TECH FAQ

CLEARSWIFT SECURE Web Gateway HTTPS/SSL decryption

Introduction

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

How does the Web Gateway inspect encrypted HTTPS traffic?

When a user's browser requests a connection to an HTTPS site the Web Gateway 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://www.clearswift.com.
2. The Web Gateway automatically creates an HTTPS web server certificate for the domain https://www.clearswift.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 Gateway - as a trusted certificate authority. Failure to import the Web Gateway 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 Gateway will not be trusted.

3. The encrypted session is then established between the browser and the Web Gateway using the details provided by the certificate provided from the Web Gateway.
4. The Web Gateway 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 Gateway and the remote server.
6. The data that passes between a user's browser and the Web Gateway is encrypted.
7. The data that passes between the Web Gateway and the remote web server is encrypted.
8. The data passing within the Web Gateway'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.

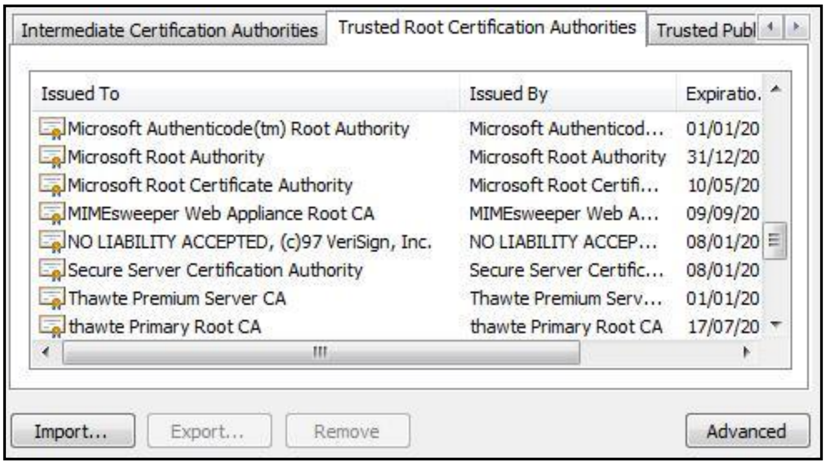
Importing the Web Gateway's root CA certificate into users' browsers

As detailed above it is essential that the users' browsers trust the certificates signed by the Web Gateway. To enable the browser to trust the Web Gateway's certificate authority (CA) you will need to export the Web Gateway root CA certificate and import it into each users' browser's certificate store. After first exporting the Clearswift Web Root Certificate from the Web Gateway (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 given to the Web Gateway as issued by MIMEsweeper as shown below.


Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced

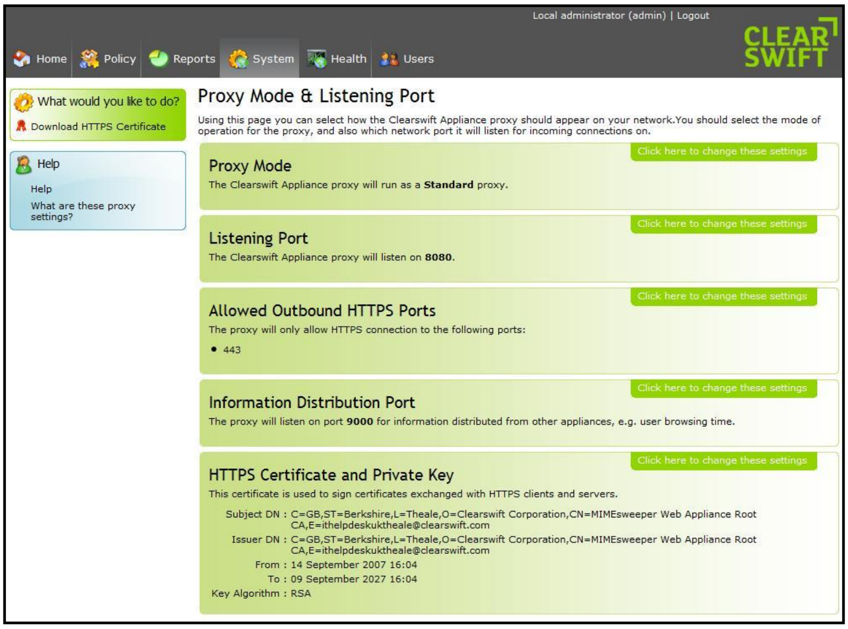
Issued To	Issued By	Expiratio.
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticod...	01/01/20
Microsoft Root Authority	Microsoft Root Authority	31/12/20
Microsoft Root Certificate Authority	Microsoft Root Certifi...	10/05/20
MIMEsweeper Web Appliance Root CA	MIMEsweeper Web A...	09/09/20
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEP...	08/01/20
Secure Server Certification Authority	Secure Server Certific...	08/01/20
Thawte Premium Server CA	Thawte Premium Serv...	01/01/20
thawte Primary Root CA	thawte Primary Root CA	17/07/20

Fig 1: Imported Web Gateway 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 Web Gateway

The *Web Gateway Root CA* certificate is exported from the following location:


Local administrator (admin) | Logout
Home
Policy
Reports
System
Health
Users
CLEAR SWIFT
What would you like to do?
Download HTTPS Certificate
Help
Help
What are these proxy settings?
Click here to change these settings

Proxy Mode & Listening Port

Using this page you can select how the Clearswift Appliance proxy should appear on your network.You should select the mode of operation for the proxy, and also which network port it will listen for incoming connections on.

Proxy Mode

The Clearswift Appliance proxy will run as a **Standard** proxy.

Listening Port

The Clearswift Appliance proxy will listen on **8080**.

Allowed Outbound HTTPS Ports

The proxy will only allow HTTPS connection to the following ports:

- 443

Information Distribution Port

The proxy will listen on port **9000** for information distributed from other appliances, e.g. user browsing time.

HTTPS Certificate and Private Key

This certificate is used to sign certificates exchanged with HTTPS clients and servers.

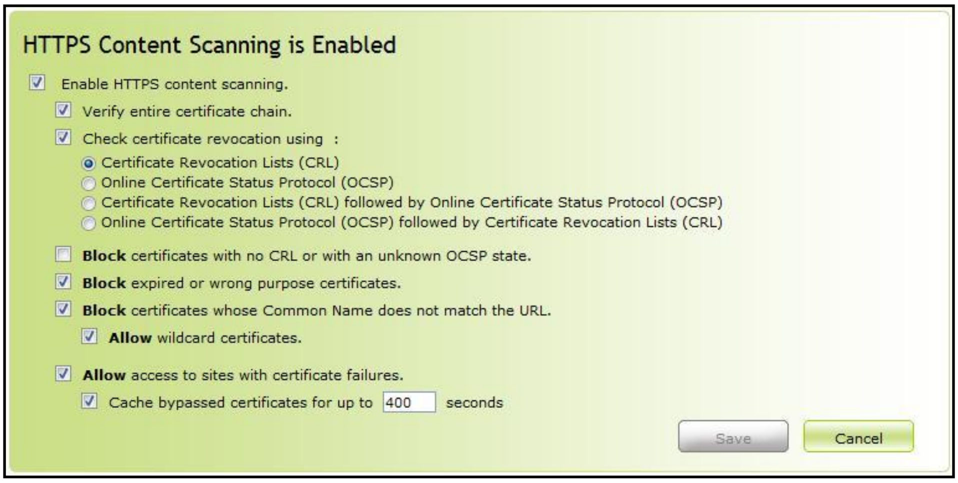
```
   Subject DN : C=GB,ST=Berkshire,L=Theale,O=Clearswift Corporation,CN=MIMEsweeper Web Appliance Root
                CA,E=ithelpdeskuktheale@clearswift.com
    Issuer DN : C=GB,ST=Berkshire,L=Theale,O=Clearswift Corporation,CN=MIMEsweeper Web Appliance Root
                CA,E=ithelpdeskuktheale@clearswift.com
         From : 14 September 2007 16:04
           To : 09 September 2027 16:04
Key Algorithm : RSA
```

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 Policy:



HTTPS Content Scanning is Enabled

☑ Enable HTTPS content scanning.

☑ Verify entire certificate chain.

☑ Check certificate revocation using :

● Certificate Revocation Lists (CRL)
○ Online Certificate Status Protocol (OCSP)
○ Certificate Revocation Lists (CRL) followed by Online Certificate Status Protocol (OCSP)
○ Online Certificate Status Protocol (OCSP) followed by Certificate Revocation Lists (CRL)

□ **Block** certificates with no CRL or with an unknown OCSP state.

☑ **Block** expired or wrong purpose certificates.

☑ **Block** certificates whose Common Name does not match the URL.

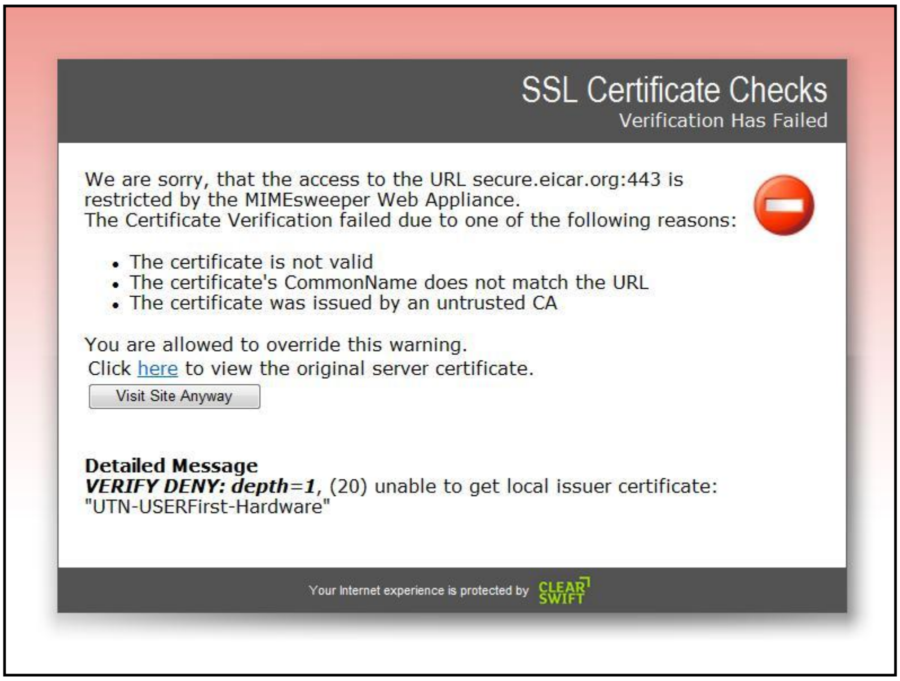
☑ **Allow** wildcard certificates.

☑ **Allow** access to sites with certificate failures.

☑ Cache bypassed certificates for up to 400 seconds

Figure 3: Enabling HTTP decryption:
Policy Center > HTTPS Policy

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.



SSL Certificate Checks
Verification Has Failed

We are sorry, that the access to the URL secure.eicar.org:443 is restricted by the MIMEsweeper Web Appliance.
The Certificate Verification failed due to one of the following reasons:

- The certificate is not valid
- The certificate's CommonName does not match the URL
- The certificate was issued by an untrusted CA

You are allowed to override this warning.
Click here to view the original server certificate.

Detailed Message
VERIFY DENY: depth=1, (20) unable to get local issuer certificate: "UTN-USERFirst-Hardware"

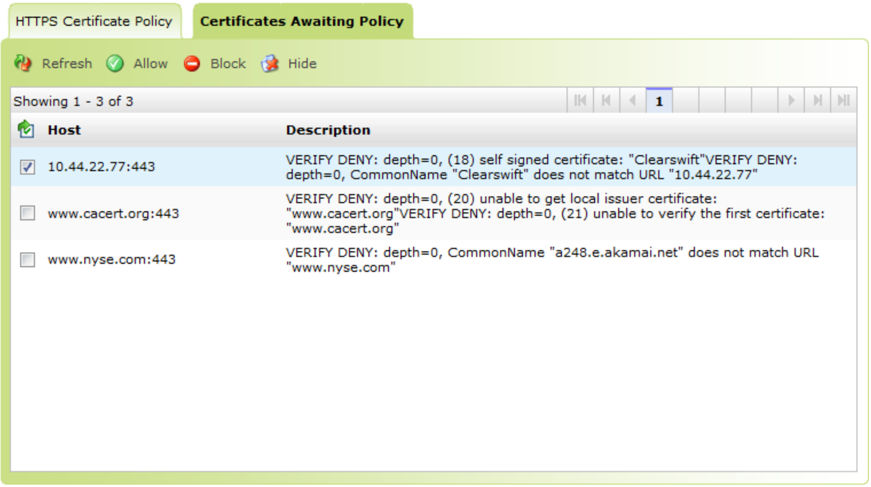
Figure 4: User certificate failure notification & override page.

There are occasions when the web server's certificate may be legitimately invalid for example, an internal intranet web server which uses a self signed certificate. In cases like these it will be desirable to allow the user access without warning the users of the certificate check failure.

The certificate policy includes a section that allows certificate violations to be managed. All certificate failures will be captured and displayed where they can be selectively 'allowed' (whitelisted) or 'blocked' (blacklisted). For those 'allowed' all future certificate violation checks will be disabled for that site and users will not be warned of certificate check failures.

As shown below the certificate failures are displayed in the 'Awaiting Certificate Policy' tab. Each site can be set to

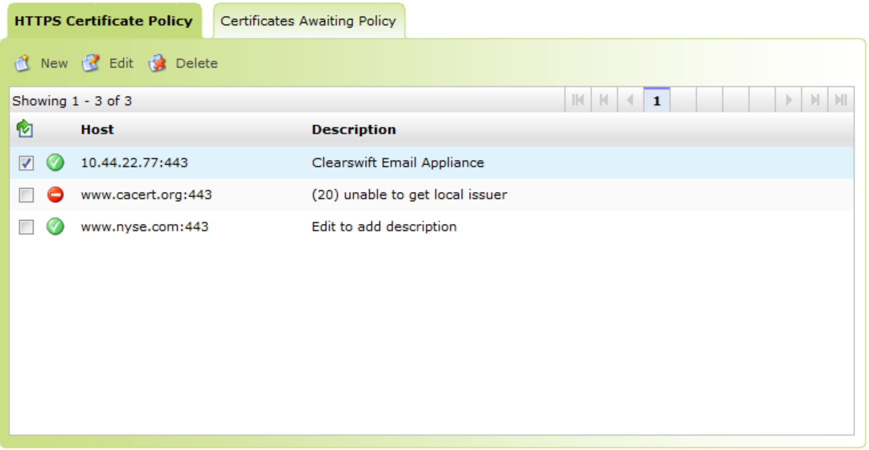
- 'Allow' to disable certificate checks for all future requests to the shown site
- 'Block' to disallow access to the site and always display a block page
- 'Hide' to remove the site from the list until another certificate failure is detected



Showing 1 - 3 of 3

	Host	Description
☑	10.44.22.77:443	VERIFY DENY: depth=0, (18) self signed certificate: "Clearswift"VERIFY DENY: depth=0, CommonName "Clearswift" does not match URL "10.44.22.77"
☐	www.cacert.org:443	VERIFY DENY: depth=0, (20) unable to get local issuer certificate: "www.cacert.org"VERIFY DENY: depth=0, (21) unable to verify the first certificate: "www.cacert.org"
☐	www.nyse.com:443	VERIFY DENY: depth=0, CommonName "a248.e.akamai.net" does not match URL "www.nyse.com"

If a site is set to 'Allow' or 'Block' it will be displayed in the 'Certificate Policy' tab as shown below.



Showing 1 - 3 of 3

		Host	Description
☑	✓	10.44.22.77:443	Clearswift Email Appliance
☐	⊖	www.cacert.org:443	(20) unable to get local issuer
☐	✓	www.nyse.com:443	Edit to add description

Future changes can be managed through the edit option to change the 'Allow' or 'Block' status or to edit the associated descriptive text.

Advanced - creating your own signing certificate and importing it into the Web Gateway

1. Connect to the Web Gateway 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 the file

   ```
   cp /etc/ssl/misc/CA.pl .
   ```

5. Run:

   ```
   ./CA.sh –newca.
   ```

6. Hit enter for default file name.
7. Enter the passphrase and confirm it.
8. Enter all of the details asked which are required to create your certificate questions but make sure the email address and challenge password are empty. It is very important that all these are set otherwise the Web Gateway 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) [UK]

   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) [webgateway.clearswift.com]

   Email Address [Enter]

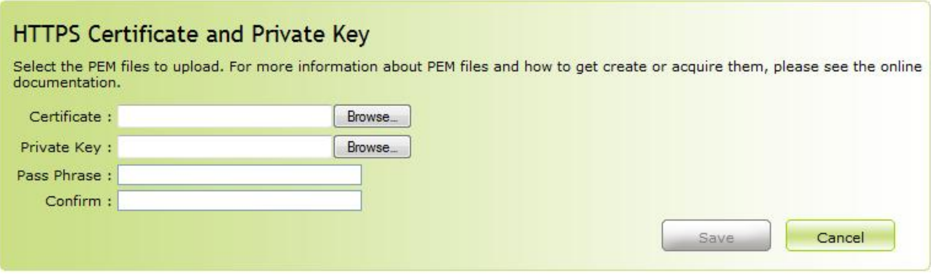
   A challenge password [Enter]

   An optional company name [Clearswift Limited]

   Enter pass phrase for . /demoCA/private/cakey.pem: [pass phrase entered previously]

9. This will create a folder called demoCA. Change to this folder, e.g. cd demoCA.
10. 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.
11. Edit the cacert.pem file in and remove all the top text until -----BEGIN CERTIFICATE-----

These two files may then be imported into the Web Gateway 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.

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 Gateway the following log can be checked to see if any errors occurred: /tmp/.csmds.log.

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

- END -