

# Konfigurieren der Systemprotokolleinstellungen auf dem Router der Serie RV34x

## Ziel

Systemereignisse sind Aktivitäten, die möglicherweise Aufmerksamkeit erfordern und erforderliche Maßnahmen, 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.

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 Artikel erfahren Sie, wie Sie die Systemprotokolleinstellungen einschließlich des E-Mail-Servers und die Remote-Servereinstellungen auf dem Router der Serie RV34x konfigurieren.

## Anwendbare Geräte

- Serie RV34x

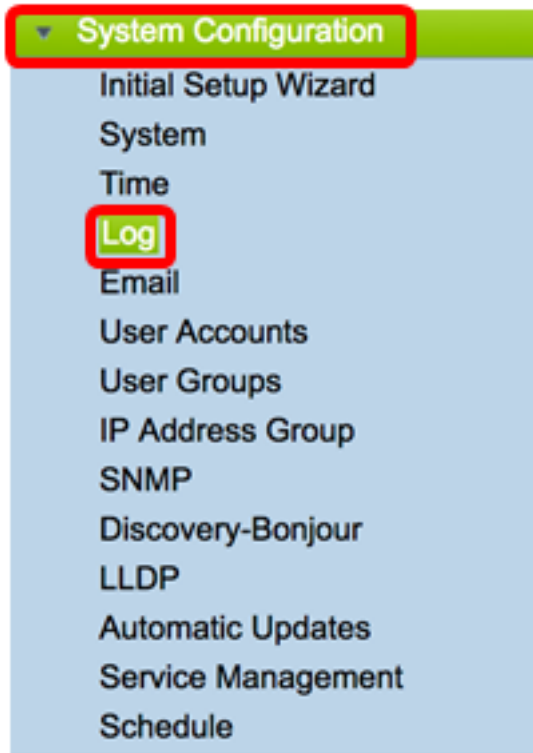
## Softwareversion

- 1,0/01,14

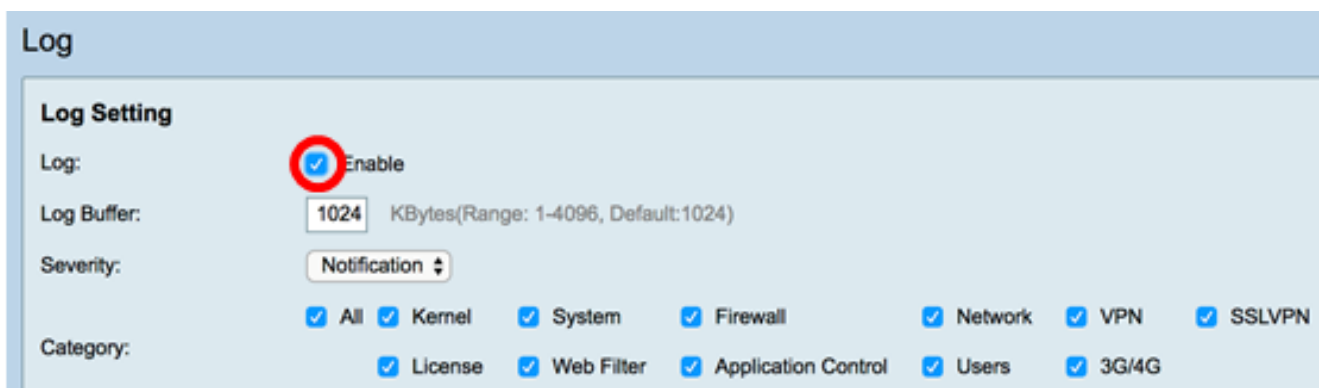
## Konfigurieren der Systemprotokolleinstellungen

### Protokolleinstellungen

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Systemkonfiguration > Protokoll** aus.

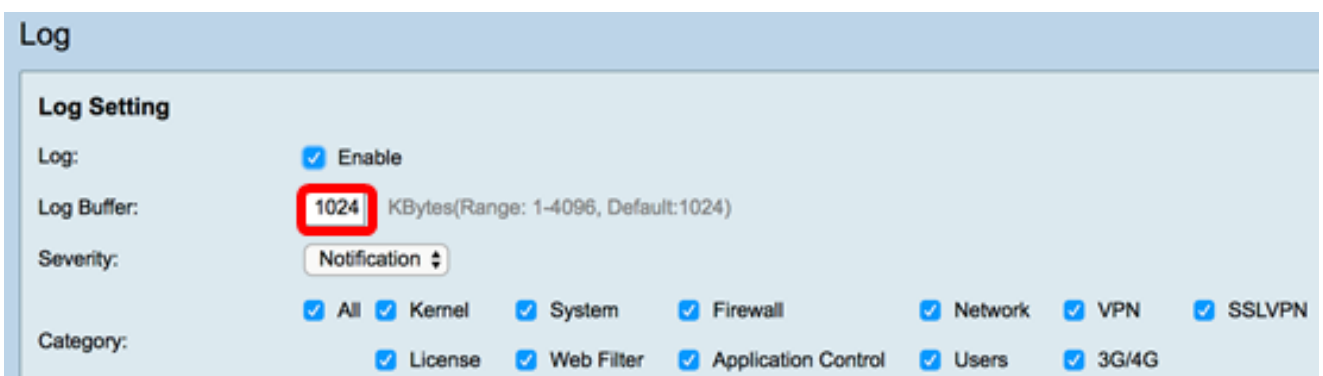


Schritt 2: Aktivieren Sie im Bereich Log Setting (Protokolleinstellungen) das Kontrollkästchen **Enable (Aktivieren)** für Log (Protokoll), um Netzwerkaktualisierungen zu empfangen.



Schritt 3: Geben Sie im Feld *Log Buffer (Protokollpuffer)* die Größe in Kilobyte (KB) ein, die der lokale Puffer für Protokolle hat. Die Puffergröße legt fest, wie viele Protokolle lokal auf dem Router gespeichert werden können. Der Bereich liegt zwischen 1 und 4096. Der Standardwert ist 1024.

**Hinweis:** In diesem Beispiel wird der Wert standardmäßig beibehalten.



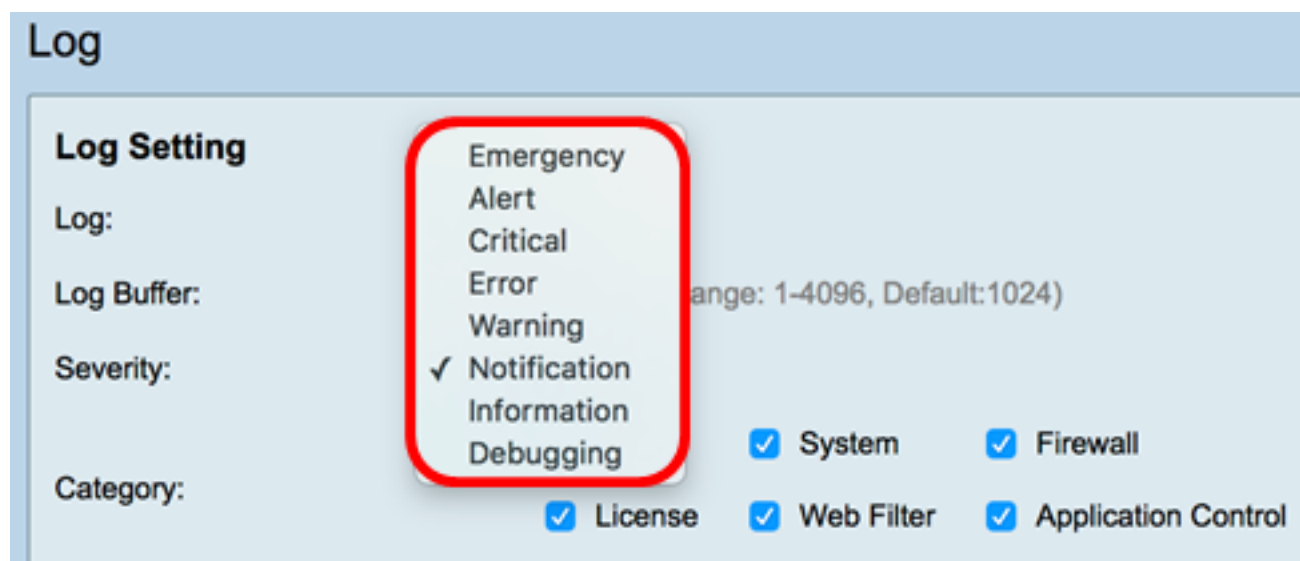
Schritt 4: Wählen Sie eine Option aus der Dropdown-Liste Severity (Schweregrad) aus. Der gewählte Schweregrad umfasst alle höheren Ebenen, daher werden Protokolle für alle

Schweregrade von der obersten Ebene bis zur gewählten Ebene aufbewahrt.

Folgende Optionen stehen zur Verfügung:

- Notfall — Stufe 0; Die Nachricht wird protokolliert, wenn ein Gerät ausgefallen ist oder nicht mehr verwendet werden kann. Die Nachricht wird normalerweise an alle Prozesse gesendet.
- Warnmeldung — Stufe 1; Bei schwerwiegenden Gerätefehlern wird eine Nachricht protokolliert, z. B. wenn alle Gerätefunktionen nicht mehr funktionieren.
- Critical (Kritisch) — Stufe 2; Bei einer kritischen Gerätefunktionsstörung wird eine Nachricht protokolliert, z. B. wenn zwei Ports nicht ordnungsgemäß funktionieren, während die verbleibenden Ports ordnungsgemäß funktionieren.
- Fehler — Stufe 3; Es wird eine Nachricht protokolliert, wenn ein Gerät, z. B. ein einzelner Port, offline ist, einen Fehler enthält.
- Warnung — Stufe 4; Eine Nachricht wird protokolliert, wenn ein Gerät ordnungsgemäß funktioniert, aber ein Betriebsproblem auftritt.
- Meldung — Stufe 5; Eine Nachricht wird protokolliert, wenn ein Gerät ordnungsgemäß funktioniert, aber eine Systemwarnung auftritt. Dies ist die Standardeinstellung.
- Information — Stufe 6; Die Meldung wird protokolliert, wenn eine Bedingung, die kein Fehler auf dem Gerät ist, aber möglicherweise Aufmerksamkeit oder besondere Behandlung erfordert.
- Debuggen - Stufe 7; Stellt alle detaillierten Debuginformationen bereit.

**Hinweis:** In diesem Beispiel wird der Standardwert ausgewählt.



Schritt 5: Überprüfen Sie die entsprechenden Kategorien, um Updates und Benachrichtigungen zu erhalten. Folgende Optionen stehen zur Verfügung:

- All (Alle): Diese Option aktiviert alle Optionen.
- Kernel - Protokolle, die den Kernel-Code beinhalten.
- System - Protokolle, die Benutzerplatzanwendungen wie Network Time Protocol (NTP), Session und Dynamic Host Configuration Protocol (DHCP) enthalten.
- Firewall - Protokolle, die durch Firewall-Verletzungen, Regeln, Angriffe und Content-Filterung ausgelöst werden.
- Netzwerk - Protokolle für Routing, DHCP, Wide Area Network (WAN), Local Area Network (LAN) und QoS.
- VPN - VPN-bezogene Protokolle (Virtual Private Network), einschließlich Instanzen wie VPN

- Tunnel Establishment Failure, VPN Gateway Failure usw.
- SSL VPN - Protokolle für SSL-VPN (Secure Sockets Layer).
- Lizenz - Protokolle, die Lizenzverletzungen enthalten.
- Webfilter - Protokolle zu Ereignissen, die die Webfilterung ausgelöst haben.
- Anwendungskontrolle - Protokolle, die sich auf die Anwendungskontrolle beziehen.
- Benutzer - Protokolle im Zusammenhang mit Benutzeraktivitäten.
- 3G/4G - Protokolle der 3G/4G/USB-Dongles, die an den Router angeschlossen sind.

**Hinweis:** In diesem Beispiel wird All (Alle) ausgewählt.

**Log**

**Log Setting**

Log:  Enable

Log Buffer:  KBytes(Range: 1-4096, Default:1024)

Severity:

Category:  All  Kernel  System  Firewall  Network  VPN  SSLVPN  
 License  Web Filter  Application Control  Users  3G/4G

Save to USB Automatically:  Enable  USB1  USB2

Schritt 6: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Protokolle auf einem USB-Laufwerk automatisch zu speichern. Dies ist standardmäßig deaktiviert.

**Hinweis:** Wenn der Router feststellt, dass kein USB-Port angeschlossen ist, um diese Funktion nutzen zu können, wird neben dem USB2-Optionsfeld eine rote Zeile angezeigt, die besagt, dass kein USB-Speicher angeschlossen ist. Die Protokolle werden erst gespeichert, wenn ein gültiges Speichergerät angeschlossen ist.

**Log**

**Log Setting**

Log:  Enable

Log Buffer:  KBytes(Range: 1-4096, Default:1024)

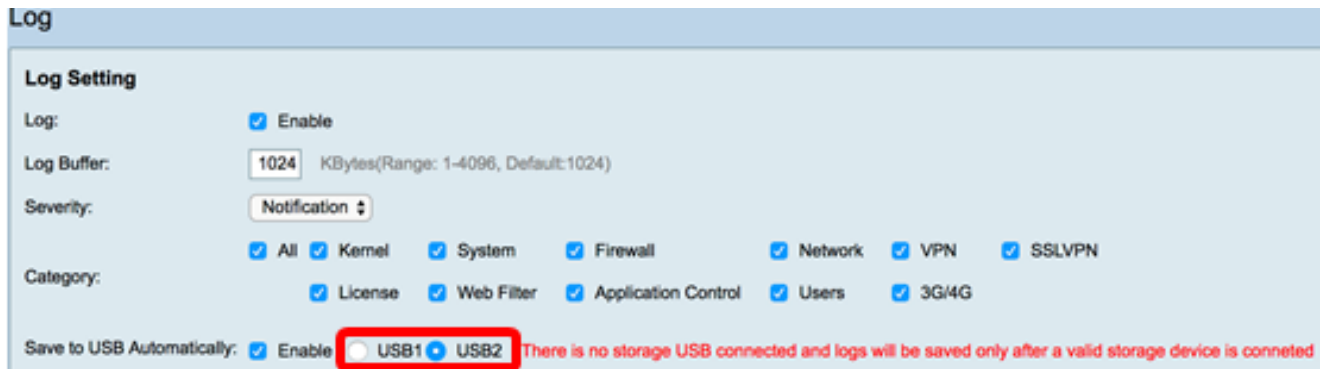
Severity:

Category:  All  Kernel  System  Firewall  Network  
 License  Web Filter  Application Control  Users

Save to USB Automatically:  Enable  USB1  USB2 There is no storage USB connected and logs w

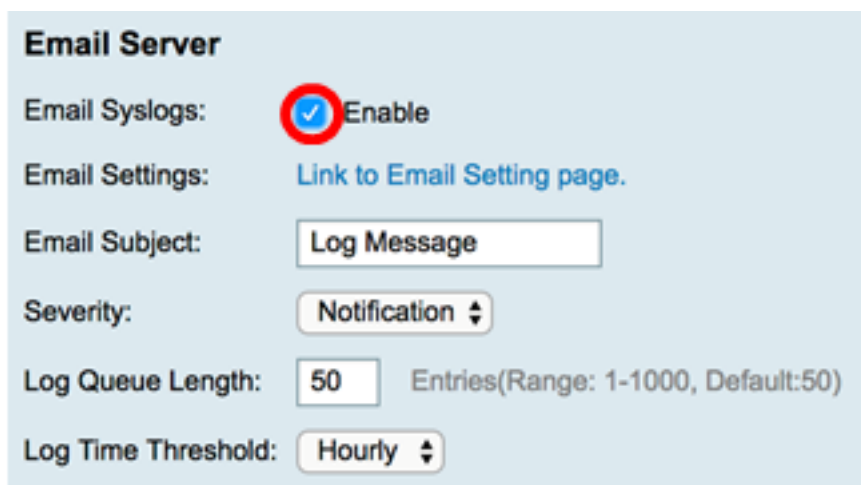
Schritt 7: Wählen Sie eine Optionsschaltfläche für den USB-Port aus, an den das Laufwerk angeschlossen ist.

**Hinweis:** In diesem Beispiel wird USB2 ausgewählt.

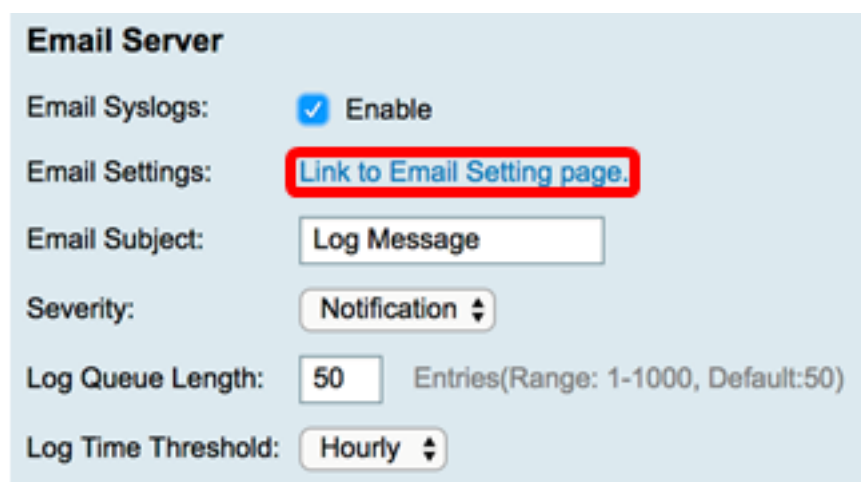


## E-Mail-Server

Schritt 8: Aktivieren Sie das Kontrollkästchen **Aktivieren** für E-Mail-Syslogs, damit der Router E-Mail-Warnmeldungen für bestimmte Netzwerkeignisse oder -verhalten senden kann, die sich auf Leistung, Sicherheit oder Debugging auswirken können.



Schritt 9: Klicken Sie zum Konfigurieren der E-Mail-Einstellungen auf die Seite "Link to Email Setting" (E-Mail-Einstellungen verknüpfen), und klicken Sie [hier](#), um Anweisungen zum Konfigurieren der E-Mail-Einstellungen auf dem Router der Serie RV34x zu erhalten.



Schritt 10: Geben Sie im Feld *E-Mail-Betreff* einen Betreff für die E-Mail-Adresse ein, die an die E-Mail-Adresse gesendet werden soll.

**Hinweis:** In diesem Beispiel wird die Protokollmeldung verwendet.

**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

Log Queue Length:  Entries(Range: 1-1000, Default:50)

Log Time Threshold:

Schritt 11: Wählen Sie in der Dropdown-Liste Severity (Schweregrad) einen 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 Optionen sind verfügbar: Benachrichtigung, Warnung, Fehler, Kritisch, Warnung und Notfall.

**Hinweis:** In diesem Beispiel wird Notification verwendet.

**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

Log Queue Length:  Entries(Range: 1-1000, Default:50)

Log Time Threshold:

Schritt 12: Geben Sie im Feld *Log Queue Length* (Länge der Protokollwarteschlange) die Anzahl der Einträge ein, die vor dem Senden des Protokolls an den E-Mail-Empfänger gemacht werden müssen. Der Standardwert ist 50.

**Hinweis:** In diesem Beispiel wird der Standardwert verwendet.

**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

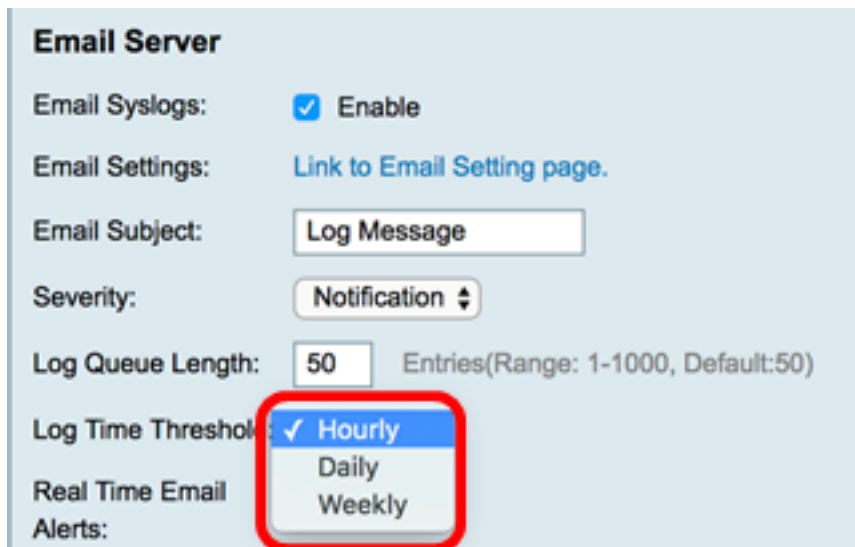
Log Queue Length:  Entries(Range: 1-1000, Default:50)

Log Time Threshold:

Schritt 13: Wählen Sie aus der Dropdown-Liste Log Time Threshold (Schwellenwert für

Protokoll-Zeit) das Intervall aus, in dem der Router das Protokoll an die E-Mail sendet. Die Optionen sind Stunden, Täglich und Wöchentlich.

**Hinweis:** Für dieses Beispiel wird die Stundenzahl gewählt.



**Email Server**

Email Syslogs:  Enable

Email Settings: [Link to Email Setting page.](#)

Email Subject:

Severity:

Log Queue Length:  Entries(Range: 1-1000, Default:50)

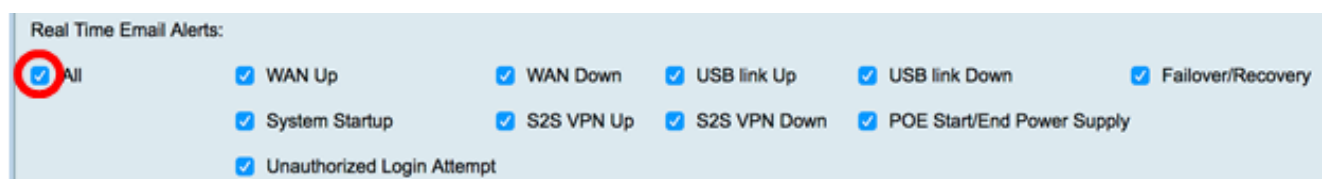
Log Time Threshold:  Hourly  
 Daily  
 Weekly

Real Time Email Alerts:

Schritt 14: Aktivieren Sie die Kontrollkästchen der Ereignisse, die eine E-Mail-Warnmeldung in Echtzeit auslösen. Folgende Optionen sind verfügbar:

- All (Alle): Prüft alle Kontrollkästchen und ermöglicht dem Router, Warnmeldungen in Echtzeit an die E-Mail zu senden.
- WAN Up (WAN-Einrichtung): Benachrichtigung per E-Mail über den WAN-Link ist aktiv.
- WAN Down - Benachrichtigung an E-Mail gesendet, wenn der WAN-Link ausfällt.
- USB link Up (USB-Verbindung aktiv) - Eine Warnung wird an E-Mail gesendet, wenn der USB-Link hochgefahren wird.
- USB link Down (USB-Link nicht verfügbar) - Warnung wird an E-Mail gesendet, wenn der USB-Link heruntergefahren wird.
- Failover/Recovery (Failover/Wiederherstellung): Eine Warnung wird an E-Mails gesendet, wenn der Router in den Wiederherstellungsmodus wechselt oder der Router zum 3G/4G-USB-Dongle zurückgekehrt ist, um eine Verbindung zum Internet herzustellen.
- Systemstart - Eine Warnung wird an eine E-Mail gesendet, wenn der Router gestartet wird.
- S2S VPN Down - Benachrichtigung an E-Mail gesendet, dass das Site-to-Site-VPN aktiv ist.
- S2S VPN Down - Benachrichtigung an E-Mail gesendet, dass das Site-to-Site-VPN ausgefallen ist.
- Unauthorized Login Attempt (Nicht autorisierter Anmeldeversuch): Die E-Mail erhält eine Warnung über einen nicht autorisierten Anmeldeversuch auf dem Router.

**Hinweis:** In diesem Beispiel ist All (Alle) aktiviert.



Real Time Email Alerts:

All  WAN Up  WAN Down  USB link Up  USB link Down  Failover/Recovery

System Startup  S2S VPN Up  S2S VPN Down  POE Start/End Power Supply

Unauthorized Login Attempt

## Remote-Syslog-Server

Schritt 15: Aktivieren Sie das Kontrollkästchen **Aktivieren** für Syslog-Server.



**Remote Syslog Servers**

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Schritt 16: Geben Sie im Feld *Syslog Server 1* die IP-Adresse des Remote-Servers ein. Syslog Server, auf dem die protokollierten Ereignisse gespeichert werden.

**Hinweis:** In diesem Beispiel wird 192.168.1.102 als Remote-Benutzer verwendet. Syslog Serveradresse.

**Remote Syslog Servers**

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Schritt 17: (Optional) Geben Sie im Feld *Syslog Server 2* die Backup-IP-Adresse des Remote-Servers ein. Syslog Server.

**Hinweis:** In diesem Beispiel wird 192.168.1.109 verwendet.

**Remote Syslog Servers**

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Schritt 18: Klicken Sie auf **Übernehmen**.




### Remote Syslog Servers

Syslog Servers:  Enable

Syslog Server 1:  hint(1.2.3.4, abc.com, or FE08::10)

Syslog Server 2:  hint(1.2.3.4, abc.com, or FE08::10) (optional)

Schritt 19: (Optional) Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite "Copy/Save Configuration" (Konfiguration kopieren/speichern) auf, oder klicken Sie auf die  Symbol oben auf der Seite.

Sie sollten jetzt die Systemprotokolleinstellungen auf dem Router der Serie RV34x erfolgreich konfiguriert haben.