Quick Note 16

Configuring HTTPS web server mode.

Table of Contents

1.1 Version

Version Number	Status
1.0	Publsihed

2.0 INTRODUCTION

2.1 Outline

This application note is intended to explain how to secure the connection to a Sarian router's web interface with HTTPS. You will create RSA key files, certificate requests, and use SCEP to retrieve a signed certificate from a Microsoft® 2003 server for use with SSL.

2.2 Assumptions

- The Sarian router's configuration is set to factory defaults

- The Sarian's firmware version is 5.002 or later.

- The user has prior knowledge of RSA Key files and certificates

- The user has prior knowledge of SSL

2.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: applicationnotes@sarian.co.uk

3.0 SETTING UP THE CERTIFICATE AUTHORITY

NB: The section covers setting up a Microsoft 2003 Server as a Certificate Authority. If you have access to a Certificate Authority that is already set up then skip this section and go to section 4.0.

For a Microsoft® 2003 server to act as a Certificate Authority the following services must be installed;

1. **IIS** (Internet Information Services)

2. **Certificate Services**, including **Certificate Services CA** and **Certificate Services Web Enrolment Support**.

The Simple Certificate Enrolment Protocol (SCEP) Add-on for Certificate Services will also require downloading to the server for installation.

At the time of publication the SCEP add-on could be obtained from the following link.

http://www.microsoft.com/downloads/details.aspx?FamilyID=9f306763-d036-41d8-8860-1636411b2d01&DisplayLang=en

3.1 Configure the Microsoft® 2003 Server as a Certificate Authority

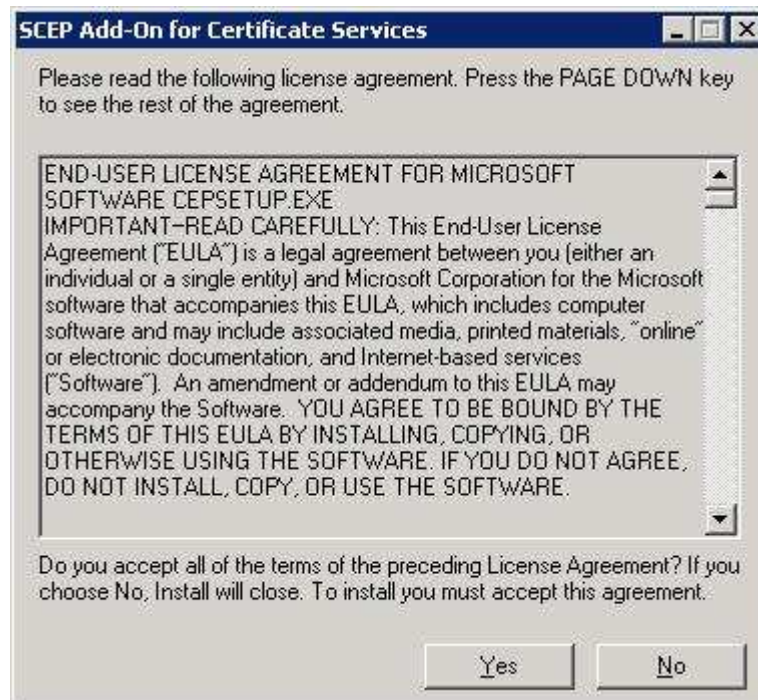### Install SCEP Add-on for certificates

Login to the Microsoft® 2003 Server with an appropriate System Administrator account

With your mouse double-click the **cepsetup.exe** icon to begin installation.

The following dialogue box will appear. Click **Yes** to proceed.

Next the end user licence agreement will appear. If you agree, click **YES**.

The SCEP Add-on for Certificate Services Setup Wizard will start. To proceed click **Next**.

A dialogue box will appear asking for the identity that IIS (Internet Information Services) should use for running the SCEP Add-on for Certificate Services.

Choose **Use the local system account** and click **Next**.

A dialogue box will appear asking if you wish to select the challenge phrase if you wish the CA to automatically issue certificates to SCEP requests.

Select the **Require SCEP Challenge Phrase to Enroll** tick box. Click **Next**.
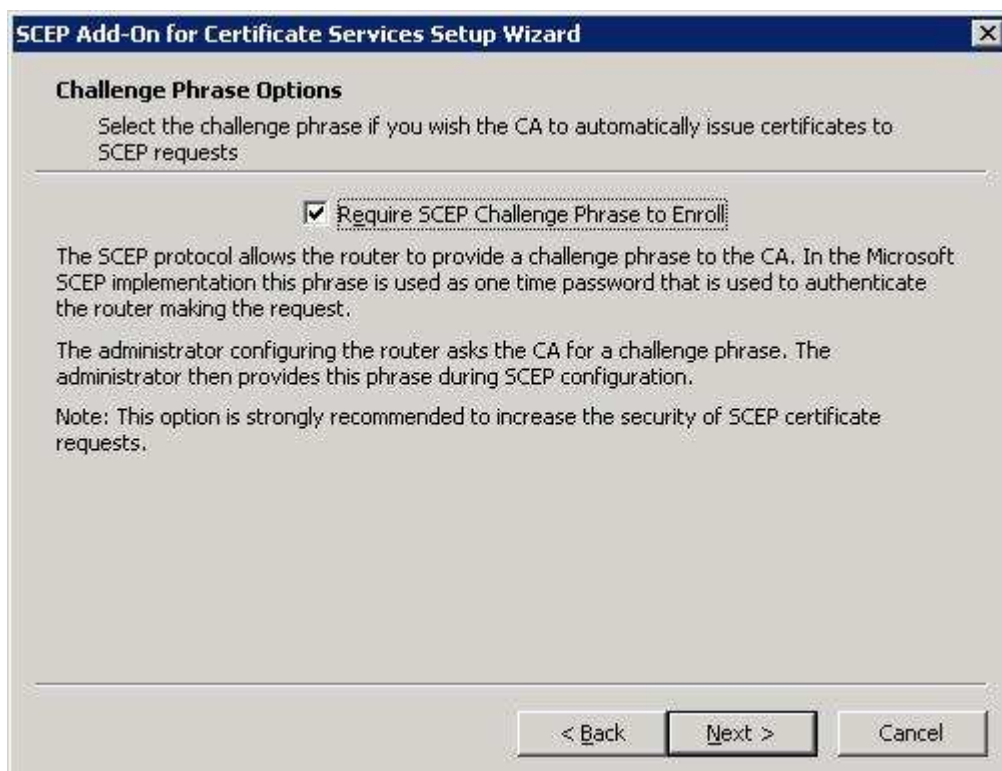
A form will appear in which you are asked for information to enrol for the RA* (Registration Authority) certificates. Enter appropriate details and click **Next**.

*RA. A computer that is configured for an administrator to request and retrieve issued certificates on behalf of other users

A dialogue box will appear completing the SCEP Add-on for Certificate Services Setup Wizard. Confirm the details shown are correct. If so click **Finish**.

Finally a dialogue box will appear containing a URL to use for SCEP enrolment.

IMPORTANT: Make a permanent note of this URL. You will need it every time you create certificates with this CA.

3.2 Check the CA Certificate service is running

To check the CA Certificate service is running, click **Start** → **All Programs** → **Administrative Tools** → **Certificate Authority**.
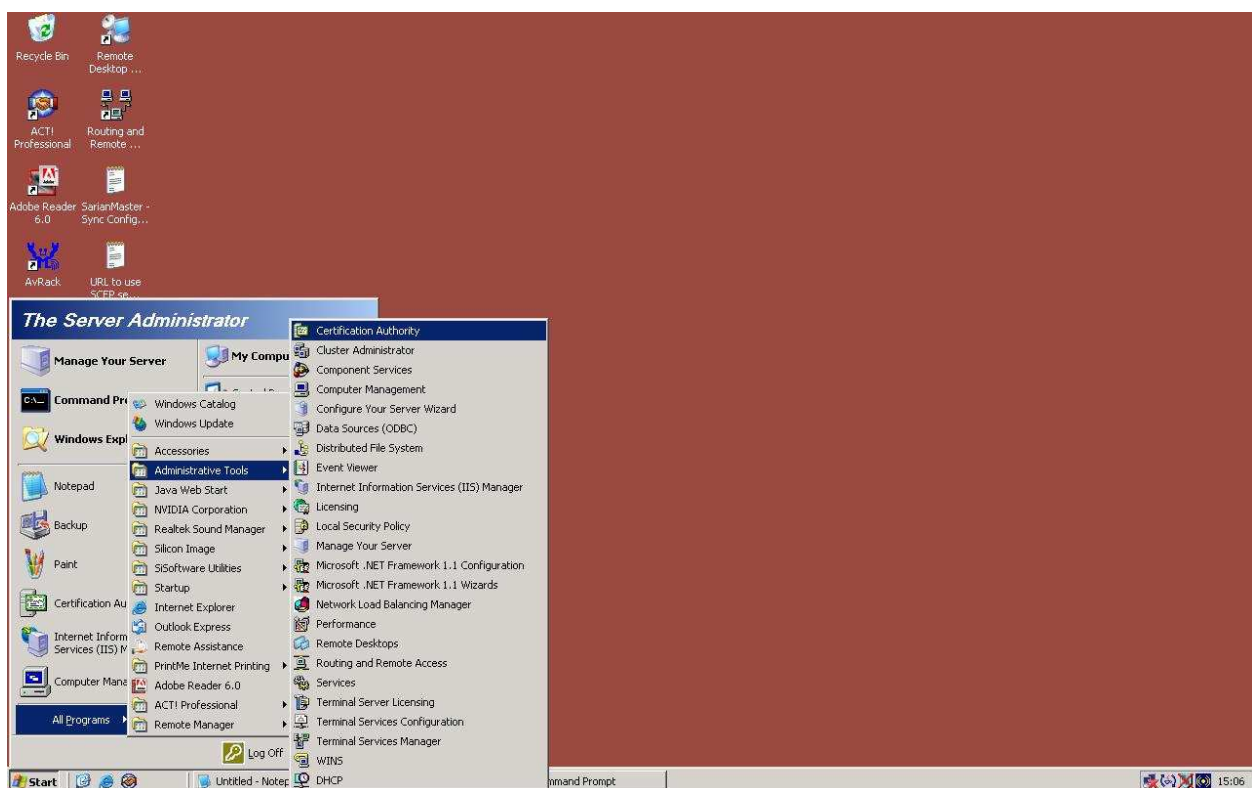
The Certificate Authority console window will open. If the service is running there will be a green tick on your Certificate Authority. If not the service will need to be started by right clicking on the Certificate Authority, select **All Tasks** → **Start Service**.
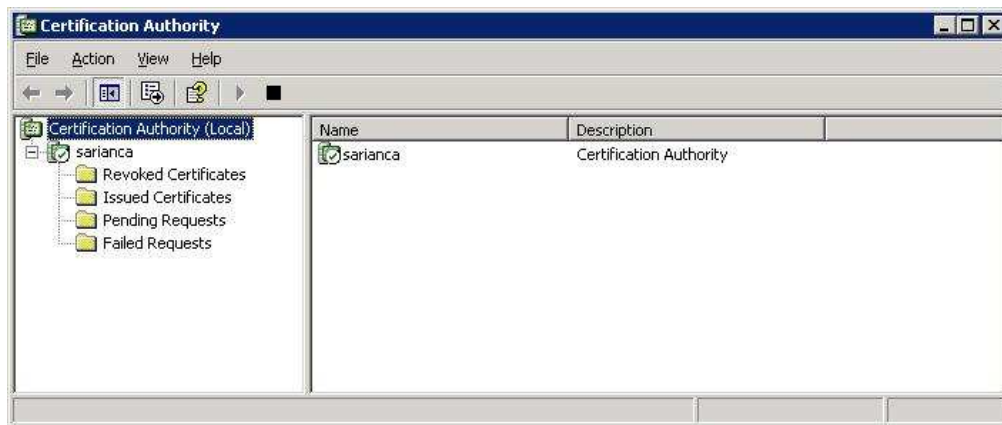
3.3 Configure IIS

When IIS is installed, the service is installed in a highly secure and locked mode. Therefore you may have to configure IIS to allow the SCEP Add-on service to run in IIS.

Open the **Computer Management** console.
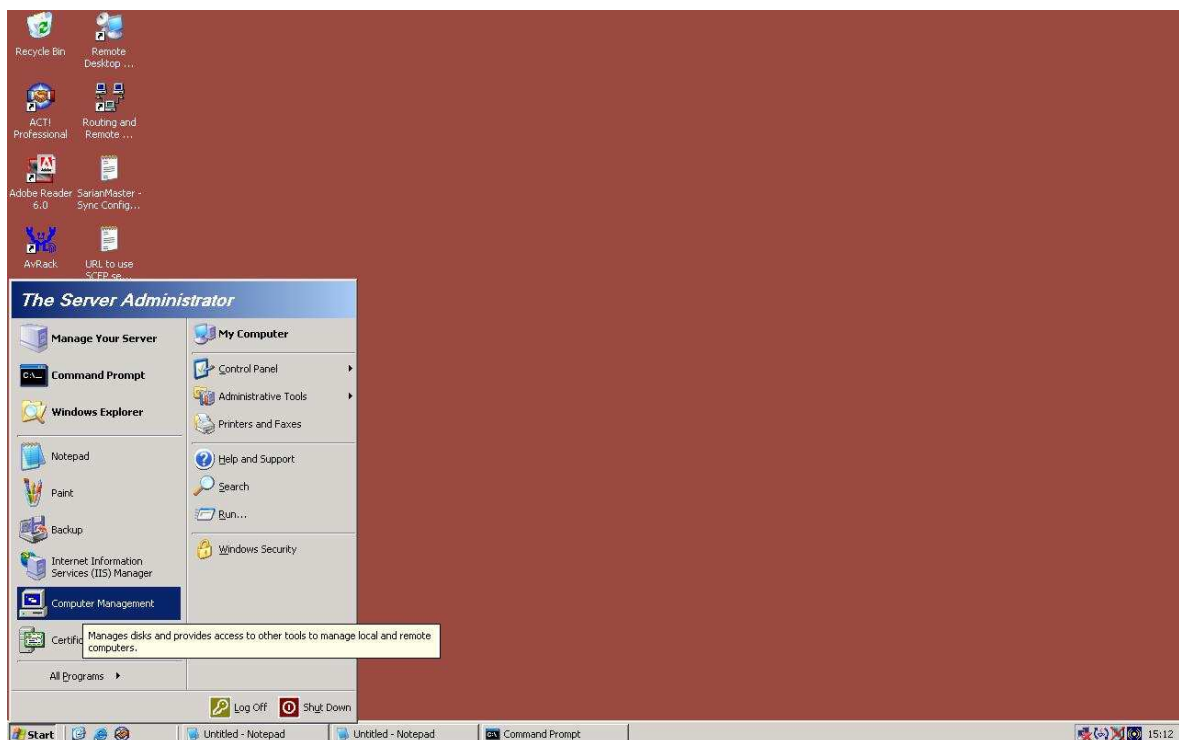
Expand the **Services and Applications icon** and **Internet Information Services** and **Web Service Extensions**.

In the **Web Service Extensions** window, highlight **Simple Certificate Enrolment Protocol (SCEP) Add-on**. Click the **Allow** button. A green tick should appear on that item.
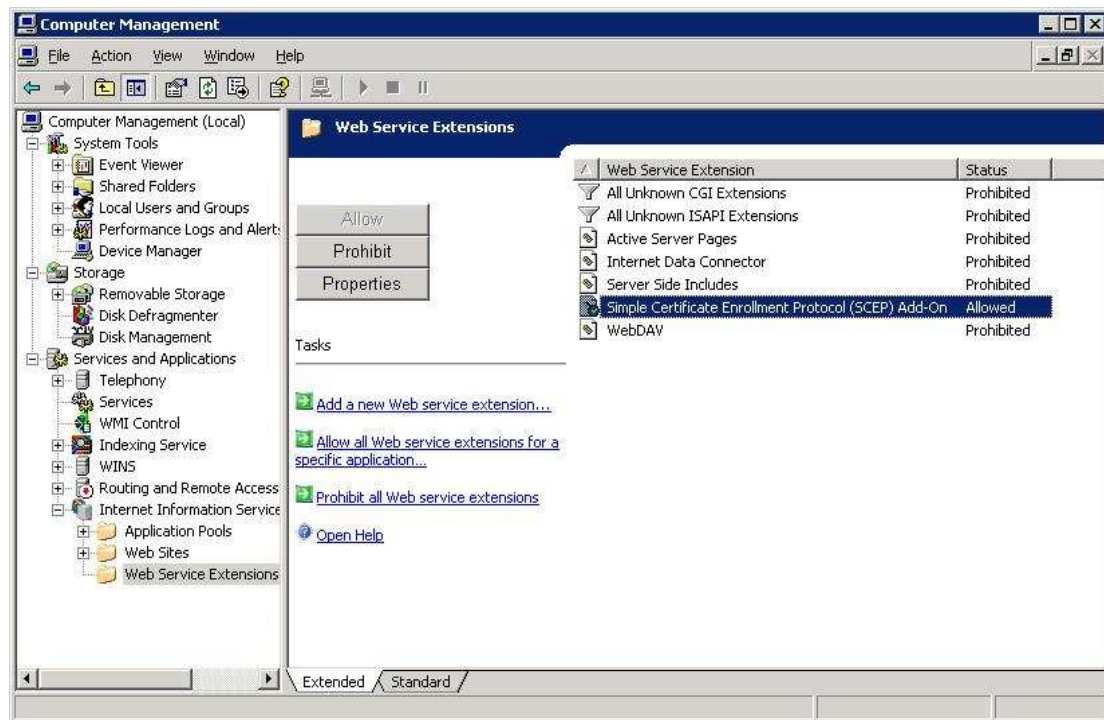
3.4 Automatic Enrolment

As with this application note, the default action for the Microsoft 2003 Certificate Authority is for all certificate requests to be issued manually by the CA administrator. This ensures that the administrator is responsible for verifying the identity of the certificate requestor.

However, Microsoft have included a facility for automatic enrolment where certificates are signed and issued by the CA server automatically on receipt of the certificate request.

To enable this feature open the Certificate Authority console as previous. click **Start** → **All Programs** → **Administrative Tools** → **Certificate Authority**.

Right click on your certificate authority and select **Properties**.
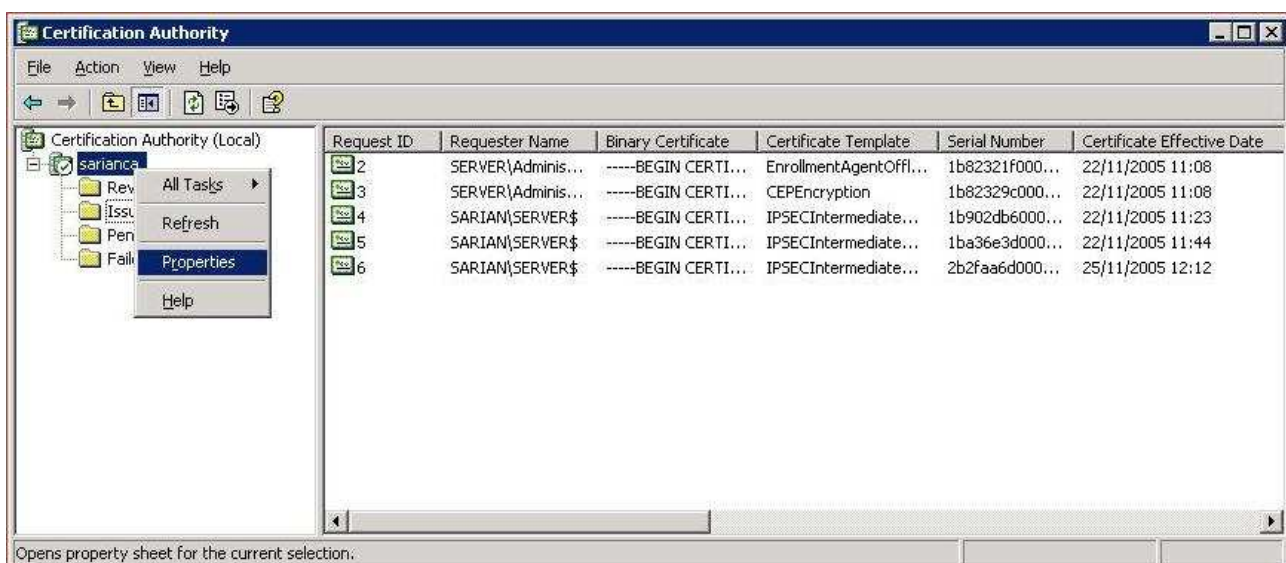
In the **Properties** window select the **Policy Module** tab.
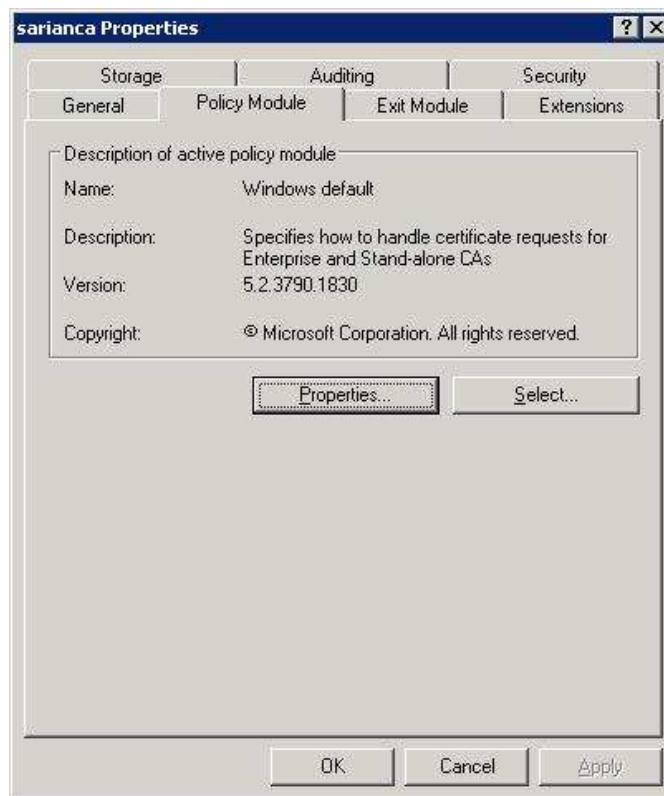
Whilst in the **Policy Module** tab click the **Properties** button.

Select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.
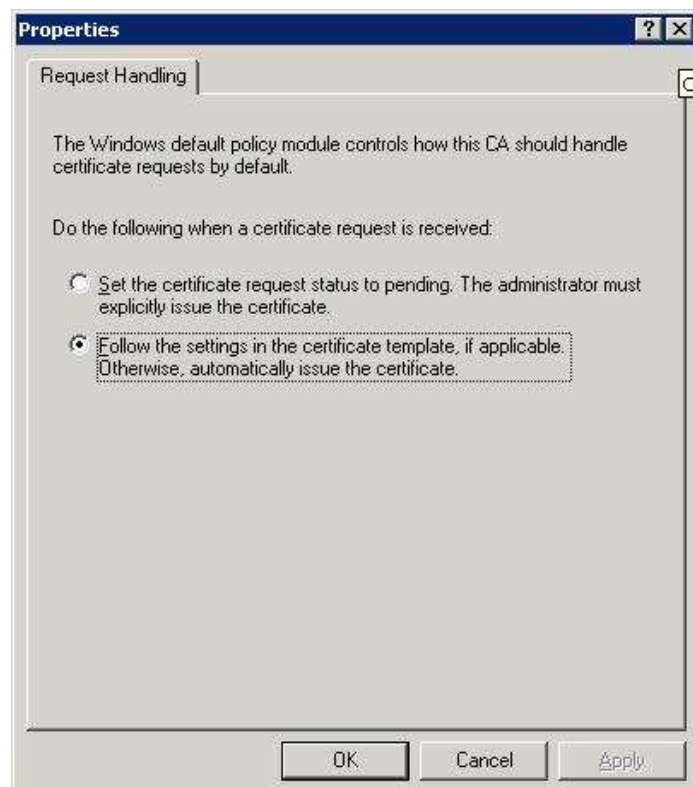
Click **OK** and again **OK** on the **Policy Module** tab.

Note: For the change to take effect, certificate services must be stopped and started again.

4.0 SARIAN SSL CERTIFICATES

4.1 Ethernet 0 LAN Configuration

The following configures the Ethernet port of the router.

Browse to **CONFIGURE → ETHERNET → ETH 0**
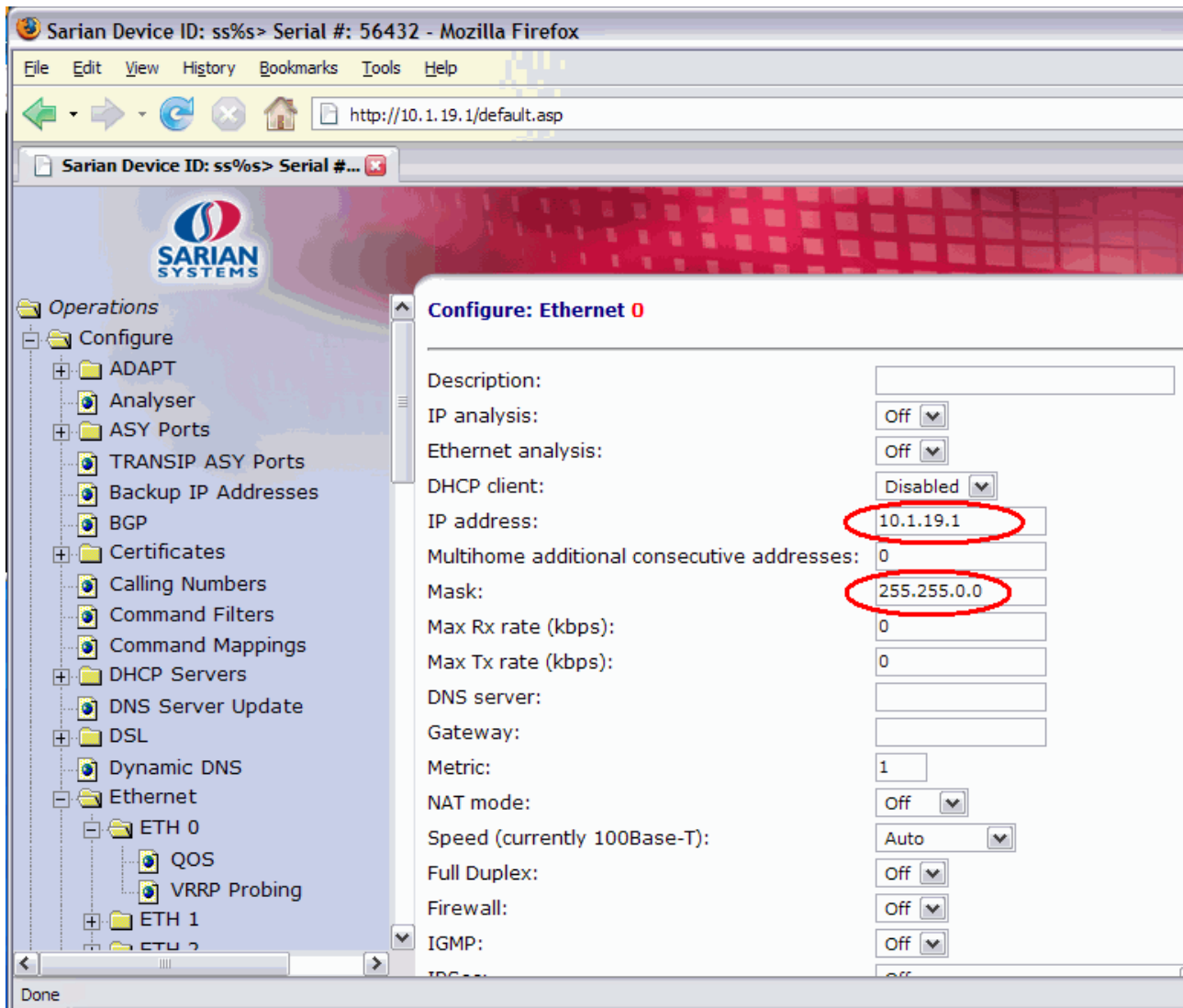
Parameter	Setting	Description
IP Address:	10.1.19.1	Configures the IP address for the LAN
Mask:	255.255.0.0	Configures the subnet mask for the LAN

4.2 Time and Date

Any certificates stored on the Sarian's flash will have a validity period. Therefore it is important that the date and time are correct.

Browse to **CONFIGURE → TIME**

Amend the time and date as appropriate and click **Set Time** button.
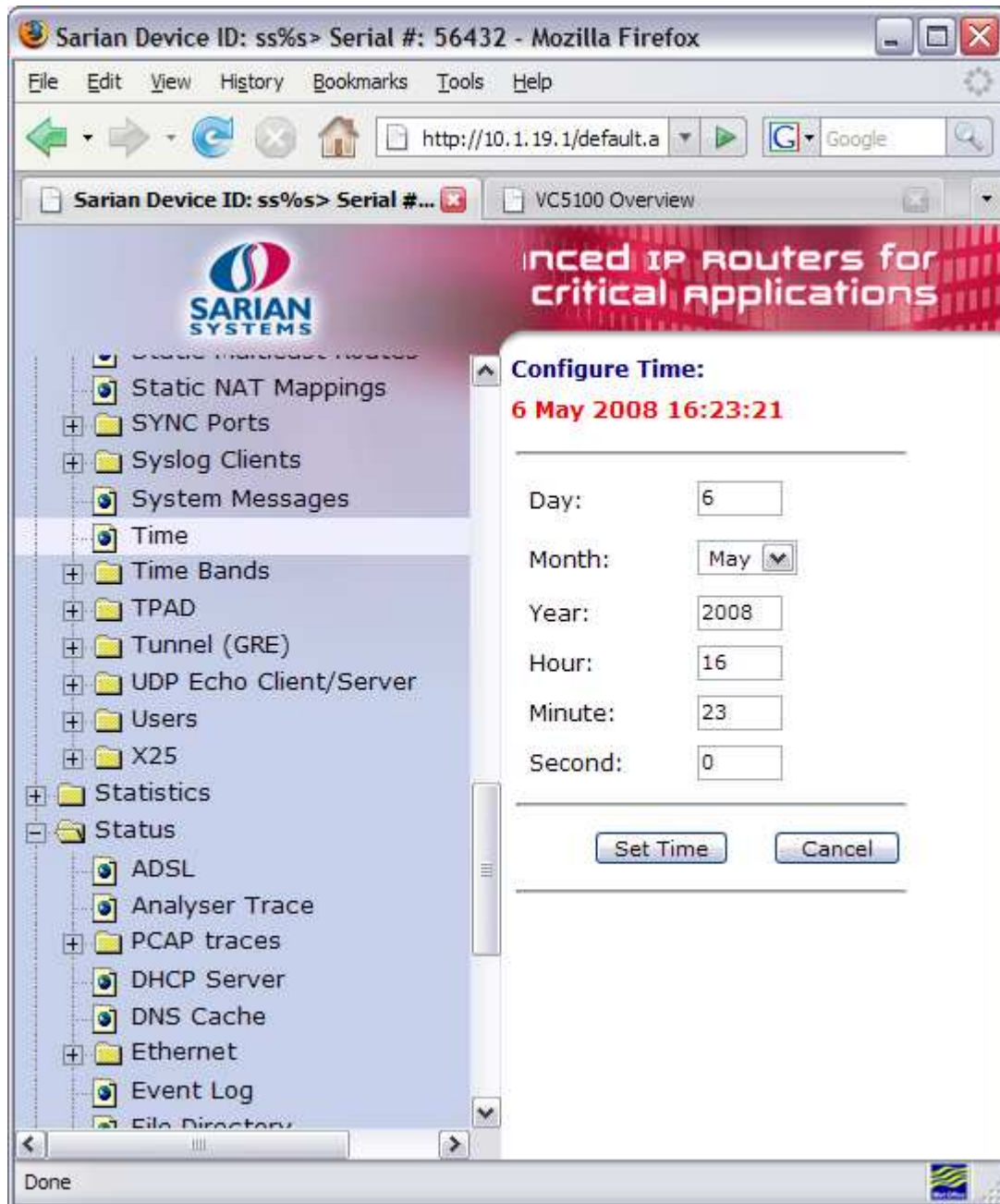
4.3 Creating the Private Key and Certificate Request

Obtain a Challenge Password for the Certificate Request.

Before you can create a certificate request you must first obtain a challenge password from the Certificate Authority Server. This password is generally obtained from the SCEP CA server by way of WEB server, or a phone call to the CA Server Administrator. For the Microsoft® SCEP server, you browse to a web interface. If the server requires a challenges password, it will be displayed on the page along with the CA certificate fingerprint.

This challenge password is usually only valid once and for a short period of time, in this case 60 minutes, meaning that a certificate request must be created after retrieving the challenge password.

From a PC browse to the following Microsoft® CA server web page using URL http://<server_hostname>/certsrv/mscep/mscep.dll (as detailed in "Microsoft® 2003 server Configuration) and make a note of the challenge password.
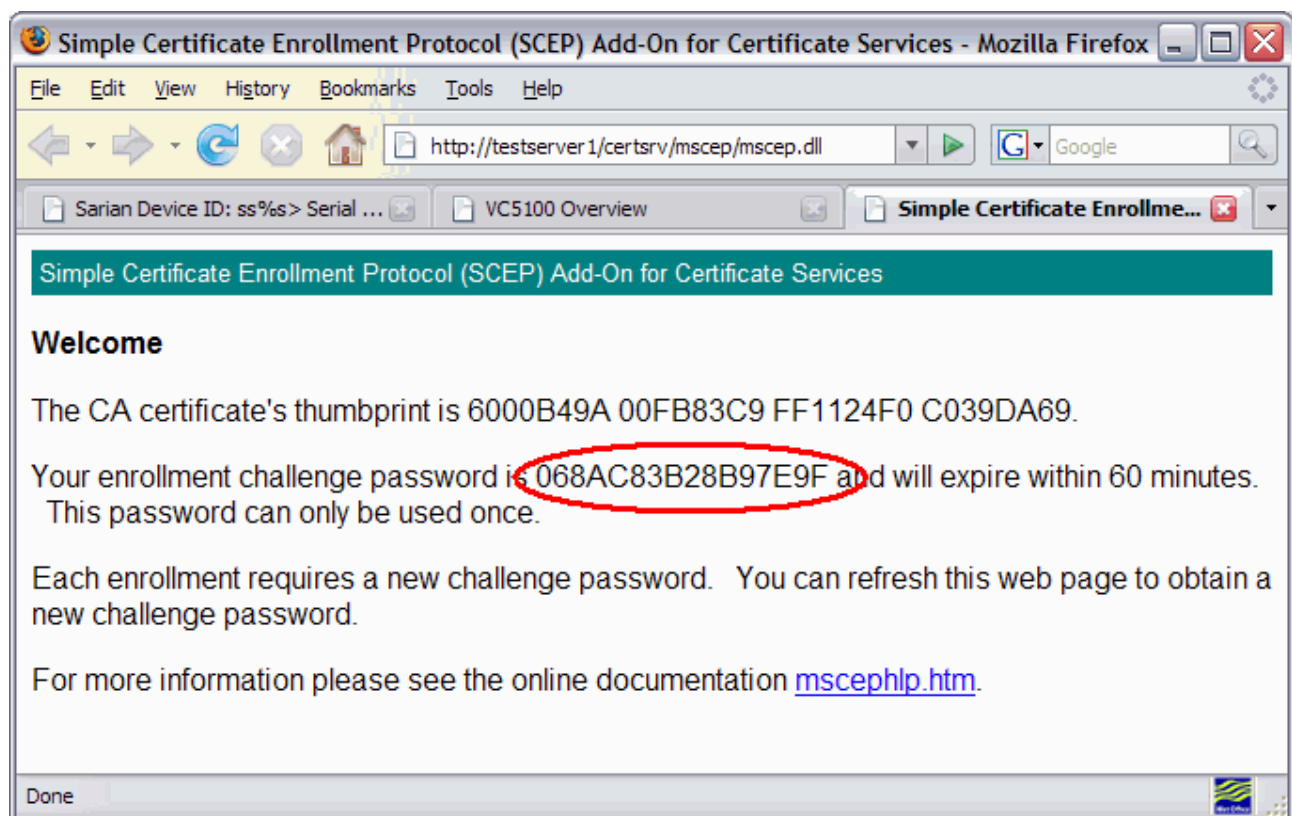
Configure the Certificate Request page

Browse to **CONFIGURE → CERTIFICATES → CERTIFICATE REQUEST**

Enter the above challenge password and configure all other fields as appropriate. These details will form part of the certificate request and thus form part of the signed public key certificate

NOTE: The **Common Name** (case sensitive) field is important as this will be used as the ID for the device for the IKE negotiations.
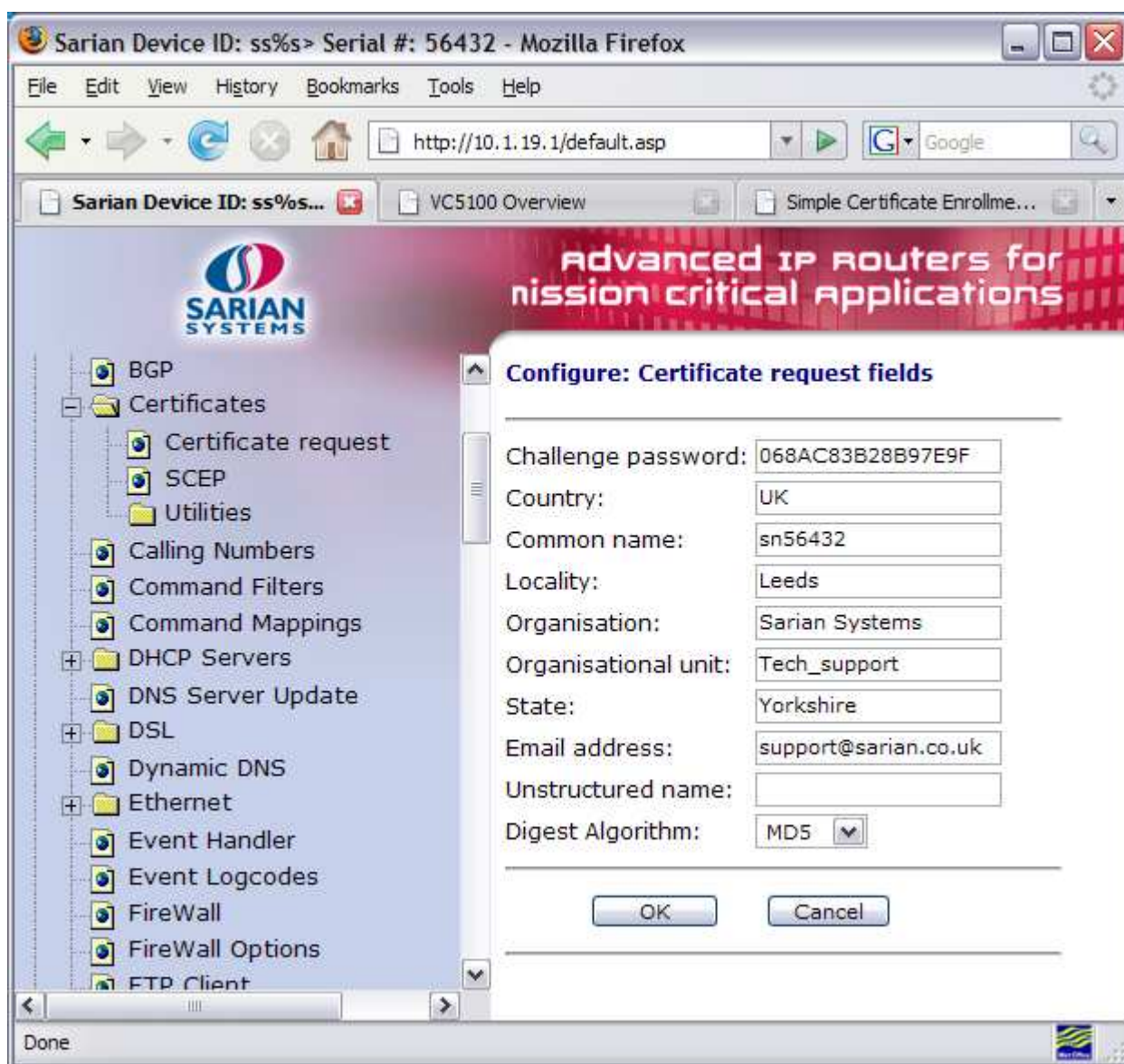
Example Settings

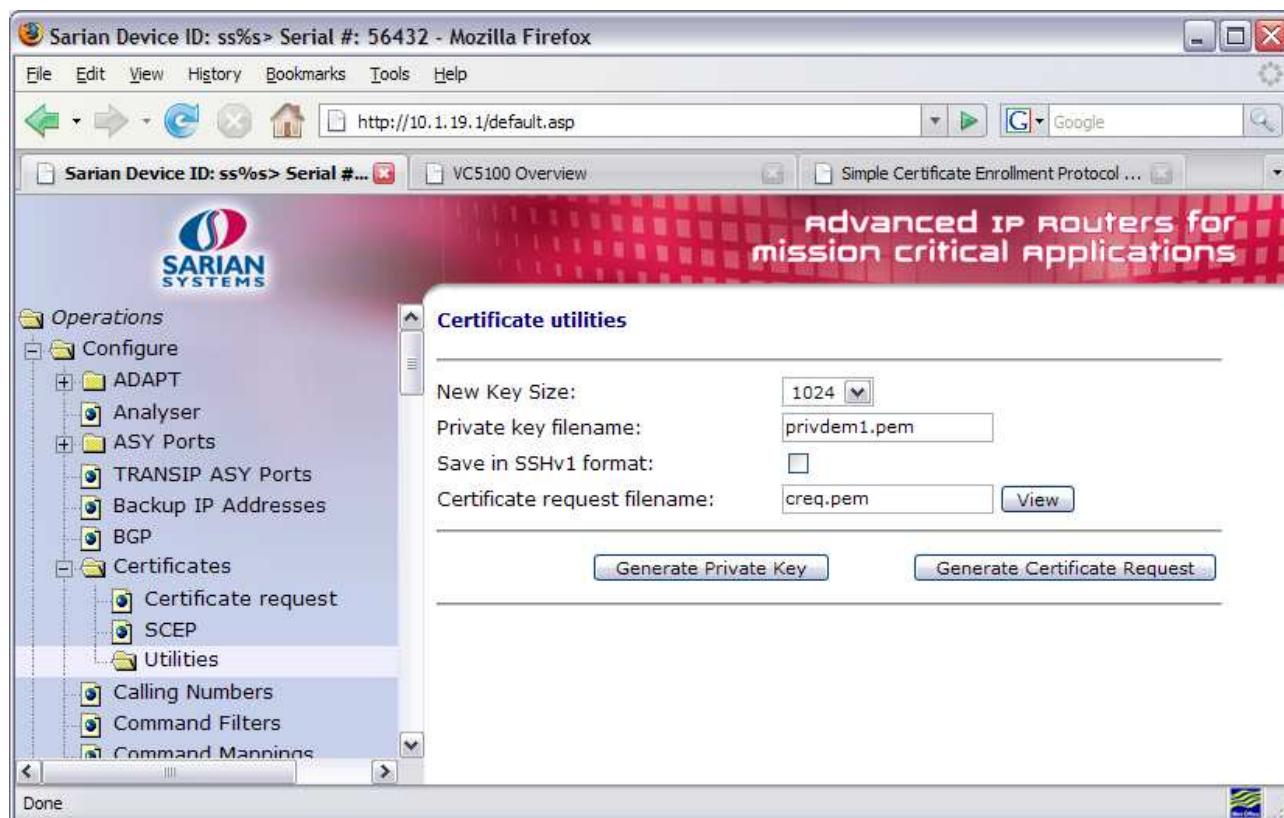| Parameter	Setting	Description
Challenge Password:	068AC83B28B97E9F	Enter the Challenge Password issued by the SCEP server
Country:	UK	Enter a two character representation of the country
Common Name:	Sn56432	Enter a Common Name for the router's ID
Locality:	Ilkley	The Location of the unit
Organisation:	Sarian Systems	An appropriate Company name
Organisational Unit:	Demo Department	An appropriate organisational unit
State:	Yorkshire	State or County or Province
Email Address:	support@sarian.co.uk	An appropriate email Address
Unstructured Name:		Optional descriptive text
Digest Algorithm:	MD5	Choose either MD5 or SHA1. This is used when signing the certificate request

Create the Private Key and Certificate Request Files

Now the details for the certificate request have been entered, the Sarian must create a Private Key and from this the certificate request will be created.

NOTE: This method assumes that a private key does NOT already exist. Both the private key and certificate request will be crested simultaneously. If the **New key size:** parameter is set to **OFF** then a private key will not be generated.

Browse to **CONFIGURE → CERTIFICATES → UTILITIES**.

Parameter	Setting	Description
New Key Size:	1024	Size of the private key in bits
Private Key filename:	privdem1.pem	Enter a name for the private key (must be prefixed with "priv" and have a .pem extension).
Certificate request filename:	creq.pem	Enter a name for the certificate request (must have a .pem extension)

Click the **Generate Certificate Request** button. This will generate both the private key and the certificate request files. You will see some indication of the progress as the Sarian generates the Private Key file and certificate request as follows;
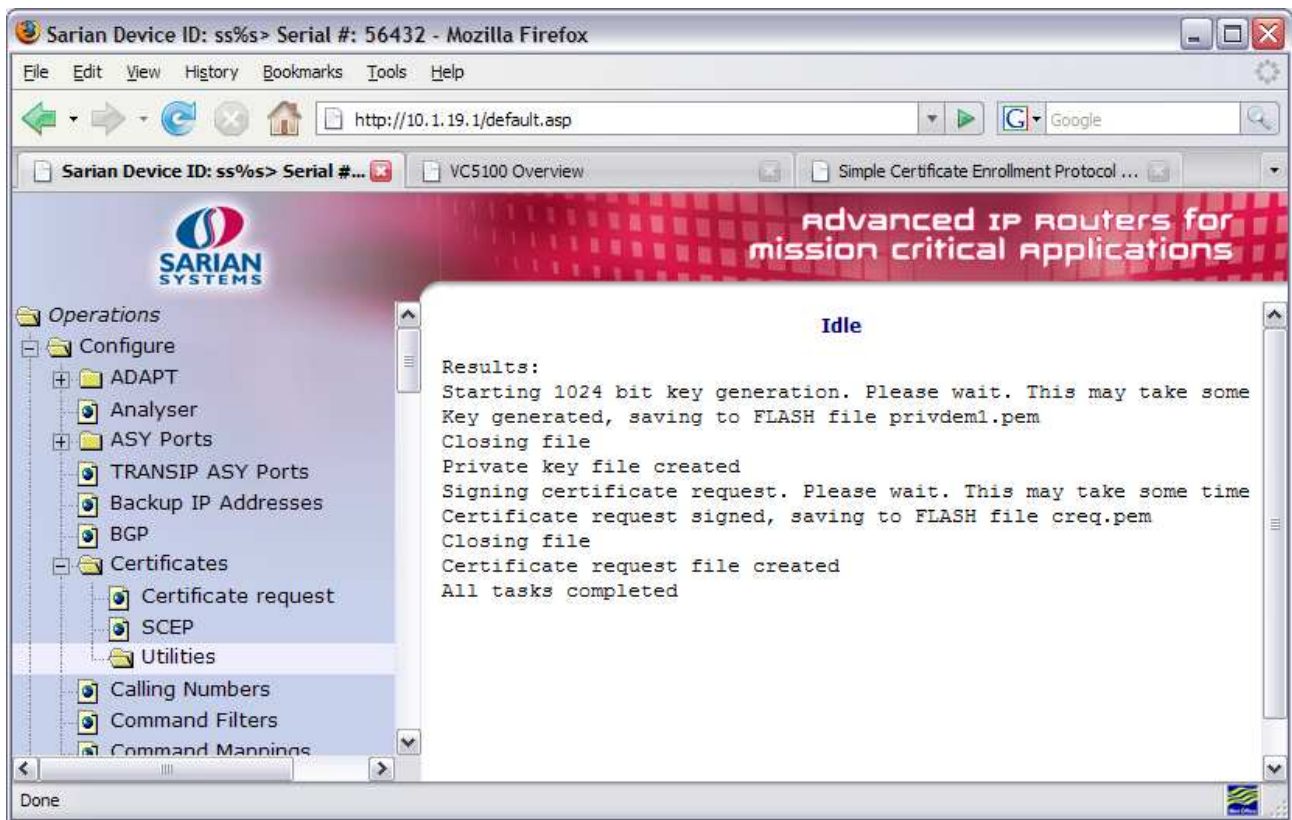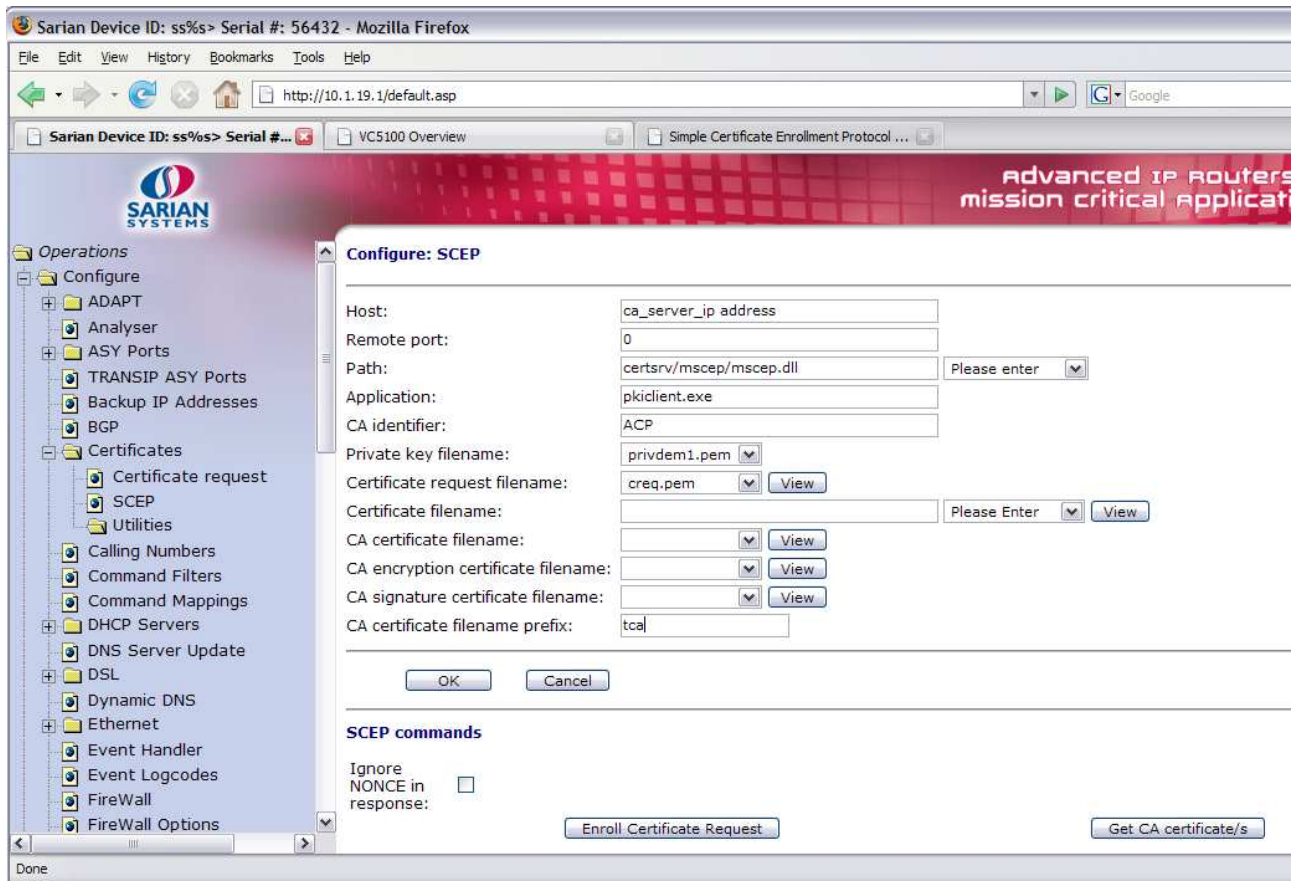
4.4 Using SCEP to retrieve the CA certificates

Before delivering the request to the server, the unit must first have access to the server CA certificate(s). Some servers require the use of more than one CA certificate. In this case the Microsoft® 2003 server requires 3 CA certificates before SCEP can work. For other servers, just one certificate may be used for all three tasks. Check your server vendor for details.

The tasks these certificates are used for are:

- **CA certificate**. This is the certificate that will contain the public key portion of the key used to sign the certificate request.

- **CA encryption certificate**. This certificate is used to encrypt the data the client will send to the server.

- **CA signature certificate**. This is attached to the reply from the CA which is validated by the client. The public key from this certificate is used to verify the signature.

Browse to **CONFIGURE → CERTIFICATES → SCEP**.

Parameter	Setting	Description
Host:	Ca server ip address	Ca server ip address
Remote port:	0	MS SCEP uses HTTP to carry the requests, If this parameter is non-zero, the unit will use this value as the destination port rather than the default of 80
Path:	certsrv/mscep/mscep.dll	Select Microsoft SCEP from drop down list and the path will be entered automatically
Application:	pkiclient.exe	This represents the SCEP application on the server
CA Identifier:	ACP	CA identifier
Private Key filename :	privdem1.pem	The name of the private key created earlier
Certificate request filename:	creq.pem	The name of the certificate request created earlier
CA certificate filename prefix:	tca	Prefix used for all CA certificates

Click the **Get Ca certificate/s** button to retrieve the CA certificates from the Microsoft® 2003 Server. An indication of progress will be shown as follows;
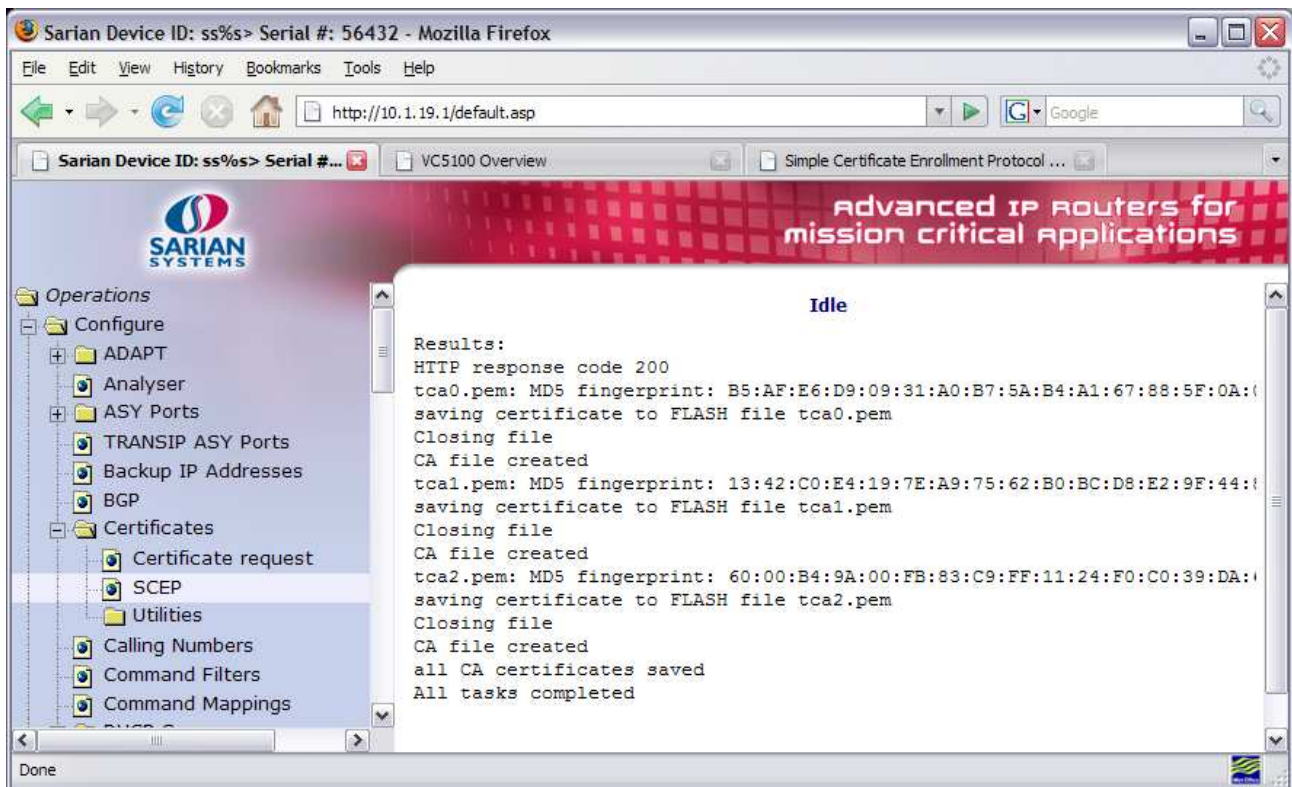
The fingerprint of each certificate is displayed. This fingerprint of the CA certificate should be checked (using some out of band mechanism) against the fingerprint of the CA certificates as advertised by the server. For the Microsoft® server the CA certificate fingerprint is displayed when the page http://<host>/certsrv/mscep/mscep.dll' is accessed.

If the fingerprints do not match, it probably means that you have some attacker sitting between the unit and the server.

Rename the CA certificates

The name of each CA certificate needs to be prefixed with 'ca' and not 'tca' as configured earlier. The reason that the prefix 'ca' was not specified when retrieving the CA certificates from the server is because this prefix has special meaning to Sarian routers and should not be use out of context.

For example one of your CA certificates will be named **tca0.pem** this will be renamed to **ca0.pem**.

On your PC, open a telnet session to the Sarian router.

START→RUN (Windows XP)

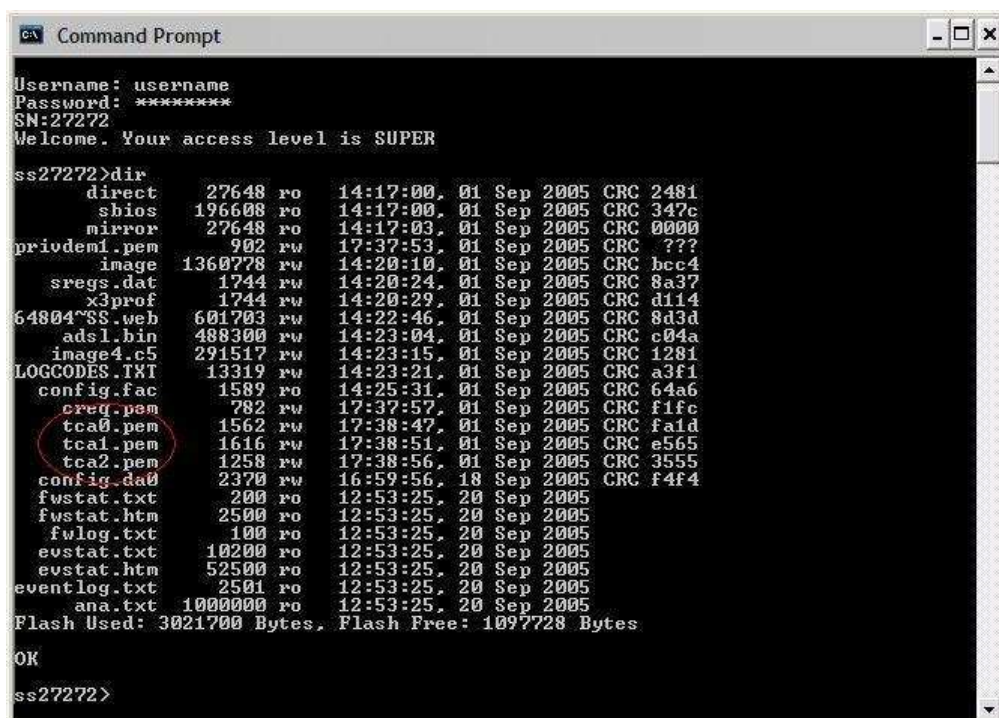In the command window type **cmd** then click **OK**.

A windows Command prompt will open. Type telnet <sarian ip_address>.

E.g. **telnet 172.16.0.254**<enter>

A login prompt will appear in the Command prompt window. Login with your usual Sarian username and password.

Enter **dir**<enter> to view the Sarian's file directory. You should see the CA certificates prefixed with 'tca'

To rename the CA certificates type the following commands and press the enter key after each line.
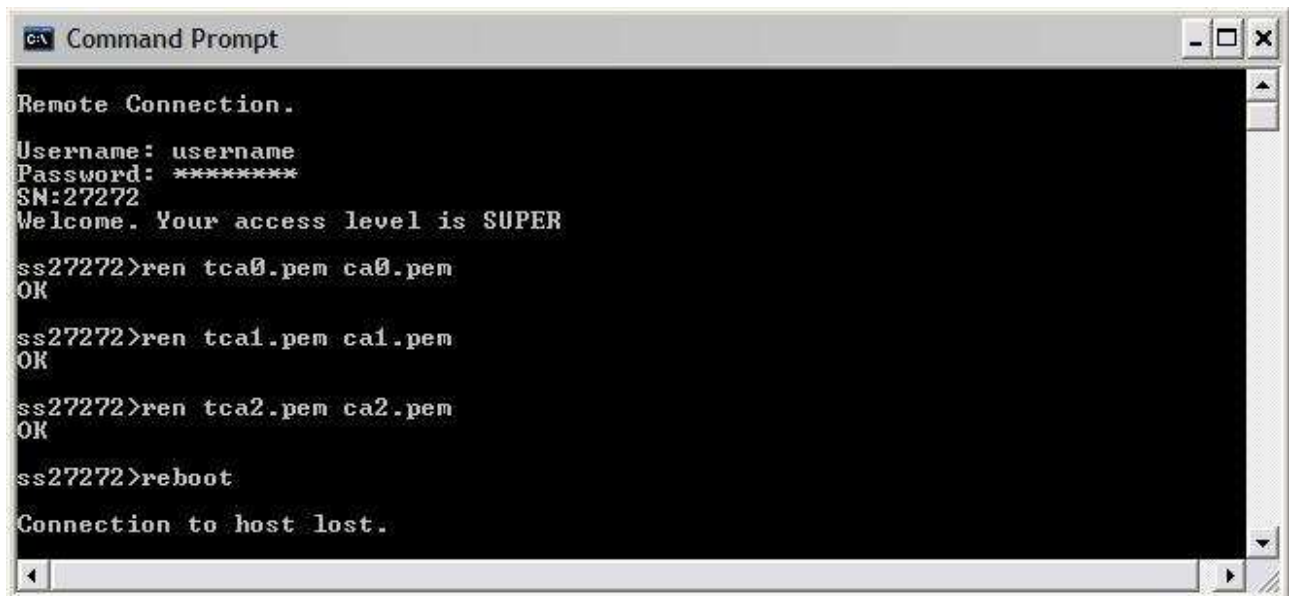
ren tca0.pem ca0.pem<enter>

ren tca1.pem ca1.pem<enter>

ren tca2.pem ca2.pem<enter>

For the changes to apply you must reboot the unit.

reboot<enter>

Once the Sarian has rebooted you can open another telnet session and issue the **dir** command to see the CA certificates with the new file names.

4.5 Using SCEP to Enrol the Certificate Request

The next process is to send the certificate request to the CA server for signing. This will be the router's 'public key'.

Now the router is in possession of all the required certificates, the SCEP configuration page can be completed in order to enrol the certificate request.

Browse to **CONFIGURE → CERTIFICATES → SCEP**.

Parameter	Setting	Description
Host:	Ca server ip address	Ca server ip address
Remote port:	0	MS SCEP uses HTTP to carry the requests, If this parameter is non-zero, the unit will use this value as the destination port rather than the default of 80
Path:	certsrv/mscep/mscep.dll	Select Microsoft SCEP from drop down list and the path will be entered automatically
Application:	pkiclient.exe	This represents the SCEP application on the server
CA Identifier:	ACP	CA identifier
Private Key filename :	privdem1.pem	The name of the private key created earlier
Certificate request filename:	creq.pem	The name of the certificate request created earlier
Certificate filename:	certdem1.pem	Enter a name for the public key certificate (must be prefixed with 'cert')
CA certificate filename:	ca2.pem	Enter the name of the CA certificate.
CA encryption certificate filename:	ca1.pem	Enter the name of the CA encryption certificate.
CA signature certificate filename:	ca0.pem	Enter The name of the CA signature certificate

Identifying the CA certificates

To complete the previous task you would normally need to determine which certificate is used for what task. For the purpose of this application note these have already been determined but for future reference the following information will be useful

If only one CA certificate is returned, it is a trivial task. When three are returned, you need to display the certificates using the 'view' button having selected a CA certificate from the drop down list and investigate the attributes of the certificate.

Identifying the CA certificate:

This certificate will have matching Issuer and Subject fields. It may have a V3 extension which shows something like…

```
X509v3 Basic Constraints: critical
            CA: TRUE
```

Identifying the encryption certificate:

This certificate will have an Issuer which matches the CA certificate. It will probably have a V3 extension something like…

```
X509v3 Key Usage: critical
            Key Encipherment, Data Encipherment
```

Identifying the signature certificate:

This certificate will have an Issuer which matches the CA certificate. It will probably have a V3 extension something like…

```
X509v3 Key Usage: critical
            Digital Signature, Non Repudiation
```
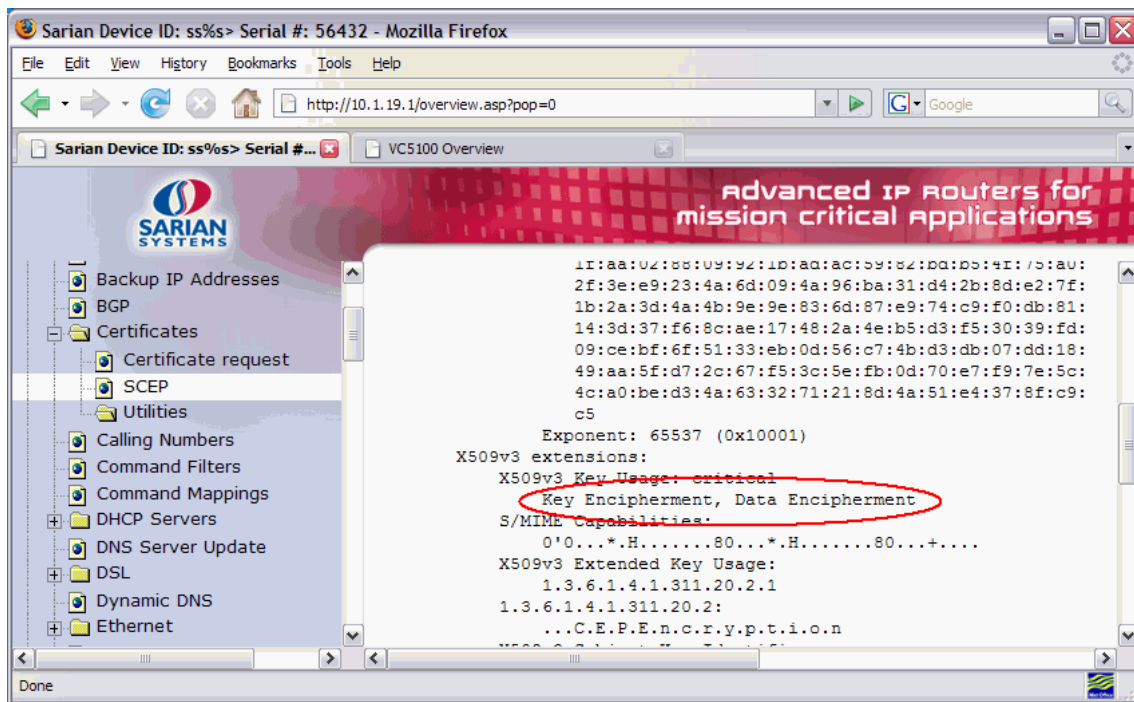
Here is an example screen shot of the same page after clicking a 'view' button to determine which of the CA certificates is the encryption certificate.

Signing the certificate request

Once the SCEP configuration page has been completed click the **Enroll Certificate Request** button.

You should receive one of three responses.

Failure - The request failed. Check that the correct CA certificates have been used. Check that the challenge password is correct. Check that the correct certificate request has been specified, and that the correct private key has been used. Check the server logs to see what the problem is.

Pending - The server has our request, but hasn't signed it yet. It may require some input by the System Administrator. The unit should poll the server occasionally until the certificate is returned. However, if you know that the certificate request has been allowed having contacted the System Administrator you can simply the **Enroll Certificate Request** button again rather than wait for the Sarian to re-poll.

Success - The response should contain the signed certificate.

In this example the CA Server has returned a **Success** message because automatic enrolment has been enabled on the CA server
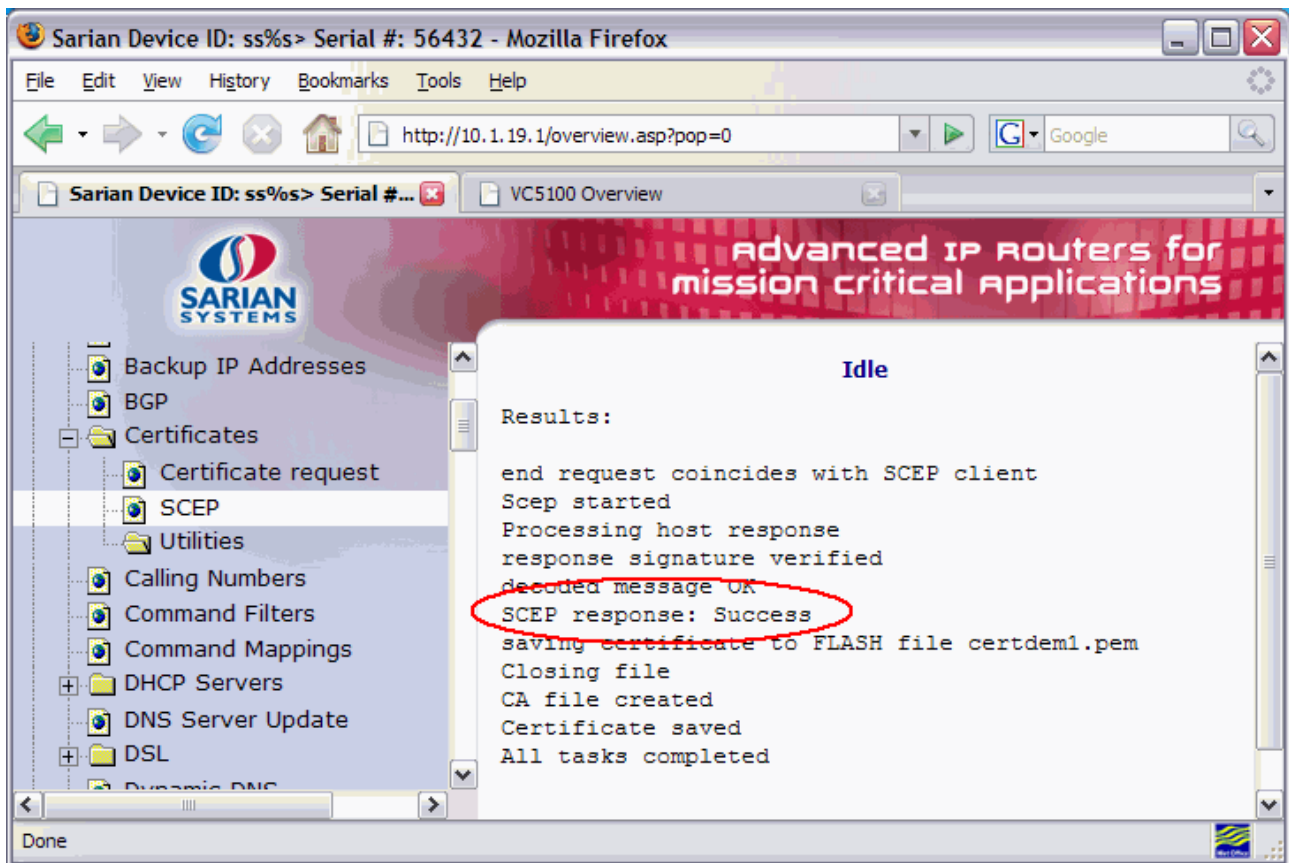
5.0 ENABLING HTTPS WEB MODE

5.1 Configure the router's SSL server.

CONFIGURE → SSL SERVER
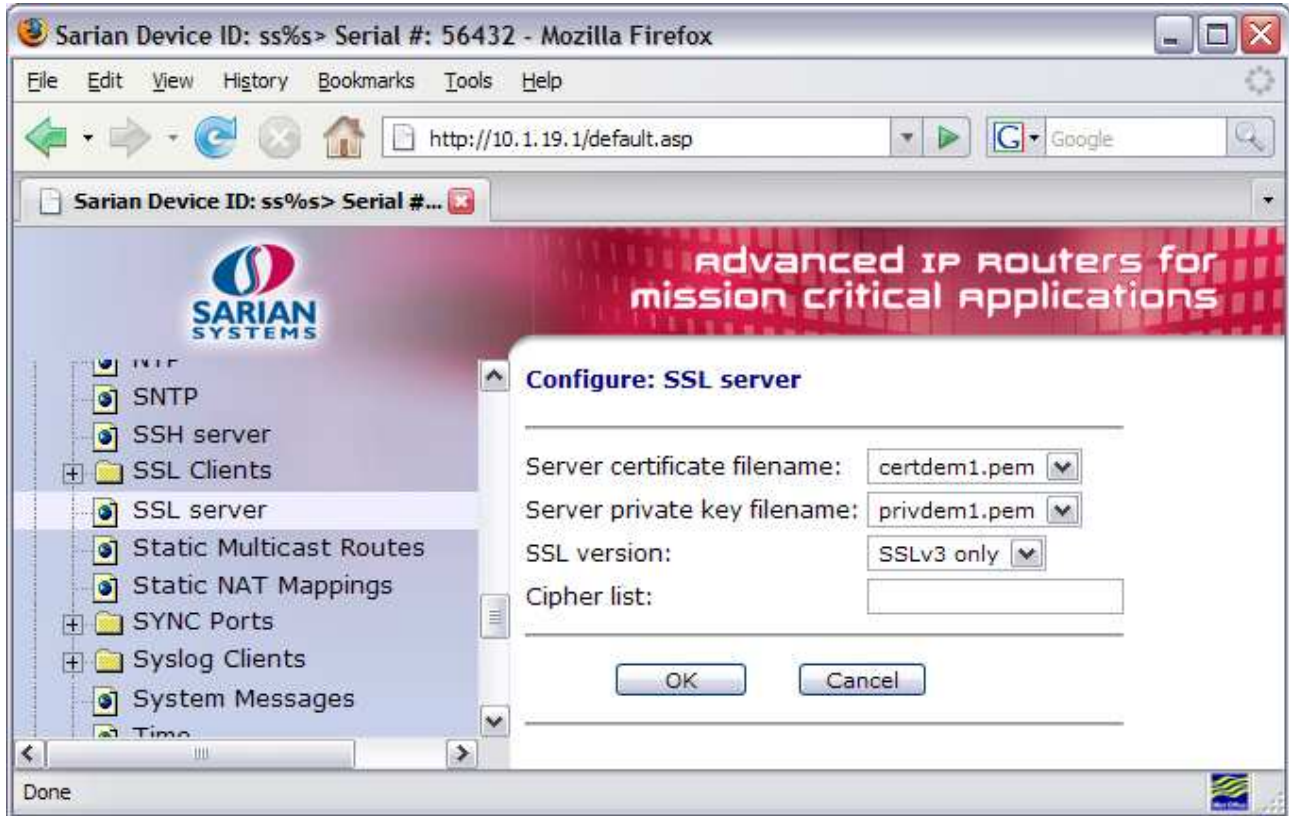
Parameter	Setting	Description
Server certificate filename:	certdem1.pem	Choose your signed certificate from the drop-down list.
Server private key filename:	privdem1.pem	Choose your private key file from the drop-down list.
SSL version	SSLv3 only	Select the version of SSL you want to use. Some browsers support different versions to others.

5.2 Enabling HTTPS web server mode

To force the Sarian's web browser to use HTTPS browse to **CONFIGURE → GP TCP SOCKETS**
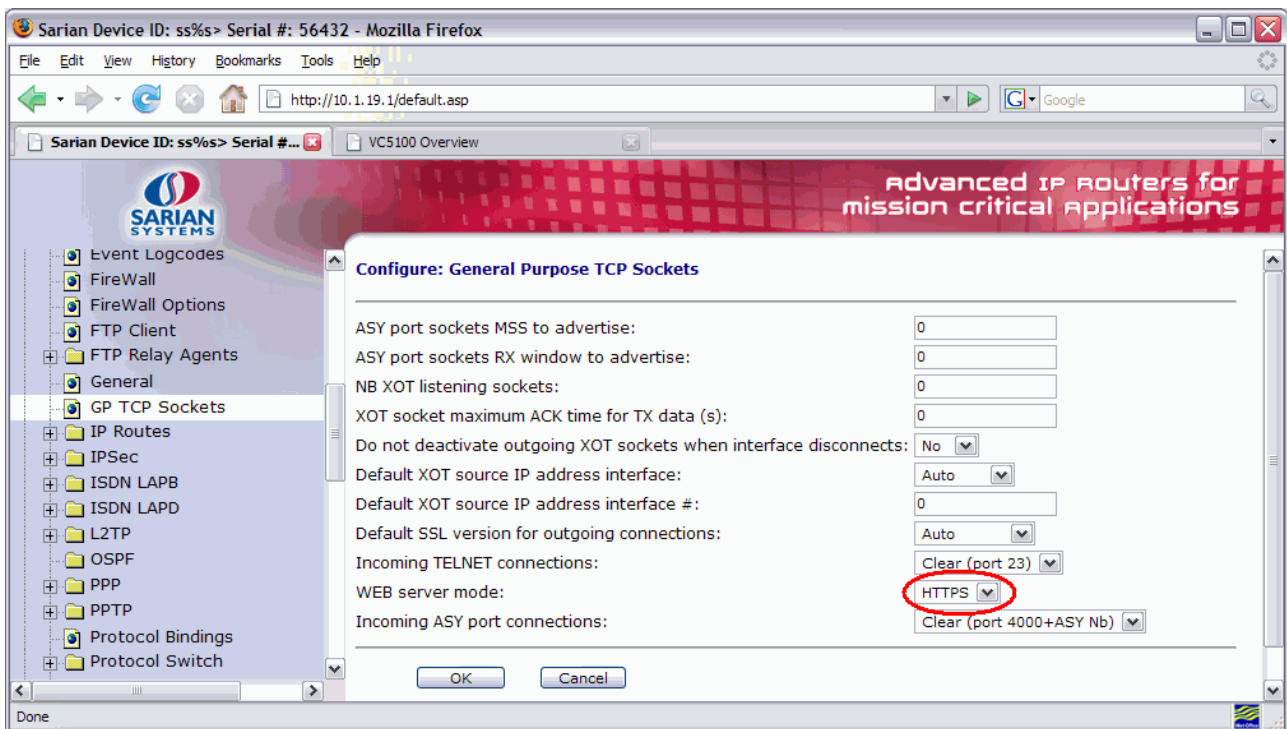
Parameter	Setting	Description
WEB server mode:	HTTPS	Select HTTPS for the web server mode.

5.3 Connecting to the router with HTTPS

Once you have selected HTTPS web server mode you will be disconnected from the router. Replace the http://<IP_address> with https://<IP_address> and reconnect. Your browser may present a warning that the website you are connecting has an unknown certificate and ask you if you wish to carry on. Accept the certificate and carry on.

Once connected to the Sarian's web page with HTTPS you will most likely see some sort of indication (usually a padlock icon) that you are connected to a secure site. Some browsers may differ.
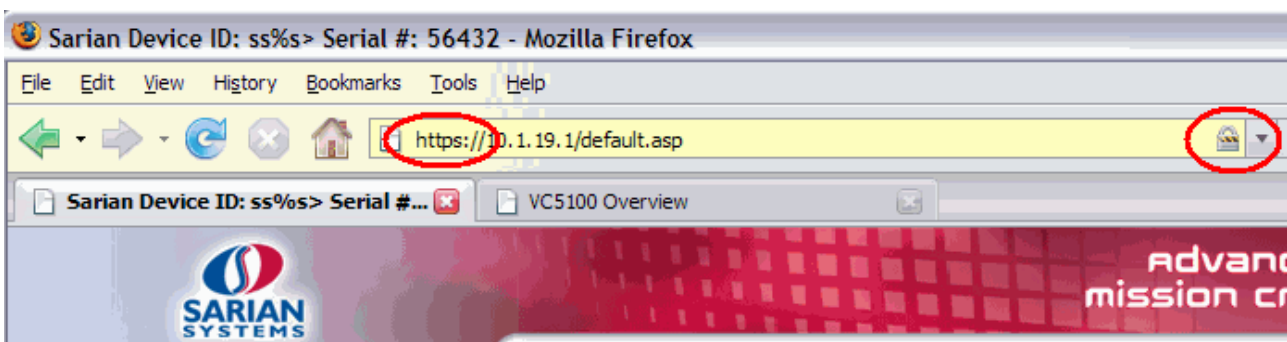
5.4 Sarian Configuration File Used For This Technical Note.

Please use the following style for any command line configuration examples and event logs or anything else that needs fixed width font:

```
eth 0 IPaddr "10.1.19.1"
eth 0 mask "255.255.0.0"
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 2 dtemode 2
x25sw 0 swfrxot 1
x25sw 0 swfrlapd 2
x25sw 0 swfrlapb0 1
x25sw 0 swfrlapb1 1
tpad 0 tl2deact 1
tpad 0 l2iface "LAPB"
tpad 0 bakl2iface "None"
tpad 1 tl2deact 1
tpad 1 l2iface "LAPB"
tpad 1 bakl2iface "None"
tpad 2 tl2deact 1
tpad 2 l2iface "LAPB"
tpad 2 bakl2iface "None"
tpad 3 tl2deact 1
tpad 3 l2iface "LAPB"
tpad 3 bakl2iface "None"
def_route 0 ll_ent "PPP"
def_route 0 ll_add 1
def_route 1 ll_ent "PPP"
def_route 1 ll_add 2
def_route 2 ll_ent "PPP"
def_route 2 ll_add 3
sockopt 0 https ON
ppp 0 timeout 300
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 do_nat 2
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 1 l1iface "AAL"
ppp 2 l_pap OFF
ppp 2 l_chap OFF
ppp 2 l_addr ON
ppp 2 r_chap ON
ppp 2 r_addr OFF
ppp 2 l1iface "Default"
ana 0 anon ON
ana 0 l1on ON
ana 0 asyon 15
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "ss.2000r"
cmd 0 tremto 120
user 0 name "Sarian"
user 0 epassword "DhwjCxUc"
user 0 access 0
user 1 name "username"
```

```
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 epassword "A==="
user 2 access 0
user 3 epassword "A==="
user 3 access 0
user 4 epassword "A==="
user 4 access 0
user 5 epassword "A==="
user 5 access 0
user 6 epassword "A==="
user 6 access 0
user 7 epassword "A==="
user 7 access 0
user 8 epassword "A==="
user 8 access 0
user 9 epassword "A==="
user 9 access 0
local 0 transaccess 2
sslsvr 0 certfile "certdem1.pem"
sslsvr 0 keyfile "privdem1.pem"
sslsvr 0 ver "SSL3"
creq 0 challenge_pwd "068AC83B28B97E9F"
creq 0 country "UK"
creq 0 commonname "sn56432"
creq 0 locality "Leeds"
creq 0 orgname "Sarian Systems"
creq 0 org_unit "Tech_support"
creq 0 state "Yorkshire"
creq 0 email "support@sarian.co.uk"
creq 0 digest "MD5"
scep 0 host "10.1.253.251"
scep 0 path "certsrv/mscep/mscep.dll"
scep 0 caident "ACP"
scep 0 keyfile "privdem1.pem"
scep 0 reqfile "creq.pem"
scep 0 certfile "certdem1.pem"
scep 0 cafile "ca2.pem"
scep 0 caencfile "ca1.pem"
scep 0 casigfile "ca0.pem"
```