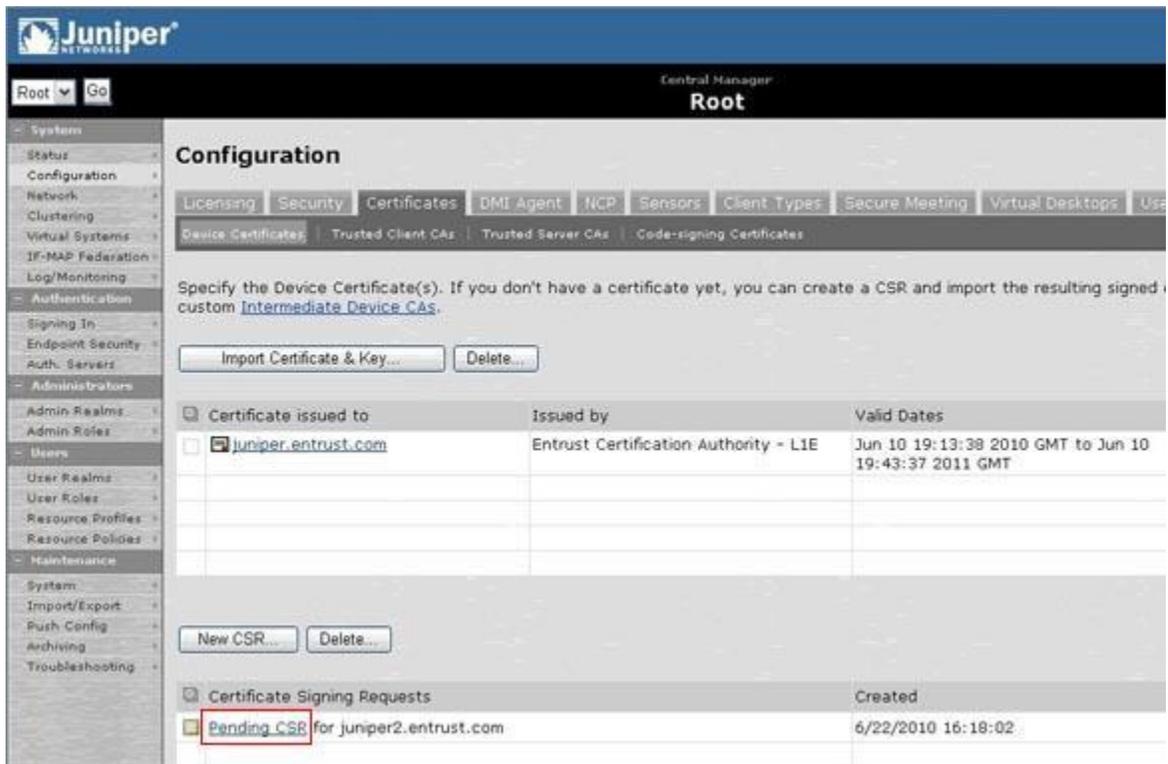


Juniper Secure Access VPN SSL Certificate Installation Procedure:

1. Copy and paste the Server Certificate (including the BEGIN and END tags) into a text editor such as Notepad and save it on your Local Computer.
2. In the admin console,
choose **System > Configuration > Certificates > Device Certificates**.
3. Under **Certificate Signing Requests**, click the **Pending CSR** link that corresponds to the signed certificate from Entrust.

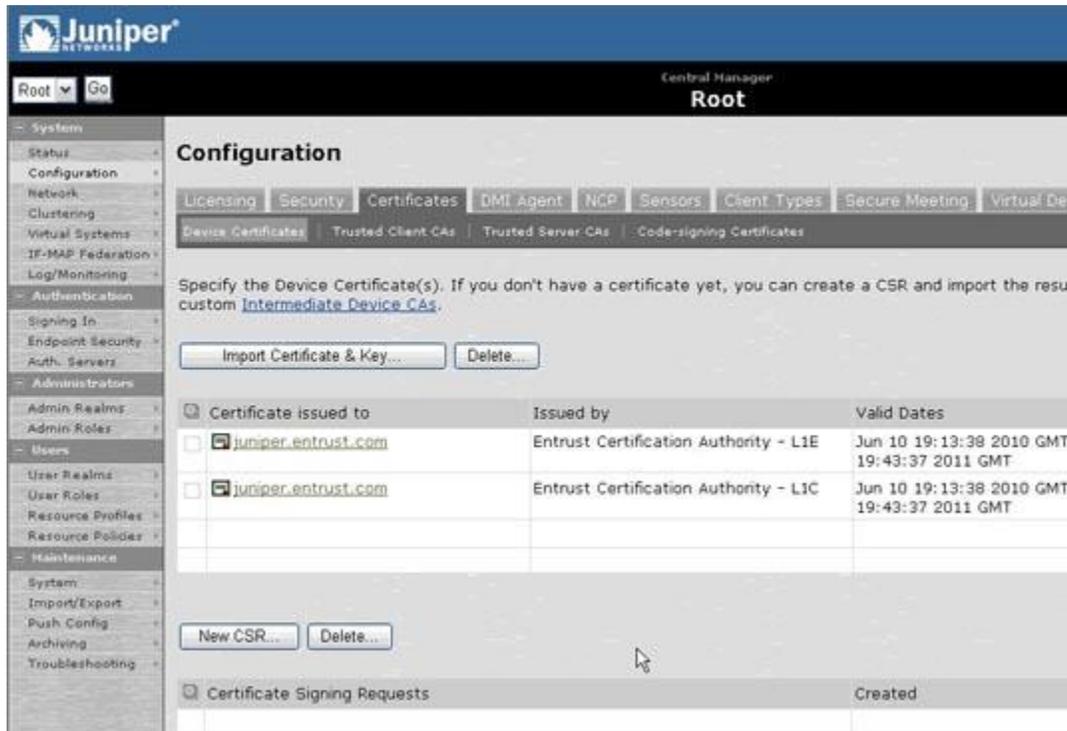


The screenshot shows the Juniper Central Manager interface. The left sidebar contains a navigation menu with categories like Systems, Configuration, Authentication, Administrators, and System. The main content area is titled 'Configuration' and has tabs for Licensing, Security, Certificates, DMI Agent, NCP, Sensors, Client Types, Secure Meeting, and Virtual Desktops. Under the 'Certificates' tab, there are sub-tabs for Device Certificates, Trusted Client CAs, Trusted Server CAs, and Code-signing Certificates. The 'Device Certificates' sub-tab is active, showing a table with columns for 'Certificate issued to', 'Issued by', and 'Valid Dates'. One entry is visible for 'juniper.entrust.com' issued by 'Entrust Certification Authority - L1E'. Below this table are buttons for 'Import Certificate & Key...' and 'Delete...'. At the bottom, there is a 'Certificate Signing Requests' section with a table showing a 'Pending CSR' for 'juniper2.entrust.com' created on '6/22/2010 16:18:02'. The 'Pending CSR' link is highlighted with a red box.

Certificate issued to	Issued by	Valid Dates
<input type="checkbox"/> juniper.entrust.com	Entrust Certification Authority - L1E	Jun 10 19:13:38 2010 GMT to Jun 10 19:43:37 2011 GMT

Certificate Signing Requests	Created
<input type="checkbox"/> Pending CSR for juniper2.entrust.com	6/22/2010 16:18:02

5. You should see a message confirming that the certificate has been imported successfully. The Server Certificate should appear in the list of Device Certificates.



Steps To Import the Intermediate Certificate onto The SSL VPN Device:

1. Log in to the admin console
2. Go to: *System > Configuration > Certificates > Device Certificates*

3. Click **Intermediate Device CAs**.

The screenshot shows the 'Configuration' page with the 'Certificates' tab selected. The 'Device Certificates' sub-tab is active. The text 'Specify the Device Certificate(s). If you don't have a certificate yet, you can create custom **Intermediate Device CAs**.' is displayed, with 'Intermediate Device CAs' circled in red. Below the text are two buttons: 'Import Certificate & Key...' and 'Delete...'. A table below shows a single entry for a certificate issued to 'test.lolocal' by 'test.lolocal'.

<input checked="" type="checkbox"/>	Certificate issued to	Issued by
<input type="checkbox"/>	test.lolocal	test.lolocal

4. Click **Import CA Certificate** and import the Intermediate certificate

The screenshot shows the 'Intermediate Device CAs' page. The text 'The following intermediate certificate authorities are used with Device Certificates.' is displayed. Below the text are two buttons: 'Import CA Certificate...' and 'Delete...'. The 'Import CA Certificate...' button is circled in red. A table below shows two entries for CA certificates.

<input checked="" type="checkbox"/>	CA certificate
<input type="checkbox"/>	www.verisign.com/CPS_Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
<input type="checkbox"/>	Comodo Class 3 Security Services CA