



ClearTunnel 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 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!.....	5
Before Installation.....	5
Validate proxy configuration.....	5
Validate client configuration.....	5
Installation of ClearTunnel.....	6
Install Procedure.....	6
Troubleshooting.....	6
Automatic activation doesn't work?.....	6
Install rolls back (with red error message at the end).....	7
Frozen or hung install.....	7
Configuring ISA to use ClearTunnel.....	8
Web Filter position.....	8
Configure ClearTunnel settings.....	8
Setting up the Certificates.....	9
Credentials.....	10
Certificate Server Identity.....	10
Details of Signing Certificate.....	11
Running on each array member, or running after a re-install.....	11
Running the wizard.....	11
Permission to Access Certificate Server.....	12
Other Settings.....	12
Excluded Sites.....	13
Syntax.....	13
Exclusion caching, and SecureNAT.....	13
Testing ClearTunnel.....	14
Troubleshooting.....	14
Support for ClearTunnel.....	14

<u>Appendix A: Manual certificate steps.....</u>	<u>16</u>
<u>Acquire Subordinate CA certificate.....</u>	<u>16</u>
<u>Certificates plugin.....</u>	<u>16</u>
<u>Installation of your Subordinate CA certificate.....</u>	<u>16</u>
<u>Certificate trust chain.....</u>	<u>17</u>
<u>Certificate Store Permissions.....</u>	<u>18</u>
<u>Certificate File Permissions.....</u>	<u>19</u>

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).
- An enterprise PKI (trusted Certificate Authority infrastructure) 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

- Web chaining is supported only when ClearTunnel is deployed at the central site, not on the remote sites. Support for additional chaining scenarios is planned for a future release.
- **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](#).
- RPC/HTTP traffic needs to be excluded from inspection due to a technical limitation.

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/>

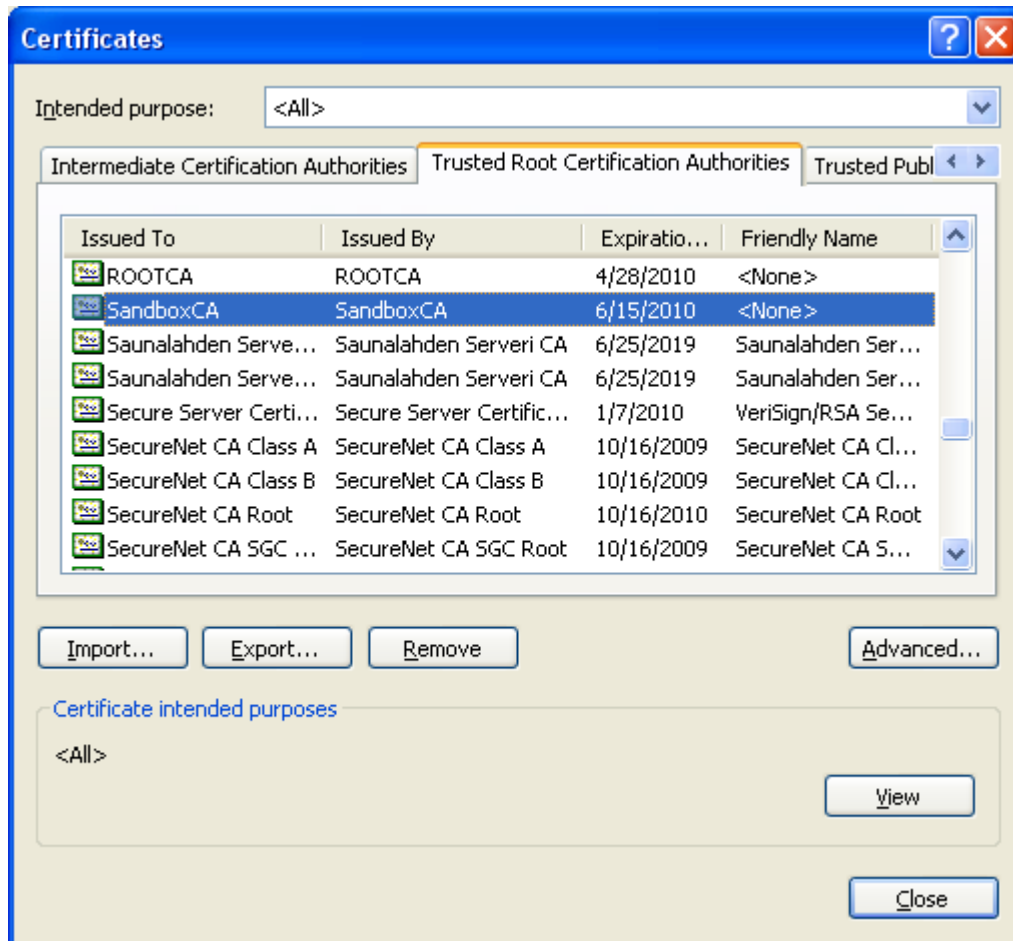
Before Installation

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. *Note for ISA Enterprise:* The installer will restart the firewall service, but on Enterprise deployments, the configuration will probably not yet be synchronized. So the firewall may not actually load the filter when it starts up! It will probably be necessary to **restart the firewall service again** once your configuration synchronizes with the CSS.
6. You must run the installer on each ISA server in an array separately.
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.

Automatic activation doesn't work?

If you're installing the full version (not the evaluation) you may receive a message that the software cannot activate automatically. Usually this means that the installer is being blocked from reaching our secure activation server at <https://www.collectivesoftware.com> over anonymous HTTPS. This can be caused by firewall policy, either on ISA or another downstream firewall. If you are unable to activate automatically and cannot (or prefer not to) change the firewall policy, you can select the Manual option, and follow the steps shown at the Manual Activation page (the URL will be shown in the installer).

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.

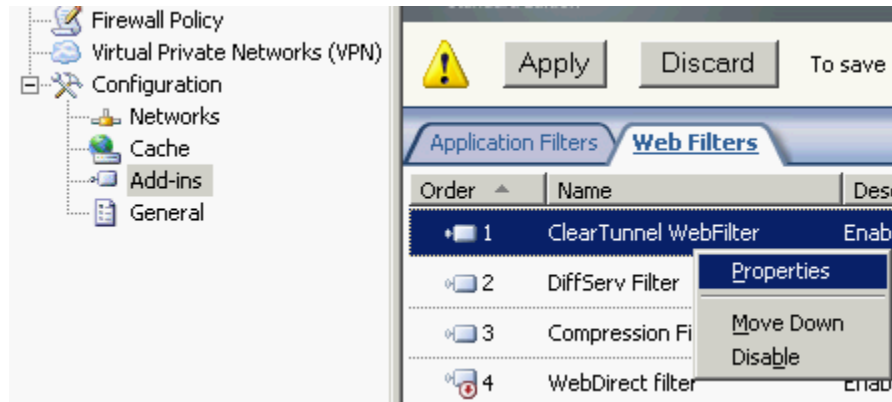
The install should eventually give up on starting the service, but it may take a long time. If necessary, you can expedite the rollback by going into the services control panel and setting the Microsoft Firewall service to Disabled temporarily (and applying that change). This will cause the installer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

Web Filter position

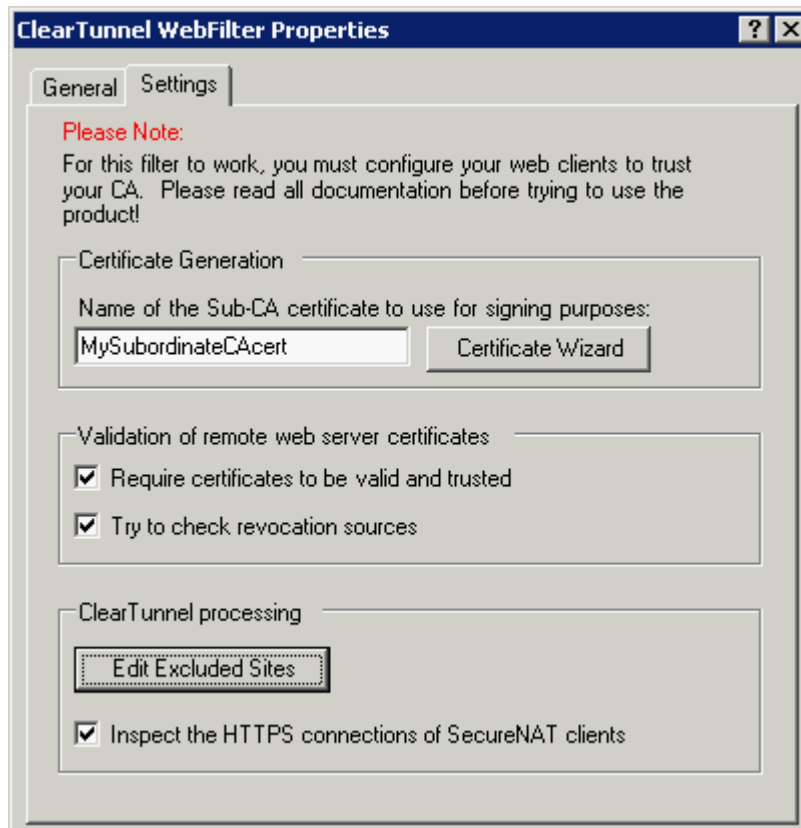
Move ClearTunnel to the top position in the list of Web Filters. (Note that there is also a ClearTunnel *Application Filter*, so don't get confused here. You want to check the order of the *Web Filter*). If any filters are called before ClearTunnel they will probably not work right because they'll be subjected to raw HTTPS traffic. Every time you install ClearTunnel, you should verify that it is in the first position. For example after uninstalling and reinstalling the position may be forgotten.



Configure ClearTunnel settings

Go into the properties view (see above image) of ClearTunnel. Click on the *Settings* tab and wait for the filter settings dialog to be displayed.

Once the tab loads you should see the following view:



Setting up the Certificates

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. We include a tool with ClearTunnel that the majority of customers can use to automate the certificate setup process. There is also a [list of manual steps](#), if necessary.

You can access the Certificate Wizard via that button on the settings tab.

You need to run this tool on *each ISA server in your array*. The interface is shown below:

Certificate Requester/Installer

Read the ClearTunnel Documentation before you use this tool!

Credentials to use when connecting to the CA

NETBIOS Domain Name: testsg

User Login Name: administrator

User Password: *****

Identity of the Certificate Server we'll use

IP Address: 192.168.1.70

Cert Service Name: ROOTCA

Details of the Signing Certificate

Certificate Name: MySubordinateCAcert

A Password for the PFX file: A secret!

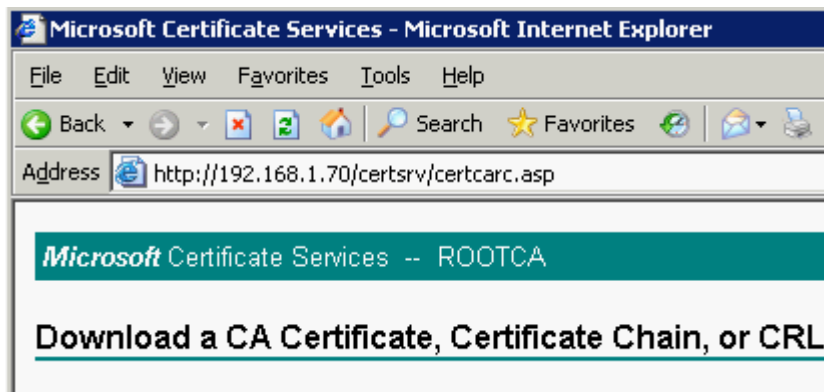
Do all the Certificate Setup!

Credentials

In order to request the certificate and install the chain of trust, you need to enter the login information of a user who has permission to request a “Subordinate CA Certificate” from a trusted CA in your enterprise. If this information is not correct, an access denied error (80070005) will be presented.

Certificate Server Identity

Enter the network IP address of the server which hosts the Certificate Services instance that will issue our signing cert. The “Cert Service Name” field **is not the DNS name** of that host. Rather, it is the name that is assigned to the certificate service instance itself. You can determine this remotely via the certificate services web tool:



In this instance the name is "ROOTCA".

NOTE: You **do not** need to use the root CA as the issuing authority here. For most customers' real domains, the CA used will be subordinate to the root (with a valid chain of trust to the root). In our test environment we're using the Root CA for convenience' sake only.

Details of Signing Certificate

Enter the name and a PFX password for the certificate that will be generated. When you first run this tool, the PFX file won't exist yet, so a new certificate will be requested from the CA and stored in a PFX file (on the root of your system drive, usually C:).

Running on each array member, or running after a re-install

We haven't actually run the wizard yet (that comes next) but this section is just a note to help you better understand how to use the tool effectively:

You may not want to keep re-requesting new certificates each time you install ClearTunnel, or for each array member. It is possible to re-use the same certificate that was issued on the first run, as long as you have saved the PFX file the tool generates.

For future runs of this wizard *including when you have to run it on the other ISA members in your array*, you may copy the generated PFX file to each server's system drive root folder (usually C:\).

You still fill out all the fields of the dialog exactly the same as the first run. If the wizard detects a correctly named PFX file, it will skip the step of requesting a certificate, and just use the one in the PFX file. In this manner you can control when you request a new certificate vs. using a previously generated one.

Running the wizard

When all fields are filled out correctly, click the setup button to carry out the automated certificate steps. All steps listed in [Appendix A](#) will be attempted (If the PFX file already exists then the certificate request will be skipped).

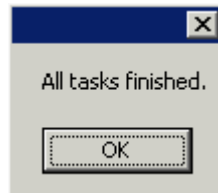
Error conditions are reported as popup messages, and normal informational messages are printed into the log window at the bottom of the dialog.

Permission to Access Certificate Server

One possible cause of errors is that ISA may be blocking the traffic to the certificate server. Please see the following KB article for details:

<http://collectivesoftware.com/Support/KB/article/23>

If all tasks finish without error, you will see:



Don't forget, if you have several servers in an enterprise array, you must run the certificate wizard on all of them to set up the certificates properly!

Other Settings

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

- *Name of certificate*: Set this to the same thing you specified in the "Certificate Name" field of the certificate wizard above (This is the subject name of the subordinate CA certificate that was installed into the fwsrv\Personal store.) This value will auto-populate with the name from the Certificate Wizard.
- *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.
- *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.
- *Excluded sites*: This button will launch the excluded sites editor (see next section).
- *Inspect the HTTPS connections of SecureNAT clients*: Select this field to automatically configure the HTTPS protocol for SecureNAT interception. If you leave this field unchecked, then any web clients that connect through ISA directly (without the web proxy settings configured in their browser) will not be proxied by ClearTunnel, and hence not available for ISA to inspect. If your organization does not use ISA as the network default gateway (or inline) for web clients, then you don't need this feature.

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.
- RPC/HTTP connections (due to a technical limitation, RPC/HTTP is not inspectable by ClearTunnel)
- 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 proxied.
- 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 from the button on the ClearTunnel settings dialog, or via the Network Objects toolbox section, under the "Domain Name Sets" item.

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.

Exclusion caching, and SecureNAT

If ISA caches content to a ClearTunnel-inspected SSL site, and then you later *exclude* that site from ClearTunnel, then future connections by SecureNAT clients may not work correctly. This is because some of the content for the new connections may be served from the cache before the connection can be checked against the exclude list. (Proxy client connections won't have this problem, because their exclusion check occurs much earlier in the process).

In order to combat this negative behavior, you should either expire the cached content

for that site via Microsoft's cachedir tool, or actually remove it as described in the following process, "ISA Server 2004: Deleting Cache Contents":

<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/deletecachecontents.mspx>

This behavior is a technical limitation between ISA and ClearTunnel.

Testing ClearTunnel

Once the above settings have been applied, you can use your web browser 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 refer to the name of the subordinate CA certificate you installed on ISA and configured in ClearTunnel.

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 Wizard, and it worked without producing error messages, this is a situation that should not occur.

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 lead to 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 particularly complex configuration working, find a bug (we're not always perfect, we admit it), or just have a feature question.

We provide several avenues of support, all available from our web site at <http://www.collectivesoftware.com/Support/>

- *Community Forum*: On the forum you can post general questions and get help informally from the support staff and other users. This is also a great way to see what issues other customers have faced and whether there might be a solution already available. For best results please make use of the Search feature to find threads related to your needs!
- *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. Like the forum, 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 request:* 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.

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.

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.

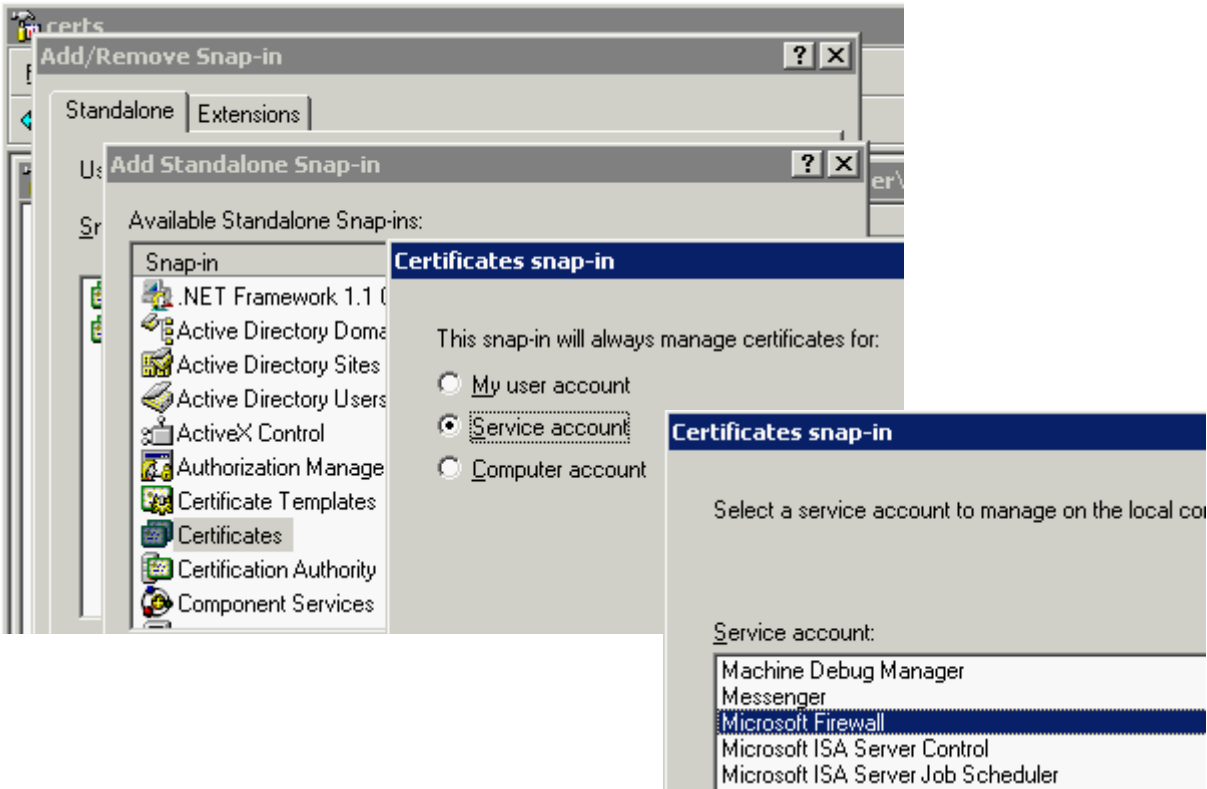
Certificates plugin

Note: The certificate 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.

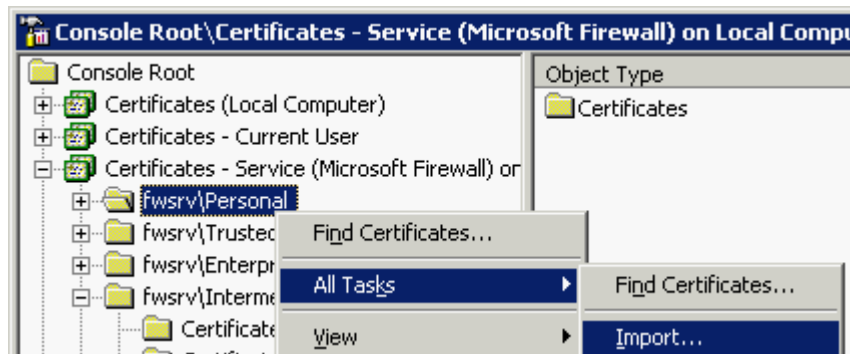
Installation of your Subordinate CA certificate

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 **both** the Local Computer and Microsoft Firewall stores manually (You can access these stores by adding more certificates plugins to your mmc window, as shown above). Make sure your root CA is listed in the “Trusted Root Certification Authorities” container of each 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 stores.

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](#).

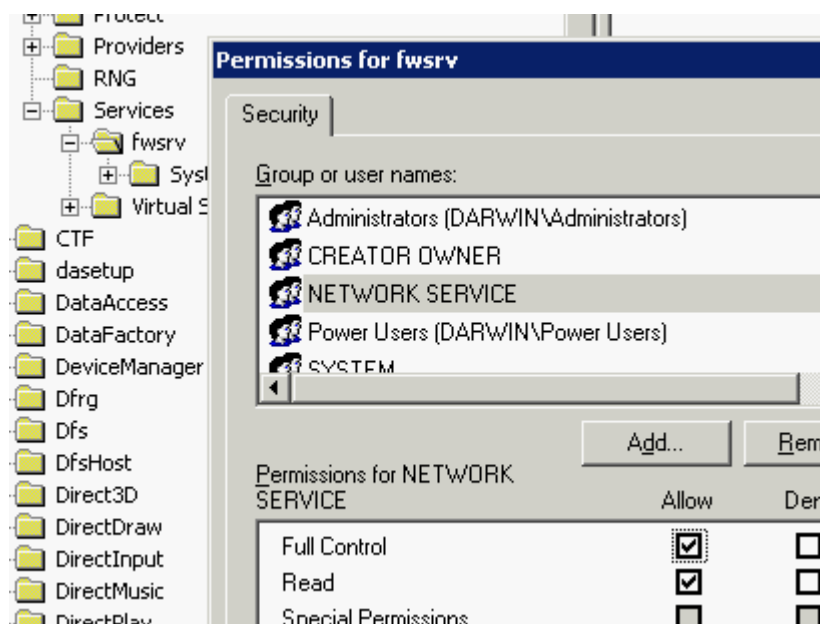
Certificate Store Permissions

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.