



Unifying Information Security

Implementing TLS on the
CLEARSWIFT SECURE Email Gateway

Contents

1	Introduction	3
2	Understanding TLS	4
3	Clearswift's Application of TLS.....	5
3.1	Opportunistic TLS.....	5
3.2	Mandatory TLS.....	5
4	Getting Started	8
5	Creating a Certificate Signing Request	9
5.1	What is a CSR?	9
5.2	Creating a Private Key and CSR using OpenSSL.....	9
5.2.1	Generating the Private Key.....	10
5.2.2	Generating the CSR.....	11
6	Using your CSR to purchase a Signed Certificate.....	13
7	What to do when you Receive Your Signed Certificate	14
7.1	Importing the Signed Certificate and Private Key Pair.....	14
8	TLS Endpoints	16
8.1	Defining a TLS Endpoint	16
9	Troubleshooting	21
9.1	Increasing SMTP Logging to Check TLS Connection.....	21
10	Appendix A - Creating a Self Signed Certificate using Microsoft Windows	22
10.1	Certificate Request.....	22
10.2	Exporting the Public Certificate and Private Key.....	29
10.3	Exporting the Microsoft CA Certificate	36
10.4	Converting the Private Key from PFX to PEM Format	38
11	Appendix B - Creating a Self-Signed Certificate	40
11.1	Creating a Gateway Based Certificate Authority.....	40
11.1.1	Generating the CA Key and CA Certificate.....	40
11.1.2	Signing the Certificate with the Gateway CA	41

1 Introduction

Although email is an integral part of modern business, it still relies on insecure transport protocols that were designed before anyone could predict how important email would become. However, network administrators can find some security and privacy assurance in the Transport Layer Security (TLS) encryption and authentication protocol.

TLS is a variation of the tried-and-true Secure Sockets Layer (SSL) protocol that is used to protect Web traffic. Using TLS to encrypt communications between two email gateways has a number of security benefits:

- Each email server authenticates to the other, making it harder to send spoofed email.
- The traffic between the two servers is encrypted, protecting the email content from prying eyes while in transit.
- The encryption of the conversation between the two hosts makes it exceedingly difficult for an attacker to tamper with the email's contents.

2 Understanding TLS

TLS protects the connection from your gateway to the first destination gateway. If there are intermediate hops when email is forwarded from one gateway to another, the protection afforded by TLS is lost after the first hop. For example, TLS is a good choice for two businesses that communicate frequently as long as both gateways communicate directly.

3 Clearswift's Application of TLS

The Clearswift SECURE Email Gateway can establish criteria for Transport Layer Security (TLS) encryption of outbound and inbound connections based on the domain, server or IP address where messages are sent and received. TLS enables you to set up secure email communications between your Email Gateway and other TLS-enabled email servers.

TLS supports two levels of security:

1. Encryption of the communications channel.
2. Optionally, strong authentication of one or both of the TLS client and TLS server, using signed certificates, during a TLS conversation.

Note: In a TLS connection, the TLS client is the host server sending the message and the TLS server is the host server receiving the message.

The Clearswift SECURE Email Gateway supports TLS in two forms:

- Opportunistic TLS
- Mandatory TLS

3.1 Opportunistic TLS

When trying to deliver emails to a remote server the Gateway will check whether the server advertises a TLS capability. If the receiving server does support TLS and the handshake succeeds, the email will be delivered using an encrypted connection.

When an SMTP client connects to the Gateway, the Gateway will advertise that it supports TLS. This allows the SMTP client to initiate a TLS handshake if it wishes to. If the handshake takes place and is successful, then the SMTP client will deliver emails to the Gateway using an encrypted connection.

If the remote client or server does not support TLS, or if the TLS handshake fails, then the Gateway will establish an ESMTP in-the-clear connection with the remote client or server.

3.2 Mandatory TLS

In this form, the Clearswift Gateway mandates TLS if an IP address or host is configured as an endpoint.

The Gateway will attempt to establish a TLS connection that meets the requirements mandated by the endpoint configuration. If the remote SMTP client/server does not advertise TLS, the connection will not be established and no email will be exchanged with the remote SMTP client/server. If the remote

machine advertises TLS, but does not meet one of the requirements of the configured endpoints, no email will be exchanged with the remote machine.

The critical difference between Mandatory TLS and Opportunistic TLS, is that when using Mandatory TLS the Gateway will not fall back to transmitting in the clear if the remote client or server does not support TLS, or if the TLS handshake fails.

Example 1:

Company A has a Clearswift SECURE Email Gateway. Company A and Company B wants to send/receive TLS encrypted email with each other. Both Company A and Company B have certificates from trusted Root Certification Authorities* or have exchanged public keys and have uploaded them into their respective SMTP (TLS-enabled) servers. Company A's Email Gateway TLS configuration with Company B has a minimal encryption setting of 128-bits. Company B is running their TLS with 40-bits. Company A's Clearswift SECURE Email Gateway will not create a connection with Company B's endpoint and no email will be exchanged because it is Company A's policy to mandate a minimum of 128-bits.

Example 2:

Company A has a Clearswift SECURE Email Gateway. Company A wants to send secure, encrypted email to Company B using Mandatory TLS. Company A has configured Company B as an endpoint and Company A is advertising TLS. Company B is not advertising TLS. Company A will not create a connection with Company B and no mail will be exchanged. This is important to note because in an Opportunistic TLS exchange, if TLS is not advertised by the accepting SMTP server, email will be sent across an unencrypted connection. Using Mandatory TLS, if the endpoint is not running TLS, the Email Gateway will not establish a connection with that endpoint and no email will be exchanged.

If you are interested in further reading about TLS encryption, a complete description can be found in RFC 2246.

More information can be gathered from:

- <http://www.linuxjournal.com/article/4823> - a Linux journal article on Sendmail and TLS.
- http://httpd.apache.org/docs/2.0/ssl/ssl_intro.html - more technical but worth scanning.

* By default, the Certification Authorities certificate store is configured with a set of third-party CAs that meet the requirements of being a globally recognized trusted certificate authority.

To see the list of Trusted Certificate Authorities:

1. Click on the System tab.
2. Click on Encryption.
3. Click on Certificate Store.

The screenshot shows the 'Certificate Store' interface in the CLEAR SWIFT application. The top navigation bar includes 'Home', 'Policy', 'Messages', 'Reports', 'System', 'Health', and 'Users'. The 'System' tab is selected, and the 'Certificate Store' sub-tab is active. The interface displays a list of Certificate Authorities (CAs) under the 'Certificate Authorities' tab. The list includes columns for 'Type', 'Details', 'Email', and 'Expires'. The first few entries are:

Type	Details	Email	Expires
S/MIME	ABA.ECOM\, INC., ABA.ECOM Root CA	admin@digsigtrust.com	10 July 2009
S/MIME	ADMINISTRACION NACIONAL DE CORREOS, S...	correo_cert@correo.com.uy	09 March 2009
S/MIME	Asociacion Nacional del Notariado Mexicano\, A...		29 June 2009
S/MIME	Belgacom, MTM, Belgacom E-Trust Primary CA	info@e-trust.be	21 January 2010
S/MIME	C&W HKT SecureNet CA Class A		16 October 2009
S/MIME	C&W HKT SecureNet CA Class B		16 October 2009
S/MIME	C&W HKT SecureNet CA Root		16 October 2010
S/MIME	C&W HKT SecureNet CA SGC Root		16 October 2009
S/MIME	Certsign Certificadora Digital Ltda., Certsign A...		27 June 2018
S/MIME	Certsign Certificadora Digital Ltda., Certsign - ...		27 June 2018
S/MIME	Certsign Certificadora Digital Ltda., Certsign A...		10 July 2018
S/MIME	Certsign Certificadora Digital Ltda., Certsign - ...		27 June 2018
S/MIME	Certplus, Class 1 Primary CA		07 July 2020
S/MIME	Certplus, Class 2 Primary CA		07 July 2019
S/MIME	Certplus, Class 3P Primary CA		07 July 2019
S/MIME	Certplus, Class 3 Primary CA		07 July 2019
S/MIME	Certplus, Class 3TS Primary CA		07 July 2019
S/MIME	Clearswift Corporation, Internal Support, Clear...	ithelpdeskuktheale@mimes...	18 July 2011
S/MIME	Clearswift Corporation, Internal Support, Clear...	ithelpdeskuktheale@mimes...	18 July 2011
S/MIME	Clearswift Demo, Demo, DemoCA	info@clearswift.com	23 October 2018

4 Getting Started

There are a number of steps that you need to perform before configuring TLS on your Clearswift SECURE Email Gateway.

1. Make sure the organization on the other end of the connection is able and willing to set up TLS. If your Gateway is configured to use TLS, but the recipient's is not, no email will be exchanged.
2. Get a digital certificate to identify your Clearswift SECURE Email Gateway. While you can create your own self-signed certificate, using a certificate issued by a trusted organization (a Certificate Authority like VeriSign, Entrust, Thawte, etc.) will make it easier for email partners to trust your server's identity. Please note that the certificate that is installed by default on your Gateway, is signed by Clearswift's CA. This is not a globally trusted Certificate Authority (CA).
3. Educate your users to recognize the presence or absence of the email header that tells them an email came in over a TLS connection. The following is an example of the received header from a message sent via TLS:

```
Received: from mail.clearswift.com (mail.clearswift.com [192.168.1.1]) by  
mail.abc.com (8.12.9/8.12.9) with ESMTP id h0UGn9P7001230  
(version=TLSv1/SSLv3 cipher=EDHRS-A-DES-CBC3-SHA bits=168 verify=OK)  
for; Tue 30 Jan 2009 15:39:10 -0500.
```

The portion of the header in bold type indicates that the message came in with 168 bit DES encryption from a server that presented a valid certificate.

5 Creating a Certificate Signing Request

5.1 What is a CSR?

A CSR is essentially a Public Key containing specific information about your Email Gateway and organisation that is used to request a Certificate from your trusted CA (VeriSign, Entrust, Thawte, etc.).

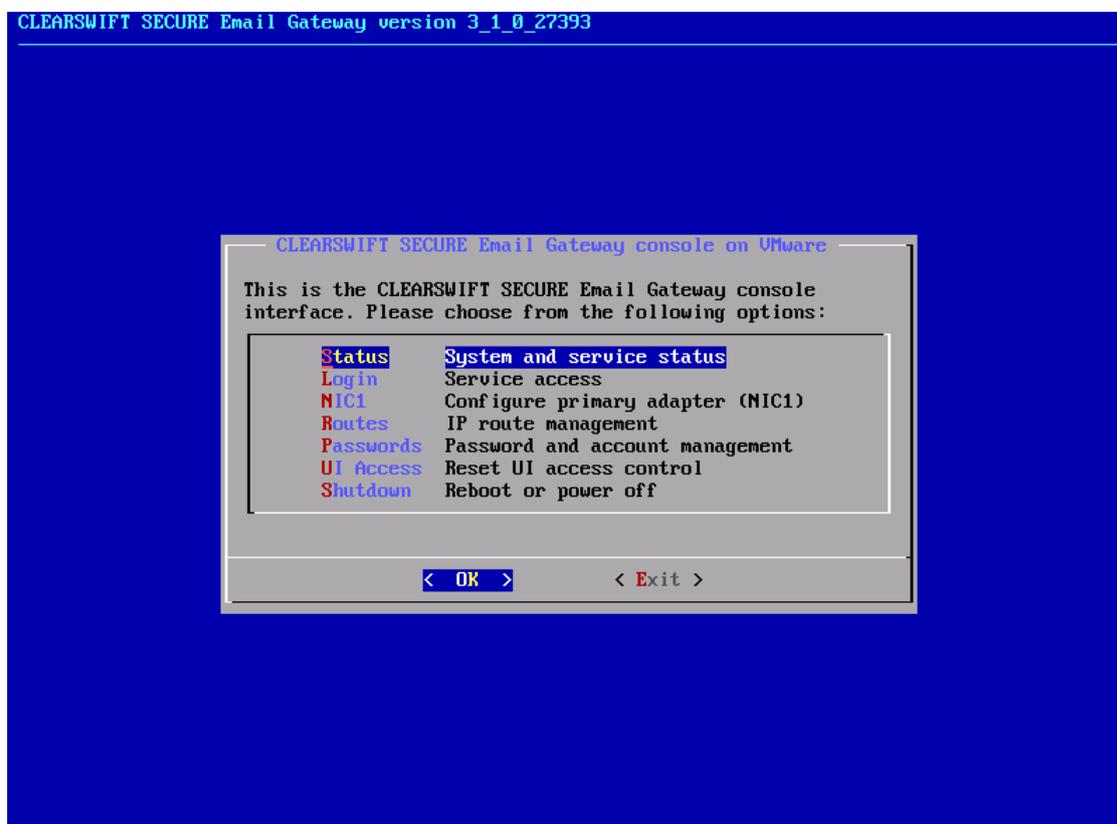
Before you can begin the process of obtaining a Certificate, you must generate a Private Key and CSR pair either from the Gateway command line or Microsoft Certificate Server. The CSR must be submitted to your Certificate Authority in order to obtain your signed certificate.

5.2 Creating a Private Key and CSR using OpenSSL

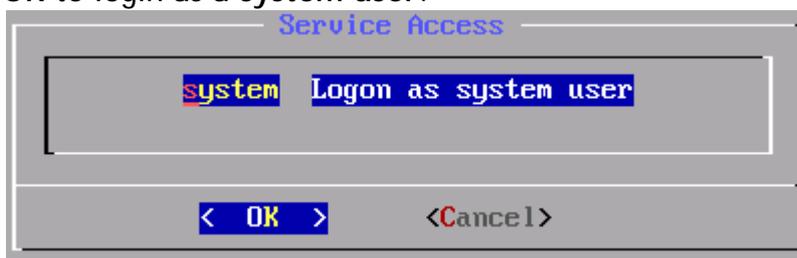
Log in to your Gateway via SSH or a KVM (keyboard/video) connection. When prompted, enter **console** for the username followed by the password you created during the initial Gateway set-up.

```
emailgateway01.examplecompany.org login: console
Password:
```

Then, choose **Login** from the Clearswift SECURE Email Gateway Console Menu.



Then, choose OK to login as a system user.



You will then be prompted for your password again.



Then, switch to root using the `sudo su -` command.

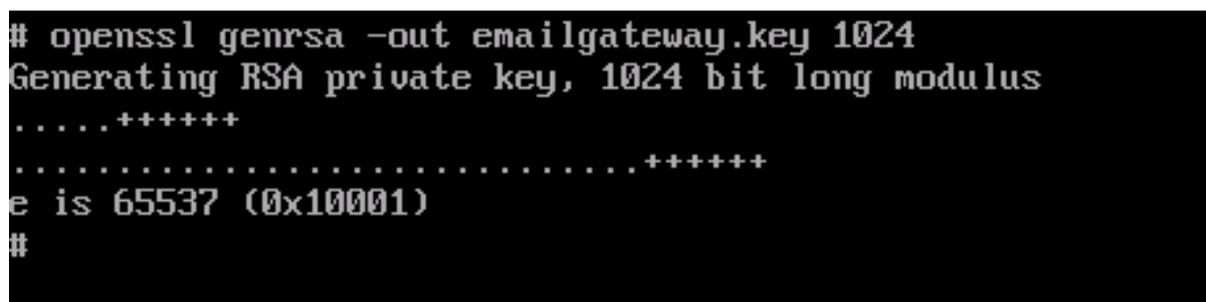


5.2.1 Generating the Private Key

The utility "openssl" is used to generate the private key and CSR.

Type the following command at the prompt:

`openssl genrsa -out emailgateway.key 1024`



This command generates a 1024 bit RSA private key and stores it in the file `emailgateway.key`. The key must be kept safe as it is used in conjunction with the signed certificate as detailed later in this document.

Note: You must protect the private key by storing it in a secure location. It is not currently possible to integrate the private key through the Gateway web interface if it is password protected. Clearswift recommends restricting access to the server so that only authorised server administrators can access or read the private key file. 1024 bit refers to the encryption strength of the private key itself preventing the contents from being read.

5.2.2 Generating the CSR

The following section provides details on creating a CSR on the Gateway which is the most commonly adopted approach. However, instructions are also available for creating the CSR on Microsoft Windows as detailed in Appendix A "*Creating a CSR using Microsoft Certificate Server*".

Type the following command at the prompt:

```
openssl req -new -key emailgateway.key -out emailgateway.csr
```

This command will prompt for the following X.509 attributes of the certificate:

```
# openssl req -new -key emailgateway.key -out emailgateway.csr
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 a 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) [AU]:GB
State or Province Name (full name) [Some-State]:Berks
Locality Name (eg, city) []:Theale
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Clearswift
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:emailgateway01.clearswift.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
# _
```

When filling out the above CSR, most Certificate Authorities will require the common name field to be populated with the full qualified domain name of the Gateway (registered DNS name). However some endpoints insist that the common name matches the MX record value. Therefore it is best to talk to your partner to understand what their specific requirements are.

The email address, challenge password or an optional company name are all optional parameters when generating the CSR.

A public/private key pair has now been created. The private key (emailgateway.key) is stored locally on the server machine and is used for decryption. The public portion, in the form of a Certificate Signing Request (emailgateway.csr), will be for certificate enrolment.

Below is a screenshot of the raw contents of the CSR in VI editor.

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIBOCCAQoCAQAwRjELMAkGA1UEBhMCVUMxCzAJBgNVBAGTAkNBMRUwEwYDUQQH  
EwxSZWR3b29kIENpdHkxEzARBgNVBAoTCkNsZWYyc3dpZnQwgZ8wDQYJKoZIhvcN  
AQEBBQADgY0AMIGJAoGBA0G4MUHtsLLwR4RLSrzb381K9bYW8gGIH9p4N/F8mVH2  
xKe4D7+q8IppoDnm72apKk1FGsr0sf nToC+33N3XW9F7gNUuy4RFnbEY1KmTidzz  
g7Lat0yxS7SGWIXVoh33pJcDbFFiaIUra0Md2tNWvHN7uT7SUsEk2qXtpQKDAWkp  
AgMBAAGgGzAZBgkqhkiG9w0BCQIxDBMKQ2x1YXJzd2lmdDANBgkqhkiG9w0BAQQF  
AAOBgQC3oYUO+APEw1FfKdf/U8CwE7JLzNCne8vX1uEzrxhbnBCT536+SCN+rChE  
d8Mu0BmUQeTo5S011SWe0bxHayw7h/kRIDB5/7FPoMpFEHyhI1+hIkIs1yTGpczq  
D+h92KEmr/8CGM0YBf87uu0z9eJPsDfecYOEE8GbyegBaYM0LQ==  
-----END CERTIFICATE REQUEST-----
```

6 Using your CSR to purchase a Signed Certificate

In order to obtain your signed certificate for use within the Gateway, the CSR created in the previous section must be submitted to the chosen Certificate Authority. An example of a typical Certificate Authority SSL submission form is displayed below:

<p>1. Copy and paste your CSR into this box:</p>	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>
<p>2. Select the server software used to generate the CSR:</p>	<div style="border: 1px solid #ccc; padding: 2px;"> Apache-ModSSL ▼ </div>
<p>3. Select the validity period for your Certificate:</p>	<input checked="" type="radio"/> 90 days

Note: You should always consult your CA before purchasing your certificate to ensure it is suitable for SMTP TLS communication.

Paste the contents of the CSR in the first window. If the CSR was created on the Gateway using OpenSSL, Apache-ModSSL can generally be used (*consult your CA first*) as the server software option. Once submitted, the CA will usually send back instructions via email for downloading the signed certificate and Root certificate. Ensure you have the original private key that was used to create the CSR in preparation for the next step.

Note: It is also possible to create a self-signed certificate for testing purposes. Details of this procedure can be found in Appendix B "Creating a Self-Signed Certificate".

7 What to do when you Receive Your Signed Certificate

For the Clearswift SECURE Email Gateway to be able to use TLS it must be enabled within the web interface and the following items imported:

- The private key and signed certificate to use when acting as a TLS client.
- The private key and signed certificate to use when acting as a TLS server.
- The CA's root certificate.

7.1 Importing the Signed Certificate and Private Key Pair

1. Copy the root certificate, `emailgateway.crt` and `emailgateway.key` to the machine that is connected to the Gateway web user interface. Open the web interface and navigate to System, Encryption.

The screenshot shows the 'Encryption' page in the Clearswift web interface. The page title is 'Encryption' and it contains the following sections:

- Configuration**
 - Certificate Store**: Manage certificates and keys.
 - Mail Encryption Endpoints**: Define the encryption endpoints for messages that should be delivered securely.
 - Encryption/Decryption Defaults**: Define the default encryption and decryption options.
- TLS Management**
 - TLS Certificates & Private Keys**: Manage the certificates and keys used for TLS.
 - TLS Endpoints**: Manage the settings for each TLS end point.

A 'Help' sidebar is visible on the left with the following items:

- What would you like to do?
 - Ping a host
 - Traceroute to a host
 - Query DNS records
 - Test SMTP Connection
- Help
 - Gateway Help
 - About Encryption
 - What are these settings?

2. Click on **TLS Certificates & Private Keys** in the **TLS Management** section.
3. Ensure that **Use TLS Communications** is enabled by highlighting the section, clicking on **Click here to change these settings** and selecting the **Use TLS** where possible checkbox.

The screenshot shows the 'Use TLS Communications' settings page. The page title is 'Use TLS Communications' and it contains the following text:

Use TLS where possible. The precise use of TLS will depend on the TLS endpoints configured.

[Click here to change these settings](#)

4. Edit the Signing Certificate section and add the CA certificate by browsing to the folder where the root certificate was placed.

Signing Certificate

Select the PEM file to upload. For more information about PEM files and how to get create or acquire them, please see the online documentation.

Certificate :

5. Edit the Server Certificate and Private Key section and add both the certificate and key to the appropriate sections by browsing to the folder where you placed emailgateway.crt and emailgateway.key.

Server Certificate and Private Key [Click here to change these settings](#)

Select the PEM files to upload. For more information about PEM files and how to get create or acquire them, please see the online documentation.

Certificate :

Private Key :

6. Edit the Client Certificate and Private Key section and add both the certificate and key to the appropriate sections by browsing to the folder where you placed emailgateway.crt and emailgateway.key.

Client Certificate and Private Key

Select the PEM files to upload. For more information about PEM files and how to get create or acquire them, please see the online documentation.

Certificate :

Private Key :

7. Navigate back to **System, Encryption** and click on **Certificate Store** to open the CA store. Click **Import** and browse to **CA.crt** adding it to the store list.

Upload Certificate or Key

Select the file containing the certificate/key

or cut and paste the certificate/key into the box below

If the certificate/key needs a password enter it below

Confirm the password

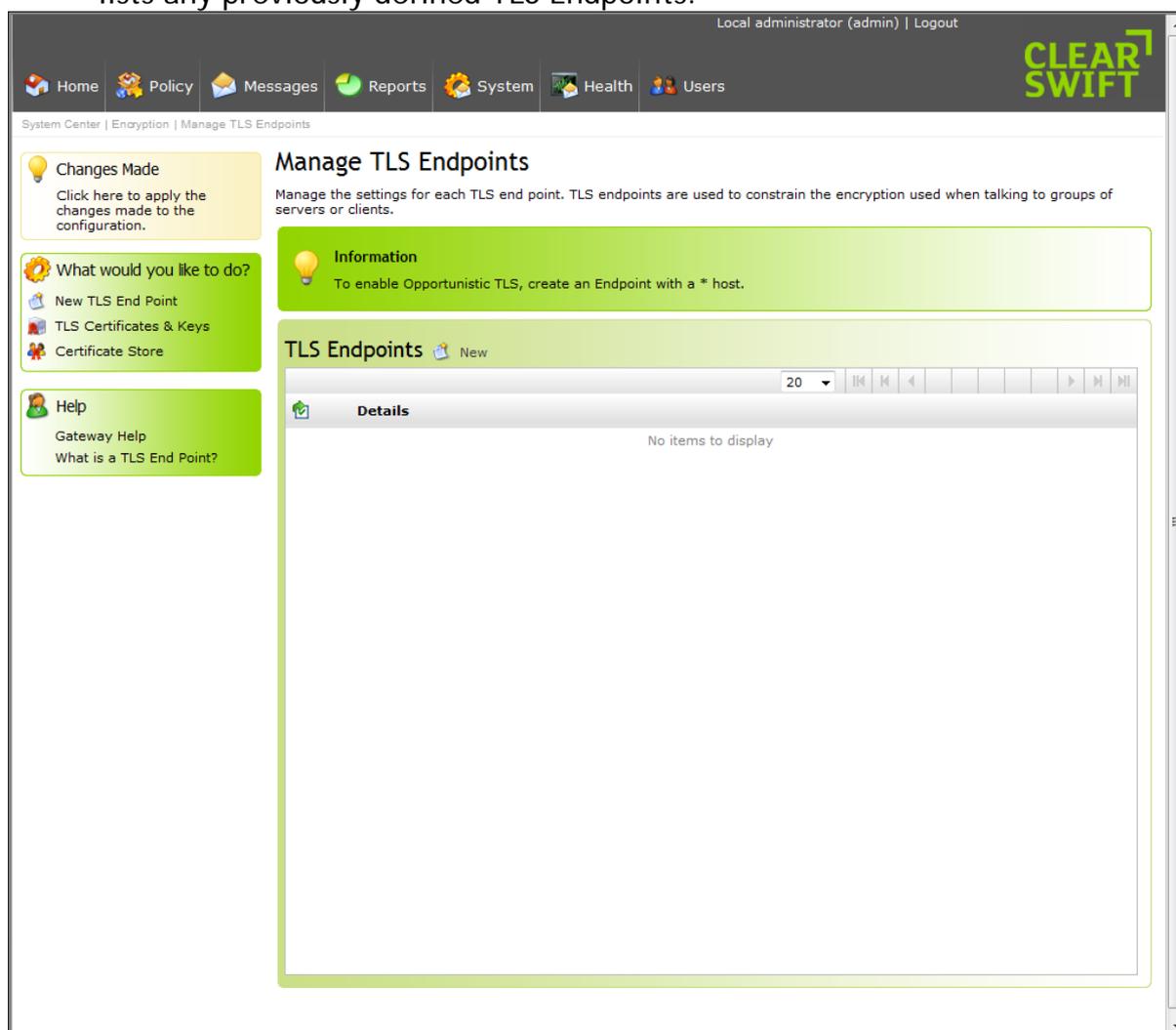
8 TLS Endpoints

A TLS Endpoint defines a profile of TLS settings for the Email Gateway to use when establishing a TLS connection with a third party. The TLS Endpoint specifies:

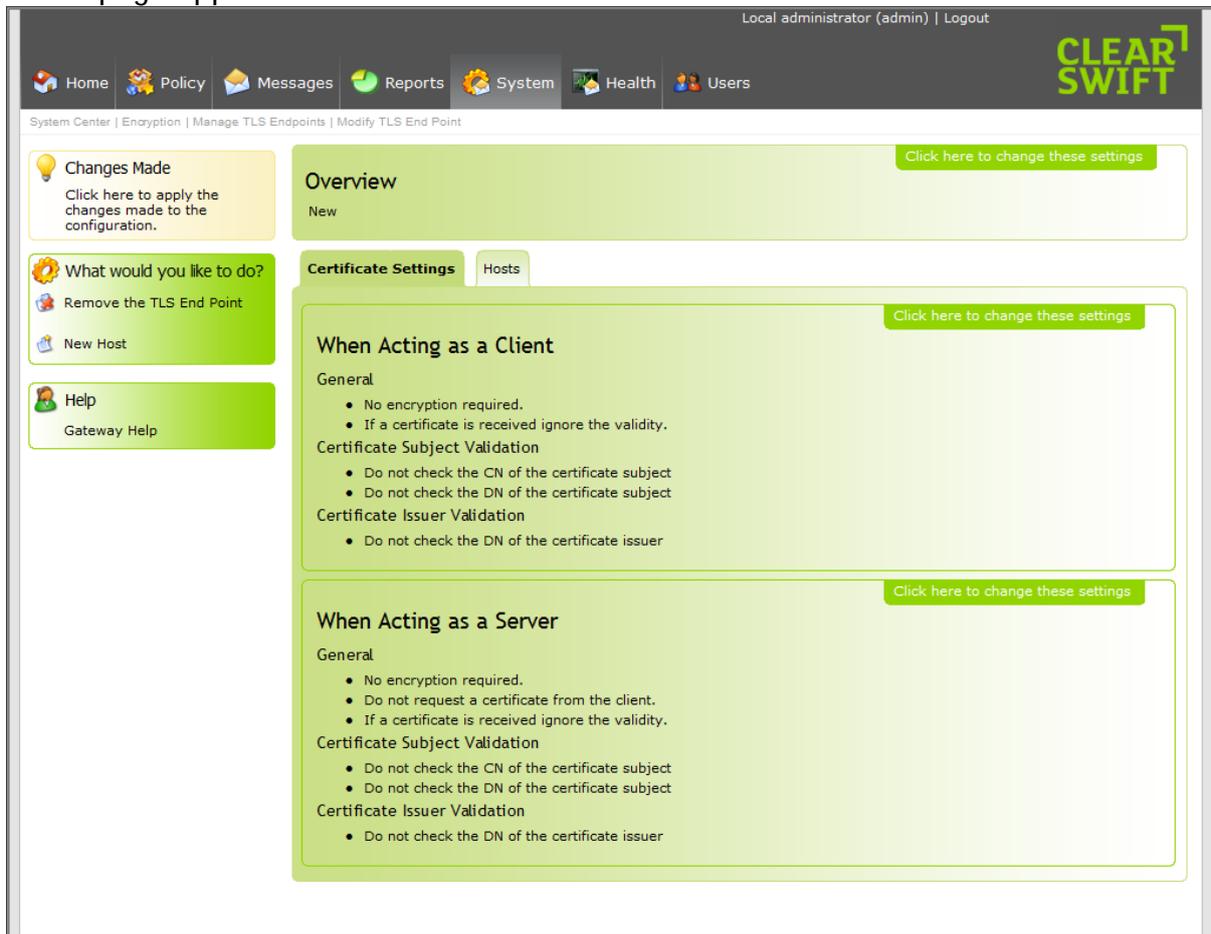
- One or more email servers with which these TLS settings are to be used.
- Whether encryption is required, and the level to enforce (or mandate).
- Whether to request a certificate from TLS clients.
- Whether the certificate of connecting TLS clients and the server must validate successfully for the conversation to proceed.
- Whether to use Opportunistic TLS.

8.1 Defining a TLS Endpoint

1. From the **System** page, click **Encryption**.
2. Click **TLS Endpoints** to display the Manage TLS Endpoints page. The page lists any previously defined TLS Endpoints.

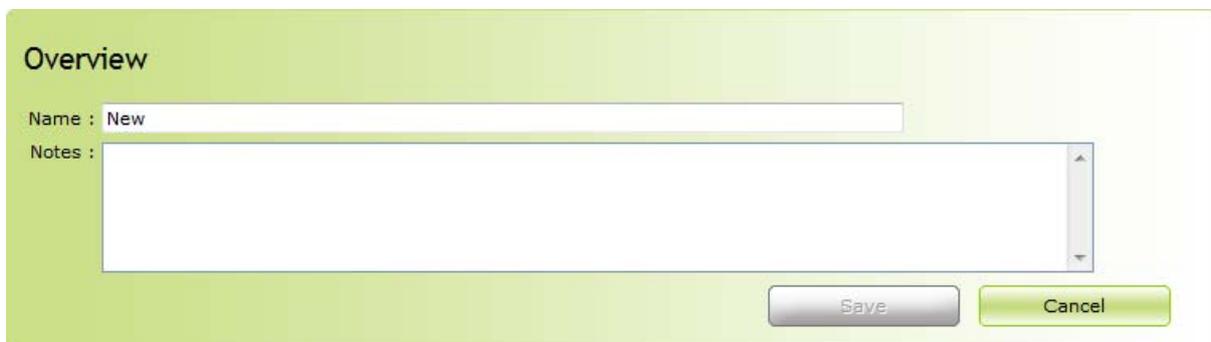


3. Click **New** adjacent to the **TLS Endpoints** heading. The **Modify TLS Endpoint** page appears.



4. Edit the **Overview** information as required:

- Move the pointer over the **Overview** area and click on **Click here to change these settings**.
- Edit the **Name** of the **TLS Endpoint**, to provide a meaningful name.
- Enter any **Notes** you want to add to describe the **TLS Endpoint**.
- Click **Save**.



5. Edit the settings to use when the Email Gateway is acting as a TLS server:
 - Move the pointer over the When Acting as a Server area and click on [Click here to change these settings](#).
 - To specify a minimum encryption level, select the **Encryption should meet or exceed** check box and enter the minimum number of bits to encrypt with. Choose a value in the range 40 to 256 bits.
 - Indicate whether you want to request a certificate from the TLS client. This option is for compatibility with some older mail servers where the TLS client does not automatically provide its certificate.
 - Indicate whether, for the conversation to proceed, the TLS client's certificate must validate successfully. A successful validation requires, among other things, a valid CA signing certificate in the Certificate Store.
 - To validate the CN of the certificate subject, select the **CN of the certificate must match** checkbox and enter the CN that the certificate subject must match.
 - If you select this option but do not specify a CN, the host name of the remote TLS host is used by default.
 - To validate the DN of the certificate subject, select the **DN of the certificate must match** checkbox and enter the DN that the certificate subject must match.
 - To validate the DN of the certificate issuer, select the **DN of the certificate issuer must match** checkbox and enter the DN that the certificate issuer must match.
 - Click **Save**.

When Acting as a Server

General

Encryption should meet or exceed : bits

Request a certificate from the client.

If a certificate is received it must validate.

Certificate Subject Validation

(Leave blank to indicate the hostname of the client)

CN of the certificate must match :

DN of the certificate must match :

Certificate Issuer Validation

DN of the certificate issuer must match :

6. Edit the settings to use when Email Gateway is acting as a TLS client:
 - Move the pointer over the When the Gateway is Acting as a Client area and click on **Click here to change these settings**.
 - To specify a minimum encryption level, select the **Encryption should meet or exceed** check box and enter the minimum number of bits to encrypt with. Choose a value in the range 40 to 256 bits.
 - Indicate whether for the conversation to proceed the TLS server's certificate must validate successfully. A successful validation requires, among other things, a valid CA signing certificate in the Certificate Store.
 - To validate the CN of the certificate subject, select **CN of the certificate must match** and enter the CN that the certificate subject must match.
 - If you select this option but do not specify a CN, the host name of the remote TLS host is used by default.
 - To validate the DN of the certificate subject, select **DN of the certificate must match** and enter the DN that the certificate subject must match.
 - To validate the DN of the certificate issuer, select **DN of the certificate issuer must match** and enter the DN that the certificate issuer must match.
 - Click **Save**.

When Acting as a Client

General

Encryption should meet or exceed : bits

If a certificate is received it must validate.

Certificate Subject Validation

(Leave blank to indicate the hostname of the server)

CN of the certificate must match :

DN of the certificate must match :

Certificate Issuer Validation

DN of the certificate issuer must match :

7. Specify the host machines to which this endpoint specification applies:
 - Click on the **Hosts** tab.
 - Click on **New** at the top of the "Hosts" area. The Add a New Host dialog appears.
 - Specify the server or range of servers to which this TLS Endpoint applies. You can specify any of the following:
 - A full IP address
 - The initial octets of an IP address range, followed by an asterisk, such as *nnn.nnn.nnn.**
 - A fully qualified hostname such as *server1.a-differentcompany.com*
 - A domain name such as *a-differentcompany.com*
 - To configure Opportunistic TLS, simply enter *** in the Host field.
 - Note: When configuring an endpoint, if a reverse DNS check of the remote TLS client or server fails, only the IP address can be trusted. Therefore, it may be necessary to specify an endpoint using an IP address (particularly in customer test scenarios where test machine hostnames are often not published in DNS).



- Click **Add** to add the host to the Hosts table.
- Add additional IP addresses or hostnames, if required. However, if configuring Opportunistic TLS, do not add any additional entries to the Hosts table.
- Click **Close** to dismiss the New Host dialog.
- Remember to apply your configuration.

9 Troubleshooting

9.1 Increasing SMTP Logging to Check TLS Connection

To ensure that TLS connection is successfully established, it is necessary to increase the SMTP logging level to 15. To do this:

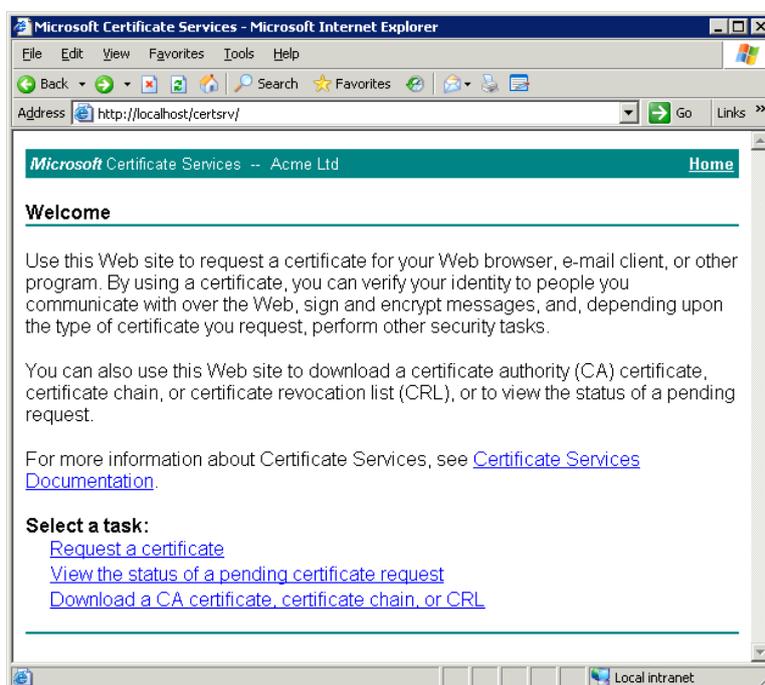
1. Navigate to **System, SMTP Settings, General Settings**.
2. In the Log Levels section, click on **Click here to change these settings** and increase the SMTP logging levels:
 - When receiving messages - 15
 - When sending messages - 15
3. Click on the **Save** button.
4. Apply the new configuration.
5. Finally, send and receive an email from the partner site you are testing and check the logs for TLS activity by navigating to **System, Logs & Alarms** and then select the **SMTP** log.

10 Appendix A - Creating a Self Signed Certificate using Microsoft Windows

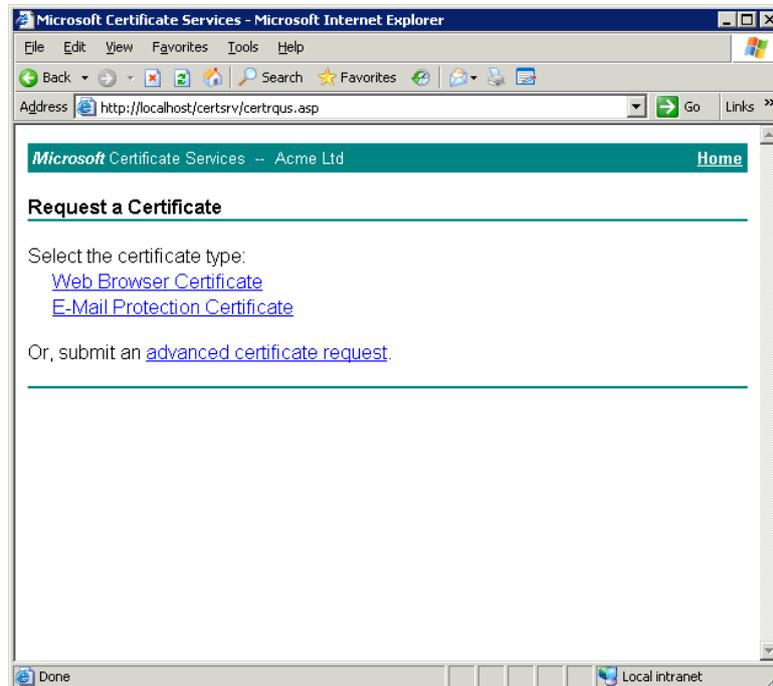
This section describes the process for generating a self signed certificate on a Microsoft Windows OS with Certificate Services installed. To generate the CSR, open the certificate server web page, i.e. <http://hostname/certsrv>.

10.1 Certificate Request

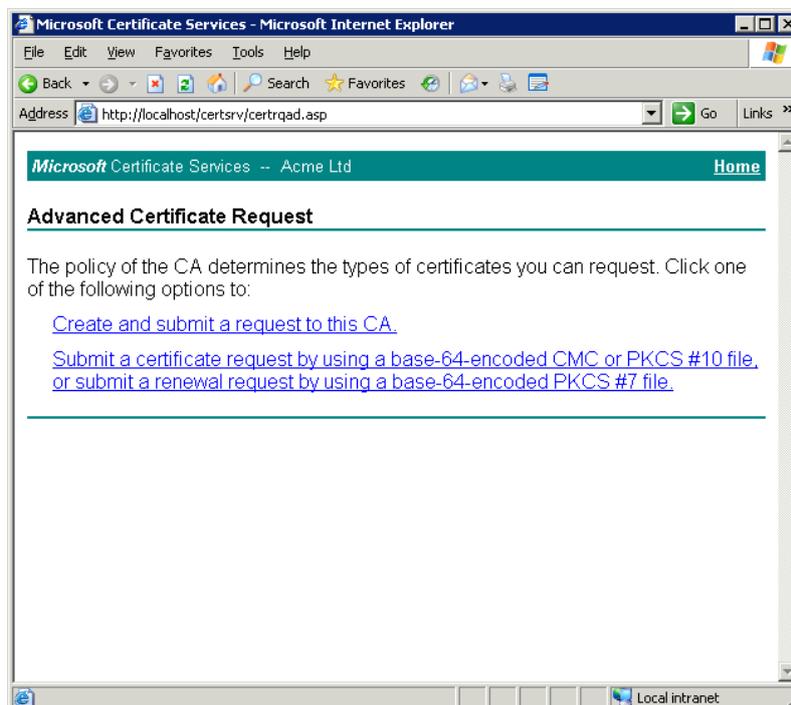
In order to request a new certificate, click on the Request a certificate link.



Select advanced certificate request from the list.



Then select Create and submit a request to this CA.



Complete the relevant fields using a similar format to that displayed and click Submit. Note: Ensure that Mark keys as exportable is checked.

Microsoft Certificate Services -- Acme Ltd
Home

Advanced Certificate Request

Identifying Information:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Type of Certificate Needed:

Key Options:

Create new key set Use existing key set

CSP:

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

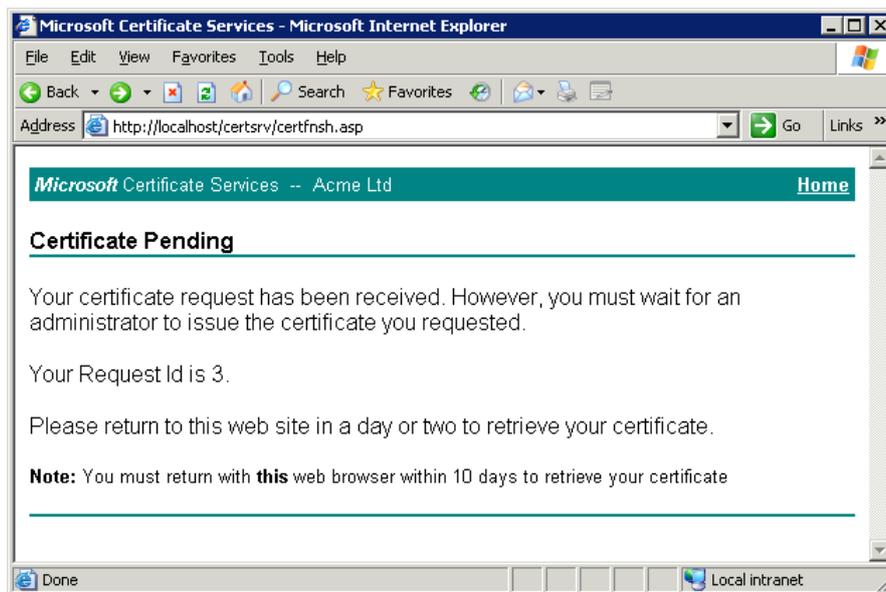
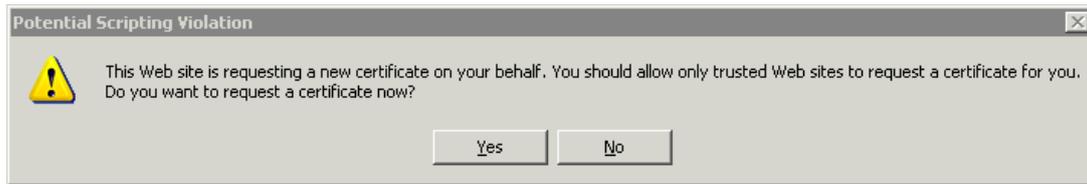
Hash Algorithm: Only used to sign request.

Save request to a file

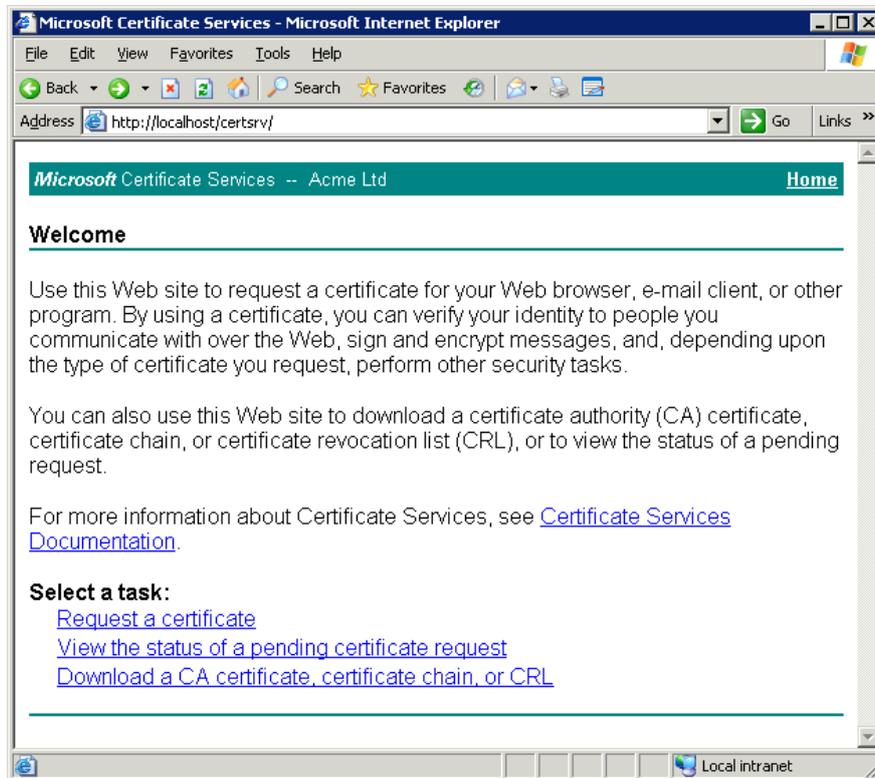
Attributes:

Friendly Name:

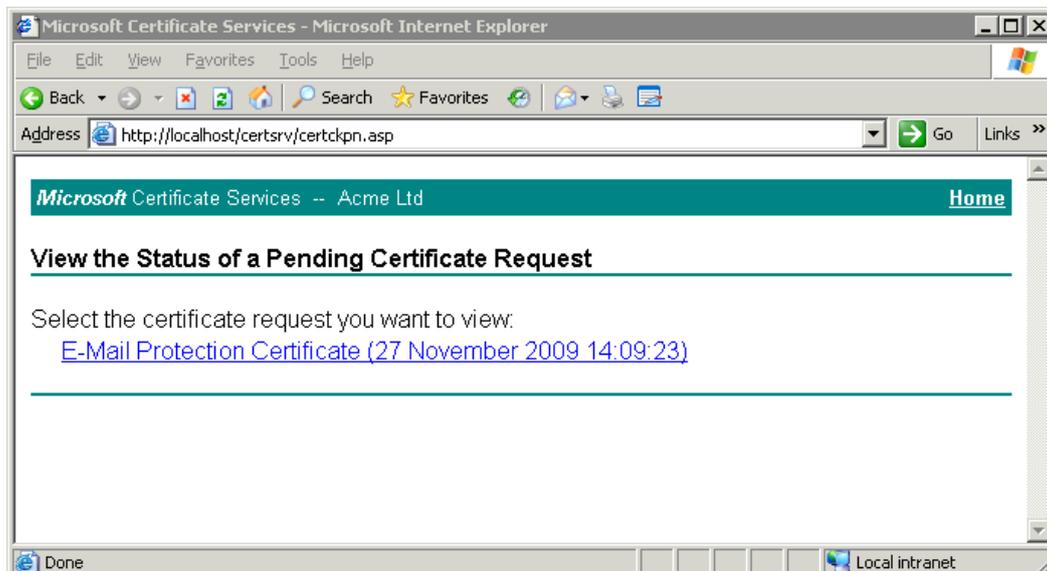
Select Yes to request the certificate.



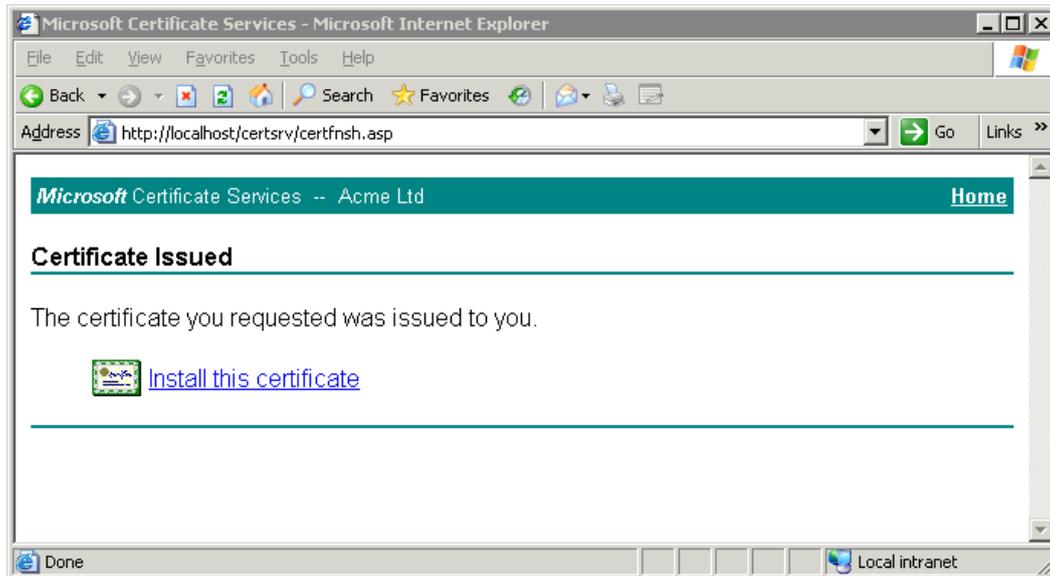
Once issued, return to the home page of the certificate services URL and select **View the status of a pending certificate request** to check if the certificate is available.



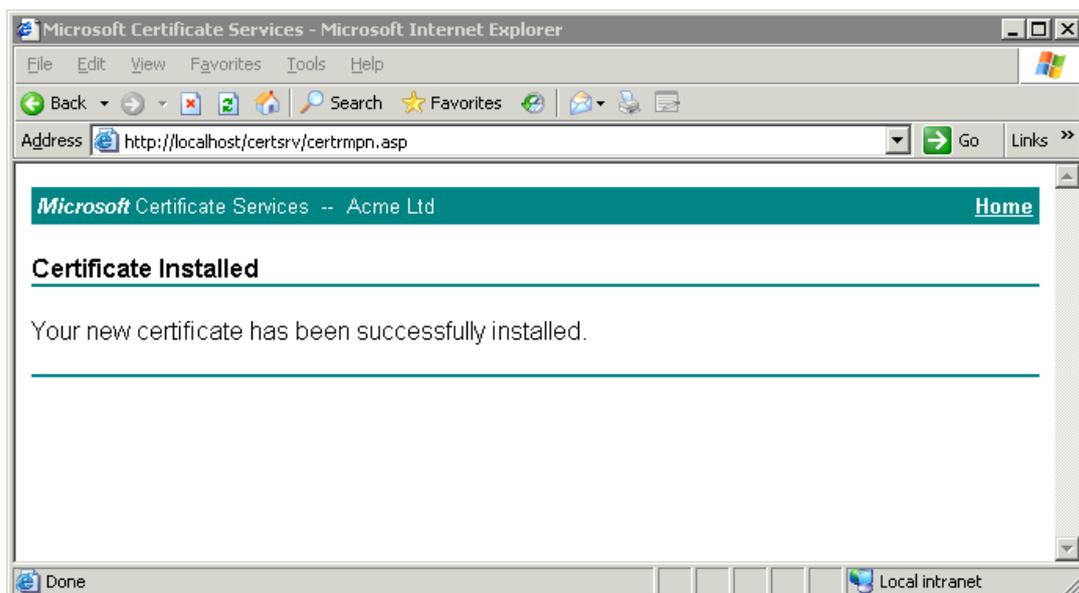
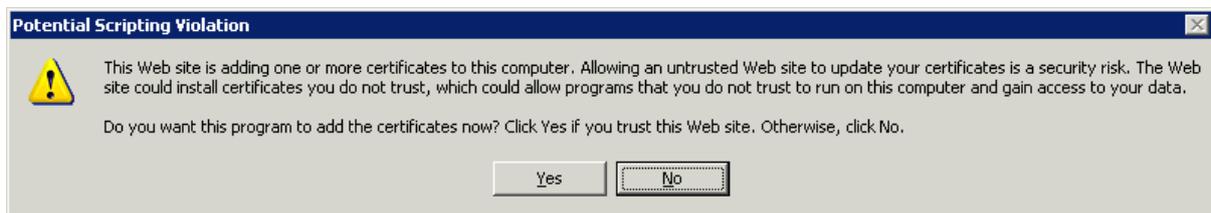
Click the link to view the certificate request.



Install the certificate by clicking the **Install this certificate** link.



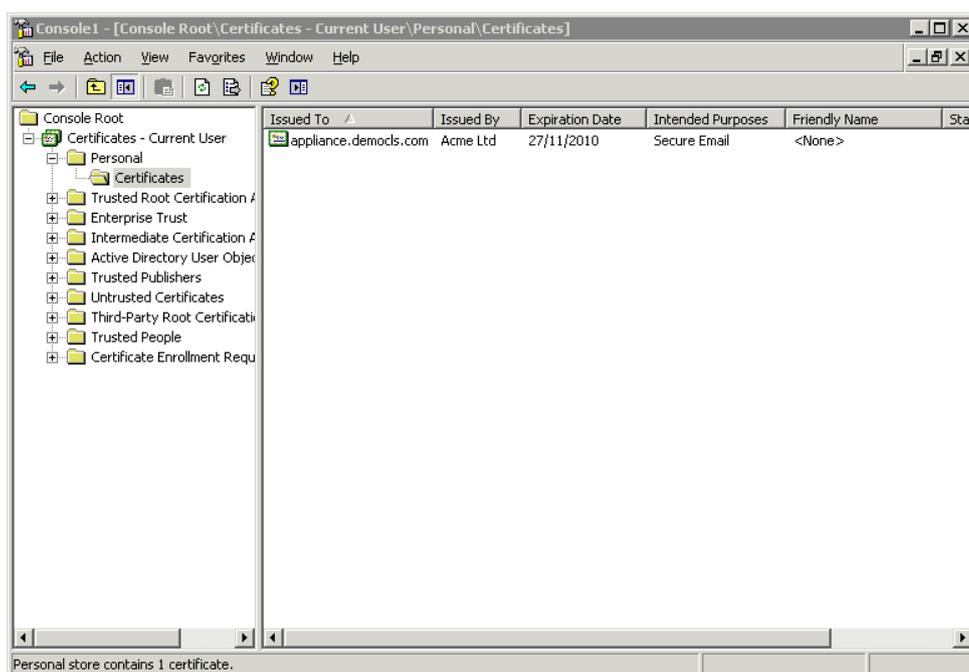
If prompted, select Yes to trust the certificate so that it can be added to the local certificate store.



10.2 Exporting the Public Certificate and Private Key

In the previous section, we were able to create a certificate request and install the issued certificate within the local certificate store. In order to import the certificate and private key into the Email Gateway, they must now be exported to Base 64 encoded X.509 files.

Open the local certificate store and locate the certificate that was installed from the previous section as shown in the following example.



The certificate is shown above on the right column. Right click the certificate and select **All Tasks, Export** to run the export wizard.

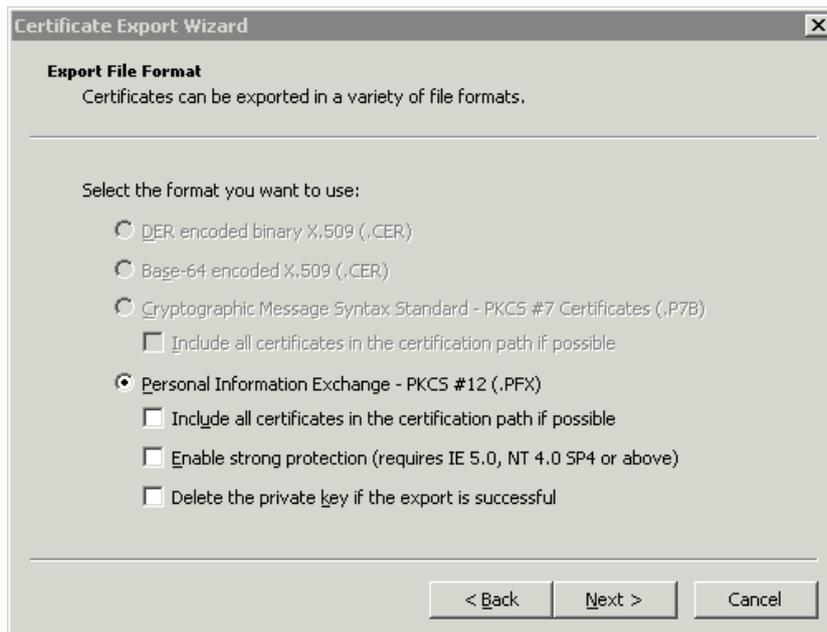
Click Next when the wizard opens.



Select the Yes, export the private key radio button below and then click Next.



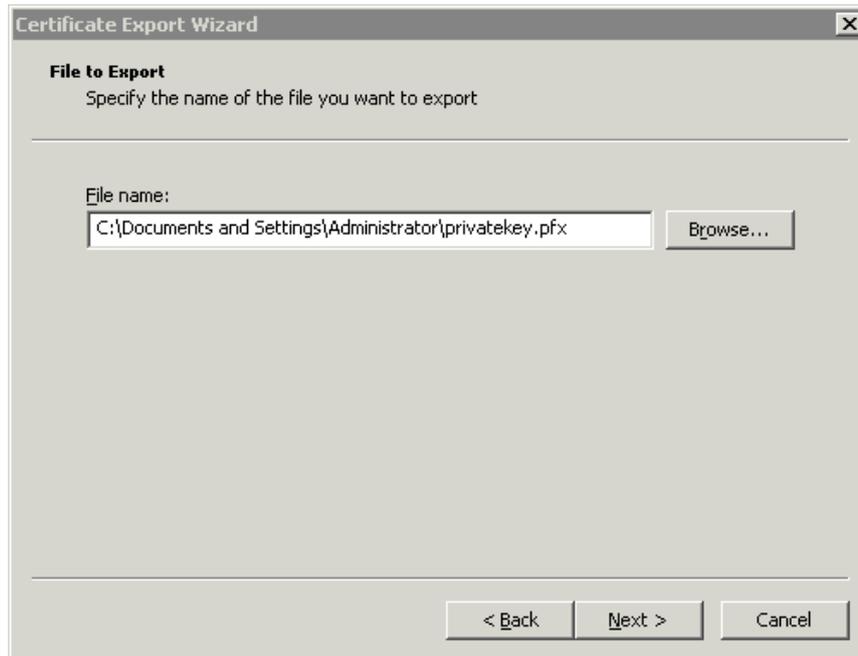
Ensure that all checkboxes are left unticked as depicted below and click Next.



Leave the password fields empty as the key needs to be imported into the Email Gateway without a password applied.



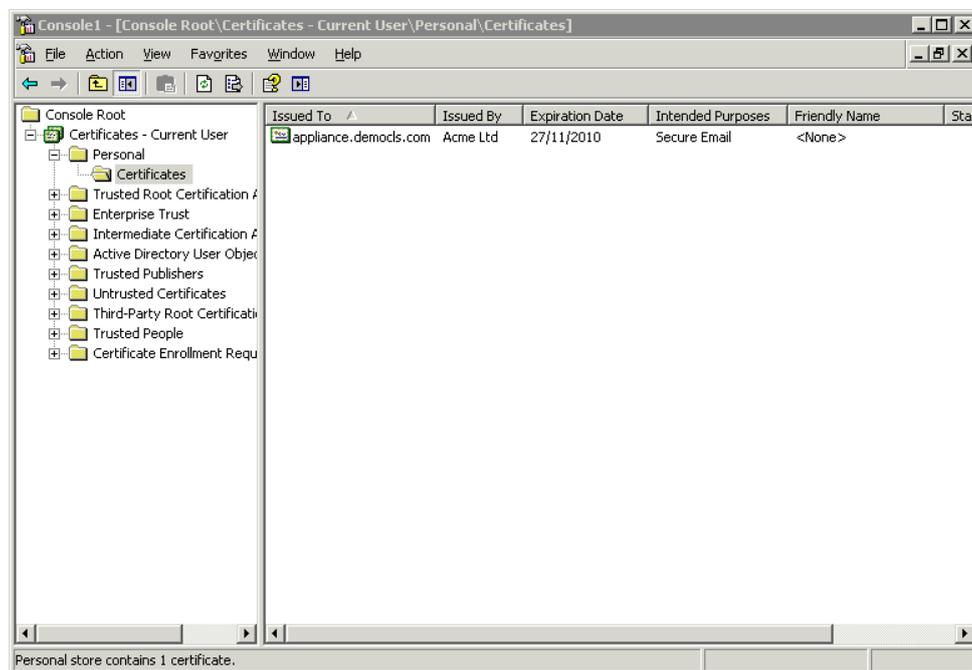
Select an appropriate name and location to store the exported key and click Next.



Click Finish to complete the process.



The final stage is to export the public certificate. Right click the certificate again and select **All Tasks, Export**.



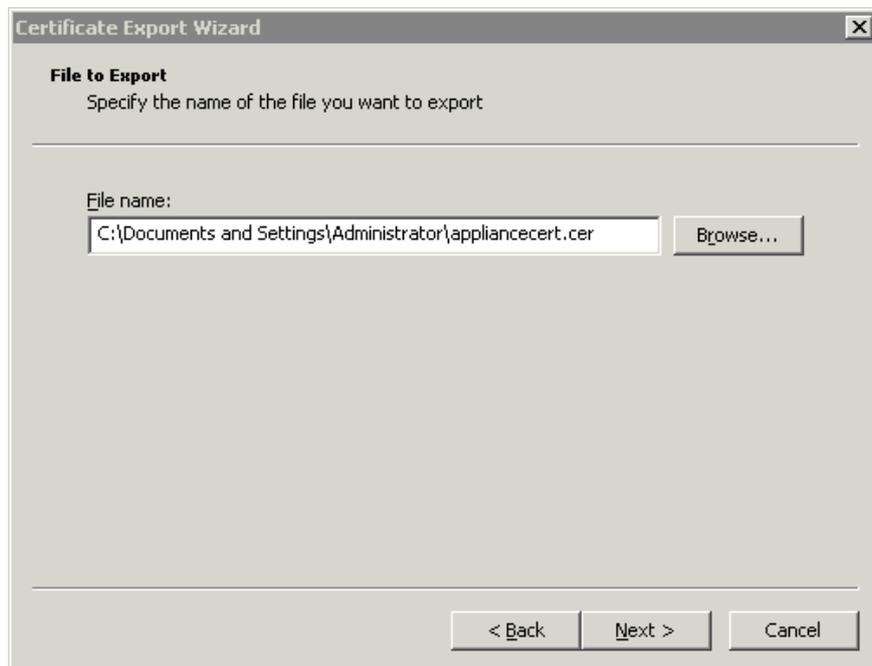
This time, select **No**, do not export the private key and click **Next**.



Select Base-63 encoded X.509 (.CER) from the list and click Next.



Select an appropriate name and location to store the exported certificate and click Next.

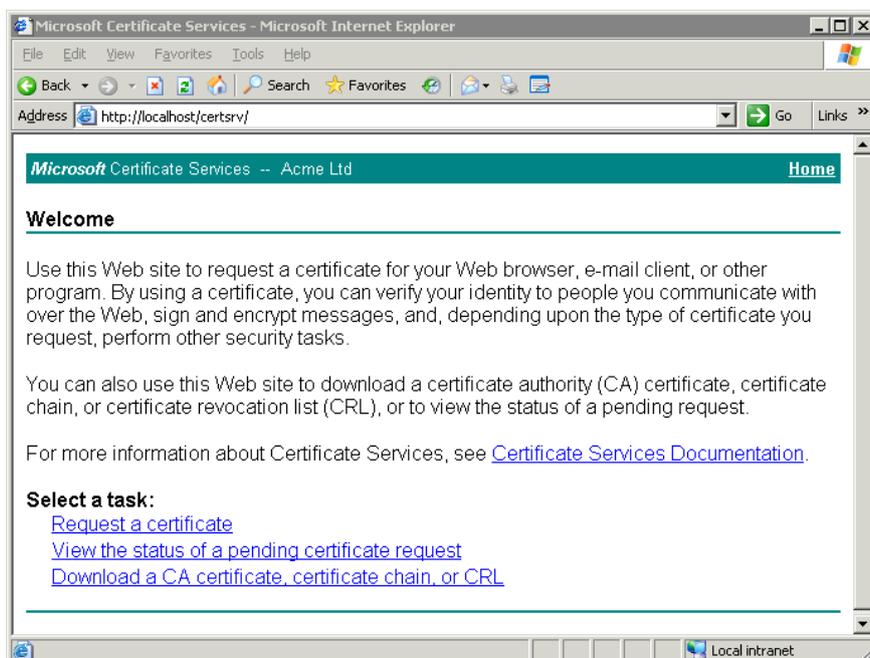


Click Finish to complete the process.

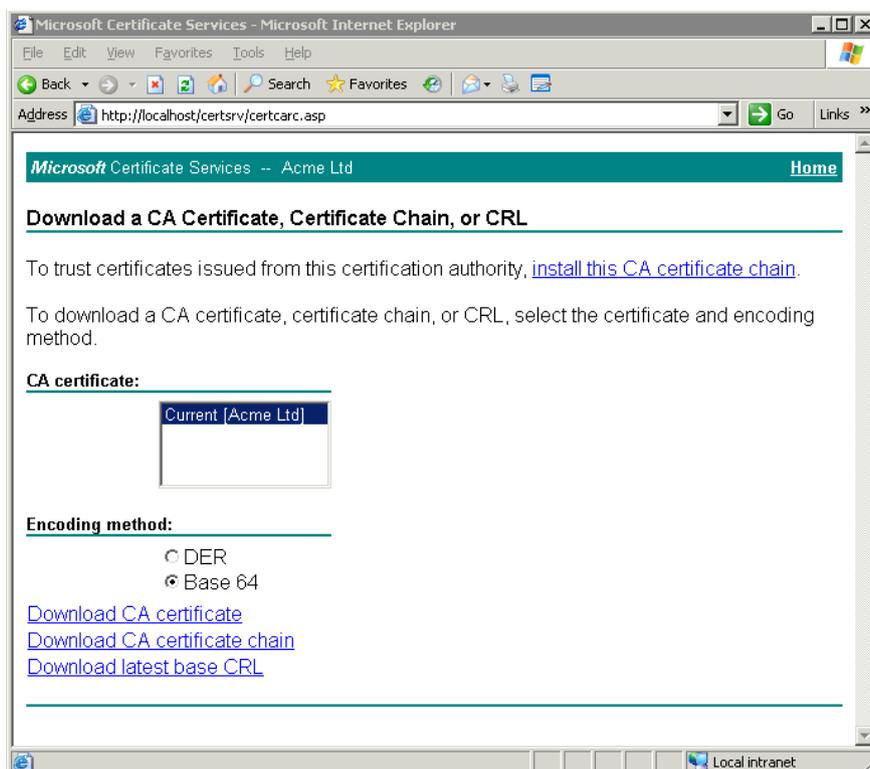


10.3 Exporting the Microsoft CA Certificate

You will need the CA certificate that was used to sign the certificates in the previous section. Open the Microsoft Certificate Server home page and select **Download a CA certificate, certificate chain, or CRL**.



Select the certificate and ensure **Base 64** is checked. Click **Download CA certificate**.



Click Save.



10.4 Converting the Private Key from PFX to PEM Format

The private key must now be converted from PFX to PEM format using Openssl either from the Gateway console (installed by default) or on Windows by installing Openssl available from the following URL:

- <http://gnuwin32.sourceforge.net/packages/openssl.htm>

If you are planning on converting the private key on the Gateway, you will need to ensure that SSH has been enabled both through the firewall (port 22) and on the Gateway to allow specific IP access (System Center, System Settings, SSH Access). The files can be copied across to the Gateway using WinSCP which can be downloaded from the following URL:

- <http://www.winscp.net/eng/download.php>

You will need to provide the console user credentials in WinSCP to access the Gateway (it is recommended that you copy the key to /tmp).

To access the Gateway command line remotely, you will need an SSH client such as putty that can be downloaded from the following URL:

- <http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

After following these steps, you should read Section 7.1 to import the key and certificate as described below.

Once you've established an SSH connection to the Gateway, you will need to access the command line as detailed in Section 5.2.

Note: The following Openssl procedure is the same on Windows and Unix platforms.

cd to /tmp or wherever the private key was copied to and type Openssl (which will allow you to input OpenSSL commands). Type the following command replacing the key name with your own:

```
Pkcs12 -in private-key.pfx -out private-key.pem -nodes
```

Type the password of the private key when prompted.

```
# ls
Clearswift-CA.cer  appliance.cer  private-key.pem  private-key.pfx
# openssl
OpenSSL> pkcs12 -in private-key.pfx -out private-key.pem -nodes
Enter Import Password:
MAC verified OK
OpenSSL> █
```

You should now have a private-key.pem file situated in the /tmp directory that should be copied back to your windows machine using WinSCP. The CA certificate, signing certificate and private key can now be imported into the Gateway as described in Section 7.1 "Importing the Signed Certificate and Private Key Pair".

11 Appendix B - Creating a Self-Signed Certificate

The easiest way to test TLS with the Gateway without investing in certificates is to sign the certificate locally. This can be achieved by setting up a local Certificate Authority on the Gateway or from a windows machine with OpenSSL installed. OpenSSL for Windows is available via the following URL:

- <http://gnuwin32.sourceforge.net/packages/openssl.htm>

Self signed certificates are not recommended for production use, but are useful for testing in preproduction or proof of concept environments. It is always recommended to purchase certificates from a commercial CA.

The following sections provide details on creating and signing a certificate for testing purposes. The following procedure is identical for both Windows and Linux environments and assumes that a CSR has already been created using the procedure defined in Section 5.2 "Creating a Private Key and CSR using OpenSSL".

11.1 Creating a Gateway Based Certificate Authority

To create a Certificate Authority on the Gateway, you will need to logon to the Gateway (as detailed in Section 5.2) and carry out the following steps:

11.1.1 Generating the CA Key and CA Certificate

1. Type the following command at the prompt:

```
cd /tmp
```

```
mkdir CA
```

```
cd CA
```

```
openssl genrsa -out CA.key 1024
```

```
# cd /tmp
# mkdir CA
# cd /tmp/CA
# openssl genrsa -out CA.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
#
```

```
openssl req -new -key CA.key -x509 -days 1095 -out CA.crt
```

2. Input all the relevant data such as Country, Company, etc. in the relevant fields for the CA certificate.

```
# openssl req -new -key CA.key -x509 -days 1095 -out CA.crt
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 a 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) [AU]:GB
State or Province Name (full name) [Some-State]:Berks
Locality Name (eg, city) []:Theale
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Clearswift
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:
Email Address []:
#
```

3. You should now have the CA private key and certificate located in the /tmp/CA directory. These files are used to sign the certificate signing request as created in Section 5.2.2.

```
# ls
CA.crt  CA.key
#
```

11.1.2 Signing the Certificate with the Gateway CA

1. You will need to copy the emailgateway.csr (as created in Section 5.2.2) to /tmp/CA.
2. From the directory /tmp/CA, run the following command:

```
openssl x509 -req -days 365 -in emailgateway.csr -CA CA.crt -CAkey
CA.key -CAcreateserial -out emailgateway.crt
```

```
# openssl x509 -req -days 365 -in emailappliance.csr -CA CA.crt -CAkey CA.key -C
Acreateserial -out emailappliance.crt
Signature ok
subject=/C=GB/ST=Berks/L=Theale/O=Clearswift/CN=emailappliance.clearswift.com
Getting CA Private Key
#
```

You should now have a signed certificate 'emailgateway.crt' situated in the /tmp/CA directory ready for use within the Gateway.

Follow the steps detailed in Section 7.1 to import the certificate and key for testing.