Managing Certificates

Managing Certificates chapter describes how to generate a Self-signed certificates and Certificate Signing Request (CSR) that can be used to obtain SSL certificates from a Certificate Authority such as Verisign, Digicert and so on. This chapter also describes how to import a generated Self-Signed certificate or CA certificate in Prime Network Operation Report.

Generating Self-Signed Certificates and Certificate Signing Request

Generate a self-signed certificate and a Certificate Signing Request (CSR) by using the **Generate Self-Signed Certificate and Certificate Signing Request** option. When you generate a self-signed certificate, a new self-signed certificate in PEM format and a CSR file are created in the $ANAHOME/scripts/CSR/ directory. When you press enter in a command without specifying any value the script will select a default option automatically. For example, if you do not specify a domain name, the script by default picks the domain name as cisco.com.

Step 1 Execute $ANAHOME/local/scripts/selfsignedcert.pl.

Step 2 Choose **Generate Self-Signed Certificate and Certificate Signing Request(.csr)** and press **Enter**. The system prompts you to enter information as listed in the following table.

Table 33-1   Parameters and Description

Parameter	Description	Display Message
`Domain Name [cisco.com]:`	Enter the domain name. By default the script accepts cisco.com as domain name.	

`How many days is self-signed certificate valid for? [365]:`	Enter the number of days that you want the self-signed certificate to be valid for.	`writing new CSR (Certificate Signing Request) to /export/home/pn430/scripts/CSR/test.csr`
		`writing private key to /export/home/pn430/scripts/CSR/test.key`
		`Generating a 2048 bit RSA private key`
		`writing new private key to /export/home/pn430/local/scripts/cisco.com.key'`
		`You are about to be asked to enter information that will be incorporated into your certificate request.`
		`What you are about to enter is what is called a Distinguished Name or DN.`
		`There are quite a few fields but you can leave some blank.`
		`For some fields there will be a default value,`
		`If you enter '.', the field will be left blank.`

`Country Name (2 letter code) [GB]: State or Province Name (full name) [Berkshire]: Locality Name (eg, city) [Newbury]:`	Enter the country name, state or province name and locality name,	
`Organization Name (eg, company) [My Company Ltd]: Organizational Unit Name (eg, section) []:`	Enter the organization name and Organizational unit name.	
`Common Name (eg, your name or your server's hostname) []:`	Enter the common name.	

Table 33-1   Parameters and Description

Parameter	Description	Display Message
`Email Address []:`	Enter the email address.	
`A challenge password []:` `An optional company name:`	(Optional) Enter a challenge password and an optional company name.	`CSR generated successfully (/export/home/pn430/scripts/ CSR/cisco.com.csr)` `Use the CSR to obtain a certificate in PEM/CER format from a CA (Certificate Authority).` `New self-signed certificate in PEM format generated (/export/home/pn430/scripts/ CSR/cisco.com.pem)`

Importing Certificate Authority or Self-Signed Certificate

Import a Certificate Authority (CA) signed certificate or self-signed certificate by using Import CA/Self-Signed Certificate option. You can either import the generated self-signed certificate or import a certificate generated by another system or third party by copying the .pem and .key (private key) files to the $ANAHOME/scripts/CSR directory. The .pem file provided is exported into PKCS12 format, and then converted to JKS format. The JKS file can be imported into Tomcat.

Step 1   Execute $ANAHOME/local/scripts/selfsignedcert.pl as PN user.

Step 2   Choose the **Import CA/Self-Signed Certificate** option and press **Enter**.

Step 3   Specify values for the following parameters and then press **Enter**:

Table 33-2   Parameters and Description

Parameters	Description
`Domain Name [cisco.com]:`	Enter the domain name.
`CA/self-signed certificate (.pem/.cer) file path:`	Enter the path to the CA signed certificate or self-signed certificate.
`private key file path:`	Enter the path to the private key.
`keystore password:`	Enter the Java KeyStore (JKS) password to set.
The following confirmation messages might appear, enter Yes or No to proceed further.	
`Existing certificate will be erased, wa.nt to proceed (Yes/No):`	Enter Yes to proceed or No to exit.
`Prime Network and Operation Report restart required applying certificate, do you want to restart (Yes/No):`	Enter Yes to proceed or No to exit. If you enter yes then a message similar to the following one appears: Restarting Prime Network and Operation Report...Done Certificate $ANAHOME /scripts/CSR/cisco.com.pem imported to server successfully.