

Configuring A Secure CSG/SSG Communication Link For ASAP

Version 2.0
November 10, 2010

1 Overview

The purpose of this document is to briefly describe the steps involved in configuring a secure, Telnet-based communication link for use by the ASAP Client.

The ASAP Client utilizes Telnet for communication with the NonStop server. All data transmitted over a Telnet connection is sent "in the clear" (i.e. it is not encrypted in any way), including logon and password information as well as all ASAP data. On public or other non-secure networks, this data is susceptible to being captured by network sniffers, which could raise security concerns.

To address these concerns, two alternatives are available for providing a secure CSG/SSG communication link for ASAP: a dedicated TelServ process configured for access only by ASAP, or use of NonStop SSL to encrypt all ASAP data flowing between the NonStop server and the ASAP Client. Each of these alternatives is discussed below.

2 Accessing ASAP Using A Dedicated TelServ Process

Use of a dedicated TelServ process is of interest if you are primarily concerned about the possibility of user ID and password information being transmitted in clear text across the local network.

By following the steps below, CSG and SSG can be configured in such a way that a logon is not required to the NonStop server. Furthermore, the TelServ process used by ASAP can be set up so that it cannot be used for any purpose other than serving as a communication pipe for ASAP. If you need to access TACL, osh, or any other NonStop-based command interpreter via this TelServ process, then the configuration steps described here do not apply.

2.1 Configuring The NonStop Server

Configuration of the NonStop server involves three separate steps: starting the TelServ process, configuring the SSGCOM Telnet service, and specifying SSG security settings in the SSGCONF file:

1) Start a TelServ Process

This step starts a "secure" TelServ process. This includes starting the process itself on a TCP/IP port other than the standard default of port 23, specifying that it should not display a banner or menu, and specifying that it should not allow access to TACL.

For the purposes of this example, we're starting a TelServ process named \$TLSV on port 8423 of TCP/IP process \$ZTC04:

```
TACL 1> PARAM ZTNT^TRANSPORT^PROCESS^NAME $ZTC04
TACL 2> TELSERV/NAME $TLSV, TERM $ZHOME, PRI 170, NOWAIT/8423 -nobanner -nomenu -notac1
```

In the above, "8423" defines the port number on which TelServ will accept connections, the "-nobanner" option prevents TelServ from displaying a banner/welcome message, the "-nomenu" option prevents TelServ from displaying a service menu, and the "-notacl" option prevents users from accessing a TACL command shell via this TelServ. Together, these options essentially deliver a TelServ process that cannot be used for doing anything on the system when it is started. Even if a user with a Telnet client connects to port 8423, they cannot access any resources on the system regardless of whether they have a user ID and password or not.

2) Configure The TelServ Process In SCF

This step adds an SSGCOM service to the TelServ created in step 1. This service is what the ASAP Client will use to access ASAP data. Our recommendation would be to define this as the default service for the TelServ process. By doing so, any user who connects to the port will be immediately presented with an SSGCOM prompt.

To continue the example above, the following SCF commands would add the SSGCOM service to the TelServ process created in step 1 above:

```
1-> ASSUME PROCESS $TLV
2-> ADD SERVICE ssgcom, PROGRAM $system.system.ssgcom, ACCESS ALL, SUBTYPE DYNAMIC, TYPE
CONVERSATION, DISPLAY OFF, DEFAULT ON
```

There is no requirement that the service name be "SSGCOM". You can call the service whatever you'd like. Also, as mentioned above, by specifying "DEFAULT ON", any user who connects to the port will be presented with an SSGCOM prompt. Since SSGCOM will be configured to only allow access to ASAP data, this configuration does not pose any security issues. However, if you would prefer to force the user to "guess" the correct service name, you can set DEFAULT to OFF. In this case, a user connecting interactively from a Telnet client will be presented with the standard TelServ "Enter Choice>" prompt and nothing more. At that point they'd have to enter "SSGCOM" to even get the SSGCOM prompt, and even then there's nothing they can do in terms of compromising system security.

3) Set SSG Security Parameters

The last step on the NonStop system is to define SSG security settings. This is done by editing the \$SYSTEM.SYSTEM.SSGCONF file and adding the following lines:

```
SET SECURE DEFAULT USER
SET SECURE TACL NONE
SET SECURE ASAP ANY
SET SECURE MEASCOM ANY
SET VERIFYUSER OFF
```

The various "SET SECURE" statements limit which server resources can be accessed by SSGCOM. Specifically, only access to ASAP and MEASCOM are permitted (the latter is used by the ASAP Client's "Show Related Measurement" capability). Thus the SSG subsystem itself will only be able to supply ASAP data, and nothing else.

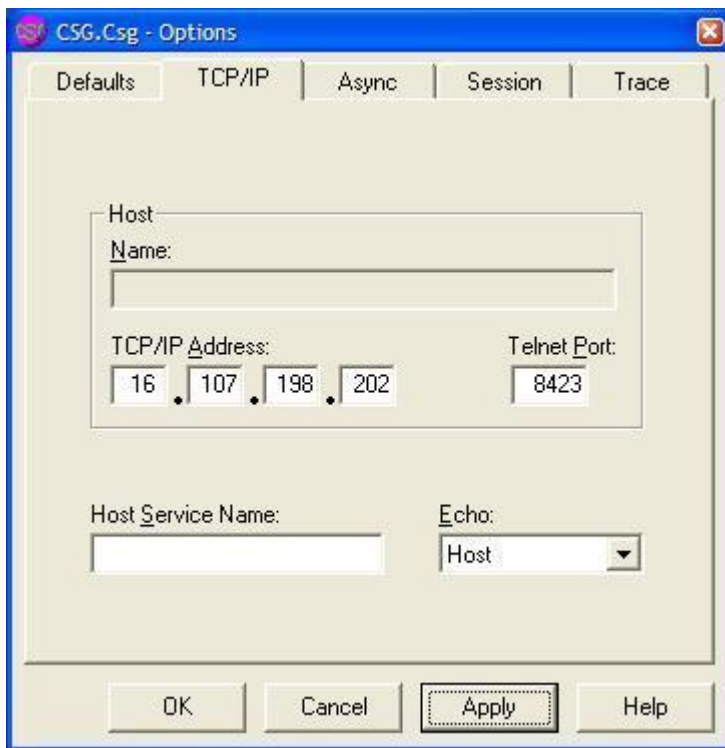
The "SET VERIFYUSER OFF" statement configures SSGCOM to bypass its internal user ID/password verification step, which means that anyone is able to utilize SSG services as no user ID and password are required or transmitted. But since the other security settings have limited the SSG to only supplying ASAP data, this access does not pose a threat. Furthermore, in many ways this type of configuration is actually more secure than those requiring a logon, because not every user who needs

to access ASAP data is required to have a valid logon to the NonStop server. They only need to be able to access the SSGCOM service across the network in order to obtain ASAP data; they do not need to have any logon information for the NonStop itself.

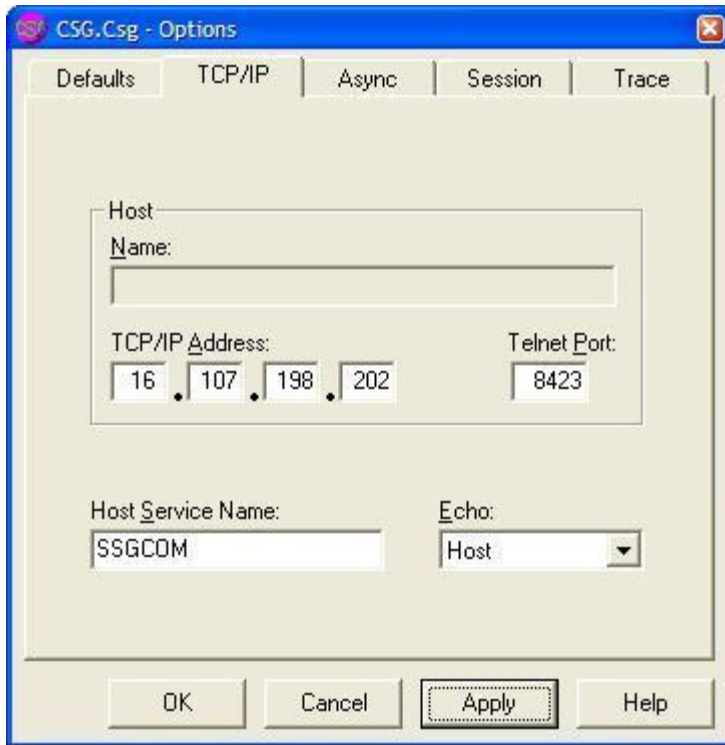
2.2 Configuring The CSG On The Windows PC

Once the NonStop server is configured, the only remaining step is to configure the CSG running on the Windows PC. Doing so is fairly straightforward:

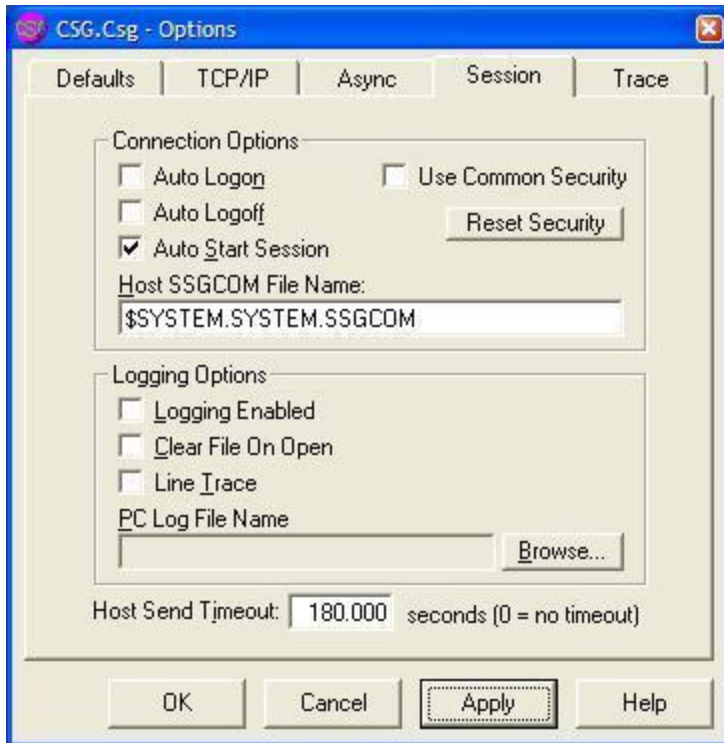
- 1) From the CSG main window, click on View...Options from the CSG main menu to bring up the CSG Options dialog, and click on the "TCP/IP" tab.
- 2) Supply the TCP/IP host name or address and the Telnet port number on the server (this is the port number specified in step 1 of "Configuring The NonStop Server" above).
- 3) If you configured the SSGCOM service with DEFAULT set to ON (i.e. SSGCOM is the default service), then clear the "Host Service Name" field on the CSG's TCP/IP tab. So the entire tab should look something like this:



- 4) If you configured the SSGCOM service with DEFAULT set to OFF (i.e. SSGCOM is not the default service), then set the "Host Service Name" field to "SSGCOM" (or whatever value you specified for the service name in step 2 of "Configuring The NonStop Server" above). So the entire tab should look something like this:



- 5) Finally, you can disable all logon/security-related settings on the Session tab of the CSG Options dialog. These settings are no longer needed. In addition, if the PC you are configuring has previously been running the ASAP Client and CSG, you may want to click on the "Reset Security" button to clear saved ID and password information from the CSG. The Session tab should look something like this when you are done:



You can now start the ASAP Client as you would normally. It will start a CSG/SSG session using the new CSG settings and new TelServ on the server. At no point will you be prompted for logon information because no component requires it. Startup and shutdown should also be a bit faster since the step of logging onto TACL, loading macros, etc. is bypassed.

3 Accessing ASAP Using NonStop SSL

If you are concerned about the sensitivity of all ASAP data flowing across the Telnet connection, or if your policy requires every user that accesses the NonStop system to supply a user ID and password, then use of a dedicated TelServ process as described above may not meet your security requirements.

In that case, another approach is to use NonStop SSL to provide an encrypted link for all ASAP data, including user ID and password information. In this scenario, the NonStop SSL process on the NonStop server and the SSL Proxy on the Windows PC are inserted between the CSG and the TelServ process in order to provide a secure communication mechanism for all data. The fact that SSL is being used is transparent to ASAP, the CSG, SSG, and TelServ. The only changes required on the NonStop server and Windows PC are configuration-related; these changes are described below.

3.1 Configuring NonStop SSL On The NonStop Server

The first step in setting up ASAP to use NonStop SSL is to configure NonStop SSL on the server. This involves determining which TelServ process will communicate over SSL, configuring SSL accordingly, and then starting the NonStop SSL process.

1) Determine Which TelServ Process Will Be Used With NonStop SSL

As stated above, NonStop SSL is installed as a layer between TelServ and your local network. In order to configure NonStop SSL, you must first decide which TelServ process will be used with it. This can be any TelServ process on your system; it could even be a TelServ process dedicated solely to ASAP created in accordance with the guidelines given in section 2.

Once you have decided which TelServ process you will use, record the name of the server TCP/IP process it uses for communication and the TCP/IP port it is listening on (by default this will be port 23). Note that **no** changes are required to the existing TelServ configuration.

For this example, we'll assume the TelServ process is using the default port of 23, and that the TelServ process is using the \$ZTC0 TCP/IP process for communication.

2) Choose The Port Number That Will Be Used For SSL Connections

In order to establish an SSL connection from the PC, you need to specify which TCP/IP port the NonStop SSL server will use. You can choose any unused port number. For this example, we'll use 8423.

3) Run The NonStop SSL SETUP Macro

This macro will create the NonStop SSL configuration on the server. The SETUP macro is located in the NonStop SSL subvolume, typically \$SYSTEM.ZNSSSL. From a TACL prompt, run the macro as follows (substituting the NonStop SSL subvolume name on your system if necessary):

```
TACL 1> VOLUME $SYSTEM.ZNSSSL
TACL 2> RUN SETUP
```

Once the macro is running, choose "TELNET SERVER" as the run mode. Then follow the installation instructions.

When prompted for the TCP/IP process name for the "listening port", enter the TCP/IP process name you recorded in step 1. In this example, that would be \$ZTC0.

When prompted for the port number for the "listening port" (i.e. the port number that NonStop SSL will use), enter the NonStop SSL port number you selected in step 2 above. In this example, that would be 8423.

When prompted for the TCP/IP process name for the "target TELNET port", again enter the TCP/IP process name you recorded in step 1. In this example, that would be \$ZTC0.

When prompted for the port number for the "target port" (i.e. the port number that your selected TelServ process is using), enter the port number you recorded in step 1. In this example, that would be 23.

The SETUP macro will create an SSL configuration file (e.g. TLNSCF0) as well as an SCF IN file (e.g. TLNSIN0) that you will use for configuring the NonStop SSL process as a persistent process in SCF.

4) Edit The SSL Configuration File If Desired

If necessary, you can make additions or changes to the SSL configuration file (e.g. TLNSCF0). See the *HP NonStop SSL Reference Manual* for details of the various configuration options. Note that no changes are required in order to configure NonStop SSL for use by ASAP.

5) Configure The NonStop SSL Persistent Process

Using the SCF IN file (e.g. TLNSIN0) created in step 3, from a TACL prompt run SCF to configure the NonStop SSL persistent process:

```
TACL 1> VOLUME $SYSTEM.ZNSSSL
TACL 2> SCF /IN TLNSIN0/
```

6) Start The NonStop SSL Process

You can now start the NonStop SSL process from SCF:

```
> SCF START PROCESS $ZZKRN.#SSL-TELNETS-0
```

At this point the SSL process will be running on the system and will be ready to accept connections from client systems.


3.2 Configuring The SSL Proxy And The CSG On The Windows PC

Once the NonStop server has been configured, you must set up the Windows PC that will be running the ASAP Client. To do so, you must first install the Remote SSL Proxy on the PC. After the installation is complete, you can configure the Remote SSL Proxy to communicate with NonStop SSL on the server, and then configure the CSG to utilize the Remote SSL Proxy. The end result is that all communication between the CSG and the NonStop server flows over an encrypted SSL connection.

1) Install The Remote SSL Proxy

NonStop SSL includes the installer for the Windows-based Remote SSL Proxy. This installer is located in the NonStop SSL subvolume on the server (by default this will be \$SYSTEM.ZNSSSL), and is named PROXYEXE. To install this on the PC:

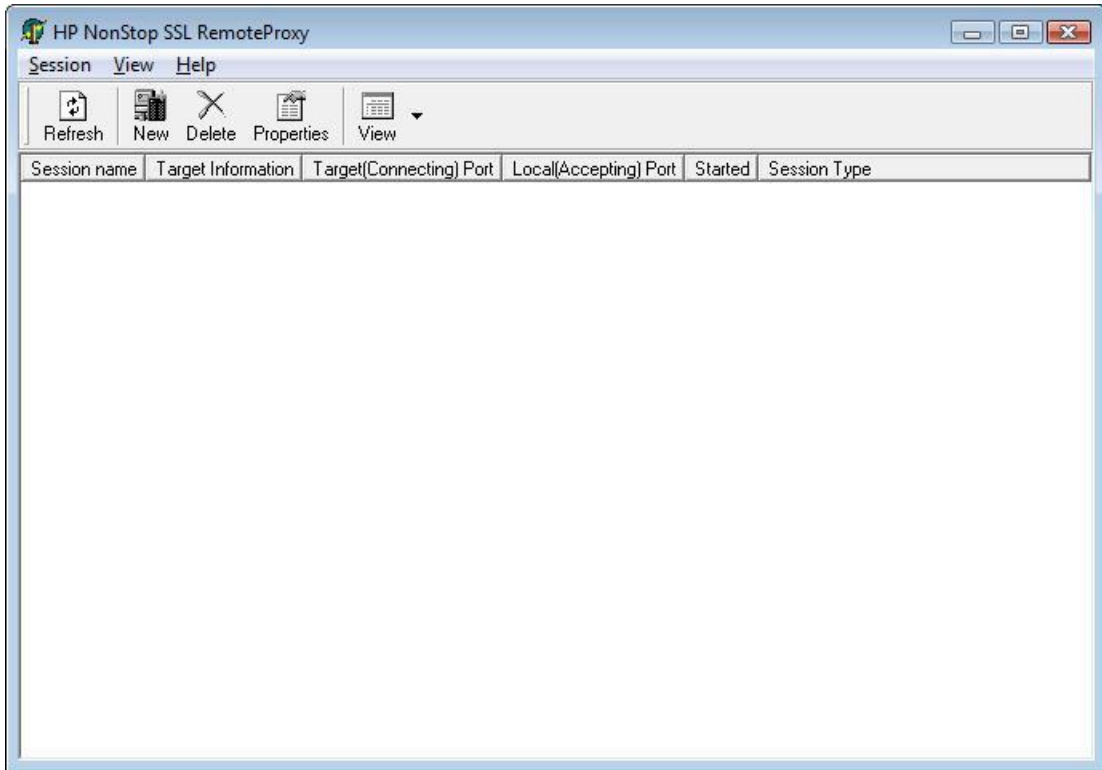
- Download PROXYEXE to the PC in binary format, and rename it to PROXY.EXE.
- On the PC, run PROXY.EXE to launch the installer.
- Follow the on-screen instructions to complete the installation.

Once the installation completes, you will be prompted to start the Remote Proxy. Choose to do so, and the Remote Proxy will be started on the PC and you will see the Remote Proxy icon () in the system tray.

2) Configure The Remote SSL Proxy

The next step is to configure the Remote SSL Proxy to connect to NonStop SSL on the server. To do so:

- Right-click on the Remote Proxy icon in the system tray and choose "Settings"; this will bring up the HP NonStop SSL RemoteProxy window:



- Click on the "New" button on the toolbar. The "New Session" property sheet will be displayed. On the "General" tab, set the values as follows:

For the "Protocol" field, select "Generic TCP/IP" from the list.

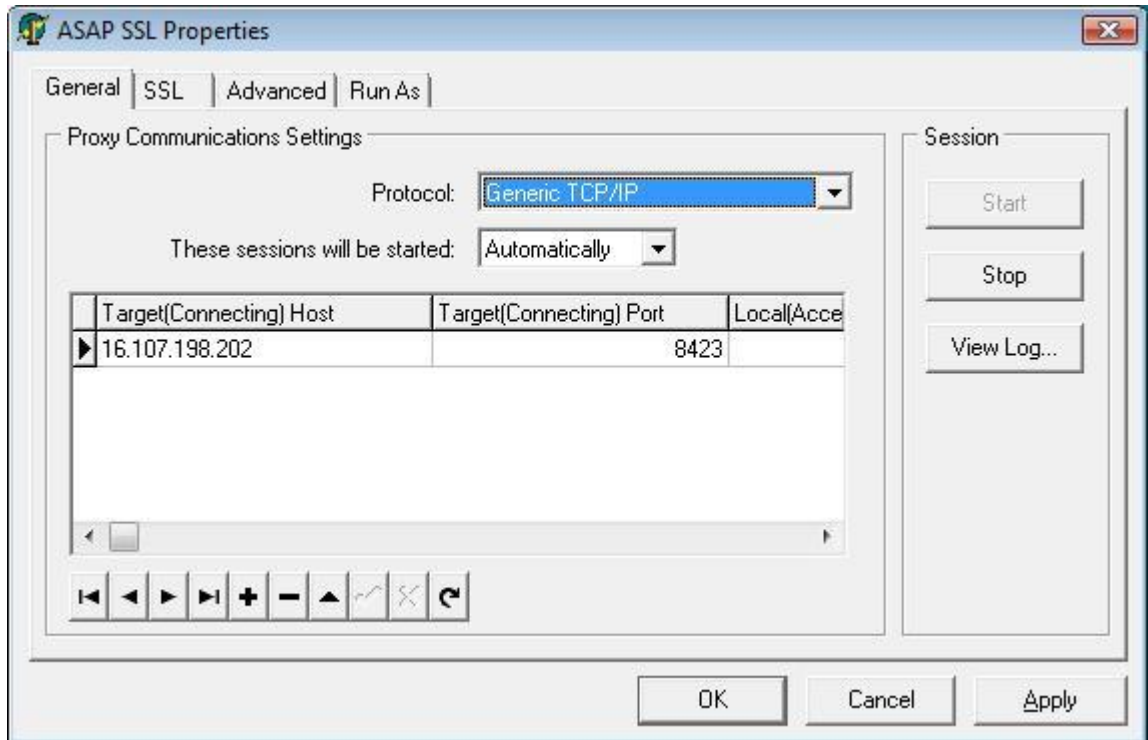
For the "These sessions will be started" field, choose "Automatically" from the list.

For the "Target (Connecting) Host" field, enter the TCP/IP address of the server configured in section 3.1. Note that you must specify the address of the server TCP/IP process being used by NonStop SSL. For this example, that value is 16.107.198.202.

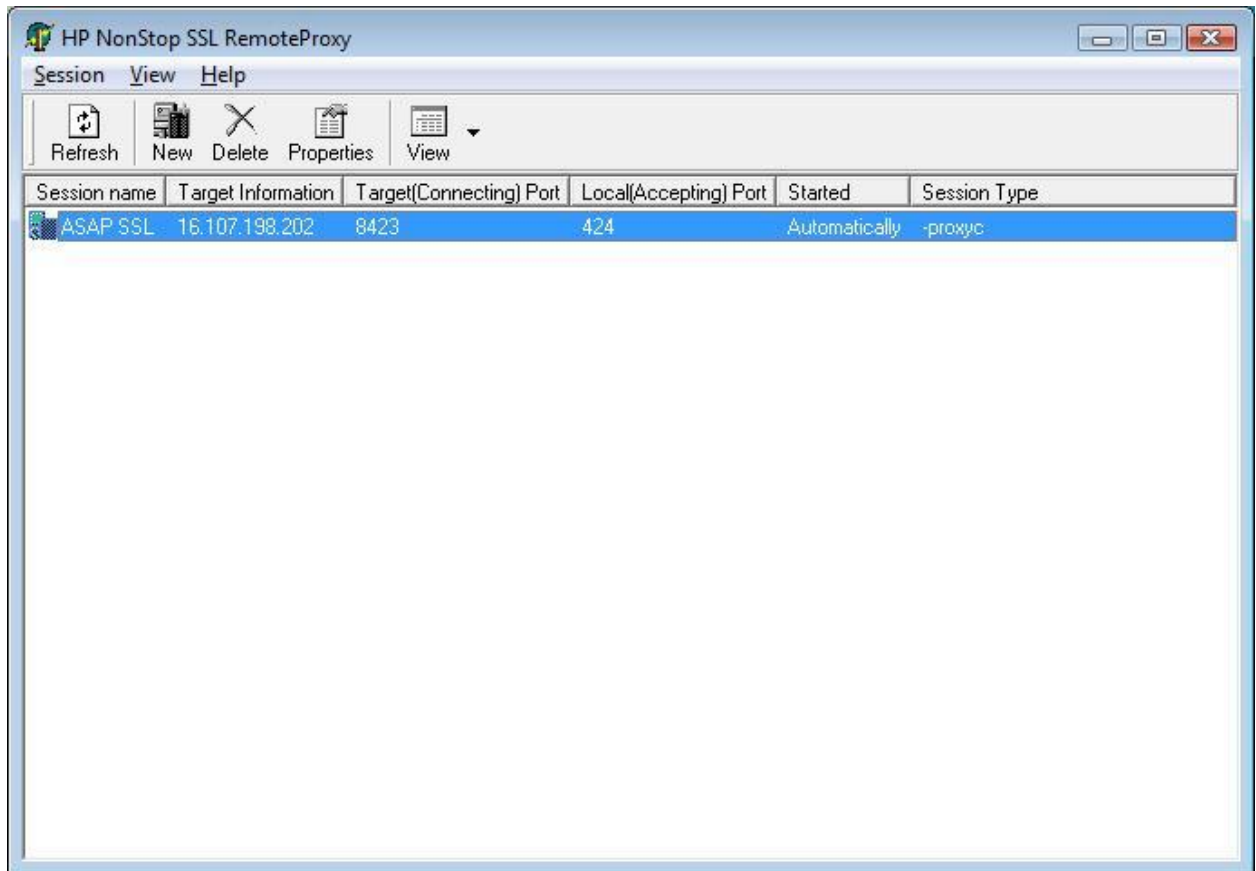
For the "Target (Connecting) Port" field, enter the port number you defined for the NonStop SSL process in section 3.1. In our example, that value is 8423.

For the "Local (Accepting) Port" field, enter any unused port number on the local PC. For this example, we'll use the value 424.

When you have finished entering these values, the property sheet should look something like this:



- Click the "OK" button to save the changes and return to the RemoteProxy window.
- On the RemoteProxy window, click on the name of the new entry in the Session list, and change the name of the session if desired (e.g. "ASAP SSL"). The RemoteProxy window would now look like this:



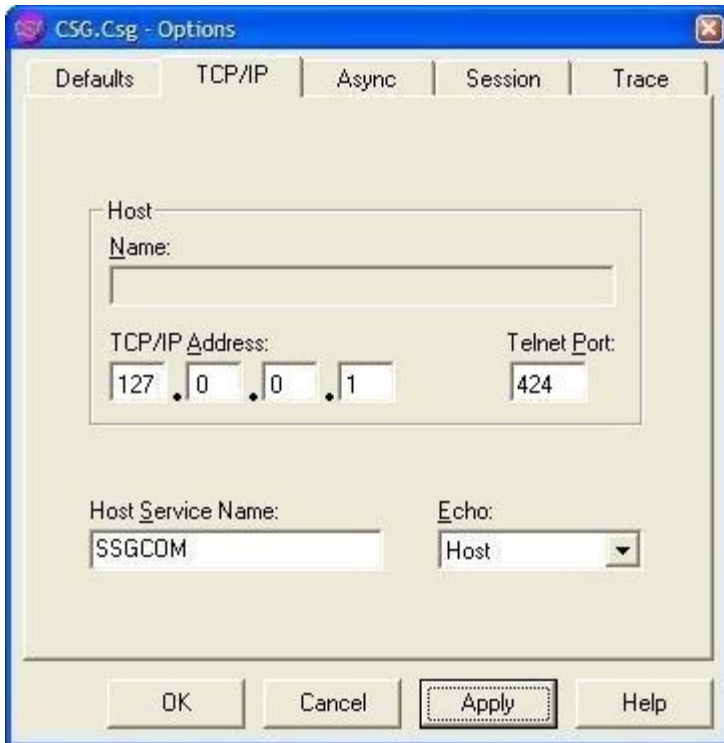
3) Start The Remote SSL Proxy

Now that the SSL proxy configuration has been defined, start the SSL connection by right-clicking on the session name and choosing "Start". The SSL connection will be started and will be ready for use.

4) Configure The CSG To Use SSL

Once the SSL connection is defined and started, the only step remaining is to re-configure the CSG to use the SSL connection. To do so:

- From the CSG main window, click on View...Options from the CSG main menu to bring up the CSG Options dialog, and click on the "TCP/IP" tab.
- Set the TCP/IP address to 127.0.0.1 (the local loopback address). This tells the CSG to communicate with the local PC.
- Set the Telnet Port number to the "Local (Accepting) Port" value configured above. In this example, that value is 424. At this point, the entire tab might look something like this:



Note that the Host Service Name might be TACL if you have not defined an SSGCOM service.

- Click "OK" to save the changes.

When the ASAP Client subsequently uses the CSG to communicate with the NonStop server, the SSL communication link will be used. This includes not only live ASAP statistical data, but also any initial logon and password that might be required.