Anzeigen/Hinzufügen eines vertrauenswürdigen SSL-Zertifikats auf RV320- und RV325-VPN-Routern

Ziel

Zertifikate werden verwendet, um die Benutzeridentität auf einem Computer oder im Internet zu überprüfen und um ein privates oder sicheres Gespräch zu verbessern. Auf dem RV320 können Sie maximal 50 Zertifikate durch Selbstsignierung oder Autorisierung von Drittanbietern hinzufügen. Sie können ein Zertifikat für einen Client oder für einen Administrator exportieren, dieses auf einem PC oder USB speichern und anschließend importieren. Secure Sockets Layer (SSL) ist die standardmäßige Sicherheitstechnologie zum Erstellen einer verschlüsselten Verbindung zwischen einem Webserver und einem Browser. Dieser Link stellt sicher, dass alle Daten, die zwischen dem Webserver und Browser übergeben werden, privat und integraler Bestandteil bleiben. SSL ist ein Industriestandard und wird von Millionen von Websites zum Schutz ihrer Online-Transaktionen mit ihren Kunden verwendet. Um eine SSL-Verbindung generieren zu können, benötigt ein Webserver ein SSL-Zertifikat.

In diesem Artikel wird erläutert, wie Sie das Trusted SSL-Zertifikat auf der RV32x VPN-Router-Serie anzeigen und hinzufügen.

Anwendbare Geräte

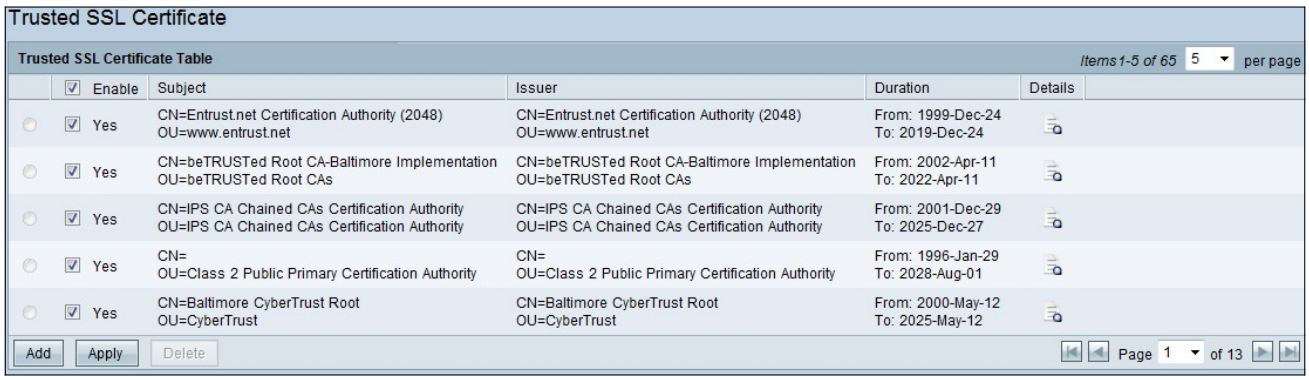
·RV320 Dual-WAN VPN-Router
· RV325 Gigabit Dual-WAN VPN-Router

Softwareversion

·v1.0.1.17

Vertrauenswürdiges SSL-Zertifikat

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Certificate Management > Trusted SSL Certificate aus**. Die Seite *Vertrauenswürdige SSL* wird geöffnet:



Die Seite *Vertrauenswürdiges SSL-Zertifikat* enthält die folgenden Felder:

·Enable (Aktivieren): Es zeigt an, ob ein Zertifikat aktiviert oder deaktiviert ist.

·Emittent: Er liefert Informationen über den Emittenten, der das Zertifikat ausstellt.

·Betreff: Es zeigt, wem das Zertifikat ausgestellt wird.

·Dauer: Es wird das Datum angezeigt, an dem das Zertifikat abläuft. Die Sicherheit der Website kann bei Überschreitung dieses Datums nicht gewährleistet werden.

·Details - Hier werden alle Details zum Zertifikataussteller, zur Zertifikatsseriennummer und zum Ablaufdatum vom Zertifizierungsstellendienst generiert. Die Informationen werden verwendet, wenn eine Signaturanforderung für das Zertifikat generieren erstellt und zur Validierung an den Zertifizierungsstellen-Dienst gesendet wird

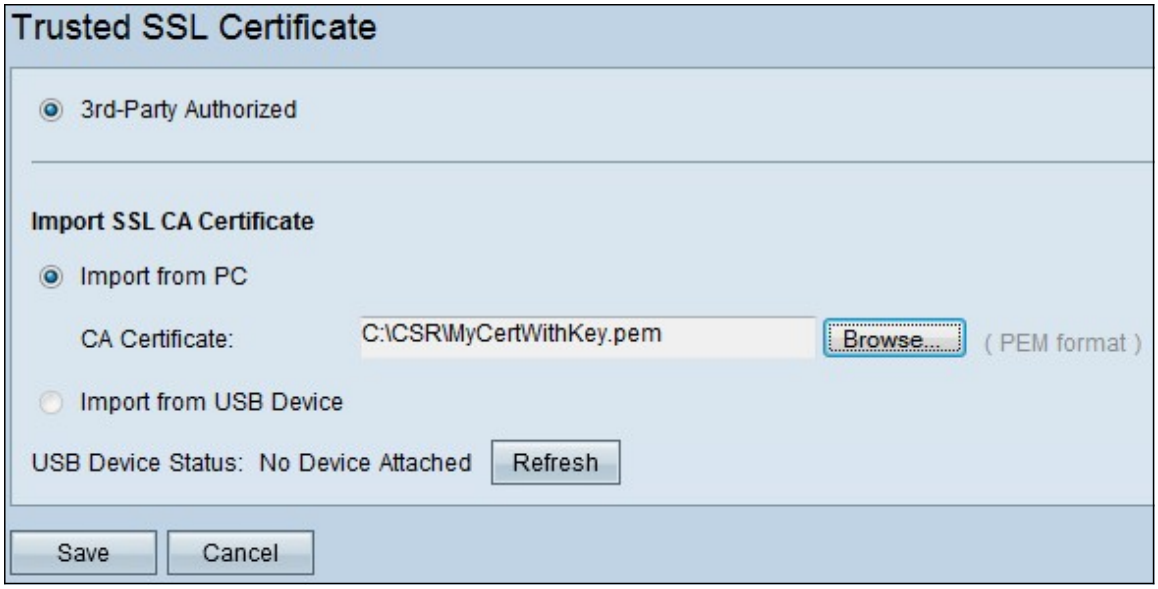
Schritt 2: Klicken Sie auf das Kontrollkästchen **Aktivieren**, um ein bestimmtes SSL-Zertifikat zu aktivieren.

Schritt 3: Klicken Sie auf **Hinzufügen**, um ein neues Zertifikat vom PC oder USB zu erhalten.

·Aus dem PC importieren: Auf dem PC können Sie das Zertifikat suchen und in das Gerät importieren.

·Import From USB (Aus USB importieren): Über den USB, der an das Gerät angeschlossen ist, können Sie auch das Zertifikat importieren.

Schritt 3: Klicken Sie auf **Durchsuchen**, um das Zertifizierungsstellen-Zertifikat vom PC zu suchen.



Schritt 4: Klicken Sie auf **Speichern**, um das Zertifikat der Tabelle mit vertrauenswürdigen SSL-Zertifikaten hinzuzufügen.