

Konfiguration und Status der Protokolleinstellungen auf WAP121- und WAP321-Access Points

Ziel

Systemprotokolle sind Nachrichtensätze, die Systemereignisse aufzeichnen. Mithilfe von Protokollen können Sie den Status des Geräts verwalten. Sie werden auch zum Debuggen des Paketflusses und zum Überwachen von Ereignissen verwendet. Protokolle werden in der Regel im flüchtigen Speicher gespeichert, d. h. die Protokolle werden gelöscht, wenn der WAP zurückgesetzt oder ausgeschaltet wird. Sie können Protokolle jedoch in nichtflüchtigen (permanenten) Speicher speichern, wenn Sie die Protokolle behalten müssen. Dies kann von Vorteil sein, wenn Sie ein Problem debuggen müssen. Dieses Dokument führt Sie durch die Konfiguration der Protokolleinstellungen und erläutert den Protokollstatus auf dem WAP121 und WAP321.

Anwendbare Geräte

WAP121
WAP321

Softwareversion

·1,0/3,4

Protokolleinstellungen

Vorsicht: Die permanente Protokollierung kann die Leistung des Flash-Speichers (nicht flüchtig) und auch die Netzwerkleistung reduzieren. Die permanente Protokollierung sollte nur verwendet werden, wenn ein Problem gedebuggt werden soll. Stellen Sie sicher, dass Sie die permanente Protokollierung nach Abschluss deaktivieren.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Administration > Log Settings (Verwaltung > Protokolleinstellungen)**. Die Seite "*Protokolleinstellungen*" wird geöffnet:

Log Settings

Options

Persistence: Enable

Severity: 7 - Debug

Depth: 512 (Range: 1 - 512, Default)

Remote Log Server

Remote Log: Enable

Server IPv4/IPv6 Address/Name:

UDP Port: 514 (Range: 1 - 65535, Default)

Save

Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Persistence (Persistenz), um die Persistenzfunktion zu aktivieren, mit der die Systemprotokolle beim Neustart des Geräts im nichtflüchtigen RAM (NVRAM) gespeichert werden. Dadurch werden Protokolle beim Neustart des Geräts nicht gelöscht. Im NVRAM können bis zu 128 Protokollmeldungen gespeichert werden. Wenn die Protokolle mehr als 128 Meldungen überschreiten, überschreiben die neuen die alten Protokolle.

Log Settings

Options

Persistence: Enable

Severity: 7 - Debug

Depth: 512 (Range: 1 - 512, Default)

Remote Log Server

Remote Log: Enable

Server IPv4/IPv6 Address/Name:

UDP Port: 514 (Range: 1 - 65535, Default)

Save

Schritt 3: Wählen Sie den Schweregrad aus der Dropdown-Liste Severity (Schweregrad) aus. Alle Protokolle mit dem gewählten Schweregrad oder höher werden protokolliert. Folgende Schweregrade sind verfügbar:

- Notfall - Eine Panik, die mehrere Anwendungen und Standorte betrifft.
- Warnung - Wenn eine Warnmeldung protokolliert wird, muss das Gerät sofort reagieren.

- Critical (Kritisch): Das System befindet sich in einem kritischen Zustand. Es müssen bestimmte Maßnahmen ergriffen werden, um die Situation zu überwinden, wenn Sie diese Botschaft sehen.
- Fehler - Es ist ein Systemfehler aufgetreten, z. B. nicht dringende Fehler. Diese müssen innerhalb einer bestimmten Zeit behoben werden.
- Warnung: Kein Fehler, sondern ein Hinweis darauf, dass ein Fehler auftritt, wenn keine Maßnahmen ergriffen werden.
- Hinweis: Das System funktioniert einwandfrei, es ist jedoch ein Systembenachrichtigungsvorgang aufgetreten. Dies sind Ereignisse, die ungewöhnlich sind, aber keine Fehlerzustände.
- Information - Stellt Geräteinformationen bereit.
- Debug - Stellt detaillierte Informationen zum Debuggingtyp und zur Debugzeit bereit.

Log Settings

Options

Persistence: Enable

Severity: 7 - Debug

Depth: 500

Remote Log Server

Remote Log: Enable

Server IPv4/IPv6 Address/Name: 192.168.0.1

UDP Port: 520

Save

Schritt 4: Geben Sie im Feld Tiefe die maximale Anzahl von Nachrichten ein, die im flüchtigen Speicher gespeichert werden können. Standardmäßig stellt ein Access Point bis zu 512 Nachrichten in die Warteschlange.

Schritt 5: (Optional) Wenn Sie die Protokollmeldungen an einen Remote-Syslog-Server senden möchten, aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Remote Log (Remote-Protokoll).

Zeitgeber: Wenn Sie das Kontrollkästchen Aktivieren nicht aktivieren, fahren Sie mit Schritt 8 fort.

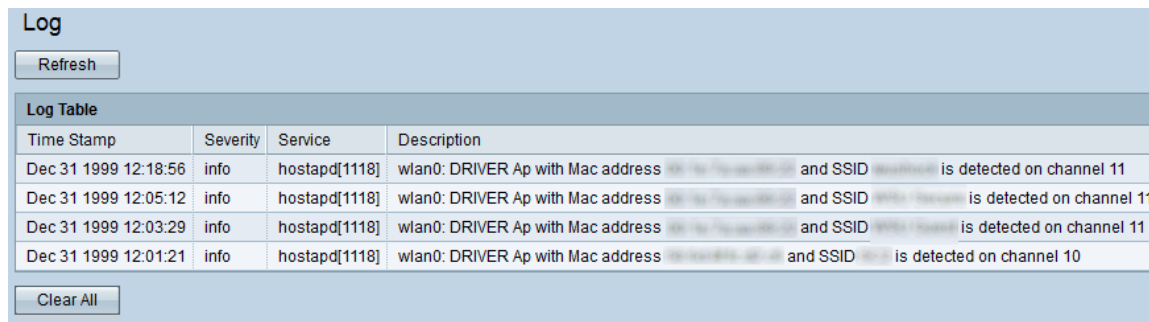
Schritt 6: Geben Sie den Domännennamen oder die IP-Adresse des Syslog-Servers in das Feld IPv4/IPv6 Address/Name des Servers ein.

Schritt 7: Geben Sie die Nummer des UDP-Ports des Syslog-Servers ein, an den die Protokolle im Feld "UDP Port" gesendet werden. Der Standard-Port ist 514.

Schritt 8: Klicken Sie auf **Speichern**, um die vorgenommenen Änderungen zu speichern.

Protokollstatus und Statistiken

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Status und Statistiken > Protokoll aus**. Die Seite *Log* (Protokoll) wird geöffnet:



Time Stamp	Severity	Service	Description
Dec 31 1999 12:18:56	info	hostapd[1118]	wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 11
Dec 31 1999 12:05:12	info	hostapd[1118]	wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 11
Dec 31 1999 12:03:29	info	hostapd[1118]	wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 11
Dec 31 1999 12:01:21	info	hostapd[1118]	wlan0: DRIVER Ap with Mac address [redacted] and SSID [redacted] is detected on channel 10

Die Protokolltabelle verfügt über folgende Felder:

- Zeitstempel - Zeigt den Monat, den Tag, das Jahr und die Uhrzeit an, zu der das Protokoll erstellt wurde.
- Severity (Schweregrad): Zeigt den Schweregrad des Ereignisses an.
- Service - Die Softwarekomponente für das Ereignis.
- Description (Beschreibung): Zeigt eine Informationsmeldung an, die das protokollierte Ereignis beschreibt.

Schritt 2: (Optional) Wenn Sie die Protokolle löschen möchten, klicken Sie auf **Alle löschen**.

Schritt 3: (Optional) Wenn Sie die Protokolltabelle aktualisieren möchten, klicken Sie auf **Aktualisieren**.