

E-Mail-Einstellungen für den RV130 und den RV130W

Ziel

Der RV130 und der RV130W können so konfiguriert werden, dass E-Mails an Ihr Konto gesendet werden, in denen Sie über wichtige Geräteinformationen wie Fehlerprotokolle und Firmware-Updates informiert werden. Die Informationen können so konfiguriert werden, dass sie in festgelegten Intervallen und für bestimmte Netzwerkereignistypen gesendet werden.

In diesem Dokument wird erläutert, wie Sie die E-Mail-Einstellungen für die VPN-Router R130 und RV130W bearbeiten.

Unterstützte Geräte

- RV130
- RV130W

Software-Version

- 1.0.1.3

E-Mail-Einstellungen konfigurieren

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Administration > Logging > E-Mail Settings** aus. Die Seite *E-Mail-Einstellungen* wird geöffnet:

E-mail Settings

E-mail Alert Configuration

New Firmware E-mail Alert: Enable

E-mail Logs: Enable

Log E-mail Configuration

Minimum Email Log Severity: All

Send E-mail Logs by Schedule

Unit:

Day:

Time:

E-mail Settings

E-mail Server Address: (Hint: mail.abc.com)

E-mail Server Port: (Range: 1 - 65535, Default: 25)

Return E-mail Address: (Hint: test@abc.com)

Send to E-mail Address (1): (Hint: test@abc.com)

Send to E-mail Address (2) (Optional):

Send to E-mail Address (3) (Optional):

E-mail Encryption:

Schritt 2. Aktivieren Sie im Feld *Neue Firmware-E-Mail-Warnmeldung* das Kontrollkästchen **Aktivieren**, damit das Gerät E-Mail-Warnmeldungen senden kann, wenn neue Firmware automatisch erkannt und/oder installiert wird.

E-mail Alert Configuration

New Firmware E-mail Alert: **Enable**

E-mail Logs: Enable

Anmerkung: Um neue Firmware-E-Mail-Warnmeldungen vollständig zu konfigurieren, müssen außerdem automatische Einstellungen für Firmware-Upgrades konfiguriert werden. Weitere Informationen finden Sie unter [Firmware-/Sprach-Upgrade auf dem RV130 und RV130W mithilfe der Webschnittstelle](#).

Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld *E-Mail-Protokolle*, um E-Mail-Protokolle zu aktivieren. E-Mail-Protokolle sind eine Funktion, die E-Mails an bestimmte Adressen sendet, wenn auf Ihrem Gerät ein bestimmtes Ereignis auftritt.

E-mail Alert Configuration

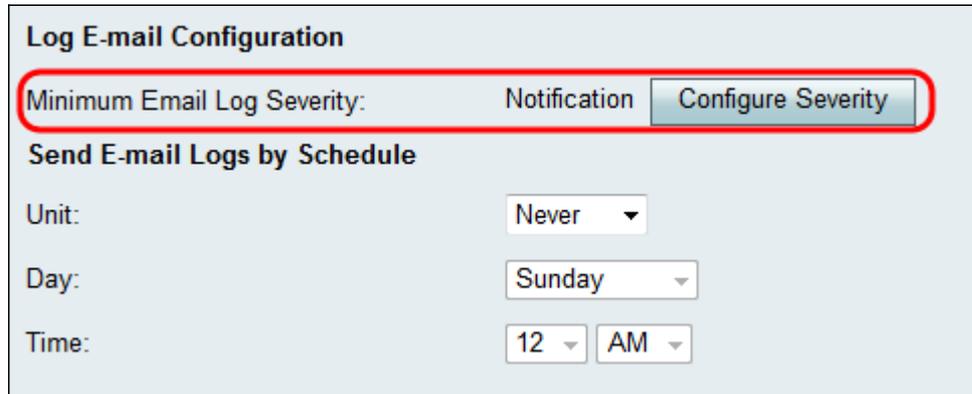
New Firmware E-mail Alert: Enable

E-mail Logs: **Enable**

Anmerkung: Um E-Mail-Protokolle zu aktivieren, müssen die Protokolleinstellungen zuerst konfiguriert werden. Weitere Informationen finden Sie unter [Configure Log Settings on the](#)

[RV130 and RV130W](#) (Protokolleinstellungen konfigurieren).

Schritt 4: (Optional) Im Feld *Minimaler E-Mail-Protokollschweregrad* wird das Ereignis mit der geringsten Priorität angezeigt, das den Versand einer Protokollmeldung auslösen kann. Durch Klicken auf die Schaltfläche **Schweregrad konfigurieren** gelangen Sie zur Seite *Protokolleinstellungen*. Von hier aus können Sie den minimalen Schweregrad und andere Protokolleinstellungen anpassen.



Log E-mail Configuration

Minimum Email Log Severity: Notification **Configure Severity**

Send E-mail Logs by Schedule

Unit: Never

Day: Sunday

Time: 12 AM

Schritt 5. Wenn Sie in Schritt 3 die E-Mail-Protokolle aktivieren möchten, wählen Sie aus der Dropdown-Liste *Unit (Einheit)* aus, wie häufig die Protokolle gesendet werden sollen. Andernfalls überspringen Sie diesen Schritt.



Send E-mail Logs by Schedule

Unit: Never

Day:

Time:

- Never
- Hourly
- Daily
- Weekly

Die verfügbaren Optionen sind wie folgt definiert:

- Niemals — Sendet niemals Protokolle. Fahren Sie bei Auswahl dieser Option mit Schritt 8 fort.
- Stündlich — Sendet Protokolle einmal pro Stunde. Fahren Sie bei Auswahl dieser Option mit Schritt 8 fort.
- Täglich — Sendet Protokolle jeden Tag zur gleichen Zeit. Fahren Sie bei Auswahl dieser Option mit Schritt 7 fort.
- Wöchentlich — Sendet Protokolle einmal wöchentlich.

Schritt 6. Wenn in Schritt 5 die Option **Wöchentlich** ausgewählt ist, wählen Sie aus der Dropdown-Liste *Tag* den Wochentag aus, an dem die Protokolle gesendet werden sollen. Andernfalls können Sie diesen Schritt überspringen.

Send E-mail Logs by Schedule

Unit: Weekly

Day: Sunday

Time:

E-mail Settings

E-mail Server Address:

Schritt 7. Wenn in Schritt 5 die Option **Täglich** oder **Wöchentlich** ausgewählt wird, wählen Sie aus den *Zeit*-Dropdown-Listen die Tageszeit aus, zu der die Protokolle gesendet werden sollen. Andernfalls können Sie diesen Schritt überspringen.

Send E-mail Logs by Schedule

Unit: Daily

Day: Sunday

Time: 12 AM

Schritt 8: Geben Sie im Feld *E-Mail-Serveradresse* entweder eine IP-Adresse oder einen Domännennamen für den E-Mail-Server der Empfängerkonten ein.

E-mail Settings

E-mail Server Address: mail.abc.com (Hint: mail.abc.com)

E-mail Server Port: 25 (Range: 1 - 65535, Default: 25)

Return E-mail Address: (Hint: test@abc.com)

Send to E-mail Address (1): (Hint: test@abc.com)

Send to E-mail Address (2) (Optional):

Send to E-mail Address (3) (Optional):

E-mail Encryption: Disable

Authentication with SMTP server: None

E-mail Authentication Username:

E-mail Authentication Password:

E-mail Authentication Test: Test

Schritt 9: Geben Sie im Feld *E-Mail-Server-Port* die Portnummer für den SMTP-Server ein, mit dem Sie eine Verbindung herstellen möchten.

E-mail Settings

E-mail Server Address: (Hint: mail.abc.com)

E-mail Server Port: (Range: 1 - 65535, Default: 25)

Return E-mail Address: (Hint: test@abc.com)

Send to E-mail Address (1): (Hint: test@abc.com)

Send to E-mail Address (2) (Optional):

Send to E-mail Address (3) (Optional):

E-mail Encryption:

Authentication with SMTP server:

E-mail Authentication Username:

E-mail Authentication Password:

E-mail Authentication Test:

Schritt 10: Geben Sie im Feld *E-Mail-Adresse zurücksenden* eine E-Mail-Adresse ein, an die zurückgegebene E-Mails gesendet werden sollen. Wenn die E-Mail nicht erfolgreich zugestellt werden kann, wird sie an die Absenderadresse gesendet.

E-mail Settings

E-mail Server Address: (Hint: mail.abc.com)

E-mail Server Port: (Range: 1 - 65535, Default: 25)

Return E-mail Address: (Hint: test@abc.com)

Send to E-mail Address (1): (Hint: test@abc.com)

Send to E-mail Address (2) (Optional):

Send to E-mail Address (3) (Optional):

E-mail Encryption:

Authentication with SMTP server:

E-mail Authentication Username:

E-mail Authentication Password:

E-mail Authentication Test:

Schritt 11: Geben Sie im Feld *An E-Mail-Adresse senden (1)* eine E-Mail-Adresse ein, an die die Protokolle gesendet werden. Wenn die Protokolle an zusätzliche E-Mail-Adressen gesendet werden sollen, geben Sie die E-Mail-Adressen in die Felder *An E-Mail-Adresse senden (2) (Optional)* und/oder *An E-Mail-Adresse senden (3) (Optional)* ein.

E-mail Settings

E-mail Server Address: (Hint: mail.abc.com)

E-mail Server Port: (Range: 1 - 65535, Default: 25)

Return E-mail Address: (Hint: test@abc.com)

Send to E-mail Address (1): (Hint: test@abc.com)

Send to E-mail Address (2) (Optional):

Send to E-mail Address (3) (Optional):

E-mail Encryption:

Authentication with SMTP server:

E-mail Authentication Username:

E-mail Authentication Password:

E-mail Authentication Test:

Schritt 12: Wählen Sie in der Dropdown-Liste *E-Mail-Verschlüsselung* die gewünschte Verschlüsselungsmethode aus. TLS wird empfohlen.

E-mail Encryption:

Authentication with SMTP server:

E-mail Authentication Username:

E-mail Authentication Password:

E-mail Authentication Test:

Die verfügbaren Optionen sind wie folgt definiert:

- Deaktivieren - E-Mail-Verschlüsselung ist deaktiviert.
- SSL - Secure Socket Layer Encryption Protocol verschlüsselt versendete E-Mails und schützt und sichert die Daten.
- TLS - Transport Layer Security Encryption Protocol ist der Nachfolger von SSL mit zusätzlichen Sicherheitsverbesserungen und der aktuelle Branchenstandard.

Schritt 13. Wählen Sie in der Dropdown-Liste *Authentifizierung mit SMTP-Server* die Authentifizierungsmethode aus, die dem von Ihnen verwendeten SMTP-Server entspricht.

E-mail Encryption:	TLS
Authentication with SMTP server:	None
E-mail Authentication Username:	
E-mail Authentication Password:	
E-mail Authentication Test:	Test

Die verfügbaren Optionen sind wie folgt definiert:

- Keine - Deaktiviert die Authentifizierung mit dem SMTP-Server.
- LOGIN — Verwendet einen Benutzernamen und ein Passwort, um Benutzer zu authentifizieren.
- PLAIN - Ähnlich wie LOGIN, bietet aber Unterstützung für Autorisierungs-Identitäten, die von Administratoren verwendet werden. Wenn Sie sich nicht sicher sind, welche Anwendung Sie auswählen sollen, sollten Sie die Option PLAIN (PLAIN) und dann LOGIN (LOGIN) wählen.
- CRAM-MD5 - Bei der CRAM-MD5-Authentifizierung sendet der Server zunächst eine Abfragezeichenfolge an den Client, und eine Antwort wird vom Client als Zeichenfolge empfangen. Dadurch wurde die Sicherheit über LOGIN und PLAIN erhöht. Autorisierungsidentitäten werden nicht unterstützt.

Schritt 14. Wenn Sie in Schritt 13 eine Authentifizierungsmethode mit dem SMTP-Server gewählt haben, geben Sie Ihren Benutzernamen in das Feld *E-Mail-Authentifizierung Benutzername* und das Kennwort in das Feld *E-Mail-Authentifizierungskennwort ein*. Wenn in Schritt 13 **Keine** ausgewählt wurde, können Sie diesen Schritt überspringen.

E-mail Settings	
E-mail Server Address:	mail.abc.com (Hint: mail.abc.com)
E-mail Server Port:	25 (Range: 1 - 65535, Default: 25)
Return E-mail Address:	test@abc.com (Hint: test@abc.com)
Send to E-mail Address (1):	test1@abc.com (Hint: test@abc.com)
Send to E-mail Address (2) (Optional):	
Send to E-mail Address (3) (Optional):	
E-mail Encryption:	Disable
Authentication with SMTP server:	None
E-mail Authentication Username:	cisco
E-mail Authentication Password:	••••••••
E-mail Authentication Test:	Test

Schritt 15: Klicken Sie auf die Schaltfläche **Test** im Feld *E-Mail-Authentifizierungstest*, um die Verbindung mit dem SMTP zu bestätigen.

E-mail Authentication Username:	<input type="text" value="cisco"/>
E-mail Authentication Password:	<input type="password" value="••••••••"/>
E-mail Authentication Test:	<input type="button" value="Test"/>

Schritt 16: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.