

FARONICS

ANTI-EXECUTABLE™

**ABSOLUTE Protection from
Unauthorized Executables**



Faronics Anti-Executable Enterprise and Remote Console Management

TECHNICAL WHITEPAPER

Last modified: November, 2005

Faronics

Toll Free Tel: 800-943-6422

Toll Free Fax: 800-943-6488

International Tel: +1 604-637-3333

International Fax: +1 604-637-8188

www.faronics.com

©1999-2006 Faronics Corporation. All rights reserved.
Deep Freeze, Anti-Executable, and WINSelect are trademarks
and/or registered trademarks of Faronics Corporation.
All other company and product names are trademarks of their respective owners.

Contents

Introduction	3
What is a Remote Console?.....	3
What is the Server Service?	3
A Remote Control Enabled (RCE) Console	3
Differences Between the Server Service and an RCE Console	4
Configuring a Server Service.....	4
Configuring a Remote Control Enabled (RCE) Console.....	6
Connecting to a Remote Console.....	8
Ports and Protocols Explained	11
Examples.....	12
Example 1 - Single Sub Net	13
Example 2 - Multiple Sub Nets One Console.....	14
Example 3 - Multiple Sub Nets Remote Control Enabled Console.....	15
Example 4 - Multiple Sub Nets Central Server Service	16
Example 5 - Multiple Sub Nets Multiple Server Services	17
Troubleshooting a Remote Console Connection.....	18
No Clients In the Console	18
Port is in Use Error When Starting the Console	19

Introduction

This document is designed to answer questions regarding the implementation of Anti-Executable Enterprise in more complex networking environments. This document supplements the information provided in the Anti-Executable Enterprise User Guide.

What is a Remote Console?

A remote console is a small utility that runs on a remote machine and acts as a communications hub that other consoles can connect to in order to control and view Anti-Executable workstations. This utility is not used on its own. There are two components that incorporate this Remote Console utility: the Server Service and the Anti-Executable Enterprise Remote Control Enabled Console.

What is the Server Service?

The Server Service is a service that is installed and configured using the Server Service Manager (SSM). The Server Service uses the Remote Console utility to allow the administrator of Anti-Executable to segment the connections to the clients.

In a basic environment, the clients connect directly to the Anti-Executable Enterprise console. Clients with either the Anti-Executable workstation or seed installed send packets every 30 seconds to the console. In smaller networks, there are no issues using the console this way. In more complex environments, involving multiple sub nets spread across multiple physical locations, the packets have more switches to pass through and must travel a greater distance to the console. The more of these factors, the greater the chance the packets may fail to reach the console. The Server Service reduces these types of issues.

The Server Service acts as a middle layer between the clients and the console. Instead of sending packets directly to the console, they instead send packets to the Server Service. In turn, a Anti-Executable Enterprise console also connects remotely to the Server Service. The Server Service can have more than one console connected to it at any given time.

In a LAN/WAN setup, the console must be run on a machine with a static IP. Using the Server Service, a console can be portable. Anti-Executable administrators can run the console on lap tops. These consoles could connect remotely to the Server Service from any location on the network to see the client machines. The administrators would plug into the network, connect to the Server Service, and see the client machines. It is recommend to install the Server Service on a server, because the IP is normally static and the server is on all the time.

A Remote Control Enabled (RCE) Console

It is possible to set up a Anti-Executable Enterprise console so other enterprise consoles can connect to it and see the client machines. This Remote Control Enabled (RCE) console works on a concept that is very similar to the Server Service. Like the Server Service, an RCE console uses the Remote Console utility. In order to turn a console into an RCE console, the remote control must be enabled. By default, this option is disabled. When it is disabled, a label at the bottom of the enterprise console reads *Remote Control Disabled*. When it is enabled, other enterprise consoles can connect to this enterprise console. At that time, the label reads *Remote Control Enabled*.

Differences Between the Server Service and an RCE Console

The following table shows the differences between the Server Service and a Remote Control Enabled (RCE) console:

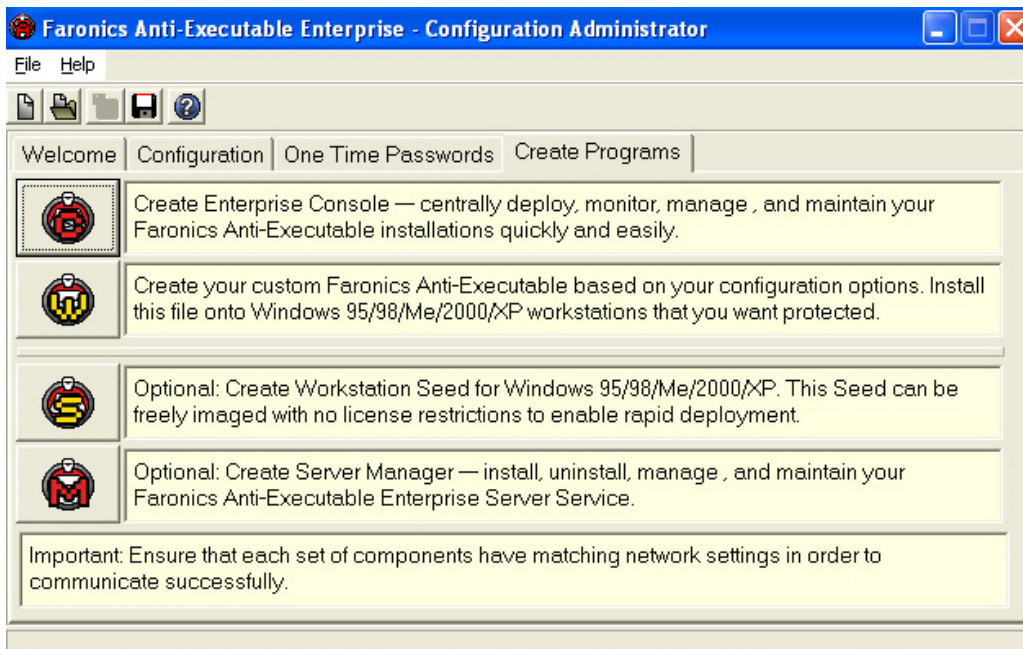
Server Service	RCE Console
Runs as a service	Runs as a process
Allows multiple consoles to connect to it	Also allows multiple consoles to connect to it
Does not allow the console to run on the same machine as the server	Can be used as a regular console
Cannot be easily shut down; less likely to lose connectivity	Can be easily shut down; more likely to lose connectivity
Can run several ports under one service	Can only run one port per RCE Console

Configuring a Server Service

In order to set up a Server Service, the Server Service Manager (SSM) program must be created. This is done using the Anti-Executable Enterprise Configuration Administrator. Once the SSM has been created, it can be run on the preferred machine to install and configure the Server Service.

To create the Server Service Manager, complete the following steps:

1. Open the Anti-Executable Configuration Administrator.
2. Click on the *Create Programs* tab. The following screen appears:



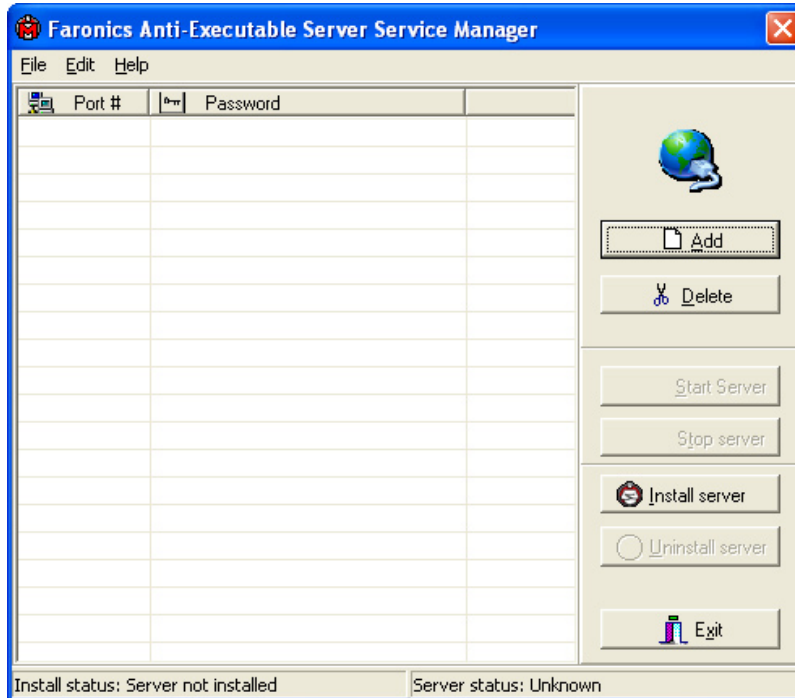
3. Click *Create Server Manager* to create the *AEServerServiceManager.exe*.

A prompt to save the file follows. By default, the file is saved to ...*Program Files\Faronics\Faronics Anti-Executable Enterprise\AE Install Programs*.

At this point the created program can be deployed to the machine where the service is to be installed.

To set up the Server Service, complete the following steps :

1. Run *AEServerServiceManager.exe*. This should be run on the machine where the service will be installed. The following dialog displays:



2. Click *Add* to add a port. The port used is the port the client machines will use.
3. Enter the port number you want your clients and the Server Service to use.
4. Press *Tab* and enter a password.

This password is the password that administrators use in order to connect to the Server Service from a console. NOTE: A password must be set in order for the console to be able to connect to the Server Service.

5. Click *Install* to install the Server Service to the machine.

A prompt to start the Server Service appears. If this prompt does not appear, go to step 6.

6. Click *Start* to start the Server Service.

At this point, the Server Service is installed. The next step is configuring the clients and consoles that will connect to the Server Service.

Configuring a Remote Control Enabled (RCE) Console

In order to create an RCE console, the console must first be created. This is done using the Anti-Executable Enterprise Configuration Administrator.

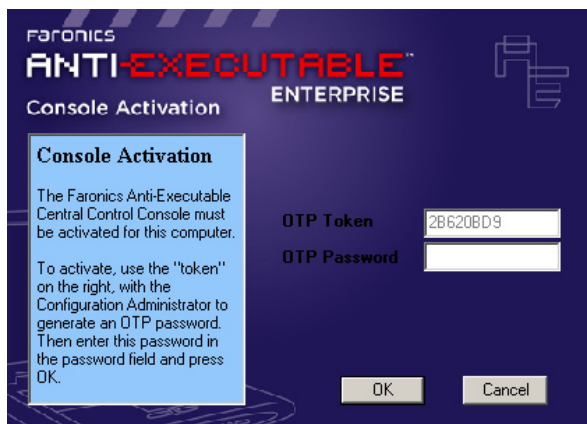
Remember that an RCE console is used in place of the Server Service; the two utilities are never used at the same time. Once the console is created, it should be moved to the machine where it is to be run. The steps used to create and deploy the console are exactly the same for any console that is created.

To create, configure, deploy, and enable an RCE console, complete the following steps:

1. Open the Anti-Executable Configuration Administrator.
2. On the *Configuration* tab, click the *Network* sub-tab.
3. Configure the port settings to match the settings used by the client machines. If the clients are using port 8825, the console must also be configured for 8825. This is explained in more detail in the section titled *Ports & Protocols Explained*. For the consoles, it does not matter whether the LAN or LAN/WAN option is selected.
4. Click the *Create Programs* tab.
5. Click *Create Enterprise Console* to create the *AEConsole.exe* program.

A prompt to save the file appears. By default, the file is saved to ...*\Program Files\Faronics\Faronics Anti-Executable Enterprise\AE Install Programs*.

6. Move the console program to the machine where it will be run. When the program is run, a prompt for a *One Time Password* appears. A token is provided, as shown below.

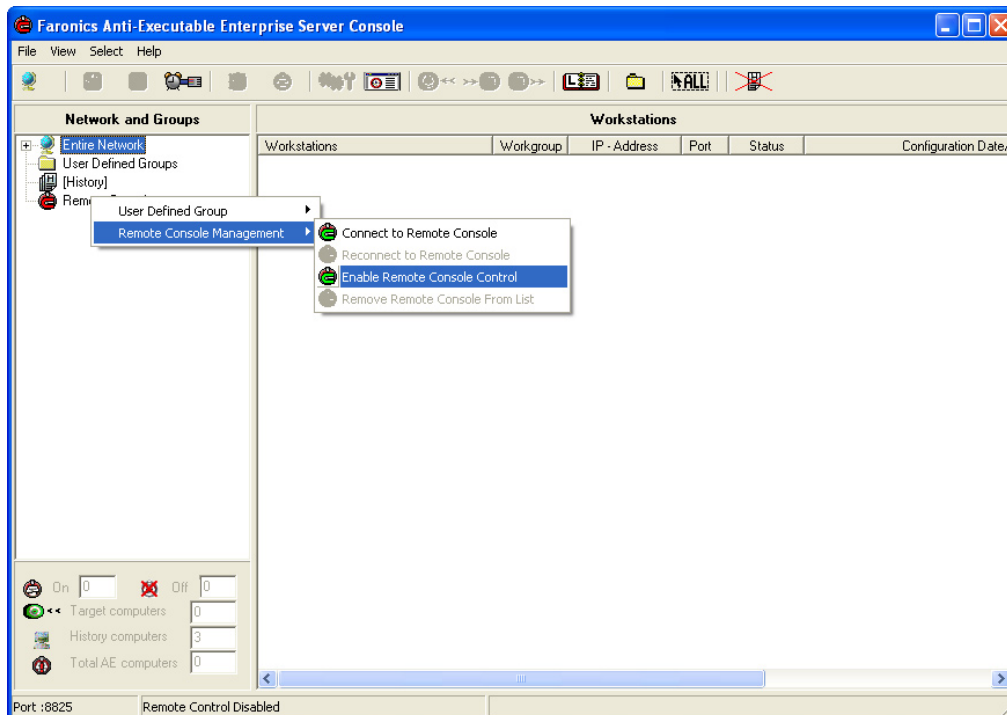


7. Use the *One Time Passwords* tab in the Configuration Administrator to generate a password. After entering the password, the console launches.

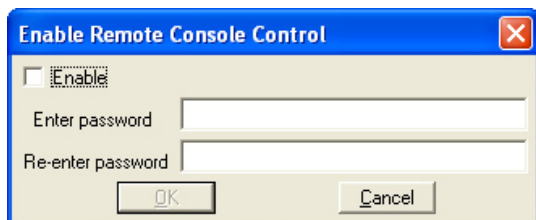
When the console is started, the following label appears at the footer of the screen indicating that remote control is disabled. The port that the console is currently using locally is also displayed.

Port :8825 Remote Control Disabled

- Right-click on *Remote Consoles* and select *Remote Console Management -> Enable Remote Console Control*.



- The following dialog appears:



- Check *Enable* and enter a password. This password is the password administrators use to connect to the RCE console.
- The following label appears at the footer of the screen, indicating that remote control is enabled. It is now possible for other consoles to connect to it.

Port :8825 Remote Control Enabled

Connecting to a Remote Console

Once the Server Service or RCE console has been created and configured, it can now be connected to a Anti-Executable Enterprise console.

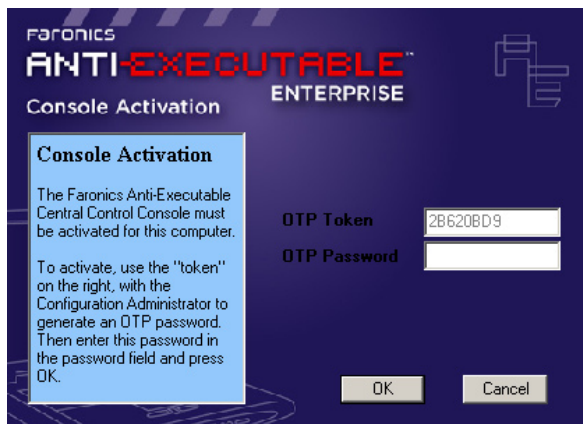
The steps to connect to a Remote Console are identical, whether the Server Service or RCE console is used.

To create the Anti-Executable Enterprise console, complete the following steps:

1. Open the Anti-Executable Configuration Administrator.
2. On the *Configuration* tab, click the *Network* sub-tab.
3. Configure the port settings. The port configured for this console must not be the same as the port used by the clients or Remote Console.

This console must use a different port so it does not conflict. When connected to the remote console, the correct port is specified. This is explained in more detail under the section titled, *Ports & Protocols Explained*. For the consoles, it does not matter whether the LAN or LAN/WAN option is selected.

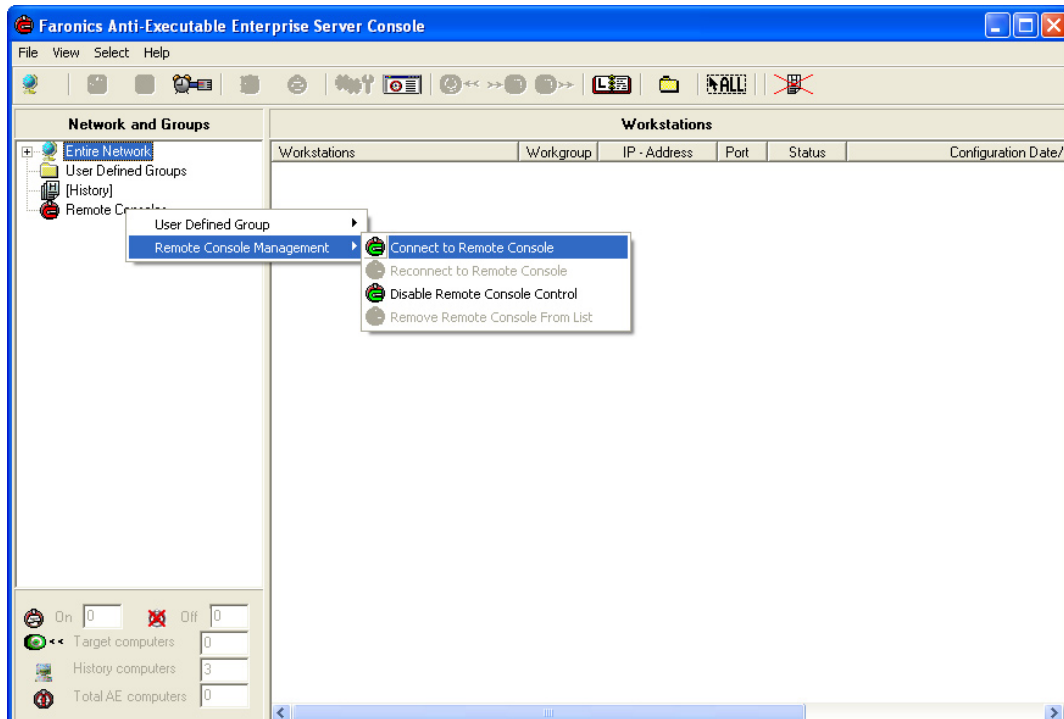
4. Click the *Create Programs* tab.
5. Click *Create Enterprise Console* to create the *AEConsole.exe* program. A prompt to save the file appears. By default, the file is saved to ...*\Program Files\Faronics\Faronics Anti-Executable Enterprise\AE Install Programs*.
6. Move the console program to the machine where it will be run. When the program is run, a prompt for a *One Time Password* appears. A token is provided, as shown below.



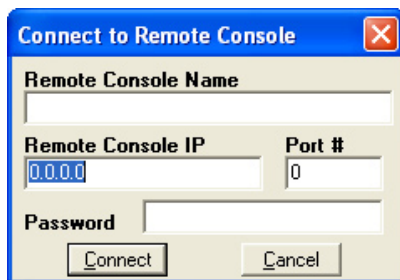
7. Use the *One Time Passwords* tab in the Configuration Administrator to generate a password. After entering the password, the console launches.

To connect a console to a Remote Console, complete the following steps:

1. Open the Anti-Executable Enterprise Console.
2. Right-click on *Remote Consoles* and select *Remote Console Management -> Connect to Remote Console*.



3. The following dialog appears:



4. Enter the connection details.

5. Press *Connect* to connect to the remote console. If the connection is successful, a new connection appears under *Remote Consoles*.



At this point, all clients located under *Entire Network* within the Remote Console connection are visible.

Ports and Protocols Explained

The key to setting up a Remote Console is knowing which ports to use. The important factor is knowing what ports are in use on the network and using ports that will not conflict with those. By default, Anti-Executable uses port 8825.

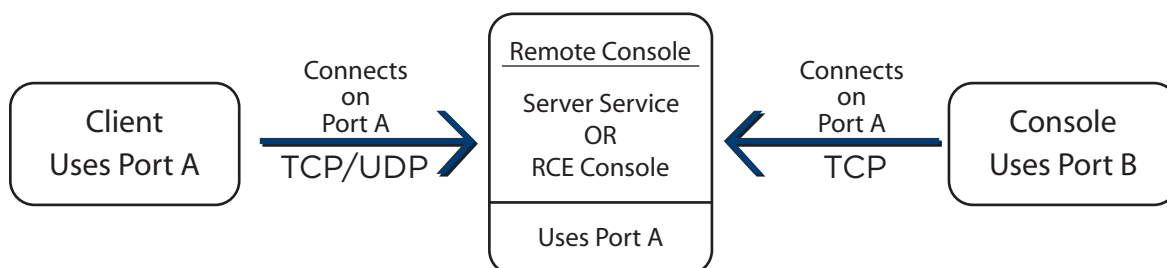
The following three components make up the Anti-Executable Architecture:

- Client (with workstation or seed installed)
- Remote Console (Server Service or RCE Console)
- Console (connects to the Remote Console)

Using the following rules, there should not be any port conflicts between the different components:

- The clients and Remote Console should use the same port.
- The consoles that connect to the Remote Console need to be created under a different port than the Remote Console. This prevents the consoles from conflicting with the Remote Console when they are both run inside the same sub net.
- One console that connects to the Remote Console can use the same local port as another console connecting to the Remote Console. These consoles do not conflict with one another, even though they are on the same sub net, because there are no clients involved on the local port.

The following diagram gives a theoretical view of the Port Settings:



Ports can also be used to divide the clients when using the Server Service. If the Server Service is set up to run under three ports (8825, 8826 and 8827), consoles can connect to the three different ports to see a different set of clients under each port. An example showing this type of architecture is shown subsequently in *Example 4 - Multiple Sub nets Central Server Services*.

In the diagram above, the client(s) use both the TCP and UDP protocols to communicate with the Remote Console. The console(s) that connects to the Remote Console uses only the TCP protocol to communicate with the Remote Console. It is important to remember the ports and protocols being used in order to prevent fire walls, switches, or routers from blocking them.

Examples

The following examples show different scenarios involving either the server service manager or remote console.

- Example 1 - Single Sub Net One Console
- Example 2 - Multiple Sub Nets One Console
- Example 3 - Multiple Sub Nets Remote Control Enabled Console
- Example 4 - Multiple Sub Nets Central Server Service
- Example 5 - Multiple Sub Nets Multiple Server Services

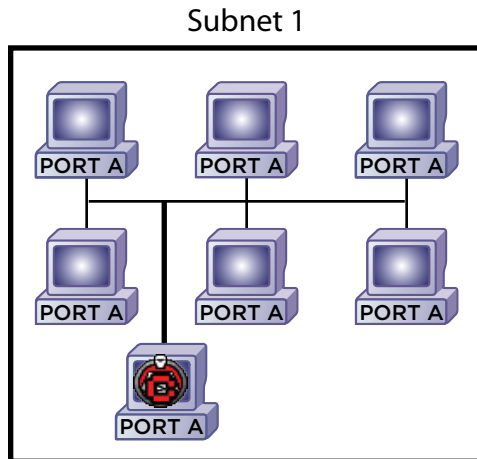
Each example explains how the different Anti-Executable components interact in different networking environments.

NOTE: In the following examples, the client machines have either the Anti-Executable workstation installation or workstation seed installed. Both installs contain the communications component which talks to the console/remote console. The difference between the workstation install and workstation seed is that the workstation install actually installs Anti-Executable while the seed has only the communications component.

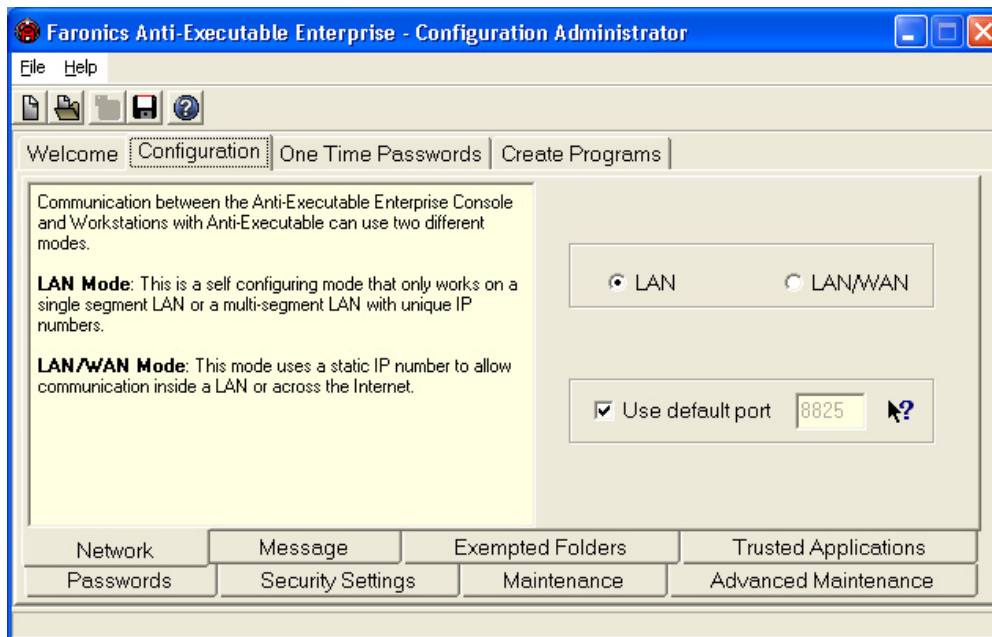
Example 1 - Single Sub Net

In this environment, all client machines are contained in the same sub net as the console machine. This environment does not require a remote console, although one could be used. In this example, the remote console is not used. This is the simplest networking environment. It is also the easiest to configure.

The following diagram shows the network topology:

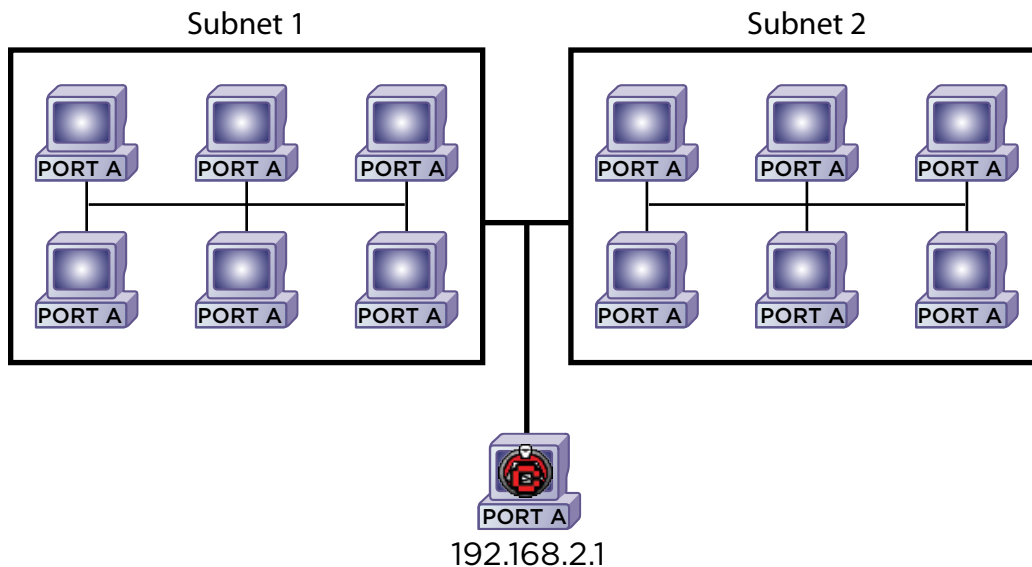


The client machines, represented by the computer icons, are located on the same sub net as the Anti-Executable Enterprise console machine, and are represented by the Anti-Executable Console icon. In this scenario, both the client and the console are using the same port. This port is configured in the Anti-Executable Configuration Administrator in the *Configuration* tab on the *Network* sub-tab, as shown below, before creating the workstation install/seed or the console program.



Example 2 - Multiple Sub Nets One Console

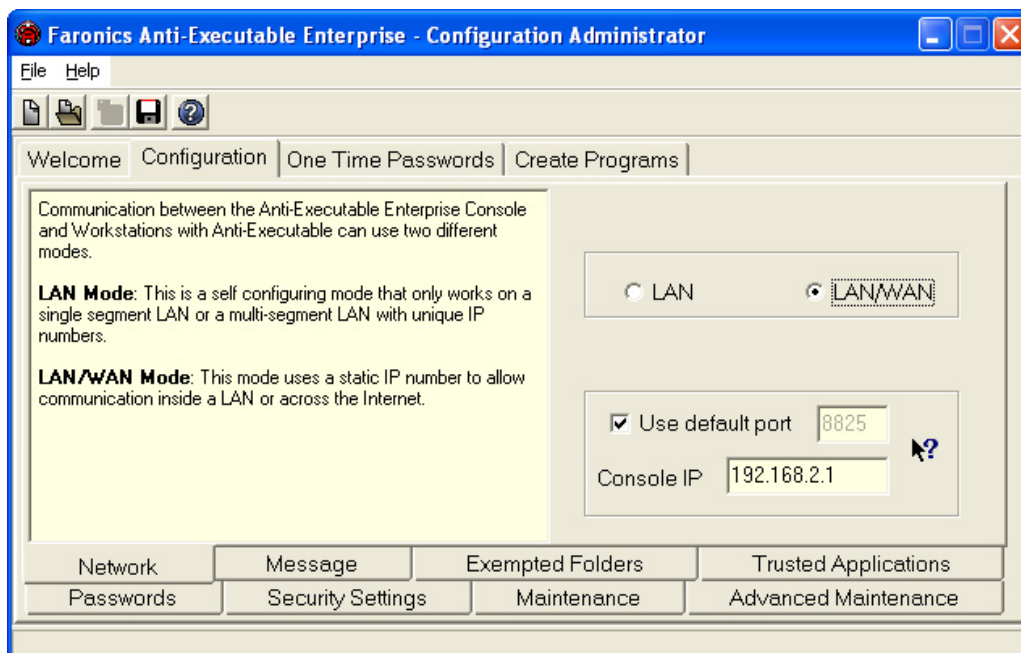
In this environment, the clients are located across more than one sub net. There is still only one console being used. This environment does not require a remote console, although one could be used. The following diagram shows the network topology:



In this scenario, both the clients and the console are using the same port. This port is configured in the Anti-Executable Configuration Administrator in the *Configuration* tab on the *Network* sub-tab, before creating the workstation install/seed or the console program.

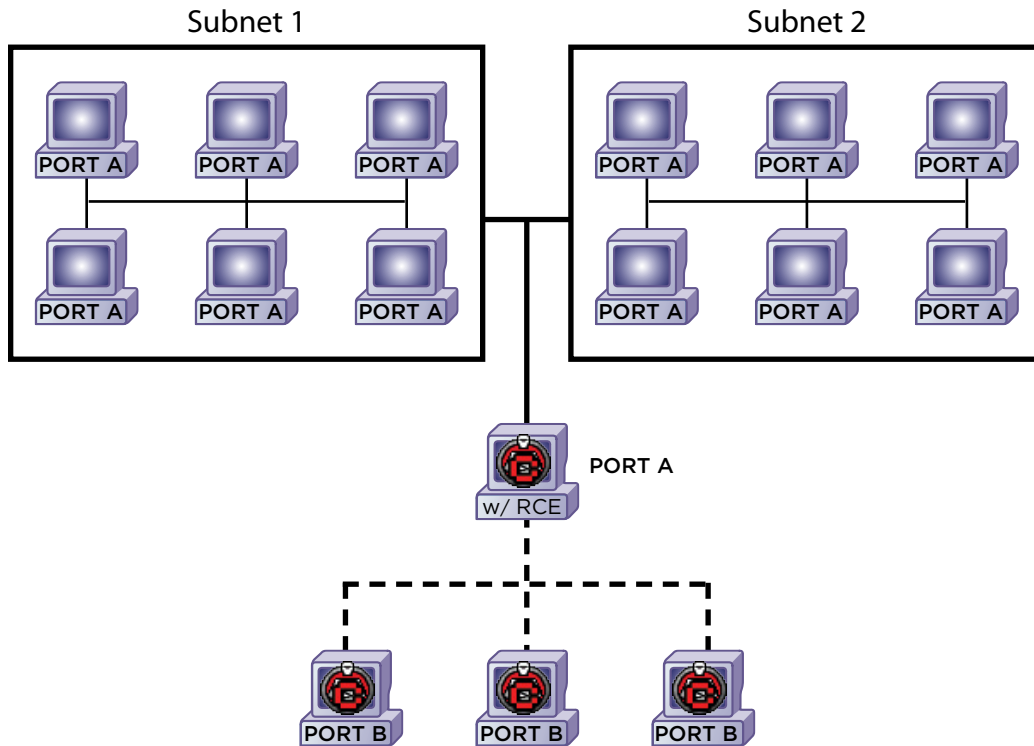
In order for the clients to be seen, they need to be configured to use a LAN/WAN connection. When the LAN/WAN option is selected, a field to enter the Console IP or Console Name appears. Specify the Console IP or name of the machine that will run the console.

An example of these settings are shown in the *Network* tab below:



Example 3 - Multiple Sub Nets Remote Control Enabled Console

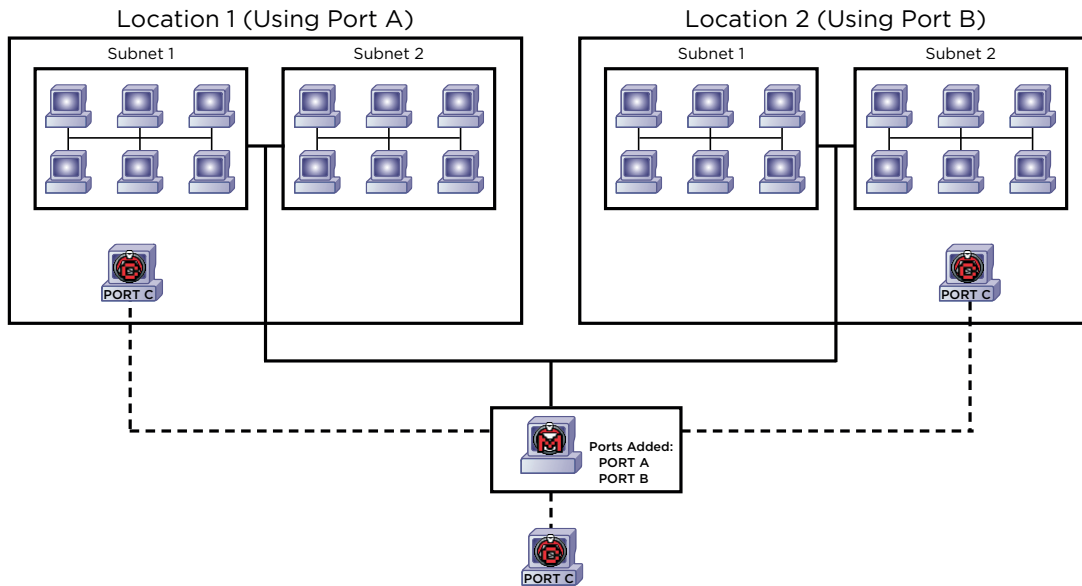
In this environment the clients are again located across multiple sub nets. In this case, more than one console is being used. There are two methods that allow multiple consoles to be used: a Server Service or a Remote Control Enabled (RCE) console. In this example, an RCE console is used. The following diagram shows the network topology:



In this scenario, the clients and the RCE console use the same port. Looking at the above diagram, three other consoles connect to the RCE console in order to see the clients. To ensure these consoles do not conflict with the RCE console (Port A), they are created under a different port (Port B).

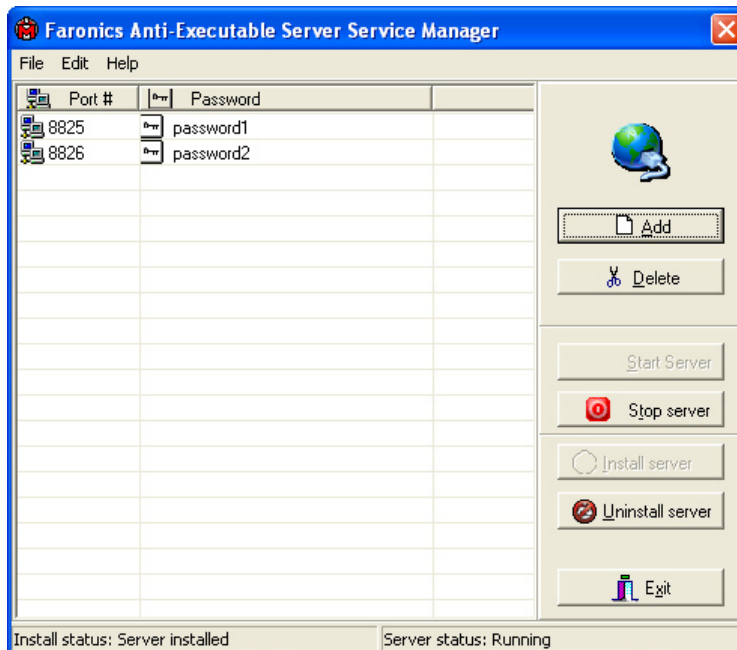
Example 4 - Multiple Sub Nets Central Server Service

In this example, there are two locations. Both locations are connected to a third location by a WAN. Location 1 is administered locally and from the third location. Location 2 is also administered locally and from the third location. In order to prevent the administrator at Location 1 from having access to Location 2, the clients must be split up.



In this example, the Server Service is going to divide the client machines from each location. The clients at Location 1 are going to use port 8825. The clients at Location 2 are going to use port 8826.

The following screen shows how this would be set up in the Server Service Manager.



The advantage of having a Remote Console at a central location is that it can be easily administered locally. The disadvantage is that the packets being sent from the clients need to travel across the WAN to reach the Remote Console.

Example 5 - Multiple Sub Nets Multiple Server Services

In this example, there are two separate locations.

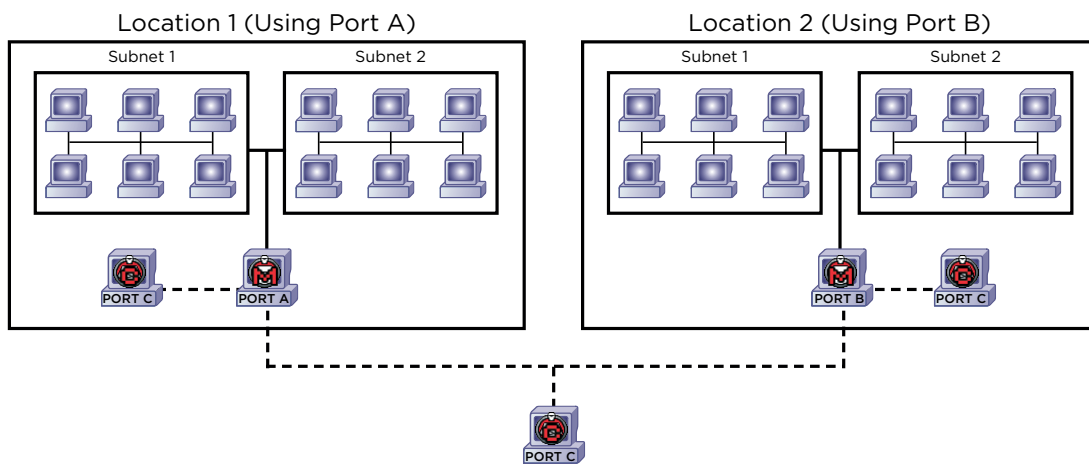
The following is a list of assumptions that are made regarding this particular example:

- the locations are spread apart and have only a minimal connection to each other
- there is a network administrator at each location who is responsible for looking after Anti-Executable at that location
- both locations need to be administered from a third location

In this example, the remote consoles are set up at each location and a Server Service is used (represented by the Server Service Manager icon).

Location 1 uses port A to communicate with the clients and the Server Service. Location 2 uses port B. The consoles at all the locations use port C. This ensures the consoles do not conflict with ports A or B.

The following diagram shows the network topology:



The benefit of this setup is that it allows all the packets sent from the clients at Location 1 to be contained at that location. The less distance a packet must travel, the less chance there is of the packet failing.

The administrator at Location 1 can connect to the Server Service at Location 1 but cannot connect to the Server Service at Location 2. The reason for this is that the Location 1 administrator does not know the password to access the Server Service at Location 2. The same goes for the administrator at Location 2. At Location 3, if the password to both Server Services is known, the Server Service at Location 1 and Location 2 can be connected to, in order to administer the clients at both locations.

Clearly, using a Remote Console is a great way to break up network environments to contain communications to a specific area or break up the network for security purposes.

Troubleshooting a Remote Console Connection

No Clients In the Console

The following are some common reasons why clients fail to appear in the console.

1. *Windows XP clients may have the XP firewall turned on.*

With SP1, the firewall must be turned off. With SP2, either the firewall must be turned off or the ports being used must be added to the *Exceptions* tab. Anti-Executable requires both TCP and UDP protocols; therefore, one exception should be added for each.

2. *The console and clients do not contain the correct network settings.*

If the console is set up to run under port 8825 and the clients are using port 8826, they will not be able to see each other. Also, if the workstations are configured for LAN/WAN, the IP must be equal to the IP of the machine where the console is running.

3. *Something on the network is blocking the port used between the console and the clients.*

If a server, router, or switch on the network is not allowing the port to get through, the clients will not be seen. By default, 8825 is the port being used.

4. *The workstations are configured to run under LAN settings but the console exists on a different sub net.*

The default LAN setup works as long as all the machines running the workstation and console exist on the same sub net. However, if a VLAN is being run, or if there are several sub nets where the clients exist, the workstation install must be configured to run under the LAN/WAN settings.

5. *The workstations were created under a different customization code than the console.*

When the Anti-Executable Configuration Administrator is first run, a prompt for a *Customization Code* appears. This code is very important as it encrypts the software. This means that any workstations created are encrypted with this customization code. If a console was created using another administrator that was installed with a different customization code, it cannot see workstations created under the original code. The workstations and console must be created under a configuration administrator installed using the same exact customization code.

6. *The network usage is quite high and may be preventing packets from getting through to the console.*

The clients send a packet to the console every 30 seconds. The console also broadcasts to the clients to let them know it is listening. If a packet does not get through, the client is not reported to the console. Using a Server Service helps resolve these types of issues.

7. *The client has no route to the host.*

Something is blocking communication or the machines are not physically connected. The clients are unable to send packets to the Console/Remote Console because there does not seem to be a route to the host. Attempting to ping the IP of the console/Remote Console does not seem to work. To resolve this issue, make sure the two machines can connect to each other.

Port is in Use Error When Starting the Console

When attempting to start the console, the error message *Unable to start console: Port is in use* appears. There are several reasons why this error message may be appearing:

1. *There is a Anti-Executable workstation or workstation seed installed under the same port as the console.*

It is possible that the workstation install is in stealth mode (the icon does not appear in the system tray). The seed does not show an icon. The best test is to run a workstation install on the machine in question. If the *uninstall* option presents itself, the workstation or seed is installed and can be uninstalled. If the *uninstall* option does not appear, the workstation or seed is not installed.

2. *The Server Service is installed and running under the same port as the console.*

It is possible the Anti-Executable Server Service Manager was run on the machine. If the Anti-Executable Server Service has been installed and is using the same port the console is using, the console will fail to run with this error.

To verify that the Server Service is not installed, go to the *Control Panel > Administrative Tools > Services*. Under the list of services look for *Anti-Executable Server Service*.

If the service exists, the Anti-Executable Server Service Manager can be run on this machine to uninstall the service. The Anti-Executable Sever Service Manager is created using the Configuration Administrator. The default file name is *AEServerServiceManager.exe*.

3. *Another program or service is using the port on this machine.*

This may involve running a port sniffer on the machine in question to see what ports are open. There are several tools available on the web to perform this action. One of these tools should show whether the port Anti-Executable is using is already in use.

4. *The network cable is unplugged.*

This message can occur if there is no network connection on the machine.