

# RV215Wのシステムログ設定

## 目的

ログは、ネットワークイベントの記録です。これらは、ネットワークの仕組みを理解するために使用される重要なツールです。ログは、ネットワーク管理やデバッグにも役立ちます。RV215Wは、ログ自体を記録したり、リモートサーバにログを送信したり、電子メールアドレスにログを送信したりできます。

この記事では、RV215Wの設定と表示方法について説明します。

## 該当するデバイス

- ・ RV215W

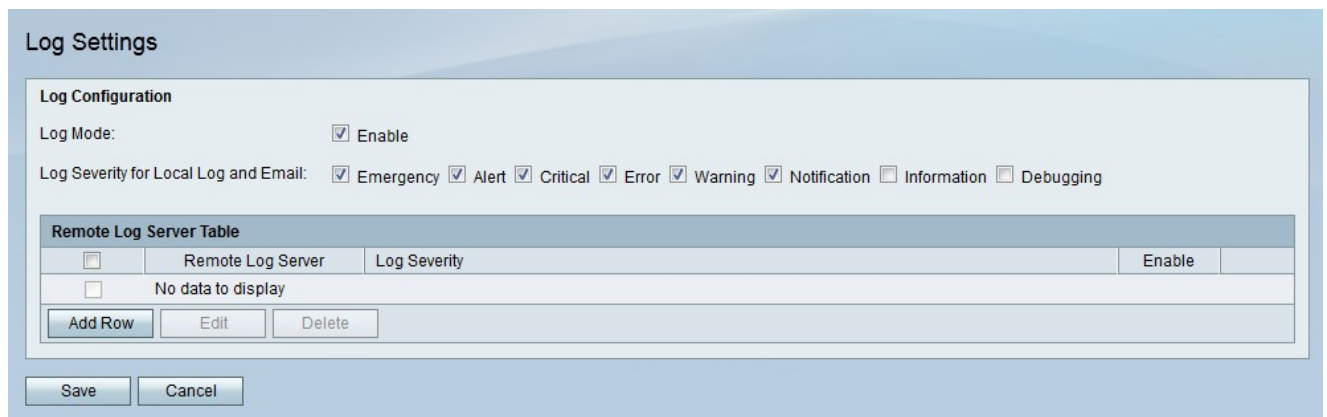
## [Software Version]

- ・1.1.0.5

## ログの設定

### ログ設定

ステップ1:Web構成ユーティリティにログインし、[Administration] > [Logging] > [Log Settings]を選択します。[ログ設定]ページが開きます。



The screenshot shows the 'Log Settings' configuration page. It includes a 'Log Configuration' section with 'Log Mode' set to 'Enable' and 'Log Severity for Local Log and Email' with checkboxes for Emergency, Alert, Critical, Error, Warning, Notification, Information, and Debugging. Below this is a 'Remote Log Server Table' which is currently empty, showing 'No data to display'. At the bottom of the table are 'Add Row', 'Edit', and 'Delete' buttons. At the bottom of the page are 'Save' and 'Cancel' buttons.

ステップ2:[Log Mode]フィールドの[Enable] をオンにして、ログを有効にします。

ステップ3 : 受信するログのタイプに対応するチェックボックスをオンにします。ログは重大度に基づいて注文されます。ボックスをオンにすると、重大度の高いログもすべてチェックされます。次のログの重大度レベルは、最高から最低の順にリストされています。

- ・ 緊急 : システムが使用できない。
- ・ アラート : アクションが必要です。
- ・ クリティカル : システムがクリティカルな状態です。
- ・ エラー : システムがエラー状態です。

- ・ 警告：システム警告が発生しました。
- ・ 通知：システム通知が発生しました。
- ・ 情報：デバイス情報。
- ・ デバッグ：イベントに関する詳細情報を提供します。

Log Settings

Log Configuration

Log Mode:  Enable

Log Severity for Local Log and Email:  Emergency  Alert  Critical  Error  Warning  Notification  Information  Debugging

You must save before you can edit or delete.

<input type="checkbox"/>	Remote Log Server	Log Severity	Enable
<input type="checkbox"/>	192.168.1.100	<input checked="" type="checkbox"/> Emergency <input checked="" type="checkbox"/> Alert <input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Error <input type="checkbox"/> Warning <input type="checkbox"/> Notification <input type="checkbox"/> Information <input type="checkbox"/> Debugging	<input checked="" type="checkbox"/>

**Add Row** Edit Delete

Save Cancel

ステップ4:[行の追加]をクリックして、リモートログサーバを追加します。

ステップ5:[Remote Log Server]フィールドに、ログデータを収集するリモートサーバのIPアドレスを入力します。

ステップ6：リモートサーバに受信させるログのタイプに対応するチェックボックスをオンにします。ログは重大度に基づいて注文されます。ボックスをオンにすると、重大度の高いログもすべてチェックされます。

ステップ7:[Enable] をオンにして、リモートログサーバを有効にします。

ステップ8:[Save]をクリックします。

## 電子メールログの設定

ステップ1:Web構成ユーティリティにログインし、[Administration] > [Logging] > [E-mail Settings]を選択します。[電子メールの設定]ページが開きます。

## E-mail Settings

### Log E-mail Configuration

E-mail Logs:	<input checked="" type="checkbox"/> Enable
Minimum Email Log Severity:	Debugging <input type="button" value="Configure Severity"/>
E-mail Server Address:	<input type="text" value="mail.server.com"/> (Hint: mail.abc.com)
E-mail Server Port:	<input type="text" value="25"/> (Range: 1 - 65535, Default: 25)
Return E-mail Address:	<input type="text" value="return@server.com"/> (Hint: test@abc.com)
Send to E-mail Address (1):	<input type="text" value="send@server.com"/> (Hint: test@abc.com)
Send to E-mail Address (2) (Optional):	<input type="text"/>
Send to E-mail Address (3) (Optional):	<input type="text"/>
E-mail Encryption (SSL):	<input checked="" type="checkbox"/> Enable
Authentication with SMTP server:	<input type="text" value="CRAM-MD5"/>
E-mail Authentication Username:	<input type="text" value="username"/>
E-mail Authentication Password:	<input type="password" value="....."/>
E-mail Authentication Test:	<input type="button" value="Test"/>

### Send E-mail Logs by Schedule

Unit:	<input type="text" value="Weekly"/>
Day:	<input type="text" value="Friday"/>
Time:	<input type="text" value="05"/> <input type="text" value="PM"/>

ステップ2：電子メールログを設定および有効にするには、[E-mail Logs]フィールドの[Enable]をオンにします。

注：電子メールに送信されるログの最小の重大度は、[Minimum Email Log Severity]フィールドに表示されます。[重大度の設定]をクリックして、送信されるログのタイプを設定します。

ステップ3：電子メールアドレスに関連付けられたシンプルメール転送プロトコル(SMTP)サーバのアドレスを[電子メールサーバアドレス(E-mail Server Address)]フィールドに入力します。

ステップ4:SMTPサーバで使用するポートを[E-mail Server Port]フィールドに入力します。

ステップ5:[Return E-mail Address]フィールドに電子メールアドレスを入力します。電子メールアドレスへの送信が使用できない場合は、返信の電子メールアドレスが使用されます。

ステップ6:[Send E-mail Address]フィールド(1)に、ログを送信するRV215Wの電子メールアドレスを入力します。

注：RV215Wは2つの追加の電子メールにログを送信できます。[Send to e-mail Address (2)]フィールドと[Send to E-mail Address (3)]フィールドに、これらの電子メールを入力します。

ステップ7:[E-mail Encryption (SSL)] フィールドの[Enable]をオンにして、電子メールを暗号化します。Secure Sockets Layer(SSL)は、データの暗号化を通じて通信セキュリティを提供する暗号化プロトコルです。

ステップ8:[Authentication with SMTP Server]ドロップダウンリストから、SMTPサーバに必要な認証方式のタイプを選択します。

ステップ9:SMTPサーバで認証が必要な場合は、[E-mail Authentication Username]フィールドに電子メールユーザ名を入力します。

ステップ10:SMTPサーバで認証が必要な場合は、[E-mail Authentication Password]フィールドに電子メールパスワードを入力します。

ステップ11: ( オプション ) 設定した電子メール認証をテストするには、[Test]をクリックします。

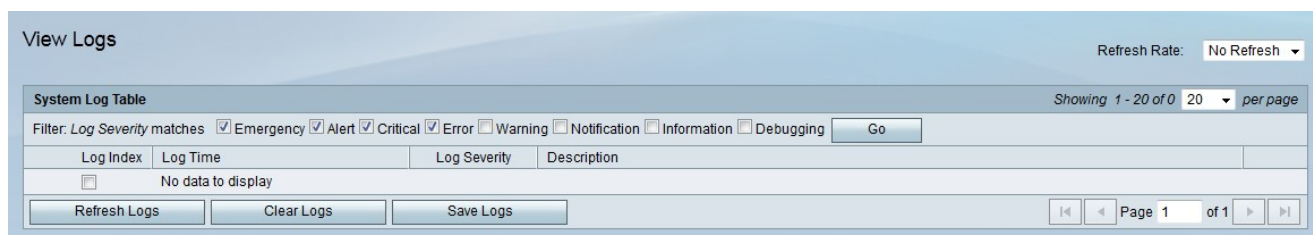
ステップ12:[Unit ( ユニット ) ]ドロップダウンリストから、ログを送信する時刻に対応するオプションを選択します。

- ・ Never : ログは送信されません。
- ・ Hourly – ログは1時間ごとに送信されます。
- ・ Daily : ログは毎日送信されます。[Time]ドロップダウンリストから、ログの送信時刻を選択します。
- ・ Weekly : ログは毎週送信されます。[Day and Time]ドロップダウンリストから、ログを送信する日時を選択します。

ステップ13:[Save]をクリックします。

## View Logs

ステップ1:Web構成ユーティリティにログインし、[Status] > [View Logs]を選択します。[ログの表示]ページが開きます。



次に、システムログテーブルに関する情報を示します。

- ・ Log Index : ログのインデックス番号。

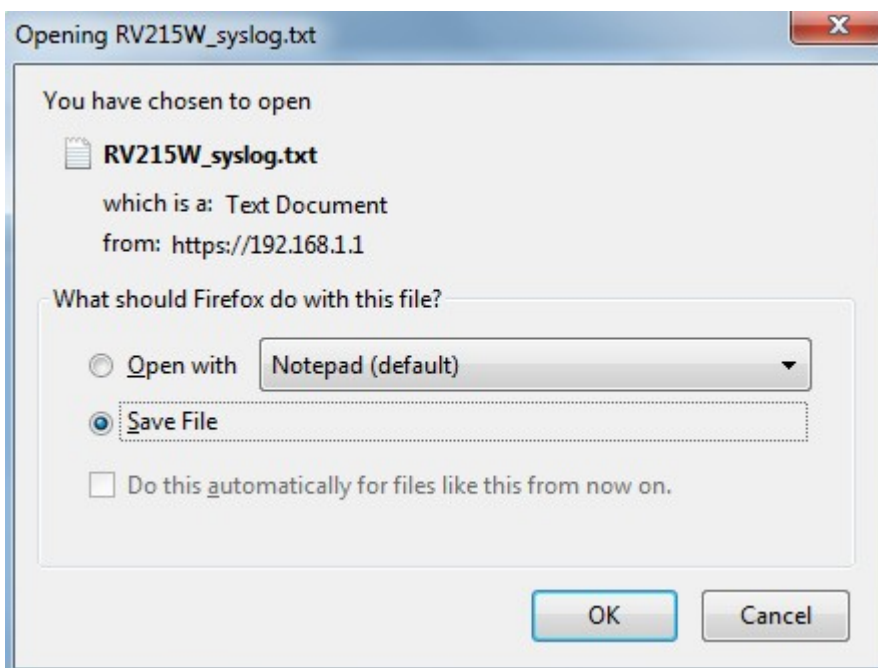
- ・ Log Time – ログが記録された時刻。
- ・ Log Severity : ログのタイプ
- ・ 説明 : ログの簡単な説明。

ステップ2 : フィルタでフィルタするログのタイプに対応するチェックボックスをオンにします。[Log Severity Matches]フィールドログは重大度に基づいて注文されます。ボックスをオンにすると、重大度の高いログもすべてチェックされます。次のログの重大度レベルは、最高から最低の順にリストされています。

- ・ 緊急 : システムが使用できない。
- ・ アラート : アクションが必要です。
- ・ クリティカル : システムがクリティカルな状態です。
- ・ エラー : システムがエラー状態です。
- ・ 警告 : システム警告が発生しました。
- ・ 通知 : システム通知が発生しました。
- ・ 情報 : デバイス情報。
- ・ デバッグ : イベントに関する詳細情報を提供します。

[ログの表示]ページでは、次のオプションを使用できます。

- ・ Refresh Rate:[Refresh Rate]ドロップダウンリストから、ログテーブルを更新する間隔を選択します。
- ・ [ログの更新]:[ログの更新]をクリックして、ログテーブルを更新します。
- ・ ログのクリア – [ログのクリア]をクリックして、ログテーブルをクリアします。



- ・ [ログの保存]:[ログの保存]をクリックして、ログを開くか保存します。