



SSL Intercept Mode

Certificate Installation Guide

Revision 1.0.0

Warning and Disclaimer

This document is designed to provide information about the configuration of CensorNet Professional. Every effort has been made to make this document as complete and accurate as possible, but no warranty or fitness is implied.

CensorNet Ltd does not accept any liability for poorly designed or malfunctioning networks.

Table of Contents

Table of Contents	2
Overview.....	3
Installing the CensorNet Certificate Authority	4
Downloading the Certificate Authority	4
Internet Explorer 7 and above – manual installation.....	5
Firefox 2.0 and above – manual installation	6
Importing Certificates using Active Directory Group Policy	7
Technical Support.....	8

Overview

CensorNet Professional v1.3 and above contains an SSL Interception mode which can be activated from the *System -> Configuration* menu within the CensorNet Control Panel. Once activated, the CensorNet proxy will intercept requests to HTTPS (SSL enabled) web sites, decrypt the page contents and filter it according to rules defined by the administrator. The act of interception replaces the requested Web server certificate with a certificate signed by the CensorNet proxy. This causes a browser warning to appear, such as the one shown below:-



This is the expected behaviour as the CensorNet proxy server is acting as a middle man between the client browser and the secure server in order to be able to decrypt the page contents.

This guide is concerned with providing instructions on how to stop the certificate warning from being displayed every time a secure Web site is requested through CensorNet with SSL Intercept Mode enabled.

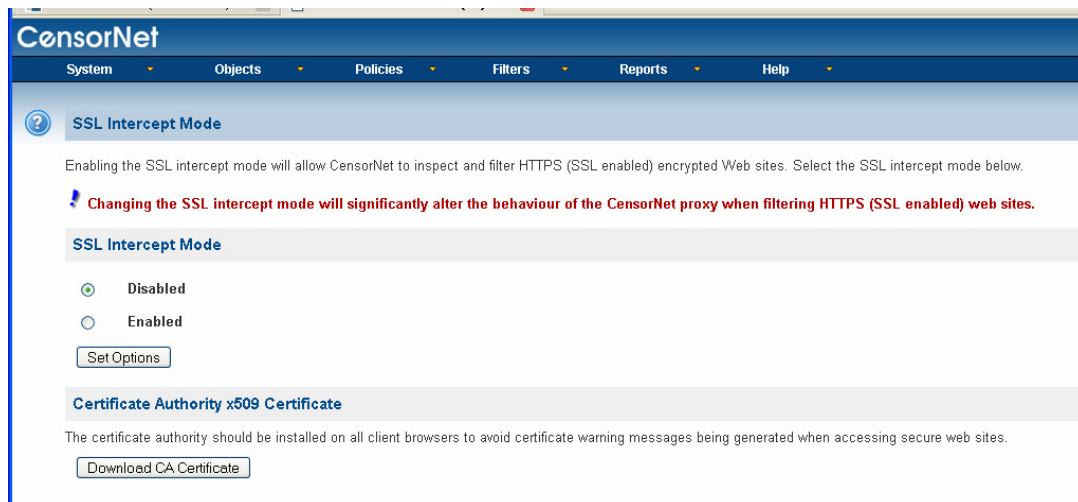
NOTE It is recommended that you make a statement in your Acceptable Usage Policy that informs users of your network that SSL interception is being performed as part of your Internet security policy.

Installing the CensorNet Certificate Authority

Downloading the Certificate Authority

To download the Certificate Authority:

1. Login to the CensorNet Control Panel.
2. Go to the "System" menu and select the "Configuration" sub-menu followed by the "SSL Intercept Mode" option.
3. The following screen will be displayed:

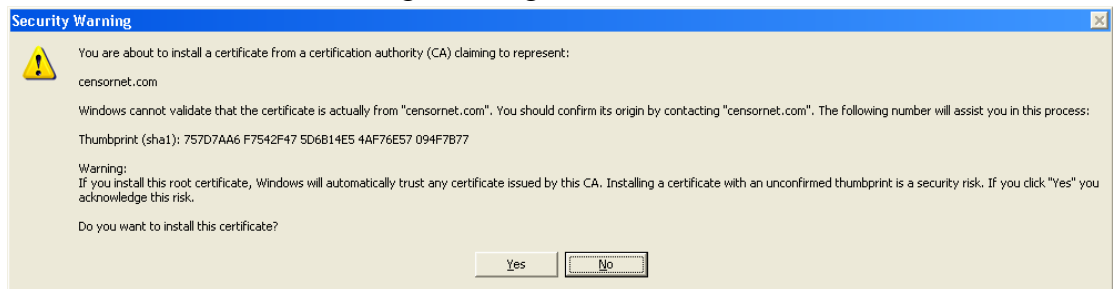


4. Click the "Download CA Certificate" button and save the "censornet_ssl_ca.pem" file to your computer.
5. You can now configure the client browsers by following the instructions in this document relating to the browser type in use.

Internet Explorer 7 and above – manual installation

To install the CensorNet Certificate Authority:-

1. Open Internet Explorer.
2. Choose *Tools* menu followed by *Internet Options*.
3. Click the “*Content*” tab followed by the “*Certificates*” button.
4. Click the “*Trusted Root Certificates*” sub tab.
5. Click “*Import*” then “*Next*” in the wizard.
6. Click “*Browse*” and locate the “censornet_ssl_ca.pem” certificate file downloaded from the CensorNet Control Panel. **N.B.** You may need to change the filter to display “All files *.*”.
7. Click “*Next*” followed by “*Next*” again and then “*Finish*” to install the certificate.
8. You will receive the following warning:-



9. Click “*Yes*” to import the certificate.
10. Close and restart Internet Explorer.

Firefox 2.0 and above – manual installation

To install the CensorNet Certificate Authority:-

1. Open Firefox.
2. Choose "Tools" menu followed by "Options".
3. Click the "Advanced" tab and then the "Encryption" sub-tab.
4. Click "View Certificates" button and then the "Authorities" sub-tab.
5. Click "Import" and locate the "censornet_ssl_ca.pem".
6. You will then be presented with the following dialog box:



7. Tick the first option to "Trust this CA to identify web sites" and then press "OK"
8. Press "OK" to exit.
9. Restart Firefox the changes to take effect.

Importing Certificates using Active Directory Group Policy

To install the certificate on every Web browser in the organisation would be extremely time consuming. Microsoft's Active Directory provides a method to distribute and install the certificate automatically on all computers in the domain.

1. Click *Start -> Programs -> Administrative Tools -> Active Directory Users and Computers*
2. In the left pane, locate the domain in which the policy you want to edit is applied.
3. Right-click the domain, and then click "*Properties*".
4. Click the "Group Policy" tab.
5. Create a new Group Policy by clicking on "New" and give the new GPO a name.
6. Click on the new object, and then click "*Edit*". A new window opens.
7. In the left pane, expand the following items: '*Computer Configuration*', '*Windows Settings*', '*Security Settings*', '*Public Key Policy*'
8. Right-click "*Trusted Root Certification Authorities*".
9. Select "*All Tasks*", and then click *Import*.
10. Follow the instructions in the wizard to import the certificate.
11. Click "*OK*".
12. Close the Group Policy window.

For further information please see your Windows Server / Active Directory configuration and user guide.

Technical Support

If you require assistance please contact our Technical Support department in the following ways.

Live Support <http://www.censornet.com/support>

Telephone 0845 230 9592 (9am-5:30pm Mon-Fri GMT)

E-mail support@censornet.com