

## Clearswift Web Appliance HTTPS/SSL decryption

### Introduction

This Technical FAQ explains the functionality of the optional HTTPS/SSL scanning and inspection module available for the Clearswift Web Appliance and how it is deployed.

### How does the Clearswift Web Appliance inspect encrypted HTTPS traffic?

When a user's browser requests a connection to an HTTPS site the web appliance will automatically create and sign an HTTPS web server certificate for the site being requested. This process of certificate creation occurs for each new web site request to an HTTPS site.

The sequence of events:

1. The user requests an HTTPS URL via their browser i.e. <https://mail.somesite.com>.
2. The web appliance automatically creates an HTTPS web server certificate for the domain <https://mail.somesite.com> and returns this certificate to the browser.

**Note:** Users browsers must be set-up to trust the certificates created and signed by the web appliance - as a trusted certificate authority. Failure to import the web appliance root signing certificate into the users' browser certificate store (see next heading below) will cause the user's browser to display a certificate warning, because certificates signed by the web appliance will not be trusted.

3. The encrypted session is then established between the browser and the web appliance using the details provided by the certificate provided from the web appliance.
4. The web appliance also connects to the remote web server requested (<https://mail.somesite.com>) and inspects that server's certificate to ensure it is valid and can be trusted
5. If the certificate is valid then an encrypted session is established between the web appliance and the remote server.
6. The data that passes between a user's browser and the Clearswift Web Appliance is encrypted.
7. The data that passes between the Clearswift Web Appliance and the remote web server is encrypted.
8. The data passing within the Clearswift Web Appliance's own analysis engine is not encrypted, and according to policy may be content checked against an acceptable use policy (AUP) as well as being automatically scanned for web malware.

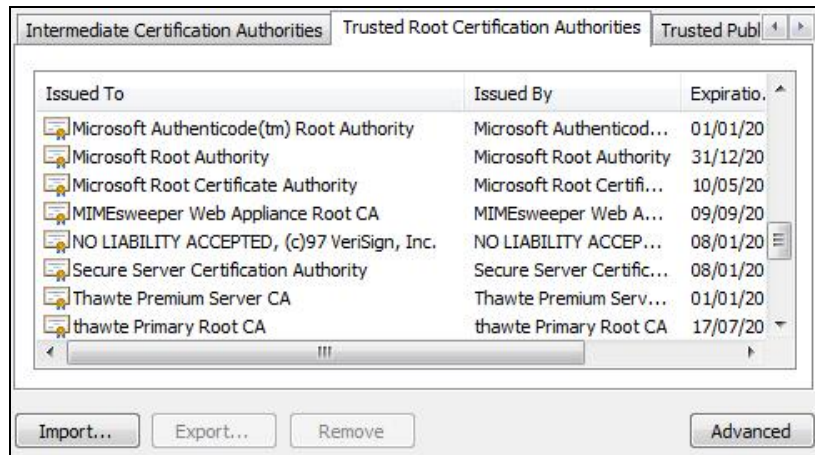
### Importing the Clearswift Web Appliance MIMESweeper root CA into users' browsers

As detailed above it is essential that the users' browsers trust the certificates signed by the web appliance. To enable the browser to trust the web appliance's certificate authority (CA) you will need to export the web appliance root CA certificate and import it into each users' browser's certificate store. After first exporting the Clearswift Web Root Certificate from the web appliance (see below) it is then imported into Internet Explorer and Firefox via the browser's certificate import option as follows:

Internet Explorer: Tools > Internet Options > Content tab > Certificates > Trusted Root Certification Authorities > Import

Firefox: Tools > Option > Advanced > Encryption tab > View Certificates > Authorities > Import and select to trust this certificate to identify web sites.

The certificate will appear in the browser certificate store and will be shown under the name MIMESweeper Web Appliance Root CA as shown below.

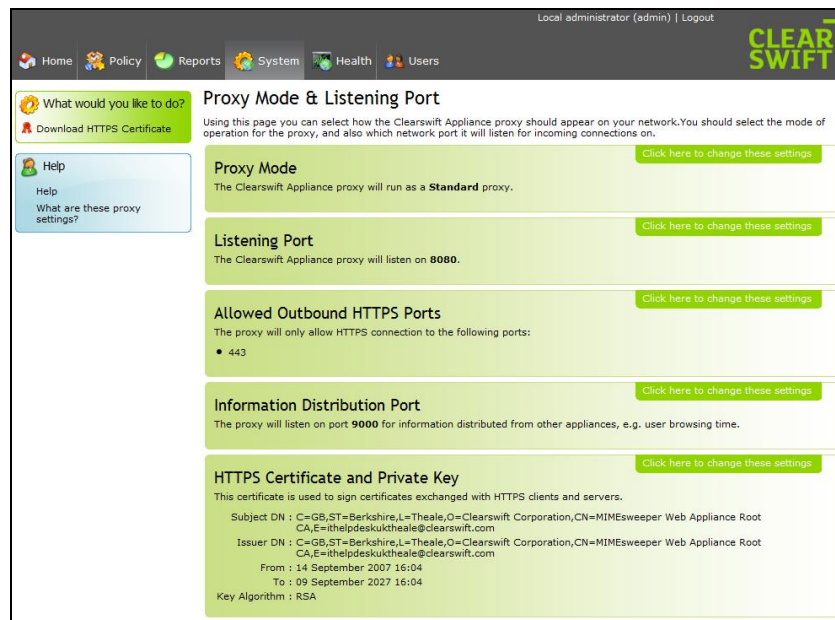


**Fig 1:** Imported MIMESweeper Web Appliance Root CA certificate as seen in Internet Explorer.

**Note:** Active Directory Group Policy may be used to import the certificates into all users' browsers.

## Exporting the root certificate from the Clearswift Web Appliance

The MIMESweeper Web Appliance Root CA certificate is exported from the following location:



**Figure 2:** Downloading the HTTPS certificate:  
 System Center > Proxy Settings > Proxy Mode & Listening Port > Download HTTPS Certificate.

The certificate exported from the location above must then be imported into all your users' browsers as described above, and before the HTTPS decryption option is enabled.

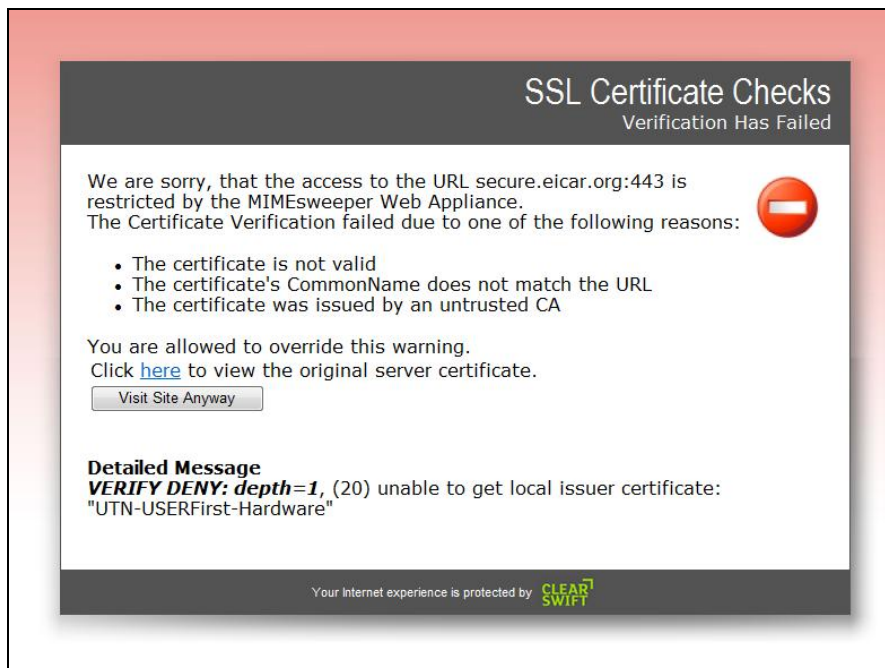
## Enabling the HTTPS decryption option

The HTTPS decryption option is enabled in the following location:



**Figure 3: Enabling HTTP decryption:**  
Policy Center > Global Web Policy > HTTPS Content Scanning.

When enabling the decryption option you are also able to stop users' from accessing sites with certificate failures, or by selecting the 'Allow access to sites with certificate failures' as shown above, users' will be warned of the certificate failure reason but still permitted to 'Visit Site Anyway' as shown in Figure 4 below.



**Figure 4: User certificate failure notification & override page.**

## Advanced - creating your own signing certificate and importing it into the Clearswift Web Appliance

1. Connect to the Web Appliance via SSH , sudo su -
2. Create a folder where certificates will be created, e.g. mkdir /root/certs .
3. Change to that folder, e.g. cd /root/certs .
4. Copy two files:
  - a. cp /etc/ssl/misc/CA.sh.
  - b. cp /etc/ssl/openssl.cnf.
5. Edit the openssl.cnf file to set the number of DAYS higher than the default 365 to increase the time the certificate remains valid. E.g. vi openssl.cnf. Look for default\_days and set this higher, e.g. 3650.
6. Run:
  - a. ./CA.sh –newca.
7. Hit enter for default file name.
8. Enter the passphrase and confirm it.
9. Enter all of the details asked which are required to create your certificate. It is very important that all these are set otherwise the Web Appliance GUI may accept the certificate when imported but it may fail to work. What you are about to enter is called a Distinguished Name or a DN.

Country Name (2 Letter code) [GB]

State or Province Name (Full name) [Berkshire]

Locality Name (e.g., City) [Theale]

Organization Name (e.g., Company) [Clearswift Limited]

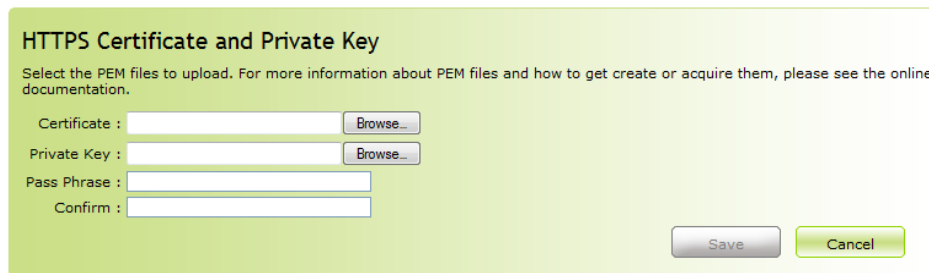
Organizational Unit Name (e.g., Section) [IT Support]

Common Name (e.g., YOUR name) [webappliance3.ocean.tld]

Email Address e.g., [admin@appliance3.ocean.tld]

10. This will create a folder called demoCA. Change to this folder, e.g. cd demoCA.
11. In this folder will be found the root CA certificate called 'cacert.pem' and in the private folder will be the key called 'cakey.pem'. FTP both these files off the system.

These two files may then be imported into the Web Appliance GUI and the certificate may also be used in users' browsers so that they trust it.



**HTTPS 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 :

Pass Phrase :

Confirm :

**Figure 5: Importing your own certificate**  
*System Center > Proxy Settings > Proxy Mode & Listening Port > HTTPS Certificate and Private Key.*

**Notes:**

1. This certificate will need to be imported into the browser so that it is trusted
2. When importing the certificate the file filter must be set to '\*' see the file with Internet Explorer
3. When importing the certificate into the Web Appliance the following log can be checked to see if any errors occurred: /tmp/.csmds.log.

To view this just: `cat /tmp/.csmds.log`

- END -