

How to Generate a Self-Signed Certificate using Parallels Remote Application Server

- Parallels Remote Application Server 18.0
- Parallels Remote Application Server 19.0
- Parallels Remote Application Server 18.1
- Parallels Remote Application Server 19.1
- Parallels Remote Application Server 18.2
- Parallels Remote Application Server 18.3

To generate a self-signed certificate, navigate to Farm > Site > Certificates. Click Tasks > Generate self-signed certificate. In the dialog that opens, specify the following options:

- Name: Type a name for this certificate. This field is mandatory.
- Description: An optional description.
- Usage: Specify whether the certificate should be used for RAS Secure Gateways or HALB, or both. This selection is mandatory.
- Key size: The certificate key size, in bits. Here you can select from the predefined values. The default is 2048 bit, which is the minimum required length according to current industry standards.
- Country code: Select your country.
- Expire in: The certificate expiration date.
- Full state or province: Your state or province info.
- City: City name.
- Organization: The name of your organization.
- Organization unit: Organizational unit.
- E-mail: Your email address. This field is mandatory.
- Common name: The Common Name (CN), also known as the Fully Qualified Domain Name (FQDN). This field is mandatory.
- Alternative names: Specify one or more subject alternative names (SANs). Click the [...] icon and then add one or more DNS or IP addresses. Note that because Parallels Client for mobile devices doesn't support the SAN field, it's safest to set your common name to the name that most mobile devices will be using.

Click Save to generate the certificate. When done, the certificate will appear in the Certificates list in the RAS Console with the Status column indicating Self-signed.
