Certificaten genereren op RV320 en RV325 VPN-routers

Doel

Eén van de meest voorkomende vormen van cryptografie vandaag de dag is de cryptografie van de openbare sleutel. Publiek-sleutelcryptografie gebruikt een openbare sleutel en een private sleutel. Het systeem versleutelt eerst informatie met behulp van de openbare sleutel. De informatie kan dan alleen worden gedecrypteerd door gebruik te maken van de privé sleutel. Een algemeen gebruik voor cryptografie op de openbare sleutel is de encryptie van toepassingsverkeer door het gebruik van een Secure Socket Layer (SSL) of Transport Layer Security (TLS) verbinding. Een certificaat is een methode die wordt gebruikt om een openbare sleutel en andere informatie over een server en de organisatie die er verantwoordelijk voor is te verspreiden. Certificaten kunnen digitaal worden ondertekend door een certificaatinstantie (CA). Een CA is een betrouwbare derde die heeft bevestigd dat de informatie in het certificaat juist is.

Dit artikel legt uit hoe u certificaten op een RV32x VPN-routerserie kunt genereren.

Toepasselijke apparaten

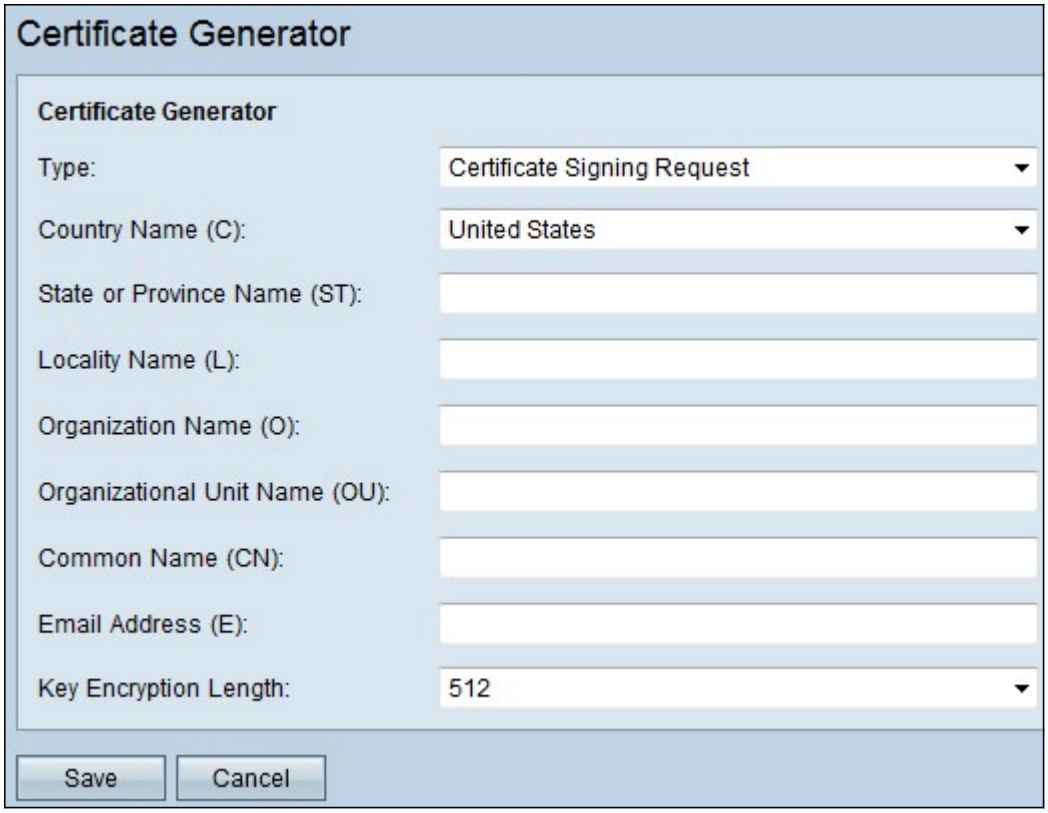
- RV320 VPN-router met dubbel WAN
- RV325 Gigabit VPN-router met dubbel WAN

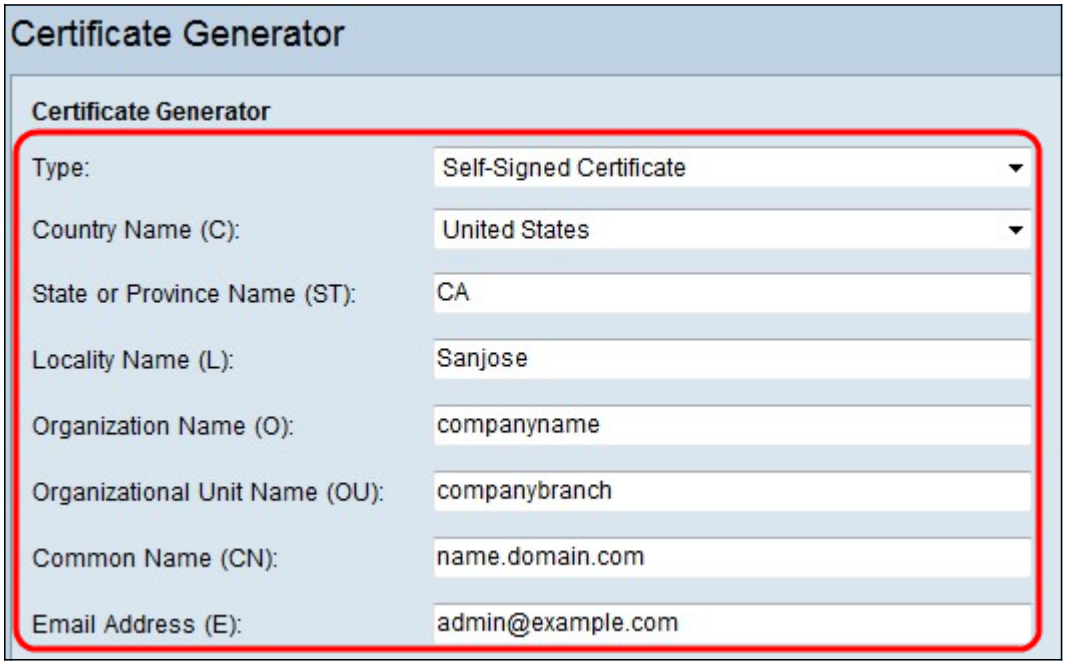
Softwareversie

- v1.1.0.09

Certificaat genereren

Stap 1. Meld u aan bij het web configuratieprogramma en kies **certificaatbeheer > certificaatgenerator**. De pagina *certificaatgenerator* wordt geopend:





Stap 2. Kies het juiste certificeringstype in de vervolgkeuzelijst Type:

- Zelfondertekend certificaat — Dit is een Secure Socket Layer (SSL) certificaat dat door zijn eigen schepper is ondertekend. Dit certificaat is minder betrouwbaar, omdat het niet kan worden geannuleerd als de privésleutel op een of andere manier door de aanvaller op het spel wordt gezet.

- Aanvraag van gecertificeerde signalering — Dit is een openbare sleutelinfrastructuur (PKI) die naar de certificeringsinstantie wordt gestuurd om een digitaal identiteitsbewijs aan te vragen. Het is veiliger dan door zichzelf getekend te worden, omdat de privé-sleutel geheim gehouden wordt.

Stap 3. Kies een landennaam waarin uw organisatie wettelijk is geregistreerd in de vervolgkeuzelijst Landnaam.

Stap 4. Voer een naam of afkorting in van de staat, provincie, regio of gebied waar uw organisatie zich in het veld Naam van de staat of provincie bevindt.

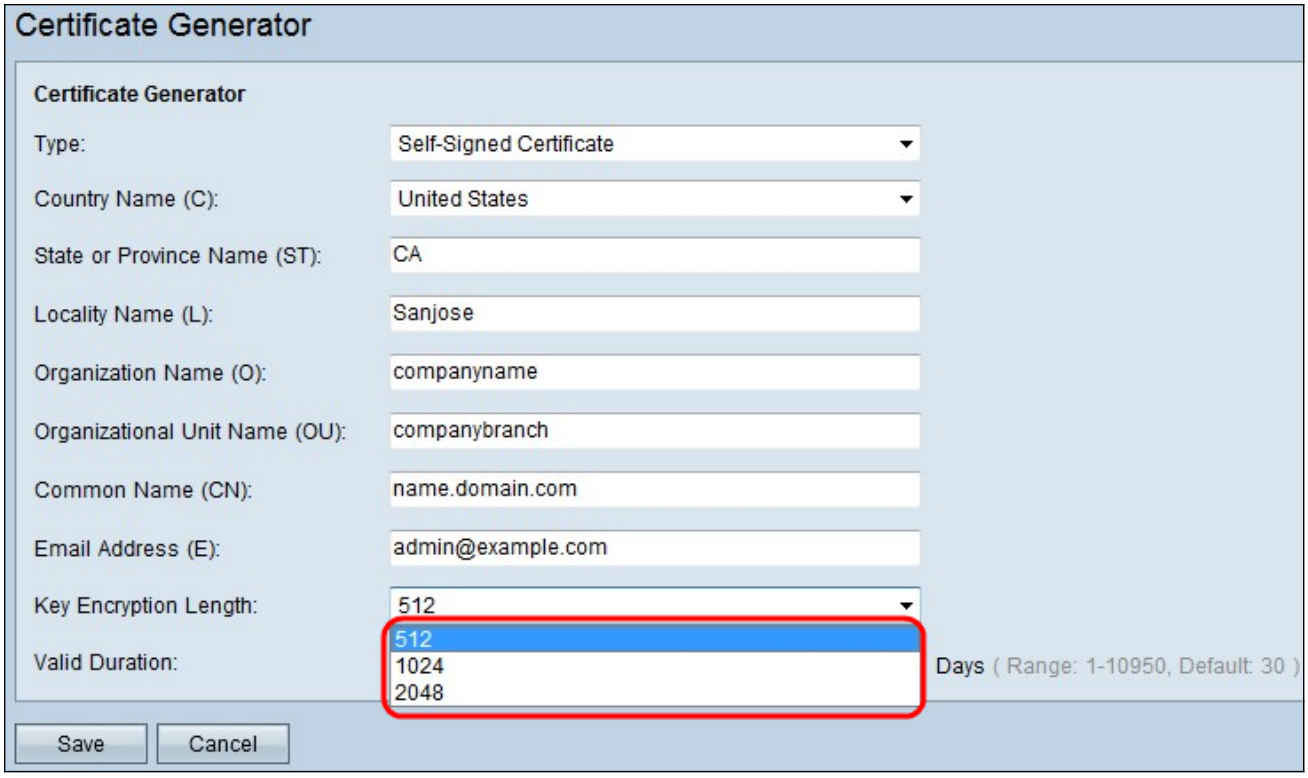
Stap 5. Voer een naam in van de stad/locatie waarin uw organisatie is geregistreerd/gevestigd in het veld Naam Locality.

Stap 6. Voer een naam in waaronder uw bedrijf wettelijk is geregistreerd. Als u zich als kleine onderneming/eenmanszaak inschrijft, voert u in het veld Naam van de organisatie de naam van de certificaataanvrager in.

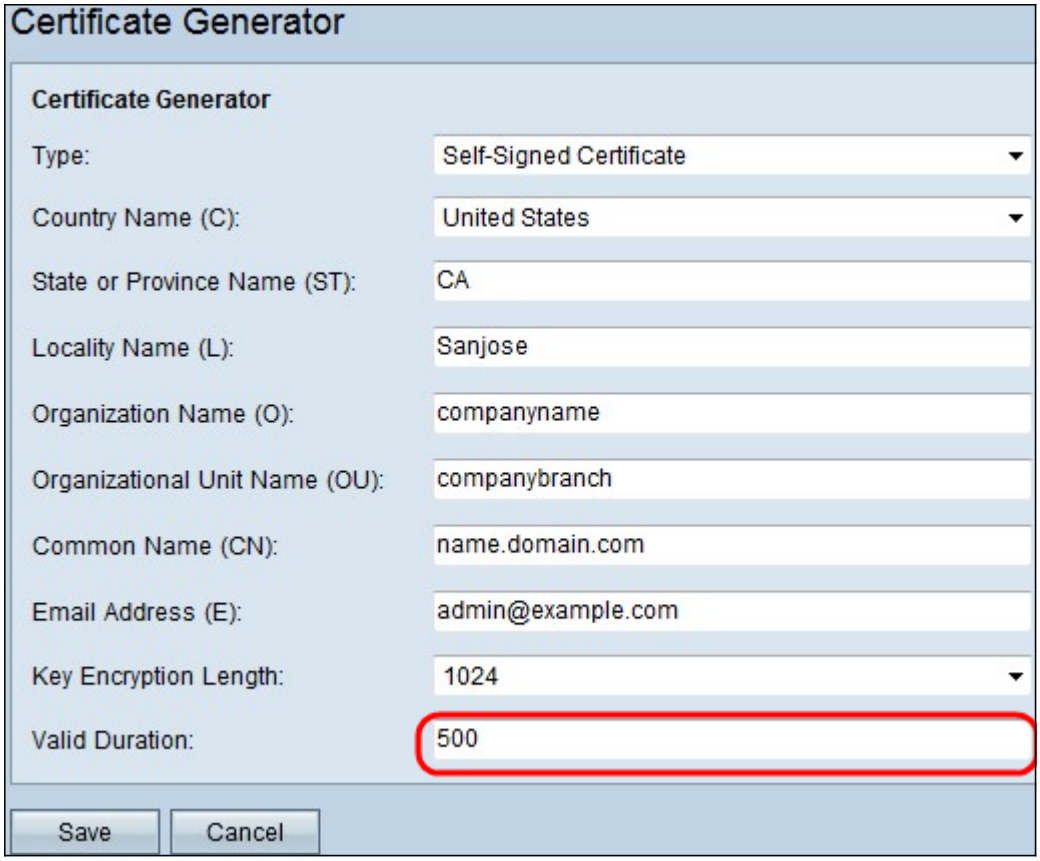
Stap 7. Voer een naam in het veld Naam van de organisatie in om onderscheid te maken tussen afdelingen binnen een organisatie.

Stap 8. Voer een naam in het veld Naam in. Deze naam moet de volledig gekwalificeerde domeinnaam zijn van de website waarvoor u het certificaat gebruikt.

Stap 9. Voer het e-mailadres in van de persoon die het certificaat wil genereren.



Stap 10. Kies een toetstitel van de vervolgkeuzelijst Lengte versleuteling, hoe groter de sleutelgrootte, hoe veiliger het certificaat. Hoe groter de sleutelgrootte, hoe groter de verwerkingstijd.



Opmerking: Als u het certificeringstype als een certificeringsaanvraag hebt geselecteerd, slaat u Stap 11 over en gaat u verder.

Stap 1. Voer het aantal dagen in waarop het certificaat geldig is.

Stap 12. Klik op **Opslaan** om het certificaat te genereren. Het gegenereerde certificaat wordt weergegeven op de pagina *Mijn certificaat*. Als u *mijn* pagina *Certificaat* wilt weergeven, kiest u **certificaatbeheer > Mijn certificaat**.