SSL1000

User's Manual

P/N 707092-001

visara international

ISSUE/REVISION SCHEDULE		
Comments	**Rev. No.**	**Date**
Initial Release	707092-001	8/18/2004

The information contained in this document is subject to change without notice. **Visara International makes no warranty of any kind with regard to this material including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose**. Visara International shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Safety and Regulatory Information

Safety

* UL1950, CSA950

* CE Mark, IEC950, EN60950, EU Low Voltage Directive

Electro-Magnetic Interference

* This equipment has been tested and found to comply with the limits for FCC part 15 Class B environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause interference to radio communications. Operation is subject to the following two conditions:
  (1) This device may not cause harmful interface, and
  (2) This device must accept any interface received, including interface that may cause undesired operation.

* This apparatus complies with the CDoC CLASS "B" limits for radio interference as specified in the Canadian Department of Communications Radio Interference Regulations. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps are necessary to correct the interference.

* Cet appariel est conformé aux normes CDoC CLASS "B: D'Interference radio tel que specifier par le Ministère Canadien des communications dans les règlements D" Interference Radio. Cet équipment ne dépasse pas les limites de Classe B d'émission de bruits radioélectriques pour les appareils numériques, telles que prescrites par le Règlement sur le brouillage radioélectrique établi par le Ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécessaires pour en éliminer les causes.

* CE mark, EN50022 Class B, EN50082-1, EU EMC Directive

* UCCI-B

Software License Agreement

You should carefully read the following terms and conditions before operating the unit. It contains software, the use of which is licensed by Visara International ("Visara") to you for your use only as set forth below. Installation of the unit indicates your acceptance of these terms and conditions. If you do not agree with them, you should promptly return the complete system, including documentation, and your money will be refunded.

1 LICENSE. **In consideration of your payment of the license fee, Visara grants to you a nontransferable and nonexclusive license to use the enclosed proprietary software program and any documentation relating thereto (collectively referred to as the "Program") on a single computer at a single location, or in the case of multiprocessor versions of the Program, on one node of a network. You assume all responsibility for the selection of the Program to achieve your intended results and for the installation, use, and results obtained from the Program.**

2 PROGRAM OWNERSHIP. **You own the physical media on which the Program is originally or subsequently recorded or fixed. This Agreement does not transfer title and ownership of the Program or any underlying rights, patents, copyrights, trademarks, and trade secrets.**

3 RESTRICTIONS. **The Program, including the accompanying documentation, is copyrighted. Unauthorized copying of the Program, including a Program that has been modified, merged, or included with other software program(s) is expressly forbidden. You may not copy the documentation accompanying the Program. You may make one copy of the Program (excluding accompanying documentation) into any machine readable or printed form solely for backup purposes in support of your use of the Program on a single computer (certain Programs, however, may include mechanisms to limit or inhibit copying). You must reproduce and include the Proprietary Notices (as defined below) on the backup copy. You must maintain an accurate record of the location of the backup copy at all times. You may not electronically transfer the Program from one computer to another over a network. You may not distribute copies of the Program to others. You may modify the Program and/or merge it into another program for your use on the single computer. Any portion of this Program merged into another program will continue to be subject to the terms and conditions of this Agreement. You may not modify, adapt, translate, reverse engineer, decompile, or disassemble, or in any manner decode the Program in order to derive source code. You agree to never remove any patent, copyright, trademark, or other proprietary notices (collectively referred to as the "Proprietary Notices") or product identification affixed to the Program.**

Any attempted sublicense, assignment, rental, sale, or other transfer of the Program or any right thereto shall be null and void. **You may not use, copy, or modify the Program, or any copy, modification, or merged portion, in whole or in part, except as expressly provided for in this Agreement.**

4 TERM. **The license granted under this Agreement is effective until terminated. You may terminate it at any other time by destroying the Program together with all copies, modifications, and merged portions in any form. It will also terminate if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the Program together with all copies, modifications, and merged portions in any form, and to certify to Visara that they have been destroyed. Upon termination there will be no refund of any monies or other consideration paid by you.**

5 LIMITED WARRANTY. **The Program is Provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the Program is with you. Should the Program prove defective, you (and not Visara or its licensors, affiliates, contractors, suppliers, or agents) assume the entire cost of all necessary servicing, repair, or correction.**

Visara and/or its licensors do not warrant that the functions contained in the Program will meet your requirements or that the operation of the Program will be uninterrupted or error free. However, Visara and/or its licensors warrant the media on which the Program is furnished to be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery.

6 LIMITATIONS OF REMEDIES. **Visara's and/or its Licensors' entire liability and your exclusive remedy shall be: (1) the replacement of any media not meeting the "Limited Warranty" which is returned postage prepaid to Visara or an authorized representative with proof of payment; or (2) if Visara and/or its licensors are unable to deliver replacement media which is free from detects in materials or workmanship, you may terminate this Agreement by returning the Program and your money will be refunded.**

In no event will Visara, its licensors, affiliates, contractors, suppliers, and agents be liable to you for any damages, including any lost profits, lost savings, or other incidental or consequential damages arising out of the use or inability to use such Program (whether based on an action or claim in contract, tort, or otherwise) even if Visara, its licensors, affiliates, contractors, suppliers, and agents have been advised of the possibility of such damages or for any claim by any other party.

This Agreement will be governed by the laws of the State of North Carolina. Should you have any questions concerning this Agreement, please contact your Visara Sales Representative or Visara International, 6833 Mt. Herman Rd., Morrisville, North Carolina 27560.

You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions. You further agree that it is the complete and exclusive statement of the Agreement between us which supersedes any proposal or prior Agreement, oral or written, and any other communications between us relating to the subject matter of this Agreement.

Table of Contents

Page

Chapter 1. About the SSL1000

Usage Notice

Warning- To reduce the risk of fire or electric shock, do not expose this product to rain or moisture.

Warning- Please do not open or disassemble the product as this may cause electric shock.

Precautions

Follow all warnings and precautions as recommended in this user's manual to maximize the life of your unit.

Do:

- Turn off the product before cleaning.
- Use a soft cloth moistened with mild detergent to clean the terminal housing.

Don't:

- Block the slots and openings on the unit provided for ventilation.
- Use abrasive cleaners, waxes or solvents for your cleaning.
- Put heavy devices upon the terminal.
- Use under extremely hot, cold or humid conditions.

About the Product

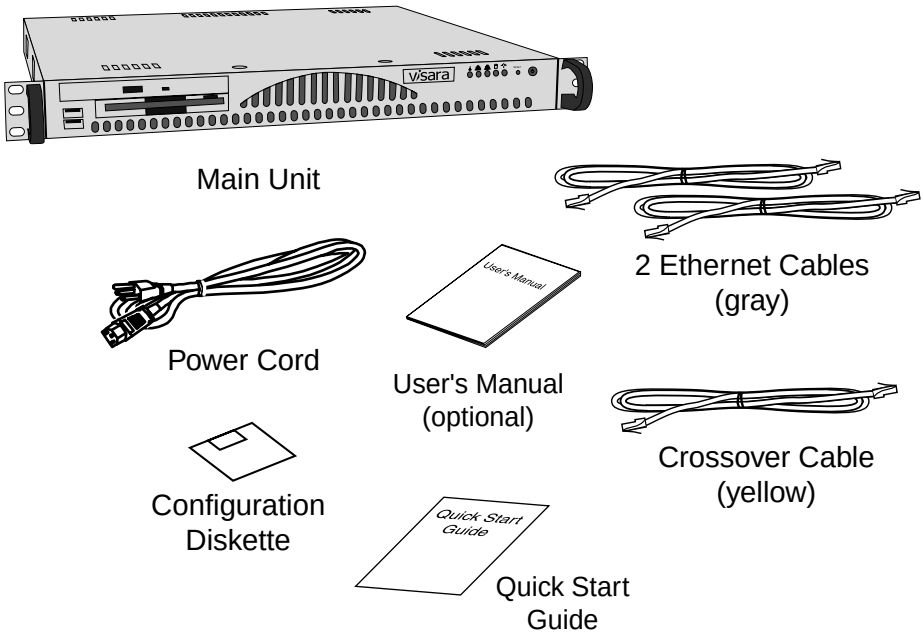
The SSL1000 allows a TN3270 to securely receive and deliver data between the server and clients across the internet. The SSL1000 is installed with the server and mainframes on one side and the internet on the other, serving as a the gateway between a secure network and the outside world.

The SSL1000 bridges the connections from "outside" to the "inside". If it receives data that is encrypted, it is decrypted first and then sent to the server. If the data is not encrypted it passes straight through the SSL1000.

Information presented in this manual includes procedures for hardware installation and software configuration and management.

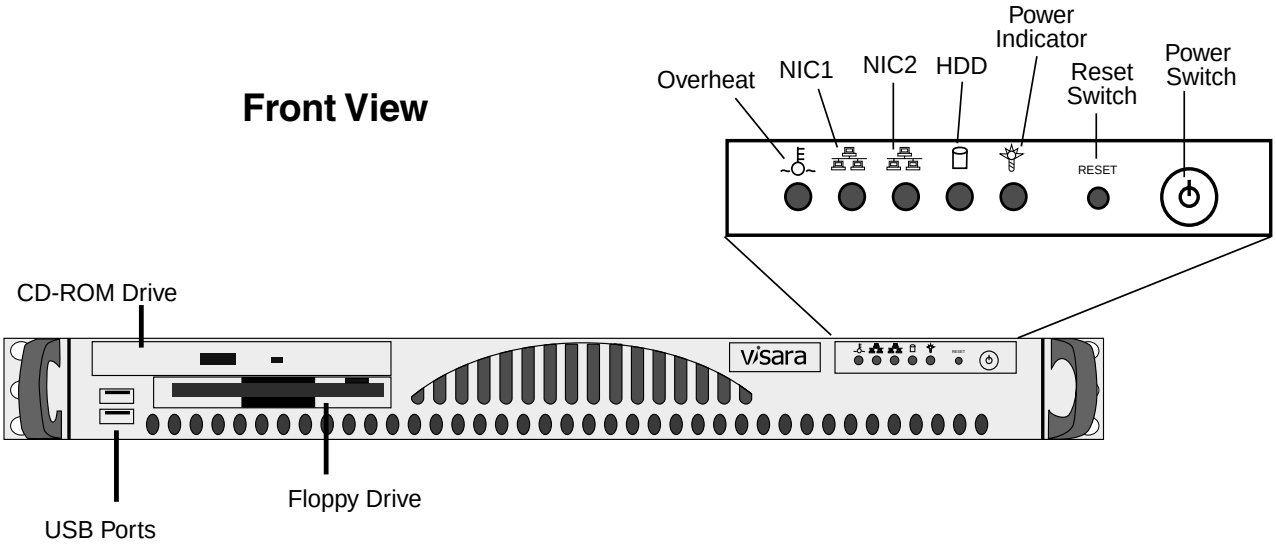
Package Overview

This unit comes with all the items shown below. Check to make sure your unit is complete. Contact your Sales person immediately if anything is missing.

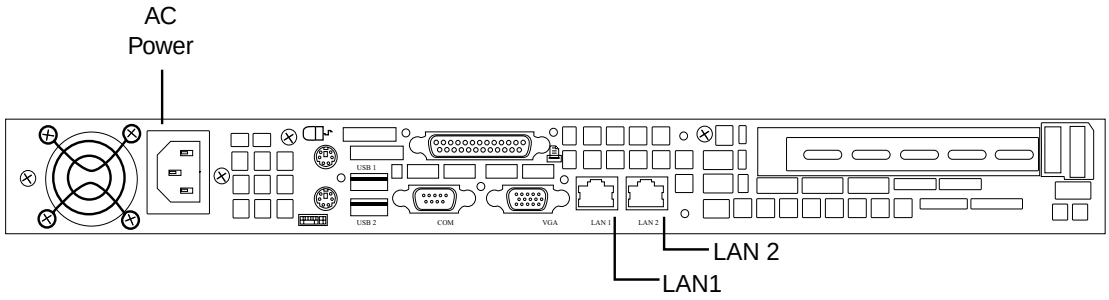


Product Overview

Front View



Rear View



Connector Introduction

- **Power Connector**
  Connects to the AC power cable.
- **Ethernet Connectors:**
  LAN1 - Connects the built-in 32-bit 10/100/1000 Ethernet network LAN Controller to the firewall/router (“outside” or “public” connection).
  LAN2 - Connects the built-in 32-bit 10/100/1000 Ethernet network LAN Controller to the TN3270 server (“private” or “trusted” connection).

Control Panel Indicators and Switches

- **Overheat**
  This led indicates that the server is overheating.
- **NIC1 and NIC2**
  These leds will flash when there is activity on LAN 1 and/or LAN 2.
- **HDD**
  This led indicates hard-drive activity.
- **Power Indicator**
  Indicates that power is being supplied to the server.
- **Reset Switch**
  The reset switch reboots the server.
- **Power Switch**
  This switch turns off the server power.

Specifications

Processor	- Intel® Pentium® IV - 2.4Ghz
Main Memory	- 512Mb DDR
Networking	- TCP/IP - 10/100/1000BaseT Ethernet, twisted pair (RJ-45)
I/O Ports	- One 3-pin AC power connector - Two 8-pin female RJ-45 ethernet connectors - One 15-pin female VGA compatible connector ** - One 6-pin female PS/2 mouse connector ** - One 6-pin female PS/2 keyboard connector ** - One 25-pin female parallel connector ** - Four Universal Serial Bus (2.0) connectors **
Peripheral Bays	- One slim 3.5" floppy drive - One slim CD-ROM drive
Power Supply	- Type: 200W - Input: AC 100~240V
Dimensions	- (W x H x D) 16.7" x 1.7" x 14" (425mm x 44mm x 355.6mm)
Weight	- Net: Full System: ~9.5 lbs. (4.3 kg.) Gross: Full System: ~17.5 lbs. (8 kg.)
Environmental	- Operating Temperature: 50ºF~90ºF (10ºC~35ºC) - Operating Humidity: 8% to 80% Non-condensing
Safety Regulation	- FCC-B, CE, UL, CUL, TUV, CISPR 22 (EN 55022)

** These connectors are not used on the SSL1000. Do not connect peripheral equipment to these ports.

Chapter 2. Installation and Configuration

Installation

Basic Setup

Follow these instructions to connect the SSL1000:

1. The SSL1000 ships with three CAT5 ethernet cables: two standard and one "crossover". The standard cables should be used to connect the SSL1000 to an ethernet hub/switch. The crossover cable (which is yellow and labeled "crossover") should only be used for a direct connection from the SSL1000 to a server.
2. LAN1 is typically used for the "public" or "untrusted" side, where the traffic must be encrypted. This will normally be the path from the firewall/router to the outside world.
3. LAN2 is typically used for the "private" or "trusted" side, where the LAN cannot be monitored, and is considered safe for unencrypted traffic.
   Facing the back of the unit, LAN1 is the RJ-45 connector on the LEFT next to the VGA connector. (The keyboard, mouse, and monitor are only used for diagnostic purposes.)

Configuration

Editing the SSL.INI File

Before powering up the SSL1000, the SSL.INI file must be configured for the correct IP addresses. Using a text editor such as Window's® Wordpad, open the SSL.INI file on the included diskette. Change the IP addresses to the desired values (see example below). If the original diskette cannot be located, the file may be created with the entries as shown below.

Note: No whitespace (spaces or tabs) is allowed in the entries in this file. The data in this file is not case sensitive.

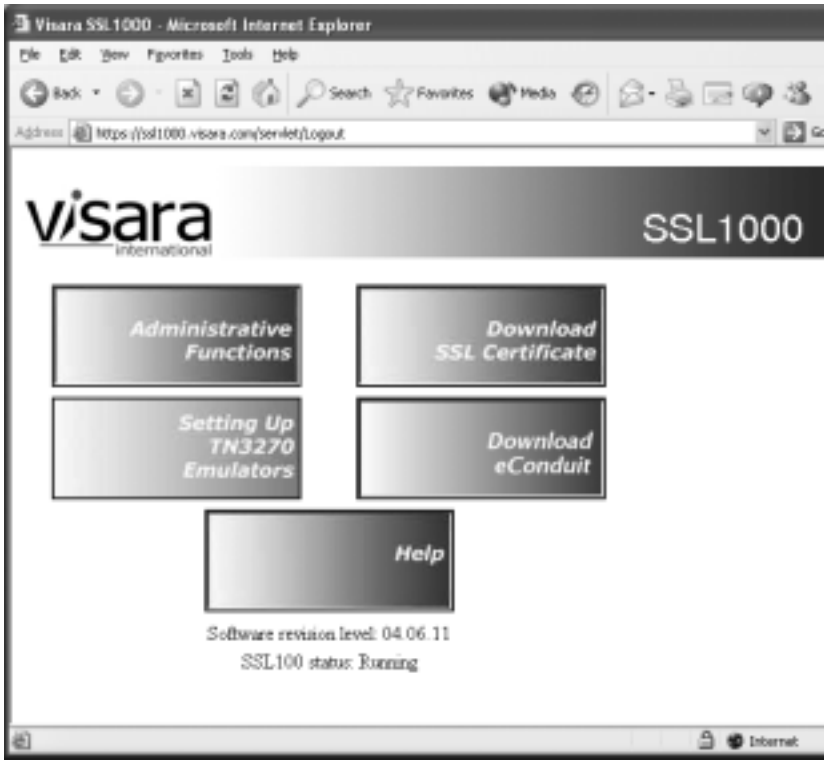
```
[Configuration]
LAN1IP=204.48.36.155
LAN1NetMask=255.255.255.0
LAN2IP=192.168.1.1
LAN2NetMask=255.255.255.0
DefaultGateway=204.48.36.254
DNSserver=204.48.35.4
```

Save the file, and insert the diskette into the floppy drive on the SSL1000. Power on the unit. As the SSL1000 boots, the file will be saved onto the hard drive. The settings in the file will become effective immediately.

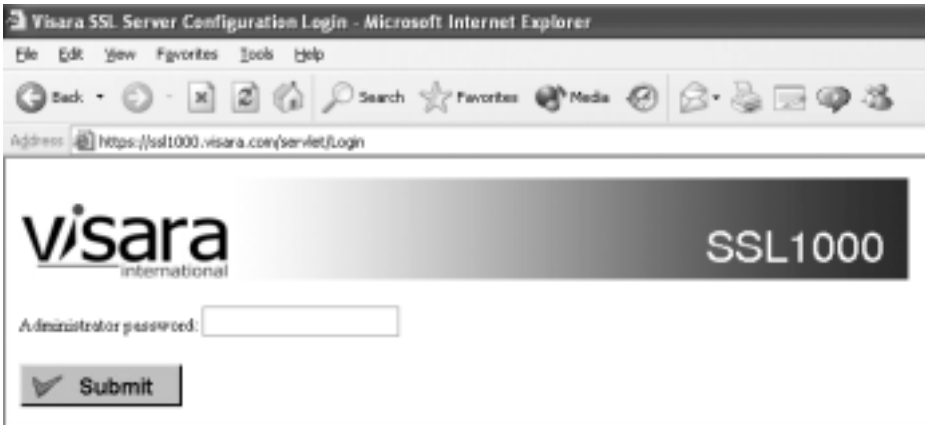
Note: The diskette is not required for future reboots and should be removed after the initial load.

Warning - If the diskette is in the drive when the SSL1000 is powered up in the future, the settings contained in its SSL.INI file will override any settings on the hard drive that have been changed or defined with a web browser.

To manage the SSL1000 configuration, all that is needed is a web browser. Log in to the server configuration utility using the IP address you assigned to the SSL1000 during the initial setup. (Either LAN connection can be used.) For instance, if the server was assigned the IP address of 204.48.51.51, you would enter **http://204.48.51.51** in the browser address window.



Click **Administrative Functions**. You will be prompted for the administrator password (the default password is **admin**, and is case sensitive).

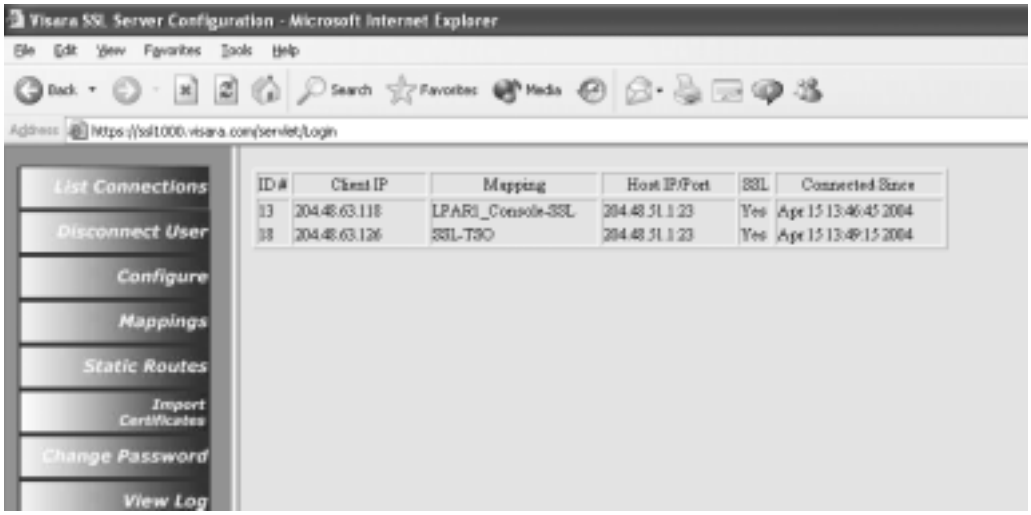


Note: The administrator password should be changed as soon as possible to protect the SSL1000 configuration.

The pages that follow describe the configuration screens that may be accessed from the web browser.

List Connections

The List Connections page will show the IP addresses of all clients that are connected to the server and the status of their connection.



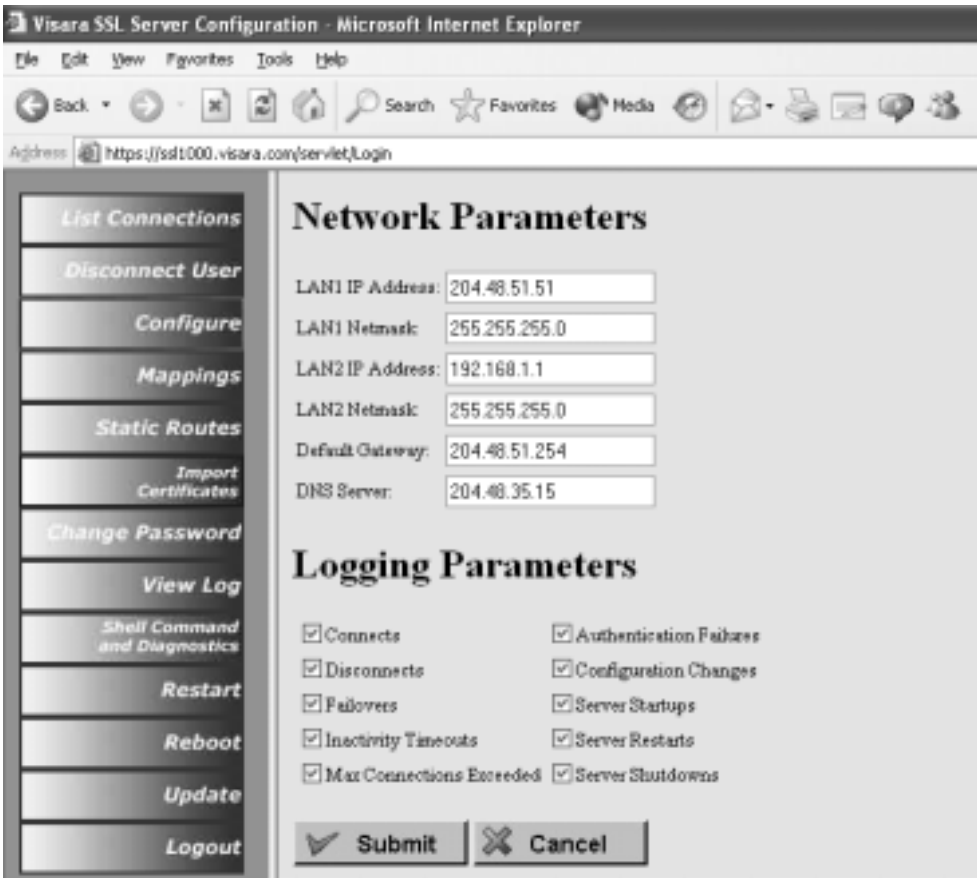
- **ID#** - An index number for this connection. It is used on another panel to disconnect that client.
- **Client IP** - TCP/IP address of the client.
- **Mapping -** The name of the defined mapping that was used to connect.
- **Host IP/Port** - The IP address of the server, and the TCP port used for the connection.
- **Connected Since -** Date and time of the origination of the connection.

Disconnect User

Enter the ID # of any user and click **Disconnect**. You will be asked to confirm the action before disconnecting the client.

Configure

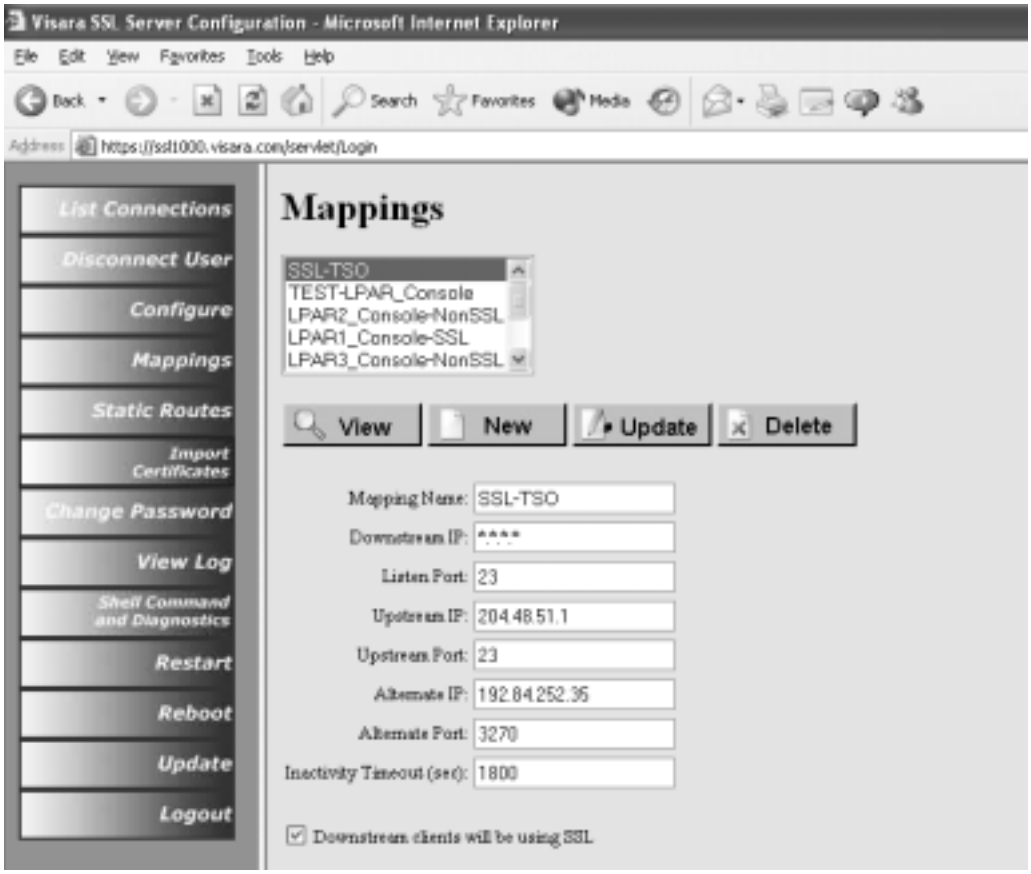
Once the initial configuration has been accomplished using the diskette, subsequent changes to the network parameters may be made on this screen. In addition, logging parameters may be set or changed. Changes in logging parameters take affect immediately. Network parameters require a complete reboot of the server.



Warning - If you enter incorrect data on this configuration screen and reboot, you may not be able to reach the SSL1000 with your browser in order to make a correction. In this case use the original floppy with the SSL.INI file to correct the settings.

Defining the Upstream and Downstream Mappings

Upstream to downstream Mappings are at the heart of the SSL1000. These define the path that the data will take, who may connect to which server, and which connections will be encrypted.



Define a new mapping

1. Enter a distinctive name for the mapping.
2. Enter the Downstream Client IP address. Asterisks may be used as wildcards. (*.*.*.*)
3. Enter the TCP port that the SSL1000 will use to "listen" for client connections. Telnet and TN3270 typically use port 23, but it is more secure to use values above 1024.
4. Enter the Server's IP address and Port number. An alternate address is optional. DNS names are not allowed.
5. Enter the inactivity timeout, which tells the SSL1000 how many seconds to wait before disconnecting an inactive (no traffic to or from) client. Entering zero will disable this feature.
6. Check **Downstream clients will be using SSL** if the client connection will be secured with SSL. Unchecking this creates a passthrough with no encryption. The host side cannot be encrypted.
7. Click the **New** button. The mapping will be saved and its name will be added to the list of mapping names in the scrollable box.

Note: If the name you entered already existed in the list, an **update** will be done.

View details of mappings that have already been defined

1. Select the name of the mapping in the scroll box.
2. Click **View**. The details will appear in the fields below.

Update any field of an existing mapping

1. Select the name of the mapping in the scroll box.
2. Click **View**. The details will appear in the fields below.
3. Change any necessary information.
4. Click **Update**. The new definition will be saved.

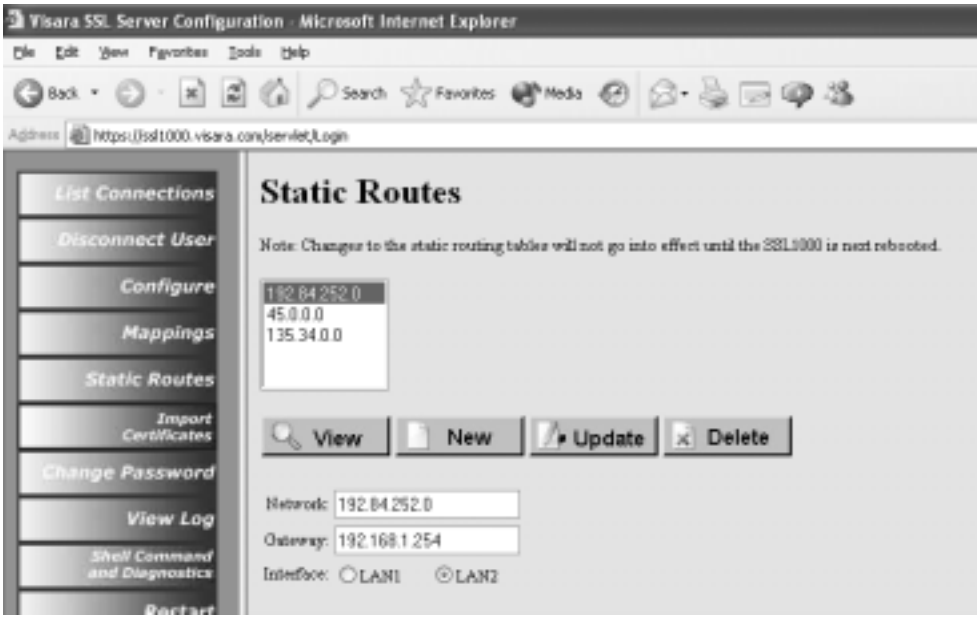
Delete an existing mapping

1. Select the name of the mapping in the scroll box.
2. Click **View**. The details will appear in the fields below.
3. Click **Delete**. The mapping will be deleted.

Note: Deleting a mapping does not disconnect a current user.

Static Routes

Static Routes are needed whenever there is a network you need to reach that cannot be reached using the Default Gateway, but instead can be reached through another router in your network. A static route consists of the destination network you need to reach, the router's IP address used to reach it, and which LAN interface in the SSL1000 to use.



Define a new static route

1. Enter the network address for the static route. The network address you enter can be an individual address or a whole subnet. Use zero(s) at the end of the IP address to indicate the entire subnet. For example:
   204.48.41.0 refers to the 254 addresses in the Class "C" network of 204.48.51.**1** through 204.48.51.**254**.

156.48.0.0 refers to the 64,534 addresses in the Class "B" network of 156.48.**1.1** through 156.48.**254.254**.

2. Enter the Gateway, the IP address of the router used to reach the destination network.
3. Select the LAN interface which will be used by the SSL1000 to reach the network.
4. Click the **New** button. The static routes are stored in the SSL.INI file immediately, but are loaded in the TCP/IP routing tables at boot time. For these routing changes to take effect a **Server Reboot** is required.

Note: If the network address you entered already existed in the list, an **update** will be done.

View details of static routes that have already been defined

1. Select the network address in the scroll box.
2. Click **View**. The details will appear in the fields below.

Update any field of an existing static route

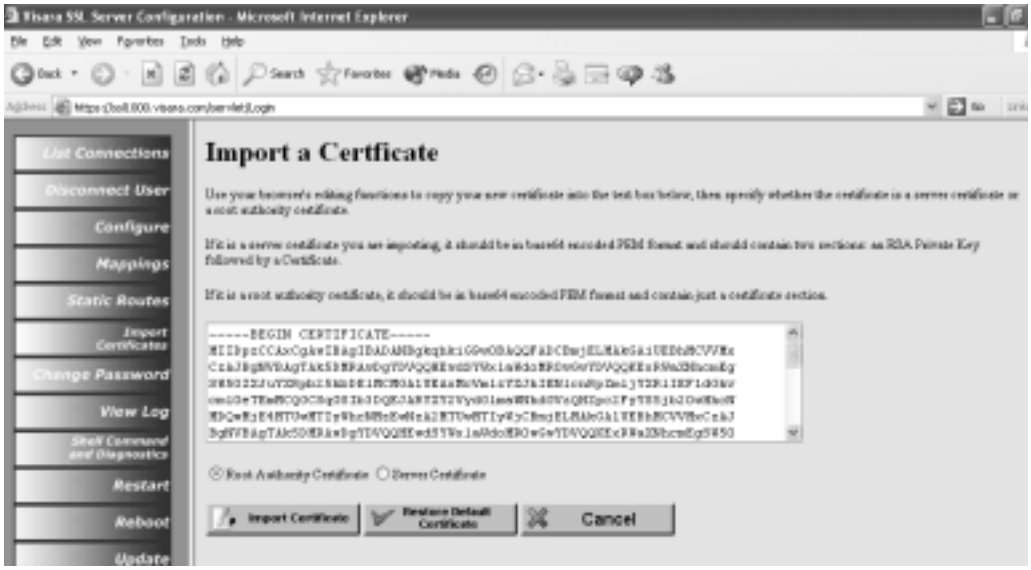
1. Select the network address in the scroll box.
2. Click **View**. The details will appear in the fields below.
3. Change any necessary information.
4. Click **Update**. The new definition will be saved.

Delete an existing static route

1. Select the network address in the scroll box.
2. Click **View**. The details will appear in the fields below.
3. Click **Delete**. The static route will be deleted.

Note: Deleting a static route does not disconnect a current user.

Import Certificates



Server Certificate

This function will import a server certificate that has been issued by a certificate authority, such as Verisign. The certificate should be in Base64 encoded PEM format and should contain two sections, a RSA private key followed by a Certificate. The text will be copied from the PEM file and pasted into the dialog box. It must include the following headers and trailers, plus the text in between:

-----Begin RSA Private Key-----

<key data>

-----End RSA Private Key-----

-----Begin Certificate-----

<certificate data>

-----End Certificate-----

Root Authority Certificate

The CA Certificate that you import here is what will be downloaded to clients using the "Download SSL Certificate" button on the SSL1000 main menu.

The certificate should be in Base64 encoded PEM format. The text will be copied from the PEM file and pasted into the dialog box. It must include the following header and trailer, plus the text in between:

-----Begin Certificate-----

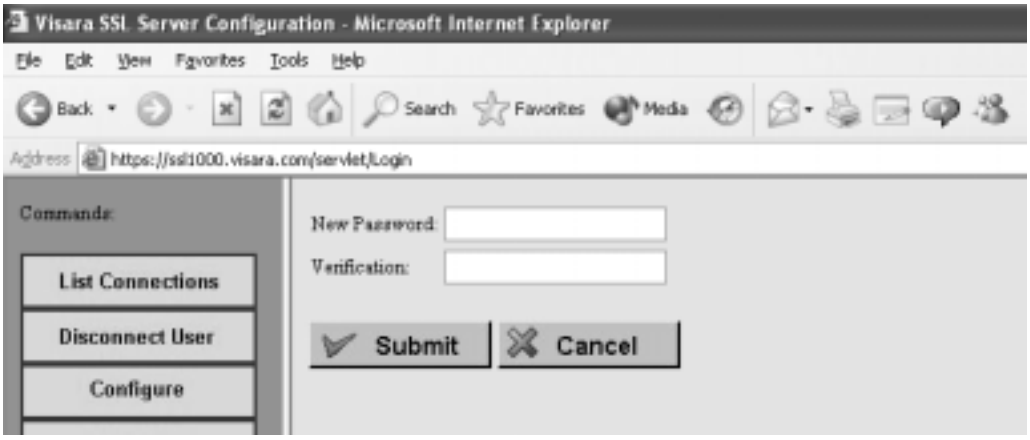
<certificate data>

-----End Certificate-----

Change Password

To change the password that will allow access to the configuration screens, enter the new password. Enter it once again as verification, and click **Submit**.

Note: Password is case sensitive.

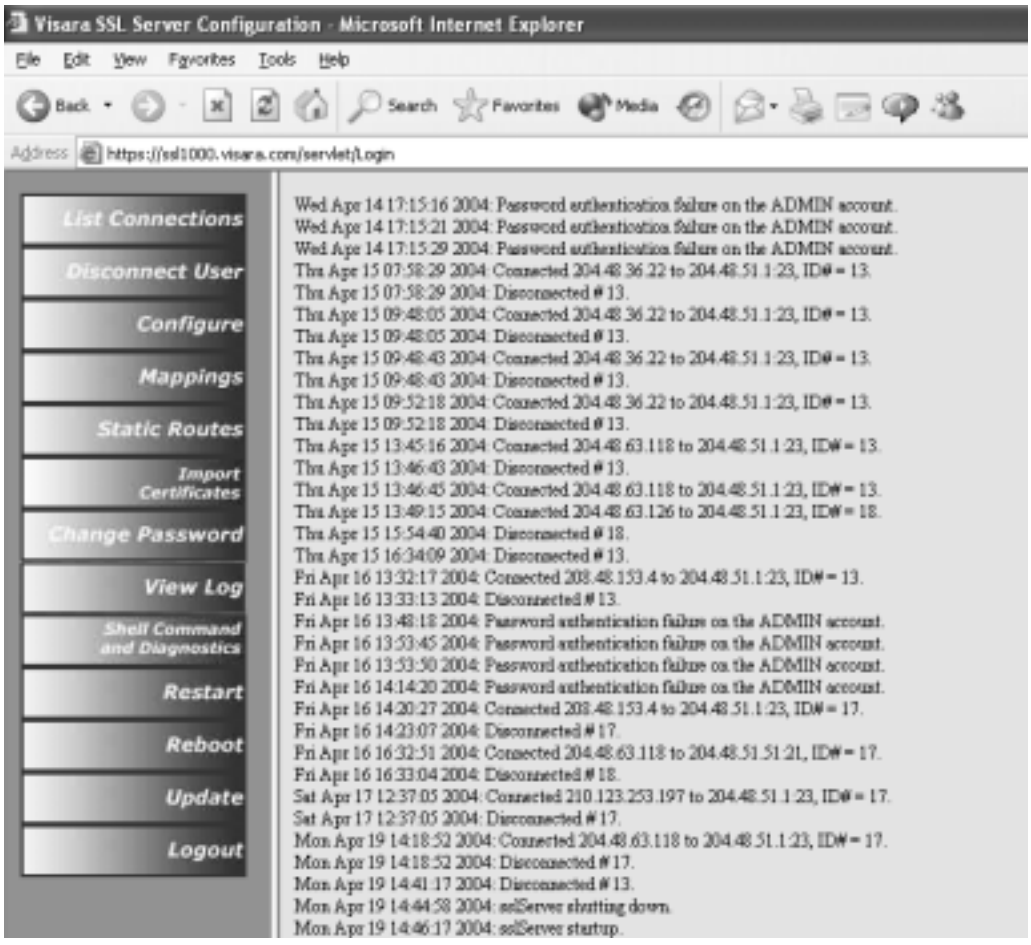


View Log

The logging parameters are defined on the configuration screen (click the **Configure** button on the left navigational menu.). You may select to have the following events logged:

- **Connects**
- **Disconnects**
- **Failovers**
- **Inactivity Timeouts**
- **Max Connections Exceeded**
- **Authentication Failures**
- **Configuration Changes**
- **Server Startups**
- **Server Restarts**
- **Server Shutdowns**

To view the log (an example is shown below) click the **View Log** button on the left navigational menu.



The log shows the oldest entries at the top, with the most recent entries at the bottom.

Shell Commands and Diagnostics

Shell commands execute the Linux bash Shell using the browser interface. Shell commands that need to be manually interrupted or require user input must be avoided. For instance, "Ping" with no count ("-c" parameter), would run until the server is rebooted.

Restart Server

Select to restart the server application. You will be asked to confirm the action. This function takes only a few seconds.

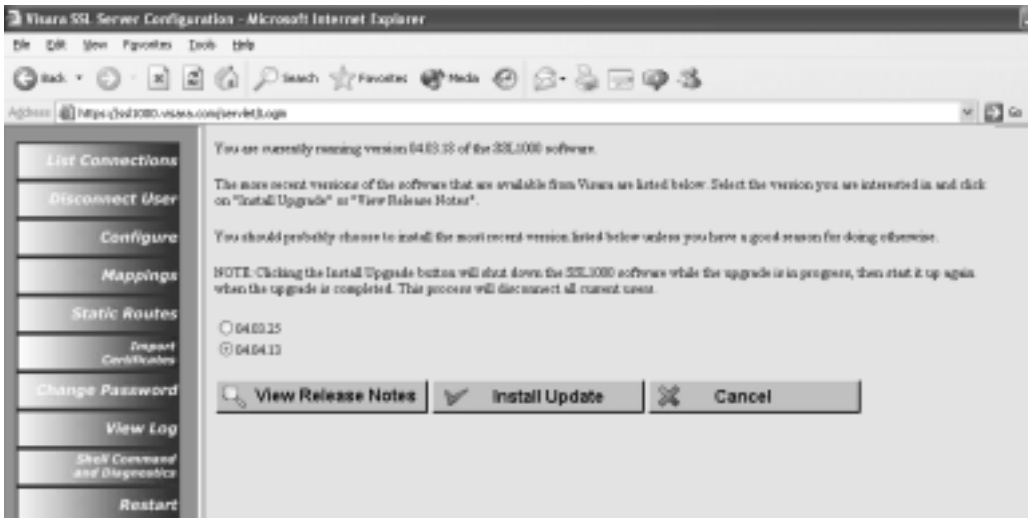
Note: This will disconnect all of the current mapped connections. The administrator interface will remain active.

Reboot Server

Select to reboot the server. You will be asked to confirm the action. Rebooting the server takes about one minute.

Note: This will disconnect all connections including the administrative interface.

Update



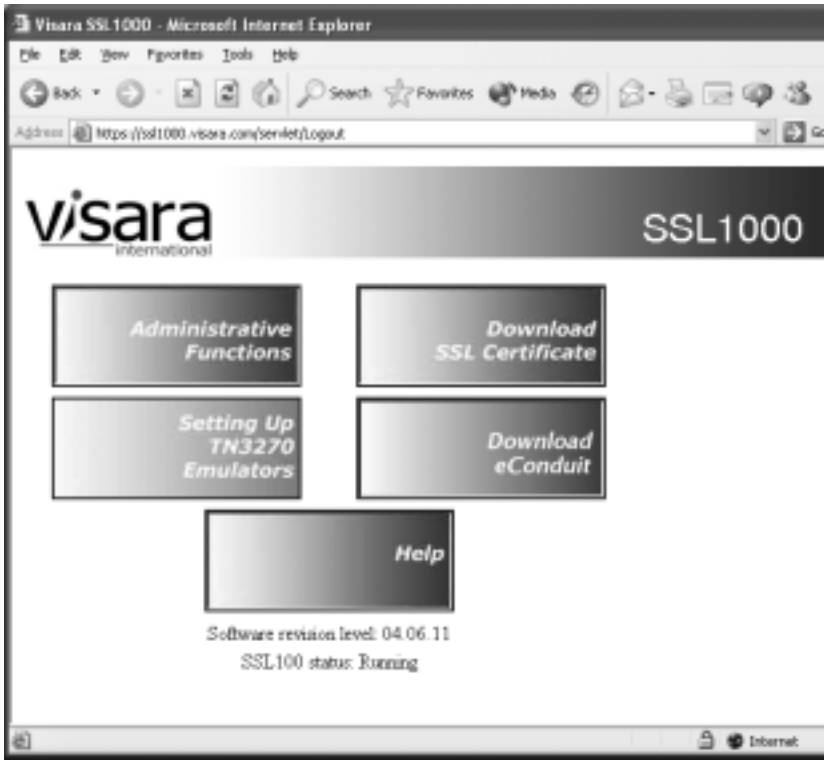
This function allows the server software to be updated directly from Visara.com. This function requires ftp access to Visara.com.

Note: The server will automatically restart after the software installation is complete.

Logout

Clicking **Logout** will immediately disconnect the current administrator session. The session will automatically logout after 30 minutes of inactivity.

Download eConduit



Clicking here will begin a download of the eConduit application for Windows. eConduit provides SSL encryption for TN3270 and Telnet clients that do not have it built in. After running the Windows Installer, you will have an entry in your Start Menu for Visara Intl > eConduit.

eConduit behaves like a miniature, client-side, SSL1000. You configure IP address and TCP port mappings, and eConduit will do the SSL encryption and decryption. This means that you point your TN3270 client to yourself (using the 127.0.0.1 "loopback" address), and eConduit, running on your PC, encrypts and forwards the traffic on to the SSL1000.

Chapter 3. SSL1000 Overview

Overview of Public Key Infrastructure (PKI)

There are two aspects of PKI:

- **Encryption** - the scrambling of data to make it unreadable (and unchangeable without detection).

- **Authentication** - the process of assuring that you're talking to whom you think you're talking to, by using certificates.

Encryption is the easier to talk about, because no one knows how it works, just that it works, and to what level it is "unbreakable". You have no doubt seen the little lock at the bottom of your web browser while conducting a *secure* transaction over the Internet. This means that the data back and forth is being encrypted, so that any evil forces (or college hackers) who happen to be somehow monitoring the traffic, will not be able see your passwords, account numbers, etc. You have also heard of the export ban of encryption technology stronger than 40 bits (now lifted).

The 40-bit and 128-bit (and now 168-bit) encryption strengths that you hear bandied around refer to the *symmetric* encryption process. (Yes, there is also an *asymmetric* process…just read on). The symmetric process means that the same 128-bit key is used to encrypt the data being sent, and to decrypt the data received. This process is fairly efficient, so it is used for the bulk of the Secure Socket Layer (SSL) traffic.

When two computers need to encrypt data, they first must exchange the 128-bit key. When they connect, the "server" side will randomly generate this key, and send it to the "client" computer. Then they both use the same key to secure the data for as long as they stay connected. But how can they prevent this key from being intercepted by the evil eavesdropper? It must be encrypted as well. Enter *asymmetric* encryption and *digital certificates.*

Asymmetric encryption is an algorithm that uses two keys. Data that is encrypted with one can only be decrypted with the other. So the plan goes like this: Give anybody and everybody one of the keys (the *public key*), and keep the other safe on your PC or server, locked away under password protection. If you want to exchange encrypted data with someone, you send them the public key. They use it to decode what they receive from you and it is also used to encrypt the data sent to you. It can only be decrypted with the private key, so even if the evil snoopers see the data, and have the public key, they can't decrypt the data.

"Why not just encrypt all the traffic with this public/private technique?" you ask. This algorithm requires *much* more processing, and requires 1024 or even 2048-bit keys in order to make it as unbreakable as the 128 bit keys in symmetric encryption. So to keep things flowing faster, an *asymmetric* process protects exchanging the *symmetric* key, which then protects exchanging the real data.

So if protecting your data from bad guys with LAN monitors is all you are after, you're done.

But how can you be sure the bad guys have not set up a fake web server, that looks just like your bank's web page, and is just sitting there waiting for you to log in so they can steal your username and password? In technical jargon, how can you *authenticate* your connection?

Authentication is done with digital *certificates*. These are encoded blocks of data, that include some information like the company name and location, a contact name, how long the certificate is valid, what algorithm is used, and the same asymmetric public key we discussed previously. Another very important piece of information included is *who created the certificate.*

This is *very important* because how can you be sure the bad guys didn't create a fake certificate too? There is a group of companies that provide the service of creating digital certificates, and everybody in the world trusts them, just like Swiss bank accounts (mysterious, but trustworthy). These trusted *Certificate Authorities*, like Verisign and Thawte, publish their digital signatures, and companies like Netscape and Microsoft include them in their browsers.

If you buy a certificate from Verisign for your web server, it will have your server information in it, along with Verisign's public key, so that the browsers will see your certificate, who issued it, and their certificate. The browser matches the issuer's certificate with its list of known Certificate Authorities. If there is a match, it declares your certificate to be trustworthy. If there is no match, the browser will put up a warning that the certificate can not be verified to be trustworthy, and will allow you to decide to accept or reject the connection.

There are several types of certificates:

- **Server Certificate**. The most common - what is passed from server to client when a connection is made. This certificate includes the issuer's certificate.
- **Certificate Authority (CA) Certificate**. This can be stand-alone or included in with an issued certificate. If it is in the list of "trusted certificate authorities", then all certificates issued by that CA are "trusted".
- **Intermediate Certificate Authority Certificate**. This is when a trusted CA gives license to someone else to issue CA certificates in his name. For example, Verisign may grant a university the right to issue CA certificates, that include Verisign's signature, for all the campus servers. As long as the "chain of trust" goes back to someone truly trusted, certificates issued by the Intermediate will be trusted.
- **Client Certificate**. These are used to authenticate a client to a server. The server has to ask the client for his certificate (the client can't just send it unsolicited), and the server has to be configured to do this. The client's public key is imported into the server's "key ring" and is checked every time the client connects. Client certificates are often used instead of usernames and passwords.
- **S/MIME Certificate**. This is typically used to encrypt email, but can be used as a client certificate. Thawte and Verisign will issue these to individuals - free for the asking.

Certificates in the SSL1000

The SSL1000 comes with three digital certificates:

- An “SSL1000” server certificate for the SSL proxy (for TN3270 mappings)
- An “SSL1000” server certificate for the web server (for administration)
- A Root Certificate Authority (CA) certificate from the Visara Certificate Authority, who issued the other two.

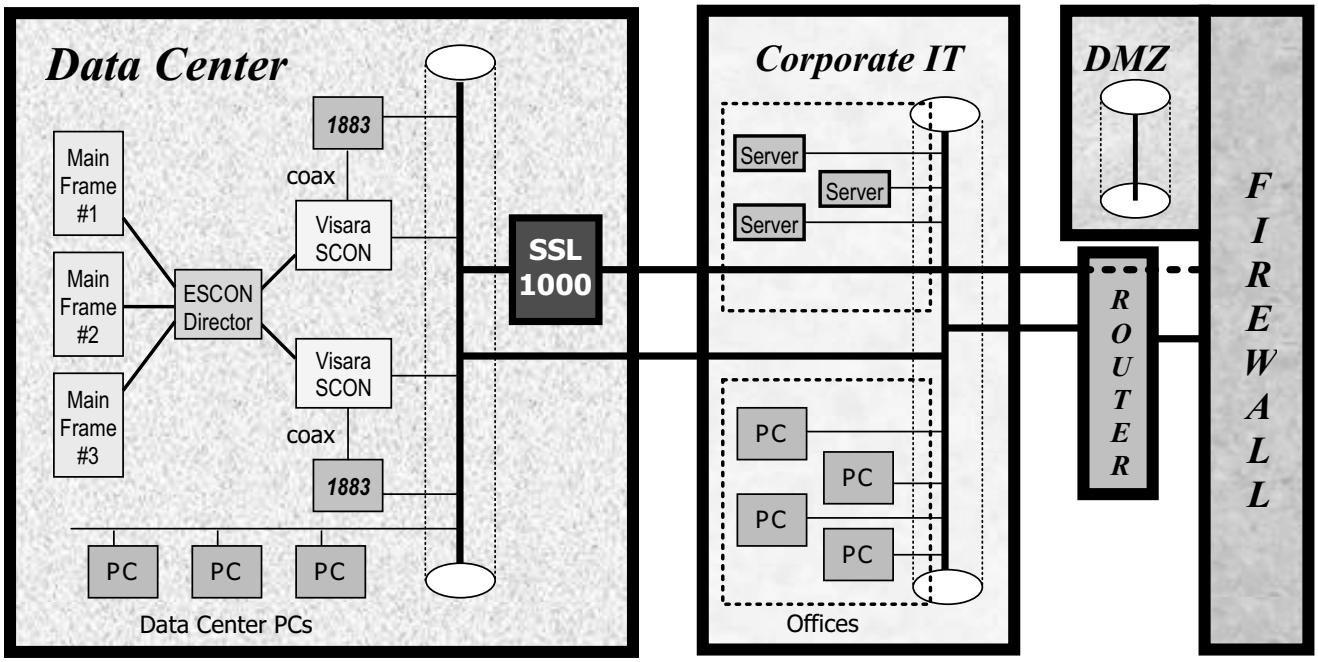
A server certificate will be sent to the client during each SSL connection that is negotiated. The Root CA certificate is available to download through the web server. If you install the CA certificate then all certificates issued by that CA will be trusted.

Note: Because Visara ships all these units with the same server certificates, you cannot rely on the built-in certificates for authentication. The built-in certificate should only be used to facilitate Encryption, and not to verify the identity of the server. Visara International, Inc. assumes no responsibility for loss of security or intellectual properties due to unsafe certificate management. To secure the identity of your SSL1000, you should obtain a valid server certificate from a trusted Certificate Authority.

The steps required to obtain a server certificate from a trusted CA are beyond the scope of this Overview. But there are directions later in this manual for importing the certificate once it is obtained.

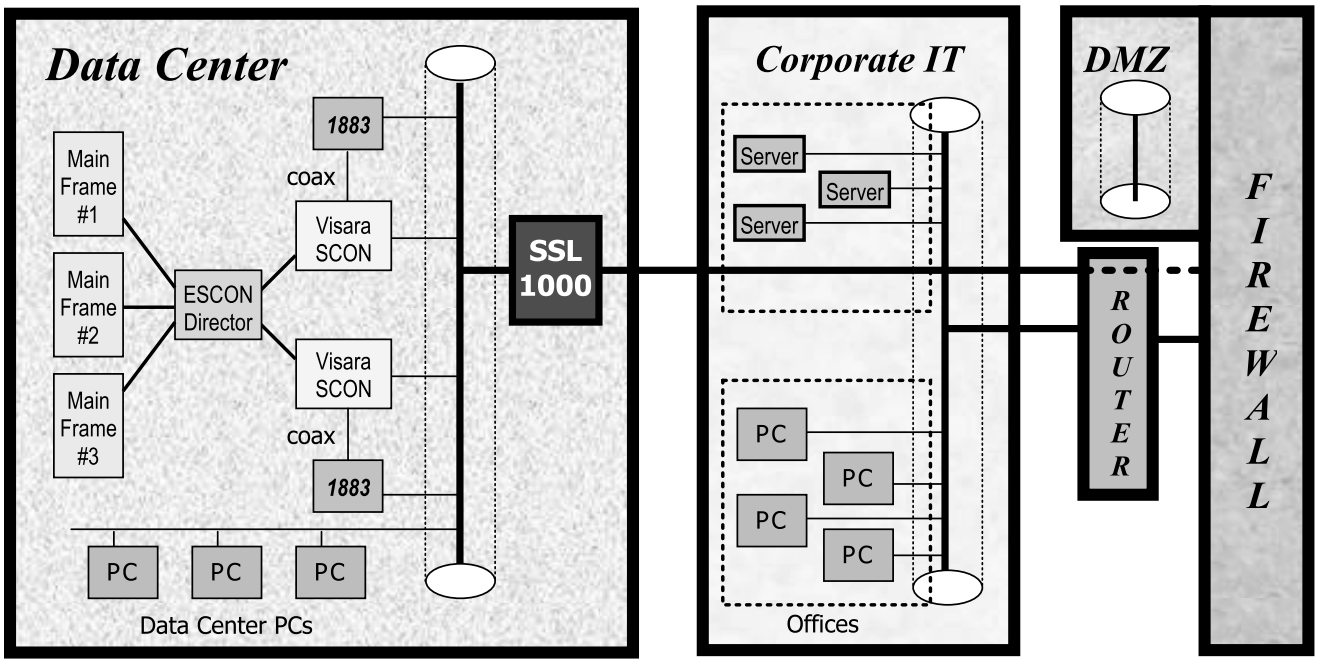
SSL Topology in Typical Network

The SSL Server furnishes a gateway between a local network and the Internet via an ISP's (Internet Service Provider's) communications server. The SSL1000 on the LAN is connected to the ISP by way of a modem, ISDN or router. The other link of the SSL Server is to the network controller or mainframe. The following diagrams illustrate three possible network configurations:



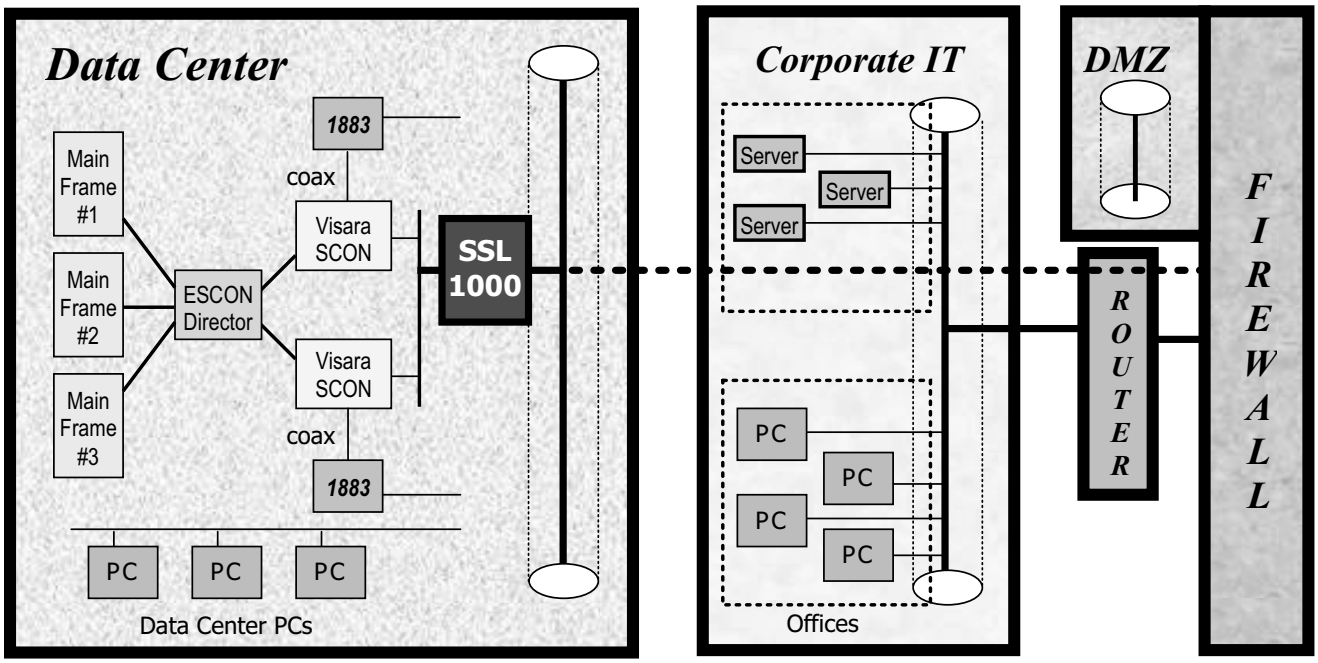
Trust Everyone Behind the Firewall

Everyone behind the firewall can reach the data center. There is no need for encryption except when coming through the firewall from the outside. There is a direct or routed path to the data center LAN, and a hole in the Firewall to reach the SSL1000. With this topology, the Data Center PCs can have Internet access.



Trust Only the Data Center Staff

Only the data center PCs have a direct path. Office PCs and remote users must use encryption. At the administrator's discretion, data center staff could have unencrypted access from their offices, but that access must be through the SSL1000. This topology allows no Internet access from the Data Center.



Trust No One

The only path to the mainframe is through the SSL1000.

Appendix A. SSL1000 Administrator's Worksheet

TCP/IP Network Parameters

LAN 1 IP Address	.	.	.	
LAN 1 Subnet Mask	.	.	.	
LAN 2 IP Address	.	.	.	
LAN 2 Subnet Mask	.	.	.	
Default Gateway IP Address	.	.	.	
DNS Server	.	.	.	

Static Routes

(IP networks not reachable via the Default Gateway)

Destination Network					Subnet Mask					Gateway IP Address			
.	.	.	.		.	.	.	.		.	.	.	
.	.	.	.		.	.	.	.		.	.	.	
.	.	.	.		.	.	.	.		.	.	.	
.	.	.	.		.	.	.	.		.	.	.	
.	.	.	.		.	.	.	.		.	.	.	

Firewall Considerations

Inbound TCP Ports

- ❑ HTTP (80) Used to download certificates and read help files
- ❑ HTTPS (443) Used for remote administration via secure web browser
- ❑ FTP (21) Used to download certificates
- ❑ Mappings Used for individual session connections - although port 23 is the Telnet standard, TCP ports above 1024 are recommended for this purpose.

_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

Outbound TCP Ports

- ❑ FTP (21) Used for software updates

Appendix B. Emulator Setup

IBM Personal Communications

To Add SSL Security to an Existing PCOMM Session

- Open the session. Under **Communication**, choose **Configure**.
  - Click on the **Link Parameters** button.
    - Change the **Host Name or IP Address** to the IP address or DNS name of the SSL1000.
    - If necessary, change the **Port Number** as specified in the SSL1000 Mapping for this session.
    - The **LU or Pool Name** remains the same. This is used after the end-to-end connection is made.
    - Click the checkbox labeled **Enable Security**.
  - Click **OK** to exit Link Parameters
- Click **OK** to save and exit Configuration

To Import the SSL1000 CA Certificate into PCOMM

You will have to import the **CA certificate** into the PCOMM Key Database if

- You use the default SSL1000 certificate as shipped (from the "Visara Certificate Authority")
- You imported a server certificate into the SSL1000 that is not from a "well known" Certificate Authority (see list below)

You will have to import the **Server certificate** into the PCOMM Key Database if

- You imported a Self-Signed server certificate into the SSL1000
- You imported a server certificate into the SSL1000 that is not from a "well known" Certificate Authority (see list below) and you do not have that CA Certificate available.

If you have replaced the factory default Server Certificate in the SSL1000 with one from one of the "well known" Certificate Authorities listed below, then you do not need to import the certificate. As shipped, PCOMM will trust any server certificate signed by one of the following CAs:

- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server CA
- VeriSign Class 1 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 3 Public Primary CA
- VeriSign Test CA Root Certificate

- VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
- VeriSign Class 2 CA Individual Subscriber-Persona Not Validated
- VeriSign Class 3 CA Individual Subscriber-Persona Not Validated

To manage certificates in PCOMM, use the **Certificate Management** application: *Start Menu >Programs>IBM Personal Communications>Utilities>**Certificate Management***

PCOMM uses a Key Database file that is password protected. The default password is ***pcomm*** and must be changed the first time you import a certificate.

- Under the **Key Database File** tab at the top, click **open**.

- Select the file **PcommClientKeyDb.kdb**. A password dialog box opens.
  - Enter the default password ***pcomm.***
  - If a confirm dialog tells you the password has expired, then click **Yes** and change it.
  - Enter a new password and confirm it.
  - Enter an expiration time (number of days)
- **Stash the password.** This is required for SSL to work without prompting you for the password every time you need to use the certificate. Check to "stash" the password for the key database in a password file *PcommClientKeyDb.sth* and click **OK** to finish with the password.

Once the password has been set and stashed, you can then use the **Certificate Wizard:** *Start Menu>Programs>IBM Personal Communications>Utilities>**Certificate Wizard*** which you may find easier to use.

Since these instructions deal with Certificate Management, we will continue there.

To import the CA certificate from the SSL1000, you must download it and save it on your local drive using your web browser. Your Certificate Administrator may have done this for you and stored it on a network drive. If so, you will receive the filename and location from him.

To download it yourself with your web browser, point it to the SSL1000 using either a DNS name or the IP address (eg http://SSL1000.MyCompany.Com, or http://204.48.51.51). You should see the Visara SSL1000 Main Menu web page. Click on the **Download SSL Certificate** button. You will see a text only page with a block of random characters that begins with —— BEGIN CERTIFICATE ——. In your browser, save this whole web page as a text file.

- Click **File.**
- Click **Save As.**
- You can leave the title *Visara SSL1000 Certificate Download* if you want, but change the ***Save As Type*** to ***Text File (.txt).***
- Save it to a directory you can easily remember and reach, such as the Desktop.

To import a certificate using the Certificate Management application

Use this to import either a CA certificate or a self-signed server certificate that has already been saved on a local drive. Your certificate administrator may have saved this on a network drive, and will give you the location and filename to use, or may have sent it to you in an email or on a floppy disk.

- Start the Certificate Management as described above and open the ***PcommClientKeyDB.kdb*** file (password required).
- Use the Drop-Down box just below *Key Database Content* (middle of the screen) to choose **Signer Certificates.**
- Click the **Add** button (on the right). You will see the **Add CAs Certificate from a File** dialog.
  - Make sure the **Data Type** is ***Base 64 Encoded ASCII.*** (That is what that block of random characters is.)
  - Change **Certificate File Name** from ****.arm*** to ****.txt*** and click **Browse**.
  - Find the directory where you saved the Download Certificate web page (eg the Desktop).
  - Find the file you saved (eg *Visara SSL1000 Certificate Download.txt)* click on it, and click **Open.**
- This will return you to the **Add CAs Certificate from a File** dialog. Click **OK**.

If the file is a valid certificate it will report the import was successful. You are now ready to run an SSL secured TN3270 session with PCOMM.

To import a certificate using the Certificate Wizard application

Use this to import either a CA certificate or a self-signed server certificate that has already been saved on a local drive. Your certificate administrator may have saved this on a network drive, and will give you the location and filename to use, or may have sent it to you in an email or on a floppy disk.

*Start Menu>Programs>IBM Personal Communications>Utilities>**Certificate Wizard***

- Choose **Import a Certificate**. Click **Next**.
- Choose **Import a Server or Certificate Authority (CA) Certificate**. Click **Next.**
- Enter the key database password that you set previously. (the default is ***pcomm***)
- Click **Browse.**
- Find the directory where you saved the Download Certificate web page (eg the Desktop).
- Find the file you saved (eg *Visara SSL1000 Certificate Download.txt),* click on it, and click **Open.**
- Enter a label for the certificate like "*SSL1000*" or "*Visara CA*", and click **Next**.

If the file is a valid certificate it will report the import was successful. You are now ready to run an SSL secured TN3270 session with PCOMM.

IBM WebSphere Host On-Demand

Using IBM Host On-Demand Certificate Wizard to import Visara's CA Certificate - Windows 2000

Importing your CA Certificate before defining clients will make for smoother connection process.

Open **Certificate Wizard** (Program\IBM Host On-Demand\Administration\Certificate Wizard).

- Welcome to the Host ON-Demand Certificate Wizard Dialog
  - Select **Import a certificate** radio button
- New Server Database or Client Database dialog
  - Enter password, or if no key database exists:
  - Enter your new password
  - Enter your new password again for confirmation
  - Click **Next** to create your key database. Defaults listed:
    Server (C:\hostondemand\bin\HODServerKeyDb.kdb)
    Client (C:\hostondemand\bin\HODSClientKeyDb.kdb)
- Import a Certificate dialog
  - Enter the path and file name of the certificate or Click BROWSE
  - If you click browse, choose file name (ex. A:\VisaraCaCert.pem)
  - Click **Next** to import. A backup of your certificate will be placed in **C:\hostondemand\sslbak**. Server certificate will be stored in your '**publish**' directory.
- Unable to Import the Certificate dialog
  - Choose **import the certificate as a Server or CA root certificate**.
  - Enter label for this certificate (ex. VisaraCaCert)
  - Click **Next** to continue.
- Import Certificate dialog
  - Successful complete. Click **Finish**.

Using IBM Host On-Demand Deployment Wizard to create a HTML-based configuration file

Open **Deployment Wizard** (Program\IBM Host OnDemand\Administration\Deployment Wizard)

- Welcome to IBM Host On-Demand Deployment Wizard
  - Select either to create a new HTML file or edit an existing HTML file. Create is the default. By default, HTML files are stored in Publish Directory **C:\hostondemand\HOD**
  - Click **Next** to continue
- Configuration Model
  - Select the configuration model that best fits your environment. A description of each model is displayed when you select that option. Here we have selected the HTML based model.
    - HTML-based model (default)

- Configuration server-based model
- Combined model

- Click **Next** to continue.

Notes:
- Use the Lock check box to prevent a user from changing session functions accessed from the session menu bar or tool bar that can be changed.
- The minimal requirements for a SSL client to connect are denoted with '**'.
- Client Message: Server "xxx.xxx.xxx.xxx:yyyy" presented a certificate that was not trusted. You need to import a certificate.

Host Sessions

- Host Session Buttons
  - **ADD**...Used to add a basic session of specified name to the list.
  - **PROPERTIES**…Use Properties to configure run-time options, such as window size, colors, etc.
  - **START**…Use Start to initiate a server connection using the selected (highlighted) session.
  - **COPY**...Use Copy to make a duplicate copy of the selected (highlighted) session.
  - **DELETE**...Use Delete to remove the selected (highlighted) session name from the list.
  - **DISABLE FUNCTIONS**…Use to disable functions you do not want to be available to end-users. This applies to all sessions defined in this HTML file.
  - **HELP**...Use Help to display a dialog that includes a description of parameters available via Host Session dialog.
- Host Type **
  - Select 3270 Display (default) from the drop-down list
- Session Name **
  - A user defined name to describe this HTML definition. 3270 Display is the default.
- Destination Address **
  - Specify target Server's IP address
  - Click **ADD** to add this definition to the list. Multiple definitions can be defined.
- Fine tuning session parameters: **Use your mouse to select (highlight) an entry in the list with the intent of making further parameter changes. Double click** Session Name **or click** Properties **to show detailed parameter settings.**
- Individual Session Buttons
  - **OK**...Use OK to return to Host Sessions dialog and retain changes.
  - **CANCEL**...Use Cancel to return to Host Sessions dialog without retaining changes.
  - **KEYBOARD**...Use Keyboard to remap keyboard.
  - **HELP**...Use Help to display a dialog that includes a description of parameters available via Session dialog.
- Select Connection Tab
  - **Session Name** ** (already filled in)
  - **Destination Address** ** (already filled in)
  - **Destination Port** ** (default = 23). Modify to match target server's port.
  - **Enable SLP** (default = NO)
  - **TN3270E** (default = YES)
  - **LU or Pool Name** (default = Blank). Modify to match server's requirements.
  - **Screen Size** (default = 24 x 80). Use drop-down list to select your specified screen size.
  - **Host Code-Page** (default = 037 United States)

- **Associated Printer Session** (default = None). Use drop-down list to select from predefined printer sessions.
- **Close printer with session** (default = grayed out)
- **File Transfer Type** (default = Host File Transfer)
  - Click **File Transfer Defaults** to show additional parameters associated with File Transfer Type.

- Select Advanced Tab
  - **Reset Insert Mode on Aid key** (default = NO)
  - **Enable Host Graphics** (default = NO)
  - **Character-Cell Size** (grayed out)
  - **Session ID** (default = Automatic). Use drop-down list to select a specific ID.
  - **Start Automatically** (default = NO)
  - **Start in Separate Window** (default = YES)
  - **Auto-Connect** (default = YES)
  - **Auto-Reconnect** (default = YES)
  - **Applet/Macro Options**
    - **Auto Start** (default = NONE). Use drop-down list to select a specific ID.
    - **Auto-Start Name** (default = grayed out). Used when Auto Start is set to either Applet or Macro.
  - **SLP Options** (default = grayed out). Options are enabled only when **Enable SLP = YES** under Connection Tab.
- Select Security Tab
  - **Enable Security SSL **** (default = NO). Enable this option by selecting YES radio button.
  - **Telnet-negotiation** (default = NO)
  - **Server Authentication SSL** (default = NO)
  - **Add MSIE browser's keyring** (default = NO). Enable this option by selecting YES radio button. This expands the scope of Host On-Demand to include your browser's certificates.
  - **If Server Request Client Certificates** (defaults)
    - Send a certificate (default = NO)
    - Other parameters are grayed out.
- Select Language Tab
  - Options are grayed out, most likely because the only language we have loaded is English, United States.
- Select Screen Tab
  - **Screen Customizer** (default = DISABLED). Use drop-down list to select ENABLE.
  - **Font Name** (default = IBM3270). Use drop-down list to select Monospaced.
  - **Font Style** (default = Plain). Use drop-down list to select either Italic or Bold.
  - **Cursor Style** (default = Underline). Use radio button to select BLOCK.
  - **Show Border** (default = YES). Use radio button to select NO.
  - **Light Pen Mode** (default = NO). Use radio button to select YES.
  - **Show OIA** (default = YES). Use radio button to select NO. OIA = Operator Information Area.
  - **Keypad** (default = NO). Use radio button to select YES.
  - **Toolbar** (default = YES). Use radio button to select NO.
  - **Toolbar Text** (default = NO). Use radio button to select YES.
  - **Status Bar** (default = YES). Use radio button to select NO.
  - **Micro Manager** (default = NO). Use radio button to select YES.
  - Click **OK** to return to Host Sessions dialog

When all Sessions have been defined, use **Next** to advance to Additional Options dialog.

- Additional Options dialog.
  - **Allow users to save selection changes** Use radio buttons to select Yes (default) or No.
  - **Cache Host On-Demand applets** Use radio buttons to select Yes (default) or No.
  - **Cache Options** buttons
  - **Advanced Options** button
  - **Preload Options** button
  - Click **Next** to advance to Page Title and Summary dialog
- Page Title and Summary dialog
  - **Enter user defined Page Title**. This entry represents the name of the HTML file as it appears in the title bar of the browser.
  - **Enter user defined File Name**. This entry specifies the name of the HTML file to create.
  - **Directory file shows when the created HTML file will be saved**. By default, the file is stored in the Host On-Demand Publish directory.
  - Summary box shows information regarding your selections.
  - When both page title and file name fields are entered, the **Create HTML** button is made available to save your information.
- Congratulation dialog
  - Shows information relating to success of creating the HTML file.
  - To create or edit another HTML file, click **Restart Wizard**…To close the Deployment Wizard, click **Close**.

Session Startup: One method would be to create a desktop shortcut to the session name assigned when defining Host Sessions.

Installing IBM WebSphere Host On-Demand v6.0 as a Resident Copy - Windows 98

If the installation dialog does not start automatically, RUN 'setupwin' from the CD. Click **Install** to start InstallShieldWizard. Once started, click **Next** to start the installation process.

- Software License Agreement
  - Click **Accept** to accept the terms and continue.
- Target Directory
  - Displays information about disk space, available and required.
  - Define destination folder. Default is **C:\hostondemand**.
  - Click **Next** to continue.
- Client Install Options
  - Select either Typical (default) or Custom by clicking the appropriate radio button.
  - Click **Next** to continue.
- Select Program Folder
  - Setup will add program icons to the specified Program Folder. Defaults to **IBM Host On-Demand**.
  - Click **Next** to continue.
- Installation Selections
  - A display of the installation options you have selected:

    Installation Type: **Client**
    Target Directory: **C:\hostondemand**
    Publish Directory: **C:\hostondemand\HOD**
    Folder: **Host On-Demand**
  - Click **Next** to continue with setup.

- InstallShield Wizard Complete
  - Click **Finish** to continue.
  - Close the dialog.

Using IBM Host On-Demand Certificate Management to add Visara's CA Certificate - Windows 98

Importing your CA Certificate before defining clients will make for smoother connection process.

Open **Certificate Management** (Program\IBM Host On-Demand\Administration\Certificate Management).

- IBM Key Management Dialog
  - Click **Key Database File\Open**
  - Change directory to **C:\hostondemand\lib**
  - Type or locate **CustomizedCAs.Class**. If the database does not exist, create a new one.
    - Click **Key Database File\New**
    - New dialog appears
    - Use drop-down list to select **Key database Type of SSLight Key database class**
    - File Name: **CustomizedCAs.class** (auto filled in)
    - Location: **C:\hostondemand\lib** (auto filled in)
    - Click **OK.**
  - Select **Signer Certificates** from drop-down list
  - Click **ADD**.
  - **Add CA's Certificate from File** dialog appears
    - Data Type must be BASE64 Encoded ASCII data
    - Enter Certificate File Name
    - Enter location (path name) of the certificate
    - Click **OK**
  - **Enter a Label** Dialog appears
    - Enter a label for the certificate (ex. VisaraCaCert)
    - Click **OK**
- Close IBM Key Management Dialog

Using IBM Host On-Demand to Setup/Start Sessions - Windows 98

Importing your CA Certificate before defining clients will make for smoother connection process.

Open **Host On Demand** (Program\IBM Host On-Demand\Host on Demand).

Note: You may see a Security Warning Dialog asking you to install Host On Demand. If so, check **Always trust contents from International Business Machines** and click **Yes**.

- Once the applet has started, you will see a browser page 'IBM WebSphere Host ON-Demand'
  - Click **Add Sessions** at bottom of page.

- Add Session dialog appears
  - Right click 3270 Display icon and select **Copy**
  - 3270 Display dialog appears
  - Configure as you would Windows 2000 client starting at Connection TAB
  - Click **OK** when complete

An icon with the session name you just created will show under the Configuration Session Window. Double click the icon to start the session.

Hummingbird V9.0 Host Explorer and Connectivity Secure Shell V9.0

Hummingbird **Host Explorer** does not include SSL with the initial installation. You must install the companion product **Connectivity Secure Shell**.

Hummingbird V9.0, Installing Connectivity Secure Shell

- RUN msetup from CD
  - Personal Installation
  - English
- Hummingbird Setup Wizard for Hummingbird Connectivity Secure Shell 9.0.0.0
  Click **Next**
- License Agreement
  - I accept ……
- Customer Information
  - Anyone (Win2k) User/Organization (Win98)
- Destination Folder
  (default = C:\Program Files\Hummingbird\Connectivity\9.00)
  - Typical
- Ready to install
  - Click **Install**
- Hummingbird Setup Wizard Completed
  - Click **Finish, Back, Exit**
- REBOOT PC

SSL Security Setup

- Open a session
  - Programs/Hummingbird Connectivity/V9.0/HostExplorer/3270
  - Click **Default 3270 CONNECT**
  - Cancel HostExplorer Window **CANCEL**
- Click Options / Edit Session Profile
- Expand Connection
  - TN3270
    - Click **Add New Host** Icon
    - Specify IP address of the SSL1000, not the destination TN3270 server.

  - Define TCP port according to the Mappings defined in the SSL1000.
- Advanced
  - Sys Req and Attention keys (used default values)
  - TN3270E support (E support is default value)
- NVT (used default values)
- Other (used default values)

- Expand Security
  - General
    - SSL/TLS
  - Kerberos (used default values)
  - SSL/TLS Options
    - Version 3
    - Negotiate via Telnet (used default value = not selected)
    - Close connection if negotiation fails (used default value = not selected)
  - User Authentication
    - User Certificate Mode
    - Select User Certificate
- Save Session Profile
- Connect Session to SSL 1000
  - File/Connect

Notes on a working Secured Connection/Non-Connection

- Secured Connection
  - See lock symbol on session status line
- Non-Secured Connection
  - If General/SSL/TLS is not selected, it appears that you have a connection (file/connect is grayed out) but there is no lock symbol.

SDI TN3270 Plus

Adding SSL Security to an existing Setup

Open a session: (Programs\TN3270Plus\TN3270Plus)

- Setup
  - Session Name does not need to change, but you could add words to indicate it is now using SSL.
  - **Host Name** will now be the SSL1000 IP address
  - **Telnet Port** will now have to agree with the SSL1000 Mapping (usually can stay the same if the port was 23 or above 1024…other ports below 1024 cannot be mapped in the SSL1000)
  - Click **Advance**
  - Security Tab
    - For security, choose SSLv3
    - Security Certificate
    - If 'Accept Any Invalid Certificate' is selected, SSL Server Certificate Details window will not be posted.

Index

T

U

V