

Protokolleinstellungen Konfiguration und Protokollstatus auf WAP551- und WAP561-Zugangspunkten

Ziel

Systemprotokolle sind Datensätze von Systemereignissen. Sie eignen sich für die Fehlerbehebung im Netzwerk, das Debuggen des Paketflusses und die Überwachung von Ereignissen. Diese Protokolle können im RAM, im NVRAM und auf Remote-Protokollservern gespeichert werden. Mithilfe von Protokollen können Sie den Status des Geräts verwalten. Dieses Dokument beschreibt die Konfiguration der Protokolleinstellungen und erläutert den Protokollstatus auf dem WAP551 und dem WAP561.

Anwendbare Geräte

WAP551
WAP561

Softwareversion

·1,0/4,2

Protokolleinstellungen

Schritt 1: Melden Sie sich beim Konfigurationsprogramm für Access Points an, um **Administration > Log Settings (Verwaltung > Protokolleinstellungen)** auszuwählen. Die Seite "*Protokolleinstellungen*" wird geöffnet:

Log Settings

Options

Persistence: Enable

Severity: 7 - Debug

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

Remote Log Server

Remote Log: Enable

Server IPv4/IPv6 Address/Name: (xxx.xxx.xxx.x /Hostname)

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

Save

Schritt 2: (Optional) Wenn die Protokolle dauerhaft gespeichert werden sollen, damit sie beim Neustart des WAP nicht verloren gehen, aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Persistence (Persistenz), um die Persistenz-Funktion zu aktivieren. Dies ist besonders dann nützlich, wenn das System unerwartet neu startet, wenn ein unerwünschtes Ereignis oder ein Fehler auftritt. Im NVRAM können bis zu 128 Protokollmeldungen gespeichert werden, nach denen die Protokolle überschrieben werden. Wenn Enable (Aktivieren) deaktiviert ist, werden Protokolle im flüchtigen Speicher gespeichert.

Log Settings

Options

Persistence: Enable

Severity: 7 - Debug

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

Remote Log Server

Remote Log: Enable

Server IPv4/IPv6 Address/Name: (xxx.xxx.x /Hostname)

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

Save

Schritt 3: Wählen Sie den Schweregrad aus der Dropdown-Liste Severity (Schweregrad) aus. Der gewählte Schweregrad umfasst alle höheren Ebenen, daher werden Protokolle für alle Schweregrade von der obersten Ebene bis zur gewählten Ebene aufbewahrt. Folgende Schweregrade sind verfügbar:

- Notfall - Eine Panik, die mehrere Anwendungen und Server/Standorte betrifft.

·Warnung - Für diese Art von Bedingung muss sofort gehandelt werden. Der Zustand muss sofort behoben werden.

·Critical (Kritisch): Das System befindet sich in einem kritischen Zustand. Dieser Protokolltyp gibt einen Fehler im primären System an. Außerdem muss es sofort adressiert werden.

·Fehler - Ein nicht dringender Systemfehler ist aufgetreten. Diese müssen innerhalb einer bestimmten Zeit behoben werden.

·Warnung: Es ist noch kein Fehler aufgetreten, aber ein Hinweis darauf, dass dieser Vorgang durchgeführt wird, 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. Sie können nützlich sein, um Bedingungen zu erkennen, die einen potenziellen Fehler verursachen können.

·Information - Stellt Geräteinformationen bereit. Möglicherweise für Berichtszwecke erforderlich.

·Debuggen - Stellt detaillierte Informationen zum Protokoll bereit, die für das Debuggen nützlich sind.

Schritt 4: Wenn Protokollmeldungen generiert werden, werden sie zur Übertragung in eine Warteschlange gestellt. Das Feld Tiefe gibt die Anzahl der Meldungen an, die im flüchtigen Speicher gleichzeitig in die Warteschlange gestellt werden können. Es können gleichzeitig bis zu 512 Nachrichten in die Warteschlange gestellt werden. Geben Sie die gewünschte Warteschlangenlänge in das Feld Tiefe ein.

Log Settings

Options

Persistence: Enable

Severity: 7 - Debug

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

Remote Log Server

Remote Log: Enable

Server IPv4/IPv6 Address/Name: 192.168.x.x (xxx.xxx.xxx /Hostname)

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

Save

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 aktiviert haben, überspringen Sie die Schritte 6 und 7. Fahren Sie mit Schritt 8 fort.

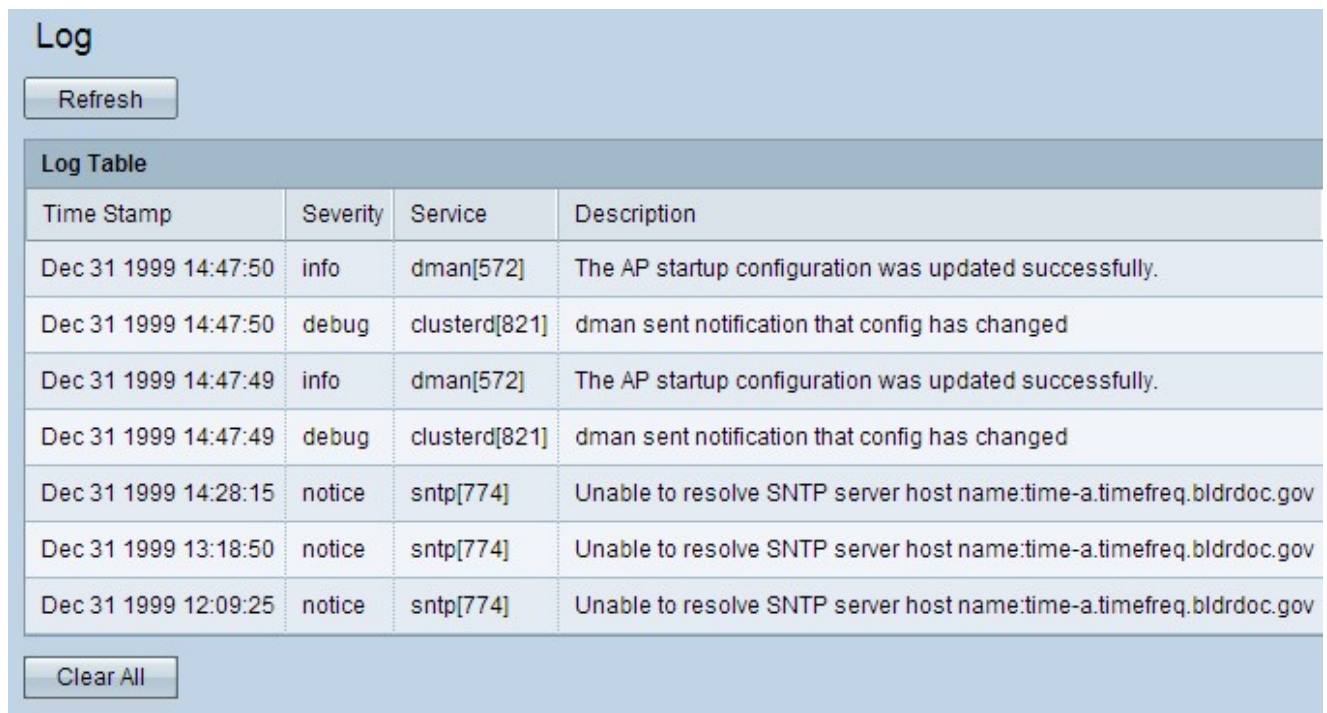
Schritt 6: Geben Sie den Domännennamen oder die IP-Adresse des Syslog-Servers in das Feld IPv4/IPv6 Address/Name des Servers ein.

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 Einstellungen zu speichern.

Protokollstatus und Statistiken

Schritt 1: Melden Sie sich beim Konfigurationsprogramm für Access Points an, um **Status und Statistiken > Protokoll** auszuwählen. Die Seite *Protokoll* wird geöffnet.



Time Stamp	Severity	Service	Description
Dec 31 1999 14:47:50	info	dman[572]	The AP startup configuration was updated successfully.
Dec 31 1999 14:47:50	debug	clusterd[821]	dman sent notification that config has changed
Dec 31 1999 14:47:49	info	dman[572]	The AP startup configuration was updated successfully.
Dec 31 1999 14:47:49	debug	clusterd[821]	dman sent notification that config has changed
Dec 31 1999 14:28:15	notice	sntp[774]	Unable to resolve SNTP server host name:time-a.timefreq.bldrdoc.gov
Dec 31 1999 13:18:50	notice	sntp[774]	Unable to resolve SNTP server host name:time-a.timefreq.bldrdoc.gov
Dec 31 1999 12:09:25	notice	sntp[774]	Unable to resolve SNTP server host name:time-a.timefreq.bldrdoc.gov

Die Protokolltabelle verfügt über folgende Felder:

- Zeitstempel - Dieses Feld zeigt den Monat, den Tag, das Jahr und die Uhrzeit an, zu der das Protokoll erstellt wurde.
- Severity (Schweregrad): Dieses Feld zeigt den Schweregrad des Ereignisses an.
- Service - In diesem Feld wird der Service oder die Softwarekomponente angezeigt, die das Protokoll generiert hat.
- Description (Beschreibung): Dieses Feld beschreibt das protokollierte Ereignis.

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**.