Einrichten von Systemmeldungsprotokollen (Syslogs) in einem CBW-Netzwerk

Ziel

In diesem Artikel wird das Festlegen und Überprüfen der Protokollierung für ein traditionelles oder Mesh-Netzwerk von Cisco Business Wireless (CBW) beschrieben.

Unterstützte Geräte | Softwareversion

Unterstützte Geräte | Firmware-Version

- 140AC (Datenblatt) | 10.4.1.0 (Laden Sie die aktuelle Version herunter)
- 145AC (Datenblatt) | 10.4.1.0 (Laden Sie die aktuelle Version herunter)
- 240AC (Datenblatt) | 10.4.1.0 (Laden Sie die aktuelle Version herunter)

Einleitung

Cisco Business Wireless Access Points basieren auf 802.11 a/b/g/n/ac (Wave 2) und verfügen über interne Antennen. Sie können als herkömmliche Standalone-Geräte oder als Teil eines Mesh-Netzwerks verwendet werden.

Sobald Ihr Netzwerk eingerichtet ist, können Dinge passieren, die Aufmerksamkeit erfordern könnten. Um sich über diese Ereignisse im Klaren zu bleiben, können Sie die Systemmeldungsprotokolle überprüfen, die häufig als Syslogs bezeichnet werden.

Wenn Sie sich über Ereignisse im Klaren sind, können Sie einen reibungslosen Netzwerkbetrieb sicherstellen und Ausfälle verhindern. Syslogs sind nützlich für die Fehlerbehebung im Netzwerk, das Debuggen des Paketflusses und die Überwachung von Ereignissen.

Diese Protokolle können auf der Webbenutzeroberfläche des primären Access Points und, falls konfiguriert, auf Remote-Protokollservern angezeigt werden. Ereignisse werden normalerweise beim Neustart aus dem System gelöscht, wenn sie nicht auf einem Remote-Server gespeichert werden.

Einrichten von Systemmeldungsprotokollen

In diesem umblätterten Abschnitt finden Sie Tipps für Anfänger.

Anmeldung

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie https://ciscobusiness.cisco ein. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein. Sie können auch auf den primären Access Point zugreifen, indem Sie https://[ipaddress] (des primären Access Points) in einen Webbrowser eingeben.

Quick-Info

Wenn Sie Fragen zu einem Feld in der Benutzeroberfläche haben, suchen Sie nach einem Tooltipp, der wie folgt aussieht:

Probleme beim Auffinden des Symbols "Hauptmenü erweitern"?

Navigieren Sie zum Menü auf der linken Seite des Bildschirms. Wenn Sie die Menütaste nicht sehen, klicken Sie auf dieses Symbol, um das Menü auf der Seitenleiste zu öffnen.

Cisco Business-App

Diese Geräte verfügen über begleitende Apps, die einige Verwaltungsfunktionen mit der Webbenutzeroberfläche teilen. Nicht alle Funktionen der Webbenutzeroberfläche sind in der App verfügbar.

iOS-App herunterladen Android-App herunterladen

Häufig gestellte Fragen

Wenn Sie immer noch offene Fragen haben, können Sie sich unser Dokument mit häufig gestellten Fragen ansehen. Häufig gestellte Fragen

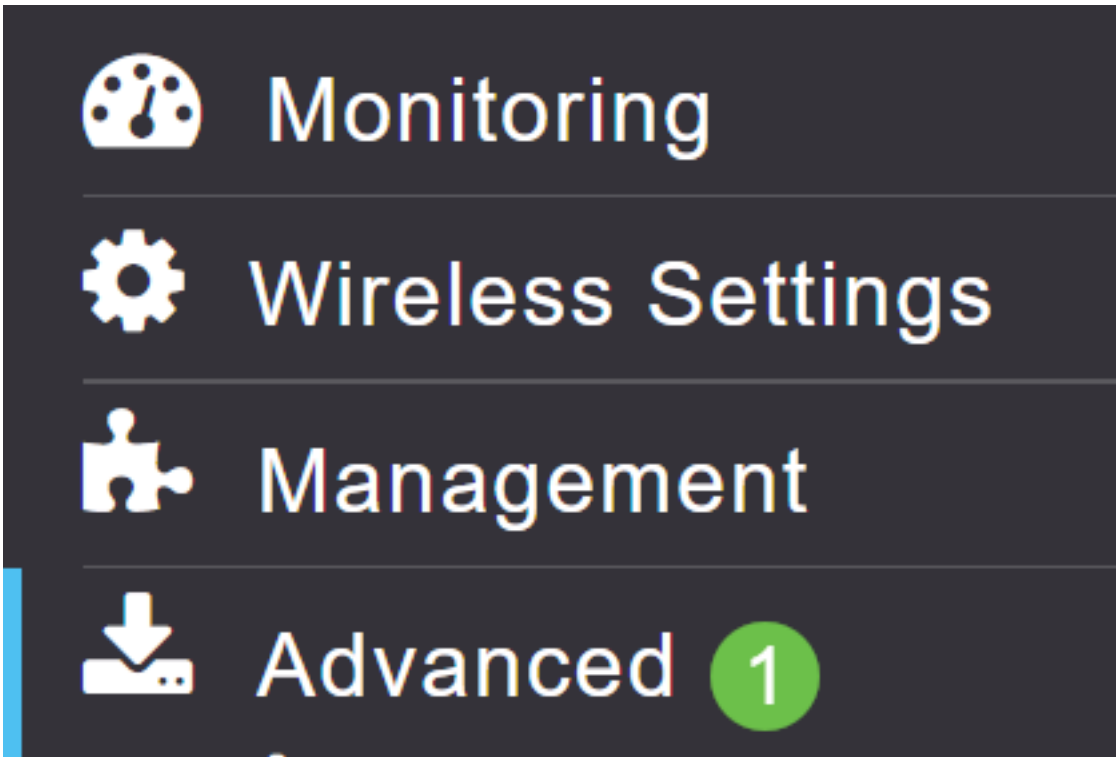
Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie *https://ciscobusiness.cisco ein*. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein.

Sie können auch auf den primären Access Point zugreifen, indem Sie *https://<ipaddress>* (des primären Access Points) in einen Webbrowser eingeben. Für einige Aktionen können Sie sich an die Cisco Business Mobile-App wenden.

Schritt 2

Wählen Sie **Erweitert > Protokollierung aus**.

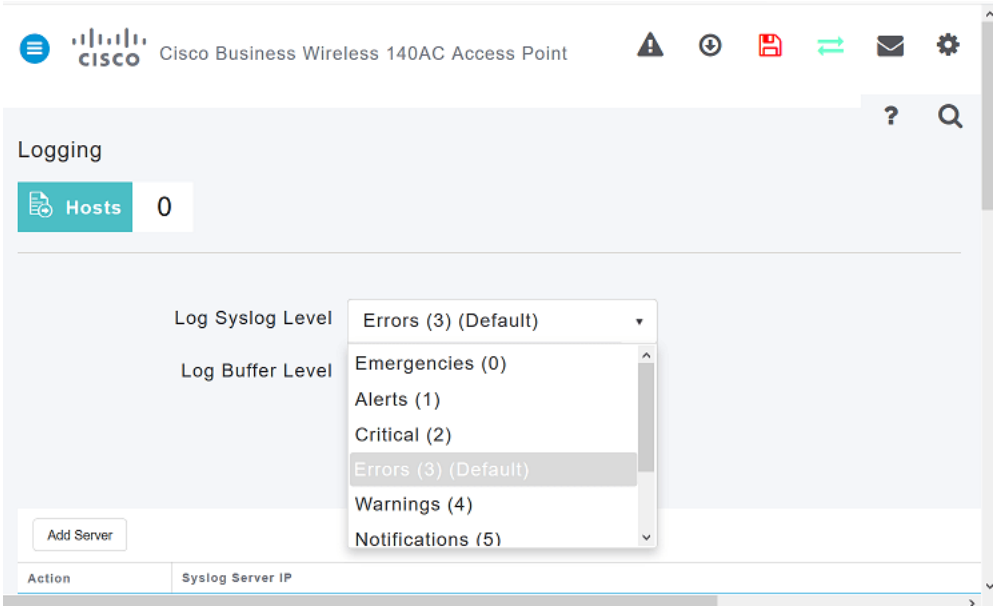


Schritt 3

Klicken Sie auf Syslog-Protokollebene. Wählen Sie aus dem Dropdown-Menü die Benachrichtigungsebene aus. Der Standardwert ist "Fehler (3)". Dies bedeutet, dass alle Schweregrade 3 oder höher protokolliert werden.

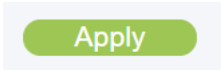
Angezeigt in der Reihenfolge des Schweregrads:

- *Notfälle* (Höchster Schweregrad): Diese Art von Meldung wird protokolliert, wenn sich das Gerät in einer kritischen Situation befindet und sofortige Aufmerksamkeit erforderlich ist. Das System ist unbrauchbar.
- *Warnungen*: Dieser Meldungstyp wird protokolliert, wenn eine Bedingung vorliegt, die sofortige Aufmerksamkeit erfordert.
- *Kritisch*
- *Fehler* (Standardeinstellung)
- *Warnungen*
- *Benachrichtigungen*
- *Informativ*
- *Debuggen* (niedrigster Schweregrad) - Dieser wird normalerweise nur verwendet, wenn Sie die Fehlerbehebung aktiv durchführen, da Sie ziemlich schnell mit Protokollen überflutet werden.



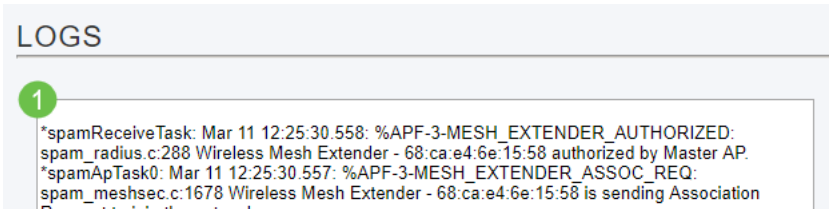
Schritt 4

Klicken Sie auf **Apply** (Anwenden).



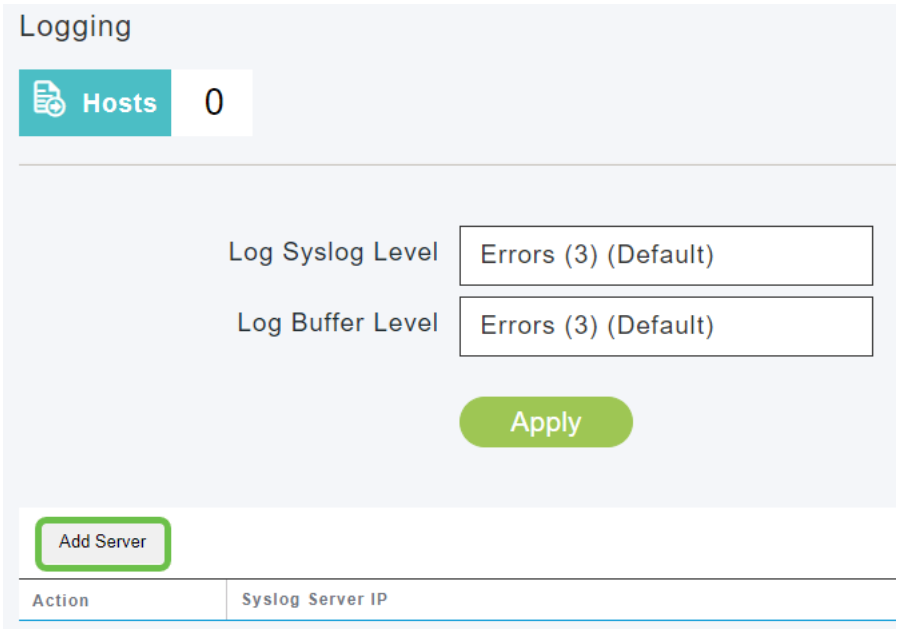
Schritt 5

Protokolle werden angezeigt, wenn Sie die *Protokollierungsseite* nach unten scrollen. Klicken Sie auf **Löschen**, wenn Sie die Protokolle löschen möchten. Wenn Sie keinen Syslog-Remote-Server einrichten möchten, fahren Sie mit Schritt 8 fort.



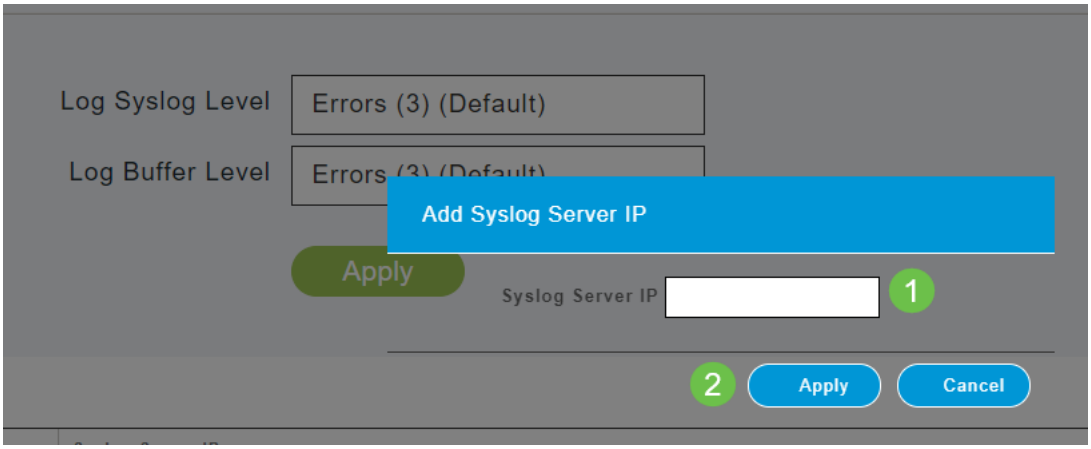
Schritt 6 (optional)

Wenn die Protokolle an einen Remote-Server gesendet werden sollen, klicken Sie auf **Server hinzufügen**.



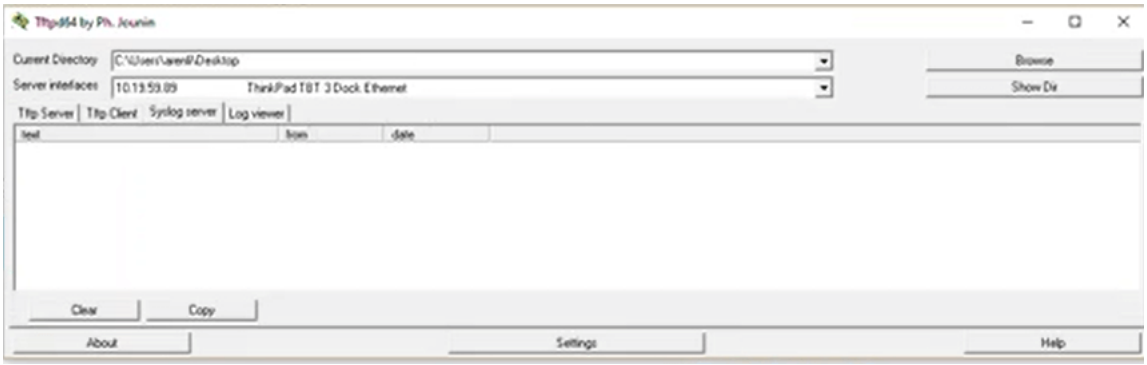
Schritt 7 (optional)

Geben Sie im Feld *Syslog Server IP (Syslog-Server-IP*) die IPv4-Adresse des Servers ein, an den die Syslog-Meldungen gesendet werden sollen. Klicken Sie auf **Apply** (Anwenden).



Schritt 8

Sie müssen einen TFTP-Server mit aktivierter Syslog-Funktion öffnen lassen, damit die Protokolle an eine Datei auf dem Server gesendet werden können.



Schritt 9

Speichern Sie Ihre Konfigurationen, indem Sie im rechten oberen Bereich der Webbenutzeroberfläche auf das **Symbol Speichern** klicken.

Beispiel für ein Systemmeldungsprotokoll

In diesem Beispiel zeigt die Meldung eine hohe Datenverkehrsauslastung. Wenn dies in den Syslogs auftaucht, würden Sie den Funkfrequenzkanal wahrscheinlich in einen ändern wollen, der weniger beschwört ist, um eine stabilere Betriebsumgebung zu schaffen.

*RRM-DCLNT-5_0: Dec 25 16:51:34:543: %RRM-3-HIGHCHANNEL_UTN: mmLrad.c:7678 Interference is high on AP: APA453.0E1F.E480 [Level: 85] on Radio: 5Ghz(Radio2)

Schlussfolgerung

Sie haben nun Zugriff auf die Systemprotokolle. Sie können jederzeit den Schweregrad ändern oder einen Remote-Server hinzufügen. Dies soll Ihnen helfen, über potenzielle Probleme im Netzwerk auf dem Laufenden zu bleiben.

Häufig gestellte Fragen RADIUS Firmware-Upgrade RLANs Erstellung von Anwendungsprofilen Client-Profilerstellung Primäre AP-Tools Umbrella WLAN-Benutzer Protokollieren Traffic Shaping Schurken Störungsquelle Konfigurationsverwaltung Port-Konfigurations-Mesh-Modus