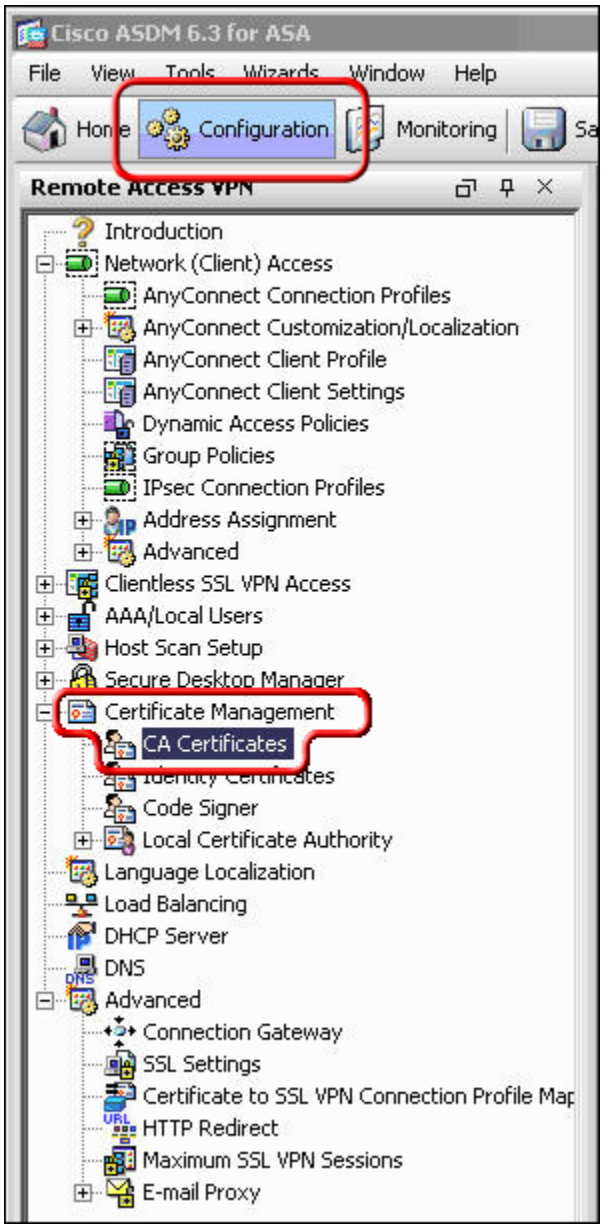
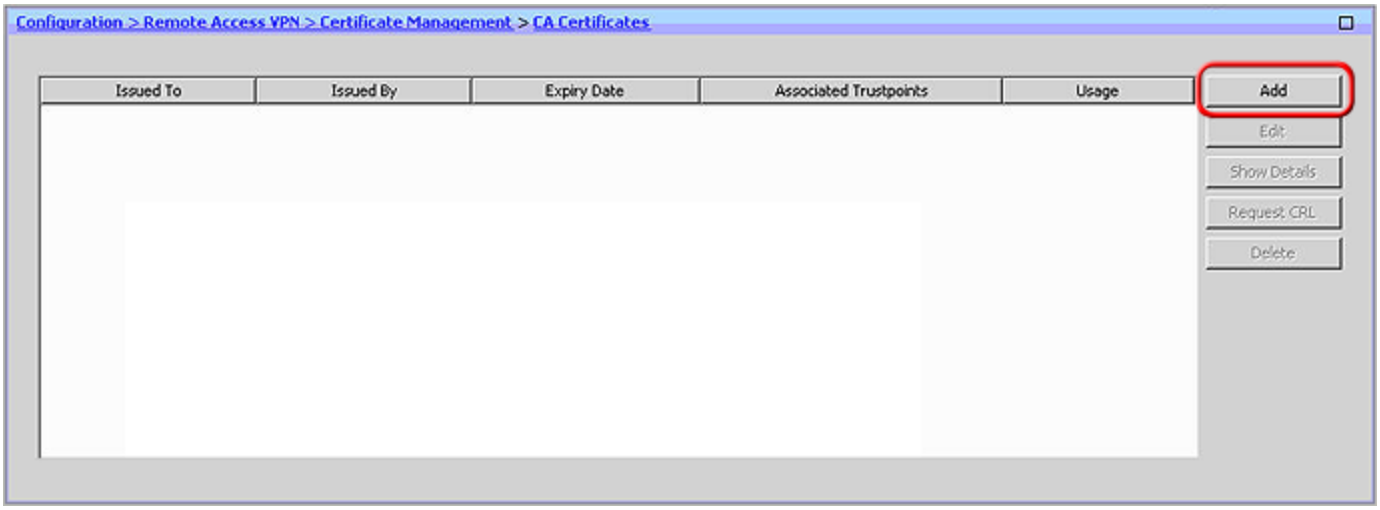
SSL VPN Firewall CSR CISCO ASA SSL Installation:

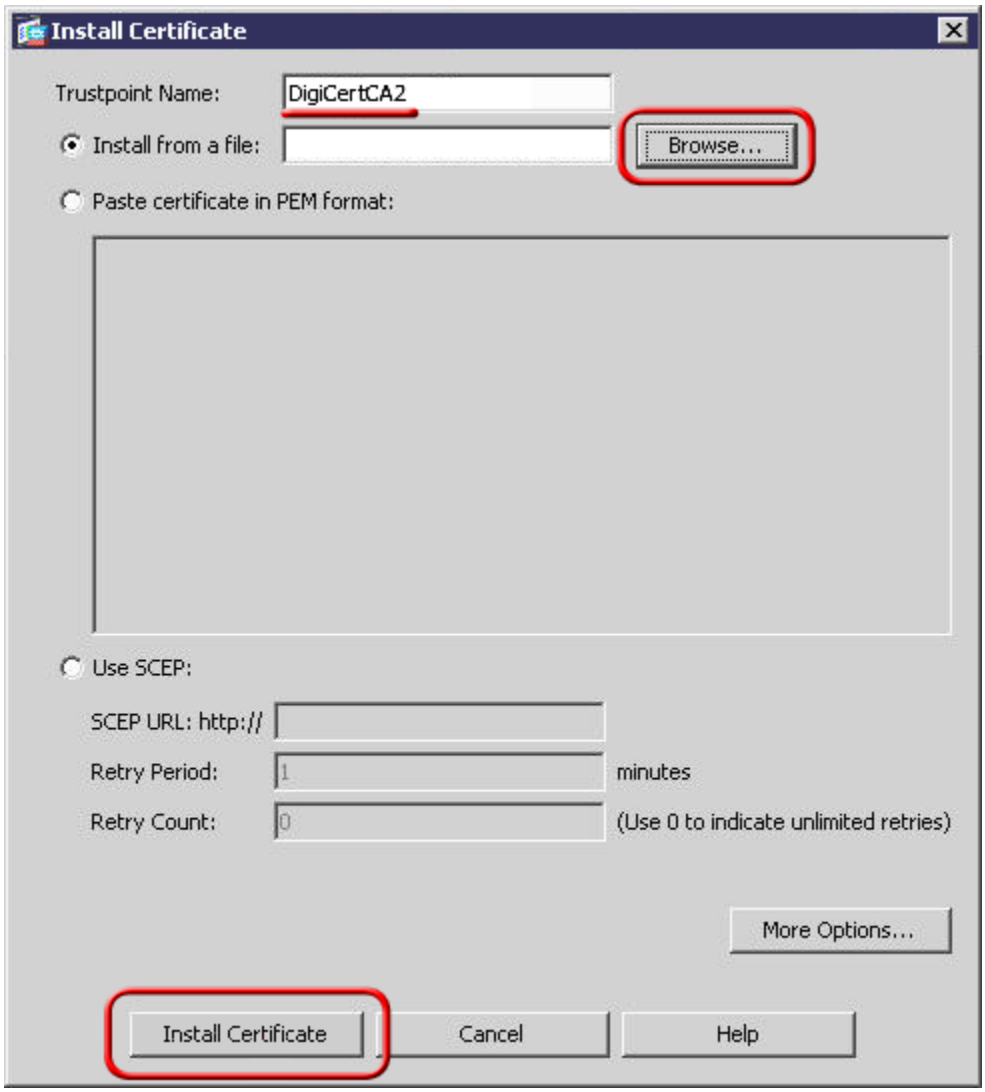
1. Open the Cisco ASDM, then Under the Remote Access VPN windowpane, then in the Configuration tab, expand Certificate Management and click 'CA Certificates'.



2. Click the 'Add' button.



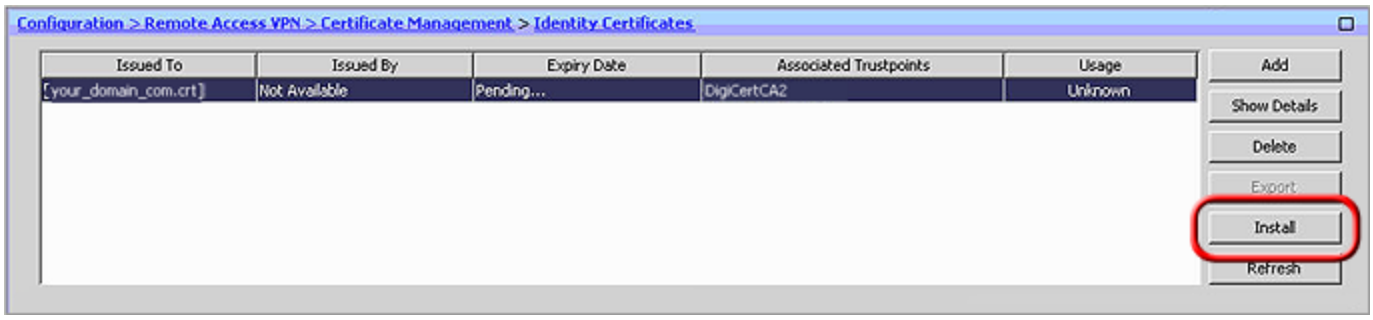
3. Assign a 'Trustpoint Name' to the certificate (e.g. DigiCertCA2), And select the 'Install from a file' Radio Button and browse to DigiCertCA2.crt. Then click 'Install Certificate'. Then repeat this process of adding a new trustpoint and installing the certificate file for 'DigiCertCA.crt'.

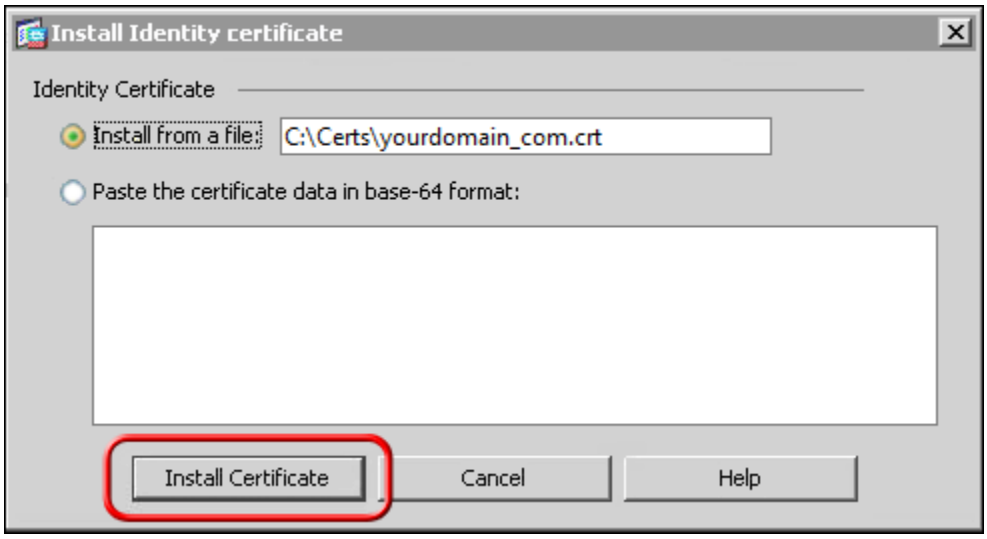


You should then see the Certificate listed with the Trustpoint Name you assigned to it.

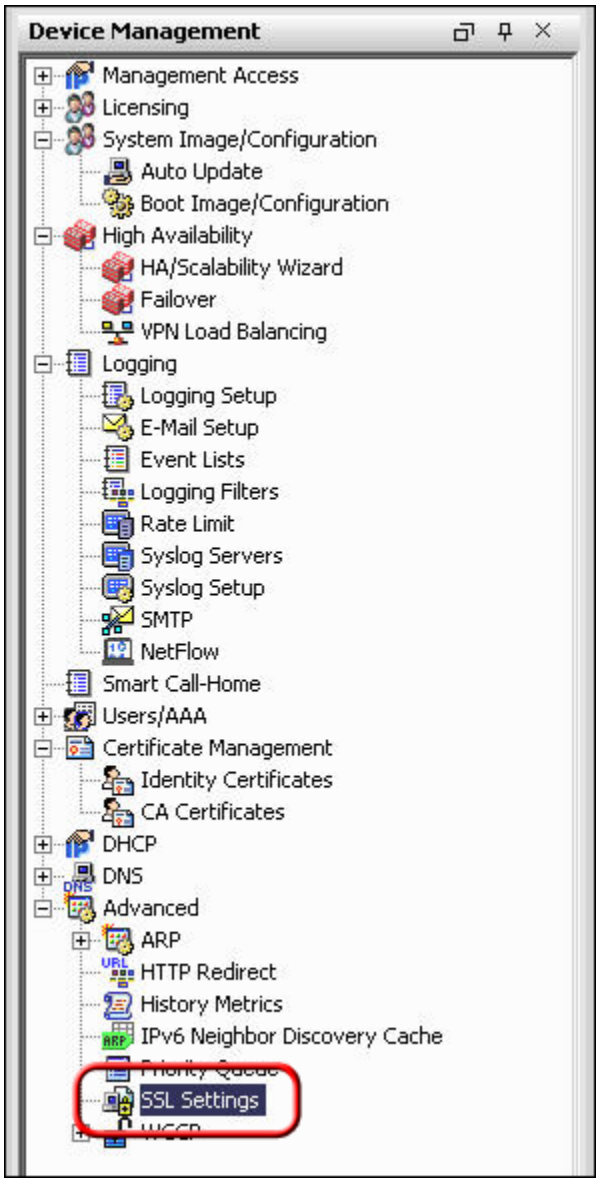
4. Then under Remote Access VPN, expand 'Certificate Management' to 'Identity Certificates'.

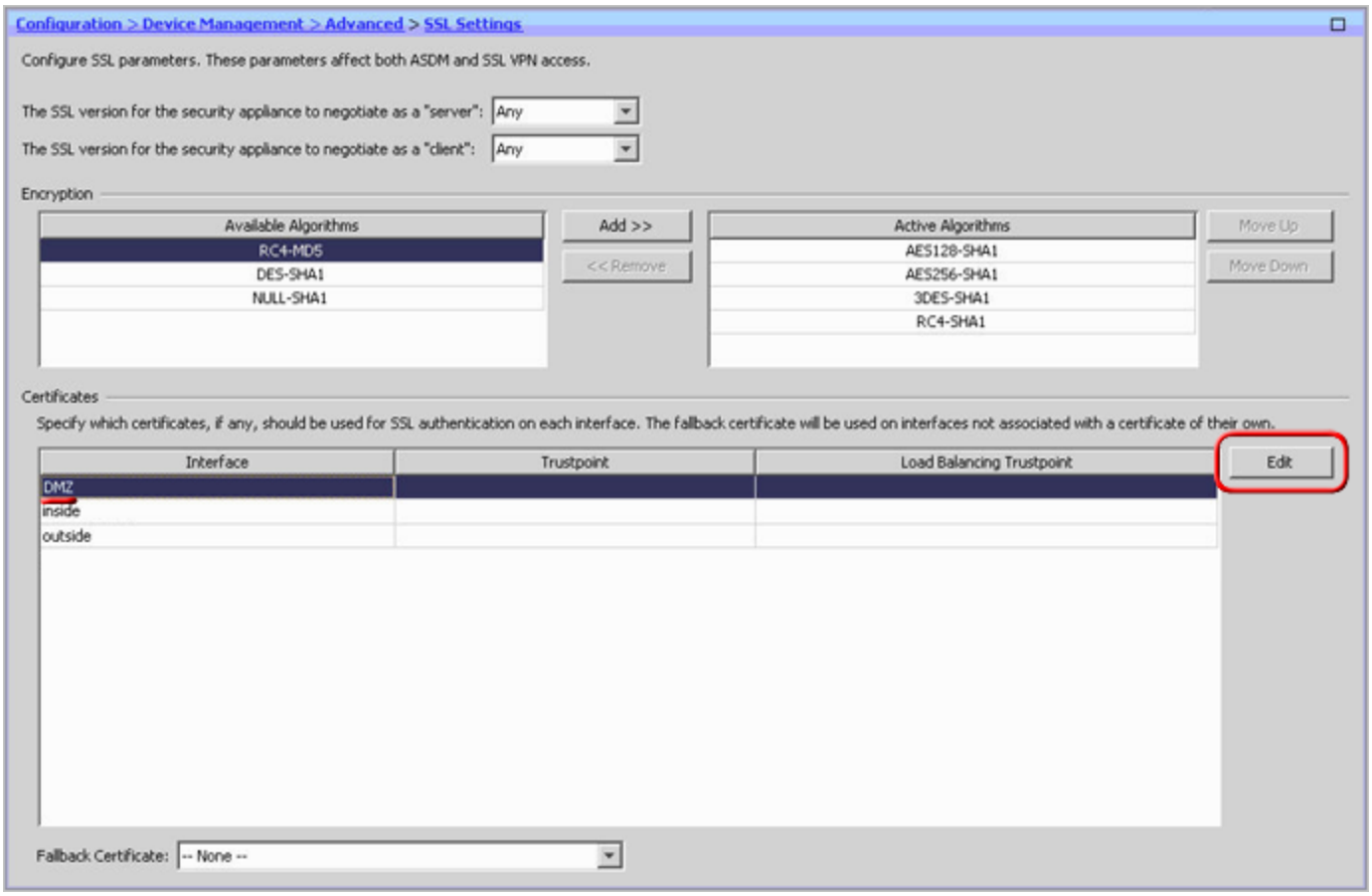
   Select the identity you created for the CSR with the 'Expiry Date' shown as pending and click **Install**, then select yourdomaincom.crt and click **Install ID Certificate File**. Once installed the Expiry Date will no longer show 'Pending'.


Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Issued To
Issued By
Expiry Date
Associated Trustpoints
Usage
[your_domain_com.crt]
Not Available
Pending...
DigiCertCA2
Unknown
Add
Show Details
Delete
Export
Install
Refresh

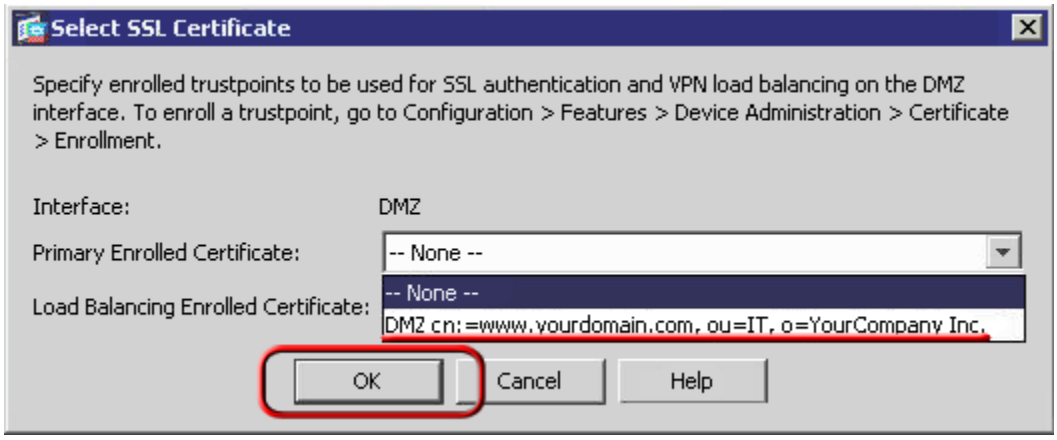

Install Identity certificate
Identity Certificate
Install from a file:
C:\Certs\yourdomain_com.crt
Paste the certificate data in base-64 format:
Install Certificate
Cancel
Help

5. The certificate now needs to be enabled. On the lower left, click **Advanced** > **SSL Settings**. Then, select the interface you want SSL enabled for and click **Edit**.





6. On the next screen, click the drop-down menu and for **Primary Enrolled Certificate** select your certificate then click **Ok**.



The ADSM will then show your certificate details under trust point.