入力したデータが保存されません。[サブスクリプション: 概要 (Subscription: Summary) ] ページに移動するには、[次へ (Next) ] をクリックします。</p>
[Trap Subscription Type] フィールド	
[IP Address/Fully Qualified Domain Name] 編集可能カラム	ホストの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
[Port] 編集可能カラム	ホストがトラップを受信できるポート番号を入力します。有効なポートの値は、0～65,535 です。デフォルトのポート番号 162 を入力することもできます。
[Comments] 編集可能カラム	(任意) コメントを入力します。
[E-Mail Subscription Type] フィールド	

グラフィカルユーザインターフェイスの要素	説明
[SMTP Server] フィールド	<p>Simple Mail Transfer Protocol (SMTP) サーバの完全修飾 DNS 名または IP アドレスを入力します (デフォルトの SMTP サーバの名前がすでに表示されている場合もあります)。</p> <p>既存の登録によって使用されているデフォルト以外の任意の SMTP サーバを選択するには、SMTP Servers ボタンをクリックします。</p> <p>デフォルトの SMTP サーバの設定方法については、「システム環境設定を使用してシステム全体のパラメータを設定する」を参照してください。</p>
[Sender Address] フィールド	<p>通知の送信元の電子メールアドレスを入力します。送信者の電子メール サービスが指定した SMTP サーバでホスティングされている場合は、ユーザ名だけを入力します。ドメイン名を入力する必要はありません。</p>
[Recipient Address(es)] フィールド	<p>通知の送信先となる 1 つ以上の電子メールアドレスを入力します。複数のアドレスはカンマまたはセミコロンで区切ります。</p> <p>受信者の電子メール サービスが指定した SMTP サーバでホスティングされている場合は、ユーザ名だけを入力します。ドメイン名を入力する必要はありません。</p>
[Send Recipient(s) Subject Only] チェックボックス	<p>電子メール メッセージにサブジェクトだけを含める場合はオンにします。</p> <p>詳細な電子メール メッセージを送信する場合はオフにします (デフォルト)。</p> <p><b>Cisco Prime Collaboration リリース 11.1 以降の場合</b></p> <p>(注) 件名を含む電子メール通知は、次の形式で送信されます。</p>
<p><i>[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY.</i></p> <p>例 : <i>[PC-ALERT-CPCM-Ent-Cluster]50.0.50.230:Gatekeeper Registration Failure:CRITICAL</i></p> <p><i>CLUSTERNAME</i> は、Unified Communications Manager と Cisco VCS のみの件名の欄に含まれています。他のすべてのデバイス タイプで、<i>CLUSTERNAME</i> は空のままになります。</p> <p><i>DEVICE IP</i> または <i>CLUSTERNAME</i> が利用できない場合は、空のままになります。</p>	

グラフィカルユーザインターフェ이스の要素	説明
[Syslog Subscription Type] フィールド	
[IP Address/Fully Qualified Domain Name] 編集可能カラム	ホストの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
[Port] 編集可能カラム	syslog デーモンがリスニングを行うポート番号を入力します。有効なポートの値は、0 ~ 65,535 です。デフォルトのポート番号 514 を入力することもできます。  リモートシステム (ホスト名) の syslog デーモンが指定したポートでリスニングを行うように設定しておく必要があります。
[Comments] 編集可能カラム	(任意) コメントを含めます。