Secure Web Appliance

SSL Intercept

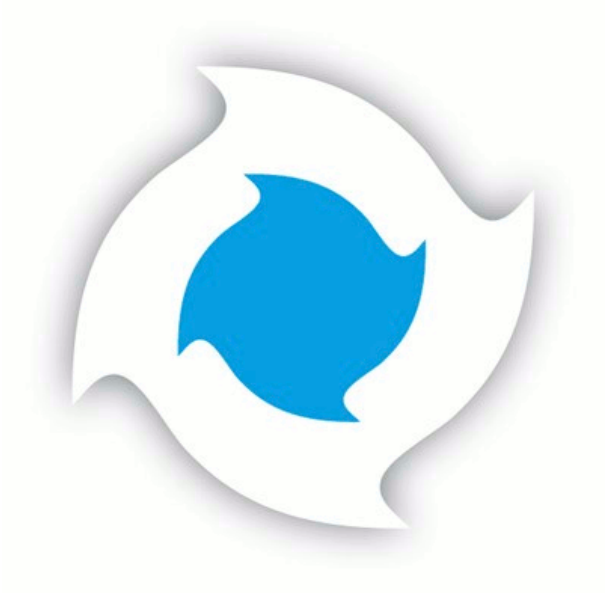

Table of Contents

1. Introduction 1
    1.1. About CYAN Secure Web Appliance 1
    1.2. About SSL Intercept 1
    1.3. About this Manual 1
        1.3.1. Document Conventions 1
2. Overview 2
3. Setting up SSL Intercept 3
    3.1. Setting up CA certificate 4
        3.1.1. Creating a CA certificate 4
        3.1.2. Importing a CA certificate 5
    3.2. SSL Intercept settings in Profiles 6
4. Supplying the CA certificate to the web browser 9
    4.1. Internet Explorer 10
    4.2. Mozilla Firefox 11
    4.3. Google Chrome 12
    4.4. Opera 13
    4.5. Microsoft Windows Operating System 14
    4.6. Microsoft Windows Domain 14
5. Browsing the certificate store 18
6. SSL Manager 19
7. Troubleshooting 21
A. Contact data 22
    A.1. How to contact our sales department 22
    A.2. How to contact our support department 22
        A.2.1. Getting Support 22

List of Figures

3.1. SSL Intercept configuration example - Intercept tab 3
3.2. Default connection denial error page 4
3.3. Certificate and Private key import 5
3.4. SSL Intercept settings in Profiles 6
3.5. Connection denial security warning - server certificate problem 8
4.1. CA Certificate enrollment - Internet Explorer 10
4.2. CA Certificate enrollment - Mozilla Firefox 11
4.3. CA Certificate enrollment - Google Chrome 12
4.4. CA Certificate enrollment - Opera 13
4.5. CA Certificate enrollment - Windows Operating System 14
4.6. CA Certificate enrollment - AD, adding a new GPO 15
4.7. CA Certificate enrollment - AD, importing CA certificate 16
4.8. CA Certificate enrollment - AD, configuring the GPO 16
5.1. Certification store example 18
6.1. SSL Manager settings dialog 19
6.2. SSL Manager - User defined hosts 20
A.1. Version information of the Secure Web 22
A.2. Version information of the Reporting System 22
A.3. Support Package 23

1. Introduction

1.1. About CYAN Secure Web Appliance

The all-in-one appliance hardware solution developed by CYAN Networks is an optimal customized platform that makes the deployment of Secure Web very easy. The Appliance includes a complete pre-installed Secure Web, as well as a Web Admin Interface used for the configuration of the entire machine. The product can easily be integrated into the already existing infrastructures. The configuration and other operating tasks are done with your favorite web browser, thus no knowledge about the integrated operating system is required.

1.2. About SSL Intercept

SSL Intercept allows inspection of an SSL encrypted traffic. Therefore, all filtering mechanisms can be applied to the HTTPS traffic. Without SSL Intercept, no data requested via the HTTPS protocol are recognizable by CYAN Secure Web. These data can include unwanted content, data or even viruses. Only the host name and port of the first request can be checked without the SSL Intercept.

1.3. About this Manual

This manual explains concept and configuration of the SSL Intercept feature present in the CYAN Appliance solution. The reader is expected to have basic knowledge of the Secure Web platform, is able to access and work with the Web Admin Interface and has successful performed the initial setup steps of Secure Web, as outlined in the Getting Started Guides.

This manual is to be used with a CYAN Appliance with Secure Web version 2.1 and above.

For additional documentation, please see our document repository on http://www.cyan-networks.com/documentation

1.3.1. Document Conventions

Indicates a potentially risky situation, leaving the appliance in an unusable state.

Indicates a potentially risky situation, causing misfunction of the solutions.

Indicates information that is substantial for successfully configuring and using the product.

Provides helpful information for the process of configuring and using the product.

Provides additional information about typical scenarios and best practices.

2. Overview

CYAN Secure Web with SSL Intercept enabled acts as “Man-in-the-middle” to a HTTPS connection. It accepts the encrypted connection from the client and opens a second encrypted connection to the destination server. To accept the client connection, a certificate must be supplied by Secure Web to prove it’s identity.

This certificate differs from the certificate of the original web site. Today’s browsers recognize such behaviour and display a warning message to their users for each connection. To avoid these warnings, Secure Web signs all certificates with a Certificate Authority (CA) certificate.

If the same CA certificate is added to the browser’s certificate management system, then the certificate is seen as valid and no warning will be displayed. Every time a client requests a page from an SSL encrypted server, Secure Web creates the client side certificate for this request. This certificate is then stored and all further requests to the same server will get the same certificate. By default, these certificates remain valid for 30 days. After this time has elapsed, a new certificated is generated.

3. Setting up SSL Intercept

This section and the following subsections will cover how to configure SSL Intercept on the Appliance.

First you have to login to the Web Admin Interface. It can be accessed by pointing your browser to the appliance IP adress:

> https://<appliance-ip>:9992/ (for example, https://192.168.1.1:9992/)

Most of the SSL Intercept settings can be found in menu *Services / Proxy Settings / SSL Intercept*. The configuration starts with the tab *Intercept*. An example can be seen in the following figure:

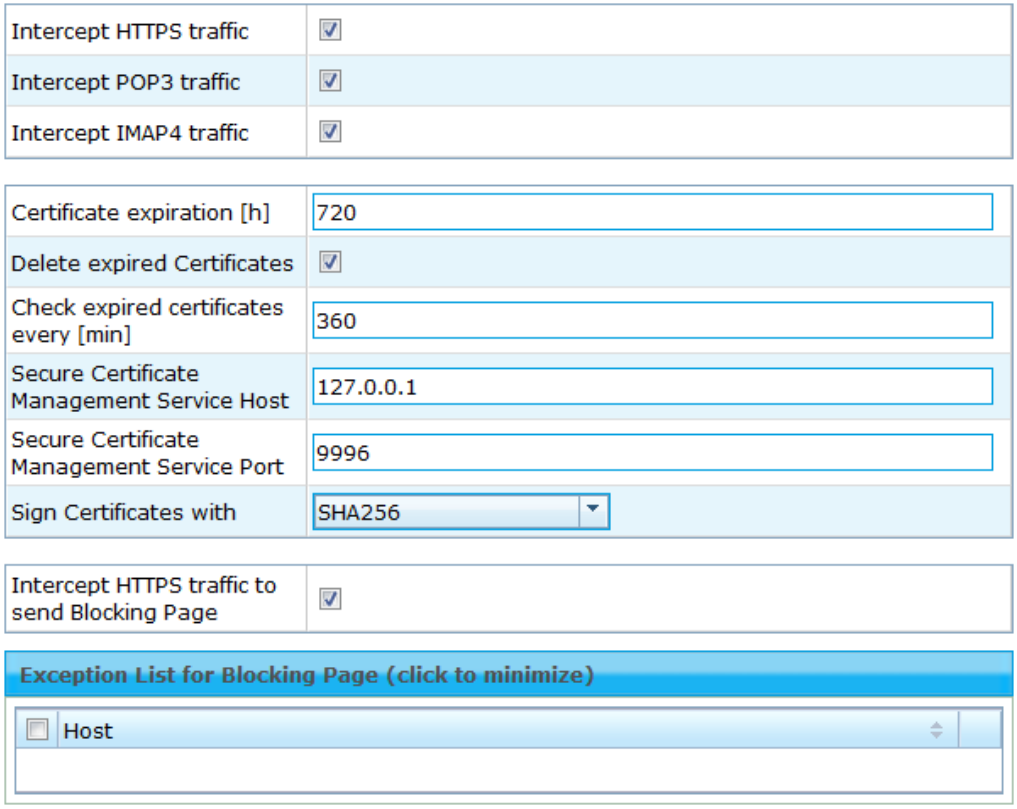

Figure 3.1. SSL Intercept configuration example - Intercept tab

- **Intercept HTTP/POP3/IMAP4** - When checked, enables SSL Intercept for the selected protocol.
- **Certificate expiration** - How long certificates for clients should remain valid. Note that an expired certificate is replaced automatically after this period. The default value is 720 hours (30 days).
- **Delete expired certificates** - When checked, an expired certificate is deleted after a new certificate is generated.
- **Check expired certificates** - Sets how often should be a check for expiring certificates performed. The default value is 360 minutes (6 hours).
- **Secure Certificate Management Service Host/Port** - By default are these set to localhost (127.0.0.1/9996). Changing these values makes sense just in cluster environment, where

generated certificates should be kept centrally, in order to avoid errors caused by multiple certificates generated for the same domain. It should be changed to an IP address and a port of a machine that will serve as a certificate store. However, this change is usually done automatically. Hence there should not be a need for this change under normal circumstances.

- **Sign Certificates With** - Signing algorithm to be used for signing generated certificates. The default and preferred option is SHA256. The MD5 option is no longer considered to be safe and it is kept solely for backward compatibility reasons.

- **Intercept HTTPS traffic to send Blocking Page** - When a HTTPS page is blocked, in order to display a neat security warning page (an example can be seen later in Figure 3.5, “Connection denial security warning - server certificate problem”), it is necessary to first accept the SSL connection and then inject the blocking page in the established connection. Otherwise the connection is simply refused with a HTTP error and the default web browser’s error information is displayed (see Figure 3.2, “Default connection denial error page”).

  When SSL Interception is enabled the security warning page is being displayed by default. However, when SSL Interception is disabled, displaying of the security warning page has to be enabled by the *Intercept HTTPS traffic to send Blocking Page* option.

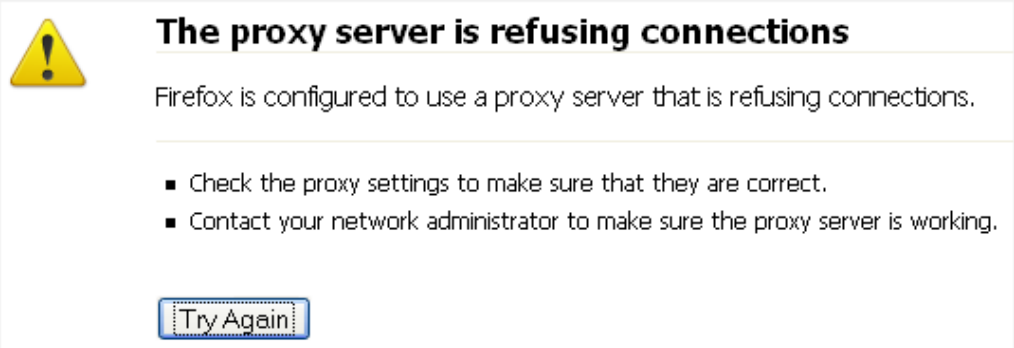

Figure 3.2. Default connection denial error page

- **Exception List for Blocking Page** - When the option *Intercept HTTPS traffic to send Blocking Page* is enabled, web sites added to this list will not be affected by this option and the default browser’s error information page will be displayed, when connection to this web sites is refused.

When a site is added to the *Exception List for Blocking Page*, the change will not take effect immediately but when the SUP (Soft Use Policy) overrule for this site expires from the cache. This is dependent on the settings in menu *Services / Authentication / Settings / General / Soft Use Policy (SUP) timeout* (the default value is 300 seconds).

3.1. Setting up CA certificate

To avoid warnings by the browser for each HTTPS request, CYAN Secure Web needs a certification authority (CA) certificate, which is supplied to the browser as well. This CA certificate can be generated directly within the Web Admin Interface, or you can import your own CA certificate. You will probably have an existing CA certificate that has been generated during the setup process of Microsoft Active Directory domain (and this certificate should be also distributed to the systems in the domain automatically).

3.1.1. Creating a CA certificate

A new CA certificate can be created in menu *Services / Proxy Settings / SSL Intercept / Create CA*. First, switch the dialog into *Edit Mode* to be able to input new values or change the existing ones. Then input all the following values:

- **Country** - A two letters long country code (e.g. US).
- **State or Province** - Full name of the state of province.
- **Locality** - A city.
- **Organisation** - Your company name.
- **Organisational unit** - A section name within the company.
- **Common name** - Your name or an identifier for the certificate.
- **Validity** - How long should the certificate be valid (in years).
- **Expiry date** - This value cannot be changed and just shows the calculated expire date of the previously generated certificate.

When all the required values are present, press the *Save* button. Now it is possible to download the certificate using the *Certificate* button or to download the private key using the *Private key* button. Both are exported in PEM format.

It is crucial to keep the private key private. In most cases, it is not necessary to download it from the Web Admin Interface at all. Making the private key public (for example sending it accidentally by email with the certificate) makes the certificate insecure, as well as any connection using this certificate, because anybody will be able to adopt your identity.

3.1.2. Importing a CA certificate

Figure 3.3. Certificate and Private key import

Import of a CA certificate or a private key can be done in menu *Services* / *Proxy Settings* / *SSL Intercept* / *Import CA*. To import it, you need to supply the certificate and/or the private key in a PEM format that is not password protected. It is the same format as the one in which are the certificate and the private key generated from the Web Admin Interface. This format is textual, so it can be copied from the file to the clipboard and then pasted to the Web Admin Interface. An example is in Figure 3.3, “Certificate and Private key import”. There is no obvious visual difference between a password protected certificate and an unprotected one.

If you now navigate to the menu *Services* / *Proxy Settings* / *SSL Intercept* / *Create CA*, you should see your CA data displayed.

3.2. SSL Intercept settings in Profiles

Some of the SSL Intercept settings can be modified for each profile. To change settings of any particular profile, navigate to the menu *Services* / *Profile Tree* and choose the desired profile. Then navigate to the tab *SSL Intercept*. An example of this dialog is in the following figure:

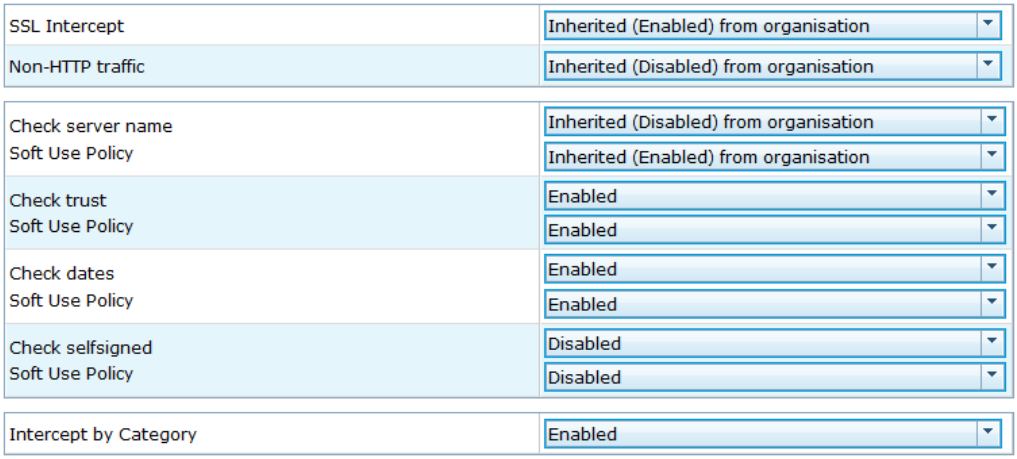

Figure 3.4. SSL Intercept settings in Profiles

Any of the options can be set to either *Enabled*, *Disabled* or can be inherited from parent profile (*organisation* in this example). Meaning of the values is following:

- **SSL Intercept** - Enables/disables the SSL Intercept feature for this profile.
- **Non-HTTP traffic** - Allows/disallows non-HTTP traffic in SSL channel (for example Skype protocol). This option has always precendence over the option *Tunneling of non-SSL traffic* in the *SSL Tunneling* settings of a profile. The *Tunneling of non-SSL traffic* option will, however, still apply to all the traffic to all hosts that have been previously put in the *List of Trusted Hosts* list (or to all traffic when the *Non-HTTP traffic* option is disabled). If both of the options are disabled, these Non-HTTP connections will be simply dropped.
- **Check server name** - Enables/disables checking whether the server name in the server certificate matches the URL that is the connection trying to access.
- **Check trust** - Enables/disables checking whether the server certificate is signed by trusted certification authority or if a chain of trust from the server certificate to some trusted certification authority can be established.
- **Check dates** - Enables/disables checking whether the server certificate is time valid (e.g. did not expire).

- **Check selfsigned** - Enables/disables checking whether the certificate is self-signed.

If any of the checks described above fails, a security warning page may be displayed (provided the option *Intercept HTTPS traffic to send Blocking Page* is enabled). An example of this error page can be seen in Figure 3.5, “Connection denial security warning - server certificate problem”.

- **Intercept by Category** - If this option is enabled, the SSL Interception will be limited to selected categories from the lists below. If disabled, the SSL Interception is done for all connections regardless of the category.

- **List of Categories** - This list controls what categories get intercepted. Any category can be set to *Enabled* (will get intercepted), *Disabled* (will not get intercepted) or *Inherited*. To enable editing of this list, the *Intercept by Category* option needs to be enabled.

- **List of User Defined Categories** - This list function is similar to the *List of Categories*, defining behavior for the user defined categories. Again, to enable editing of this list, the *Intercept by Category* option needs to be enabled. These categories can be quickly changed by right clicking the list and selecting *Edit User Defined Categories*. If you wish to add a web site to some category, you need to navigate to the *URL filter* tab and add it into the *List of Private URLs*.

- **Inherit List of Trusted Hosts** - If this option is enabled, the list of trusted hosts will be inherited from the parent profile.

- **List of Trusted Hosts** - Hosts included in this list will never get SSL Intercepted in this profile, regardless of the settings above. To add a new host, right click the list and select *Add item*.

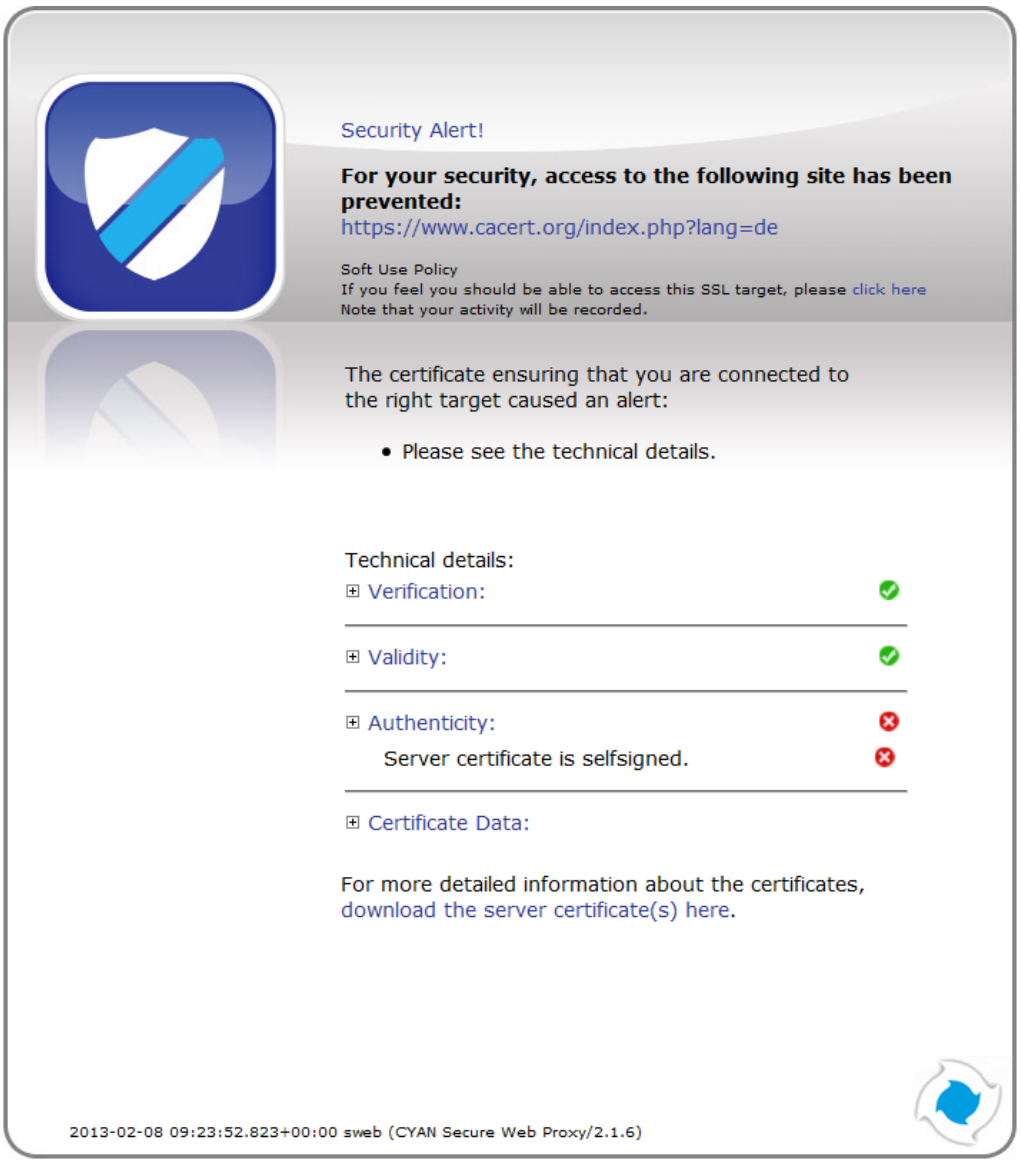

Figure 3.5. Connection denial security warning - server certificate problem

4. Supplying the CA certificate to the web browser

As mentioned previously, the SSL Interception process involves substituting the original certificate from the server with its own certificate. Today's browsers recognize such behavior and display a warning message to their users for each connection. To avoid these warnings, Secure Web signs all certificates with a CA certificate (either supplied or created in the Web Admin Interface, as described in Section 3.1.2, "Importing a CA certificate" and Section 3.1.1, "Creating a CA certificate" respectively).

The same CA certificate needs to be added to the browser's certificate management system, so the certificate will be seen as valid and no warning will be displayed. This section describes how to enroll this certificate in different browsers, as well as globally in the system.

All of the following options assume you have already managed to obtain the CA certificate.

Internet Explorer and Google Chrome Browsers use the operating system certification storage. Therefore if a CA certificate is enrolled in any of these browsers, it will always end up in the operating system certification store. This may result in a strange behavior: if for example, both browsers are installed and the CA certificate is enrolled in the Internet Explorer browser, it will also work in the Google Chrome browser.

4.1. Internet Explorer

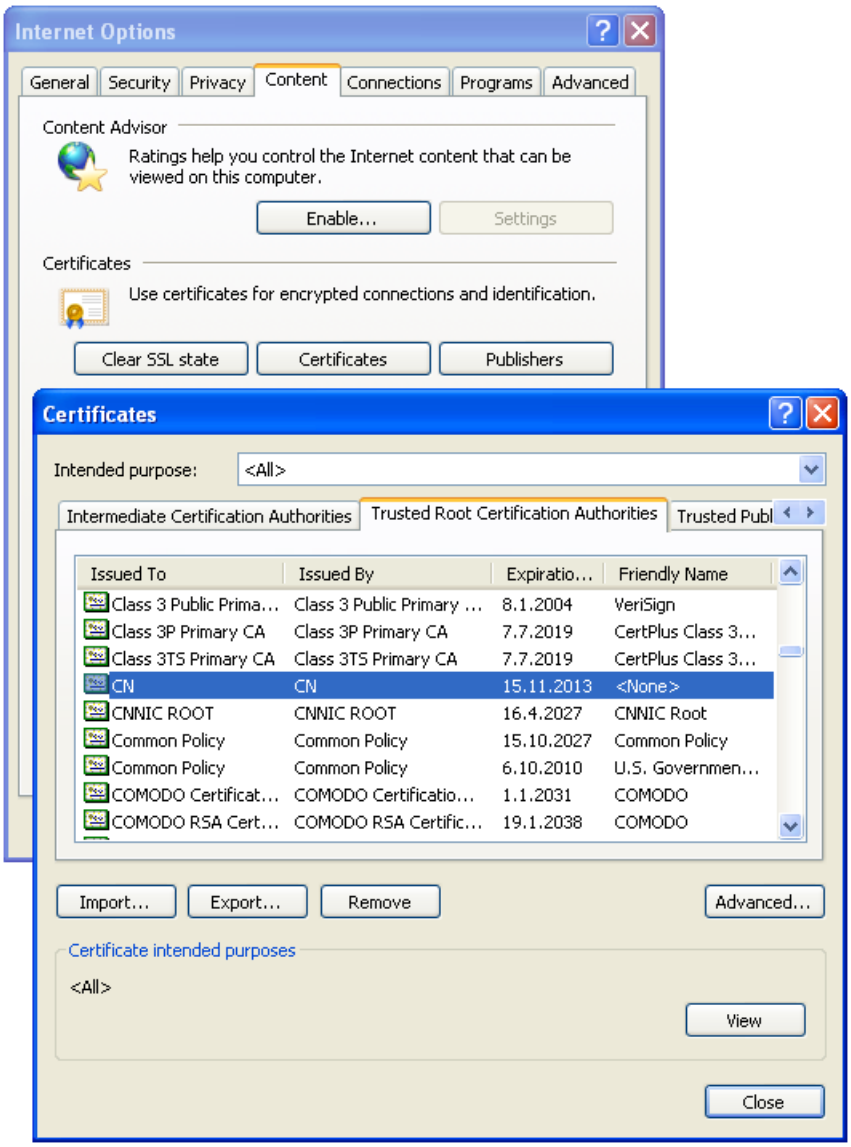

Figure 4.1. CA Certificate enrollment - Internet Explorer

This guide is written for Internet Explorer version 8. For any other version the steps are similar. To configure an Internet Explorer browser to use the CA certificate, follow these steps:

1. Go to menu *Tools* / *Internet Options*, then navigate to tab *Content* and click on the button *Certificates*.

2. In the dialog that appears, navigate to the *Trusted Root Certification Authorities* tab and click on the *Import…* button.

3. Click on *Next*, then click on *Browse…*, find the CA certificate on your file system, select it, click on *Next* and then once again in the following dialog.

4. Click on *Finish* button and then confirm the Security Warning dialog with the *Yes* button.

Now you should be able to see the CA certificate among the others in the list (see Figure 4.1, “CA Certificate enrollment - Internet Explorer”) and warnings in the browser should not be displayed

anymore. The certificate can be removed later by selecting it in the list of certificates and clicking on the *Remove* button.

4.2. Mozilla Firefox

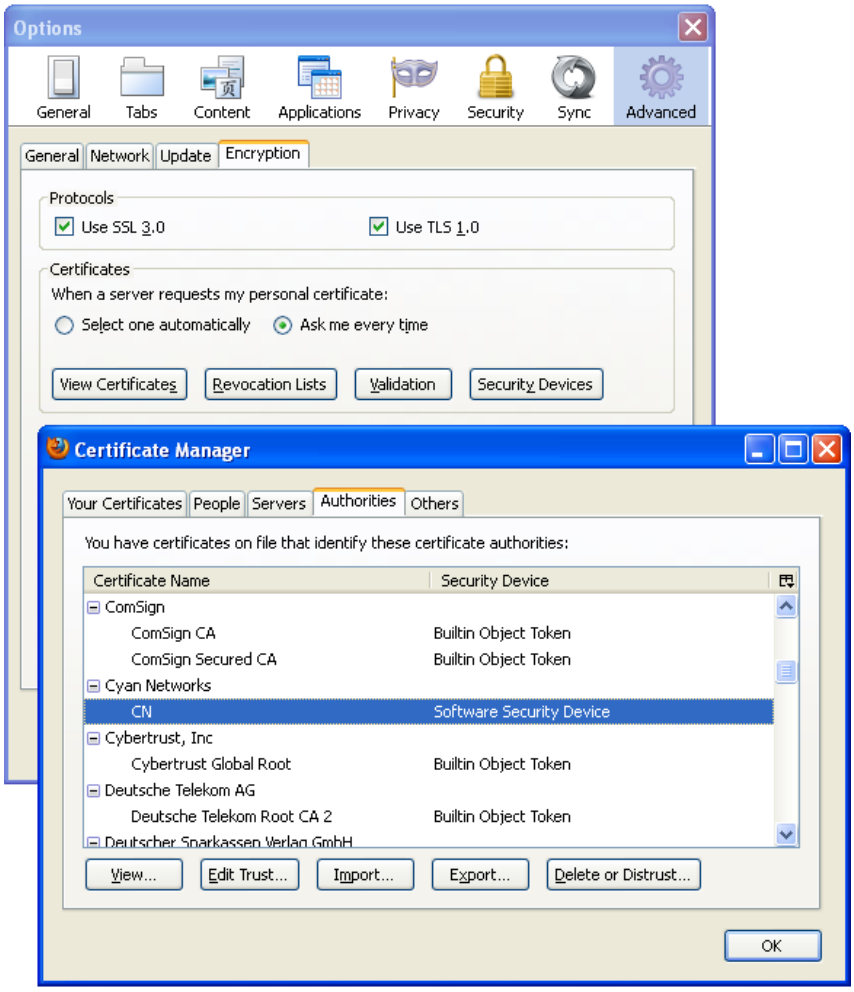

Figure 4.2. CA Certificate enrollment - Mozilla Firefox

To configure a Mozilla Firefox browser to use the CA certificate, follow these steps:

1. Go to menu *Tools / Options*, then navigate to tab *Advanced*, sub tab *Encryption* and in the *Certificates* box click on the button *View Certificates*

2. In the dialog that appears navigate to the *Authorities* tab and click on the *Import…* button.

3. Find the CA certificate on your file system and select it.

4. In the following dialog, check all the options present there and click on *OK*.

Now you should be able to see the CA certificate among the others in the list (see Figure 4.2, “CA Certificate enrollment - Mozilla Firefox”) and warnings in the browser should not be displayed anymore. The certificate can be removed later by selecting it in the list of certificates and clicking on the *Delete or Distrust* button.

4.3. Google Chrome

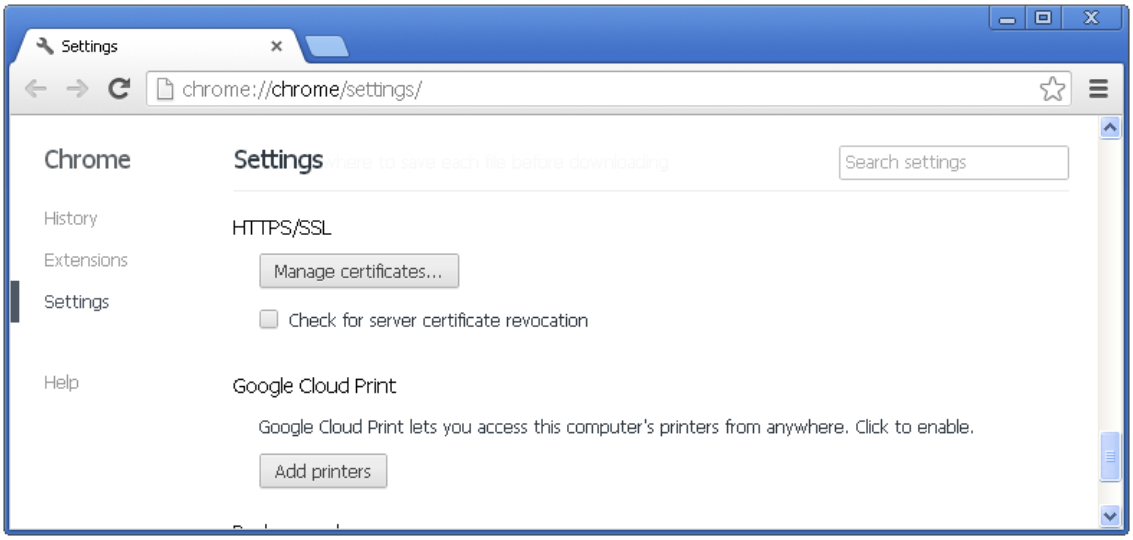

Figure 4.3. CA Certificate enrollment - Google Chrome

To configure a Google Chrome browser to use the CA certificate, follow these steps:

1. Go to menu *Settings*

2. At the bottom of the page click on *"Show advanced settings"*, scroll down to *HTTPS/SSL* heading and click on the *Manage certificates…* button (see Figure 4.3, “CA Certificate enrollment - Google Chrome”).

3. The rest of the configuration is the same as for Internet Explorer browser from step 2, described above.

4.4. Opera

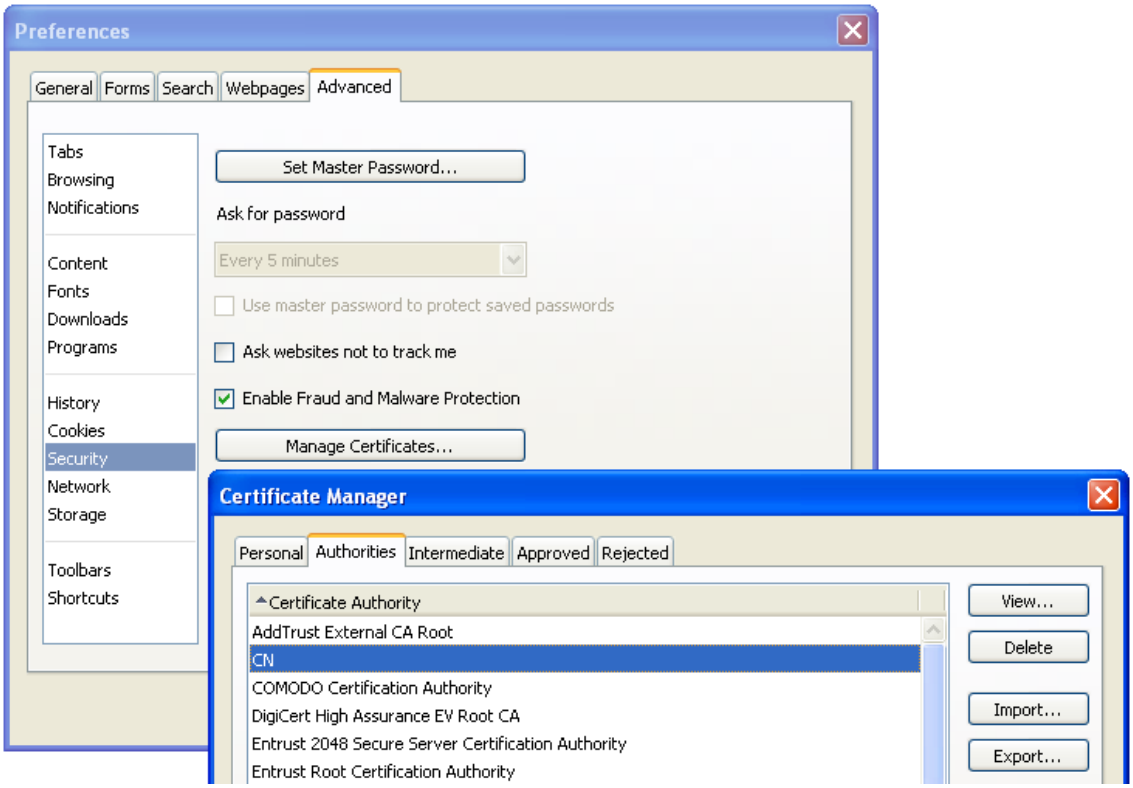

Figure 4.4. CA Certificate enrollment - Opera

To configure an Opera browser to use the CA certificate, follow these steps:

1. Go to menu *Settings / Preferences…*, then navigate to tab *Advanced*, select *Security* in the list and click on the *Manage Certificates…* button.

2. In the dialog that appears navigate to the *Authorities* tab and click on the *Import…* button.

3. Find the CA certificate on your file system and select it.

4. In the following dialog click on *Install* and confirm it by clicking on the *OK* button.

Now you should be able to see the CA certificate among the others in the list (see Figure 4.4, “CA Certificate enrollment - Opera”) and warnings in the browser should not be displayed anymore. The certificate can be removed later by selecting it in the list of certificates and clicking on the *Delete* button.

4.5. Microsoft Windows Operating System

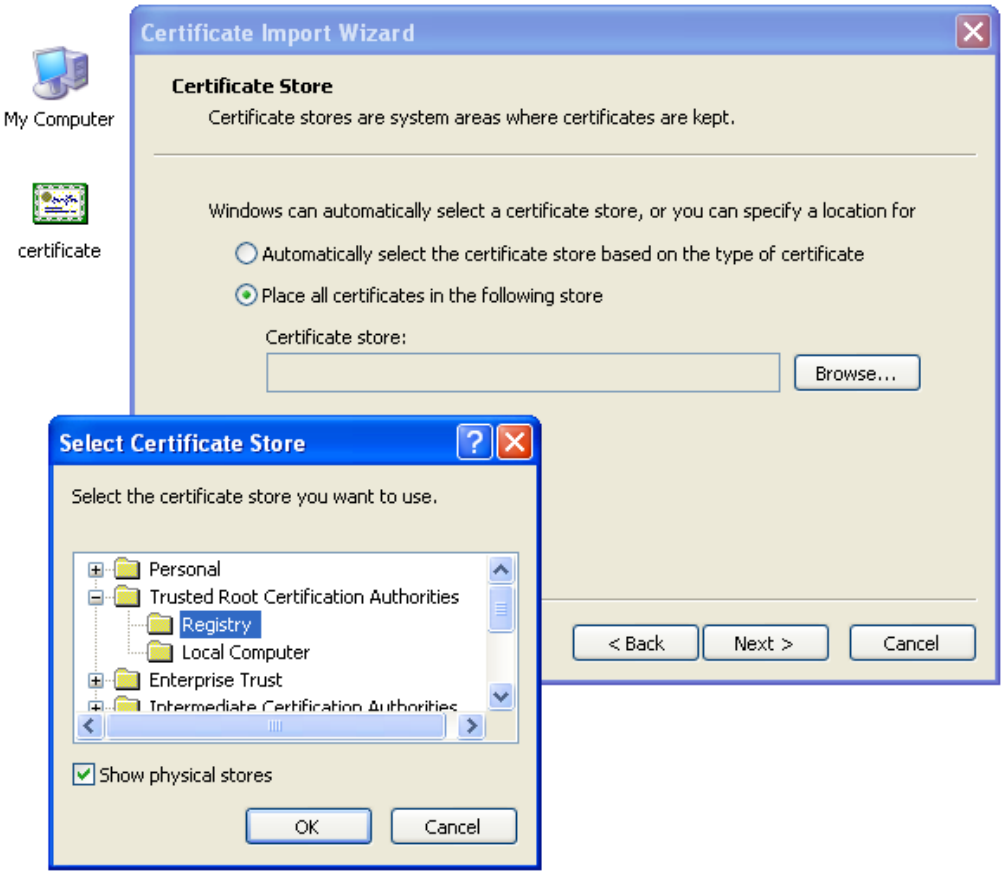

Figure 4.5. CA Certificate enrollment - Windows Operating System

The CA certificate can be also enrolled directly into the operating system. In all of the Microsoft Windows operating systems, version XP or higher, the process is the same:

1. Find the CA certificate on your file system, right click on the file and select *Install Certificate*.

2. Click on *Next*, select *Place all the certificates in the following store* and then click on the *Browse…* button.

3. Check the *Show physical stores* check box, select *Trusted Root Certification Authorities / Registry* and click on *OK* (see Figure 4.5, “CA Certificate enrollment - Windows Operating System”).

4. Click on the *Next*, then on the *Finish* button and then confirm the Security Warning dialog with the *Yes* button.

Now the warnings in the Internet Explorer and Google Chrome browsers should not be displayed anymore. The certificate can be removed later as described at the end of Section 4.1, “Internet Explorer”.

4.6. Microsoft Windows Domain

There is a possibility to enroll the CA certificate into multiple computers that are part of a Microsoft Active Directory (AD) domain. Let us assume the following example AD domain:

- One domain called *ict.local*.
- One Organizational Unit (OU) within the domain called *company*.
- One Security Group *Computers* that is part of the OU *company*.
- Any number of computers, that are placed in the Security Group *Computers* and in which should be the CA certificate enrolled.

To successfully enroll the CA certificate in all the computers within the *company/Computers* group, the following steps are necessary:

First, open the **Group Policy Management Console**. Click *Start*, click *Run…*, type "gpmc.msc" and press *OK*.

If the Group Policy Management Console fails to start, especially in the Microsoft Windows 2003 Server, you need to install it first. For the Microsoft Windows 2003 Server it can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=21895

In the Group Policy Management Console, add a new Group Policy Object (GPO). Navigate to *Group Policy Objects*, right click in the *Contents* tab and select *New*, as showed in the following figure:

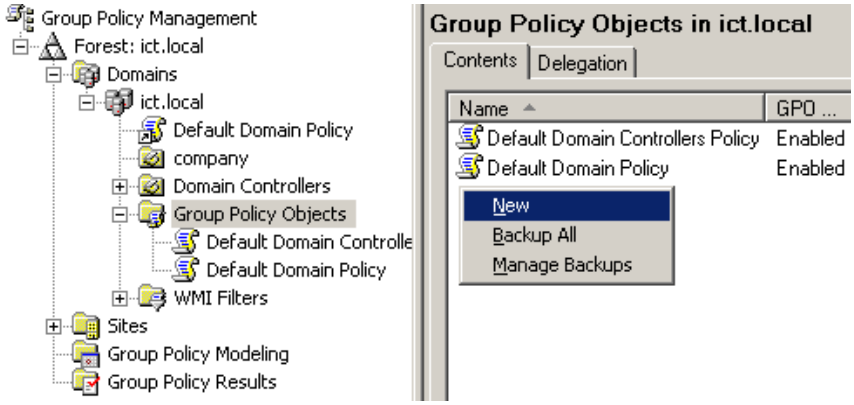

Figure 4.6. CA Certificate enrollment - AD, adding a new GPO

Input new name for the GPO (for example "Enroll SWeb CA Certificate"). Now right click the newly created GPO, select *Edit…* and navigate to *Computer Configuration / Windows Settings / Security Settings / Public Key Policies / Trusted Root Certification Authorities*. Right click in the list and select *Import…*, as showed in the Figure 4.7, “CA Certificate enrollment - AD, importing CA certificate”.

Click *Next*, click *Browse…*, find the CA certificate on your file system, select it. Then click *Next* twice and then *Finish*. This is all the settings needed to be done for this GPO, so you can close the Group Policy Object Editor.

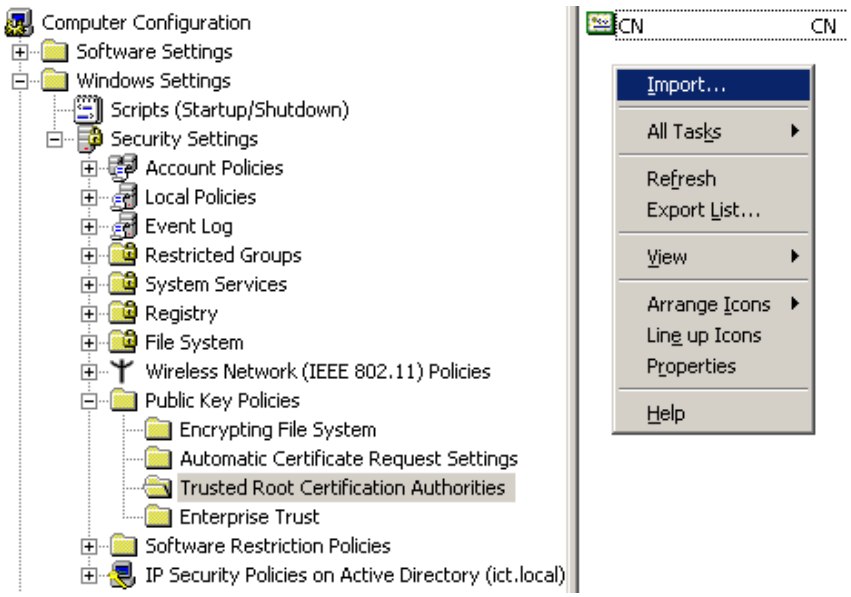

Figure 4.7. CA Certificate enrollment - AD, importing CA certificate

Now it is necessary to link the "Enroll SWeb CA Certificate" GPO to the desired OU (in this example OU *company*). It can be done simply by dragging the GPO and dropping it on the desired OU. The other way is right clicking the OU in the list, selecting *Link an Existing GPO…* and selecting the "Enroll SWeb CA Certificate" GPO from the list. The following figure shows the desired result:

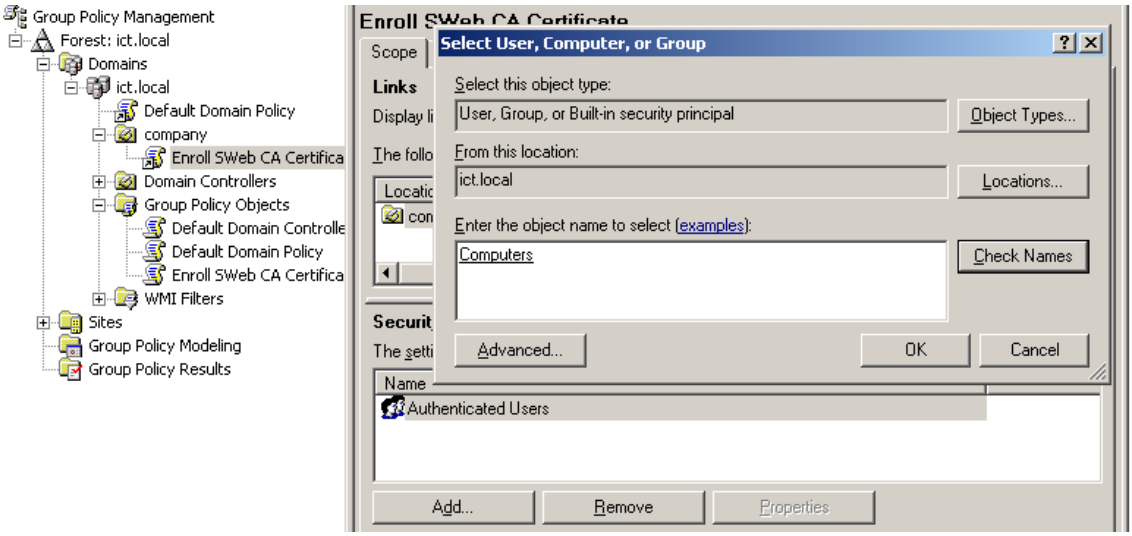

Figure 4.8. CA Certificate enrollment - AD, configuring the GPO

By default, the GPO is restricted to all objects present in the *Authenticated Users* group. This group should cover all the objects (Users, Computers, etc.), that can successfully connect to the domain. To limit the GPO just to a group of selected computers (in this example grouped in the Security Group *Computers*), in the GPO view, tab *Scope*, click on the *Add…* button and select the appropriate Security Group. You can also remove the *Authenticated Users* group with the *Remove* button.

Please note that depending on the Active Directory settings, it may take up to 20 minutes to see the changes on the targeted computers and a re-login may be required after this

time. To speed up the changes, it may help to issue command *gpupdate /force* on the targeted computers (but it is not required).

5. Browsing the certificate store

All the client certificates created during SSL Interception can be viewed and managed in the menu *Services* / *Proxy Settings* / *SSL Intercept* / *Certificates*. An example of the list of created certificates is in the following figure:

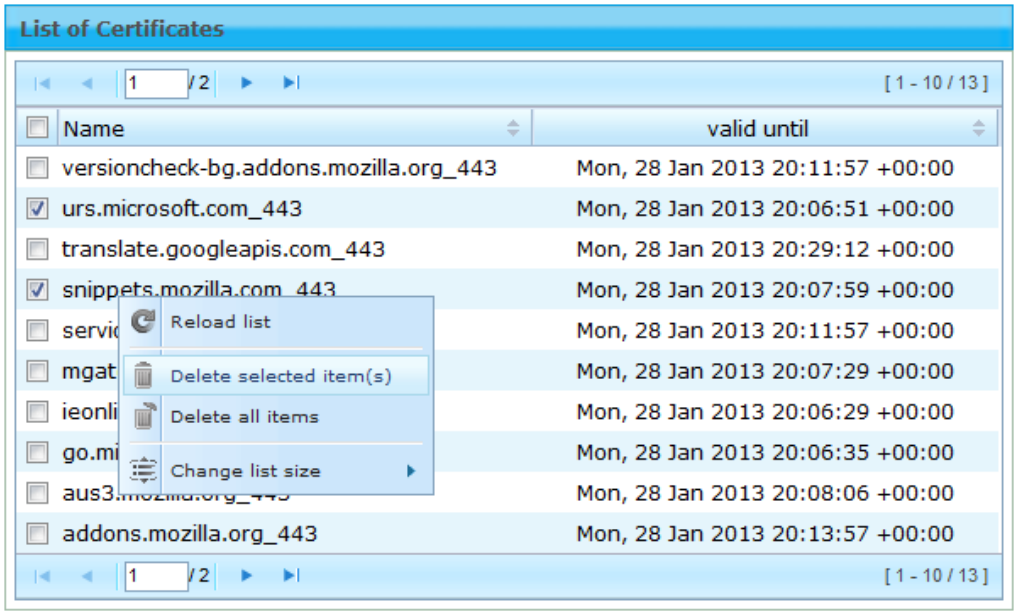

Figure 5.1. Certification store example

In the column *Name* can be seen the URL for which has been the certificate generated and the used port. In column *valid until* is the expiration date of the certificates. Any of the certificates can be deleted by selecting it with the check box, right clicking it and selecting *Delete selected item(s)*. Please note that normally there is no need to delete these items manually.

If a certificate is deleted, it will be generated again when the same web site is accessed again.

6. SSL Manager

As part of the SSL Interception process, the Secure Web tries to determine port and SSL protocol version to be used in the connection. This task is being accomplished by the SSL Manager.

The supported SSL versions are SSLv2, SSLv23, SSLv3 and TLSv1. Most of the connections use TLSv1 nowadays. However, some servers may still use older versions so they are present too, for compatibility reasons. The version SSLv23 is in the SSL Manager also called a *compatibility mode* and it is used when the SSL version cannot be determined. Connections with higher versions of TLS will always fall back into TLSv1.

To change settings of the SSL Manager, navigate to the menu *Services / Proxy Settings / SSL Intercept / SSL Manager*. An example of the dialog can be seen in the following figure:

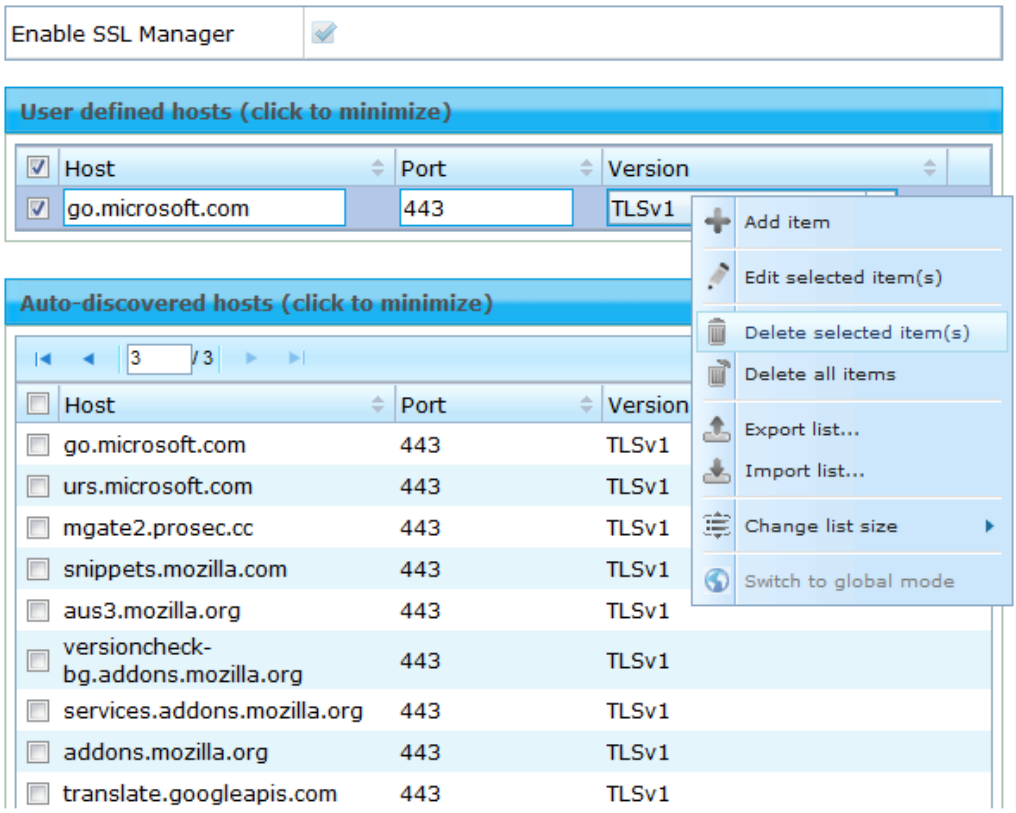

Figure 6.1. SSL Manager settings dialog

The option **Enable SSL Manager** allows to enable or disable the automatic discovery of the SSL connection properties. If the SSL Manager is disabled, the default *compatibility mode* (SSLv23) is used for all connections.

The list **Auto-discovered hosts** lists all the SSL secured web sites, that have been accessed in the past and the options, that have been set to these connections. These options cannot be deleted from the list, but they can be overridden by putting the same site in the *User defined hosts* list. This list always takes precedence over the *Auto-discovered hosts* list.

Any record from the *Auto-discovered hosts* list can be easily moved to the **User defined hosts** list by right clicking any desired record and selecting *Overwrite item(s)*. Records can be also managed from the right click context menu (as showed in the Figure 6.1, “SSL Manager settings dialog”). An example of setting options in the *User defined hosts* list can be seen in the following figure:

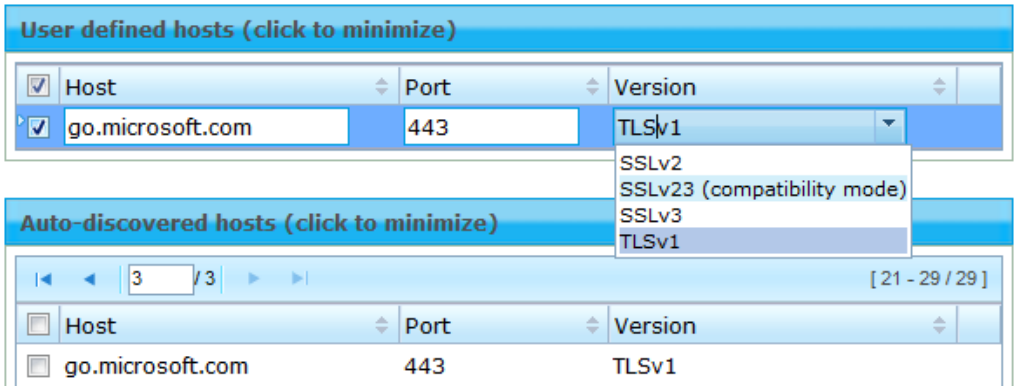

Figure 6.2. SSL Manager - User defined hosts

7. Troubleshooting

A web site using invalid certificate can be tested using the following link:

https://www.cacert.org

You can also easily verify, that the Virus scanning works even for SSL enabled sites. If you would like to test it, you can use the following site, containing the EICAR file:

https://secure.eicar.org/eicar.com

Please note that on the link above is just a testing code designed to test reactions of any virus-scanning engine. It does not pose any threat by itself.

A suggested solution of some of the common problems follows:

- **Your browser displays a warning for every HTTPS request:**
  - Did you supply the CA certificate to your browser? You need to do this for the browser to stop alerting. See Chapter 4, *Supplying the CA certificate to the web browser*.
  - Did you upload or create a new CA certificate on the Secure Web? If you did, you need to delete all certificates from the certificate store (see Chapter 5, *Browsing the certificate store*). Since Secure Web is caching the certificates for a few minutes, you need to wait until the cache entry is revalidated.
- **Secure Web does not accept your CA certificate:**
  - The supplied certificate must be in PEM format. Verify it is in the necessary format and that the file is not corrupted.
  - The private key contained in the certificate must not be password protected.
- **Some services do not work with SSL intercept enabled:**
  - The service could expect a certain certificate from the web server and since Secure Web does sent a generated certificate to the client it may not meet this expectation. You need to exclude the target of this service from SSL Interception. See Section 3.2, “SSL Intercept settings in Profiles”, *List of Trusted Hosts*.
  - Client certificates are not passed through Secure Web either. The communication between internal servers or services should be direct.
- **The CA certificate enrollment process for AD does not work:**
  - Verify that the GPO is linked to the right OU.
  - Verify that all the desired computers are in a group that is set in the GPOs Security Filtering option.
  - Verify that a WMI filter does not prevent the GPO to be applied.
  - Wait at least 20 minutes after the GPO is activated, then restart the targeted computers.

Appendix A. Contact data

A.1. How to contact our sales department

Tel.: +43 (1) 33933-0

Email: sales@cyan-networks.com

A.2. How to contact our support department

Tel.: +43 (1) 33933-333

Email: support@cyan-networks.com

A.2.1. Getting Support

In case you should have any technical problems, or questions and would like to get support from our team, we kindly ask you to provide us with the following information:

- Description of your question or problem
- The version information of the product:
  - The version information of Secure Web can be found after logging into the Web Admin Interface in the top part of the screen:

Figure A.1. Version information of the Secure Web

  - The version information of the Reporting System can be found after login in the top part of the screen of the Web Admin Interface:

Figure A.2. Version information of the Reporting System

  - All the information contained in the screen found in menu *Services* / *Services* / *Overview*
- In the case authentication is activated, provide us with the method in place (via Windows Agent, via Linux Agent, etc.)
- The deployment method of the Appliance (Out-of-line, In-Line, DMZ)
- The operation mode of the Appliance (dedicated mode, transparent mode)

- Information about the environment (proxy cascades that are used, firewalls and gateways involved in the infrastructure that are of relevance to the Appliance)

The appliance interface provides the possibility to create a support package that includes the configuration and log files of the system. This package can help us to track down the issue easier and faster. Please attach this package to your e-mail.

In order to create a support pack, navigate to menu *Appliances / Maintenance / Support* and click on the *Download* button. You may select the files you want to provide to our support team and then download a package, which we kindly ask you to send to our support email address.

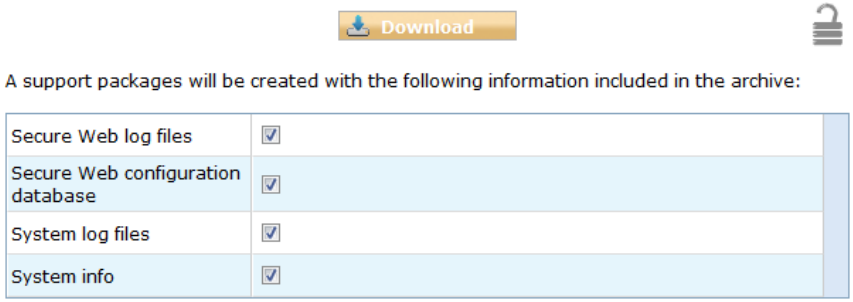

Figure A.3. Support Package

Further documentation about the product as well as technical white papers that describe certain use cases can be found in our documentation repository on our homepage:

http://www.cyan-networks.com/documentation