



ClearTunnel (v1.2) Documentation

(The following graphics are screen shots from Microsoft® ISA Server 2004/2006 which is the property of Microsoft Corp. and are included here for instructive use. Some images illustrate ClearTunnel, which is the property of Collective Software.)

Table of Contents

ClearTunnel (v1.2) Documentation.....	1
Problem: Is your traffic sneaking through the “SSL Hole”?.....	3
Problems.....	3
Solution.....	3
Features.....	3
Requirements.....	4
Caveats.....	4
Help is Available!.....	4
Before Installation.....	5
Validate proxy configuration.....	5
Validate client configuration.....	5
Installation of ClearTunnel.....	6
Install Procedure.....	6
Troubleshooting.....	6
Install rolls back (with red error message at the end).....	6
Frozen or hung install.....	6
Configuring ISA to use ClearTunnel.....	8
Mode tab.....	8
Split Mode setups.....	9
About web chaining and ClearTunnel.....	9
Certificates tab.....	10
Choosing the Certificate Service.....	10
Firewall Policy considerations for Certificate Enrollment.....	11
Status “Please enter service IP and name”.....	11
Status “Need to request certificate”.....	11
Status “Need to install certificate”.....	12
Status “Need to renew certificate”.....	12
Status “Need to install renewed certificate”.....	12
Status “Certificate is installed”.....	12
Settings tab.....	13
License tab.....	15
Excluded Sites.....	15
Syntax.....	16
Demo/Lab mode.....	16

Understanding the “Local Host” workaround.....	16
Certificate renewal (normally after 2 years).....	17
Testing ClearTunnel.....	17
Troubleshooting.....	18
Support for ClearTunnel.....	18
Appendix A: Manual certificate steps.....	19
Acquire Subordinate CA certificate.....	19
Certificates mmc plugin.....	19
Installation of your Subordinate CA certificate.....	19
Certificate trust chain.....	20
Certificate Store Permissions.....	21
Certificate File Permissions.....	22
Appendix B: Upgrade Notes from ClearTunnel 1.1.....	23

Problem: Is your traffic sneaking through the “SSL Hole”?

Your organization uses ISA Server 2004 or 2006 in a “forward proxy” scenario for proxying, caching, controlling and filtering HTTP requests from clients on your LAN out to the public Internet. Your web clients are configured in one of two ways:

- Clients configured to use ISA as a proxy server, **or**
- Clients use ISA as their default gateway (i.e. Secure NAT mode)

ISA Server provides industry-leading HTTP application-level filtering capabilities, and can also leverage a rich community of third-party filters to achieve unprecedented control over your traffic at an extremely affordable value.

However, outbound HTTPS (SSL) web traffic can not be inspected by the ISA web proxy. This leads to the following issues:

Problems

- ISA's HTTP Filter rule settings cannot be applied to HTTPS (SSL) traffic.
- Third-party web filtering products that integrate into the ISA web proxy system cannot operate on the contents of SSL traffic. (The best they can do is allow or deny based on IP address/domain name).
- It is not possible to cache responses from forward SSL requests, therefore all traffic (even when the requests are for the same cacheable static content) is repeated for each user.
- Once an SSL tunnel is established between a client on your LAN and a server on the Internet, there is no way to monitor the data traveling in that tunnel. There is no way to detect, prevent, or control:
 - Unauthorized web requests (to prohibited or illegal content).
 - Viruses, trojan code, or browser exploits sent to your LAN from a malicious or compromised web server on the Internet.
- Many people mistakenly believe that the SSL protocol provides some security in these situations. On the contrary, SSL itself only provides assurance of the identity of the web server, and protection from eavesdropping on the contents of the SSL tunnel. SSL does not

Solution

Collective Software is proud to present ClearTunnel, a native ISA Server filter designed to solve all these problems, allowing you to **close the SSL Hole** in your organization.

Features

- ClearTunnel enables ISA Server to “see inside” all forward proxied SSL tunnels.
- Contents of HTTPS connections are exposed to the web proxy as normal HTTP requests/responses.

- Apply HTTP filter rules to HTTPS connections.
- Cache forward proxied HTTPS responses, decreasing your external bandwidth usage.
- Automatically compatible with most third-party web filters, enabling them to operate on HTTPS traffic as though it was HTTP.

Requirements

- ISA Server 2004 or 2006, used by your internal web clients as a proxy (either via proxy settings or Secure-NAT).
- Microsoft .NET Framework version 2 should be installed on each ISA server.
- An enterprise certificate service in your Active Directory environment.

In order for the browsers on your LAN to seamlessly work with ClearTunnel, the client workstations must trust your enterprise CA. This way they will automatically trust certificates issued by a properly-configured ClearTunnel system.

If you use ClearTunnel without this PKI in place, your client browsers will always display a warning when connecting over HTTPS. This is because they won't see the certificate issued by ClearTunnel as originating from a trusted source.

This requirement is substantively identical to the needs of any other forward proxy SSL inspection technology. It arises from design limitations of SSL encryption itself, which was not initially envisioned to provide support for forward proxies.

Caveats

- **The privacy laws of your country or locality may dictate limitations on the interception of encrypted traffic even on your own internal network. To protect your organization, please ensure that you follow all applicable laws! Collective Software does not offer legal advice.**
- ClearTunnel cannot inspect SSL connections that require a client certificate. This is because the certificate resides on the workstation itself, and cannot be "proxied" by ClearTunnel. Therefore the remote SSL server will not view a ClearTunnel connection as authorized, in situations where client certificates are needed. For these connections to work, they can be exempted from ClearTunnel via the [configuration](#).

Help is Available!

We are always happy to help you get our software set up and working. If you have questions or need assistance understanding/configuring/testing a Collective product, you can get in touch with our support staff quickly and easily. For the most up-to-date information, please see our Support page at <http://www.collectivesoftware.com/Support/>

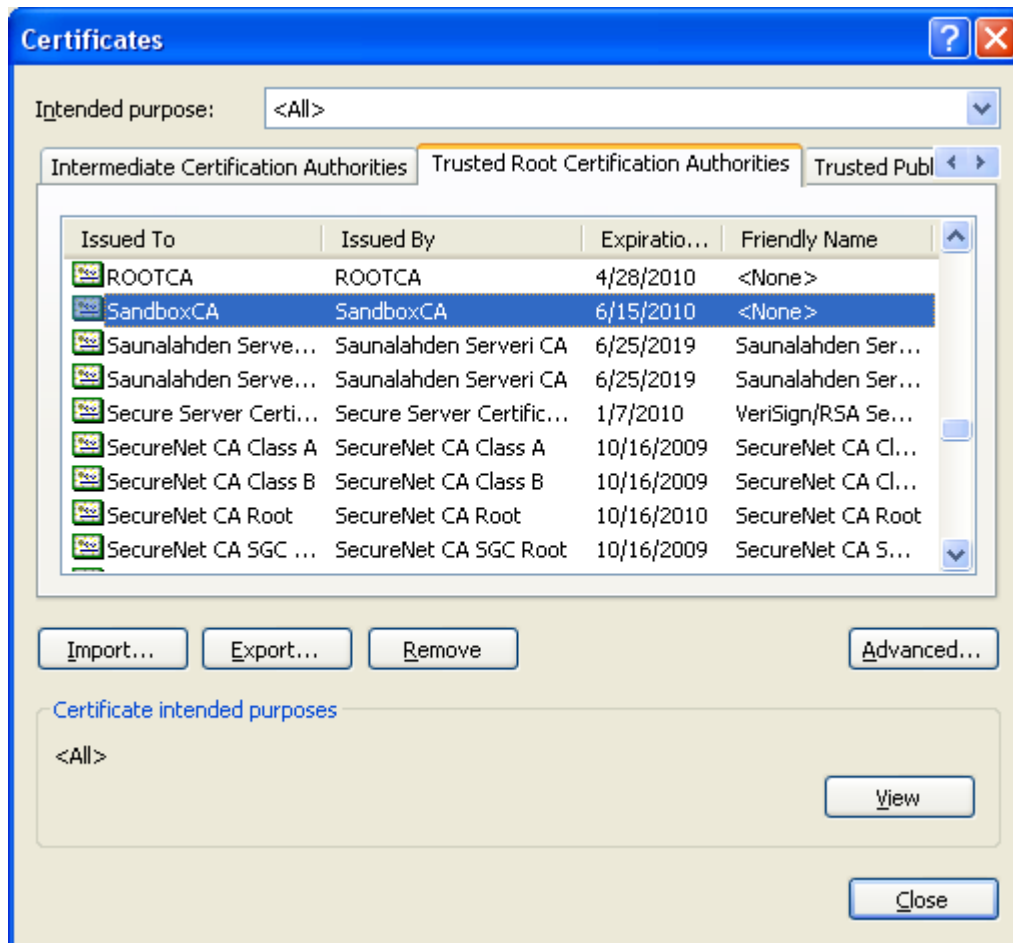
Before Installation

Validate proxy configuration

The ISA Web Proxy should be active and functioning on your internal network.

Validate client configuration

Verify that your web clients trust your root certificate authority. This can be done via Internet Explorer → Tools → Internet Options → Content → Certificates → Trusted Root Certification Authorities:



Verify that you can access HTTPS sites with your client machines. You should make sure these requests are “going through” ISA by viewing the web proxy log. If you require authentication to get out to the Internet, verify that the browser is prompting for those proxy credentials as you expect.

Ensuring all these things are in place and working will make any troubleshooting easier later on.

Installation of ClearTunnel

Install Procedure

1. Close the ISA management console if it's open.
2. Execute the ClearTunnel.msi file. This will stop your firewall service, install the ClearTunnel filters and interface software, register the filters, and then re-start the firewall service.
3. If your ISA installation is not in the default folder (i.e. If you have ISA on the D:\ drive, etc) then you can choose the Custom installation type and select the appropriate folder.
4. If you are installing over a remote desktop session, keep in mind that when the firewall service stops and restarts your RDP connection may be frozen, dropped or timed out. If an error occurs during the installation and the firewall service cannot be restarted, you will need to access the console to troubleshoot further (see below).
5. You must run the installer on each ISA server in an array separately, so they will all have the filter files installed and registered.
6. If upgrading from ClearTunnel 1.1, see the [upgrade notes](#).
7. If the installation completes with no errors, then you can proceed to the configuration section.

Troubleshooting

The installation normally completes without errors. However there are a few possible failure modes that can occur for this complex install process.

Install rolls back (with red error message at the end)

If you are presented with an error message on the final screen, then check out the application event log, which often will contain details on why the installation failed. The problem may be immediately solvable from this information, or you may need to work with Collective support for additional troubleshooting assistance.

Frozen or hung install

The installer tries to start the firewall service after it is done registering the filter components. In rare cases, everything may register properly but there could still be a problem preventing the firewall service from starting. In this situation, the installation may appear to hang on the "Starting services..." item. This is because it is trying repeatedly to start the service, and failing. In fact if you look at the application event log, you will see several errors from the firewall service as it tries to start. These messages may help identify the cause of the problem.

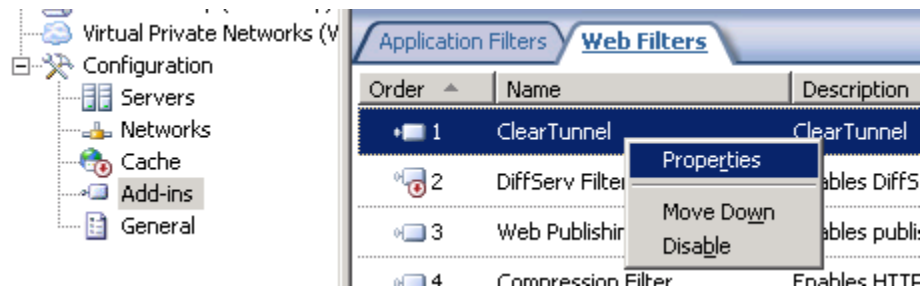
The install should eventually give up on starting the service, but it may take a long time. If necessary, you can expedite the rollback by going into the services control panel and setting the Microsoft Firewall service to Disabled temporarily (and applying that

change). This will cause the installer to quickly give up, and it should then correctly roll back the installation while leaving the firewall service down. After this happens you can then re-enable and restart the firewall service.

This kind of problem should not normally occur, and will probably require additional troubleshooting by Collective support. However if you are able to fix the problem you can re-run the install safely after completing this procedure.

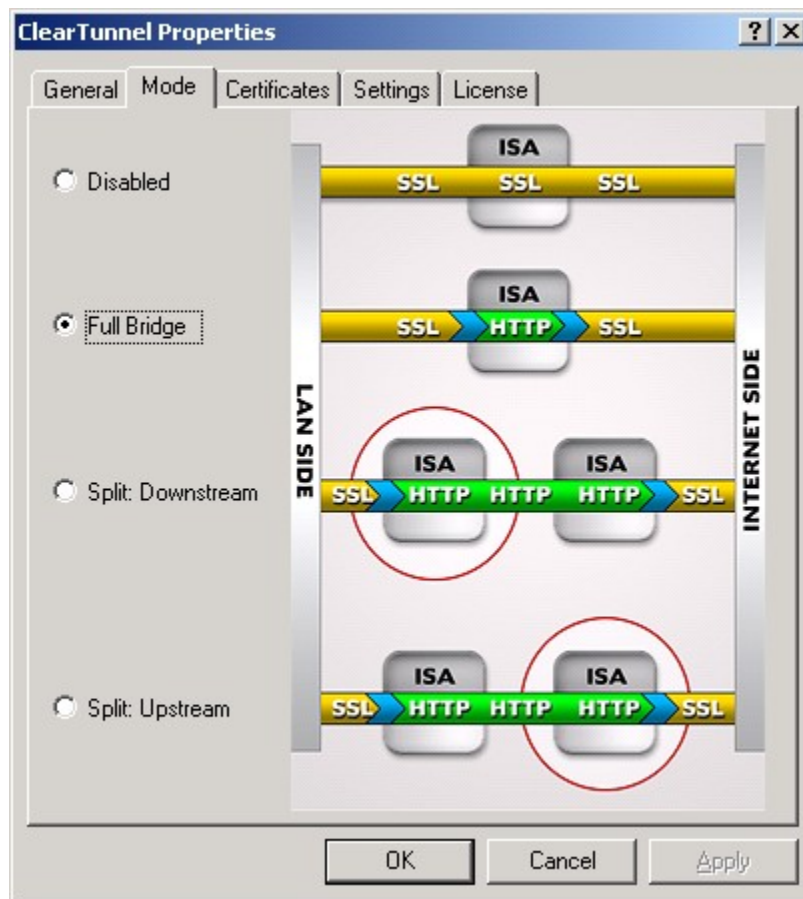
Configuring ISA to use ClearTunnel

Navigate to the web filter configuration section under Configuration->Add-ins->Web Filters, and select the ClearTunnel properties:



Mode tab

Click on the Mode tab and you should see the following view:



You have the following choices:

- **Disabled:** ClearTunnel will not inspect SSL traffic, and the ISA web proxy will operate normally. If you want to keep ClearTunnel installed but disable it from affecting your traffic, choose this mode. This is the mode that the filter installs in by default.

- *Full Bridge*: For most simple installations this is the correct selection. It means that both the decryption and encryption steps are performed on the same server/array.
- *Split- Downstream*: You have a web chaining setup and this is the downstream server/array, closest to the web clients.
- *Split- Upstream*: You have a web chaining setup and this is the upstream server/array, closest to the Internet.

Split Mode setups

In split mode, the settings of two separate ISA servers/arrays must be configured so that:

1. Web requests received at Downstream are routed to the Upstream array.
2. Authentication (if any) is performed on the Downstream array.

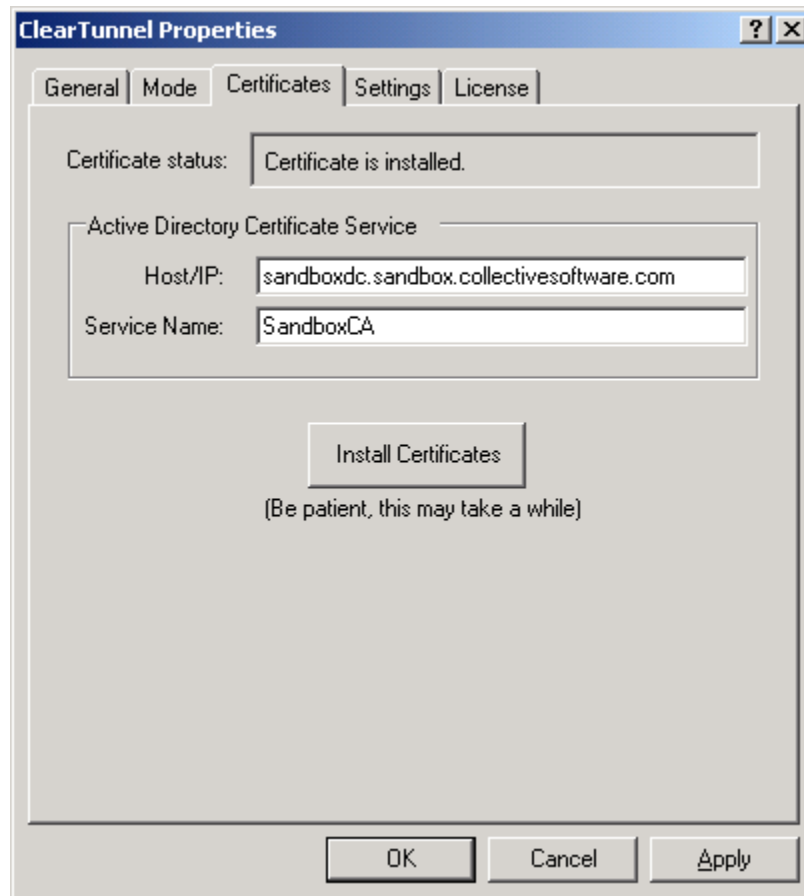
Troubleshooting Split mode setups can be challenging due to the number of places the configuration can “go wrong”, so don't hesitate to ask for support if you are stuck at this step! For easiest troubleshooting, you should get the web chaining to work first, and then install and configure ClearTunnel afterwards.

About web chaining and ClearTunnel

In chaining setups, the traffic between the two ISA servers in the chain will (by default) be **unencrypted**. This feature exists so that you can use a network IDS/IPS on the link between the servers and inspect traffic that would normally be encrypted in the HTTPS tunnel. If you want the inter-proxy traffic to be secured, then you can set up ISA's proxy chaining rules to send all the traffic over SSL between the two proxies. That configuration is recommended when the chained traffic must cross over a public WAN, or other unsecured link.

Certificates tab

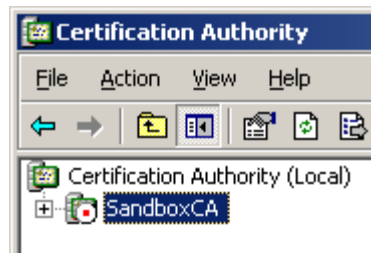
ClearTunnel needs to act as a trusted certificate authority in order to create and sign web server certificates that your internal browsers will trust as being authentic. The Certificates tab includes a wizard that tries to guess correct settings and perform as much setup automatically as possible. (There is also a [list of manual steps](#), that can be followed if for some reason the wizard cannot be used.)



Choosing the Certificate Service

On the first ISA server in your array (or the only one, for ISA-SE installations), you will need to request a certificate from your enterprise Microsoft Certificate Services server. The "Certificate status" readout will show that the certificate needs to be requested.

If your ISA is a member of the Active Directory, the wizard should detect the location and name of an issuing certificate server for your domain. If it does not identify the correct service that you want to use, then you can adjust those fields. For non-member servers, you will always need to set this information manually. If not detected, enter the IP address of the certificate server. The service name can be found from the Certification Authority mmc snap-in:



Firewall Policy considerations for Certificate Enrollment

For most installations, the ISA server will not have a policy rule that allows it to connect to your certificate server over RPC and obtain the certificate. Creating a tightly defined rule for this RPC access is a multi-step and error-prone process. Instead, you could simply consider making a temporary access rule from *Local Host* to the certificate server and allow *all outbound protocols*. As soon as you complete the certificate enrollment on the first ISA server, you can remove that rule.

In the following sections we will cover the various status readouts that the Certificate wizard can display, and what tasks need to be performed for each one.

Status “Please enter service IP and name”

The certificate service could not be auto-detected. See above for manual entry steps.

Status “Need to request certificate”

This is a new installation, and certificate enrollment has not yet been completed.

Click the Install Certificates button and the wizard will attempt to perform certificate enrollment, as well as install the certificate, the trust chain, and set permissions on the local machine that are needed for certificate access.

Possible results:

- *All tasks finished*: The certificate was installed and is ready for use after you apply the ISA configuration changes.
- *Could not connect to certificate service*: Either the certificate service IP/name is incorrect, the service is not operating, or the firewall policy rules have blocked the enrollment request (see above section).
- *Enter Credentials*: An enrollment request needs to be done, but the logged-in user does not have permission to request a subordinate CA certificate from the certificate services. Enter credentials of a more powerful user who has that permission. These credentials are not stored in your configuration, they are only used for the certificate request and then forgotten.
- *An exception occurred*: Certificate request/installation is very complicated and the wizard performs many steps behind the scenes. For most users it will work if you follow the above instructions. However if you get an error and can't determine the cause/solution, then you can create a support ticket and we can help you to diagnose the issue.

Status “Need to install certificate”

After a successful enrollment on the first server, your ISA configuration will store a copy of the certificates. This means on other array members you need not request new certificates, the first one will be re-used. However you **must still install the certificate on each ISA server separately**: unfortunately there are many steps that cannot be “pushed” automatically to each server.

So on each server in your array after the first one, come to the Certificates tab and again click the “Install Certificates” button. The necessary steps to install and configure the certificates will be performed.

Status “Need to renew certificate”

This means the signing certificate will expire within the next 6 weeks, so you should request a new one by clicking the button “Renew Certificate”. Possible results are the same as above in the “request certificate” section.

Status “Need to install renewed certificate”

After the first server successfully gets a renewed certificate, your ISA configuration will store a copy of the certificate. This means on other array members you need not request renewed certificates, the first one will be re-used. However you **must still install the renewed certificate on each ISA server separately**: unfortunately there are many steps that cannot be “pushed” automatically to each server.

So on each server in your array after the first one, come to the Certificates tab and again click the “Install Certificates” button. The necessary steps to install and configure the certificates will be performed.

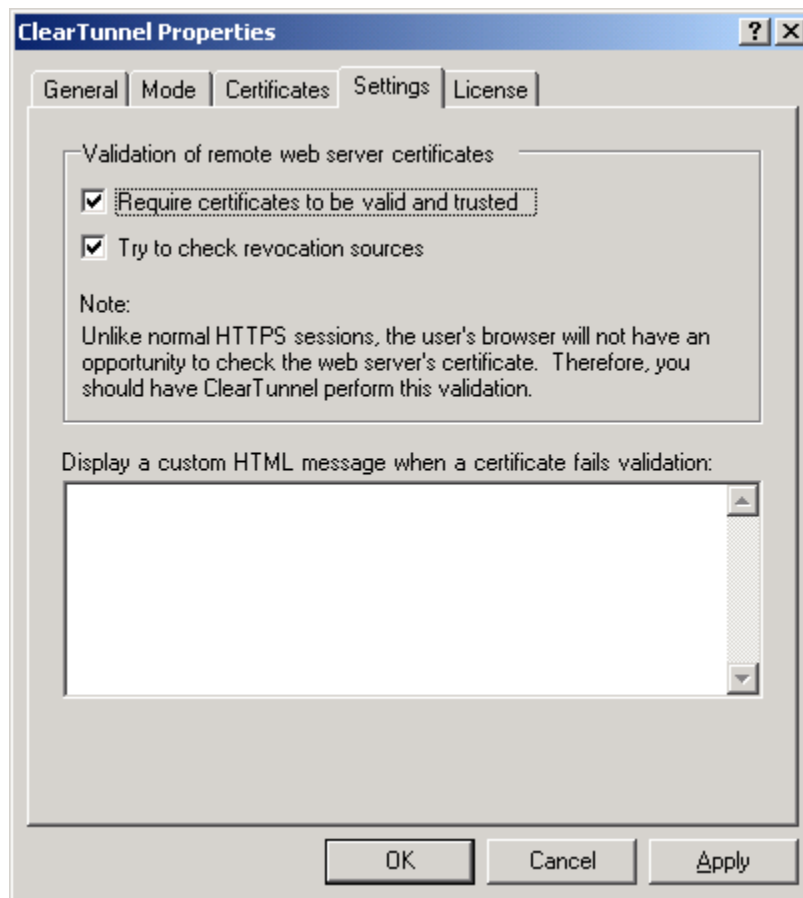
Status “Certificate is installed”

The signing certificate is installed on this host. Normally this means everything is OK and no further action is required here.

In some instances you may suspect that the certificate permissions have been changed, or some other certificate-related problem has occurred. If you click the “Install certificates” button here, and all the installation and setup tasks will be performed again, to get the machine's certificate configuration back to a good state. As long as the certificate is cached in the ISA configuration and not within 6 weeks of expiring, then a new request will not be made to the certificate service. Otherwise, a fresh request will be performed.

Settings tab

After the certificate infrastructure is set up on the ISA box, there are some other settings to go over:

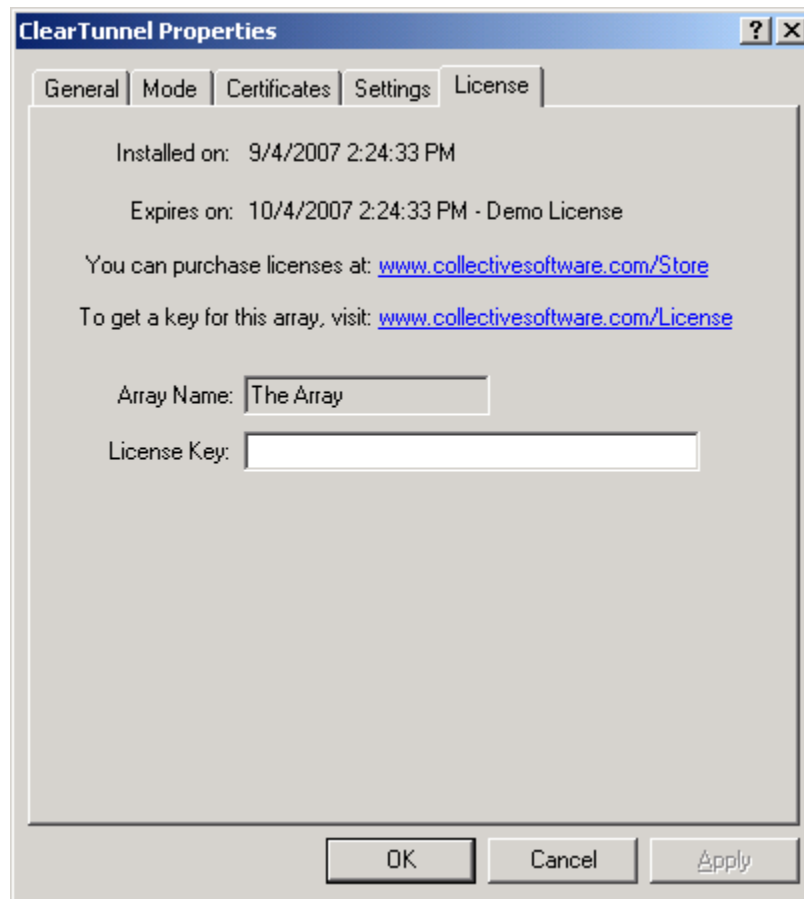


- *Require certificates to be valid and trusted:* When this is checked, ClearTunnel will use ISA's local machine certificate store to verify the identity of remote web servers. If you uncheck this field then there will be no checking of certificate validity at all. Since the browser is receiving a different certificate than the one on the remote web server, the end user won't have a chance to check the certificate validity. Therefore we recommend that this setting remain turned on. On a Downstream mode ClearTunnel server, this setting is not used.
- *Try to check revocation sources:* If you select to check revocation sources then ISA will attempt to confirm whether the certificate has been revoked by its issuer. This normally entails making additional connections to the Internet, and may require you to apply the appropriate system policy or firewall policy rule. If the revocation check cannot be run (i.e. If the server cannot be contacted, etc.), then this check will be skipped over. On a Downstream mode ClearTunnel server, this setting is not used.
- *Custom HTML Message when certificate fails validation:* When ClearTunnel determines that a certificate is invalid or not issued by a trusted source, an HTML error message is sent to client browsers. This message can be replaced by custom HTML markup you enter into this field. On a Downstream mode

ClearTunnel server, this setting is not used.

Former ClearTunnel 1.1 users: If you are wondering where the proxy port setting went, see the [upgrade notes](#).

License tab



The License tab is used to check how long remains in the evaluation period, and to activate a permanent license.

To be eligible for a license key, you need to purchase license(s). You can do this on our [web store](#) or by [contacting us](#).

Once you have available license(s) you can request a key for your array (or single server) at our [licensing page](#). When requesting a license key, you will need to tell us the name of the ISA array, which is indicated on this dialog. The exact name is important, because it will be used to validate the key.

The license key is sensitive to the number of servers in the array. For example if you begin with only 2 servers in the array but plan to have 4, you can purchase 4 ClearTunnel licenses and request a license key for a 4-server array. Then as you bring future servers online, they will be licensed automatically (you still need to [install the certificates](#) though.) **Warning:** if you install more servers than you have licensed then the license key will be seen as invalid, and the servers will begin to operate in [demo/lab mode](#). So if you need to add more servers to a live array then you should acquire and apply your new license key in advance, so this behavior does not take place.

Excluded Sites

Your organization may require certain SSL traffic to pass through ISA without being

inspected, as in the following cases:

- Applications which operate on port 443 but do not use the HTTP protocol.
- Sites which require a client certificate for authentication (since ClearTunnel cannot obtain the client's private key, there's no way to “proxy” this certificate).
- Sensitive traffic that you do not wish to be inspected.
- Content that you do not wish to have cached (however you could also just use the cache rules to exclude that traffic).
- If a particular SSL site or application is malfunctioning as a result of being proxied through ISA. Some apps assume that since they are operating in SSL that they will necessarily be talking directly to the end client, and may become confused when they encounter an HTTP proxy along the way.

ClearTunnel uses an ISA “domain name set” to keep track of what servers and domains should be allowed to “pass through” without being inspected. You can access this list via the Network Objects toolbox section, under the “Domain Name Sets” item. The set is named “ClearTunnel Excluded Sites”.

Syntax

You can enter exact server names, or also use an asterisk (*) as the first character to denote all machines in that domain. Please note the following limitations:

- You can't use the wildcard (*) anywhere else except at the left (the first character). Otherwise it will just be treated as part of the real server name, which isn't what you want.
- If you have an entry “*.example.com” this will match www.example.com and foo.example.com, but it will **not match** “example.com” (note that there's no “dot” so the pattern doesn't match). To match example.com too, you can either include a second item “example.com”, or else you could use the expression “*example.com” (no dot after the star). The problem with the latter is that it would also exclude any site such as foexample.com. Depending on the specifics of your situation, that behavior may or may not be considered negative.

Demo/Lab mode

When the evaluation period expires (after 30 days) or when an invalid license key is used, ClearTunnel runs in demo/lab mode. In this mode the filter will work normally for a period of 2 hours from the starting of the Firewall Service, and then report a “license expired” message to client browsers after that period. This mode is meant to be useful for test labs where you don't wish to purchase licenses but still want to be able to run meaningful test setups. After 2 hours, you can restart the firewall service and the lab timer will reset again.

Understanding the “Local Host” workaround

All revisions of ISA server 2004 and 2006 (where the component version is less than 5.0.5721.250) have an issue that affects the operation of ClearTunnel. This problem is detailed in the following Microsoft Knowledge Base article:

<http://support.microsoft.com/kb/941634/>

The effect of this bug is that the Web Proxy cannot process ClearTunnel's decrypted traffic. In order to make ClearTunnel 1.2 and later work in this situation, you can either use a workaround or update ISA Server 2006 to a version that contains the fix for this problem.

Please refer to the following knowledge base article for more information and instructions:

<http://collectivesoftware.com/Support/KB/article/26>

For best results, we *highly recommend* obtaining the updated ISA build via hotfix (or service pack, not available at the time of writing).

Certificate renewal (normally after 2 years)

Note: ClearTunnel versions prior to 1.2.17 do not support certificate expiry notification and renewal features. All users are strongly encouraged to update to 1.2.17 or later to take advantage of these very important features.

Certificate authorities typically grant certificates that are valid for some period of years. The Microsoft CA defaults to a 2 year life span for subordinate CA signing certificates. This is important, because ClearTunnel uses a subordinate CA certificate to impersonate web sites during the course of its operation. If the ClearTunnel certificate is allowed to expire, then ClearTunnel **cannot function** until it is renewed.

When the signing certificate reaches 6 weeks before the end of its validity period, you will receive an ISA Alert each time the firewall service starts, advising you to renew the certificate. This can be done in the [Certificates tab](#). The ClearTunnel Certificate wizard will attempt to renew using the same keys as the old certificate. If the keys cannot be found, you will receive an error message. In that case, [a manual process](#) must be followed.

If you are able to configure your CA to grant a long validity period before requesting the initial signing certificate, this renewal process need not occur as frequently. Detailed control of the certificate service is beyond the scope of this document. However, to change the default issuing period to 5 years, you would execute the command:

```
certutil -setreg CA\ValidityPeriodUnits 5
```

Certificate templates also limit the validity interval for requests. But in this case, we use the "SubCA" template, which itself already defaults to 5 years.

Testing ClearTunnel

Once the above settings have been applied, you can use a web browser on the *Internal* network to test the ClearTunnel configuration. Close all browsers on the desktop first, to ensure you get a fresh connection.

When connecting to an HTTPS site in a properly configured environment, the browser will not display any security warnings to the user. You can verify that ClearTunnel is processing the connection by viewing the certificate used in the browser session (double-click the little lock icon).

The “Issued by” field should contain the name “ClearTunnelSigning”.

The “Certification Path” should list a tree hierarchy of CA's starting with your root CA and ending with the web server certificate itself. If you do *not* see a list here, but rather only the name of the certificate itself, then the trouble most likely is that you haven't [configured the CA chains](#) exactly right on the ISA server. In general if you are using the Certificate tab, and it worked without producing error messages, this is a situation that should not occur.

If you receive a security warning about the certificate not being trusted, then it is likely this browser does not have your root CA set as a trusted root authority. For domain members using Internet Explorer, this type of issue shouldn't occur, because the root issuing CA certificate is pushed out to domain members during their group policy update. For non-members, or for alternate browsers that use their own separate certificate storage location, you may need to manually install the root CA certificate to mitigate this issue.

Troubleshooting

The first place to look if something seems to be working incorrectly is the ISA alerts tab in the Monitoring section. Often this will directly indicate the cause of the problem. This information will also be required in almost all cases if you need support.

Support for ClearTunnel

Collective is proud to offer support for ClearTunnel, whether you need help getting a configuration working, find a bug, or just have a feature question.

Support is available from our web site at <http://www.collectivesoftware.com/Support/>

- *Knowledge Base*: When our staff answers questions that will apply to the whole community, they will often create a permanent KB item to disseminate this knowledge. There is a Search feature here; you can also easily browse by topic. To get fast answers to FAQs (frequently asked questions) the knowledge base is the best place to start.
- *Support ticket*: We are always happy to help you get set up and working. If you have questions or need assistance understanding/configuring/testing a Collective product, you can get in touch with our support staff quickly and easily. For the most up-to-date information, please see our Support page.

Appendix A: Manual certificate steps

In some instances the certificate wizard shipped with ClearTunnel may be inadequate to set up your environment. Therefore we reproduce the steps of the wizard below in a manually-applicable, though tedious, fashion. **You should not need to do these things unless you are unable to use the Certificate wizard.**

Acquire Subordinate CA certificate

ClearTunnel's internal software behaves as a certificate authority, issuing and signing web server certificates for the consumption of your internal web clients. In order for ClearTunnel to be a recognized, trusted CA for your enterprise, you need to obtain a special certificate from your enterprise CA and install it on ISA. You can obtain this certificate from any CA in your enterprise that is authorized to issue subordinate CA certs.

Please Note: We are not talking about installing Certificate Services on the ISA box, or creating a subordinate CA “server”. All you need is to obtain a public/private key pair for a Subordinate Certificate Authority from an issuing CA in your enterprise. We just want the certificate, we don't want to provision an entire cert server.

Detailed assistance on the Microsoft PKI is outside the scope of what Collective Software is able to provide, however obtaining a sub-ca certificate from an enterprise cert server's web tool is one easy way to do it.

The subject name of the subordinate signing certificate you request should be “ClearTunnelSigning”. If you need to use a certificate with a different name this is possible, please contact support.

When you request your key pair from the CA, **be sure to specify that the keys should be exportable**. Even if you are requesting the certificate via web browser on the ISA box, you still need to do this so that you can import the cert into the proper place later.

Once you are issued the certificate, you need to export it **with private key**, to a .pfx file. You should *also* export a separate .cer file containing just the public key.

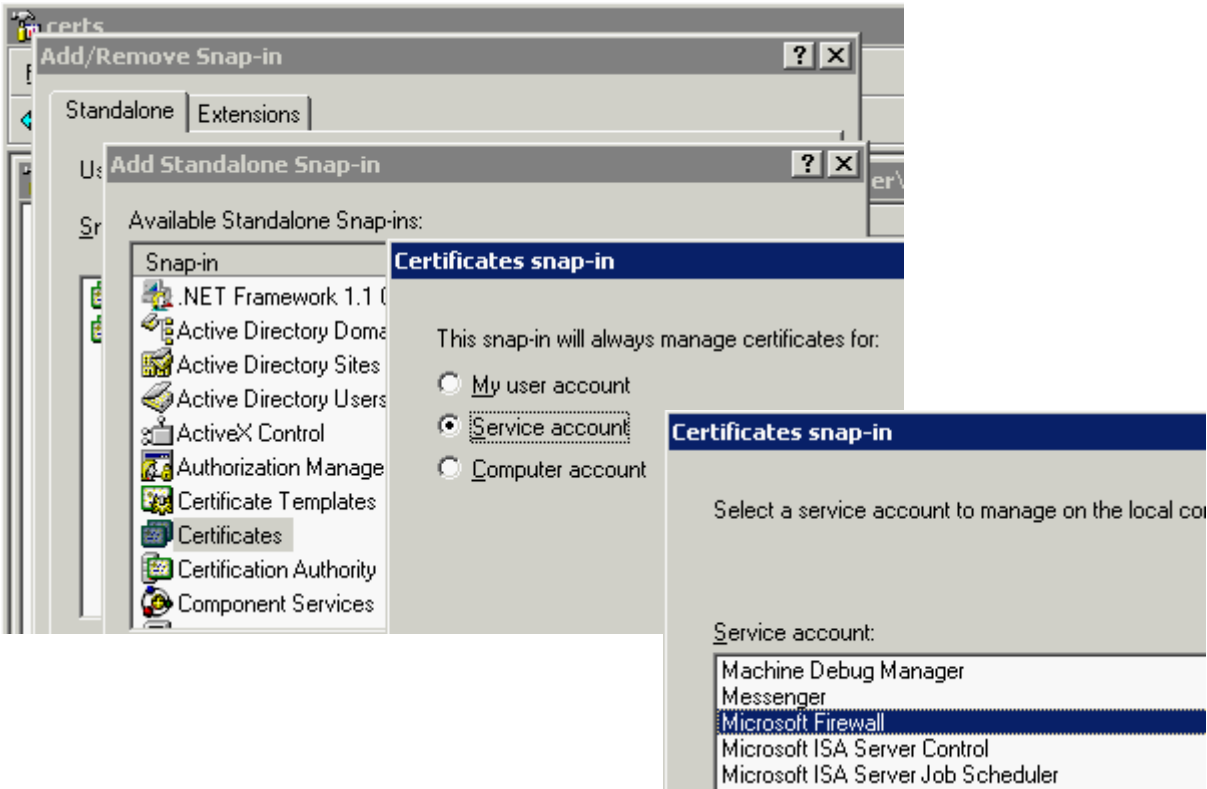
Certificates mmc plugin

Note: The certificate mmc plugin offers a “copy and paste” feature, *but we have found it to be unreliable in terms of setting the correct permissions*. In essence it works correctly, but in subtle ways that are easy to get wrong. Therefore, we recommend **always using export/import** instead of this copying functionality.

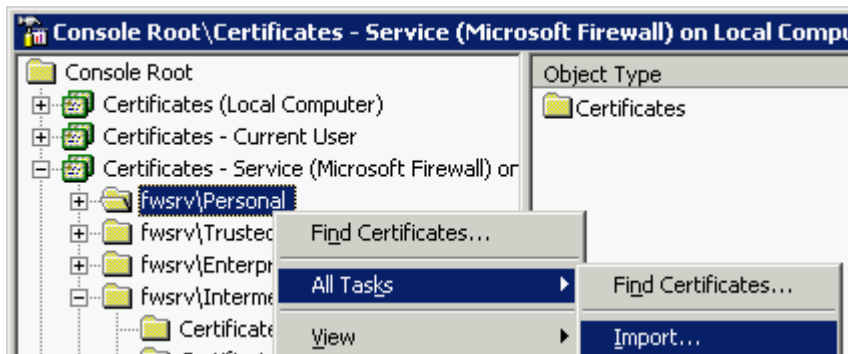
Installation of your Subordinate CA certificate

You must import the public/private key .pfx file into the firewall's “Personal” container.

On the ISA server, connect to the “Microsoft Firewall” service certificate store mmc plugin:



Right-click on the fwsrv\Personal container and select Import:



Locate the .pfx file and import it into this container. Once the import is completed, open the certificate (by double clicking on its name) and make sure the dialog indicates that the private key is installed.

Next, you need to place (at least) the public key for this sub-ca certificate into the “Intermediate” container of the Microsoft Firewall store. This is necessary so Windows can associate the created certificates to the trusted chain (see below). To accomplish this step you could import the .pfx again into the other container, or just export the public key only (recommended to minimize locations the private key is stored!) and import it here.

Certificate trust chain

Next you must install the whole certificate chain of the CA that issued the subordinate

CA certificate to you. This can be done via the Certificate Server web tool. After running that, the root and intermediate CA public certificates are installed into the “user account” certificate store. For some configurations, this will also place the certs into the Local Machine and Microsoft Firewall stores.

If not already present automatically, then you must import all the public keys for the chain into the Local Computer store manually (You can access this store by adding another certificates plugin to your mmc window, as shown above). Make sure your root CA is listed in the “Trusted Root Certification Authorities” container of the store, and any intermediate CA's are listed in the “Intermediate Certification Authorities” container. We recommend exporting the public keys for these certs from your personal store, and re-importing them into the new store.

These import procedures must be repeated on each ISA server in an array.

You **do not** need to install the entire certificate chain on your web clients, but the root CA must be in the Trusted Roots container as [specified above](#).

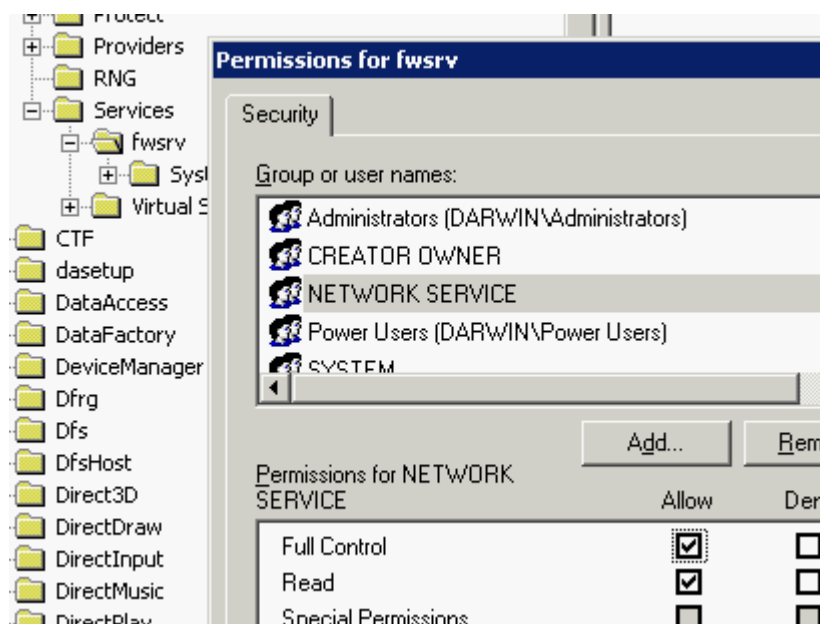
Certificate Store Permissions

You need to give the NETWORK SERVICE account full permissions to access the Microsoft Firewall certificate store, since ClearTunnel will be creating certificates and writing them to that location.

In Regedit, browse to the key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\fwsvr

and in the fwsvr properties, add Full Control permissions for the NETWORK SERVICE account, as shown:



This procedure must be repeated on each ISA server in an array.

Certificate File Permissions

When you import and install the subordinate CA certificate onto the ISA server, its private key will need to be readable by the "NETWORK SERVICE" account. **This permission is not ordinarily set on the private key file by default.** To correct this problem, you should take the following actions:

- In Explorer, go to: C:\ Documents and Settings\ All Users\ Application Data\ Microsoft\ Crypto\ RSA\ MachineKeys
- Examine the files' permissions. There is one file that corresponds to each certificate in the local machine store that has a private key.
- Annoyingly, the files are not named in any human-readable fashion. It is often easiest to figure out which one belongs to which certificate by looking at the file timestamps. The key file for a certificate you just recently imported will have a very recent modified time.
- Add the NETWORK SERVICE user to the appropriate file's permission, giving that user "Read" access.
- **Do not broadly add permissions** to the other files, or the MachineKeys folder itself, as that would be a security risk. The ability to access private key data could be useful to a malicious user or program, who could then use that information to assume the identity of any of those certificates.
- This must be repeated on each ISA server in an array.

Appendix B: Upgrade Notes from ClearTunnel 1.1

Version 1.2 doesn't need to use its own separate proxy port. It just observes the normal tcp/8080 port that ISA uses (or whichever port number you have configured).

When you install version 1.2 it will try to figure out if you were using a unified port setup before with CT listening on 8080. If so it will put the proxy port settings back to normal.

But this isn't foolproof because there are many ways to have the various ports configured. So after installation of CT 1.2, you should confirm that the web proxy on the internal network is listening at 8080, or whichever port your clients expect.

Appendix C: Command line certificate management

You can execute the tool InstallCert.exe (in the ClearTunnel folder after installation) to perform the same steps as on the [Certificates tab](#).

Optional Arguments

- /CertServer:<fqdn or ip>
- /ServiceName:<Certificate authority name>
- /PFX:<path to pfx file containing signing certificate>
- /PFXPassword:<your password> (skip this option if the password is empty)
- /Chain:<path to base-64 encoded certificate trust chain>

Notes

If you are requesting certificates, you must be logged in with an account that has permission to do so. Also, [the firewall must allow this traffic](#).

In a multi-server enterprise array, after you request and install the certificates on the first server, they are also stored within the ISA configuration. You still must run the Certificate wizard or InstallCert.exe on each array member. But after the first server, you don't need to contact the certificate service any more or manually specify pfx/cer files, because they can be read out of the ISA array configuration.

The .cer file for the trust chain must be base-64 encoded, not DER encoded.

Examples

To do the exact same steps as the [Certificates tab](#):

```
InstallCert.exe
```

It will attempt to detect the certificate server, install the signing certificate (if necessary) and the trust chain, and set appropriate permissions on the certificate store and private key file.

```
Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator.SANDBOX>cd "\Program Files\Microsoft ISA
Server\Collective Software\ClearTunnel"

C:\Program Files\Microsoft ISA Server\Collective Software\ClearTunnel>InstallCer
t.exe
Need to request certificate.
Requesting certificate...
Requesting trust chain...
Installing trust chain...
Removing old certificate, if any...
Importing new certificate...
Setting store permissions...
Setting private key file permissions...
All tasks finished.
Checking...
Certificate is installed, expires 7/5/2010 2:09:46 PM

C:\Program Files\Microsoft ISA Server\Collective Software\ClearTunnel>
```

To specify the certificate service, if it cannot be detected:

```
InstallCert.exe /CertServer:192.168.4.70 /ServiceName:sandboxDC
```

You can import the certificate from a PFX file, but still get the trust chain by contacting the certificate server. You can specify a pfx password; here we quote that argument so the apostrophe does not get interpreted by the command shell.

```
InstallCert.exe /PFX:c:\ThePfxFile.pfx "/PFXPassword:1'abaoe"
```

You can also specify the trust chain. It must be one or more certificates that are base-64 encoded together in a single file. Usually there will be one certificate for each intermediate authority, and the root certificate.

```
InstallCert.exe /PFX:c:\ThePfxFile.pfx /Chain:c:\TheChain.cer
```