

Konfigurieren der Ereignisprotokollierung auf einem Wireless Access Point

Ziel

Systemereignisse sind Aktivitäten, die möglicherweise Aufmerksamkeit erfordern und erforderliche Maßnahmen erfordern, um das System reibungslos auszuführen und Ausfälle zu verhindern. Diese Ereignisse werden als Protokolle aufgezeichnet. Mithilfe von Systemprotokollen kann der Administrator bestimmte Ereignisse auf dem Gerät verfolgen.

Ereignisprotokolle sind nützlich für die Fehlerbehebung im Netzwerk, das Debuggen des Paketflusses und die Überwachung von Ereignissen. Diese Protokolle können im RAM (Random Access Memory), im NVRAM (Non-volatile Random Access Memory) und auf Remote-Protokollservern gespeichert werden. Diese Ereignisse werden normalerweise beim Neustart aus dem System gelöscht. Wenn das System unerwartet neu startet, können Systemereignisse nur angezeigt werden, wenn sie im nichtflüchtigen Speicher gespeichert werden. Wenn die Persistence-Protokollierungsfunktion aktiviert ist, werden Systemereignismeldungen in den nichtflüchtigen Speicher geschrieben.

Protokolleinstellungen definieren die Protokollierungsregeln und Ausgabeziele für Meldungen, Benachrichtigungen und andere Informationen, wenn im Netzwerk verschiedene Ereignisse aufgezeichnet werden. Diese Funktion benachrichtigt verantwortliches Personal, sodass bei einem Ereignis die erforderlichen Maßnahmen ergriffen werden. Protokolle können ihnen auch per E-Mail-Benachrichtigung gesendet werden.

In diesem Dokument werden die verschiedenen Konfigurationen erläutert und erläutert, wie Sie System- und Ereignisprotokolle erhalten.

Anwendbare Geräte

WAP100-Serie

WAP300-Serie

WAP500-Serie

Softwareversion

1.0.1.4 — WAP131, WAP351

1.0.6.2 — WAP121, WAP321

1.2.1.3 — WAP371, WAP551, WAP561

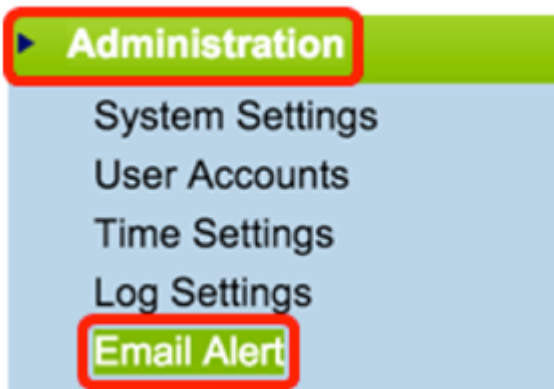
1.0.1.2 — WAP150, WAP361

1.0.0.17 — WAP571, WAP571E

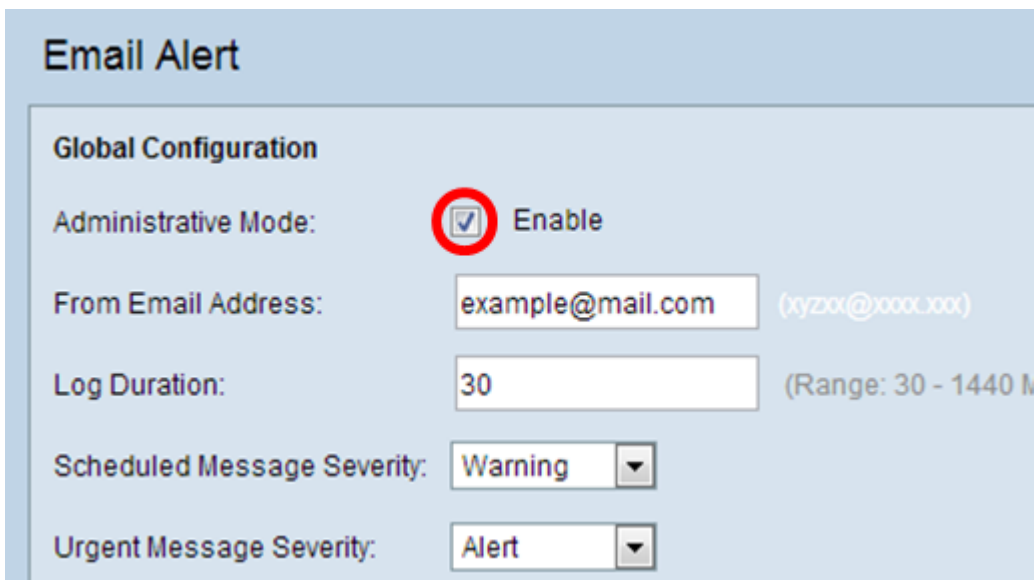
Konfigurieren der Ereignisprotokollierung

E-Mail-Benachrichtigung konfigurieren

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Administration > Email Alert** aus.



Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Verwaltungsmodus, um die E-Mail-Warnfunktion global zu aktivieren.

A screenshot of the 'Email Alert' configuration page. The page has a light blue background. At the top, the title 'Email Alert' is displayed. Below the title is a section titled 'Global Configuration'. In this section, there are several configuration items: 'Administrative Mode:' with a checked checkbox (circled in red) and the text 'Enable'; 'From Email Address:' with a text input field containing 'example@mail.com' and a placeholder '(xyz@xxx.xxx)'; 'Log Duration:' with a text input field containing '30' and a placeholder '(Range: 30 - 1440 M)'; 'Scheduled Message Severity:' with a dropdown menu showing 'Warning'; and 'Urgent Message Severity:' with a dropdown menu showing 'Alert'.

Schritt 3: Geben Sie eine E-Mail-Adresse in das Feld *Von E-Mail-Adresse ein*. Die Adresse wird als Absender der E-Mail-Warnung angezeigt. Der Standardwert ist null.

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

Hinweis: Es wird dringend empfohlen, ein separates E-Mail-Konto zu verwenden, anstatt Ihre persönliche E-Mail-Adresse zu verwenden, um die Privatsphäre zu wahren.

Schritt 4: Geben Sie im Feld *Log Duration (Dauer des Protokolls)* die Uhrzeit (in Minuten) ein, wie oft die E-Mail-Warnmeldungen an die konfigurierte E-Mail-Adresse gesendet werden sollen. Der Bereich liegt zwischen 30 und 1440 Minuten, der Standardwert ist 30.

Email Alert

Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

Schritt 5: Um den Schweregrad der geplanten Nachricht festzulegen, wählen Sie den entsprechenden Meldungstyp aus, der gesendet werden soll, z. B. Emergency, Alert, Critical, Error, Warning, Notice, Info oder Debug. Diese Meldungen werden bei jedem Ablauf der Protokolldauer gesendet. Diese Optionen werden je nach verwendetem Gerät im webbasierten Dienstprogramm unterschiedlich angezeigt.

Aktivieren Sie für WAP131, WAP150, WAP351 und WAP361 in den Kontrollkästchen für den Schweregrad der geplanten Nachricht den entsprechenden Meldungstyp.

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

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

Klicken Sie für WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 und WAP571E in der Dropdown-Liste "Scheduled Message Severity" (Schweregrad der geplanten Nachrichten) auf den entsprechenden Meldungstyp.


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

Keine - Es werden keine Nachrichten gesendet.

Emergency (Notfall): Diese Art von Nachricht wird an den Benutzer gesendet, wenn sich das Gerät in einer kritischen Situation befindet und sofortige Aufmerksamkeit erforderlich ist.

Alert (Warnung): Dieser Meldungstyp wird an den Benutzer gesendet, wenn eine Aktion auftritt, die von der normalen Konfiguration abweicht.

Critical (Kritisch) - Diese Art von Nachricht wird an den Benutzer gesendet, wenn ein Port ausfällt oder der Benutzer nicht auf das Netzwerk zugreifen kann. Sofortige Maßnahmen sind erforderlich.

Fehler: Diese Art von Meldung wird an den Benutzer gesendet, wenn ein Konfigurationsfehler auftritt.

Warnung - Diese Art von Nachricht wird an den Benutzer gesendet, wenn ein anderer Benutzer versucht, auf die Bereiche mit Zugangsbeschränkung zuzugreifen.

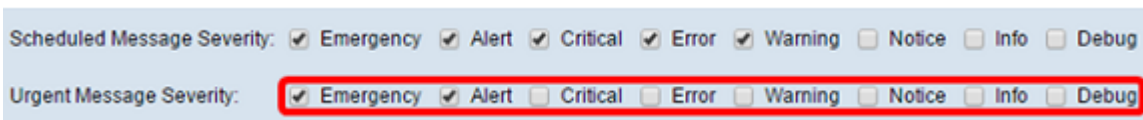
Hinweis: Diese Art von Nachricht wird an den Benutzer gesendet, wenn im Netzwerk Änderungen mit niedriger Priorität vorgenommen werden.

Info - Dieser Meldungstyp wird an den Benutzer gesendet, um das Verhalten des Netzwerks zu beschreiben.

Debug - Diese Art von Nachricht wird mit den Protokollen des Netzwerkverkehrs an den Benutzer gesendet.

Schritt 6: Um den DringlichkeitsSchweregrad der Nachricht festzulegen, wählen Sie die entsprechende Dringlichkeitsmeldung aus, die gesendet werden soll, z. B. Emergency, Alert, Critical, Error, Warning, Notice, Info oder Debug. Diese Nachrichten werden sofort gesendet. Diese Optionen werden je nach verwendetem Gerät im webbasierten Dienstprogramm unterschiedlich angezeigt.

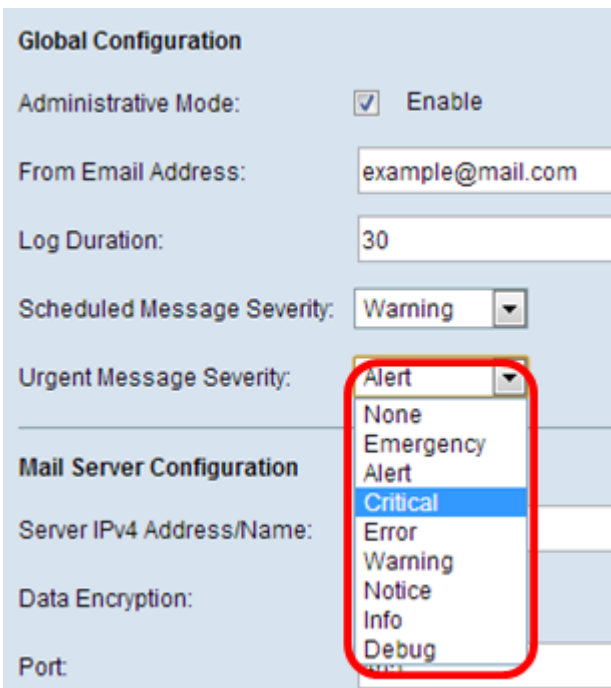
Aktivieren Sie für WAP131, WAP150, WAP351 und WAP361 in den Kontrollkästchen für den Dringlichkeitsschweregrad der Nachricht die entsprechenden Dringlichkeitsmeldungen.



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

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

Für WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 und WAP571E klicken Sie in der Dropdown-Liste "Urgent Message Severity" (Dringlichkeitsmeldungen) auf den entsprechenden Meldungstyp.



Global Configuration

Administrative Mode: Enable

From Email Address:

Log Duration:

Scheduled Message Severity:

Urgent Message Severity:

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

Mail Server Configuration

Server IPv4 Address/Name:

Data Encryption:

Port:

Hinweis: Wenn die Option auf Keine eingestellt ist, werden keine Nachrichten gesendet.

Schritt 7: Geben Sie im Feld *IPv4-Adresse/Name* des *Servers* den gültigen Hostnamen des Mailservers oder die gültige IP-Adresse ein.

Hinweis: Im Beispiel unten wird 200.168.20.10 verwendet.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Schritt 8: Wählen Sie den Sicherheitsmodus aus der Dropdown-Liste Datenverschlüsselung aus. Folgende Optionen stehen zur Verfügung:

- TLSv1 - Transport Layer Security Version 1 ist ein kryptografisches Protokoll, das Sicherheit und Datenintegrität für die Kommunikation über das Internet bietet.
- Offen - Es ist das Standard-Verschlüsselungsprotokoll, aber es gibt keine Sicherheitsmaßnahmen für die Datenverschlüsselung.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: Open
✓ TLSv1

Port: 465

Username: Cisco_1

Password:

Hinweis: In diesem Beispiel wird TLSv1 ausgewählt. Wenn Sie Öffnen ausgewählt haben, fahren Sie mit [Schritt 12 fort](#).

Schritt 9: Geben Sie die Portnummer des Mailservers im Feld *Port ein*. Es ist eine ausgehende Portnummer, die zum Senden von E-Mails verwendet wird. Der gültige Port-Nummernbereich liegt zwischen 0 und 65535, der Standardwert ist 465 für das Simple Mail Transfer Protocol (SMTP).

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Schritt 10: Geben Sie den Benutzernamen für die Authentifizierung im Feld *Benutzername ein*.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

Hinweis: Als Beispiel wird Cisco_1 verwendet.

Schritt 11: Geben Sie das Kennwort für die Authentifizierung in das Feld *Kennwort* ein.

Mail Server Configuration

Server IPv4 Address/Name: 200.168.20.10

Data Encryption: TLSv1

Port: 465

Username: Cisco_1

Password:

[Schritt 12](#): Geben Sie unter Nachrichtenkonfiguration die gewünschte E-Mail-Adresse in die Felder *E-Mail-Adresse 1, 2 und 3* ein.

Hinweis: Je nach Anforderung können Sie entweder Werte in alle Felder für *E-Mail-Adressen* eingeben oder nur eine E-Mail-Adresse eingeben und die restlichen Felder leer lassen.

Message Configuration

To Email Address 1: Test_1@mail.com (xyz@xxx.xxx)

To Email Address 2: Test_2@mail.com (xyz@xxx.xxx)

To Email Address 3: Test_3@mail.com (xyz@xxx.xxx)

Email Subject: Log message from AP

Save Test Mail

Schritt 13: Geben Sie den Betreff der E-Mail in das Feld *E-Mail-Betreff* ein. Der Betreff kann bis zu 255 alphanumerische Zeichen enthalten.

Message Configuration

To Email Address 1: (xyz@xxx.xxx)

To Email Address 2: (xyz@xxx.xxx)

To Email Address 3: (xyz@xxx.xxx)

Email Subject:

Hinweis: In diesem Beispiel wird die Protokollmeldung vom AP verwendet.

Schritt 14: Klicken Sie auf **Test Mail**, um die konfigurierten Anmeldeinformationen des Mailservers zu validieren. Dadurch wird eine E-Mail an die konfigurierten E-Mail-Adressen gesendet, um zu überprüfen, ob die Konfiguration funktioniert.

Message Configuration

To Email Address 1: (xyz@xxx.xxx)

To Email Address 2: (xyz@xxx.xxx)

To Email Address 3: (xyz@xxx.xxx)

Email Subject:

Schritt 15: Klicken Sie auf **Speichern**.

Message Configuration

To Email Address 1:

To Email Address 2:

To Email Address 3:

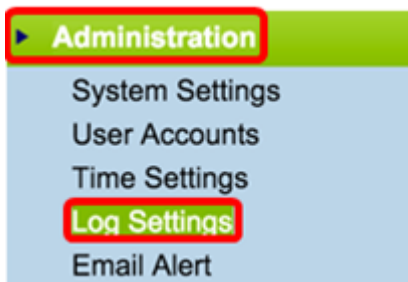
Email Subject:

Protokolleinstellungen konfigurieren

In diesem Bereich werden System- und Ereignisprotokolle im Volatile- und im NVRAM lokal konfiguriert.

Schritt 1: Melden Sie sich beim webbasierten Access Point-Dienstprogramm an, um

Administration > Log Settings auszuwählen.



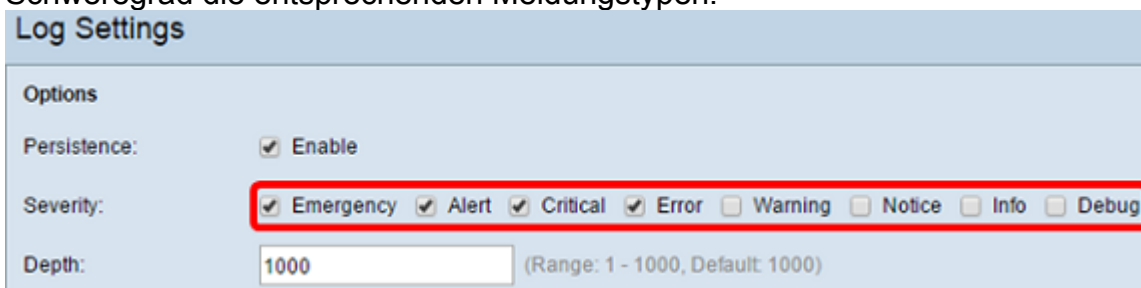
Schritt 2: (Optional) Wenn Protokolle dauerhaft gespeichert werden sollen, damit die Einstellungen beim Neustart des WAP erhalten bleiben, aktivieren Sie Persistence (Beständigkeit), indem Sie das Kontrollkästchen **Aktivieren** aktivieren. Dies ist besonders dann nützlich, wenn das System unerwartet 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.



Hinweis: Wenn Enable (Aktivieren) deaktiviert ist, werden Protokolle im flüchtigen Speicher gespeichert.

Schritt 3: Um den Schweregrad festzulegen, wählen Sie den entsprechenden Meldungstyp aus, der gesendet werden soll, z. B. Emergency, Alert, Critical, Error, Warning, Notice, Info oder Debug. Diese Meldungen werden bei jedem Ablauf der Protokolldauer gesendet. Diese Optionen werden je nach verwendetem Gerät im webbasierten Dienstprogramm unterschiedlich angezeigt.

Aktivieren Sie für WAP131, WAP150, WAP351 und WAP361 in den Kontrollkästchen für den Schweregrad die entsprechenden Meldungstypen.



Klicken Sie für WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 und WAP571E in der Dropdown-Liste "Severity" (Schweregrad) auf den entsprechenden Meldungstyp.

Log Settings

Options

Persistence: Enable

Severity: **7 - Debug** ▼

- 0 - Emergency
- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warning
- 5 - Notice
- 6 - Info
- 7 - Debug**

Depth:

Remote Log Server

Remote Log:

Server IPv4/IPv6 Address/Name:

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

Geben Sie für WAP131, WAP150, WAP351 und WAP361 den Tiefenbereich im Feld Tiefe ein. Der Bereich liegt zwischen 1 und 1.000. Der Standardwert ist 1000.

Log Settings

Options

Persistence: Enable

Severity: Emergency Alert

Depth: **1000** (F)

Geben Sie für WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 und WAP571E den Tiefenbereich in das Feld Tiefe ein. Der Bereich liegt zwischen 1-512 und 512 ist der Standardwert. In diesem Beispiel wird 67 verwendet.

Log Settings

Options

Persistence: Enable

Severity: **7 - Debug** ▼

Depth: **67**

Schritt 5: Klicken Sie auf **Speichern**.

Hinweis: Der Access Point erfasst mithilfe eines Network Time Protocol-Servers Zeit- und Datuminformationen. Diese Daten sind im UTC-Format (Greenwich Mean Time).

Diese Konfigurationen sollten die Ereignisprotokollierung auf Ihrem lokalen Gerät weiterleiten und E-Mail-Warnmeldungen empfangen.