

ワイヤレスアクセスポイントでのイベントロギングの設定

目的

システムイベントは、システムを円滑に実行して障害を防ぐために、注意と必要なアクションを実行する必要があるアクティビティです。これらのイベントはログとして記録されます。システムログを使用すると、管理者はデバイスで発生した特定のイベントを追跡できます。

イベントログは、ネットワークのトラブルシューティング、パケットフローのデバッグ、およびイベントの監視に役立ちます。これらのログは、ランダムアクセスメモリ(RAM)、不揮発性ランダムアクセスメモリ(NVRAM)、およびリモートログサーバに保存できます。通常、これらのイベントはリブート時にシステムから消去されます。システムが不意にリブートすると、システムイベントは不揮発性メモリに保存されない限り表示されません。持続性ロギング機能を有効にすると、システムイベントメッセージが不揮発性メモリに書き込まれます。

ログ設定は、ネットワーク上でさまざまなイベントが記録されるときメッセージ、通知、およびその他の情報のロギングルールと出力先を定義します。この機能は、イベントが発生したときに必要なアクションが実行されるように、担当者に通知します。ログは、電子メールアラートを介して送信することもできます。

このドキュメントの目的は、システムログとイベントログを受信するためのさまざまな設定について説明し、その設定手順を示すことです。

適用可能なデバイス

- WAP100シリーズ
- WAP300シリーズ
- WAP500シリーズ

[Software Version]

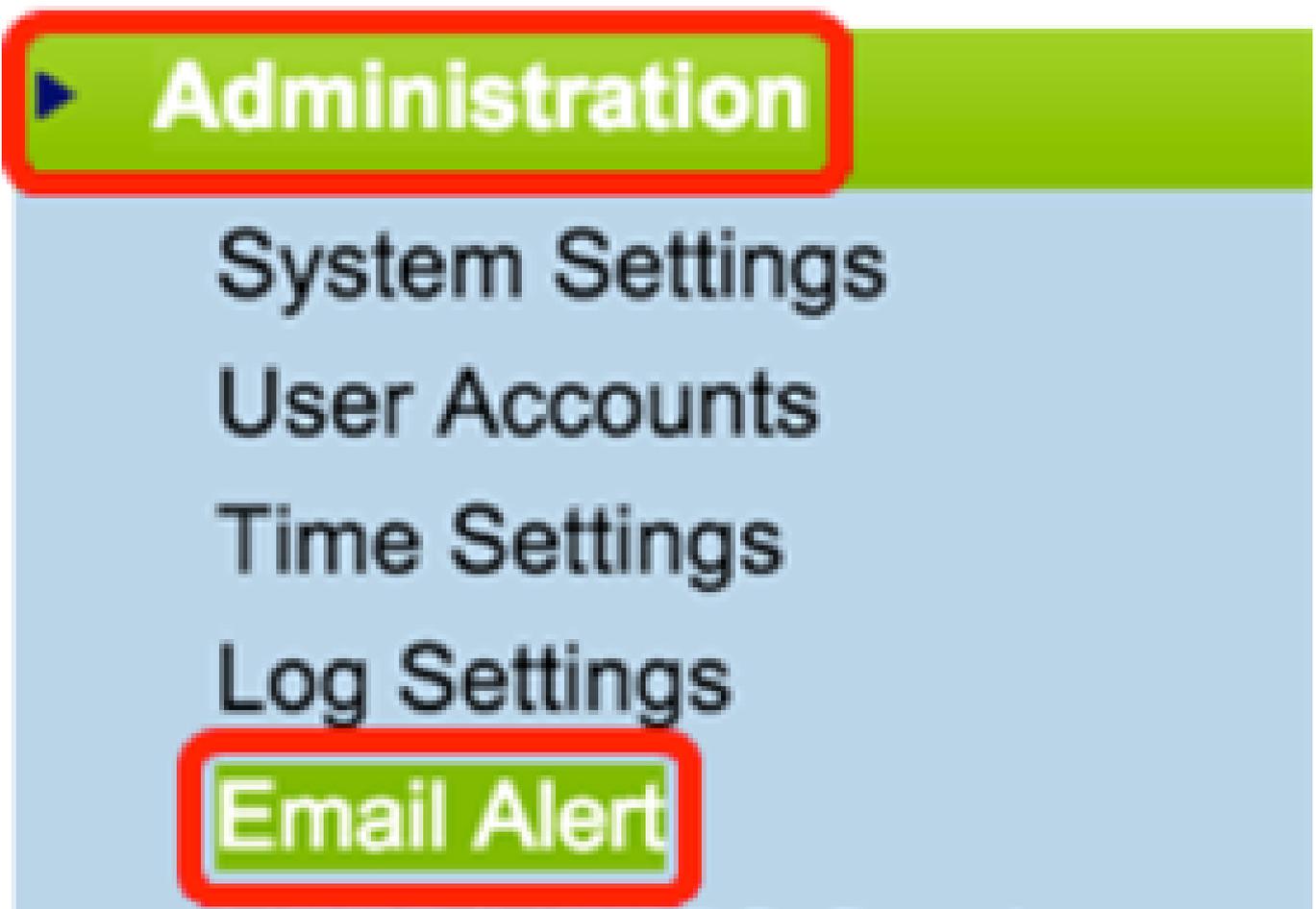
- 1.0.1.4 — WAP131、WAP351
- 1.0.6.2 — WAP121、WAP321
- 1.2.1.3 — WAP371、WAP551、WAP561

- 1.0.1.2 — WAP150、WAP361
- 1.0.0.17 — WAP571、WAP571E

イベントロギングの設定

電子メール通知の構成

ステップ 1 : Webベースのユーティリティにログインし、Administration > Email Alertの順に選択します。



ステップ 2 : 電子メールアラート機能をグローバルで有効にするには、Administrative ModeチェックボックスでEnableにチェックマークを付けます。

Email Alert

Global Configuration

Administrative Mode:

Enable

From Email Address:

example@mail.com

(xyz@xxxx.xxx)

Log Duration:

30

(Range: 30 - 1440 M)

Scheduled Message Severity:

Warning



Urgent Message Severity:

Alert



ステップ 3 : From Email Addressフィールドに電子メールアドレスを入力します。アドレスは、電子メールアラートの送信者として表示されます。デフォルト値はnullです。

Email Alert

Global Configuration

Administrative Mode:

Enable

From Email Address:

example@mail.com

Log Duration:

30

Scheduled Message Severity:

Warning



Urgent Message Severity:

Alert



注：プライバシーを維持するために、個人の電子メールを使用する代わりに、個別の電子メールアカウントを使用することを強くお勧めします。

ステップ 4：Log Durationフィールドに、設定した電子メールアドレスに電子メールアラートを送信する頻度を分単位で入力します。範囲は30 ~ 1440分で、デフォルト値は30です。

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity: ▼

Urgent Message Severity: ▼

ステップ 5：スケジュールされたメッセージの重大度を設定するには、送信するメッセージのタイプ（緊急、アラート、重大、エラー、警告、通知、情報、デバッグなど）を選択します。これらのメッセージは、ログ期間が経過するたびに送信されます。これらのオプションは、使用しているデバイスのモデルに応じて、Webベースのユーティリティで異なる方法で表示されます。

WAP131、WAP150、WAP351、およびWAP361の場合は、Scheduled Message Severityチェックボックスで適切なメッセージタイプにチェックマークを入れます。

Scheduled Message Severity: Emergency Alert Critical Error Warning Notice Info Debug

Urgent Message Severity: Emergency Alert Critical Error Warning Notice Info Debug

WAP121、WAP321、WAP371、WAP551、WAP561、WAP571、およびWAP571Eの場合、Scheduled Message Severityドロップダウンリストで適切なメッセージタイプをクリックします。

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption:

Warning ▼

None

Emergency

Alert

Critical

Error

Warning

Notice

Info

Debug

- None : メッセージは送信されません。
- Emergency (緊急) : このタイプのメッセージは、デバイスが危機的な状況にあり、緊急の対応が必要な場合にユーザに送信されます。
- Alert : このタイプのメッセージは、通常の設定とは異なるアクションが発生したときに

ユーザに送信されます。

- Critical：このタイプのメッセージは、ポートがダウンしているか、ユーザがネットワークにアクセスできない状況が発生したときにユーザに送信されます。早急な対策が必要です。
- エラー：設定エラーが発生すると、このタイプのメッセージがユーザに送信されます。
- 警告：このタイプのメッセージは、別のユーザが制限領域にアクセスしようとする時と送信されます。
- 通知：このタイプのメッセージは、ネットワーク上で優先度の低い変更が行われたときにユーザに送信されます。
- 情報：このタイプのメッセージは、ネットワークの動作を説明するためにユーザに送信されます。
- デバッグ：このタイプのメッセージは、ネットワークトラフィックのログとともにユーザに送信されます。

手順 6：緊急メッセージの重大度を設定するには、緊急、アラート、重大、エラー、警告、通知、情報、デバッグなど、送信する緊急メッセージの適切なタイプを選択します。これらのメッセージはすぐに送信されます。これらのオプションは、使用しているデバイスのモデルに応じて、Webベースのユーティリティで異なる方法で表示されます。

WAP131、WAP150、WAP351、およびWAP361の場合は、緊急メッセージの重大度のチェックボックスで該当する緊急メッセージタイプにチェックマークを付けます。



The image shows a configuration interface for message severity. It has two rows of checkboxes. The first row is labeled 'Scheduled Message Severity:' and has checkboxes for Emergency (checked), Alert (checked), Critical (checked), Error (checked), Warning (checked), Notice (unchecked), Info (unchecked), and Debug (unchecked). The second row is labeled 'Urgent Message Severity:' and has checkboxes for Emergency (checked), Alert (checked), Critical (unchecked), Error (unchecked), Warning (unchecked), Notice (unchecked), Info (unchecked), and Debug (unchecked). A red rectangular box highlights the 'Urgent Message Severity:' row.

WAP121、WAP321、WAP371、WAP551、WAP561、WAP571、およびWAP571Eの場合、緊急メッセージの重大度のドロップダウンリストで該当する緊急メッセージタイプをクリックします。

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

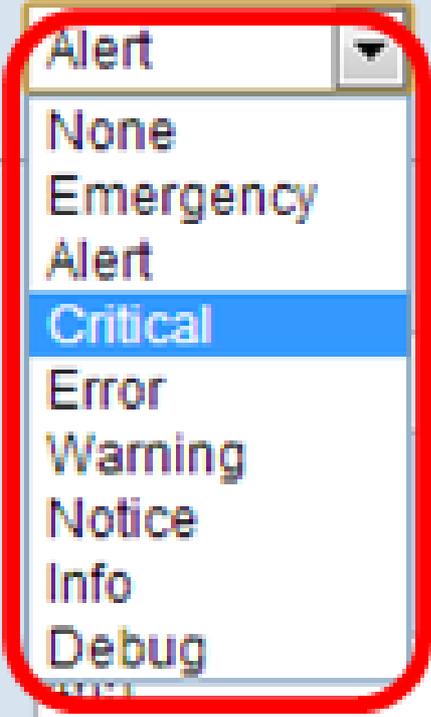
Urgent Message Severity:

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption:

Port:



- Alert
- None
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

注：このオプションを[なし]に設定すると、メッセージは送信されません。

手順 7：メールサーバの有効なホスト名またはIPアドレスをServer IPv4 Address/Nameフィールドに入力します。

注：次の例では、200.168.20.10が使用されています。

Mail Server Configuration

Server IPv4 Address/Name:

200.168.20.10

Data Encryption:

TLSv1

Port:

465

Username:

Cisco_1

Password:

.....

ステップ 8 : Data Encryption ドロップダウンリストからセキュリティモードを選択します。使用可能なオプションは次のとおりです。

- TLSv1: Transport Layer Security (TLS) バージョン 1 は、インターネット経由の通信にセキュリティとデータ整合性を提供する暗号化プロトコルです。
- Open : デフォルトの暗号化プロトコルですが、データ暗号化のセキュリティ対策はありません。

Mail Server Configuration

Server IPv4 Address/Name:

200.168.20.10

Data Encryption:

Open

TLSv1

Port:

465

Username:

Cisco_1

Password:

注：この例では、TLSv1が選択されています。「オープン」を選択した場合は、[ステップ12](#)に進んでください。

ステップ 9：メールサーバのポート番号をPortフィールドに入力します。これは、電子メールの送信に使用される発信ポート番号です。有効なポート番号の範囲は0 ~ 65535で、Simple Mail Transfer Protocol(SMTP)のデフォルトは465です。

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption:

Port:

Username:

Password:

ステップ 10 : Usernameフィールドに認証用のユーザ名を入力します。

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption:

Port:

Username:

Password:

注 : 例としてCisco_1を使用します。

ステップ 11 Passwordフィールドに認証用のパスワードを入力します。

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption: 

Port:

Username:

Password:

ステップ 12 Message Configurationの下で、To Email Address 1、2、および3フィールドに必要な電子メールアドレスを入力します。

注：要件に基づいて、すべての電子メールアドレスフィールドに値を入力するか、電子メールアドレスを1つだけ入力して残りのフィールドを空白のままにすることができます。

Message Configuration

To Email Address 1: (xyZXX@X000LJ00X)

To Email Address 2: (xyZXX@X000LJ00X)

To Email Address 3: (xyZXX@X000LJ00X)

Email Subject:

ステップ 13 Email Subjectフィールドに電子メールの件名を入力します。件名には、最大255文字の英数字を使用できます。

Message Configuration

To Email Address 1: (xyz0x@x000Lj00x)

To Email Address 2: (xyz0x@x000Lj00x)

To Email Address 3: (xyz0x@x000Lj00x)

Email Subject:

注：この例では、APからのログメッセージを使用しています。

ステップ 14：Test Mailをクリックして、設定したメールサーバのクレデンシャルを検証します。設定が機能していることを確認するために、設定された電子メールアドレスに電子メールが送信されます。

Message Configuration

To Email Address 1: (xyz0x@x000Lj00x)

To Email Address 2: (xyz0x@x000Lj00x)

To Email Address 3: (xyz0x@x000Lj00x)

Email Subject:

ステップ 15 : [Save] をクリックします。

The screenshot shows a web interface titled "Message Configuration". It contains four input fields for email addresses and one for the email subject. At the bottom, there are two buttons: "Save" and "Test Mail". The "Save" button is highlighted with a red rectangular border.

To Email Address 1:	Test_1@mail.com
To Email Address 2:	Test_2@mail.com
To Email Address 3:	Test_3@mail.com
Email Subject:	Log message from AP

Save Test Mail

ログ設定の構成

この領域では、揮発性およびNVRAMのシステムログとイベントログをローカルに設定します。

ステップ 1 : アクセスポイントのWebベースユーティリティにログインして、Administration > Log Settingsの順に選択します。

▶ Administration

System Settings

User Accounts

Time Settings

Log Settings

Email Alert

ステップ2: (オプション) ログを永続的に保存して、WAPのリブート時に設定が維持されるようにする場合は、 EnableチェックボックスをオンにしてPersistenceを有効にします。これは、望ましくないイベントまたは障害が発生したときに予期しないシステムの再起動が発生した場合に特に役立ちます。最大128個のログメッセージをNVRAMに保存でき、その後ログが上書きされます。

Log Settings

Options

Persistence:

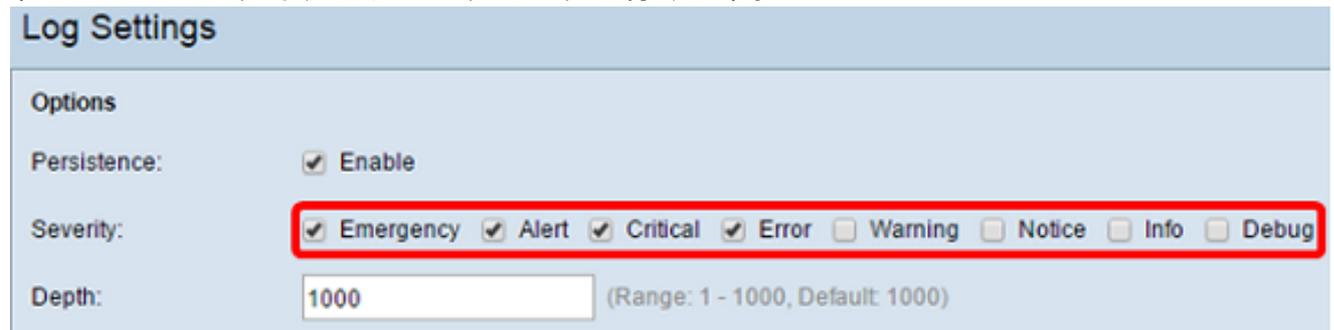


Enable

注 : Enableがオフの場合、ログは揮発性メモリに保存されます。

ステップ3 : 重大度を設定するには、送信するメッセージのタイプ (緊急、アラート、重大、エラー、警告、通知、情報、デバッグなど) を選択します。これらのメッセージは、ログ期間が経過するたびに送信されます。これらのオプションは、使用しているデバイスのモデルに応じて、Webベースのユーティリティで異なる方法で表示されます。

WAP131、WAP150、WAP351、およびWAP361の場合は、重大度のチェックボックスで適切なメッセージタイプにチェックマークを付けます。



Log Settings

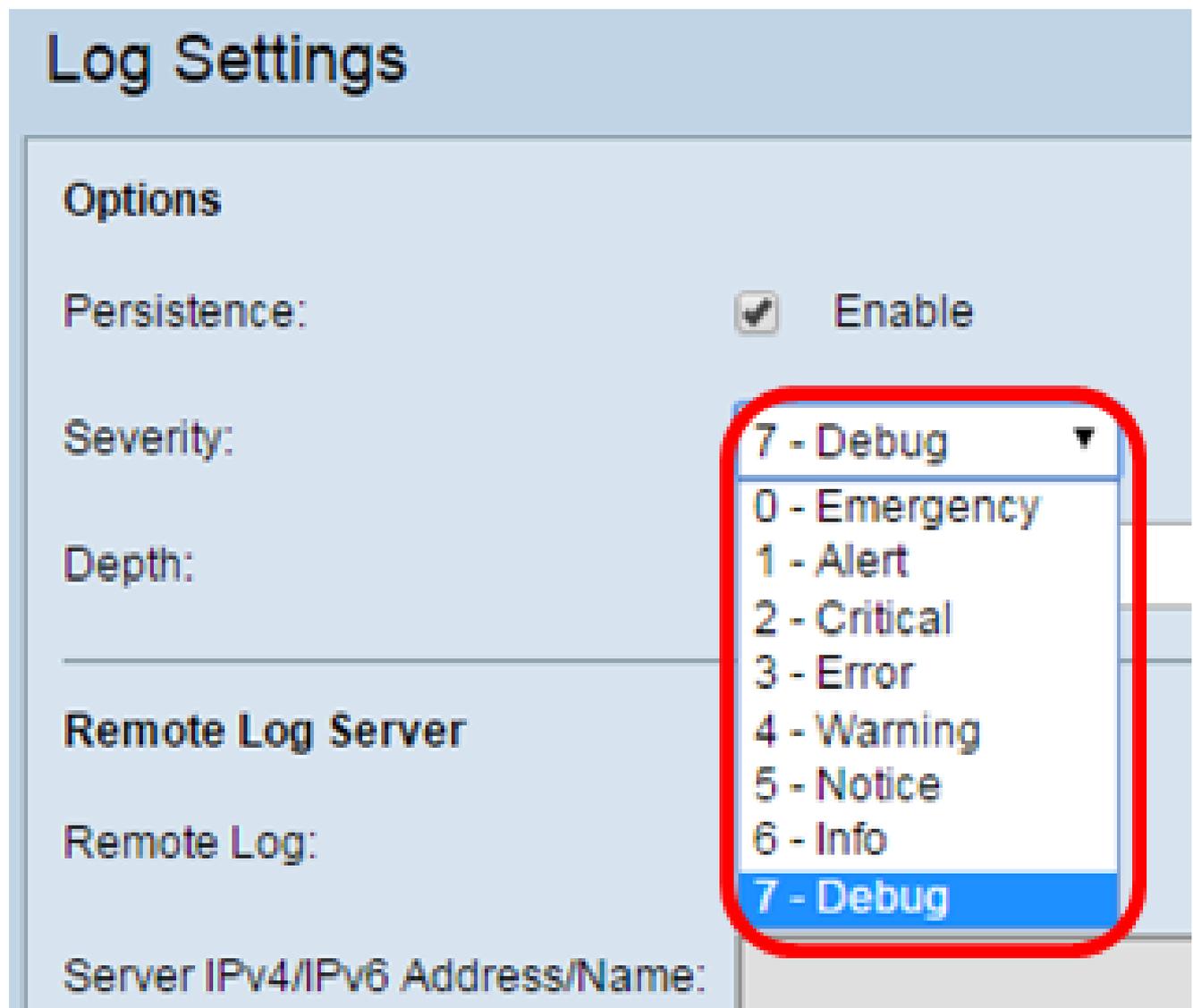
Options

Persistence: Enable

Severity: Emergency Alert Critical Error Warning Notice Info Debug

Depth: (Range: 1 - 1000, Default: 1000)

WAP121、WAP321、WAP371、WAP551、WAP561、WAP571、およびWAP571Eの場合、重大度ドロップダウンリストから適切なメッセージタイプをクリックします。



Log Settings

Options

Persistence: Enable

Severity:

Depth:

Remote Log Server

Remote Log:

Server IPv4/IPv6 Address/Name:

- None : メッセージは送信されません。
- Emergency (緊急) : このタイプのメッセージは、デバイスが危機的な状況にあり、緊急の対応が必要な場合にユーザに送信されます。
- Alert : このタイプのメッセージは、通常の設定とは異なるアクションが発生したときにユーザに送信されます。
- Critical : このタイプのメッセージは、ポートがダウンしているか、ユーザがネットワ

ークにアクセスできない状況が発生したときにユーザに送信されます。早急な対策が必要です。

- エラー：設定エラーが発生すると、このタイプのメッセージがユーザに送信されます。
- 警告：このタイプのメッセージは、別のユーザが制限領域にアクセスしようとするとき送信されます。
- 通知：このタイプのメッセージは、ネットワーク上で優先度の低い変更が行われたときにユーザに送信されます。
- 情報：このタイプのメッセージは、ネットワークの動作を説明するためにユーザに送信されます。
- デバッグ：このタイプのメッセージは、ネットワークトラフィックのログとともにユーザに送信されます。

ステップ4：ログメッセージが生成されると、送信のためにキューに入れられます。

Depthフィールドに、揮発性メモリ内で一度にキューイングできるメッセージの数を指定します。一度に最大512のメッセージをキューに入れることができます。

WAP131、WAP150、WAP351、およびWAP361の場合は、Depthフィールドに深さの範囲を入力します。範囲は1 ~ 1000です。デフォルト値は1000です。

The image shows a screenshot of a web interface titled "Log Settings". Under the "Options" section, there are three rows of settings:

- Persistence:** Enable
- Severity:** Emergency Alert (F)
- Depth:** (F)

The "Depth" input field is highlighted with a red rectangular border.

WAP121、WAP321、WAP371、WAP551、WAP561、WAP571、およびWAP571Eの場合は、Depthフィールドに深さの範囲を入力します。範囲は1 ~ 512で、デフォルトは512です。この例では、67が使用されます。

Log Settings

Options

Persistence: Enable

Severity: 7 - Debug ▼

Depth: 67

ステップ 5 : [Save] をクリックします。

注 : アクセスポイントは、Network Time Protocol(NTP)サーバを使用して日付と時刻の情報を取得します。このデータはUTC形式 (グリニッジ標準時) です。

これらの設定では、ローカルデバイスにイベントロギングを伝播し、電子メールアラートを受信する必要があります。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。