Setting up and Using the IBM® Express Logon Feature

Contents

Part 1: Introduction to the Express Logon Feature

This paper describes the requirements, setup, configuration, and use of the IBM® Express Logon Feature. The Express Logon Feature is an IBM cross product solution that allows a user with a TN3270 client session and an X.509 certificate to log on to a SNA application residing on a host system without having to enter a user ID and password.

This new feature has several advantages:

1. It helps reduce the time administrators spend maintaining user IDs and passwords.
2. It helps reduce the number of user IDs and passwords that users have to remember.
3. It helps remove a potential security risk of users writing down user IDs and passwords, losing them, or sharing them with someone else.
4. It helps remove a potential security risk of users using trival or easily guessed passwords.

1.1 General Requirements:

The following IBM products currently support the Express Logon Feature:

- HOD V5.0
- TN3270 Servers (at least one of the following is required)
  - Communications Server for OS/2® 6.1
  - Communications Server for Windows NT® 6.1.1 PTF
  - Communications Server for AIX® 6.0.0.1 PTF
- OS/390® V2R10 with the following required components:
  - Communications Server for OS/390 V2R10 plus PTF PQ41276 - provides SNA and TCP/IP transport, and the Digital Certificate Access Server (DCAS) which supports the Express Logon Feature by interfacing to the TN3270 Servers and RACF®.
  - Security Server for OS/390 V2R10 (RACF) - provides general security services and services for digital certificates and passtickets
  - RACF APAR OW44393 is required when using one of the following:
    - TSO with Generic Resources and PTKTDATA Class profiles
    - Applications with shared user IDs that could access the application simultaneously. RACF requires the PTKTDATA profile to specify APPLDATA('NO REPLAY PROTECTION').

Note: Only IBM products were supported by the Express Logon Feature when this document was produced.

The following SNA applications have been tested successfully with the Express Logon Feature:

- TSO
- CICS®
- IMS®
- NetView®

Any application which uses RACF for logon validation is a candidate for using the Express Logon Feature.

In order for an application to be accessed using the Express Logon Feature, it must satisfy the following requirements:

- The target application must utilize RACF services for end user logon.
- One of the following configurations must be in place for the Express Logon feature environment:
  - The target application must reside on the same host as the DCAS and RACF Servers.
  - A shared RACF environment across multiple hosts must be in place for each host on which any target applications reside, as well as the host where the Digital Certificate Access Server (DCAS) is running.
  - A passticket data class profile (PTKTDATA) must be defined on each target RACF system (i.e. the host where DCAS is running, and any host where RACF and a target application is located). *This paper describes the instructions for setting up this method.*

Please Note: If the TN3270 Express Logon Feature is enabled, some TN3270 and TN3270E clients may fail to connect to any port, secure or non-secure, due to TN3270 negotiation errors. To correct this problem, please apply the latest maintenance to your clients as follows:

- Host On-Demand Version 4, CSD 4 or later, APAR IC27730
- Personal Communications (PCOMM) Version 5, APAR IC27654
- Personal Communications (PCOMM) Version 4.3, APAR IC27653
- Host Access Class Library, sna.ecl.data @ 6.0.0.1 or later, APAR IY12323 (this is an AIX client)

- Host On-Demand Entry, host_on_demand_entry.rte @ 4.0.0.1 or later, APAR IY12323 (this is an AIX client)

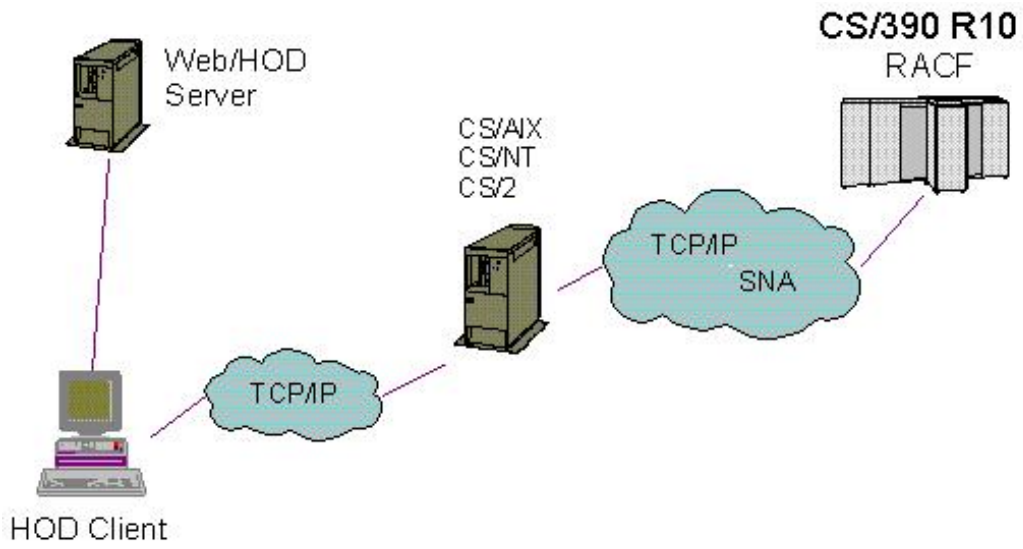
Return to Contents

1.2 Overview of Express Logon Feature

The Express Logon Feature design consists of the following components (refer to Figure 1):

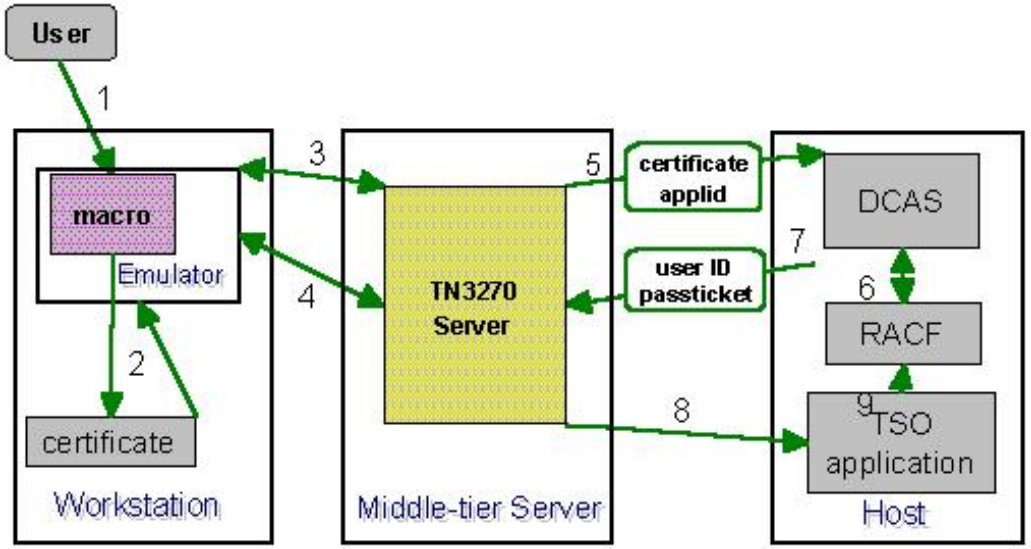
- A client workstation, running Host On-Demand, that supports Secure Sockets Layer (SSL) connections with client authentication and an X.509 certificate. The certificate must be associated with a valid user ID using RACF services in OS/390 V2R10.
- A TN3270 Server, which resides between the client and the host. This must be one of the supported TN3270 Servers mentioned in the General Requirements section.
- A Digital Certificate Access Server (DCAS) which is part of Communications Server for OS/390 V2R10 and resides on the host. DCAS uses RACF services to obtain a user ID. The host also provides RACF Secured Signon services, which DCAS uses to generate a passticket. A passticket is a RACF token similar to a password except that it is valid only for ten minutes.

Figure 1: Network Design



1.2.1 Express Logon Flow Description

Figure 2: Express Logon Feature flow



In the following example, the client wants to access a TSO session on the Host.

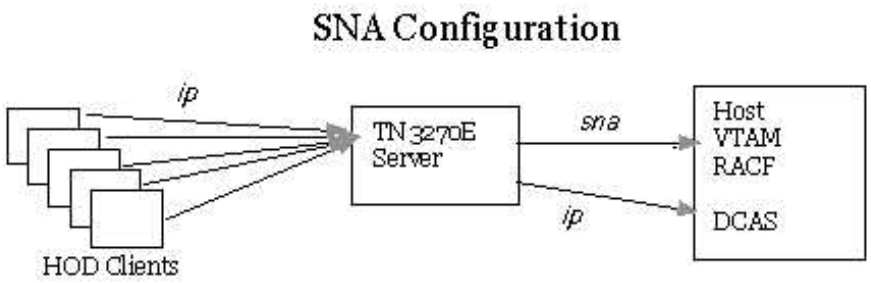
1. The user has a HOD icon which starts an emulator session configured to use SSL client authentication. The session has a macro associated with it.
2. The certificate file is unlocked with a password and then used in the SSL handshake.
3. During the SSL handshake, the client certificate is passed to the TN3270 Server and validated. During telnet function negotiation, the ELF capability is negotiated using RFC 1572.
4. The applid is sent from the client to the TN3270 server. The logon screens come down to the emulator as usual, but the macro plays and inserts placeholder strings in the user ID and password fields. The TN3270 Server intercepts the placeholder strings.
5. The TN3270 server sends the certificate and the target application ID to a program (DCAS) on the OS/390 host over a secure, trusted connection.
6. The DCAS Server makes SAF calls to convert the certificate to a user ID and passticket.
7. The DCAS Server sends the user ID and passticket back to the TN3270 Server.
8. The TN3270 Server inserts the user ID and passticket into the 3270 datastream at the macro-inserted placeholder locations and sends it to the application.
9. The application presents the user ID and passticket to RACF or other compatible host access control facility, which approves them and the logon completes as usual.

Return to Contents

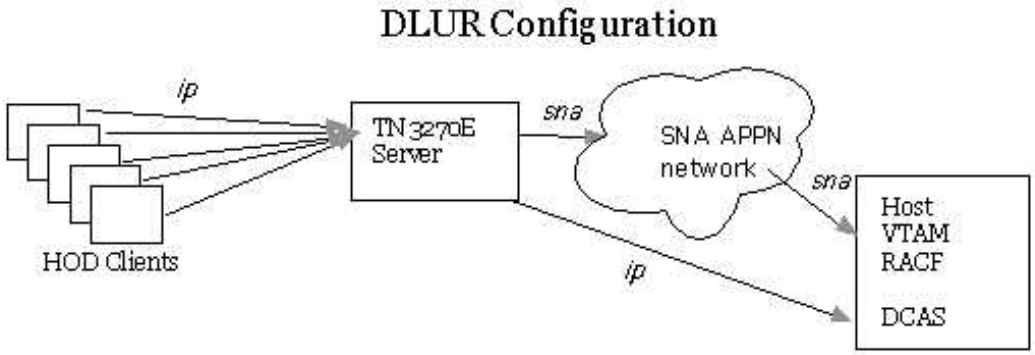
1.2.2 Sample Express Logon Feature Networks

This section contains examples of networks in which HOD clients use the Express Logon Feature to connect over a TN3270 Server to the Host.

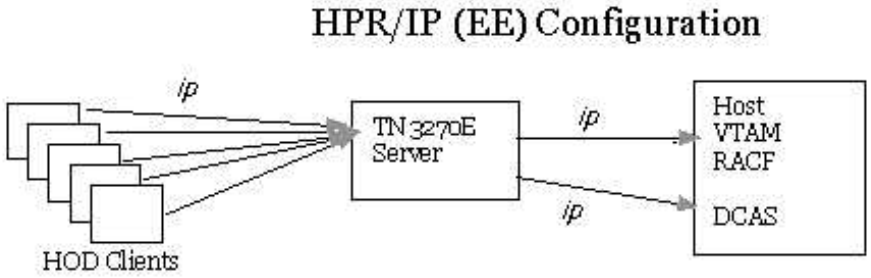
SNA Configuration



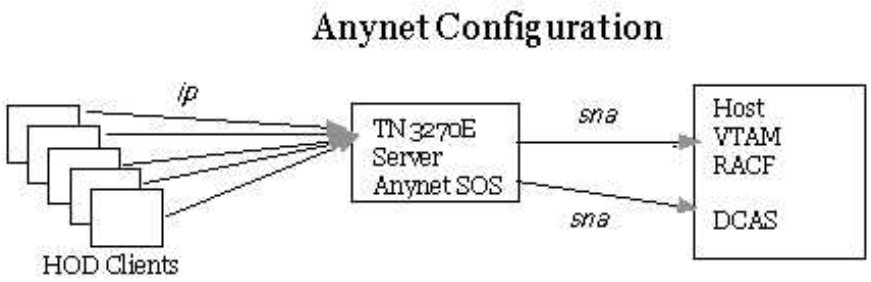
DLUR Configuration



HPR/IP (EE) Configuration



AnyNet Configuration



Return to Contents

1.3 Overview of Secure Sockets Layer-Based Security

Secure Sockets Layer (SSL) is required in the configuration of the Express Logon Feature on the HOD client, TN3270 server, and CS/390 server. This security uses SSL Version 3 to provide data encryption and authentication using signed certificates. The following types of certificates have been successfully tested for the Express Logon feature:

- IBM Trust Authority
- IBM Vault Registry
- Entrust
- Verisign
- Thawte
- Self-signed - can be generated by the user. Each Communications Server product contains a key management utility which can be used to generate self-signed certificates.

Understanding what SSL is and how it works will help the administrator in setting up the required environment for Express Logon Feature. Refer to *Planning for Secure Sockets Layer-Based Security* and *How SSL Security Works.*

Return to Contents

1.3.1 Planning for Secure Sockets Layer-Based Security

Secure Sockets Layer (SSL) provides data privacy and integrity as well as client and server authentication based upon public-key certificates. For each SSL connection, SSL uses a public/private key (PKI) mechanism for authenticating each side of the connection and for agreeing on encryption keys. These keys are generated and stored in: keyrings for DCAS on the host, key databases on the TN3270 Servers, and a key class on HOD clients.

X.509 certificates, containing public keys, are also required. The X.509 certificates can be created or requested and received.

For Express Logon Feature, SSL-based security will be used on connections between TN clients and the TN3270 Server, as well as between the TN3270 Server and the host. This security uses SSL Version 3 to provide data encryption and authentication using signed certificates.

For Express Logon Feature, a SSL client authentication port must be configured on the TN3270 Server to verify that the client is authorized to establish a secure connection to the server. This same port must be used by the HOD client when attempting to use Express Logon Feature to connect to an application on the host. In addition, the TN3270 Server can optionally request certificate revocation list (CRL) processing of client certificates. The TN3270 Server specifies the location of the LDAP server that maintains

the CRL to determine if the client certificate has been revoked.

Note: Support for CRL processing of client certificates requires the use of the IBM Vault Registry product, which publishes Certificate Revocation Lists to an LDAP server.

Return to Contents

1.3.2 How SSL Security Works

Secure Sockets Layer (SSL) is an industry standard protocol that uses symmetric-key and public-key cryptographic technology. Symmetric-key cryptography uses the same key to encrypt and decrypt messages. Public-key cryptography uses a pair of keys, a public key and a private key. Each server's public key is published, and the private key is kept secret. To send an encrypted message to the server, the client encrypts the message using the server's public key. When the server receives the message, it decrypts the message using its private key.

SSL provides three basic security services:

1. Message privacy
   - Message privacy is achieved through a combination of public-key and symmetric-key encryption. All traffic between an SSL client and an SSL server is encrypted using a key and an encryption algorithm negotiated during session setup.
2. Message integrity
   - The message integrity service ensures that SSL session traffic does not change in route to its final destination. SSL uses a combination of public/private keys and hash functions to ensure message integrity.
3. Authentication
   - Authentication is the process whereby the client and the server convince each other of their identities. The client and server identities are encoded in public-key certificates. A public-key certificate contains the following components:
     - Subject's distinguished name
     - Issuer's distinguished name
     - Subject's public key
     - Issuer's signature
     - Validity period
     - Serial number

Return to Contents

1.3.3 Deciding What Type of Certificates to Use

There are three types of certificates available for use when setting up SSL for Express Logon Feature. One type of certificate, self-signed, can be generated by the user. The other two types of certificates, Well-Known and Unknown, require the user to request a certificate from a certificate provider. The type of environment the user will be implementing will dictate the type of certificate the user should use. The following is a brief description of each type of certificate that will aid the user in deciding what type of certificate is best for them.

Self-Signed Certificates

Receipt of a certificate from a well-known trusted Certificate Authority can take up to three weeks. Until you receive the public server certificate(s), you can create a self-signed certificate by using the IBM Key Management database to enable SSL sessions between clients and the server.

Certificates from a Well-Known Trusted Certificate Authority (CA)

A certificate issued by a well-known Certificate Authority (CA) is termed 'well-known' because many of the most widely used signer (CA root) certificates generated by trusted certificate authority providers are already stored in the IBM Key Management database, and marked as trusted certificates. Using well-known certificates requires the user to contact a well-known CA provider (e.g., Verisign or Thawte) and apply for the additional certificate(s) the user needs. Certificates from a well-known CA are adequate for a production environment.

Certificates from an Unknown Certificate Authority (CA)

A certificate issued by an unknown Certificate Authority (CA) is termed 'unknown' if the user has decided to purchase certificates from a CA whose signer (CA root) certificate is not already present in the IBM Key Management database, or does not want to depend on an outside vendor to provide certificates. The user can purchase software such as IBM Vault Registry to generate certificates for their secure environment. Certificates generated from an unknown CA or generated by IBM Vault Registry software are adequate for a production environment.

Return to Contents

1.3.4 Client Authentication

The Express Logon Feature requires client authentication to be configured for the HOD client and the TN3270 Server. Client authentication allows the TN3270 Server to verify that the HOD client is authorized to establish a secure connection to the server and allows the HOD client to verify that the TN3270 Server's identity is valid. Client authentication requires the following;

1. a key pair, to allow data encryption and decryption to be carried out
2. a certificate on the TN3270 server for authentication
3. a certificate on the HOD client for authentication

The key pair and the certificates are stored in a key database file on the TN3270 Server and the HOD client and comprise a single record in the database. Setting up certificates for use with the Express Logon Feature is described in Part 3: Setting up Required Certificates for Express Logon Feature.

Return to Contents

1.4 Checklist of Activities Required to Set up and Use Express Logon Feature

The following checklist will be helpful to the administrator's effort in setting up the required environment to use the Express Logon Feature.

Table 1. Express Logon Feature Task Checklist

Task	Target Machine	Links to task instructions
Ensure prereqs are satisfied including necessary APARs / PTFs	Clients, TN3270 servers, Hosts	General Requirements

Determine the type of Certificates that will be used		Deciding What Type of Certificates to Use
Configure VTAM®, RACF®, and the DCAS (Digital Certificate Access Server)	OS/390 V2R10 Host system	Configuring VTAM®, RACF®, and the DCAS
Configure the TN3270 server	CS/2	Configuring ELF Support on Communications Server for OS/2® (CS/2)
	CS/AIX	Configuring ELF Support on Communications Server for AIX® (CS/AIX)
	CS/NT	Configuring ELF Support on Communications Server for Windows NT® and Windows 2000 (CS/NT)
Configure the HOD Client	HOD workstation	Defining the HOD TN3270 Session Properties
Set up Required Certificates	HOD, TN3270 servers, and DCAS	Setting up Required Certificates for Express Logon Feature
Test the client authentication session	HOD workstation	Establishing the Initial 3270 SSL Connection
Record and playback HOD macros	HOD workstation	Recording the ELF Logon Macro ---------- Playing Back the ELF Logon Macro
Distribute HOD macros to clients	HOD workstation	Exporting HOD ELF Sessions and HOD Macros ---------- Importing HOD ELF Sessions and HOD Macros ---------- Establishing a 3270 SSL Connection for Another User

Return to Contents

Part 2: Configuring the Express Logon Feature (ELF)

Part 2 contains instructions for configuring the products necessary to use the Express Logon Feature.

Return to Contents

2.1 Configuring VTAM®, RACF®, and the Digital Certificate Access Server (DCAS)

The Digital Certificate Access Server (DCAS) is a TCP/IP server that runs on OS/390 V2R10. The TN3270 servers connect to DCAS using Secure Socket Layer V3 (SSL). The purpose of DCAS is to receive an applid and a digital certificate from a TN3270 server, then ask RACF to return a valid user ID that has been associated with the certificate and to generate a passticket for the input user ID and application ID (APPLID).

This section describes the configuration needed for VTAM, DCAS, and RACF for the Express Logon feature.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.1 Initial Setup

DCAS (which is a TCP/IP server running on OS/390 V2R10) must run from a user ID defined with a UID=0 and from an APF authorized library. The shipped executable resides in /usr/lpp/tcpip/sbin with the setuid bit on. The DCAS uses the OS/390 SSL product, shipped with the OS/390 base element. The SSL library hlq.SGSKLOAD must be in the run-time STEPLIB. The default port used by the DCAS is port 8990. If you want to ensure that no other application uses the same port, use the following statement in the TCPIP profile dataset:

```
PORT
    8990 TCP DCAS
```

If you choose to run the DCAS from the OS/390 UNIX shell, use the following statement:

```
PORT
    8990 TCP OMVS
```

It is recommended that you use port access controls. For details on access controls, refer to the description of port access controls in the *OS/390 IBM Communications Server: IP Migration.*

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.2 VTAM Requirements

On the host you need to have both an IP connection and an SNA link between the TN3270 Server and the host. These connections may be over separate physical transports or they may be combined using a common protocol, as described in section 1.2.2 Sample Express Logon Feature Networks. This document presumes that the host administrator is already familiar with how to set up the connections.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.3 Configuring RACF Services for the DCAS

This section describes how to configure RACF services for the DCAS including sample commands. These commands are in EZARACF in the SEZAINST dataset. For information on RACF commands, refer to *OS/390 SecureWay® Security Server RACF Security Administrator's Guide* and *OS/390 SecureWay® Security Server RACF Command Language Reference.*

In the following example RACF commands, ***italicized items*** should be replaced with values appropriate for your environment.

Defining a User ID as Superuser to OMVS Services:
The DCAS server runs as a system daemon and must be started under a controlled user ID that has superuser authority (i.e., not an end-user or system programmer's user ID). To define the user ID to use OMVS services, use the following command:

ADDUSER *dcasid* DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))

Providing a User ID with Access to MVS.SERVMGR.DCAS:
Starting the DCAS from an MVS procedure requires that the user ID from which it is started have access to the MVS.SERVMGR.DCAS resource in the OPERCMDS class. To provide this access, use the following commands:

RDEFINE OPERCMDS (MVS.SERVMGR.DCAS) UACC(NONE)
PERMIT MVS.SERVMGR.DCAS CLASS(OPERCMDS) ACCESS(CONTROL) ID(*dcasid*)

Providing a RACF Definition for MVS Start-up:
If DCAS is started as an MVS procedure, the following RACF definition is needed:

RDEFINE STARTED DCAS.* STDATA(USER(*dcasid*))
SETR RACLIST(STARTED) REFRESH

At a minimum, you must register all workstation client certificates with RACF. This associates the certificates, which are passed by the TN3270 server to the DCAS, with the IDs of users attempting to log on. To associate certificates with user IDs, use the RACDCERT command. You must also create a RACF PTKTDATA profile for each application ID the end user is attempting to access. The PTKTDATA profile allows the DCAS to obtain a passticket for the application and user ID and to pass it back to the TN3270 server. For HOD V5, the application ID part of the profile name must be the same as that configured in the HOD V5 Express Logon Application ID pop-up window. In most cases, the application name with which the user logs on will match the application ID portion of the RACF PTKTDATA class profile. However, for TSO and some other applications, the names and IDs may not match:

- If VTAM generic resources are used for TSO, define the application name portion on the RACF profile using the TCASGNAME defined in the TSOKEYxx, SYS1.PARMLIB member.
- If VTAM generic resources are not used, define the application name on the RACF profile as TSO<SMF_system ID>. The SMF system ID is defined in the SMFPRMxx member of SYS1.PARMLIB and is specified by the SID keyword.

For applications that allow shared user IDs (can request access to the application simultaneously), you must specify the APPLDATA('NO REPLAY PROTECTION') option

on the RDEFINE command in the PTKTDATA profile. This bypasses the default RACF protection against replay of passtickets.

If CLIENTAUTH LOCAL2 is coded in the DCAS configuration file, at a minimum, you must use RACF to associate the TN3270 server certificate with a valid user ID. You can do this using the RACDCERT ADD command. The user ID could be the one associated with the DCAS itself or it could be any valid user ID. If you want additional checking, you must activate the SERVAUTH class and define an EZA.DCAS.cvtsysname profile with the user ID associated with the TN3270 server certificate to access the profile.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.4 DCAS and System SSL

This section gives an overview of using System SSL with the DCAS.

The DCAS and the TN3270 server use SSL to communicate. The SSL protocol begins with a handshake. Then, the TN3270 server authenticates the DCAS and vice versa. At this time, the DCAS and the TN3270 server also agree on how to encrypt and decrypt the data.

You can specify the cipher level used for encryption and decryption for each connection at the time DCAS is configured, using the V3CIPHER configuration keyword. Alternatively, you can set the cipher level dynamically when DCAS starts, based on the level of cipher installed on the system. To set the cipher level dynamically, do not specify the V3CIPHER keyword.

SSL provides data privacy and integrity as well as client and server authentication based upon public-key certificates. For each SSL connection, SSL uses a public/private key (PKI) mechanism for authenticating each side of the connection and for agreeing on encryption keys. These keys are generated and stored in key databases, known as *keyrings*.

X.509 certificates, containing public keys, are also required. The X.509 certificates can be created or requested and received. In either case, a certificate is then associated with and becomes part of a keyring. You have access to several services for creating and managing keyrings and certificates:

- The gskkyman tool
  This tool is shipped with System SSL and runs out of the OS/390 UNIX shell. You can use it to create keyrings and certificates that are stored in HFS. Specify keyrings created with gskkyman in the DCAS configuration file using the KEYRING keyword.

  If you use gskkyman, you must also create a password stash file. The password stash file protects the keyring file because it contains private keys associated with the certificates contained in the keyring. Specify the password stash file in the DCAS configuration file using the STASHFILE keyword. For details on using the gskkyman tool, refer to the *OS/390 System Secure Sockets Layer Programming Guide and Reference*.
- The RACDCERT command
  You can also use the RACDCERT command in RACF to create, register, store, and administer keys and certificates. If you use RACDCERT, specify the keyring to the DCAS server in the configuration file using the SAFKEYRING keyword. A keyring created this way does not have a password file associated with it. For details on digital certificates, refer to the *OS/390 SecureWay Security Server RACF Security Administrator's Guide* and *OS/390 SecureWay Security Server RACF Command Language Reference*.

Authenticating the DCAS and the TN3270 Server

The type of security and authentication required will determine the way certificates are created and managed. The DCAS, in conjunction with SSL and RACF, supports several levels of authentication.

Authenticating the DCAS: DCAS authentication is always performed by the TN3270 server. Authentication requires that the DCAS has a private key and an associated X.509 digital certificate defined in a keyring. To conduct commercial business on the Internet, you can use a Certificate Authority (CA), such as VeriSign, to obtain a high-assurance certificate. For small, private environments, you can create a self-signed DCAS certificate. If you use self-signed certificates, all TN3270 servers connecting to the DCAS must be able to treat the certificate as a CA certificate. This requires that the self-signed certificate be transmitted to any SSL clients.

Authenticating the TN3270 server: The TN3270 server is the client that interacts with the DCAS. Authenticating the TN3270 server involves additional levels of control in which the client must have a key database with a certificate. Depending on the control level, the certificate is authenticated by SSL and the DCAS using RACF services.

There are three levels of client authentication from which to choose:

- Level 1
  With Level 1 authentication, the DCAS uses the client authentication provided by SSL at the time of the SSL handshake. The keyring used by the DCAS must contain the following certificates:
  – The DCAS certificate
  – The TN3270 server certificate
  To configure DCAS for this level of authentication, specify the CLIENTAUTH LOCAL1 keyword and value in the DCAS configuration file. Use the KEYRING or the SAFKEYRING keywords in the DCAS configuration file to specify the keyring used by the DCAS.

- Level 2
  Level 2 includes Level 1 authentication plus additional verification that the TN3270 server certificate has been associated in RACF with a valid user ID. (This user ID must be the user ID that DCAS is running under.) To configure DCAS for this level of authentication, specify the CLIENTAUTH LOCAL2 keyword and value in the DCAS configuration file. Use FTP (with the BINARY send option) to send the TN3270 Server DER certificate to an MVS dataset. Use the RACDCERT ADD command to add the certificate to RACF and associate it with a user ID, as shown in the following example:
  RACDCERT ID(*dcasid*) ADD('DCAS.TN3270.CERT') TRUST

- Level 3
  Level 3 includes level 2 authentication plus it verifies that the TN3270 server has access to the DCAS. The user ID derived from the certificate using the RACF checks from Level 2 is defined as having access to the SERVAUTH RACF class and the EZA.DCAS.cvtsysname resource in the SERVAUTH class. The following conditions apply:
  - If the SERVAUTH class is not active or the EZA.DCAS.cvtsysname profile is not defined, or both, it is assumed this enhanced level is not requested.
  - If the SERVAUTH class is active and the EZA.DCAS.cvtsysname profile is defined (but not for the user associated with the certificate) the requestor's connection is terminated:

  RDEFINE SERVAUTH EZA.DCAS.cvtsysname UACC(NONE)
  PERMIT EZA.DCAS.cvtsysname CLASS(SERVAUTH) ACCESS(CONTROL) ID(*dcasid*)

  To configure DCAS for Level 3 authentication, follow these steps:
  1. Specify the CLIENTAUTH LOCAL2 keyword and value in the DCAS configuration file.
  2. Activate the SERVAUTH RACF class.
  3. Define a profile for the EZA.DCAS.cvtsysname resource and associate the profile with the user ID associated with the certificate.
     Note: The ID associated with the certificate and the EZA.DCAS.cvtsysname can be any valid user ID.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.5 Using RACF's Common Key Ring Support to Manage Keys and Certificates

For information on RACF commands, refer to *OS/390 SecureWay Security Server RACF Security Administrator's Guide* and *OS/390 SecureWay Security Server RACF Command Language Reference*.

Initial Setup

1. Before using RACF to store your key database information, ensure that the digital certificate and digital keyring (DIGTCERT and DIGTRING) classes are active before defining certificates or keyrings to RACF:
   SETROPTS CLASSACT(DIGTCERT DIGTRING)
2. Be sure to perform a refresh after each update or change:
   SETROPTS RACLIST (DIGTRING DIGTCERT) REFRESH
3. Also, ensure that the RACDCERT command is defined as an authorized TSO command in the IKJTSOxx member.
4. In order to issue the RACDCERT command, you must have access to the FACILITY class IRR.DIGTCERT.function with UPDATE or CONTROL access. If the DCAS is started as an MVS started procedure, you must permit the RACF user ID to IRR.DIGTCERT.LIST. If the DCAS is started from a TSO user ID under the OS/390 UNIX shell, you must also permit that ID, as shown in the following example:

   RDEFINE FACILITY (IRR.DIGTCERT.function)
   UACC(NONE)
   PERMIT IRR.DIGTCERT.LIST
   CLASS(FACILITY) ID(*dcasid*)
   ACCESS(control)

Create a Keyring:

You will need to create a keyring for your DCAS server. For example:

RACDCERT ID(*dcasid*) ADDRING(*SERVERKeyring*)

Create and Connect a Certificate:

You can use RACF to create self-signed certificates. Refer to section Creating Self-Signed Certificates on the Host for details.

Request and Connect a Well-Known Certificate:

You can alternately request a well-known certificate from a Certificate Authority, such as Verisign, and add it to RACF. Refer to section 2.1.5.2 Creating Well-Known Certificates on the Host for details.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.5.1 Creating and Connecting Self-Signed Certificates on the Host

Because the clients will not know about the issuer of the self-signed certificate, in most cases it is necessary to add the server's self-signed certificate to the client's signer certificates. This process requires the following high-level steps:

1. Generate the DCAS server self-signed certificate on the host.
2. Transfer the DCAS server's certificate to the TN3270 server machine.

Following are detailed steps describing the process. DCAS server self-signed certificates can be created using RACF or GSKKYMAN.

If using RACF

1. Generate the DCAS server self-signed certificate on the host and transfer to the TN3270 server.

(a.) Create a self-signed server certificate using RACDCERT gencert:

RACDCERT ID(*dcasid*)

```
SUBJECTSDN(CN('DCASCERT')
 OU('TEST')
 C('US'))
 TRUST
 SIZE(512)
 WITHLABEL('DCASCERT')
```

(b.) Use RACDCERT Connect to connect the certificate to a keyring and make it default. This example assumes a keyring called SERVERKeyring already has been created.

```
RACDCERT ID(dcasid)
     CONNECT(ID(dcasid)
      LABEL('DCASCERT')
      RING(SERVERKeyring)
      USAGE(PERSONAL) DEFAULT)
```

(c.) Use RACDCERT EXPORT to export the DCAS server self-signed certificate in ".DER" format to an MVS file.

```
RACDCERT ID(dcasid) EXPORT(LABEL('DCASCERT'))
     DSN('dcasid.SAFCERT.DER')
     FORMAT(CERTDER)
```

2. FTP the exported DCAS server certificate to the TN3270 server using the FTP binary option.

If using a GSKKYMAN keyring

1. Generate the DCAS server self-signed certificate on the host.
(a). Open your keyring file and select 'Create a self-signed certificate.'
(b). Specify Version 3, label, key size, and certificate information when requested.
(c). Set the key as the default in your key database.
(d). Save the certificate to a file, select binary format (the certificate will be saved in binary ".DER" format).

The following is a sample of GSKKYMAN output for creating a self-signed certificate. GSKKYMAN's default action appears in the brackets.

(a). Enter version number of the certificate to be created (1,2, or 3) [3]: 3
(b). Enter a label for this key.....> selfsignedcert
(c). Select desired key size from the following options (512): 1: 512 2: 1024
(d). Enter the number corresponding to the key size you want: 1
(e). Enter certificate subject name fields in the folowing.

```
Common name (required).....>test server certificate
Organization (required).....>dev
Organization Unit (optional).....>
City/Locality (optional).....>
State/Province (optional).....>
Country Name (required 2 characters).....>US
```

(f). Enter number of valid days for the certificate[356]:
(g). Do you want to set the key as the default in your key database? (1=yes, 0=no) [1]: 1
(h). Do you want to save the certificate to a file? (1=yes, 0=no) [1]:
(i). Should the certificate binary data or Base64 encoded ASCII data be saved? (1=ASCII, 2=binary) [1]: 2

(j). Enter certificate file name or press ENTER for "cert.crt": ss-servercert.crt

The following message is displayed: Please wait while the self-signed certificate is created....

To pick up the new default server certificates, restart TCP/IP or stop all secure ports and issue a VARY OBEY command to bring the secure ports back online.

(2). Transfer the host's certificate to the TN3270 server machine. If using FTP, transfer with the binary ftp option.

Return to Part 2. Configuring Express Logon Feature
Return to 3.2 Using Self-Signed Certificates
Return to Contents

2.1.5.2 Creating and Connecting Well-Known Certificates on the Host

Following are the steps for adding a Certificate Authority Root and Personal Certificates to the Host.

1. Create a self-signed certificate and key pair for the DCAS server:

   RACDCERT ID(*dcasid*)
   GENCERT SUBJECTSDN(CN('*labelname*') C('us'))
   WITHLABEL('*labelname*')

2. Create a certificate request for a Certificate Authority (CA) by issuing RACDCERT GENREQ against the self-signed certificate:

   RACDCERT ID(*dcasid*)
   GENREQ(LABEL('*labelname*'))
   DSN(*labelname.certreqname*)

3. Send the certificate request to a Certificate Authority. (For example, IBM Trust Authority, Entrust, Verisign.)

4. When you receive the DCAS server certificate from the Certificate Authority, transfer the file to the DCAS host.

5. If RACF doesn't already have the root certificate for the Certificate Authority, then you need to get it in .DER format, and add it to RACF using this command:

   RACDCERT CERTAUTH ADD(*caroot.der*)
   TRUST WITHLABEL('*caroot*')

6. Add the DCAS server certificate from the Certificate Authority back into RACF:

   RACDCERT ID(*dcasid*) ADD(*certname*) WITHLABEL('*certname*')

7. Connect the CA root certificate to the keyring with usage CERTAUTH:

   RACDCERT ID(*dcasid*)
   CONNECT(CERTAUTH LABEL('*caroot*')
   RING(*SERVERKeyring*)
   USAGE(CERTAUTH) DEFAULT)

8. Connect the DCAS server certificate to the keyring with usage PERSONAL:

   RACDCERT ID(*dcasid*)
   CONNECT(ID(*dcasid*) LABEL('*certname*')

RING(*SERVERKeyring*)
USAGE(PERSONAL) DEFAULT)

Return to Part 2. Configuring Express Logon Feature
Return to 3.3 Using Well-Known Certificates
Return to Contents

2.1.6 Defining A Passticket Profile For Each Application

A Passticket profile must be created for each application that users will log on to using the Express Logon Feature. This profile must be created on each separate RACF system (the system where the users will be logging on to) that contains target applications for Express Logon Feature.

The RACF PTKTDATA (passticket data) profile allows the DCAS to obtain a passticket for the application and user ID and to pass it back to the TN3270 server. Note that the application ID portion of the profile must match that which was configured on the HOD V5 Workstation Application ID panel (see section 4.2 Recording the ELF Logon Macro.)

The PTKTDATA class profile defined in the 'target' RACF system must match the PTKTDATA class profile in the system where the passticket is created, which in the case of Express Logon Feature, is the system where the DCAS server executes. These PTKTDATA class profiles need to have corresponding profile names and identical secret keys (defined using the KEYMASKED parameter).

Example of a passticket data class profile for the application TSORUS (the KEYMASKED value is a hex string of your choice):

RDEFINE PTKTDATA *TSORUS*
SSIGNON(KEYMASKED(*E1E2E3E4E5E6E7E8*)
UACCESS(NONE))
SETR RACLIST(PTKTDATA) REFRESH

Take special care in what is used for APPLID name. For example, for TSO the profile is TSO+SID. The SID is the SMF system id that is defined in the SMFPRMxx member in SYS1.PARMLIB. For more information on defining Passticket profiles, refer to the *OS/390 SecureWay Security Server RACF Security Administrator's Guide.*

If VTAM generic resources are used for TSO, define the application name portion on the RACF profile using the TCASGNAM defined in the TSOKEYxx, SYS1.PARMLIB member. RACF APAR OW44393 is required if using VTAM generic resources with Express Logon Feature.

For applications that allow shared user IDs (multiple users request access to the application simultaneously), you must specify the APPLDATA('NO REPLAY PROTECTION') option on the RDEFINE command in the PTKTDATA profile. RACF APAR OW44393 is required for this as well.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.7 Configuring the DCAS

Make sure the DCAS configuration file and the DCAS start procedure are updated as appropriate to your installation.

The DCAS configuration file (/etc/dcas.conf) contains the following keywords:

```
TCPIP tcpstackname          ; Server will have affinity to tcpip stackname
IPADDR xx.xx.xx.xx          ; IP address used to bind to for SSL connection
                            ;    (defaults to inaddr_any)
```

```
PORT xxxx                  ; DCAS listens on this port number (default is 8990)
KEYRING  /etc/ssl/xxx.kdb  ; HFS file name of Keyring for SSL negotiation
STASHFILE  /etc/ssl/xx.sth ; Stash file containing the Password of Keyring file
SAFKEYRING SERVERKeyring   ; Keyring via RACF
CLIENTAUTH xxxxxx          ; Client Authentication level
                           : LOCAL1 (SSL does authentication)
                           ; LOCAL2 (default - use RACF to validate the
                           ;    client's certificate)
LDAPSERVER xx.xx.xx.xx     ; Fully qualified name or IP address of LDAP Sever
LDAPPORT xxxx              ; Port# that LDAP Server is listening on
V3CIPHER cipherspec        ; Specify a subset of the supported SSL V3 cipher
                           ;    algorithms
                           ; The following cipher levels are valid:
                           ; 01=NULL MD5  02= NULL SHA  03=RC4 MD5 Export
                           ; 04=RC4 MD5 US  05=RC4 SHA US   06=RC2 MD5 Export
                           ; 09=DES SHA  0A=Triple DES SHA US
```

Refer to the *OS/390 IBM Communications Server Express Logon User's Guide* for details on the configuration file keywords and parameters.

Following is a sample procedure used to start DCAS: (you will also find a sample in EZADCASP in the SEZAINST dataset)

```
//DCAS   PROC
//* DEBUGGING AND LOGGING MAY BE REQUIRED TO HELP DETERMINE A PROBLEM
//* THE DCAS.
//*
//* -D OR -D - INDICATES DEBUGGING LEVEL REQUESTED.
//*         FORMAT:    -D LEVEL
//*         LEVEL IS:     1=LOG ERROR AND WARNING MESSAGES
//*                   2=LOG ERROR, WARNING, AND INFO
//*                   3=LOG ERROR,WARNING, INFORMATI
//*
//*
//DCAS   EXEC PGM=EZADCDMN,REGION=4096K,TIME=NOLIMIT,
//      PARM='POSIX(ON) ALL31(ON) / -d 3 -l SYSLOGD'
//*
//SYDENV   DD DUMMY
//SYSPRINT DD SYSOUT=*
//SYSIN    DD DUMMY
//SYSERR   DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//CEEDUMP  DD SYSOUT=*
//*
```

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.1.8 Starting and Stopping DCAS

DCAS can be started as either a generic server without stack affinity or as a server with affinity to a specific TCP/IP stack. You can start the DCAS automatically when the TCP/IP address space is started or from the OS/390 UNIX shell:

- To start the DCAS automatically when the TCP/IP address space is started, specify DCAS on the AUTOLOG statement in the TCPIP profile dataset as shown in the following example:
  AUTOLOG
  DCAS
  ENDAUTOLOG

  A sample start procedure for the DCAS is provided in EZADCASP in the SEZAINST dataset. If using the sample procedure in section 2.1.7 Configuring the DCAS, you would start DCAS by entering the following command from the MVS console: **S DCAS**
  To pass optional parameters to DCAS, specify them after the final slash (/) on the PARM statement.

  For example:
  // PARM=('POSIX(ON) ALL31(ON)'
  // 'ENVAR("LIBPATH=/usr/lib")/-d 3 -l SYSLOGD')

- To start the DCAS from the UNIX shell, use the **dcas** command with optional parameters for debugging, logging, and specifying the configuration file. Note that the DCAS must run as a background job. The format of the dcas command is
  dcas <parameter_1> <parameter_2> <parameter_3> &

  For example:
  dcas -D 1 -L SYSLOGD -C /etc/dcas.conf &

The following are optional parameters that can be used with both the DCAS UNIX command and the MVS started procedure:

- -d or -D
  Indicates debugging level
  1 - Specifies log error and warning messages
  2 - Specifies log error, warning, and informational messages
  3 - Specifies log error, warning, informational, and debug messages (this is the default)
- -l or -L
  Indicates logging to SYSLOGD or to a designated log file. If you do not specify this parameter, logging defaults to /tmp/dcas.log.
  If you specify a debug level, but not logging, then the DCAS attempts to open the default log file /tmp/dcas.log. If this fails, debugging is turned off.
  For SYSLOGD, the DCAS uses the log facility local0.
- -c or -C
  Indicates the requested configuration file (for example, /u/userx/passtick.conf). If you do not specify this parameter, the DCAS looks for the configuration file using the following search order:
  - DCAS_CONFIG_FILE environment variable
  - /etc/dcas.conf
  - tsouserid.DCAS.CONF
  - TCPIP.DCAS.CONF

  If the DCAS does not find a valid configuration file, it will not start.

When DCAS is started, it stores its process ID (pid) in a Hierarchical File System (HFS) file. The file name under which it is stored depends upon how you configure DCAS:

- If you configure the DCAS with TCP/IP stack affinity, the pid file is named /tmp/dcas.tcpipname.pid where tcpipname is the name of the TCP/IP stack for which DCAS has affinity.
- If you configure the DCAS without stack affinity, the process ID file is named /tmp/dcas.INET.pid.

You can stop the DCAS from the UNIX shell or from MVS:

- To stop the DCAS from the UNIX shell, use the following command:
  kill -s SIGTERM pid
- To stop the DCAS from MVS, use the following command:
  P DCAS

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2 Configuring the TN3270 Servers for ELF

This section of the document describes the steps needed to configure the TN3270 server. Please refer to the section that describes the Communications Server (CS/2, CS/AIX, or CS/NT) in your environment.

2.2.1 Configuring ELF Support on Communications Server for OS/2® (CS/2)

Your Express Logon Feature system is made up of HOD clients, a TN3270 server, and a host system. This section of the white paper is dedicated to the setup and operation of the OS/2 TN3270E server using the Express Logon Feature. Subsections contain information about:

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.1.1 TN3270E Server software components and prereqs

You must install the following software components on your TN3270E server:

- IBM Operating System/2
  - The TN3270E server with ELF was tested with the following OS/2 versions:
    - Warp Server Version 3 Advanced with Service Pack 42
    - Warp Version 4 (Merlin) with Service Pack 13
    - Warp Server Version 4.5 (Aurora) with Service Pack 1
- IBM LAN Adapter and Protocol Support
  - We used MPTS Version 6.0 (WR08700) to pick up the latest SSL support.

  - MPTS is packaged with OS/2 and with CS/2.
  - Version 6.0 is packaged with CS/2 v.6.1.
- Netscape® Communicator V4.61 for OS/2, Secure US-only, Service Level 5 is required for Feature Install.
- IBM Feature Install (FI) 1.2.5
  - You may download the IBM Feature Installer from http://www.ibm.com/software/os/warp/swchoice
- IBM Java for OS/2
  - IBM Java 1.1.8 for OS/2 is required.
  - Java is required by the TCP/IP configurator and by the SSL Key Manager Utility.
  - You may download the IBM Java for OS/2 from http://www.ibm.com/software/os/warp/swchoice
- IBM Lan Services
  - This is optional, depending on whether you have a LAN with shared resources.
- IBM TCP/IP
  - This component is needed for TN3270 support and ELF support.
  - You must install TCP/IP version 4.3
- IBM Communications Server/2
  - CS/2 Version 6.1 is required for the TN3270 server with ELF support.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.1.2 Communications Server for OS/2

This section describes the configuration needed for Communications Server for OS/2 for the Express Logon Feature.

ELF Support for the Communications Server for OS/2 (CS2) is available with the 6.1 level. This document outlines the steps needed to do a TN3270E server configuration using SSL and client authentication. This is a prerequisite to enabling ELF. Details are provided for doing the ELF part of the configuration.

The items listed below should be configured to allow ELF support.

- Node Characteristics
- DLC Type
- SNA Connections
- DLUS Definitions (optional)
- LUA and 3270 Support
- TN3270E Server Definitions
  - TN3270E Ports (SSL Client Authentication must be enabled on the port definition.)
  - LU Pools
  - TN3270E Filters (optional)
  - CRL (optional)
  - ELF

Once the CS/2 TN3270E server has been defined to support SSL client authentication sessions, you can define ELF.

To define ELF you will need two pieces of information:

- TCP/IP name or address of the host DCAS
  If a TCP/IP name is used, CS/2 must be able to resolve it into an address when the node is started.
- TCP/IP port number of the host DCAS
  This defaults to 8990, but may be changed.

There is also a field to enable or disable ELF. Disabling ELF leaves the DCAS address and port number definitions in the configuration file, so they don't have to be re-entered when ELF is re-enabled.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.1.3 Configuring ELF (Express Logon Feature) Support

Configuration of DCAS for CS/2 is a manual process. The parameters are specified in either the .RSP file or the .NDF file and compiled using the cmsetup /r ...rsp or cmverify ...ndf utilities.

Express Logon Support (.RSP format)

The parameters for the .RSP file for the EXPRESS_LOGON_SUPPORT record are defined as follows:

1. EXPRESS_LOGON_SUPPORT_ENABLED - enabled/disabled switch, 1 = enabled, 0 = disabled
2. DCAS_ID - The IP Address or hostname of the DCAS server (see DCAS_ID_TYPE)
3. DCAS_ID_TYPE - The address type of the specified DCAS server, 0=IP Address, 1=Hostname
4. DCAS_PORT - The port number that the DCAS server is listening on

For example:

```
EXPRESS_LOGON_SUPPORT = (
    * COMMENT: This is a .RSP file example to enable/configure Express Logon feature in CS/2
    EXPRESS_LOGON_SUPPORT_ENABLED = 1
    DCAS_ID = 10.22.16.238
    DCAS_ID_TYPE = 0
    DCAS_PORT = 8990
)
```

Express Logon Support (.NDF format)

The parameters for the .NDF file for the DEFINE_EXPRES_LOGON_SUPPORT record are defined as follows:

1. ENABLED - The value can be either 'YES' or 'NO'
2. DCAS_ID - The IP address or hostname of the DCAS
3. DCAS_ID_TYPE - The value can be either 'IP_ADDRESS' or 'HOST_NAME'
4. DCAS_PORT - The port number that the DCAS server is listening on

For example:

```
DEFINE_EXPRESS_LOGON_SUPPORT
    ENABLED(YES)
    DCAS_ID(10.22.16.238)
```

DCAS_ID_TYPE(IP_ADDRESS)
DCAS_PORT(8990);

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.1.4 Configuring CRL (Certificate Revocation List) Support (optional)

Certificate Revocation List (CRL) is a feature that allows certificates to be revoked. Using CRL is optional when using ELF. To use this feature, a certificate must be created with a certificate issuer that supports certificate revocation (e.g., Verisign, IBM Trust Authority). When the certificate is created, a record of the certificate is stored in the issuer database and is exported to an LDAP server for runtime processing (i.e., for revoked certificate checking). When a request is made to connect using the certificate, the LDAP server is queried to determine if the certificate is revoked, expired, etc. If the certificate is revoked, the connection will not occur.

The CRL checking is only done on the SSL client authentication session from the HOD client to the CS/2 TN3270E server. CRL checking is not done on the SSL session to DCAS, although DCAS can do CRL checking at the host end of the CS/2 server certificate. The default root server certificate used by CS/2 also has to be issued by the Certificate Authority that maintains the LDAP that is being queried. CS/2 only supports checking one CRL.

To configure CRL support in the CS/2 platform , press the *TN3270E Optional parameters* button, press the *Define Ports* button, and then press the *Define CRL support* button. This will bring up the *CRL support information* panel. Now you can:

- Check the *Enable CRL support* box,
- Enter the LDAP IP address or hostname,
- Enter the Port number and optionally, under LDAP security, enter user ID and password, and
- Choose *OK*.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.1.5 Testing Your System

To test your system, make sure VTAM is started, your switched major node is active, and DCAS is started. Start communications on your CS/2 server. Monitor your CS/2 system using Subsystem Management:

Verify all of the services are started.

Choose details to verify your SNA subsystem and TN3270E server.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.2 Configuring ELF Support on Communications Server for AIX® (CS/AIX)

This section describes the configuration needed for Communications Server for AIX for the Express Logon Feature. Subsections contain information about:

Return to Part 2. Configuring Express Logon Feature
Return to Contents

ELF Support for the Communications Server for AIX (CS/AIX) is available with the 6.0.0.1 level and later. This document will only outline the steps needed to do a TN3270 server configuration using SSL and client authentication. This is a prerequisite to enabling ELF. Detailed steps will be given for doing the ELF part of the configuration.

The items listed below should be configured to allow ELF support.

- Node
- Port
- Link Station
- DLUR PU (optional)
- Dependent LUs
- LU Pools (optional)
- TN3270 server
  - TN3270 Port (SSL Client Authentication must be enabled on the port definition.)
  - CRL (optional)
  - SLP (optional)
  - ELF
    The ELF configuration in CS/AIX can only be done when the node is inactive.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.2.1 Hardware/Software Requirements

Communications Server v6.0.0.1 for AIX, when used for ELF, will need:

- Software
  - Communications Server for AIX v6.0.0.1 (APAR IY12323)
  - AIX 4.3.3 or later
  - gskit.rte @ 4.0.3.89
  - AIXWindows support
  - Java™ 1.1.6 or later
- Hardware
  - any RS/6000 system which will run AIX 4.3.3

- a TCP/IP network connection for the HOD clients
- an SNA network connection for the Linkstation (PU) and LUs
  This SNA connection may use TCP/IP via HPR/IP and DLUR.
  For example, see the sample HPR/IP (EE) Configuration and DLUR Configuration diagrams
- a TCP/IP network connection to DCAS on the host
  This TCP/IP connection may use SNA via AnyNet.
  For example, see the sample AnyNet Configuration diagram.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.2.2 Configuring ELF Support

Once the CS/AIX TN3270 server has been defined to support SSL client authentication sessions, you can define ELF. The ELF configuration in CS/AIX can only be done when the node is inactive. To define ELF you will need two pieces of information:

- TCP/IP name or address of the host DCAS
  If a TCP/IP name is used, CS/AIX must be able to resolve it into an address when the node is started.
- TCP/IP port number of the host DCAS
  This defaults to 8990, but may be changed.

There is also a field to enable or disable ELF. Disabling ELF leaves the DCAS address and port number definitions in the configuration file so they don't have to be re-entered when ELF is re-enabled.

Any of the CS/AIX configuration methods can be used to do the ELF configuration, including:

- SMIT
- xsnaadmin (Motif Administration)
- snaadmin (command line)
- Web Admin
- NOF API

2.2.2.2.1 Configuring ELF Support with SMIT

Follow this hierarchy in the SMIT panels:

smit sna

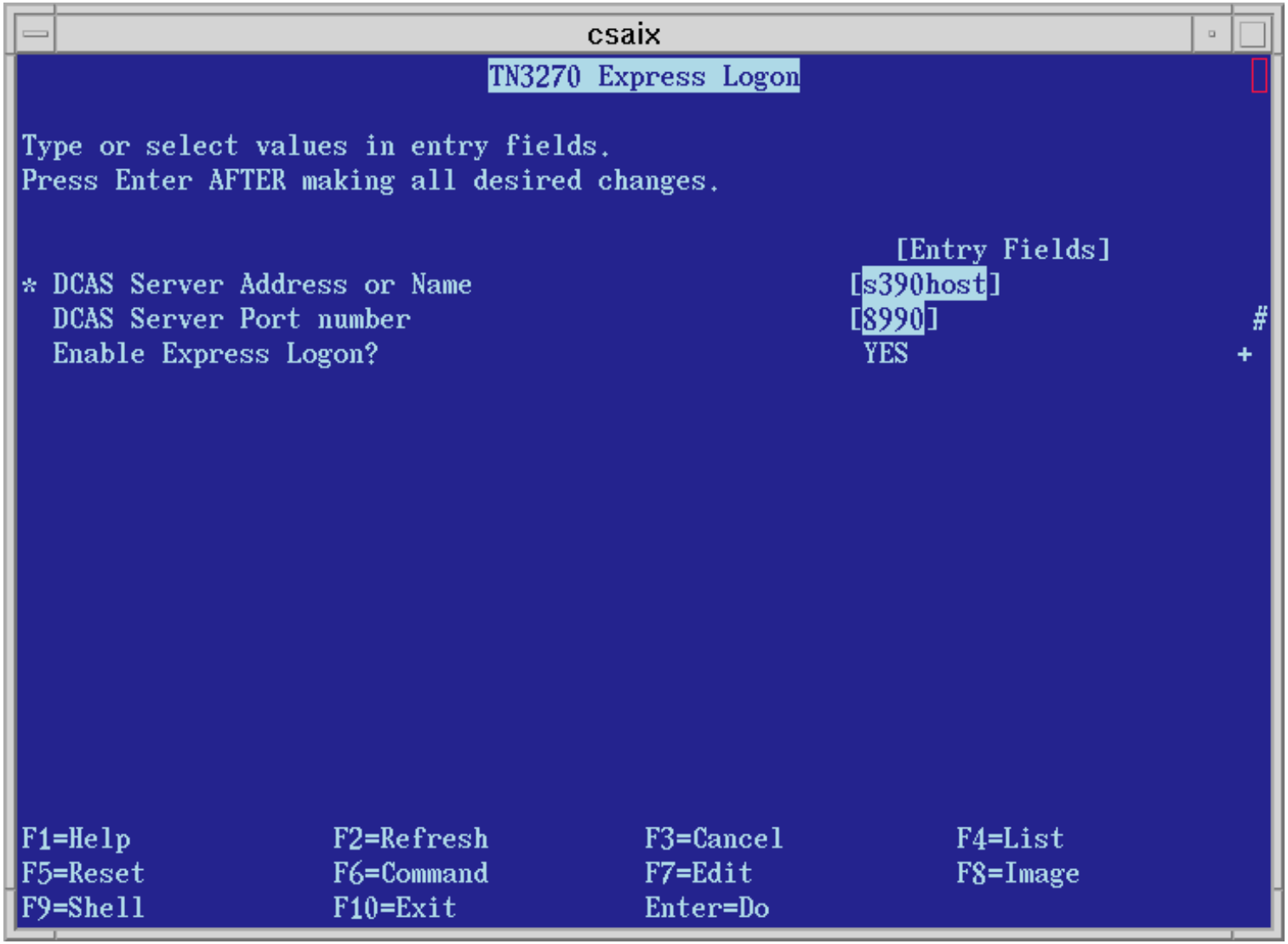
Configure SNA Resources

Local Node Resources

TN Server/Redirector

TN3270 Express Logon

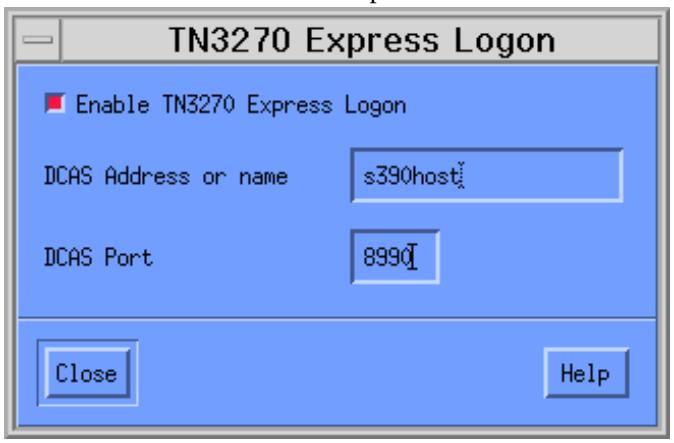
This will lead to the SMIT panel shown below:



2.2.2.2.2 Configuring ELF Support with 'xsnaadmin'

Follow this hierarchy in the xsnaadmin panels:
xsnaadmin
Services
TN Server
TN Server ...
Services (from the TN Server window)
TN3270 Express Logon

This will lead to the xsnaadmin panel shown below:



2.2.2.2.3 Configuring ELF Support with 'snaadmin'

The command line command for configuring ELF is:
snaadmin define_tn3270_express_logon, dcas_server=s390host, dcas_port=8990, enabled=YES

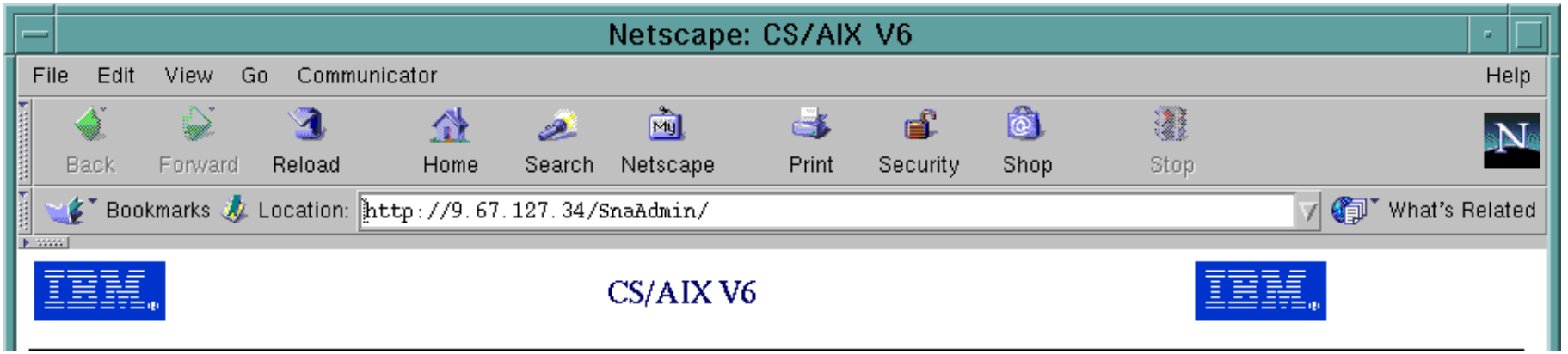
The usage statement can be displayed with the command:
snaadmin -d -h define_tn3270_express_logon

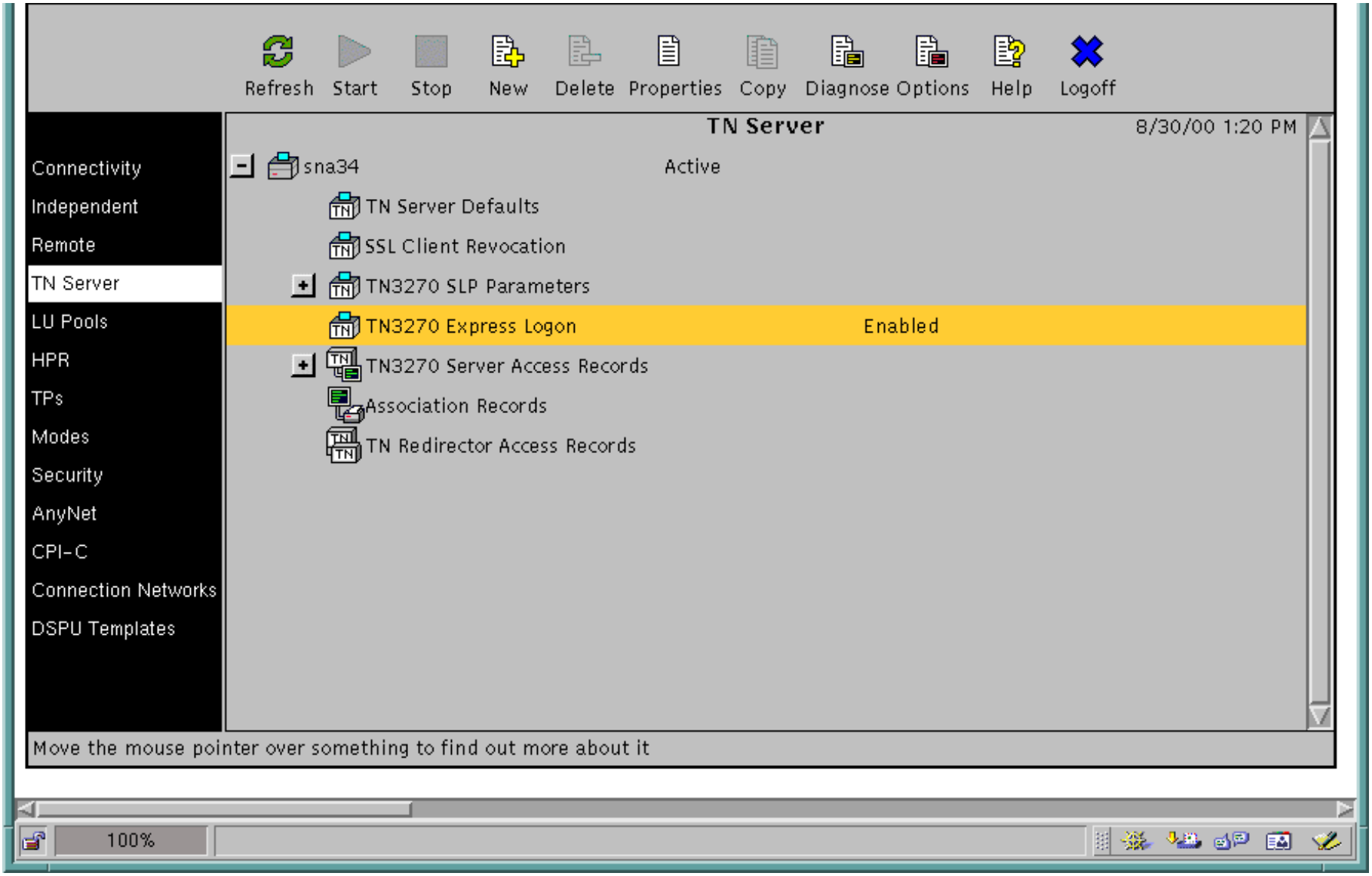
The current settings can be displayed with the command:
snaadmin query_tn3270_express_logon

2.2.2.2.4 Configuring ELF Support with Web Admin

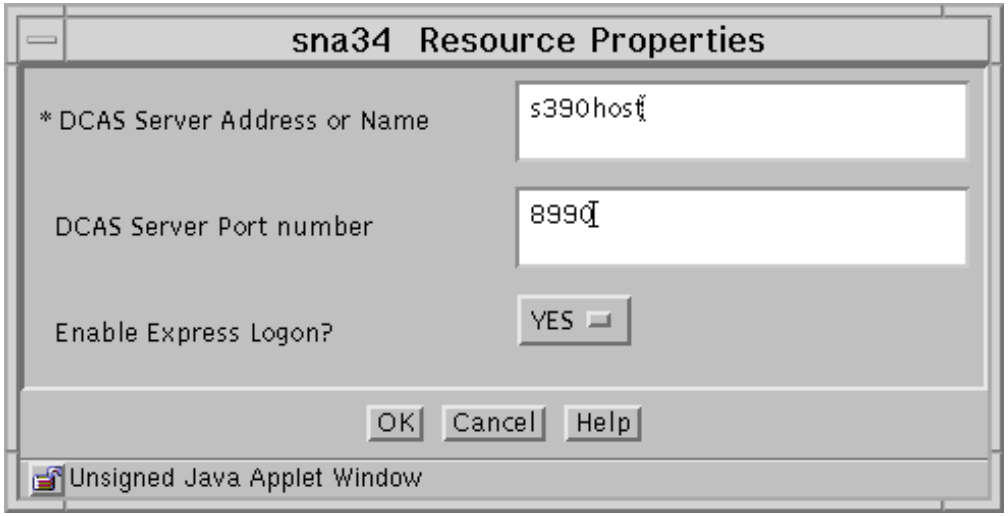
Follow these steps in the Web Admin tool:

- **http://*aixaddr*/SnaAdmin/**
  Where *aixaddr* is the TCP/IP address of the CS/AIX system.
- Logon to Web Admin
- Select **TN Server** from the list on the left.
  This will lead to the panel shown below:





- Select the **TN3270 Express Logon** item
- Click on **Properties**
  This will lead to the panel shown below:



Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.2.3 CS/AIX CRL Support (optional)

Certificate Revocation List (CRL) is a feature that allows certificates to be revoked. Using CRL is optional when using ELF. To use this feature, a certificate must be created with a certificate issuer that supports certificate revocation (e.g., Verisign, IBM Vault Registry). When the certificate is created, a record of the certificate is stored in the issuer database and is exported to an LDAP server for runtime processing (i.e., for revoked certificate checking). When a request is made to connect using the certificate, the LDAP server is queried to determine if the certificate is revoked, expired, etc. If the certificate is revoked, the connection will not occur.

The CRL checking is only done on the SSL client authentication session from the HOD client to the CS/AIX TN3270 server. CRL checking is not done on the SSL session to DCAS, although DCAS can do CRL checking at the host end of the CS/AIX server certificate. The default root server certificate used by CS/AIX also has to be issued by the Certificate Authority that maintains the LDAP that is being queried. CS/AIX only supports checking one CRL.

The LDAP server is configured in CS/AIX the same way that ELF is configured. The LDAP parameters can only be added/changed when the node is inactive. Enabling CRL checking is not required to use ELF. There are five parameters to configure CRL in CS/AIX:

- Enable/Disable CRL checking
- TCP/IP address or hostname of the LDAP Server which stores the CRL
- TCP/IP port number of the LDAP Server (defaults to 389)
- LDAP user ID (optional)
- LDAP Password (optional)

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.2.4 CS/AIX SLP Support (optional)

Service Location Protocol (SLP) is a feature that allows a HOD client to locate a TN Server dynamically instead of having the HOD client configure the explicit IP address and port number of the TN Server. Using SLP is optional when using ELF. Using SLP allows automatic load balancing between multiple TN Servers, even TN Servers running on different platforms (i.e. CS/NT, CS/AIX). If the HOD clients use SLP and you replace the TN Server, the HOD clients won't need to be updated to find the new

server.

Using SLP also gives you a form of fail-over. For example:

1. TN Server #1 fails
2. HOD client disconnects
3. HOD client sends SLP locate
4. TN Server #2 responds
5. HOD client reconnects using TN Server #2, with no configuration changes.

If this Communications Server is configured to use the SLP protocol for Load Balancing, you should only configure one encryption level on the various ports configured to allow ELF. This is because many TN3270 clients do not make full use of the SSLv3 details published by the Communications Server's SLP response packets. The clients (Host On-Demand V5 as one example) will typically connect to any port which has SSLv3 with the desired load factor if these are looking for an SSLv3 connection. If the client is not configured to use client authentication, the session negotiation will fail and another port will be chosen for an attempt. If client authentication is desired (as it is for ELF), the client will connect to the first port it finds with the right load factor, SSLv3 support and valid certificates. The encryption level is ignored by the HOD V5 client.

SLP is configured in CS/AIX the same way that ELF is configured.
The SLP parameters can be added/changed at any time.
Enabling SLP is not required to use ELF.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.3 ELF Support on Communications Server for Windows NT® and Windows 2000 (CS/NT)

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.3.1 Hardware/Software Requirements

Communications Server v6.1.1 for Windows NT and Windows 2000, when used for ELF, will need:

- Software
  - Communications Server for NT v6.1.1
  - Windows NT 4.0 with Service pack 6 or later
  - Java™ 1.1.6 or later (A Java JDK is installed with CS/NT 6.1.1)
- Hardware

- any computer system which will run CS/NT 6.1.1
- a TCP/IP network connection for the HOD clients
- an SNA network connection for the Linkstation (PU) and LUs
  This SNA connection may use TCP/IP via HPR/IP and DLUR.
  For example, see the sample HPR/IP (EE) Configuration and DLUR Configuration diagrams
- a TCP/IP network connection to DCAS on the host
  This TCP/IP connection may use SNA via AnyNet.
  For example, see the sample AnyNet Configuration diagram.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.3.2 Configuring ELF Support

ELF Support for the Communications Server for NT (CS/NT) is available with the 6.1.1 level and later. This section will only outline the steps needed to do a TN3270(E) server configuration using SSL and client authentication. This is a prerequisite to enabling ELF. Detailed steps will be given for doing the ELF part of the configuration. The SNA Node Configuration program can be used to configure the SNA Node. Since ELF is an "Advanced" function the Configuration Wizard is not used in the following discussion. Upon starting a new configuration, select the "Advanced" check box and proceed to the next panel.

The items listed below should be configured to allow ELF support.

- Node
- Port
- Link Station
- DLUR PU (optional)
- Dependent LUs
- LU Pools
- TN3270E Server
  - 2.2.3.3 Defining a TN3270(E) Port
  - 2.2.3.4 Configuring ELF Support (DCAS definition)
  - 2.2.3.5 Configuring CRL (optional)
  - 2.2.3.6 CS/NT SLP Support (optional)

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.3.3 Defining a TN3270E port

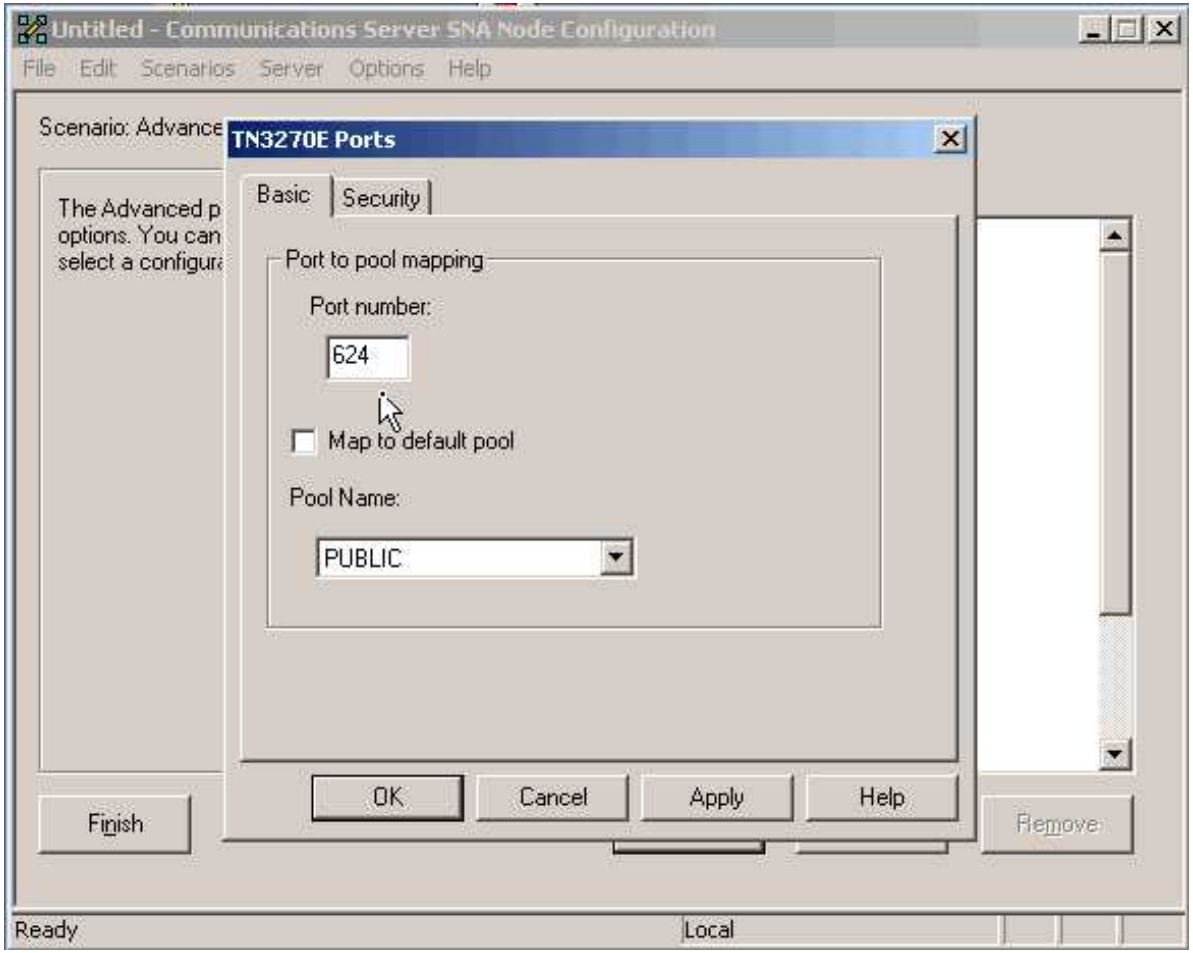
To create a TN3270E port, select the TN3270E Ports item in the configuration tree and press the Create button with the cursor. This will bring up a window which has two definition tabs:

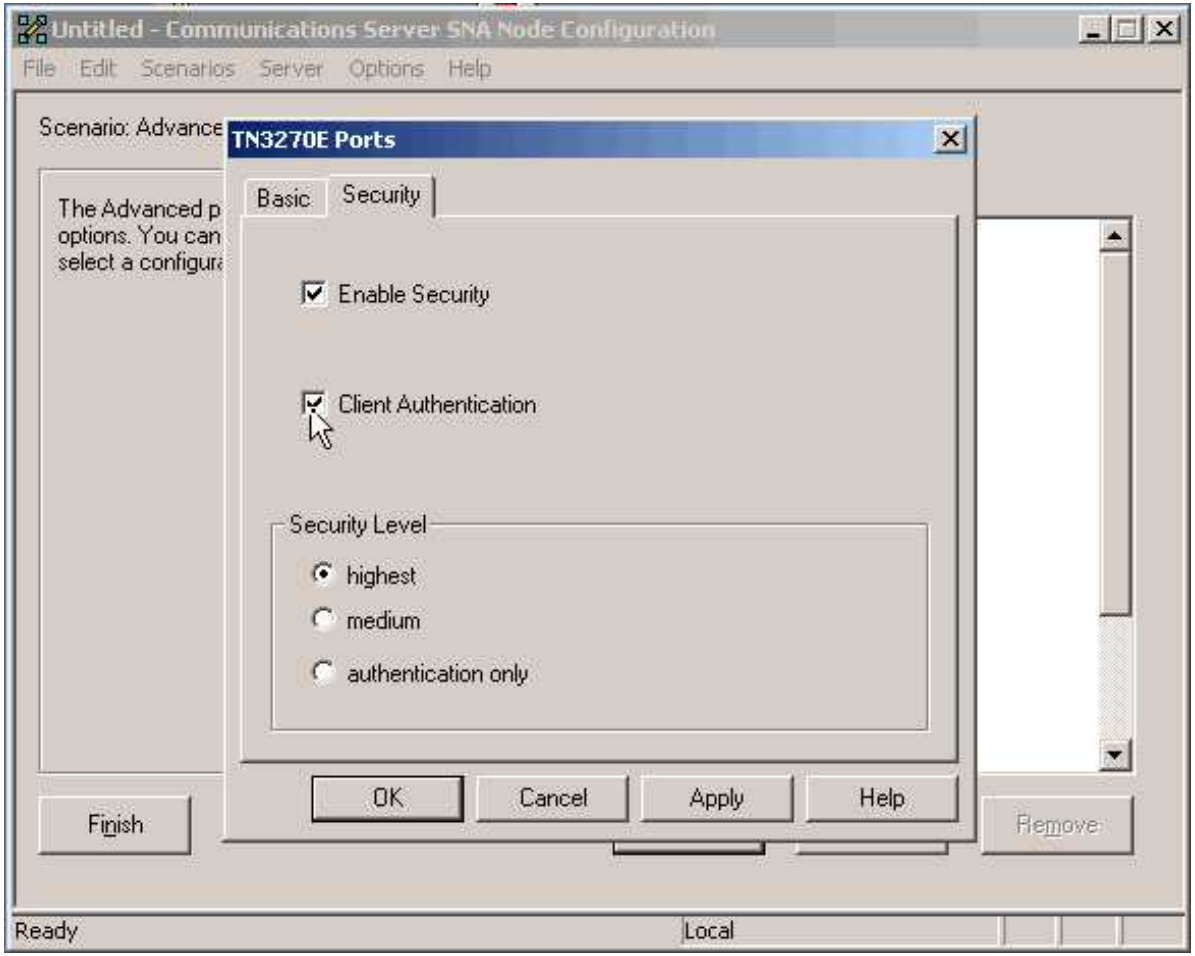
Basic

The Port number, Pool Name (or a map to default pool) are defined here.

Security

In this panel you define whether or not to use security and encryption functions. To enable encryption for the current port, check off the "Enable Security" box. This will allow an SSL session to connect over this port. Once enabled, the Security Level can be chosen (highest, medium, or authentication) To allow ELF to function over this port, select the "Client Authentication" check box. The port definition is now complete. Upon closing this Port definition a pop-up window will warn you that a certificate needs to be created and stored in the Communication Server keyring database.



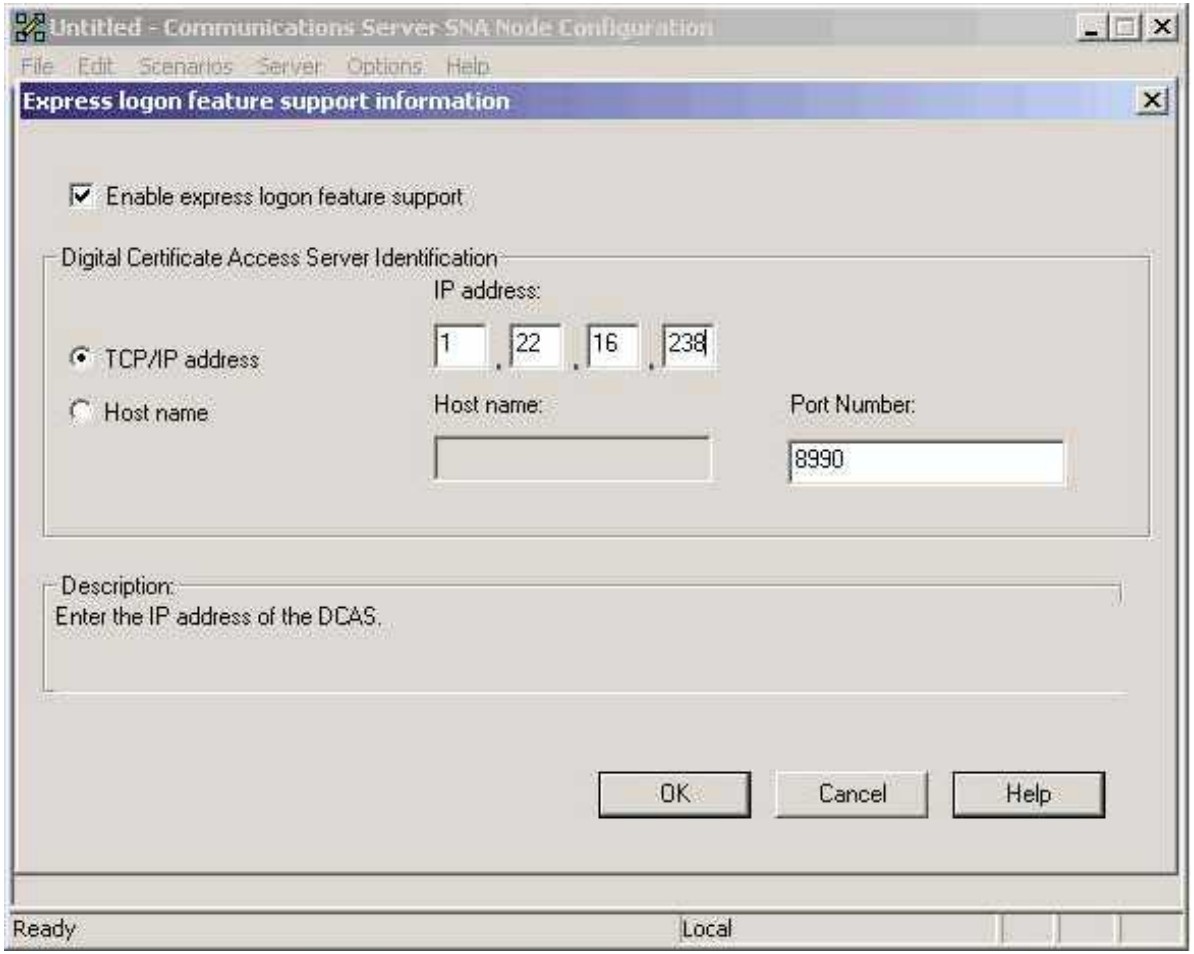


Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.3.4 Configuring ELF Support (DCAS definition)

The last item found under the TN3270E Server area is the "ELF Support" item. To enable the ELF support, press the create button. This will bring up a window where you can:

- Enable the function
- Record the TCP/IP address (or host name) associated with the DCAS
- Record the Port Number which the DCAS Server is listening on.
  The default value given is 8990, but the local DCAS installation might have changed this port number.



Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.3.5 CS/NT CRL Support (optional)

Certificate Revocation List (CRL) is a feature that allows certificates to be revoked. Using CRL is optional when using ELF. To use this feature, a certificate must be created with a certificate issuer that supports certificate revocation (e.g., Verisign, IBM Vault Registry). When the certificate is created, a record of the certificate is stored in the issuer database and is exported to an LDAP server for runtime processing (i.e., for revoked certificate checking). When a request is made to connect using the certificate, the LDAP server is queried to determine if the certificate is revoked, expired, etc. If the certificate is revoked, the connection will not occur.

The CRL checking is only done on the SSL client authentication session from the HOD client to the CS/NT TN3270(E) server. CRL checking is not done on the SSL session to DCAS, although DCAS can do CRL checking at the host end of the CS/NT server certificate. The default root server certificate used by CS/NT also has to be issued by the Certificate Authority that maintains the LDAP that is being queried. CS/NT only supports checking one CRL.

The LDAP server is configured in CS/NT the same way that ELF is configured. The LDAP parameters can only be added/changed when the node is inactive. Enabling CRL checking is not required to use ELF. There are five parameters to configure CRL in CS/NT: Certificate Revocation List (CRL) Support can be enabled by highlighting the CRL Support item in the configuration tree and pressing the create button. A "CRL Support Information window will be brought up. Here you can:

- Enable CRL Support
- Enter the TCP/IP address or hostname of the LDAP Server which stores the CRL.
- Enter the port tcp number used by the LDAP process.
- LDAP userid, if needed
- LDAP password, if needed for access to the LDAP Server.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.2.3.6 CS/NT SLP Support (optional)

Service Location Protocol (SLP) is a feature that allows a HOD client to locate a TN Server dynamically instead of having the HOD client configure the explicit IP address and port number of the TN Server.Using SLP is optional when using ELF. Using SLP allows automatic load balancing between multiple TN Servers, even TN Servers running on different platforms (i.e. CS/NT, CS/AIX). If the HOD clients use SLP and you replace the TN Server, the HOD clients won't need to be updated to find the new server.

Using SLP also gives you a form of fail-over. For example:

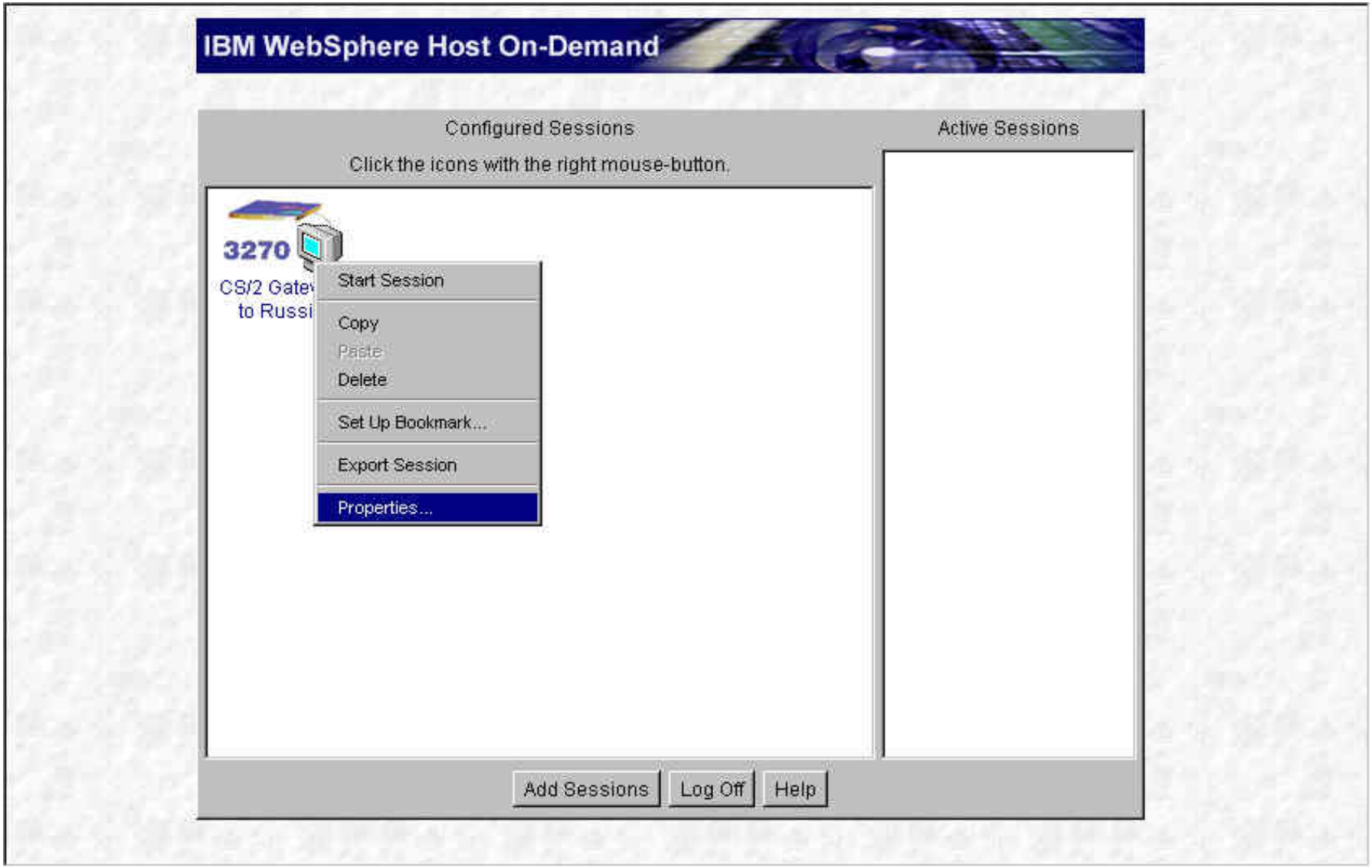
- TN Server #1 fails
- HOD client disconnects
- HOD client sends SLP locate
- TN Server #2 responds
- HOD client reconnects using TN Server #2, with no configuration changes.

If this Communication Server is configured to use the SLP protocol for Load Balancing, you should only configure one encryption level on the various ports configured to allow ELF. This is because many TN3270 clients do not make full use of the SSL details published by the Communications Server's SLP response packets. The clients (Host On-Demand V5 as one example) will typically connect to any port which has SSL with the desired load factor if these are looking for an SSL connection. If the client is not configured to use client authentication, the session negotiation will fail and another port will be chosen for an attempt. If client authentication is desired (as it is for ELF), the client will connect to the first port it finds with the right load factor, SSL support and valid certificates. The encryption level is ignored by the HODv5 client.

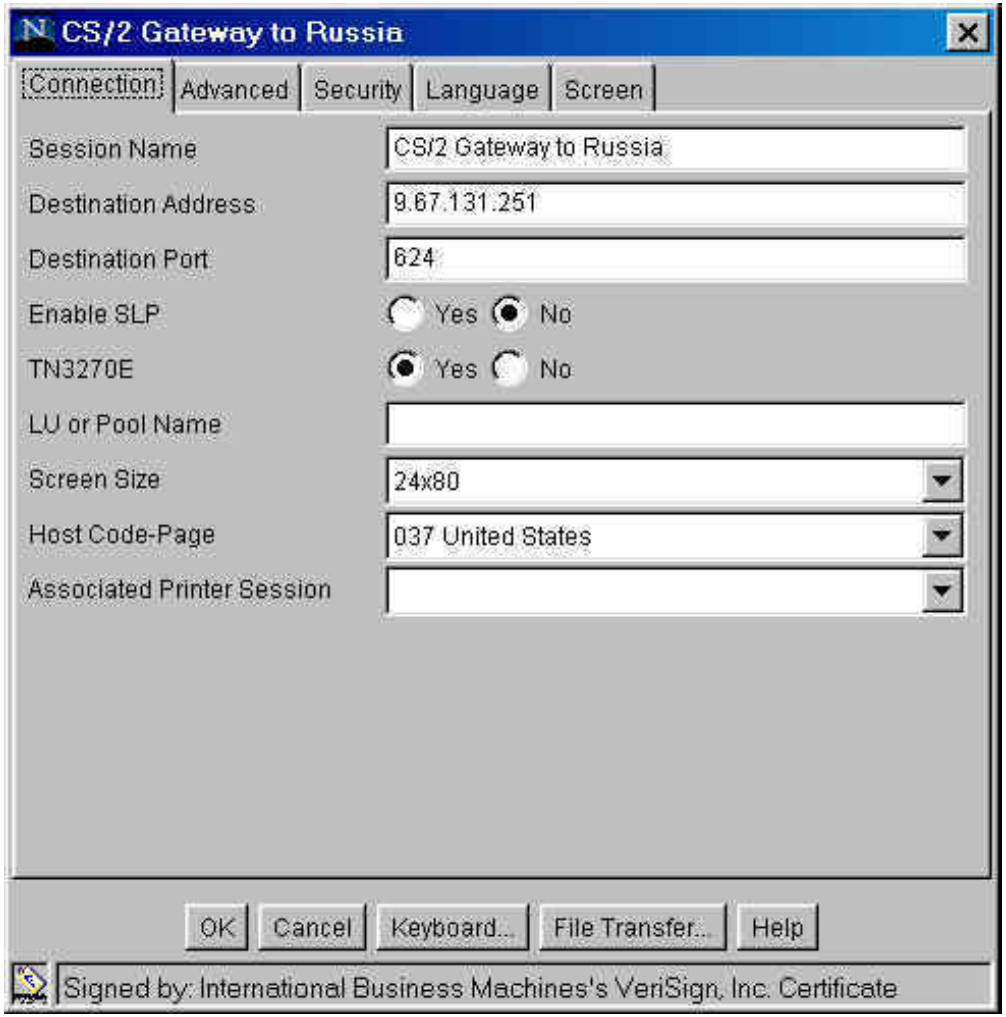
Return to Part 2. Configuring Express Logon Feature
Return to Contents

2.3 Defining the HOD 3270 Session Properties

Before an ELF Macro can be recorded, the Host On-Demand 3270 Session must be configured correctly. This task can be accomplished by the HOD Administrator (HODAdmin.html), or by a HOD user, if there are any preconfigured sessions. To configure the session for ELF, certain security properties must be defined. If a HOD session has already been defined, right click on the 3270 session icon, to modify the session properties:

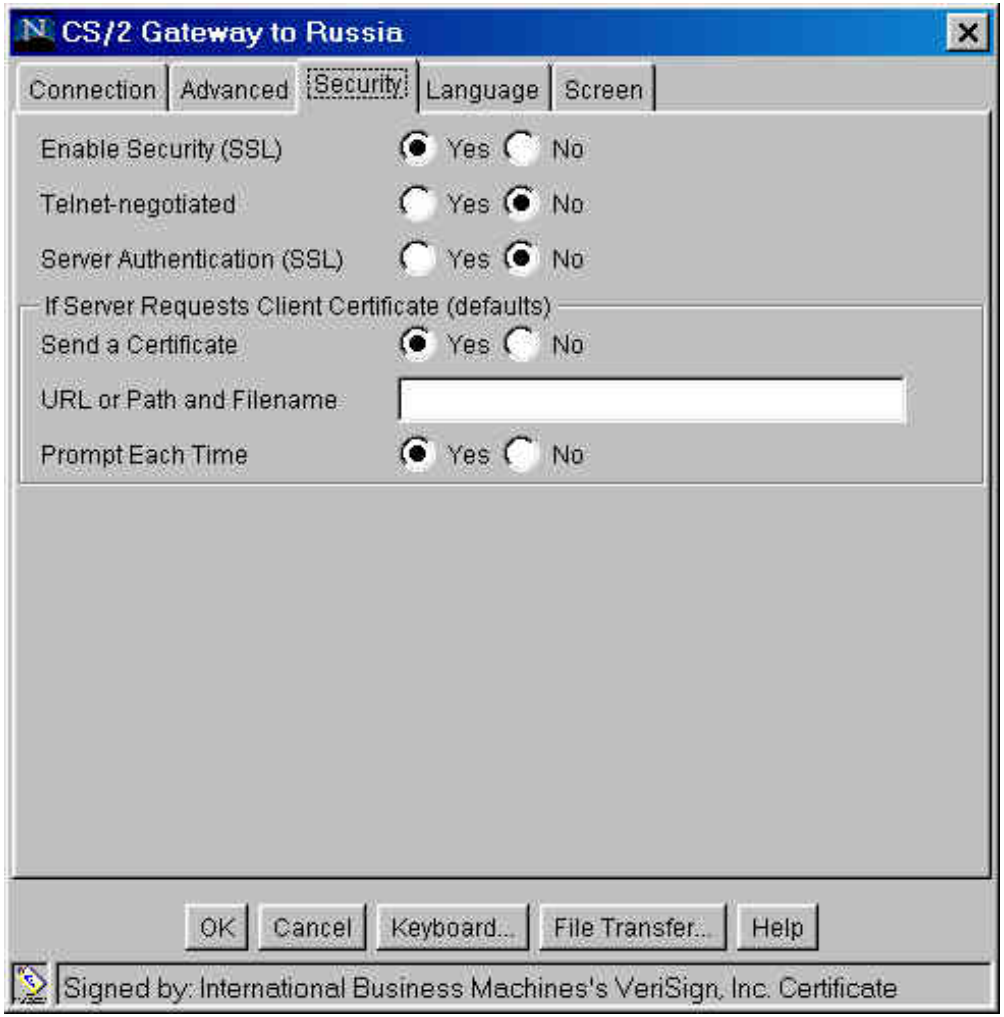


This will bring up the session properties. Note, there are five tabs. The first tab, which is the Connection tab, is used to define the address of the TN3270 server which will be the TN3270 gateway for the HOD client to the S/390® host. Both the TN3270 server and the S/390 host MUST be at levels that support ELF, for the ELF function to work.



ELF requires both SSL and client authentication to function correctly. For SSL to function correctly, the HOD client must have the TN3270 server certificate, if the server uses a self-signed certificate in its CustomizedCAs.class file. If the TN3270 server uses a certificate issued by a trusted CA, such as Verisign or IBM Trust Authority, then the trusted CA's root certificate must be in the HOD client's CustomizedCAs.class file. The HOD download and cached clients download the CustomizedCAs.class file for use from their (HOD) server, where it is located in the \hostondemand\hod (/usr/opt/hostondemand/HOD for HOD v5 on AIX) directory. Locally installed HOD clients access this file in their local \hostondemand\bin (/usr/opt/hostondemand/bin for HOD v5 on AIX) directory.

The client must be able to access a valid client certificate, stored in P12 format. For the TN3270 server to accept the client's certificate, it must either be issued by a trusted CA, or if the client uses a self-signed certificate, then it must be stored in the TN3270 server's key database.
The HOD client Security tab must be configured to Enable Security (SSL), and to Send a Certificate. The URL or Path and Filename and Prompt Each Time fields may be optionally selected and filled in.



Configure any additional HOD 3270 session information, as desired, then save and close the session properties.

Return to Part 2. Configuring Express Logon Feature
Return to Contents

Part 3: Setting up Required Certificates for Express Logon Feature

The third major step in setting up your environment to use Express Logon Feature is setting up the appropriate SSL certificates on each machine in your environment. The steps to set up certificates have been broken down into three sections:

3.1 Starting the Key Management Utility

Before executing any of the steps involving the creation or addition of certificates you must first open the Key Management Utility. The Key Management Utility for each product is used to create, add, and delete all required certificates. Below is a brief description of how to open the Key Management Utility for each product on each platform:

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.1.1 Opening the Key Management Utility for CS/NT

The Key Management Utility for CS/NT can be started by selecting '**Start**', then '**Programs**', then '**IBM Communications Server**' and then '**Key Management Utility**'.

Before using the database, a database file must be selected. To do this, left mouse click on Key Database File in the top left corner of the GUI display:

- If **New** is selected, you will need to provide a new database name. The type must be defaulted to CMS key database file, and name must be ibmcs.kdb. (Install automatically creates an ibmcs.kdb. Hence, only select New if the original ibmcs.kdb has become corrupt or if you simply want to create a new kdb from scratch.) The required location for this file is in **Install_Drive:\ibmcs\private.** Once this panel has been filled in, press **OK** and the password prompt window will now pop up. This password will be used each time you open this key database file so it is important to remember it. In addition, be sure to stash your password, so that SNA can access the key database file for SSL use. Choose **OK**, and the database is ready for use.
- If **Open** is selected, a list of files from **Install_Drive:\ibmcs\private** will come up. Locate the **ibmcs.kdb** file, highlight it, and choose OK. At this point a password prompt will pop up. The password is initially set to **ibmcs**. However, you should change this once you have entered the database. To change your database password, select Key Database File from the upper left corner of the IBM Key Management graphical interface. Select Change Password, and at the change password pop-up enter your new password. Be sure to stash the password.

You have now completed the initial step to start working with certificates on the CS/NT server. When the CS/NT key database is updated, you must close the key database and then stop and start the node before CS/NT will recognize the new certificates.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.1.2 Opening the Key Management Utility for CS/AIX

The Key Management Utility for CS/AIX is an XWindows application. If you have an XWindows capable terminal available, set the DISPLAY variable to point to it:

export DISPLAY=myXWindowsDisplay:0

If your CS/AIX system does not have a graphics display, you can use the Key Management Utility from another platform (e.g. HOD) to create the CS/AIX key database and

then move it (e.g., binary FTP) to the /etc/sna directory on the CS/AIX system.

The Key Management Utility for CS/AIX is also a Java™ application. You need to set up the environment to point to the Java location. For Java 1.1.6 or 1.1.8 you need to:

export JAVA_HOME=/usr/jdk_base
(Note: /usr/jdk_base is the directory where Java 1.1.6 or 1.1.8 is installed)

For Java 1.3.0 you need to:
export PATH=/usr/java130/jre/bin:/usr/java130/bin:$PATH

Once the export(s) have been run, type in the following to start the Utility:
snakeyman

Before using the database, a database file must be selected. To do this, left mouse click on **Key_Database_File** in the top left corner of the GUI display:

- If **Open** is selected, a list of files from /etc/sna/ will come up. Locate the ibmcs.kdb file, highlight it, and choose **OK**. At this point a password prompt will pop up. The password is initially set to ibmcs. However, you should change this once you have entered the database. To change your database password, select **Key_Database_File** from the upper left corner of the IBM Key Management graphical interface. Select **Change_Password**, and at the change password pop-up enter your new password. Be sure to stash the password.
- If **New** is selected, the user will need to provide a new database name. The type must be defaulted to CMS key database file, and name must be **ibmcs.kdb**. (Install automatically creates an ibmcs.kdb. Hence, only select New if the original ibmcs.kdb has become corrupt or if the user simply wants to create a new kdb from scratch.) The required location for this file is in /etc/sna/. Once this panel has been filled in, press **OK** and the password prompt window will now pop up. This password will be used each time you open this key database file so it is important to remember it. In addition, be sure to stash your password, so that CS/AIX can access the key database file for SSL use. Choose OK, and the database is ready for use.

You have now completed the initial step to start working with certificates on the CS/AIX server.

When the CS/AIX key database is updated, you must close the key database and then stop and start the node before CS/AIX will recognize the new certificates:
snaadmin term_node
snaadmin init_node

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.1.3 Opening the Key Management Utility for CS/2

The Key Management Utility for CS/2 can be opened by clicking on the "**Key Management Utility**" icon in the "**IBM Communications Server**" folder on the OS/2 desktop.

Before using the database, a database file must be selected. To do this, left mouse click on Key Database File in the top left corner of the GUI display:

- If **New** is selected, you will need to provide a new database name. The type must be defaulted to "CMS key database file", and name must be ibmcs.kdb. (Install automatically creates an ibmcs.kdb. Hence, only select New if the original ibmcs.kdb has become corrupt or if you simply want to create a new kdb from scratch.) The required location for this file is in **Install_Drive:\CMLIB\SSL.** Once this panel has been filled in, press **OK** and the password prompt window will now pop up. This password will be used each time you open this key database file so it is important to remember it. In addition, be sure to stash your password, so that CS/2 can access the key database file for SSL use. Choose **OK**, and the database is ready for use.
- If **Open** is selected, a list of files from **Install_Drive:\CMLIB\SSL** will come up. Locate the **ibmcs.kdb** file, highlight it, and choose OK. At this point a password

prompt will pop up. The password is initially set to **ibmcs**. However, you should change this once you have entered the database. To change your database password, select Key Database File from the upper left corner of the IBM Key Management graphical interface. Select Change Password, and at the change password pop-up enter your new password. Be sure to stash the password.

You have now completed the initial step to start working with certificates on the CS/2 server. When the CS/2 key database is updated, you must close the key database and then stop and start the node before CS/2 will recognize the new certificates.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.1.4 Opening the Key Management Utility for HOD

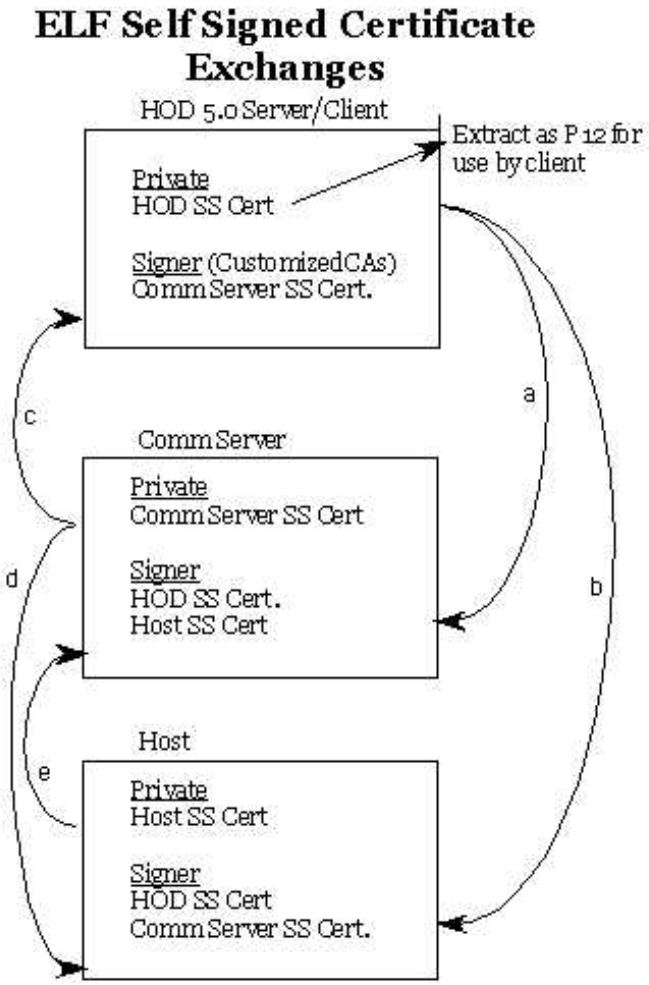
The Key Management Utility for HOD can be opened by selecting '**Start**', then '**Programs**', then '**IBM Host On-Demand**', then '**Administration**', and finally '**Certificate Management**'. The next step is to either Open a key database, if it already exists, or create a New key database. For this example, the key database which will be used already exists. From the **IBM Key Mangement** window, select 'Open' from the Key Database File dropdown list.

When the HOD key database is updated you have to restart the Web Browser before HOD will recognize new certificates.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.2 Using Self-Signed Certificates

The picture seen here gives you a visual overview of the certificates that must be generated and copied to each of the three locations when using self-signed certificates. Each arrow in the figure represents where a certificate has been created and where it must then be distributed. For example, arrow 'a' below illustrates that the self-signed certificate created on the HOD client must be added as a Signer certificate in the TN3270 Server's key database.



Below are steps necessary to complete certificate setup (illustrated in the figure above) when using self-signed certificates for Express Logon Feature.

2.1.5.1 Creating Self-Signed Certificates on the Host
3.2.1 Creating Certificates for the TN3270 Communications Server
3.2.2 Creating Certificates for the HOD Client
3.2.3 Adding Certificates to the Host
3.2.4 Adding Certificates to the TN3270 Communications Server
3.2.5 Adding Certificates to the HOD Client

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.2.1 Creating Certificates for the TN3270 Communications Server

To set up the TN3270 Communications Server to use self-signed Certificates, open the Key Management Utility (see section 3.1) and complete the following steps.

1. Select **New Self-signed Certificate** from the Create menu option to create a new self-signed certificate. The Create New Self-Signed Certificate dialog appears.

2. Enter the name (label) that is used to identify the key and certificate within the database. Select **X509 V3** as the certificate version.

3. Enter the number of the key size you want to use. Choosing a larger key size results in stronger security, but requires more processing on the client and the server to establish a connection and to encrypt/decrypt each packet.

4. Enter the TCP/IP host name of the Communications Server as the common name (for example, aix01.raleigh.ibm.com).

5. Enter an **organization name** (free form text).

6. Enter an organization unit (optional).

7. Enter a city or locality (optional).

8. Enter a state or province (optional).

9. Enter a ZIP code (optional).

10 Enter a country code. You must specify at least 2 characters (for example, US).

11. Enter the number of days the self-signed certificate is to be valid.

12. Click **OK**

13. Click **Yes** when prompted to set the key as the default key in the key database if there is already another key in the database. If this is the first key in the database, it will automatically be set as the default.

Once the self-signed certificate has been created it will need to be extracted so it can be distributed to the HOD client and the Host. To extract the self-signed certificate:

14. Select **Personal Certificates** from the drop-down list, highlight your self-signed certificate and click **Extract Certificate**. The Extract Certificate to a File dialog appears.

15. Select **Binary DER**, as the data type.

16. Enter the certificate file name. The file should have a file type of .der (for example, ibmcs.der).

17. Enter the location (absolute path name) of the certificate.

18. Click **OK**.

You now have a self-signed certificate that in later steps will be distributed to the HOD client and Host.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.2.2 Creating Certificates for the HOD Client

To implement SSL, certificates also need to be stored on the client(s). The client will need a client certificate (client certificate will be a .p12 file, i.e, filename.p12) located somewhere on the local client drive. (Note: If your environment is set up so that local client installations of the HOD client are not present on a user's machine, but instead you use a HOD server to provide users with HOD emulation via a web browser, the p12 file that is generated in the steps that follow must be copied to local client machine.)

The following text describes the procedure used to create self-signed certificates using IBM's Host On-Demand V5.0 emulator software.

1. Open Host On-Demand's Key Management utility.

2. Open the database file '**HODClientKeyDb.kdb**' by first selecting **Key Database File** from the top left corner of the GUI. Next select **Open**, and then select **HODClientKeyDb.kdb** as the file to open.

A password prompt panel will pop up. The initial password for this database file is **ncod** (it is suggested that you change this password for security reasons.)

3. Select **New Self-Signed Certificate** from the Create menu option to create a new self-signed certificate. The Create New Self-Signed Certificate dialog appears.

4. Enter the name (label) that is used to identify the key and certificate within the database. Select **X509 V3** as the certificate version.

5. Enter the number of the key size you want to use. Choosing a larger key size results in stronger security, but requires more processing on the client and the server to establish a connection and to encrypt/decrypt each packet.

6. Enter the TCP/IP host name of the Host On-Demand client as the common name (for example, clienta.raleigh.ibm.com).

7. Enter an **organization name** (free form text).

8. Enter an organization unit (optional).

9. Enter a city or locality (optional).

10. Enter a state or province (optional).

11. Enter a ZIP code (optional).

12. Enter a country code. You must specify at least 2 characters (for example, US).

13. Enter the number of days the self-signed certificate is to be valid.

14. Click **OK**.

15. Click **Yes** to set the key as the default key in the key database.

Once the self-signed certificate has been created it will need to be extracted out of the client's database in .der format so it can be distributed to the TN3270 Server and Host.

Using the IBM Key Management Utility for HOD on the client, follow these steps:

16. Select **Personal Certificates** from the drop-down list, highlight the self-signed certificate that was just created and click Extract Certificate. The Extract Certificate to a File dialog appears.

17. Select **Binary DER** as the data type.

18. Enter the certificate file name. The file should have a file type of .der (for example, ibmcs.der).

19. Enter the location (path name) of the certificate.

20. Click **OK.**

Export client's personal self-signed key to create filename.p12

21. Select **Personal Certificates** from the drop down menu.

22. Highlight the self-signed certificate that was just created and select **Export/Import**. The Export/Import Key dialog box will appear.

23. Select **Export Key** for Action Type.

24. Key file type should be PKCS12 file.

25. Enter a filename with the .p12 extension (e.g. cert.p12).

26. Enter the location of where the file will be stored.

27. When prompted, enter a password for the key and click **OK**.

You now have a self-signed certificate in .der format that will in later steps be distributed to the TN3270 Server and Host. You also have a filename.p12 file and associated password that will be used when connecting an ELF TN3270 session to the TN3270 server when using client authentication.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.2.3 Adding Certificates to the Host

Two certificates need to be added to the host's keyring. The TN3270 server's self-signed certificate and the HOD client's self-signed certificate must be added as Signer certificates.

FTP the binary .DER data file to the host using ftp's binary option. If using RACF for the keyring or CLIENTAUTH SAFCERT, an MVS file will need to be created. If ftp created an HFS file, use the OGET comment to create an MVS file:
OGET 'hfs-path-and-filename' 'mvs-file-name' BINARY
example: **OGET '/ETC/SSL/HODCLIENT.DER' 'DCASID.HODCLIENT.DER' BINARY**

To add the TN3270 server's self-signed certificate as a Signer Certificate:

1. Be sure to use a user ID that has been set up as described in section 2.1.3 Configuring RACF Services for the DCAS. This is so the TN3270 server has the authority to do DCAS queries and get passtickets. For example:

RACDCERT ID(*dcasid*) ADD(*TNSERVSS*.der)
WITHLABEL('*TNSERVSS.dcasid*') TRUST

2. If this certificate is for the TN3270 server, you need to run one more RACF command to connect the certificate to the keyring. This does not have to be done for the HOD Client certificates.

RACDCERT ID(*dcasid*) CONNECT(ID(*dcasid*)
RING(*SERVERKeyring*) LABEL('*TNSERVSS.dcasid*')
USAGE(CERTAUTH))

3. Refresh the DIGTCERT and DIGTRING class:

SETROPTS RACLIST (DIGTRING DIGTCERT) REFRESH

NOTE: The DCAS server must be restarted after the SETROPTS command is issued in order to recognize the RACF changes.

To add the client's self-signed certificate:

1. To add the HOD client's self-signed certificate:
   Use the appropriate TSO/Netview/CICS user ID.
   RACDCERT ID(*user90*) ADD(*hod90ss.der*)
   WITHLABEL('*hod90ss.user90*') TRUST

2. Refresh the DIGTCERT class:
   SETROPTS RACLIST (DIGTCERT) REFRESH

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.2.4 Adding Certificates to the TN3270 Communications Server

Two certificates need to be added to the TN3270 server. The host's self-signed certificate and the HOD client's self-signed certificate both need to be added as Signer Certificates to the TN3270 Server's key database (ibmcs.kdb).

To add the host's self-signed certificate as a Signer Certificate:

1. Start the Key Management Utility.

2. Open the key database file '**ibmcs.kdb**' by first selecting **Key Database File**, from the top left corner of the GUI. Next select Open, and then select **ibmcs.kdb** as the file to open.

3. Select **Signer Certificates** from the drop-down list and click Add to receive the self-signed certificate that was previously generated on the Host. The Add CA Certificate from a File dialog appears.

4. Ensure that the data type is Binary DER.

5. Enter the certificate file name.

6. Enter the location (path name) of the certificate. Click **OK.** The file is marked as trusted and is stored as a signer certificate.

To add the Client's self-signed certificate as a Signer Certificate:

7. Click **Add** again to receive the self-signed certificate that was previously generated on the Client. The Add CA Certificate from a File dialog appears.

8. Ensure that the data type is Binary DER.

9. Enter the certificate file name.

10. Enter the location (path name) of the certificate. Click **OK**. The file is marked as trusted and is stored as a signer certificate.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.2.5 Adding Certificates to the HOD Client

One certificate needs to be added to the HOD Client. The TN3270 server's self-signed certificate must be added as a Signer Certificate to HOD's CustomizedCAs.class file. (Note: If your environment is set up so that local client installations of the HOD client are not present on a user's machine, but instead you use a HOD server to provide users with HOD emulation via a web browser, the CustomizedCAs.class file mentioned below will be on your HOD server.)

To add the TN3270 Server's self-signed certificate as a Signer Certificate:

1. Start the Key Management Utility for HOD.

2. Open the class file '**CustomizedCAs.class**' by first selecting **Key Database File**, from the top left corner of the GUI. Next select **Open**, and then select **CustomizedCAs.class** as the file to open. The path to CustomizedCAs.class will be: **'installdrive:\hostondemand\lib\CustomizedCAs.class.'**

3. Select **Signer Certificates** from the drop-down list and click **Add** to receive the self-signed certificate that was previously generated on the TN3270 Communication Server. The Add CA Certificate from a File dialog appears.

4. Ensure that the data type is Binary DER.

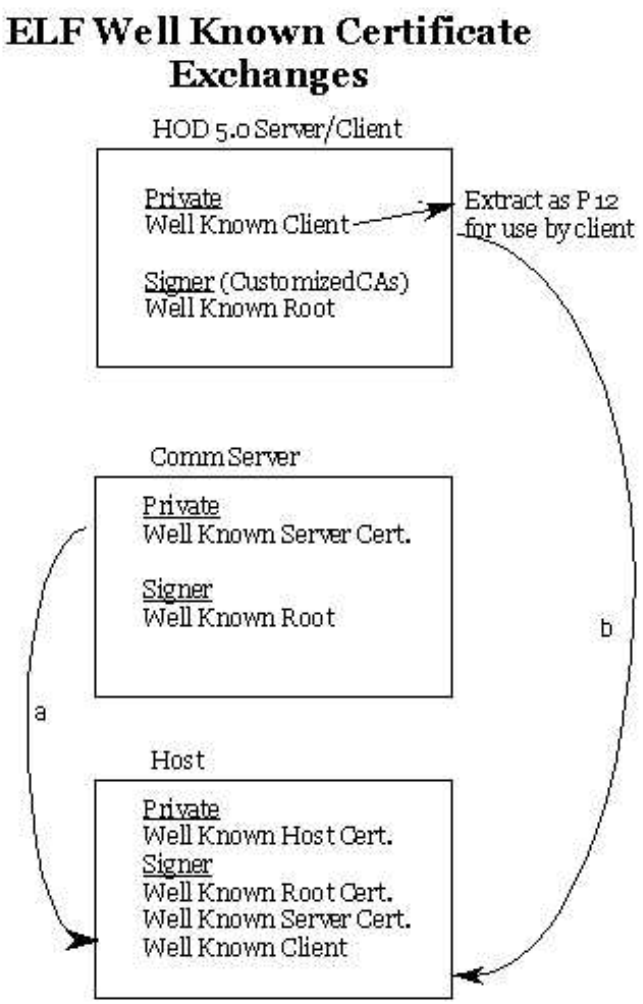
5. Enter the certificate file name.

6. Enter the location (path name) of the certificate. Click **OK**. The file is marked as trusted and is stored as a signer certificate.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.3 Using Well-Known Certificates

The picture seen here gives you a visual overview of the certificates that must be generated and copied to each of the three locations when using Well-Known certificates. Each arrow in the figure represents where a certificate has been created and where it must then be distributed. For example, arrow 'a' below illustrates that the Well-Known Server certificate on the Communications Server must be added as a Signer certificate in the host's keyring database.



Below are steps necessary to complete certificate setup (illustrated in the figure above) when using Well-Known Certificates for Express Logon Feature.

2.1.5.2 Creating Well-Known Certificates on the Host
3.3.1 Creating Certificates for the TN3270 Communications Server
3.3.2 Creating Certificates for the HOD Client
3.3.3 Adding Certificates to the Host
3.3.4 Adding Certificates to the TN3270 Communications Server
3.3.5 Adding Certificates to the HOD Client

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.3.1 Creating Certificates for the TN3270 Communications Server

To set up the TN3270 Communications Server to use an unknown CA certificate (not already defined in the database, such as certificates obtained from IBM's Vault Registry), the following procedures are necessary:

- Create a key and certificate request
- Submit a certificate request to the CA
- Obtain the CA's root certificate and your certificate to add them to the TN3270 server's key database

Creating a Key and Certificate Request

Use the following steps in the TN3270 Communication Server's Key Management Utility to create the public/private keys and certificate request:

1. Select **Personal Certificate Requests** from the drop-down list of the main menu and click **New** to create a new key pair and certificate request. The Create New Key and Certificate Request dialog appears.

2. Enter the name (label) that is used to identify the key and certificate within the database.

3. Enter the number of the key size you want to use. Choosing a larger key size results in stronger security, but requires more processing on the client and the server to establish a connection and to encrypt/decrypt each packet.

4. Enter the TCP/IP host name of the Communications Server as the common name (for example, aix01.raleigh.ibm.com).

5. Enter an **organization name.**

6. Enter an organization unit (optional).

7. Enter a city or locality (optional).

8. Enter a state or province (optional).

9. Enter a ZIP code (optional).

10. Enter a country code. You must specify at least 2 characters (for example, US).

11. Enter a certificate request file name, or use the default file name.

When you click OK, the information you supplied is processed. You should now have a certificate request under Personal Certificates Requests. You must now Extract this request from the database to be submitted to a certificate authority. To extract the request:

12. Select **Personal Certificate Requests** from the drop-down list, highlight the self-signed certificate that was just created and click **Extract Certificate.** The Extract Certificate to a File dialog appears.

13. Select Binary DER as the data type.

14. Enter the certificate file name. The file should have a file type of .der (for example, ibmcs.der).

15. Enter the location (path name) of the certificate.

16. Click **OK.**

Submitting a Certificate Request

Follow the procedures of the Well-Known Certificate Authority (CA) to submit the server certificate request. Depending on the CA you choose, either e-mail the certificate request generated by the Key Management Utility or incorporate the certificate request into the form or file provided by the CA. Once, the request is submitted, you should

receive a Well-Known Server certificate from your CA.

Obtaining a Well-Known Root Certificate from your CA.

Follow the procedures of the Well-Known CA to obtain the Well-Known CA root certificate. Depending on the CA you choose, there should be a way to download the Well-Known CA root certificate from their website. This Well-Known root certificate will not only be needed for your TN3270 server, but also for the HOD Client and the host.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.3.2 Creating Certificates for the HOD Client

A client certificate from the Well-Known Certificate Authority (CA) must be obtained for your HOD client. To obtain this client certificate:

Start a Web browser and access the Web page of the CA the user is using to receive certificates. Follow the instructions provided to submit the client certificate request. Note: The user may be using IBM Vault Registry to generate certificates - this same procedure applies.

The user may or may not get the client certificate from the vendor (or IBM Vault Registry) in filename.p12 format. If the certificate is received in .p12 format, simply copy the certificate to the client machine (anywhere on the hard drive is fine). If the certificate is not received in .p12 format, the certificate will have to be added to HODClientKeyKdb.dkb file using the IBM Key Management Utility for HOD, and then the key (filename.p12) will have to be exported from the database.

Return to Part 3: Setting Up Required Certificates for Express Logon Feature

---

3.3.3 Adding Certificates to the Host

Three certificates will need to be added to the host. The Well-Known Root Certificate and Well-Known Server Certificate, and the HOD Client's Well-Known client certificate.

Adding the Well-Known Root Certificate and Well-Known Server Certificate

1. Add the Well-Known Root Certificate

   RACDCERT CERTAUTH ADD(*WKRoot*.der)
   TRUST WITHLABEL('*CARoot*')

2. RACDCERT ADD Well-Known Server certificate back into RACF.

   RACDCERT ID(*dcasid*) ADD(*DCASCA*.bin) WITHLABEL('*DCASCA*')

3. RACDCERT CONNECT CA (Certificate Authority) root certificate to keyring with usage CERTAUTH

   RACDCERT ID(*dcasid*) CONNECT(CERTAUTH LABEL('*CARoot*')
   RING(*SERVERKeyring*) USAGE(CERTAUTH) DEFAULT)

4. RACDCERT CONNECT server certificate to keyring with usage PERSONAL

   RACDCERT ID(*dcasid*) CONNECT(ID(*dcasid*) LABEL('*DCASCA*')
   RING(*SERVERKeyring*) USAGE(PERSONAL) DEFAULT)

5. Refresh the DIGTCERT and DIGTRING class:

SETROPTS RACLIST (DIGTRING DIGTCERT) REFRESH

NOTE: The DCAS server must be restarted after the SETROPTS command is issued in order to recognize the RACF changes.

Adding the Well-Known HOD Client Certificate:

1. RACDCERT ADD the HOD client certificate:

   RACDCERT ID(*user52*) ADD(*CAhod52.der*)
   WITHLABEL('*CAhod52.user52*') TRUST

2. Refresh the DIGTCERT class:
   SETROPTS RACLIST (DIGTCERT) REFRESH

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.3.4 Adding Certificates to the TN3270 Communications Server

Two certificates will need to be stored in ibmcs.kdb. The Well-Known Root certificate and the Well-Known Server certificate.

Storing the Well-Known Root Certificate in the Key Database

Before the user can add the server certificate the user has received from the CA, the signer (CA root) certificate must first be added as a Signer Certificate. Contact the CA to obtain this signer (CA root) certificate. You must store the CA root certificate in the key database before you store the certificate that you applied for. The signer (CA root) certificate validates the certificate you applied for. Use the IBM Key Management Utility for the TN3270 Communications server to store the signer (CA root) certificate.

1. Select **Signer Certificates** from the drop-down list and click **Add** to receive the CA root certificate. The Add CA Certificate from a File dialog appears.
2. Ensure that the data type is BASE64-encoded ASCII data (encoded 64 format).
3. Enter the certificate file name.
4. Enter the location (path name) of the certificate. Click **OK**. The file is marked as trusted and is stored.

Storing the Well-Known Server Certificate in the Key Database

To store the Well-Known Server certificate you applied for, use the Key Management Utility for TN3270 Communications Server to put the certificate into the key database file, ibmcs.kdb, located on the server.

5. Select **Personal Certificates** from the drop-down list of the main menu and click **Receive** to receive the key pair and certificate request. The Receive Certificate from a File dialog appears.
6. Ensure that the data type is BASE64-encoded ASCII data (encoded 64 format).
7. Enter the certificate file name.
8. Enter the location (path name) of the certificate. Click **OK.** The stored certificate displays as the first item.
9. Highlight the stored certificate and click **View/Edit**. The Key information dialog appears.
10. Click **Set the certificate as the default**. The selected key becomes the default.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

3.3.5 Adding Certificates to the HOD Client

The following steps describe how to add the well-known root certificate to the HOD CustomizedCAs.class file.
(Note: If your environment is set up so that local client installations of the HOD client are not present on a user's machine, but instead you use a HOD server to provide users with HOD emulation via a web browser, the CustomizedCAs.class file mentioned below will be on your HOD server.)

1. Start HOD Key Management Utility.

2. Open the class file '**CustomizedCAs.class**' by first selecting **Key Database File**, from the top left corner of the GUI. Next select **Open**, and then select **CustomizedCAs.class** as the file to open. The path to CustomizedCAs.class will be: '**installdrive:\hostondemand\lib\CustomizedCAs.class.**' open.

3. Select **Signer Certificates** from the drop-down list and click **Add** to receive the well-known root certificate. The Add CA Certificate from a File dialog appears.

4. Ensure that the data type is BASE64 armored ASCII data (armored 64 format).

5. Enter the certificate file name.

6. Enter the location (path name) of the certificate. Click **OK**. The file is marked as trusted and is stored as a signer certificate.

Return to Part 3: Setting up Required Certificates for Express Logon Feature
Return to Contents

Part 4: Using the Express Logon Feature

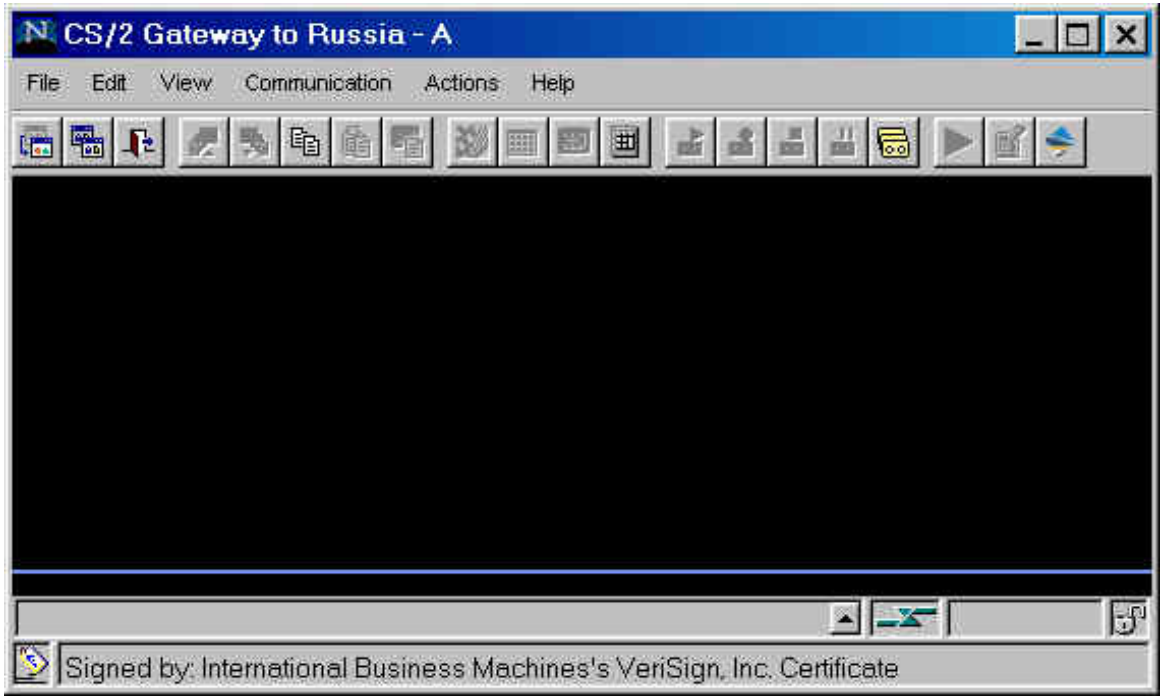
If you have correctly configured DCAS, at least one TN3270 server, and HOD using the instructions in this document, you are now ready to set up the end-user icons for HOD users to use the Express Logon Feature.

The following activities are described:

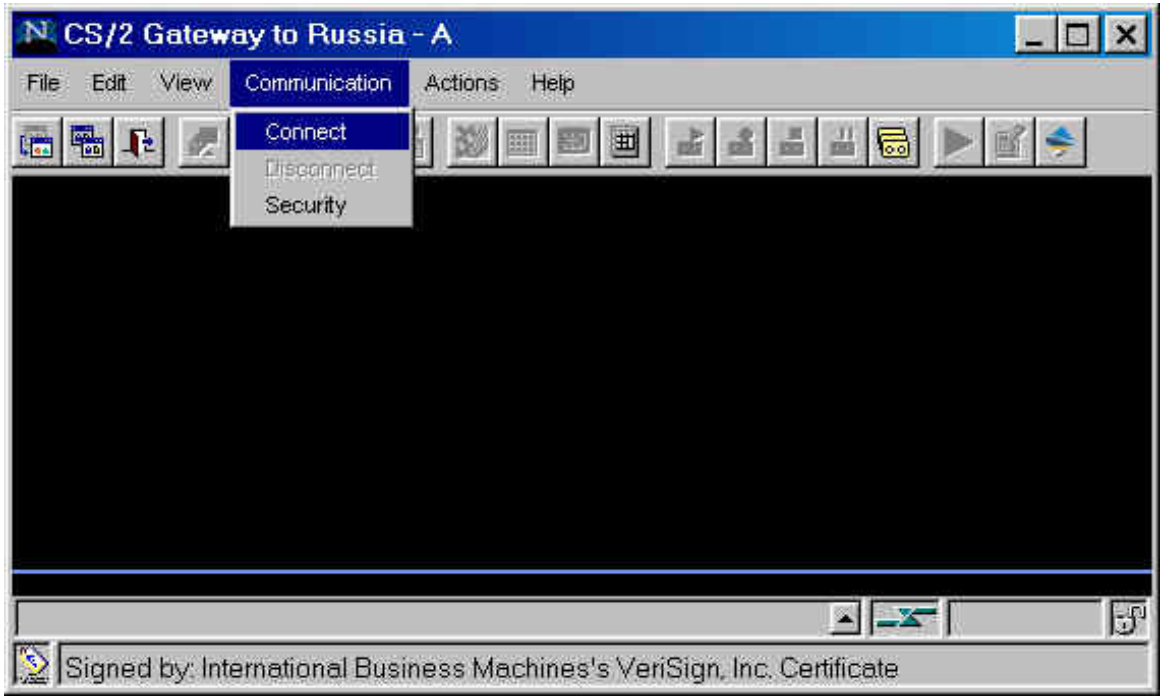
Return to Contents

4.1 Establishing the Initial 3270 SSL Connection

After the HOD 3270 session has been configured for ELF, it can be started by double-clicking on the session icon, or by right-clicking on the session icon, and then selecting **Start Session**. The HOD 3270 session window will come up. If it has been configured to **Connect Automatically**, on the **Advanced** tab of **Session Properties**, the connection will be attempted. The session window, shown below, has not been configured to automatically connect.



The 3270 session can then be started by selecting **Connect**, from the **Communication** pull-down menu.



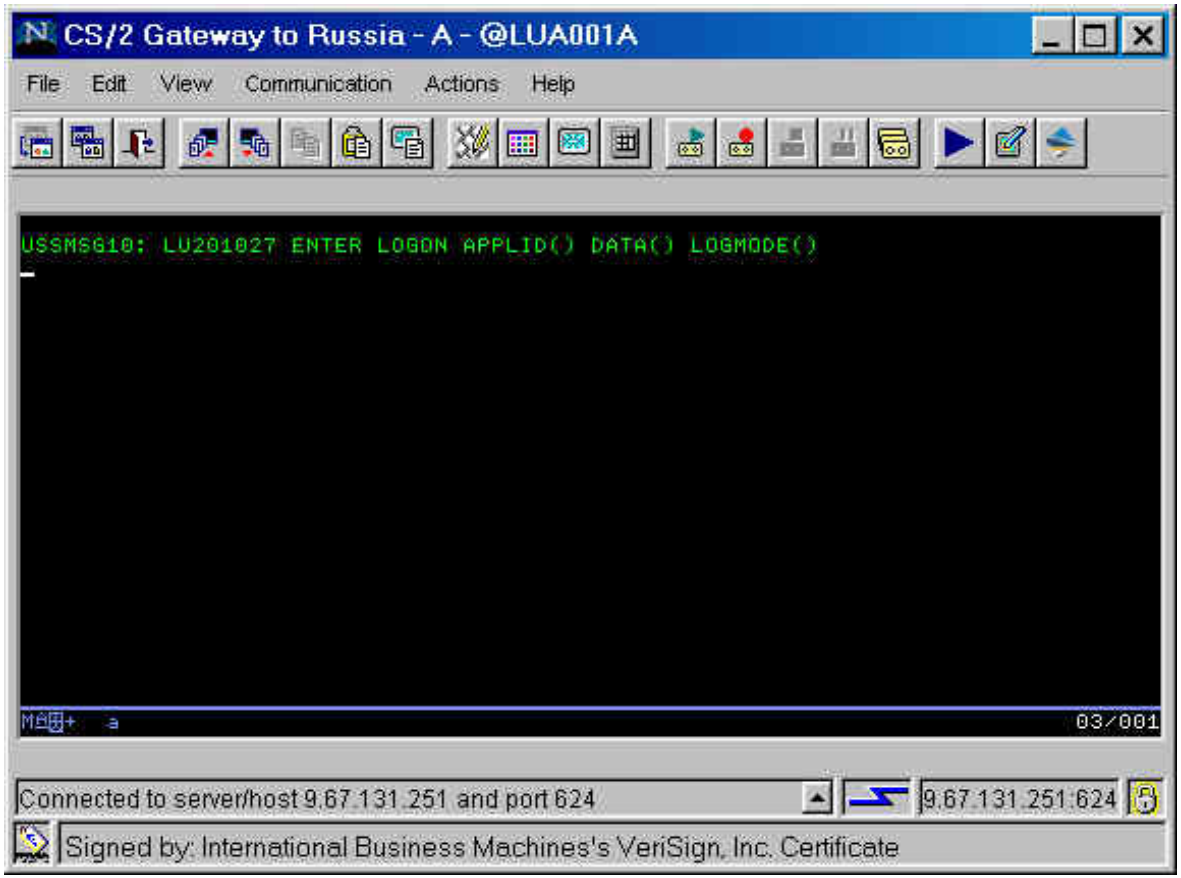
During the connection sequence, as part of the SSL negotiation, the TN3270 Server will send its certificate to the HOD client, and will request that the HOD client return its (client) certificate. This will start the following **Server Requesting Certificate** window for the HOD client.

Clicking on the **Details** button of the Server Requesting Certificate window will pop up a **Security Information** window, which will allow the HOD user to view the details of the TN3270 server certificate.

In order to continue with the establishment of the SSL connection to the TN3270 Server, the HOD user must supply the location of a valid client certificate, in P12 format, and the password for that P12 file.

At this point, it is possible to view the fields of the Client Certificate. This may be done by clicking on the **View Certificate** button of the Server Requesting Certificate window. Note: The certificate used here is for user51.

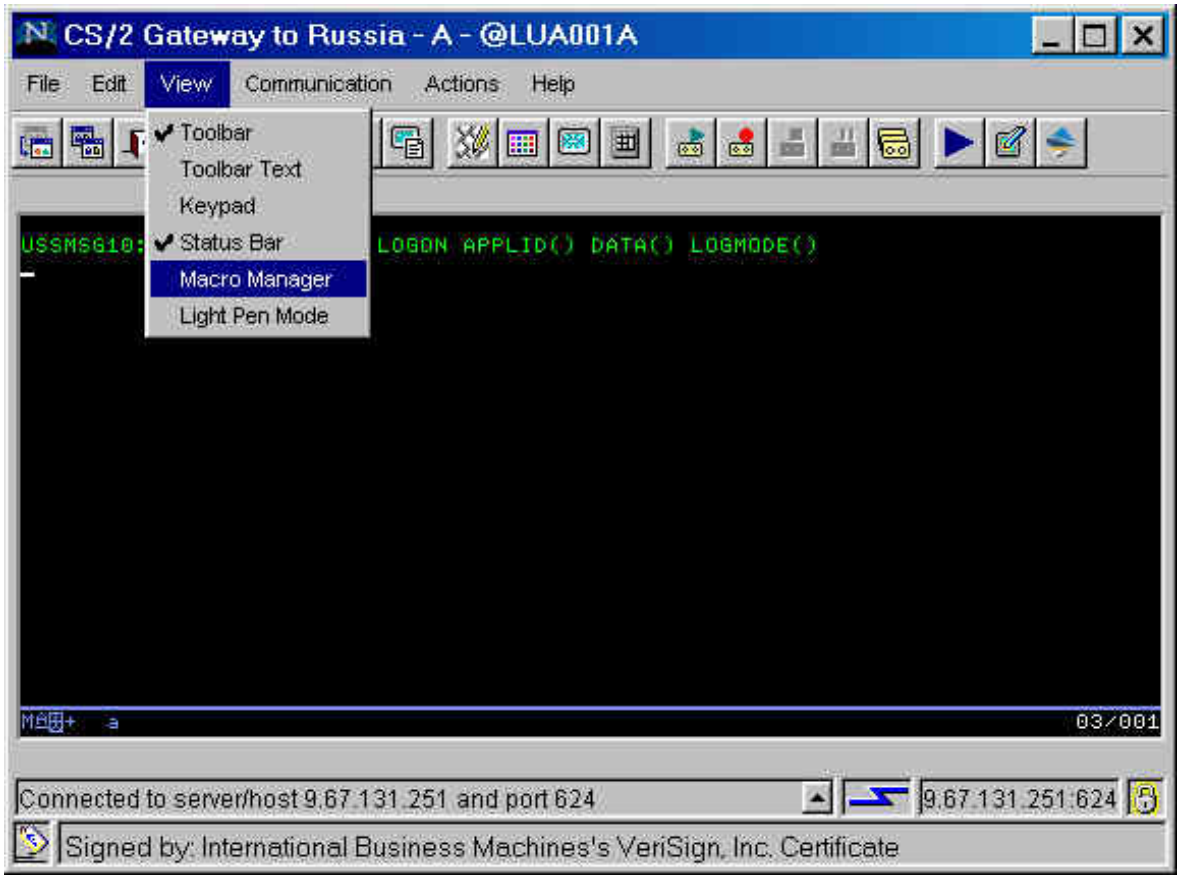
After clicking on the **OK** button to send the client certificate, the 3270 session will be established. The HOD client will sequence through several progress messages before the session is finally established. Once the session is established, a host USSMSG10, or other application logon message will be displayed within the session window.



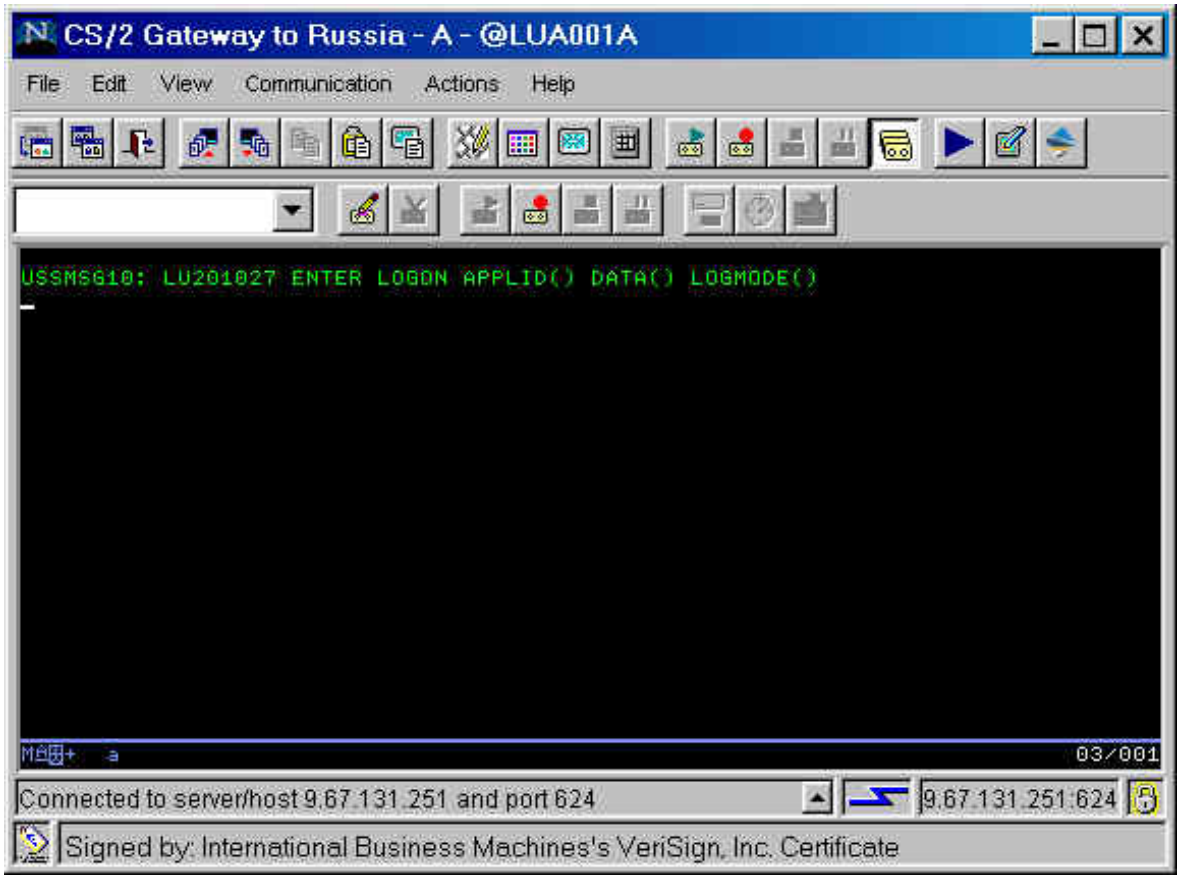
Return to Part 4: Using the Express Logon Feature
Return to Contents

4.2 Recording the ELF Logon Macro

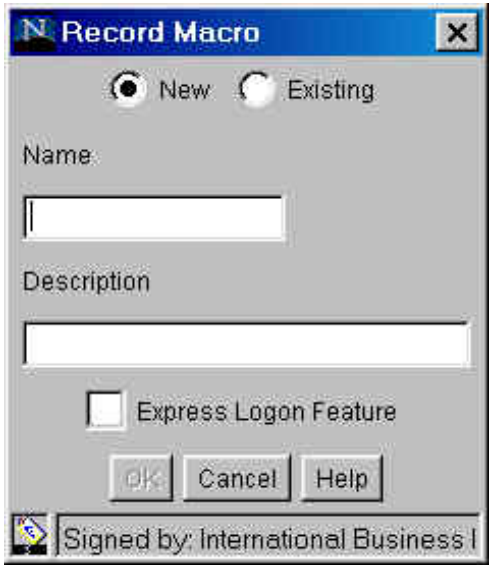
Once the 3270 session has been initially established, then the ELF macro may be recorded. The record process may be started by clicking on the **Record** button on the main toolbar, or the **Macro Manager** may be started. Macro Manager is started by selecting **Macro Manager** from the **View** pulldown.
Hint: To view the text for each icon on the toolbar, select **View-Toolbar Text** to turn this option on.



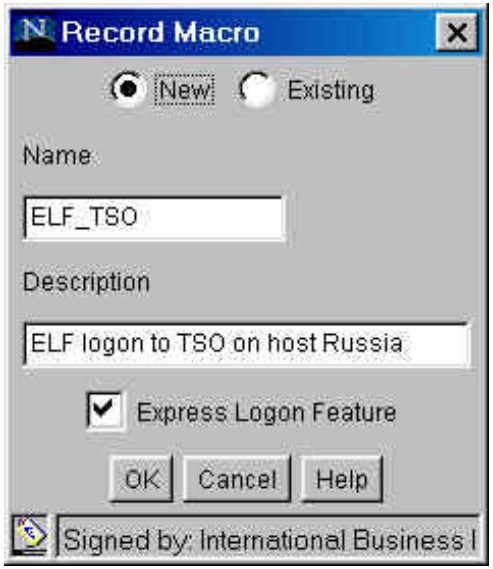
Once Macro Manager has been started, a new row of buttons will now be visible, just below the main toolbar.



Once the record button has been clicked, either from Macro Manager, or the main toolbar, then a Record Macro dialog window will appear.



Use this window to specify the macro Name and Description. The Express Logon Feature box must be checked to initiate the wizard to make this an ELF macro.



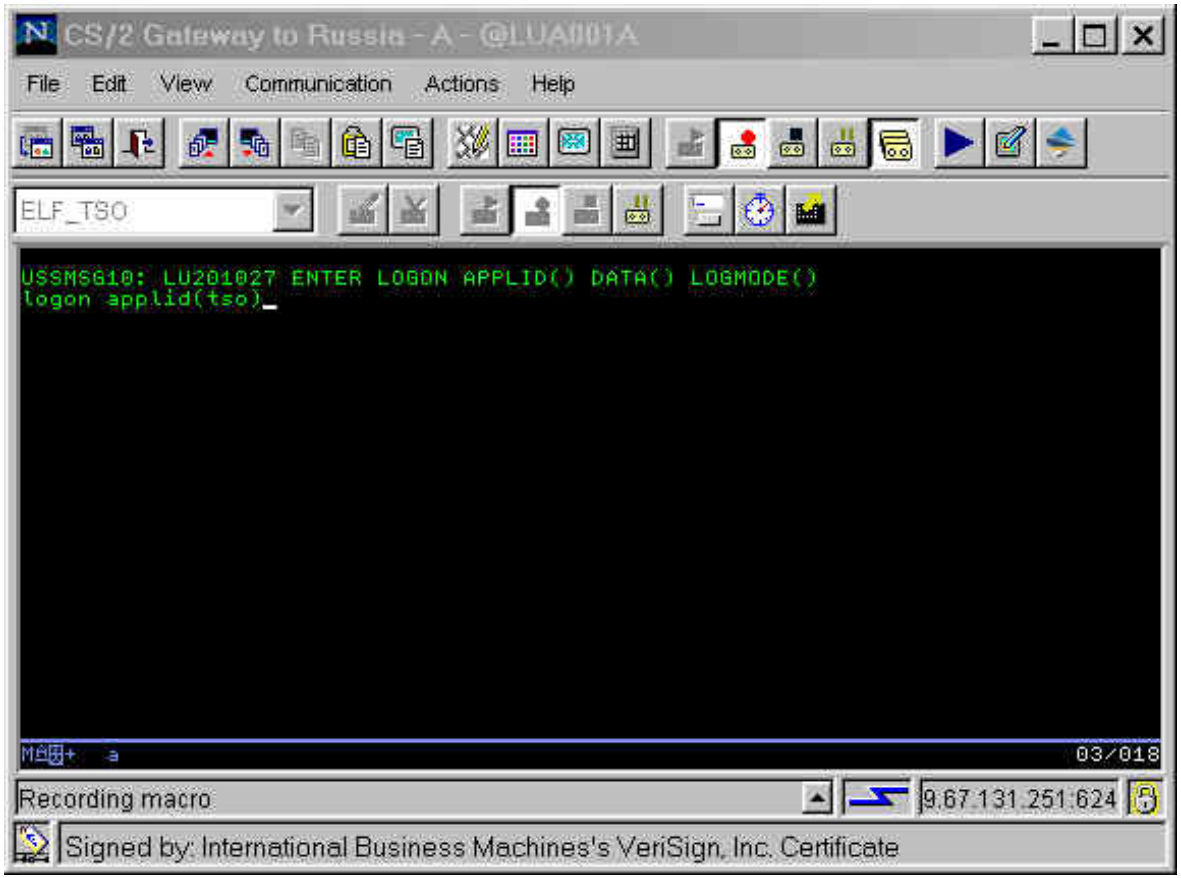
After clicking **OK** from the Record Macro window, an Express Logon Configuration Application ID window will appear. Use the Application ID which has been defined using RACF on the host to match the target application for the HOD client user (refer to section 2.1.6 Defining a Passticket Profile for each Application).

The following is configured to log on to TSO on our test host system.

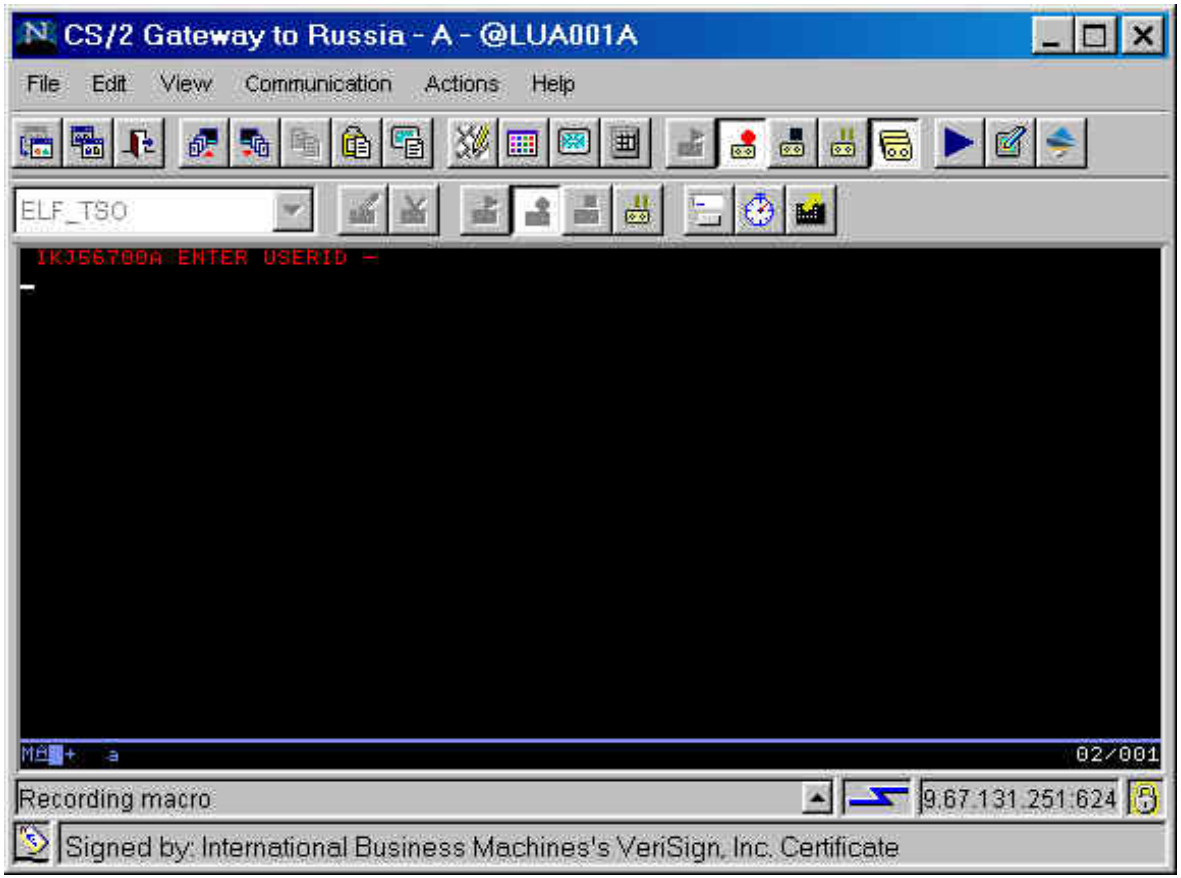
After clicking the **OK** button, the recording of the ELF macro will proceed. The next window, the Screen Criteria window, should not be clicked until the 3270 window contains information that matches any of the listed criteria, which is:

- Is an alternate start screen (refer to section 4.2.1 Recording an Alternate Start Screen for the ELF Logon Macro.)
- Contains a User ID field
- Contains a Password field

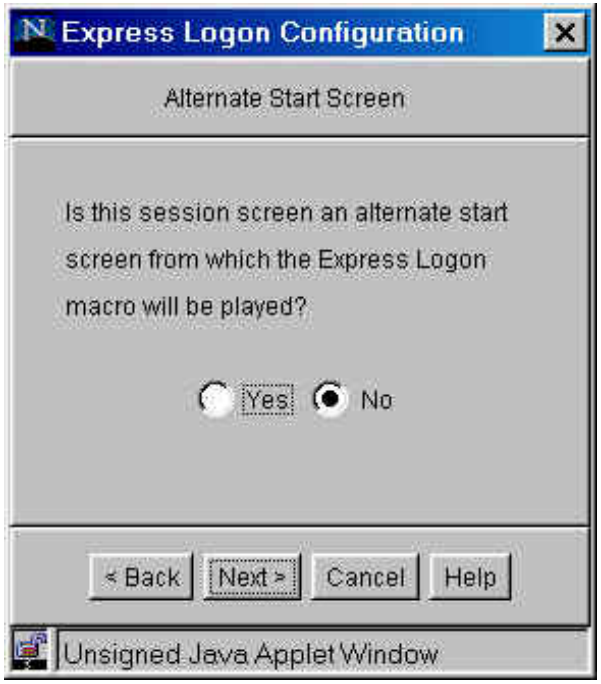
Leave that window open, and then make the HOD 3270 session the active window, and then type in an appropriate logon command and press the **Enter** key.



That will initiate a user ID prompt in the 3270 session window.

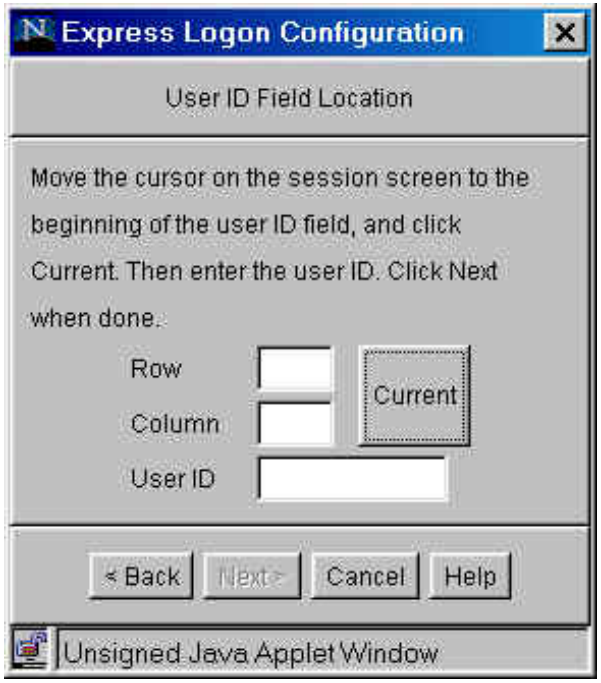


Since there is now a user ID prompt in the session window, it is now time to make the ELF screen criteria window the active window, and click on the **OK** button. This will pop up another ELF Configuration window, for Alternate Start Screen.

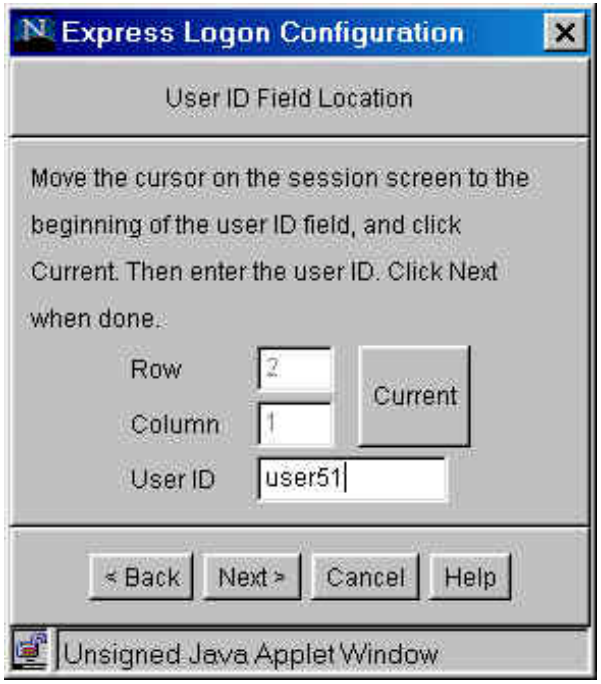


Since this is not an alternate start screen, select **No**, and then click the **Next >** button. This will pop up an ELF User ID Field dialog window. With the Yes radio button selected, click **Next >** to proceed. (Note: for instructions on recording a macro using an alternate start screen, refer to section 4.2.1 Recording an Alternate Start Screen for the ELF Logon Macro.)

The next ELF Configuration window will be the User ID Field Location window. Note: The cursor in the HOD 3270 session window should be positioned to the first character of the user ID input field. Clicking on the **Current** button will select the current curson position. After selecting the cursor position, type a valid user ID in the User ID box. This user ID must be valid to logon to this application. It will NOT be used for future ELF logons, which will instead, use the user ID that corresponds to the client certificate according to RACF supplied for the SSL connection.

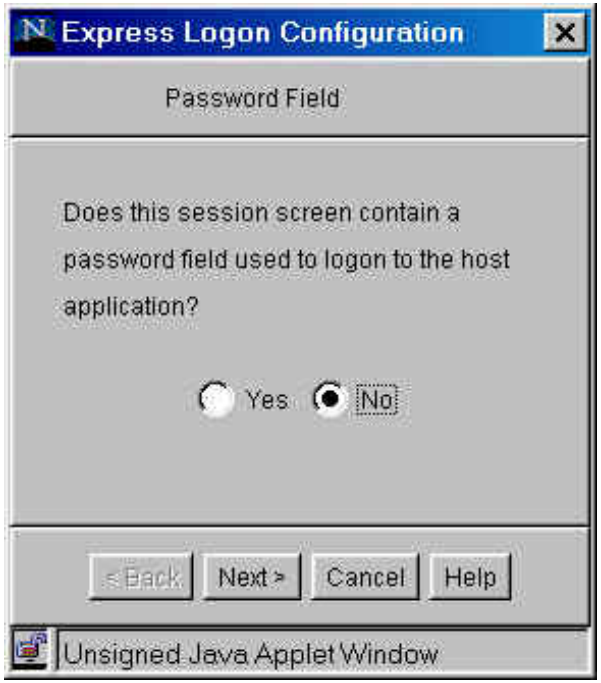


The following User ID Field Location window has been configured for the correct cursor location, and the User ID field has been typed in. Proceed by clicking on the **Next >** button. Note: the user ID for this session is user51.



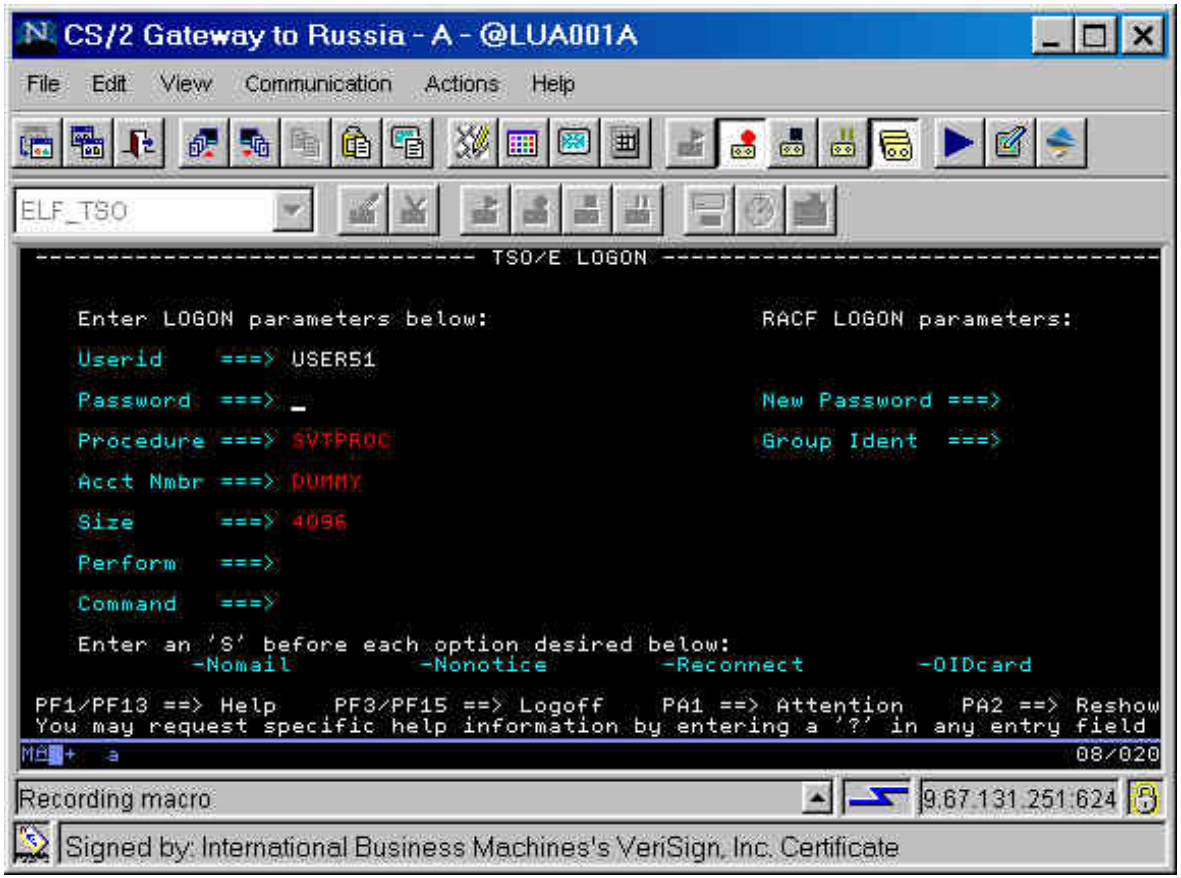
The ELF Password Field window will now be presented. If the 3270 session window had a field to provide the User's password, then Yes should have been selected.

However, the 3270 window does not have a password field. Therefore, click on the **Next >** button, with the No radio button selected.

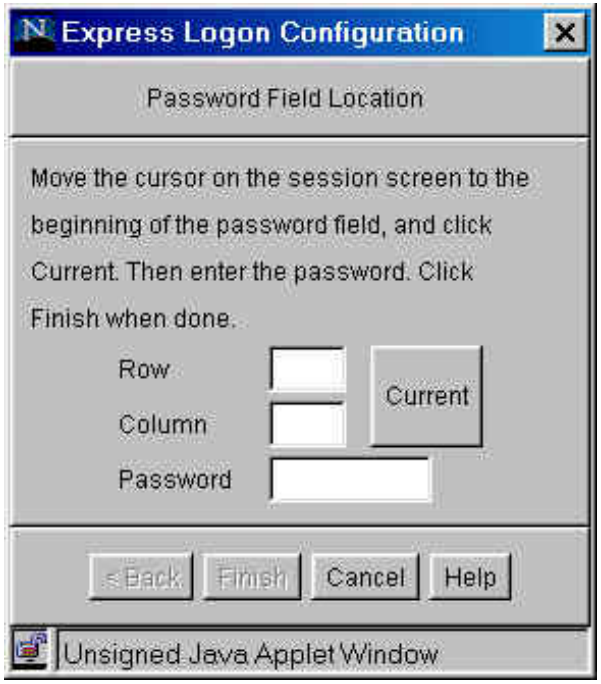


That will pop up an ELF Screen Criteria window. As with the previous Screen Criteria window, leave this window open, and switch back to the HOD 3270 session window, and continue with the logon sequence until prompted to supply a password.

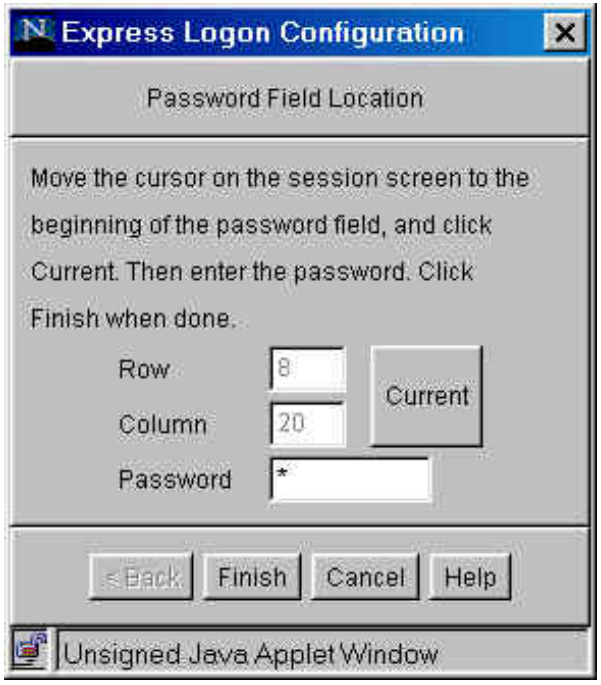
The 3270 TSO/E logon screen now has a Password field. Now it is appropriate to click the **OK** button of the ELF Screen Criteria window.



The ELF Password Field Location window will now be presented. As with the previous User ID Field Location window, ensure that the 3270 cursor is located at the position for the first character of the Password input field. Click the **Current** button of the Password Field Location window to select this (3270 window) cursor position. Type in the password (which will not display).

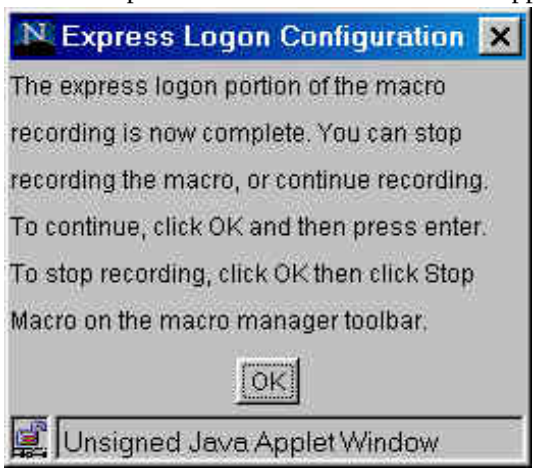


This Password Field Location window has been completed. Proceed by clicking on the **Finish** button.

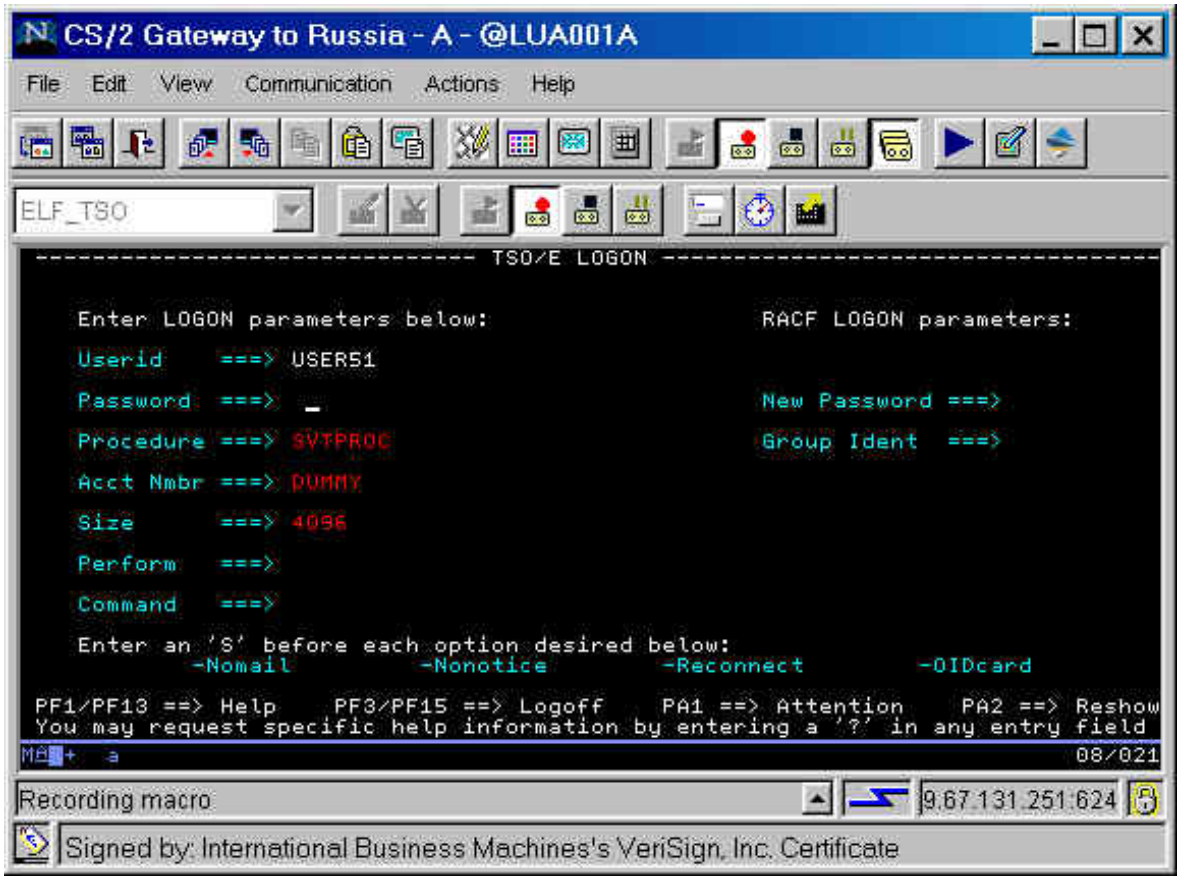


An ELF Configuration window will appear to inform you that the ELF logon sequence has been completed. At this time it is possible to continue recording the macro to

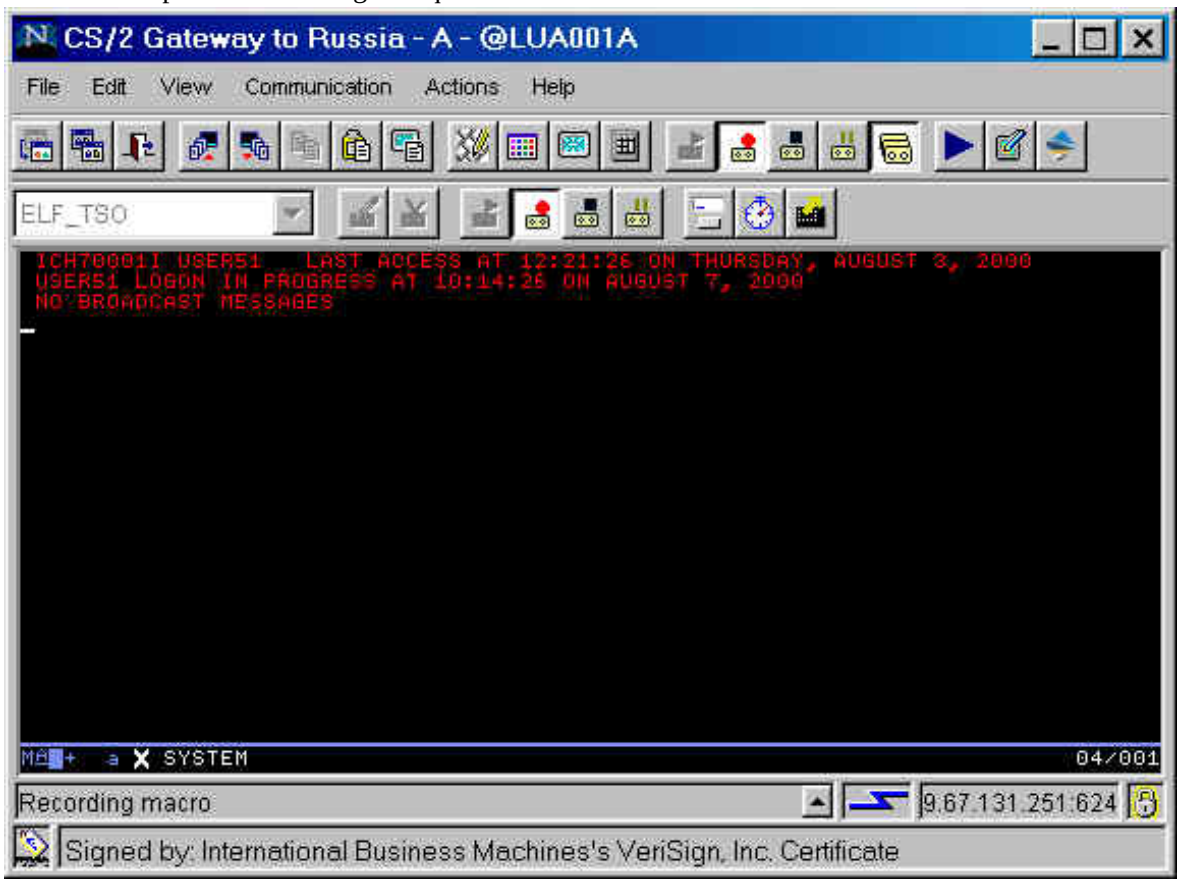
include steps which interact with the user's application. It is not required that you continue recording the macro. To close this window, click on the **OK** button.



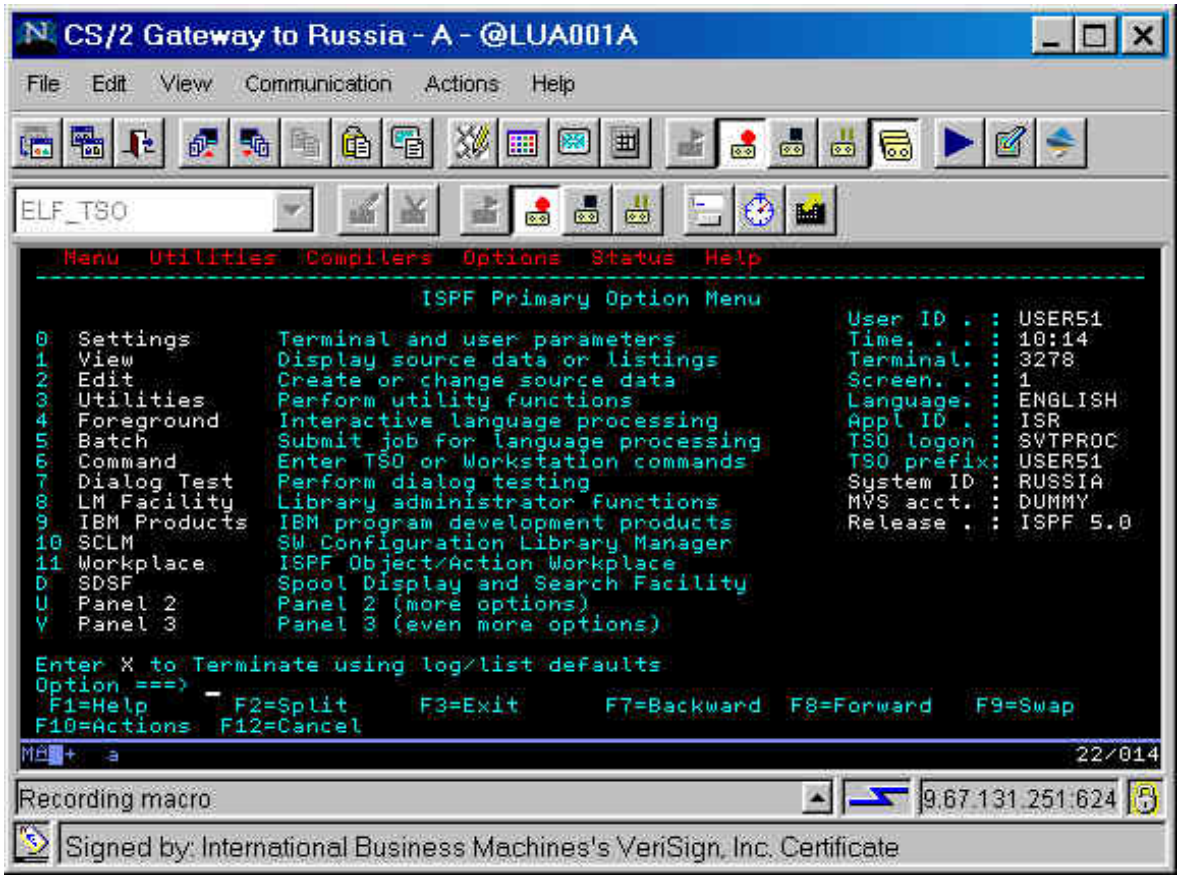
After clicking the **OK** button for the ELF window, make the HOD 3270 session window the active window, and press the **Enter** key (as instructed by the previous ELF window).



This will complete the 3270 logon sequence.



Since the target host application is TSO, an ISPF primary window appears.
Note - the macro record button is still depressed - this signifies that the macro is still being recorded. Click on the **Stop** button whenever you wish to stop recording the macro.



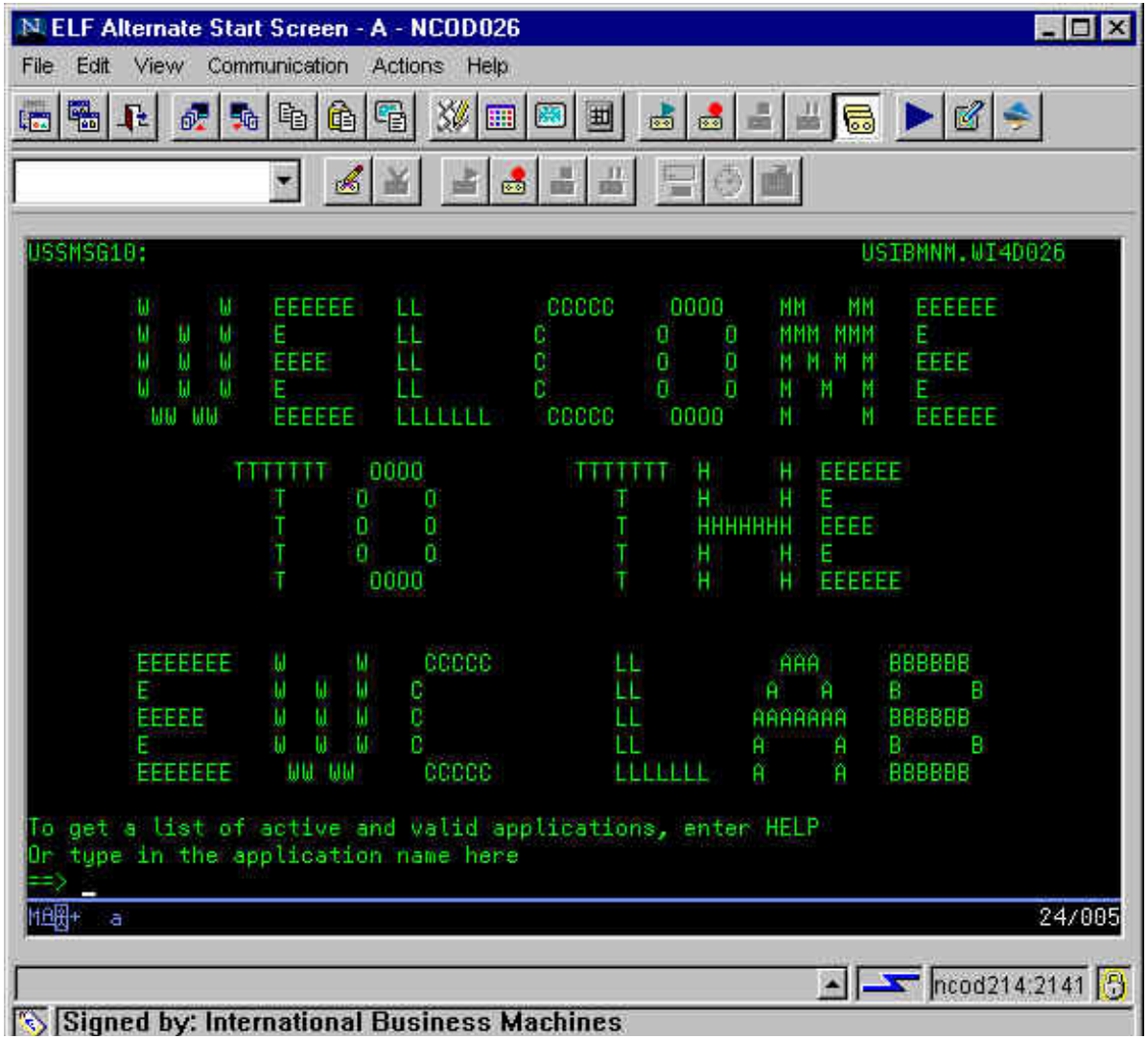
Once the recording has been stopped, an Auto-Start dialog window will appear which will allow you to autostart this macro for the HOD 3270 session. If Yes is selected, the macro will begin playing once the session window has been activated. Since this is an ELF macro, it will attempt to log on to the host application, once the session activates (connects). This Auto-Start value may be changed later from HOD session properties, on the Advanced tab.

4.2.1 Recording an Alternate Start Screen for the ELF Logon Macro

A start screen is the first screen from which the macro is played. In addition, one or more subsequent screens can be designated as an alternate start screen. You should identify alternate start screens during the recording process so that the macro can be played successfully from any of those screens. For example, when the 3270 Host On-Demand session is started, you might see a USSMSG10 screen. On that screen, you enter the host application name (e.g., TSO or MVS) and then go to the application's logon screen. The application's logon screen could be identified as an alternate start screen. This allows you to play the macro from either the start screen (USSMSG10) or the alternate start screen (application's logon screen). Note that you cannot designate an alternate start screen once the user ID has been recorded.

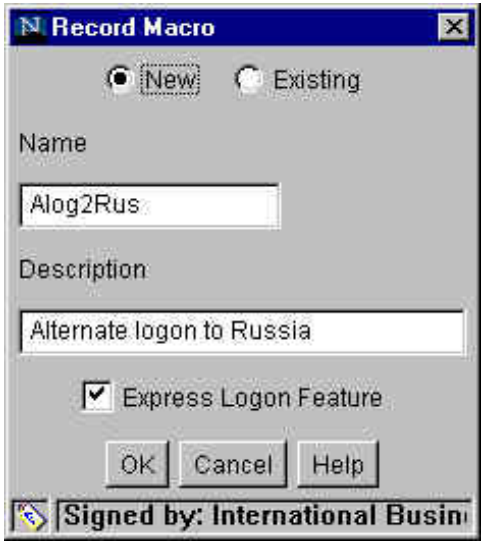
The following steps will show the recording process for designating an alternate start screen.

The HOD 3270 session window displays a USSMSG10 screen, for the logon to our test lab network.



Start the recording of the ELF macro by clicking on any of the 'record' buttons that are available.

The initial Record Macro dialog window will appear. Complete all of the fields to name, describe, and identify the ELF macro.

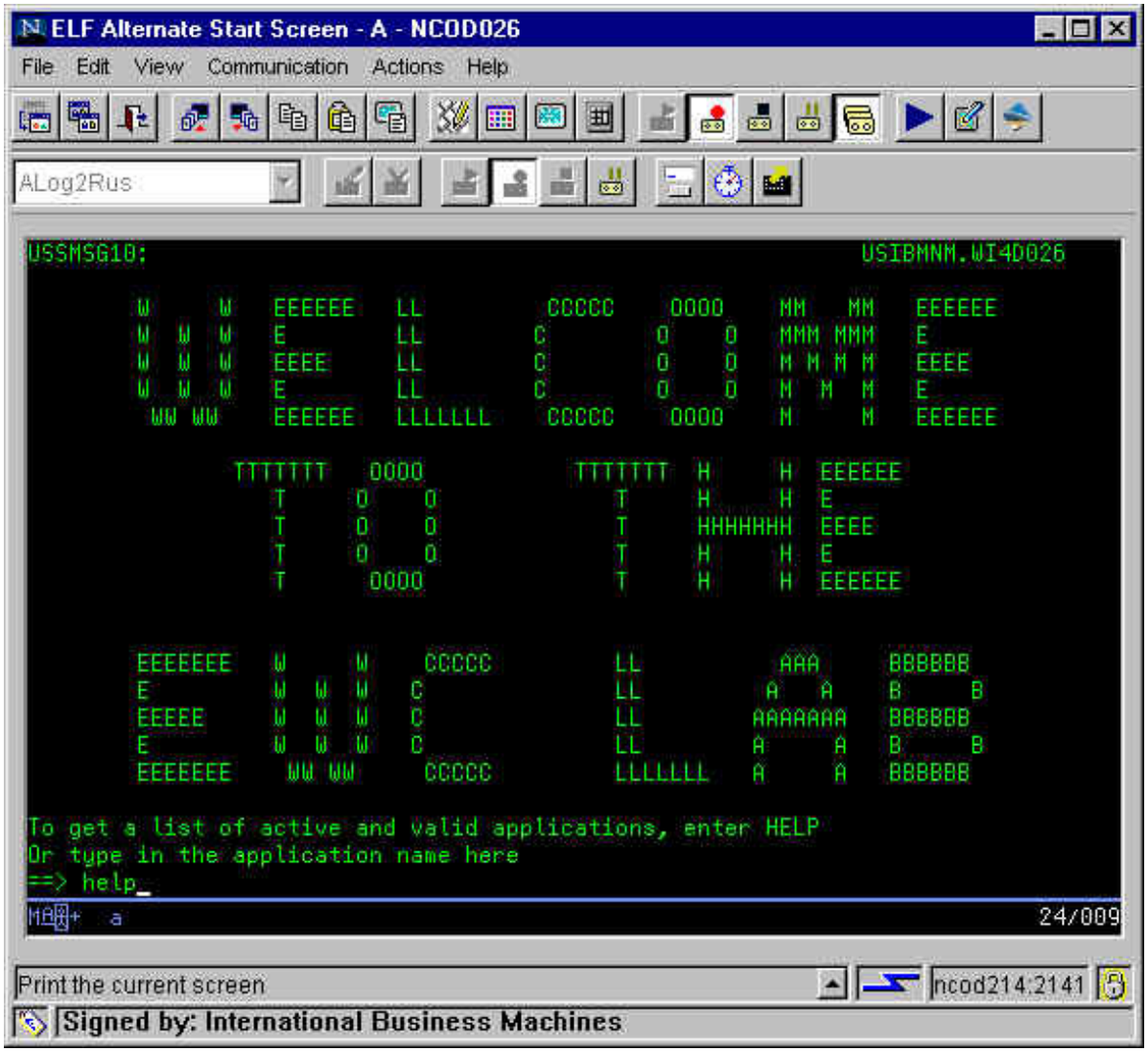


Click the **OK** button to continue with the ELF macro.

This will bring up the Express Logon Configuration**Application ID** dialog window.

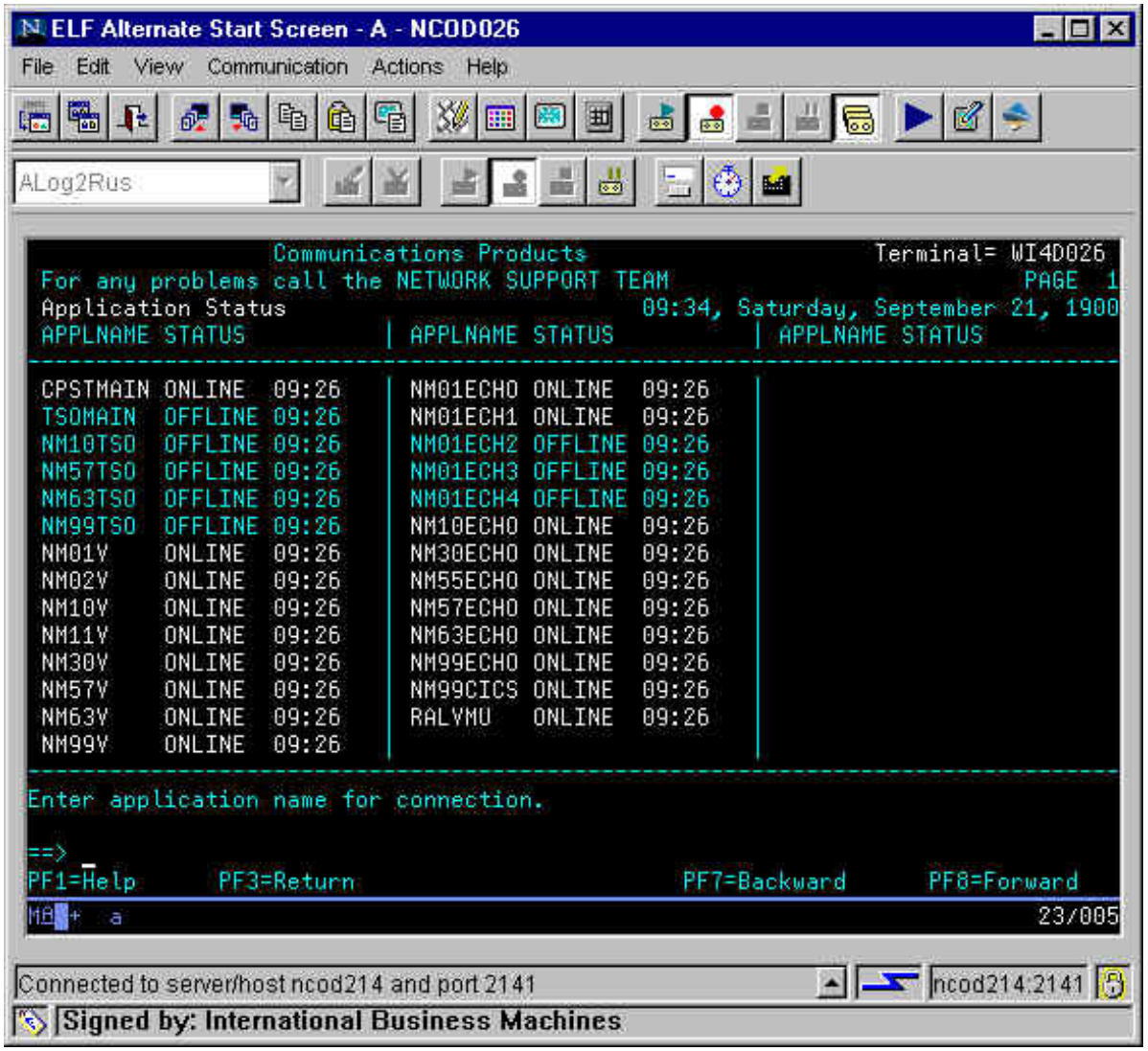
Enter the name of the host application to be logged on to and click on the **OK** button.

Proceed with the logon sequence to reach the Alternate Start Screen.



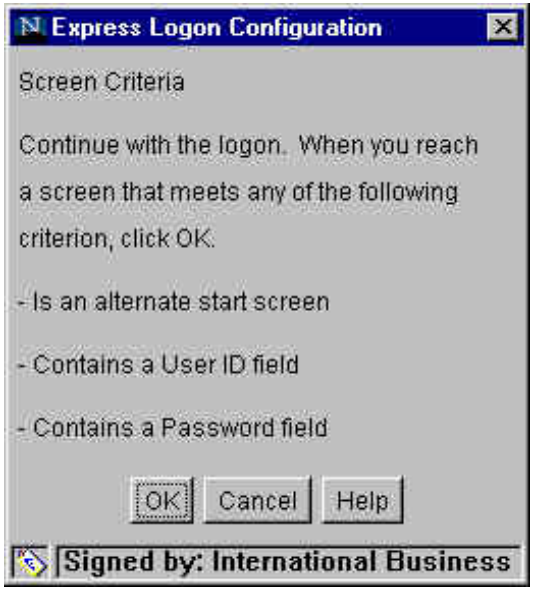
For this example, you type in **help**, and then press the Enter key. This will proceed to an alternate start screen.

This is the alternate start screen for our system, which lists additional target host applications and their status.



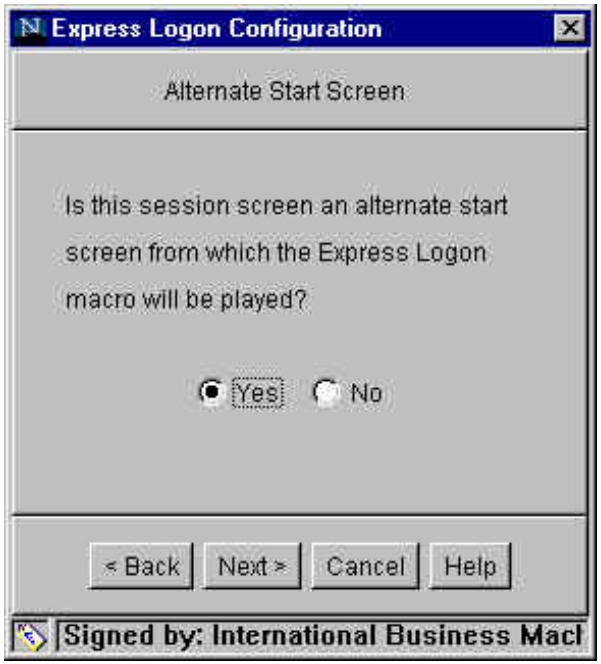
This alternate start screen will meet one of the Express Logon Configuration Screen Criteria.

Express Logon Configuration**Screen Criteria** window.



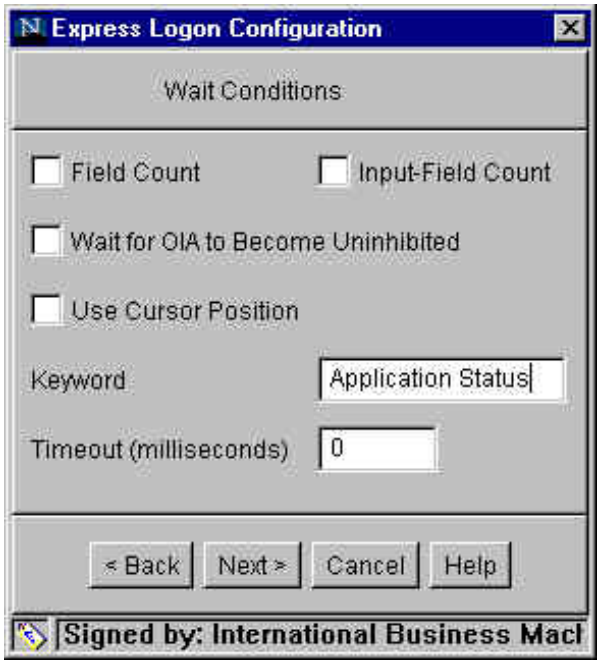
Click on the **OK** button, since the host session window is at an alternate start screen.

This will initiate a new Express Logon Configuration window, which contains the **Alternate Start Screen** dialog. Select the **Yes** radio button, instead of the (default) **No** button.



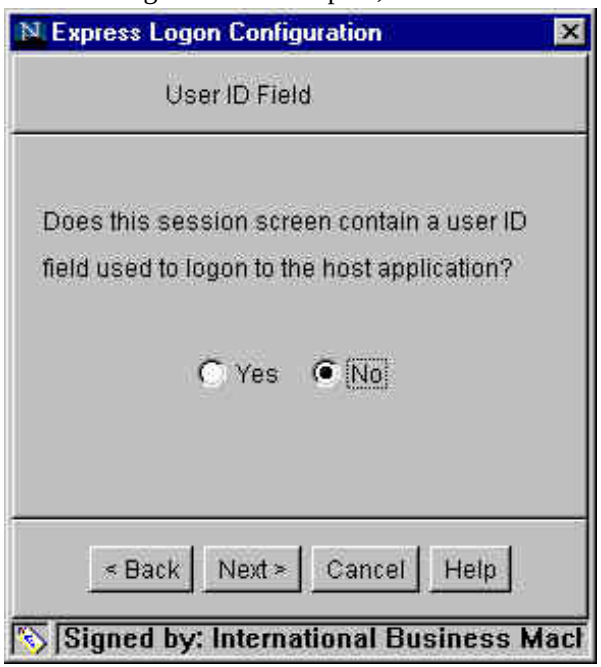
Click on the **Next>** button to proceed to the next panel.

This will bring up an Express Logon Configuration **Wait Conditions** window. This window is used by the macro to identify when the correct host alternate start screen is being displayed.



Complete the information in the window to correctly identify the alternate start screen. Click on the **Next>** button to proceed to the next panel.

A new dialog window will apear, which will ask if a **User ID Field** is present on the host screen. At this time, for our example, the value is **No.**

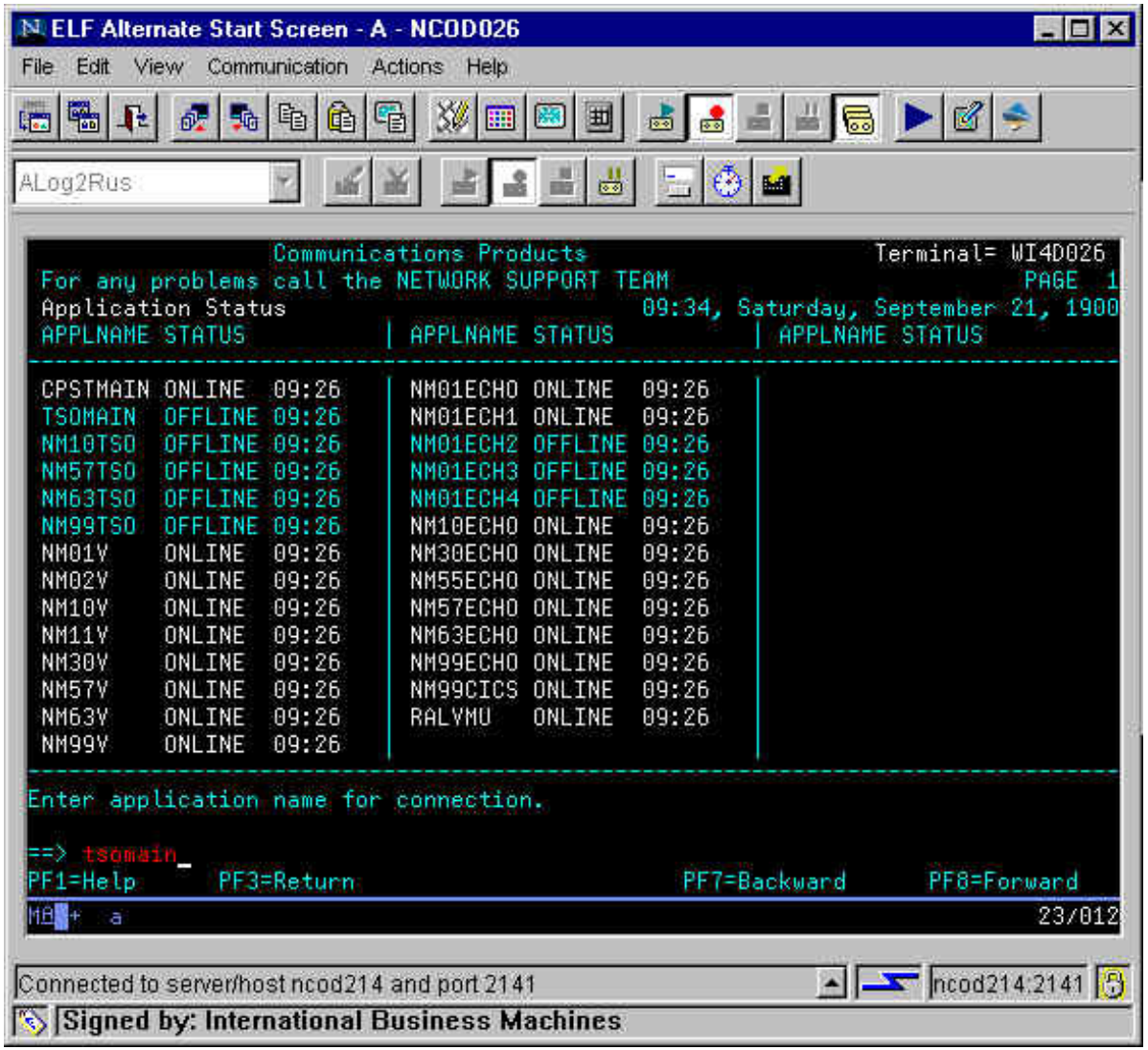


Ensure the **No** radio button is selected, and click the **Next>** button to proceed to the next panel.

This will return to the Express Logon Configuration **Screen Criteria** window.

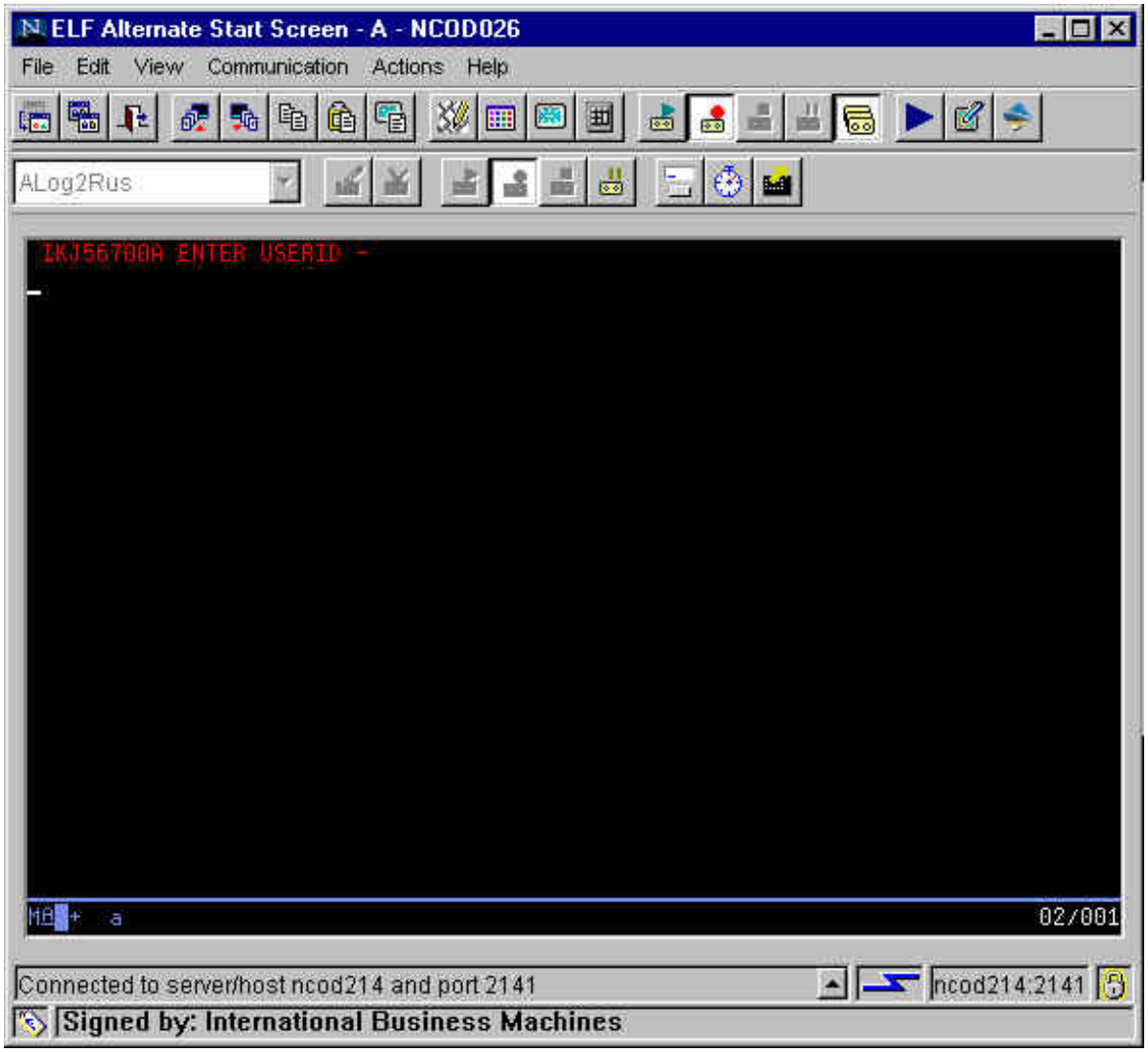
Leave this window open, and continue with recording the logon sequence, until one of the listed screen criteria is reached. When that happens, click on the **OK** button.

Make the HOD 3270 session window the active window. This window will still display the alternate start screen.



Continue with the alternate logon sequence. For our example, you type in the **APPLNAME**, which is **tsomain**, and then press the enter key.

This will initiate the actual logon to the target host application which is tsomain (TSO).

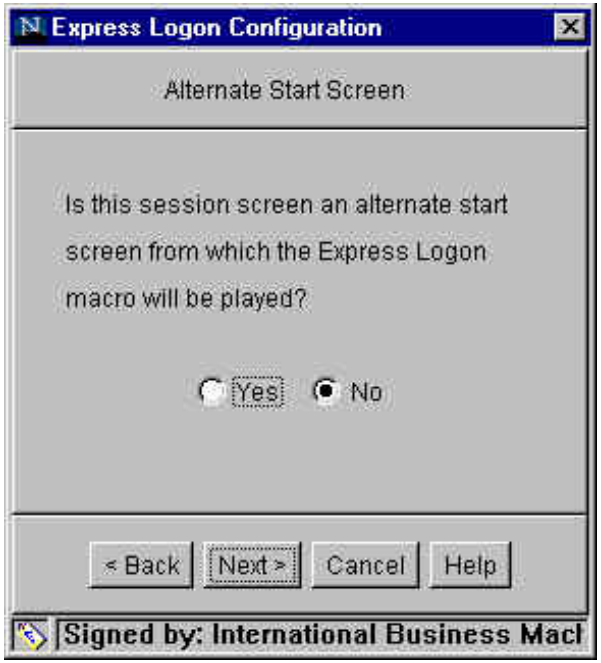


The tsomain logon will then prompt the user for a User ID. This prompt for a User ID then matches one of the **Screen Criteria**, for the ELF macro.

Select (make active) the Express Logon Configuration **Screen Criteria** window.

Click the **OK** button, since a **Screen Criteria** has been met.

This will return to the **Alternate Start Screen** dialog.

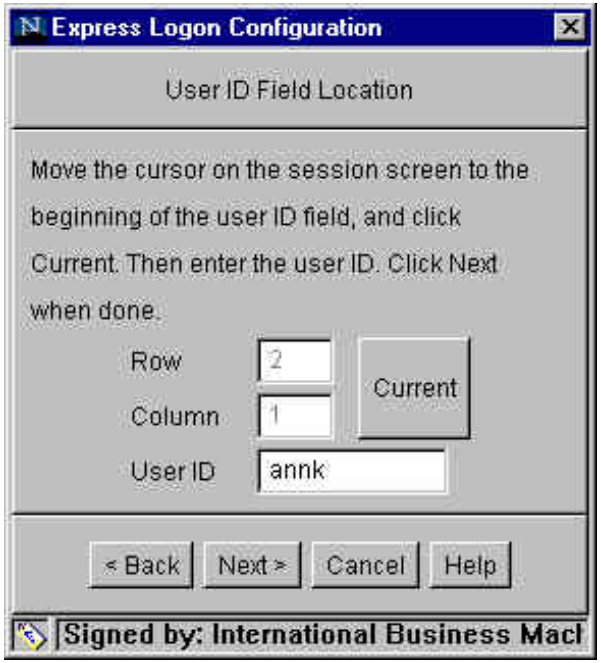


Since this is not an **Alternate Start Screen**, leave the **No** radio button selected, and continue by clicking on the **Next>** button.

This will bring up an Express Logon Configuration **User ID Field** Window. Use this window to identify the host screen as currently prompting for a **User ID**.

To continue, select the **Yes** radio button and then click on the **Next>** button.

This will bring up the Express Logon Configuration**User ID Field Location** dialog window. Use this window to identify the location, within the HOD 3270 session window, of the input field for the host application User ID. Identify the location of the **User ID** input field, which can usually be done by clicking on the **Current** button. Type in the **User ID** value and click on the **Next>** button to continue the logon sequence.



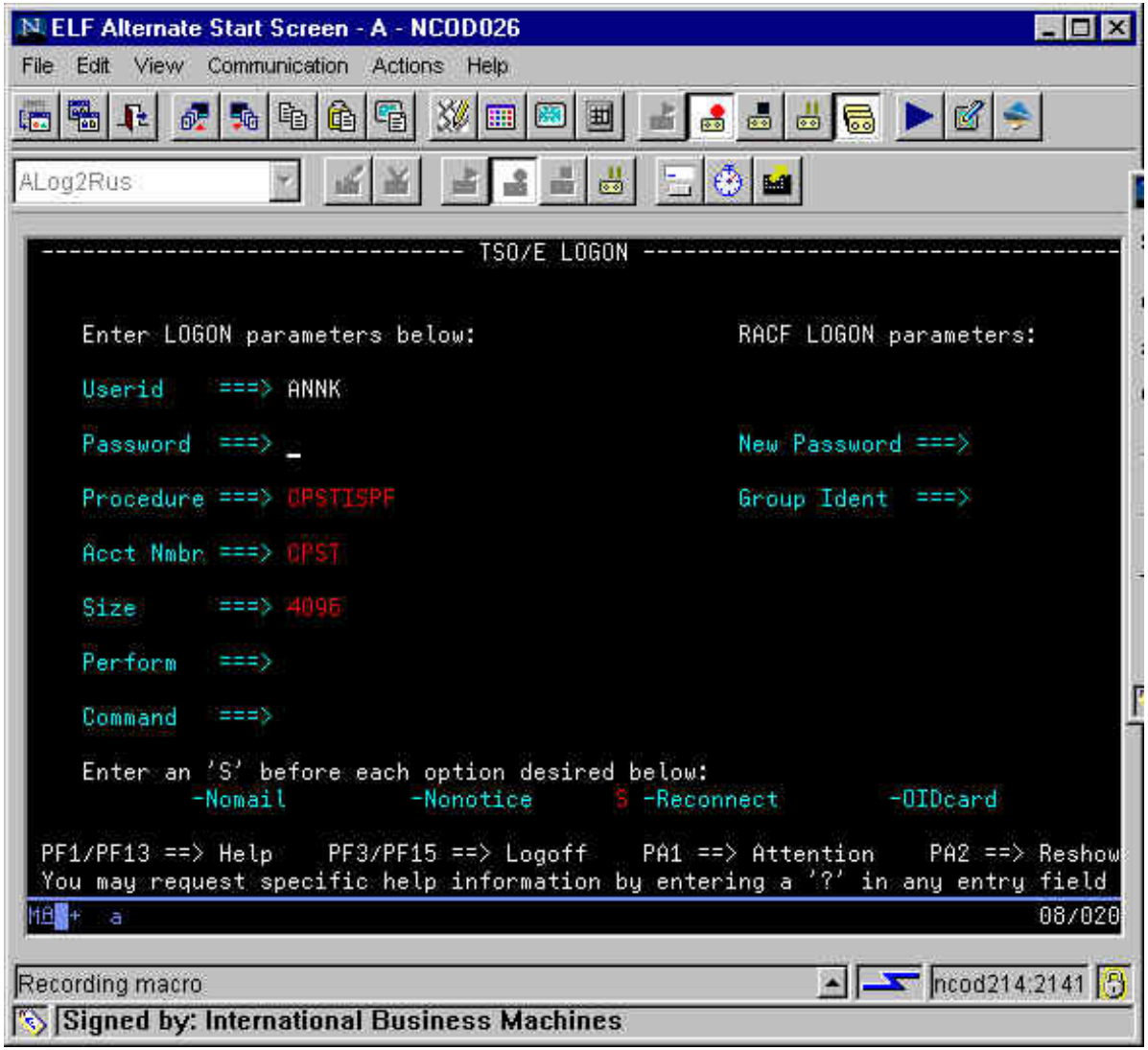
The Express Logon Configuration **Password Field** window will be the next dialog window. Select **Yes** or **No** depending upon whether the current 3270 session window contains a field to input the password for the host application.

Since our application does not currently have a password field, proceed by selecting the **No** radio button and then clicking on the **Next>** button.

This will bring up the Express Logon Configuration **Screen Criteria** window again. Notice, this time, that the only screen criteria left is '**- contains a Password field**' and the other two screen criteria are now greyed out.

Don't do anything with this window until the last screen criteria is met.

Switch back to the 3270 session window and continue the logon sequence until the Password input field is displayed for the host application.

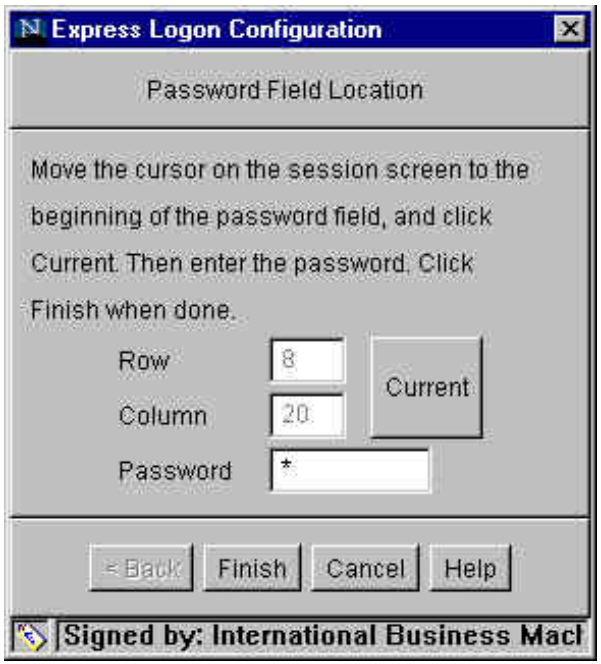


Since the Password input field is now displayed, switch back to the ELF Screen Criteria window.

Express Logon Configuration **Screen Criteria** window.

Click the **OK** button since the final Screen Criteria, the Password Field, has now been matched.

Select the screen location for the position of the first character of the password input field. The easiest way to do this is to position the 3270 cursor to that location and then click the **Current** button in the ELF **Password Field Location** window.



After identifying the location for the password input field, type the appropriate password into the **Password** field of the **Password Field Location** window. Click on the **Finish** button to complete the recording process for the ELF (Alternate Start Screen) macro.

The last Express Logon Configuration window states that the recording of the ELF macro has been completed.

Click the **OK** button to complete the recording of the ELF macro. The macro will now be saved.

Return to Part 4: Using the Express Logon Feature
Return to Contents

4.3 Exporting HOD ELF Sessions and HOD Macros

The following sections describe the steps necessary to export HOD ELF sessions and macros. Exporting is the method used to copy an existing session or macro for use by another user.

4.3.1 Exporting HOD Sessions

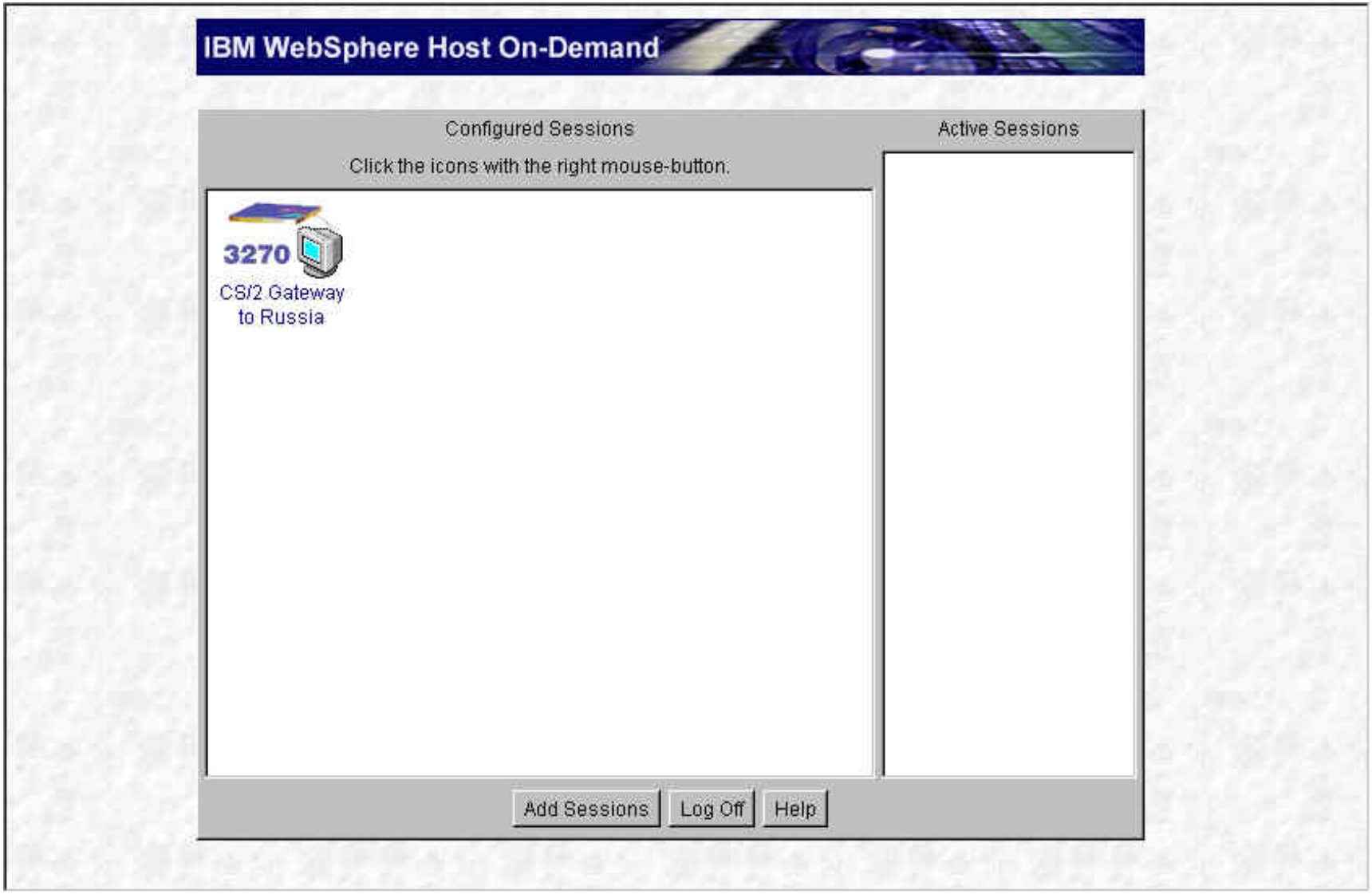
Both HOD sessions and macros that have been defined for ELF can be shared with other users. This can be done without having to redefine each session and macro. If the HOD session can be defined at the group level (by the HOD Administrator), then all of the members of that group will have that session defined for them. That is the simplest way to share a session that has been set up for ELF. Adding a new user to that group will allow the new user access to all of the sessions that have been defined for that group.

Another option is to Export the session. Either a HOD user (client) or HOD Administrator may initiate the export session function.
HOD User Exporting a Session.
HOD Administrator Exporting a Session.

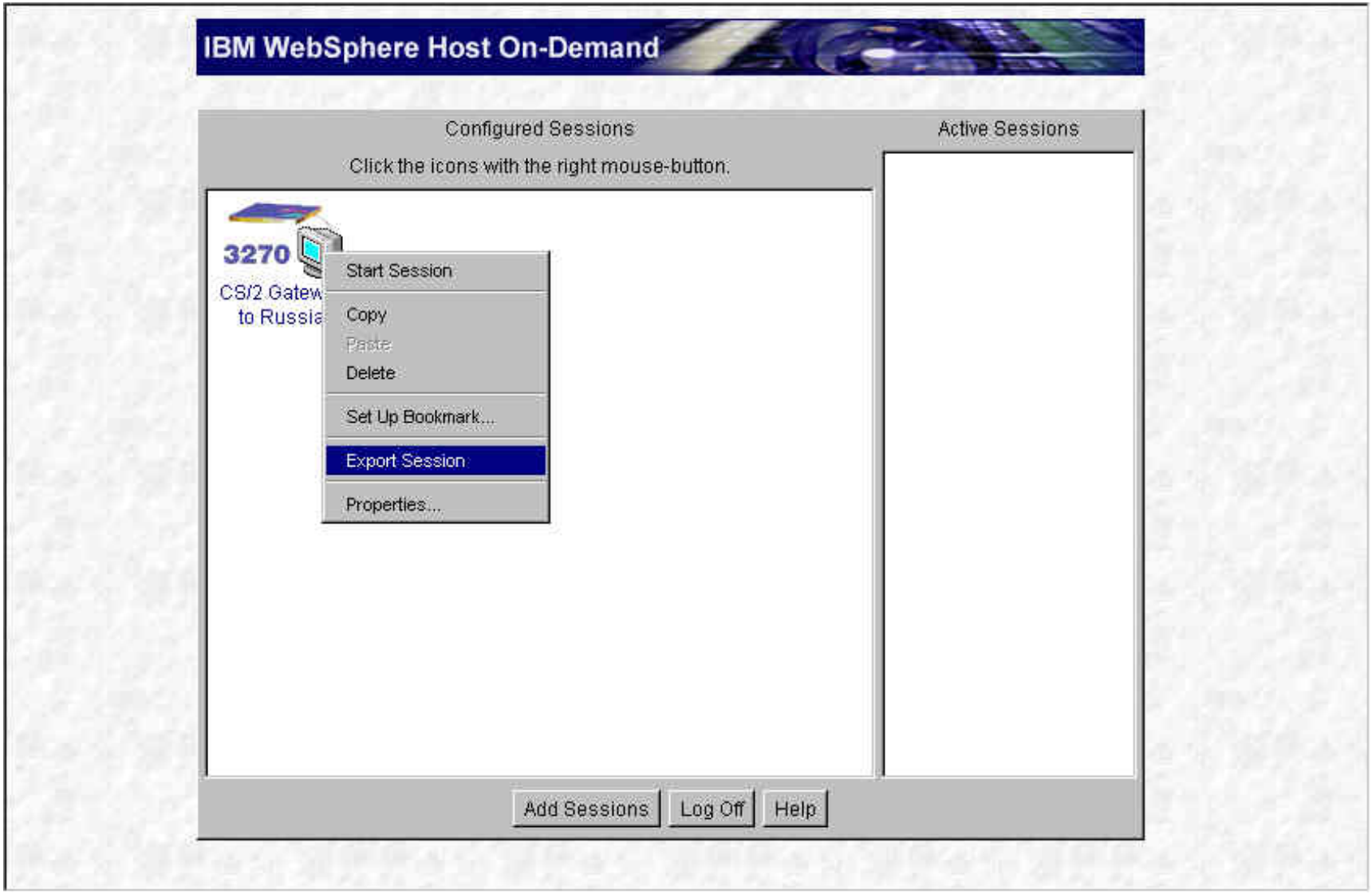
After the first initial steps, the Export Session procedure is the same for either a HOD user, or HOD Administrator.
HOD Export Session Dialog

4.3.1.1 HOD User Exporting a Session

The HOD (client) user may export sessions. The only requirement to export a session is that it exists in the **HOD Configured Sessions** window.



The first step to export a session is to **right click on the defined session icon**. This will pop up a window which has the Export Session option. Highlighting the **Export Session** selection will bring up the export session dialog window.

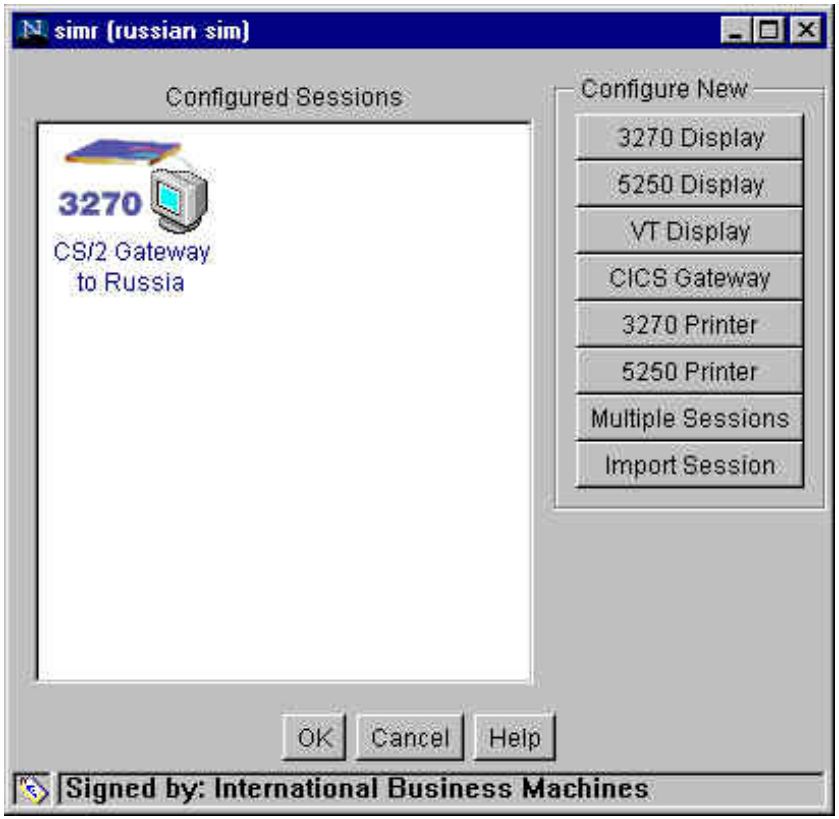


Now proceed to 4.3.1.3 HOD Export Session Dialog to complete the export of the session.

4.3.1.2 HOD Administrator Exporting a Session

The HOD Administrator may export any session that has been defined, at either the user, or group level. Following is an example of exporting a user session. **Left click on the All Users section**, on the left side of the HOD Admin panel, and all of the defined HOD users will be displayed on the right side of the panel. Then, **right click on the user** for whom you wish to export the session. Select **Sessions** from that window.

This will bring up the **Configured Sessions** window for the selected HOD user. This is similar to the Configured Sessions window that would be displayed to a HOD user (client).



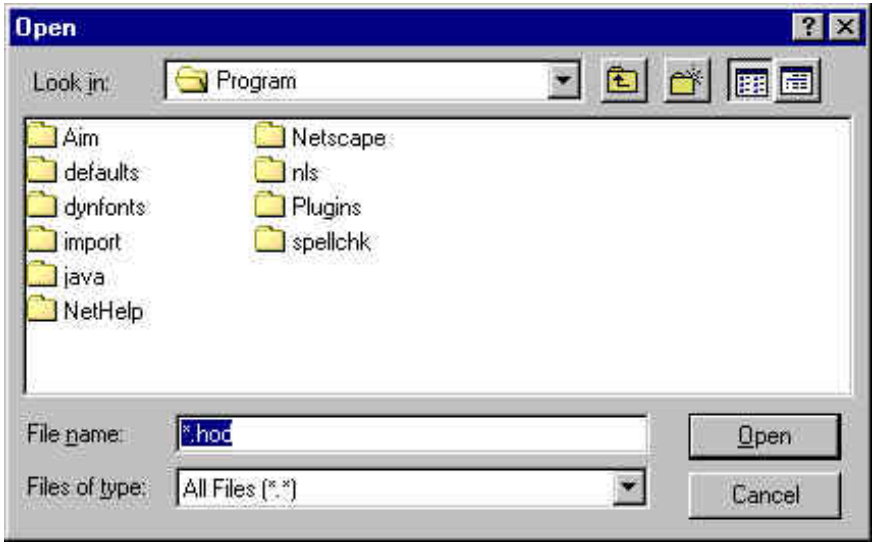
Right Clicking on the defined session icon will pop up a window that will have a selection for **Export Session.**

Now proceed to [4.3.1.3 HOD Export Session Dialog](#) to complete the export of the session.

4.3.1.3 HOD Export Session Dialog

Once the selection has been made, either by a HOD user or HOD Administrator, the export session dialog is brought up. The **Export Session** window appears as follows, and allows both the session-file name and path to be specified. Click on the Browse button to use Windows dialogs to select the pathname and to supply the file name.

Specifying the **session path and file name** follows standard Windows dialog windows.



Specify the **file name.**

Once the session and path have been determined, click on the **OK** button to save the exported session.

At this point, the session has been copied and saved. It can be transferred to another machine, if necessary, for the import process described later.

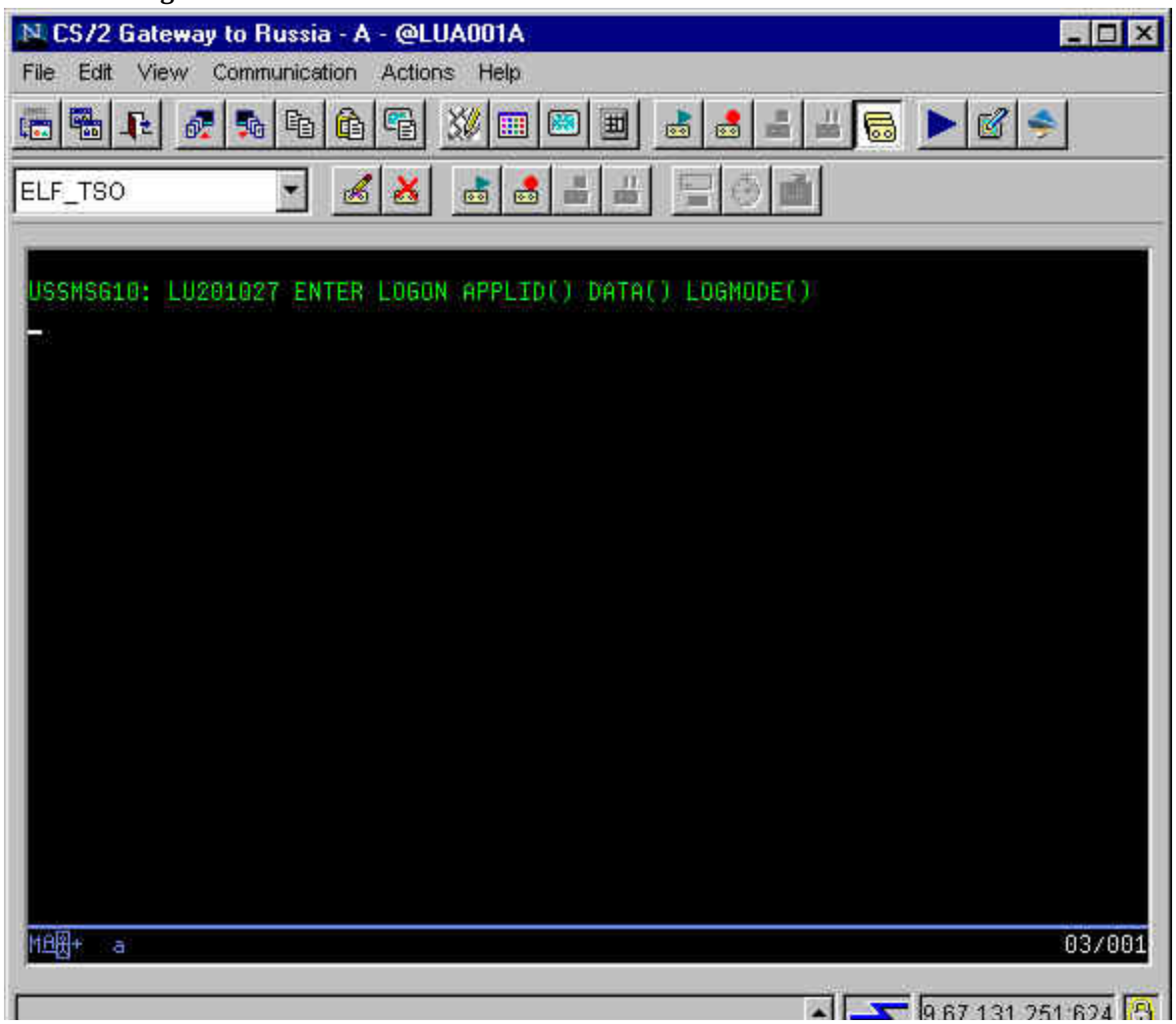
Return to Part 4: Using the Express Logon Feature
Return to Contents

4.3.2 Exporting HOD Macros

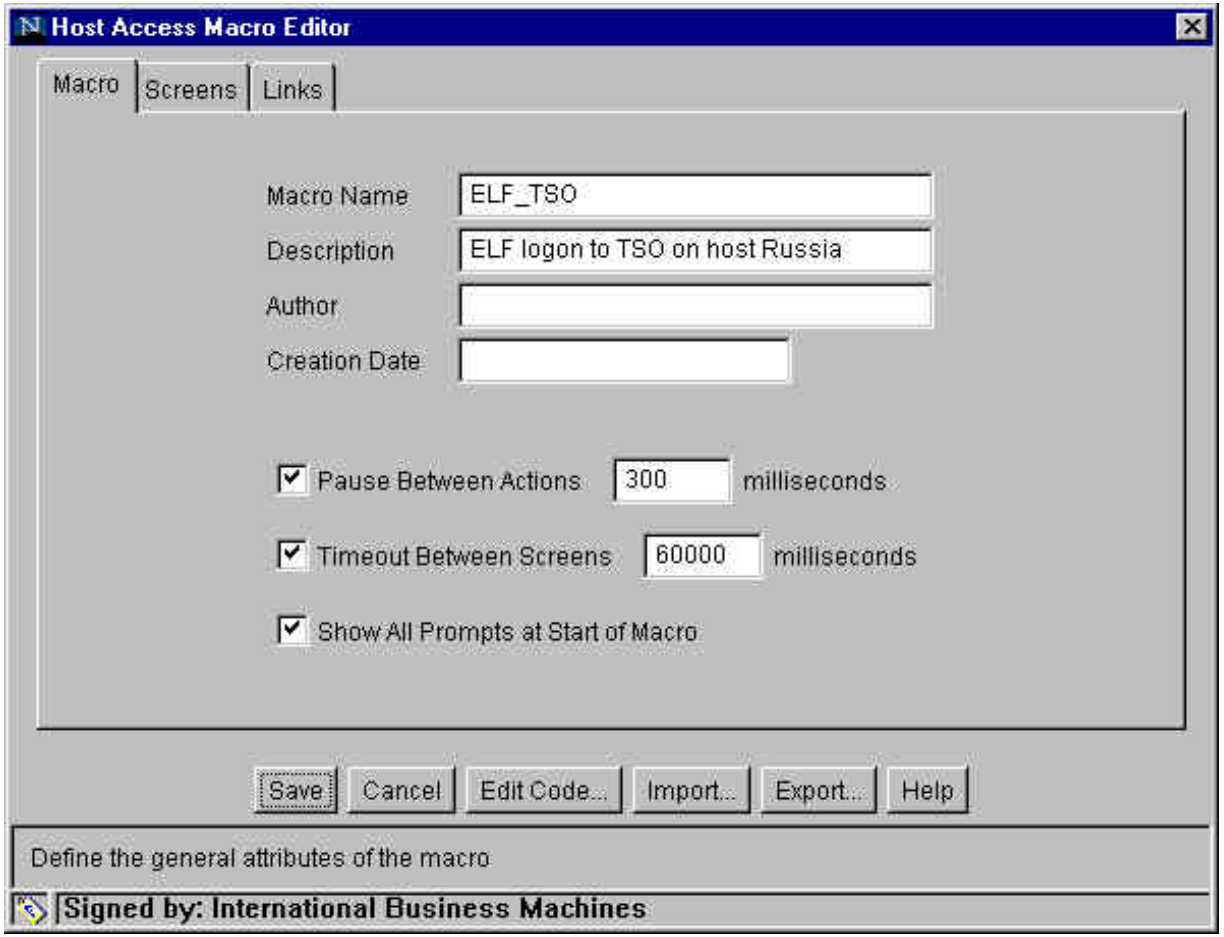
Exporting an ELF macro must be done from Macro Manager. Therefore, this is a step which can only be done by the HOD user, and not the HOD Administrator. Following are instructions on how to export a HOD ELF macro:

In order to export an ELF macro, the session (which was used to record the macro) must be started. Macro Manager, which is the line of macro buttons underneath the main toolbar, must also be started. If **Macro Manager** is not displayed, it may be activated from the View pulldown on the main menu bar.

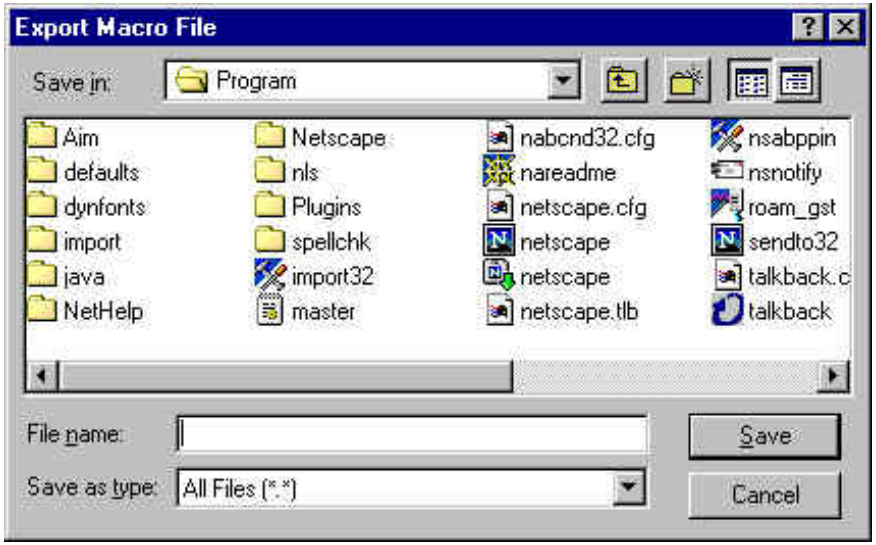
Macro Manager for active 3270 Session:



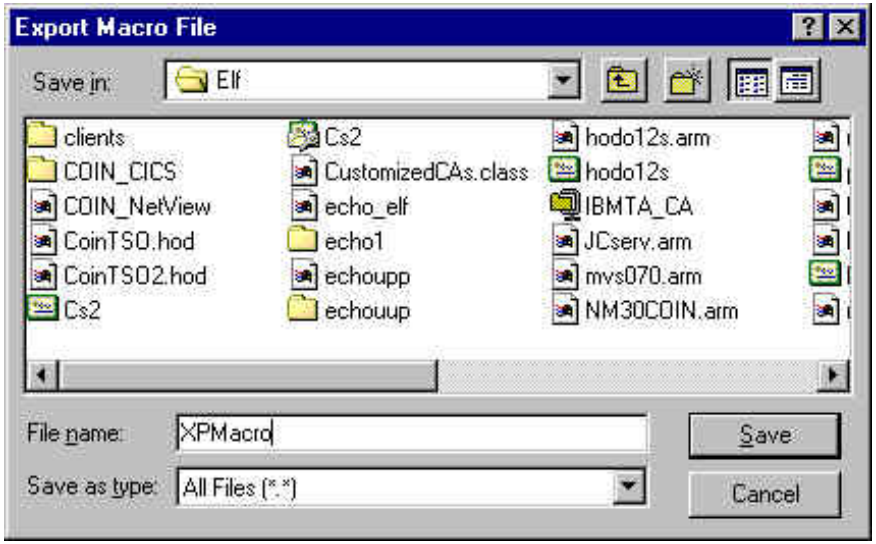
Macros may be exported from the Macro Editor. Macro Editor is started by right clicking on the edit icon, which is the first icon from the left, for Macro Manager (next to the window that contains the macro name.) This will bring up the Macro Editor.



The selected macro (to be edited) may then be exported by clicking on the **Export...** button. This will bring up the Windows dialog to specify the path and file name for the Export Macro File. Specify the **Path.**



Specify the **Macro File name** and Click the **Save** button to complete the Export of the HOD ELF macro.



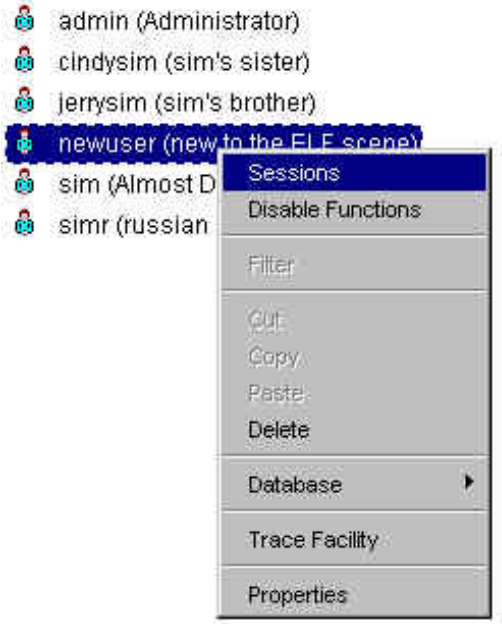
Return to Part 4: Using the Express Logon Feature
Return to Contents

4.4 Importing HOD ELF Sessions and HOD Macros

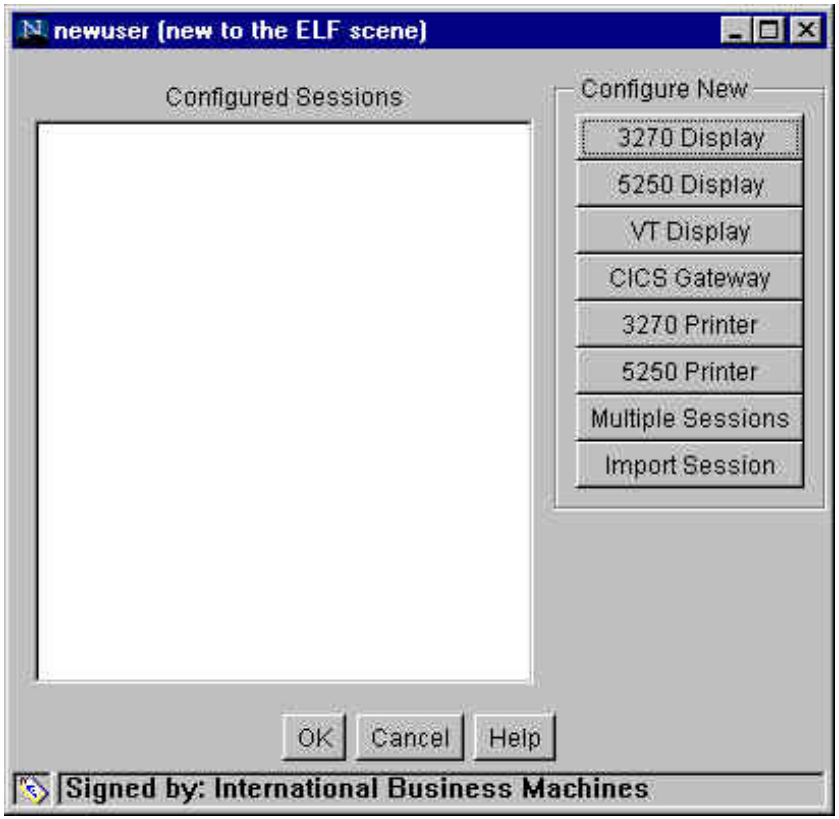
4.4.1 Importing HOD Sessions

If the session cannot be shared at the group level, then it must be imported. This is a task which is done by the HOD Administrator.

To import a HOD session for a user, you must be logged on as the HOD Administrator (HODAdmin.html). Select the user for whom you wish to add the session, and **right click**. This will open a window which contains the sessions option. Select the sessions option to bring up the dialog to import the session.



The **Configured Sessions window** is empty as this user inherits no sessions from the group level, and no sessions have yet to be defined. Notice the Import Session button at the bottom.

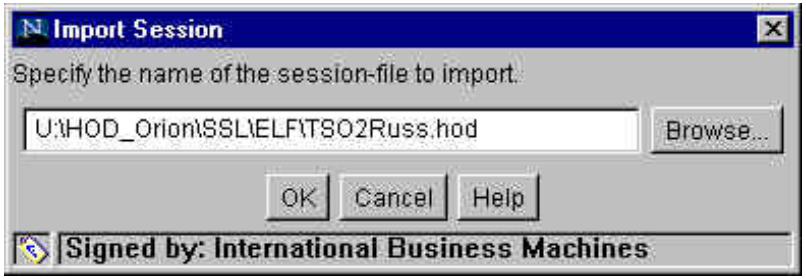


Left Click on the Import Session button, to activate the **Import Session** dialog window.

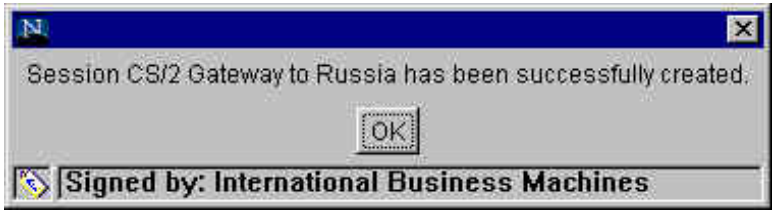
Continue the dialog to specify the **path to the directory** that contains the session to be imported.

Select the **file name** containing the session to be imported.

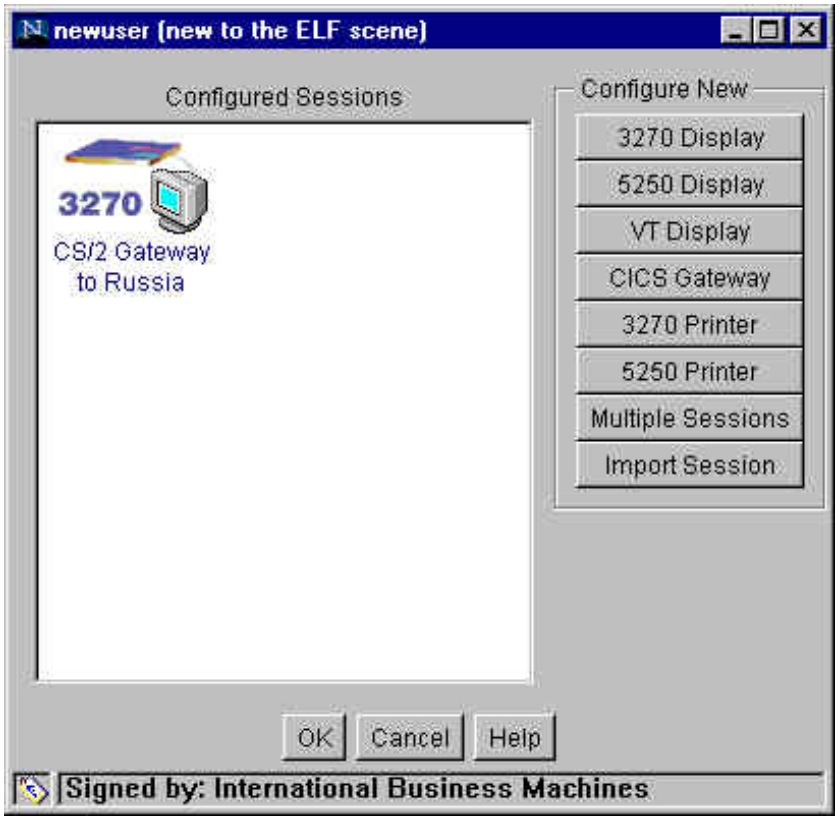
Return to the initial **Import Session** dialog window. Now the path and file name for the session to be imported are displayed in the window.



Click the OK button to complete importing the session. A window will appear confirming the import of the session.



The imported session will now appear in the **Configured Sessions** window.



The user "newuser" will now have access to this session icon from his HOD Configured Sessions window.

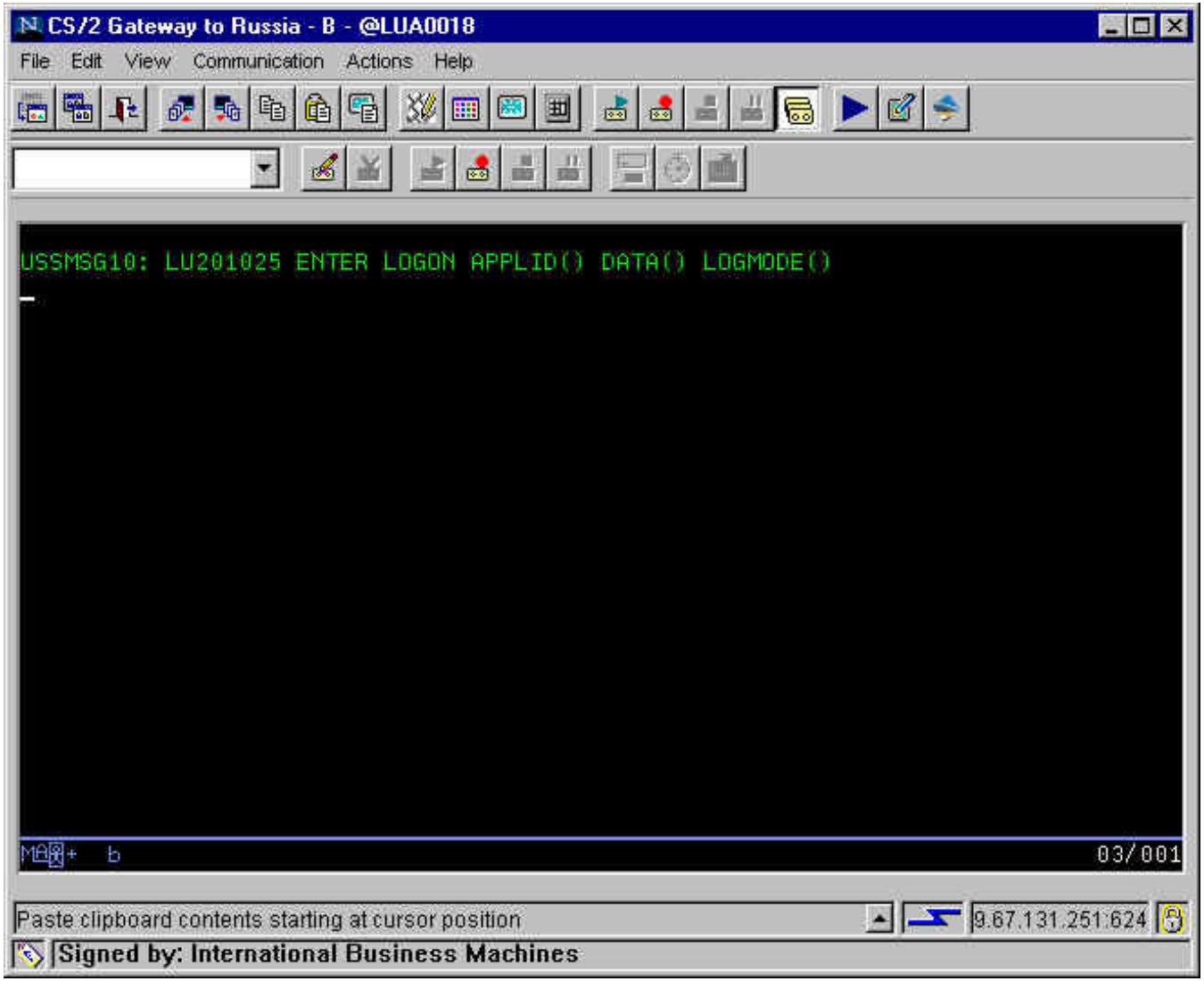
Return to Part 4: Using the Express Logon Feature
Return to Contents

4.4.2 Importing HOD Macros

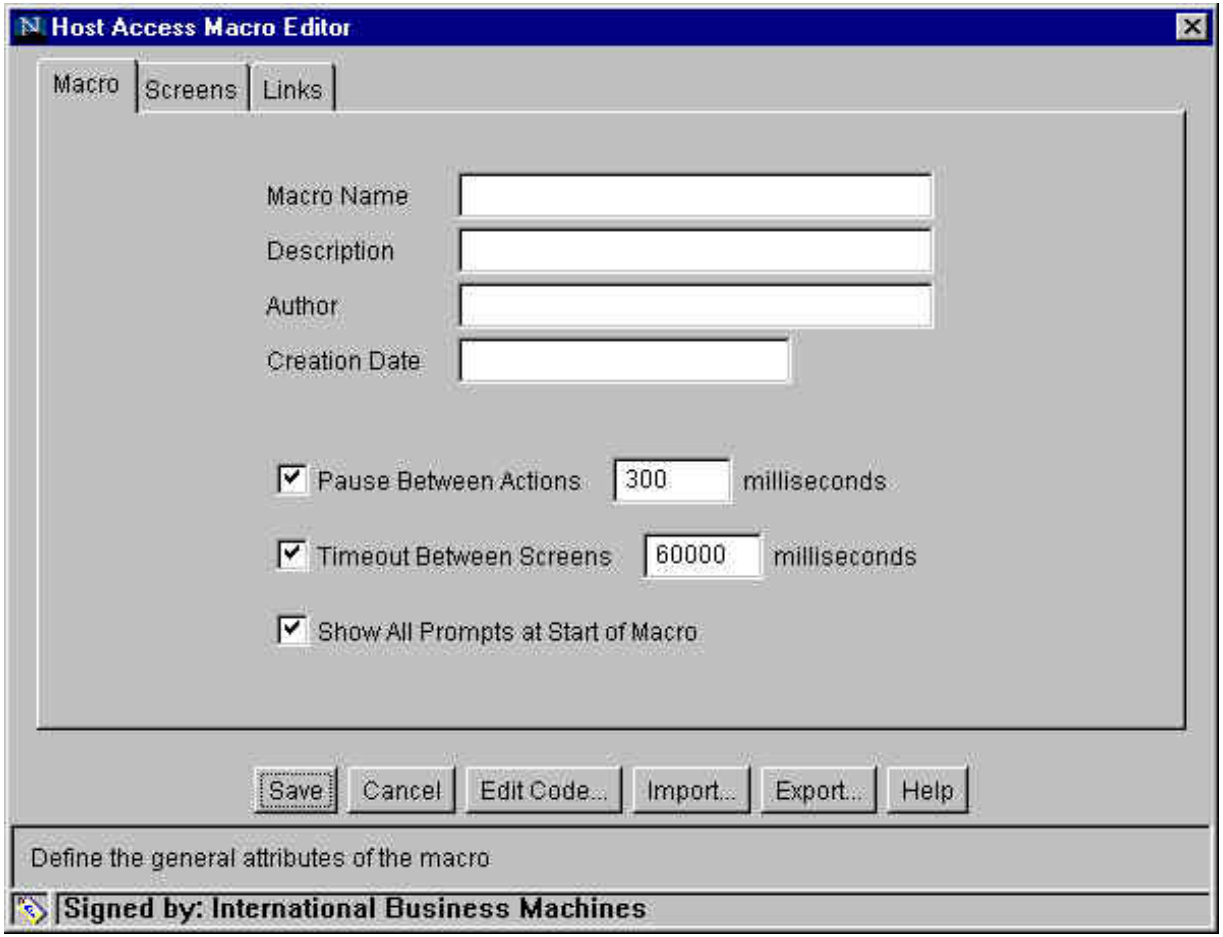
Once the session has been created (imported), the ELF macro may be imported into the session using the HOD Macro Manager.

For a HOD macro to be imported, a HOD session must be started. This will display the HOD Macro Manager. If Macro Manager is not active, it may be activated from the View window. Click on the Edit button, the first Macro Manager icon from the left, to initiate the import macro process.

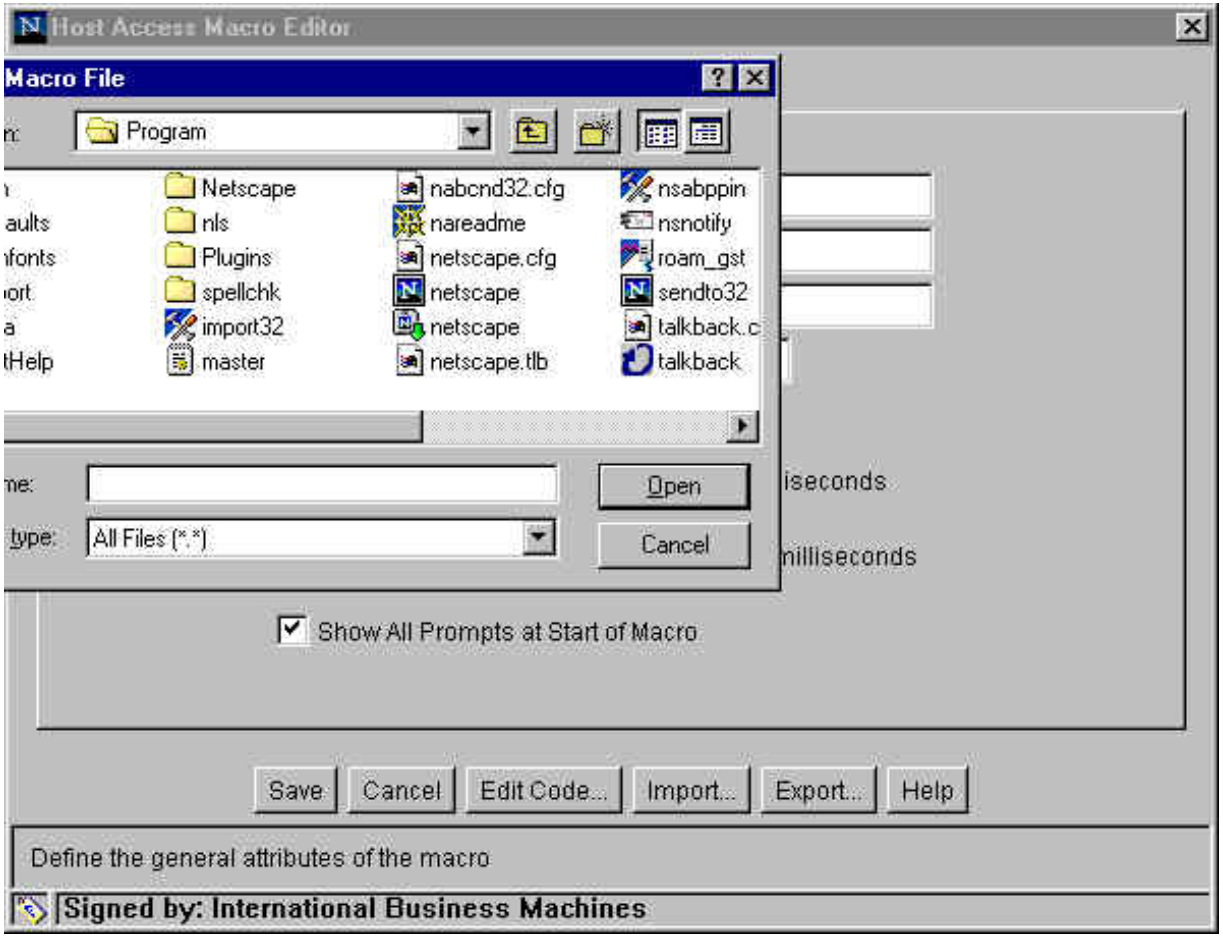
HOD 3270 Session Window active, with Macro Manager



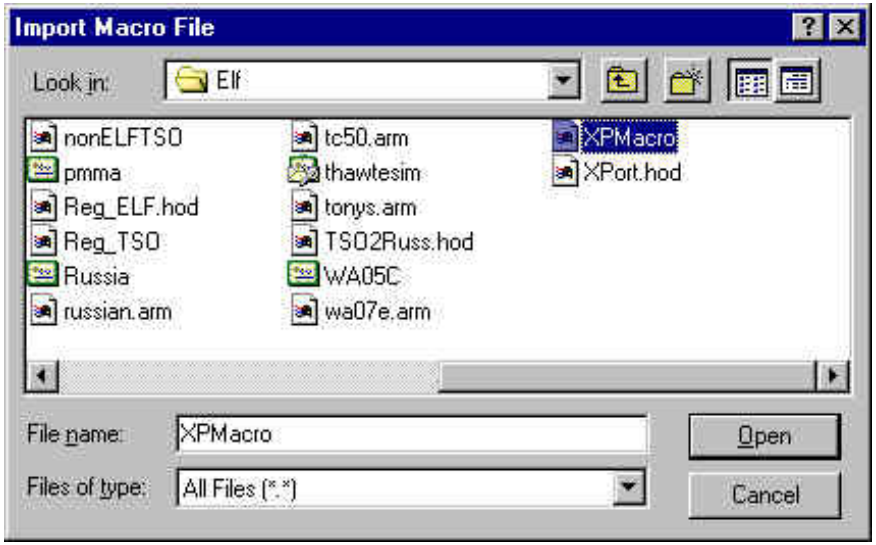
After clicking on the Edit Macro button above, the HOD Macro Editor will start.



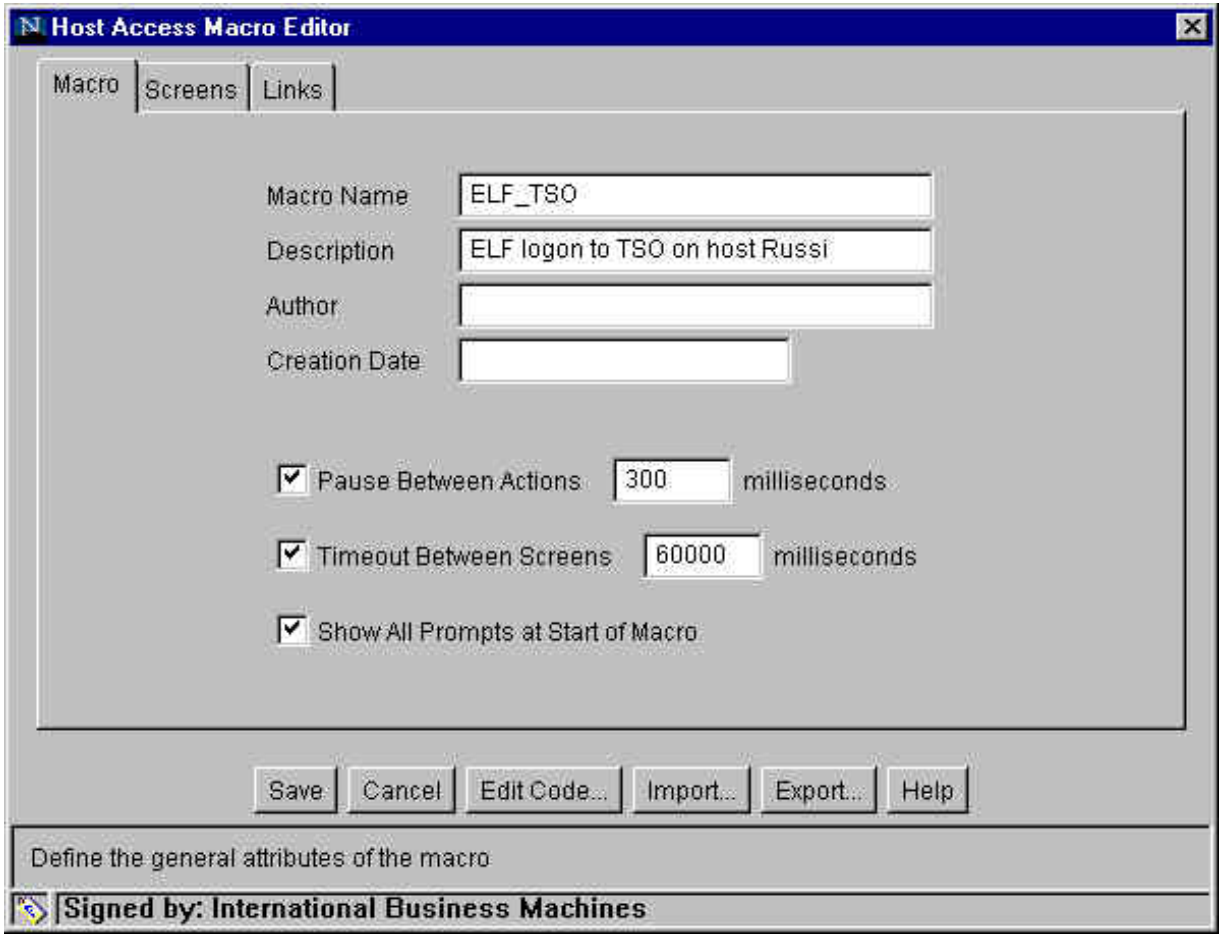
Click on the **Import...** button to initiate the import of a HOD macro. The import of the macro is completed using standard Windows dialog boxes for path and filename. Specify the location of the HOD macro file.



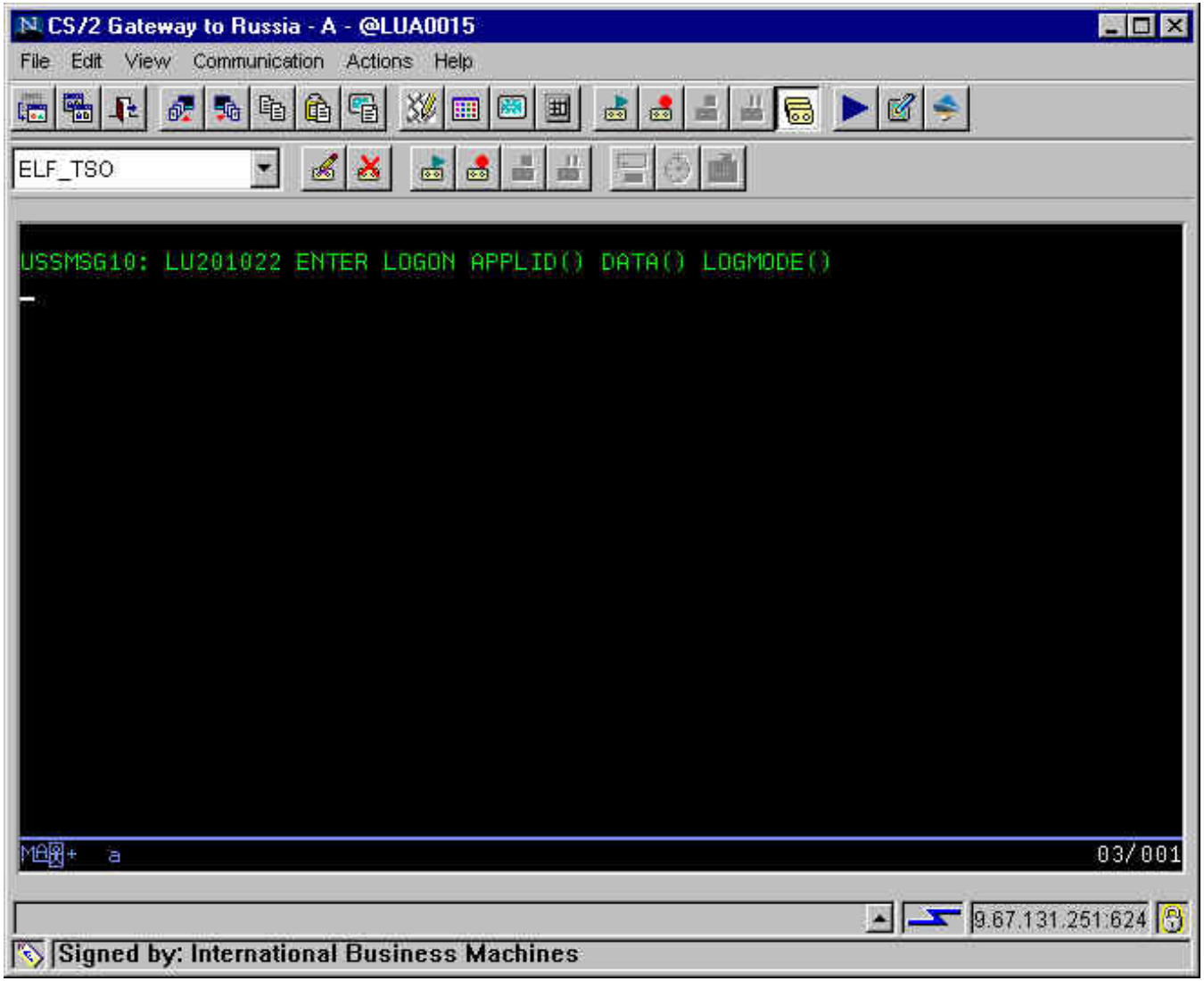
Select the HOD macro **file name.**



The imported macro is now displayed by the Macro Editor. Click on the **Save** button to save the macro for the HOD session.



The imported macro is now displayed by Macro Manager. Notice that additional Macro Manager buttons are enabled. Therefore, the imported macro may now be played back.



Now the ELF macro is ready to be replayed by the new user. The session may be further modified, through Session Properties, to automatically start the ELF macro whenever the session is started.

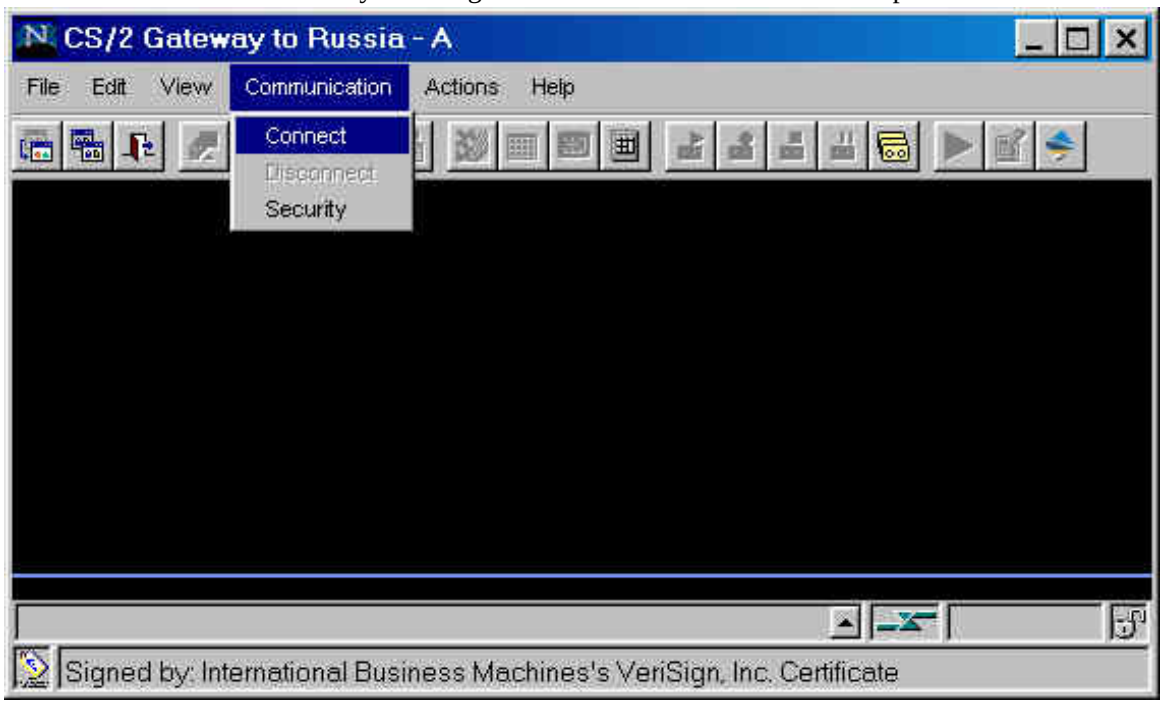
[Return to Part 4: Using the Express Logon Feature]
[Return to Contents]

4.5 Establishing a 3270 SSL Connection for Another User

Once an ELF macro is created, it may be shared among different users, which is an advantage. The only stipulation is that those users are restricted to logging on to the same host application (Application ID). That is, if the macro is created to log on to TSO, all users sharing the macro also use it to log on to TSO. RACF on the host system will match the certificate that the HOD client has supplied for Client Authentication to the specific host user ID.

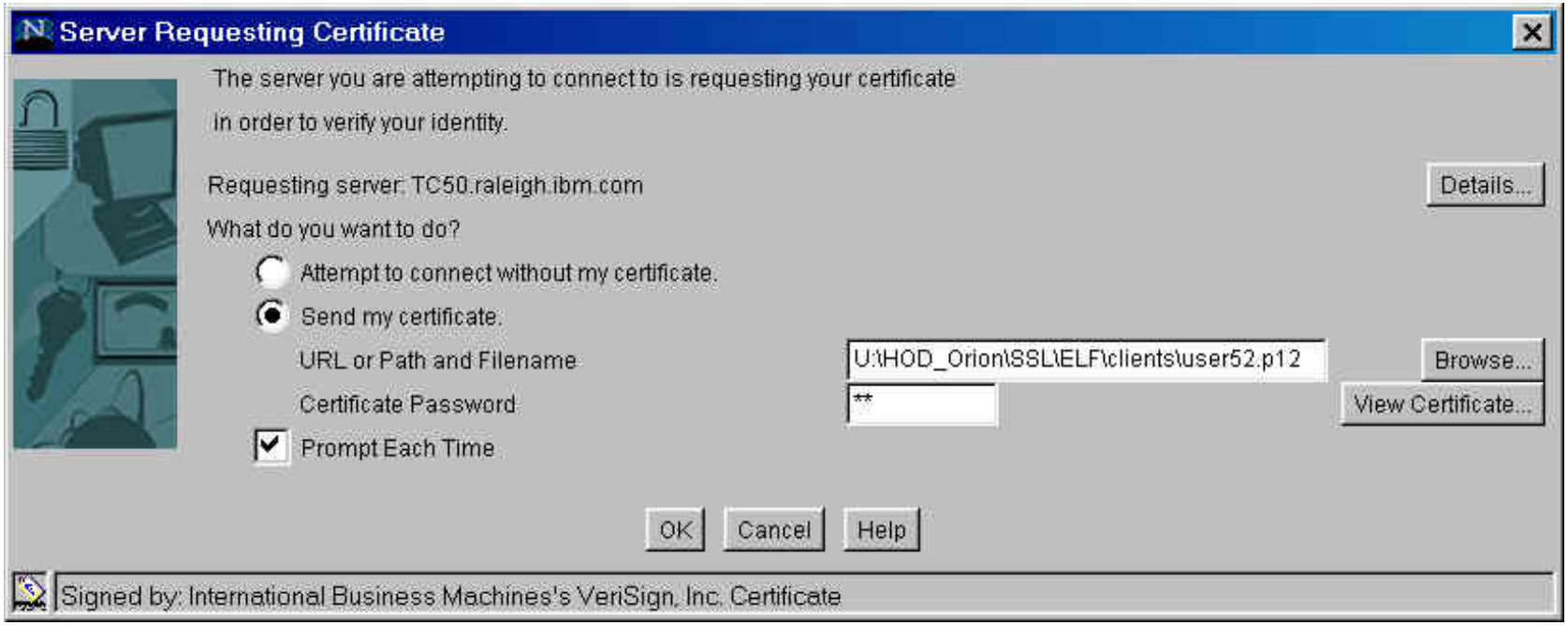
The next sequence of screens will show the establishment of a new 3270 session using a different Client Authentication certificate (.P12 file), than was previously used. Each user who shares a HOD ELF macro must use a different certificate.

The 3270 session is activated by selecting **Connect** from the Communication pulldown.

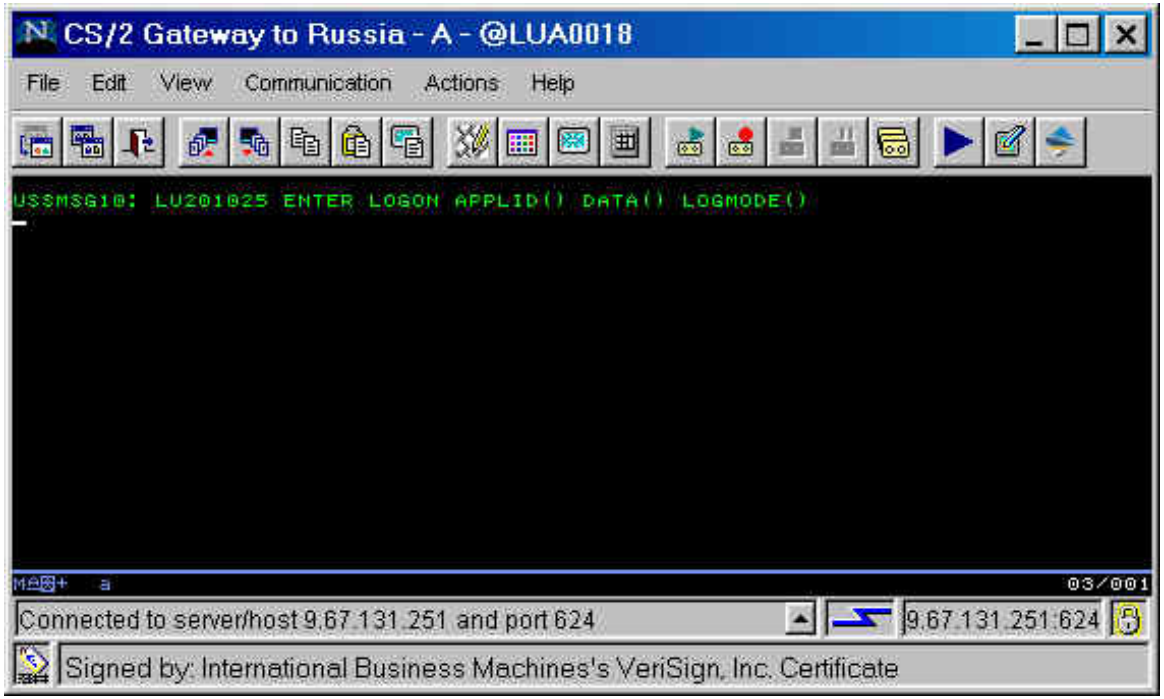


As part of the process to establish the SSL connection, the TN3270 server will respond by sending its certificate and will request the client to send a certificate.

Respond by sending the certificate for user52 (as an example). The previous session had been established using user51's certificate. Enter the certificate name and location, and its password.



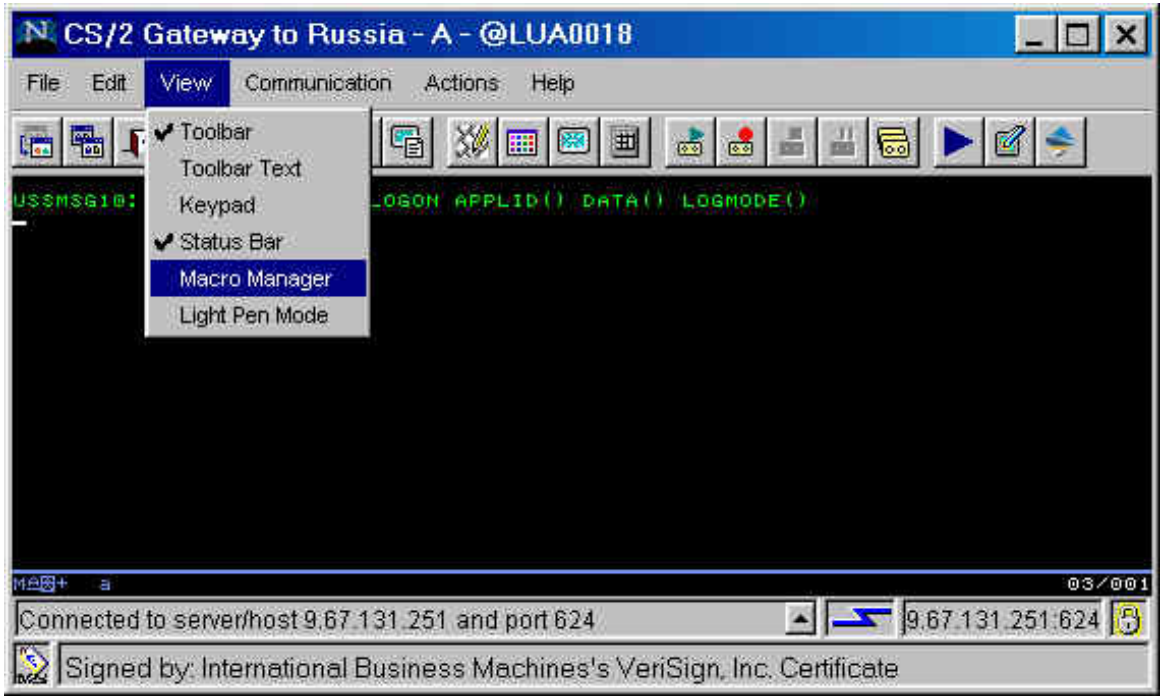
After the session has been activated, a USSMSG10 will be shown in the session window.



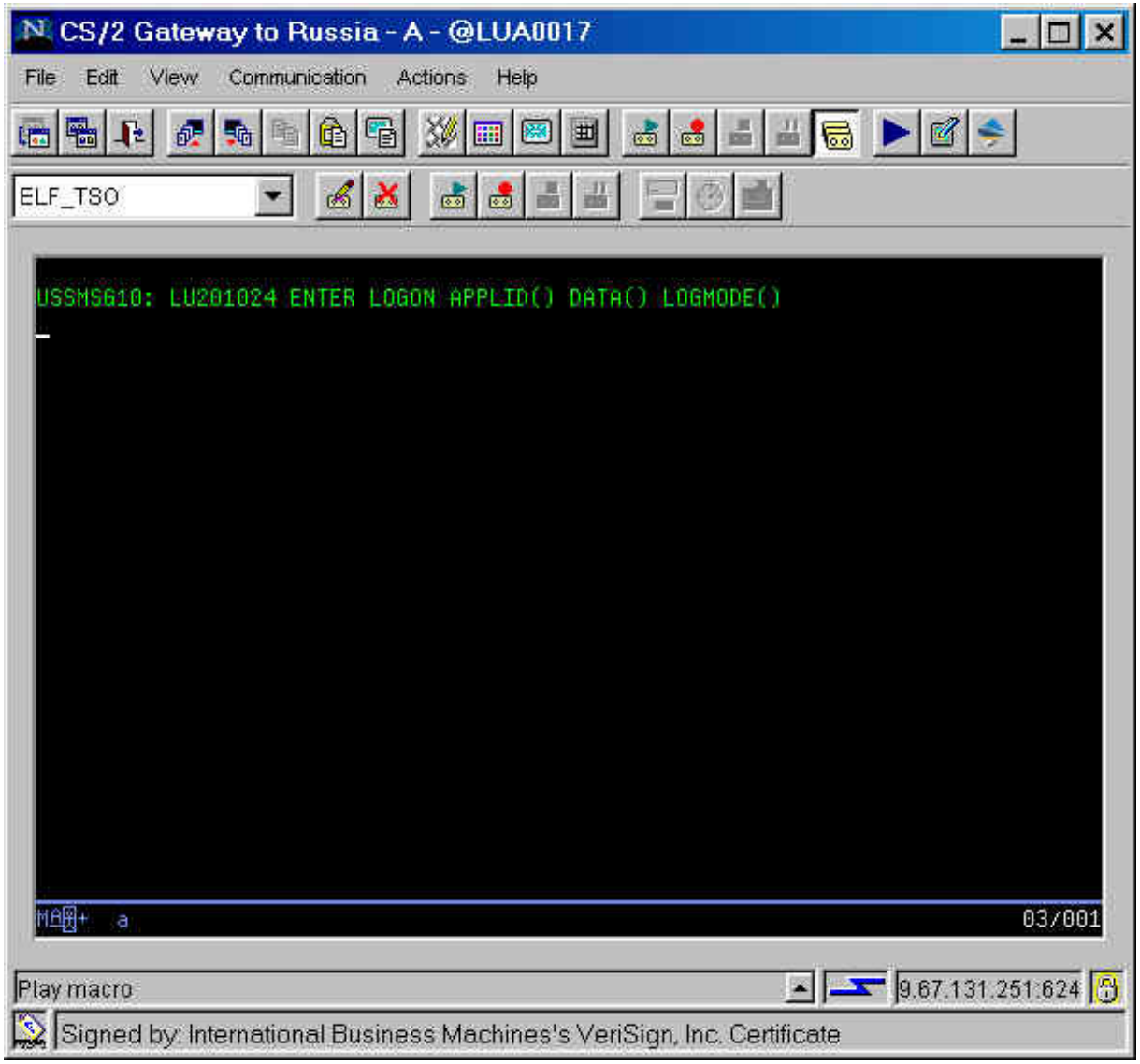
Return to Part 4: Using the Express Logon Feature
Return to Contents

4.6 Playing Back the ELF Logon Macro

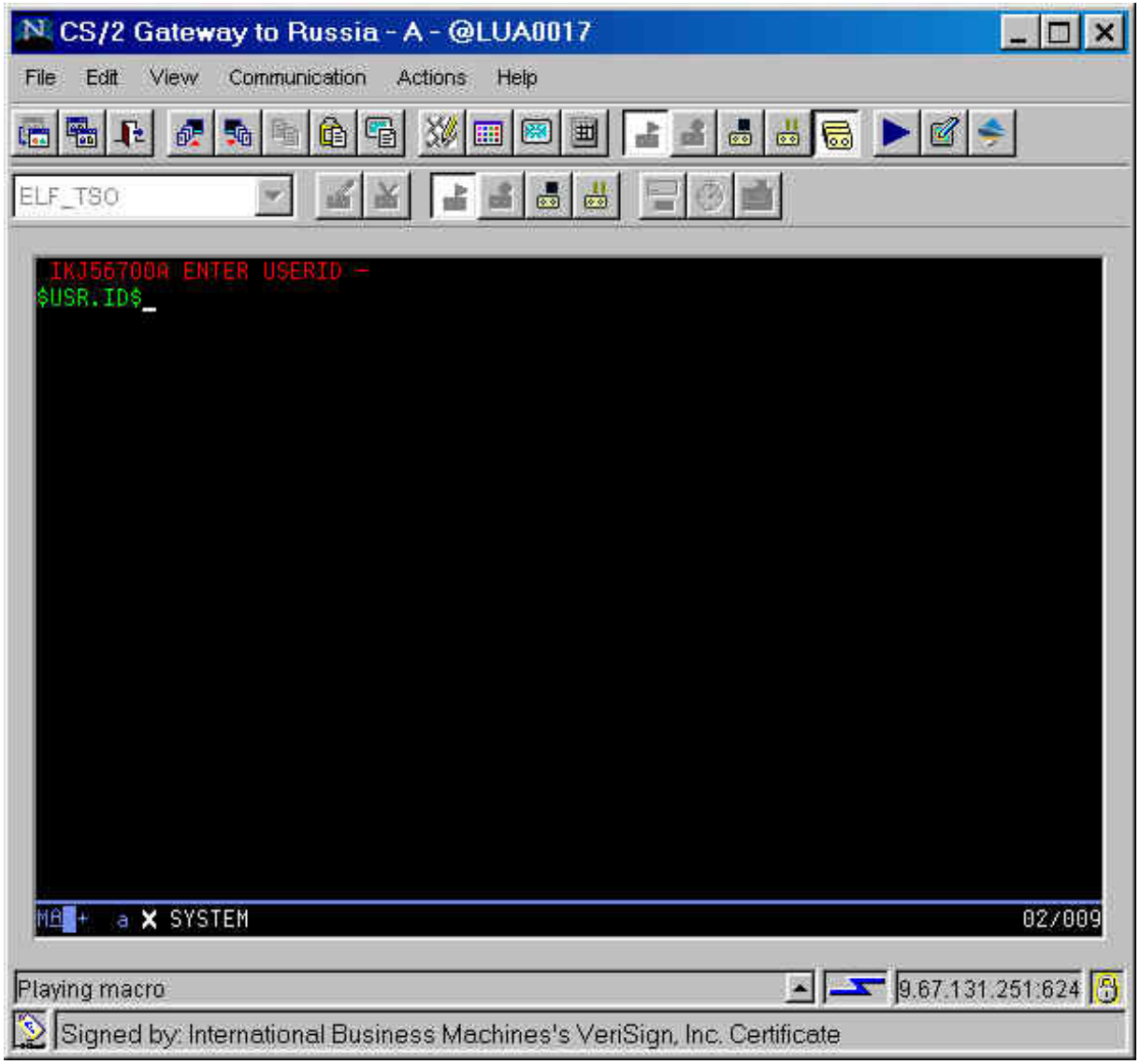
Selecting **Macro Manager** from the View pulldown will result in the Macro Manager buttons being displayed.



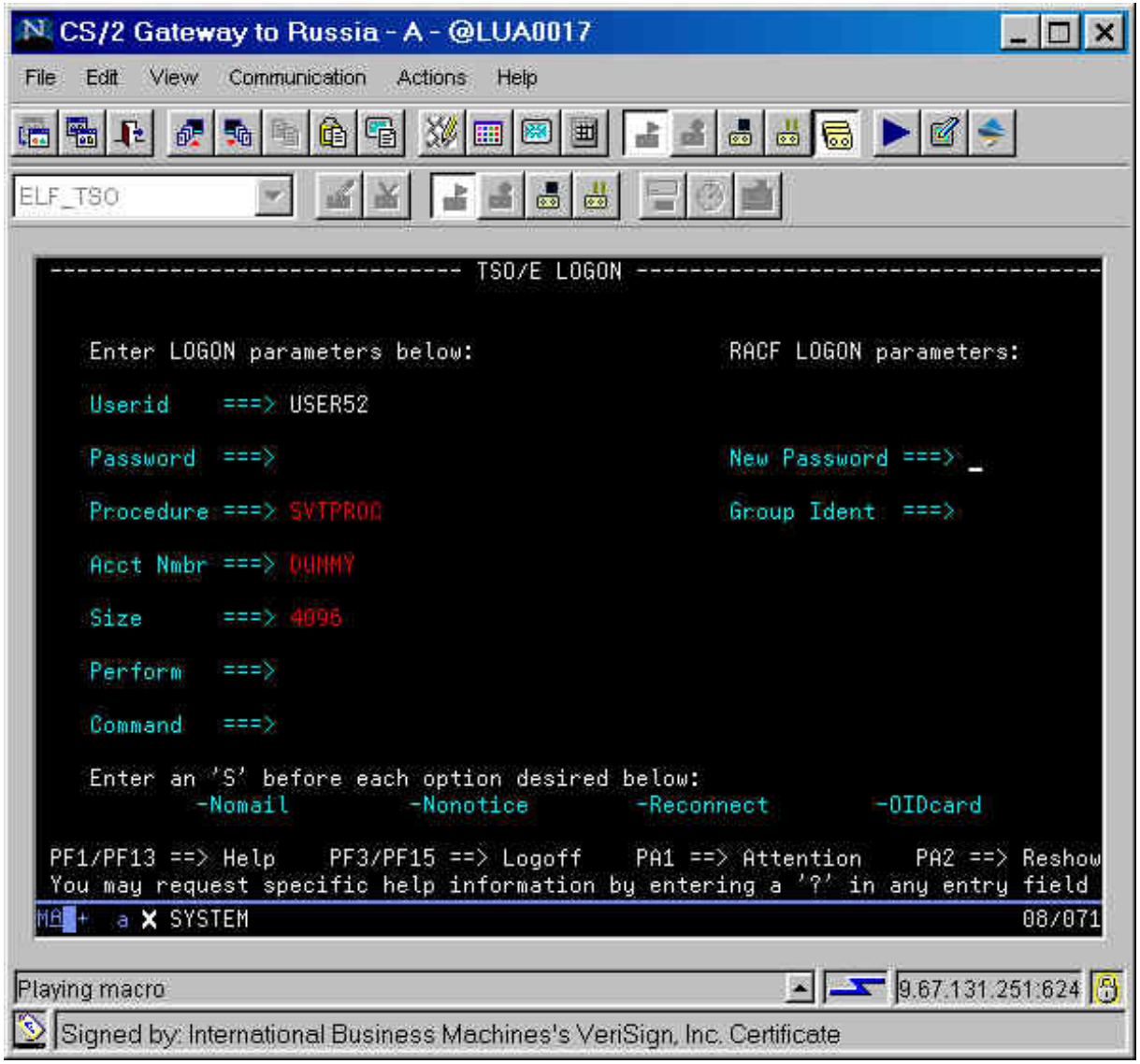
Macro Manager is now displayed. Notice the second row of icons on the action bar.



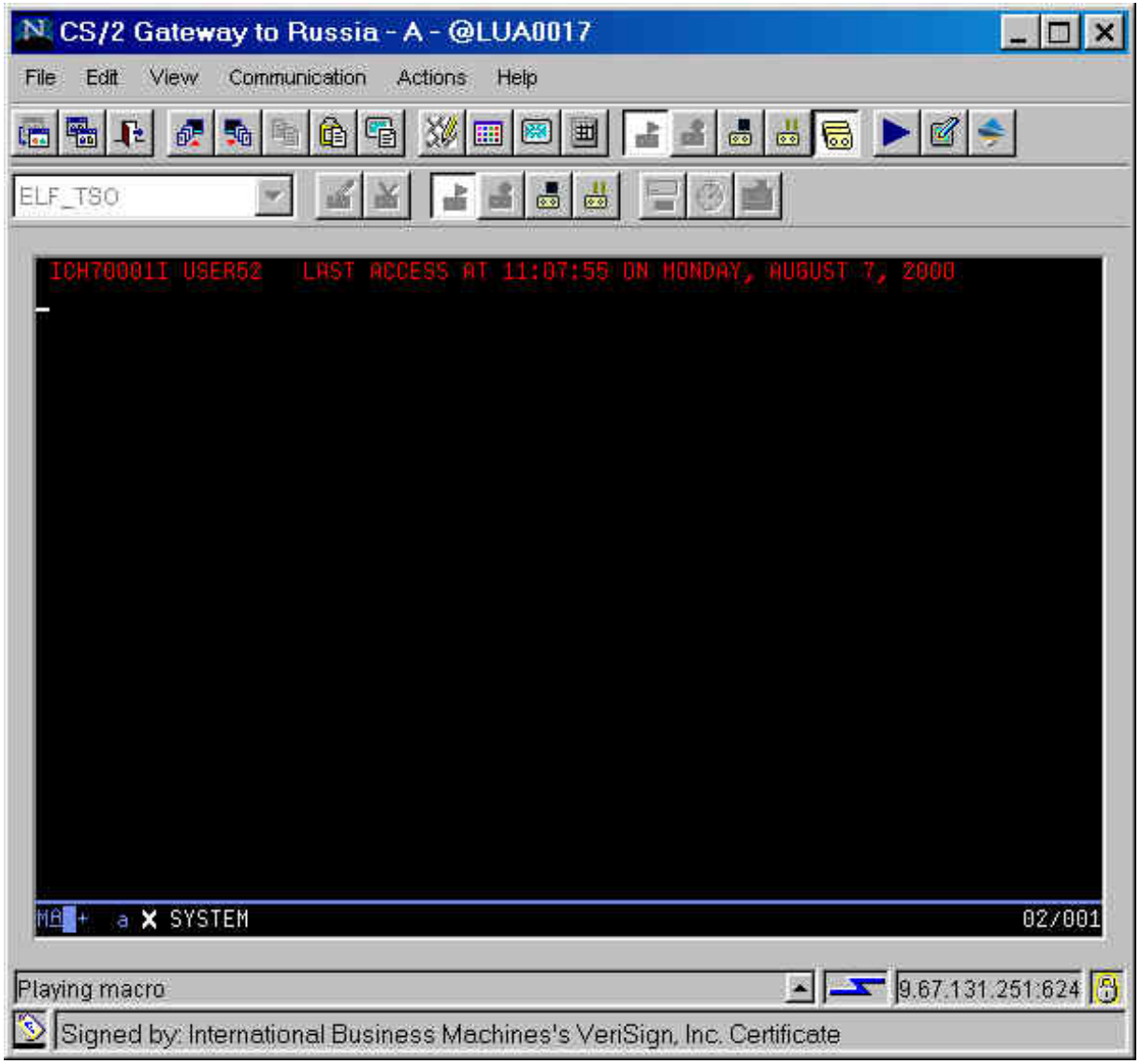
Click on the (macro) **Play** button, and the HOD ELF macro will begin playing. Note: the name of the macro is displayed in the Macro Manager display window. Notice in the following screen the ELF macro has supplied the value $USR.ID$ for the application User ID. RACF on the host will use the HOD Client Authentication certificate to determine the real User ID and generate the passticket for that User ID to log on to the specified host application, which in our case is TSO.



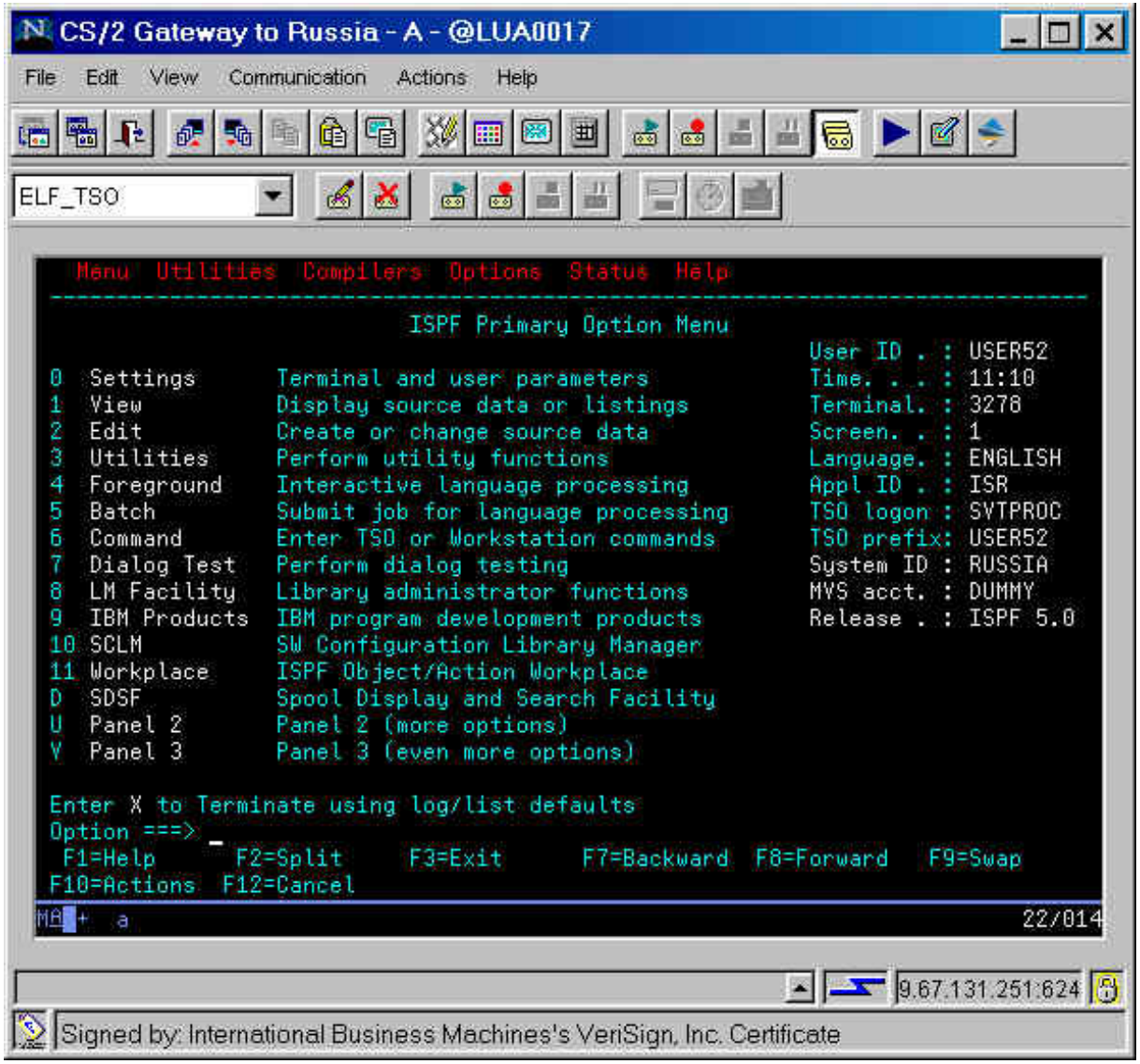
Notice on the TSO/E logon panel that the value of USER52 has been substituted for $USR.ID$. This value was determined by RACF at the host and the substitution was done by the TN3270 Server.



DCAS generates a passticket for that User ID and host application, which the TN3270 Server substitutes into the password field. After that passticket has been supplied to the host application, the logon continues.



The logon has completed at the TSO ISPF Primary Menu. Notice that the User ID is user52 and the the macro has completed playing (the macro buttons are no longer greyed out).



[Return to Part 4: Using the Express Logon Feature]
[Return to Contents]

Part 5: Troubleshooting Tips

Return to Contents

5.0 ELF Troubleshooting Overview

When troubleshooting a problem in the ELF environment, it is recommended that you verify the following steps in the order shown. Details are only given for the ELF specific steps.

Verify that:

1. The TN3270 Server has an active SNA link/connection to the host.
2. There are LUs in SSCP state (Available) on that link/connection.
3. There is a TN3270 Server port definition which points to those LUs.
4. That TN3270 Server port definition is defined for SSL client authentication.
5. The TN3270 Server's SSL certificate is acceptable to the HOD client.
6. The HOD client's SSL certificate is acceptable to the TN3270 Server.
7. The HOD client can access the IP address and port of the TN3270 Server.
8. The HOD client and TN3270 Server complete SSL negotiation.
9. The HOD client gets assigned an LU and the USS MSG10 is displayed.
10. The TN3270 Server has ELF enabled.
    For CS/2, use the '**cmtn3270 p**' command to check.
    For CS/AIX, use the '**snaadmin query_tn3270_express_logon**' command to check.
    For CS/NT, use *Node Operations* to check.
11. The HOD client plays a macro which has an ELF APPLID defined.
    The HOD macro will have a line like:

<custom id="Application_ID" args="*tso9672* />"

12. The ELF APPLID is defined to the DCAS host in a RACF PKTKDATA profile.
    Use the RACF '**RLIST PTKTDATA ***' command to check.
13. The ELF APPLID is defined to the application's host in a RACF PKTKDATA profile with the same KEY as on the DCAS host. This only applies if DCAS and the application are on separate hosts or their hosts do not share a RACF database.
14. DCAS is up and listening on the host.
    Use the TSO '**NETSTAT (PORT 8990**' command or the OE '**onetstat -P 8990**' command to check.
    You should see a line like:
    DCAS 00000xxx a.b.c.d..8990 0.0.0.0..0 Listen
    where a.b.c.d is the OS/390 IP interface that DCAS listens on.
    If a.b.c.d is 0.0.0.0, then dcas will accept connections on all OS/390 ip interfaces.
15. The TN3270 Server has an IP path to DCAS and can resolve to DCAS hostname into an IP address.
    Use the '**ping**' and '**netstat**' commands on the TN3270 Server to check.
16. The TN3270 Server's SSL certificate is defined to DCAS's keyring.
    Use the RACF '**RACDCERT ID(*dcasid*) LISTRING(*dcaskeyring*)**' command to check.
17. The HOD client's SSL certificate is defined to RACF with the userid it belongs to.
    Use the RACF '**RACDCERT ID(*userid*)**' command to check.

If the ELF session still fails, there is detailed information for each platform below.

Return to Part 5: Troubleshooting Tips
Return to Contents

5.1 Host ELF Troubleshooting

This section contains a few troubleshooting tips for the DCAS host when implementing ELF.

5.1.1 Host ELF Problem Diagnosis

- Turn on debugging and logging using -d and -l start options. If DCAS has been started, the following can be issued to toggle debug level 3 on and off.
- To toggle from the OS/390 UNIX shell, use the following command: **kill -s SIGHUP *pid***
- To toggle for an MVS started procedure, use the MODIFY command: **F DCAS,*x*** where *x* is any character.

Note: The **F DCAS,*x*** and **kill-s SIGHUP *pid*** commands are off/on toggles. For example, if logging is active using these commands turns it off. If logging is off using these commands turns it on at the highest tracing level. If you don't know whether it is currently on or off you have to toggle it, look at /tmp/dcas.log, and then decide whether to toggle it again.
The '-d' and '-l' are not part of the toggle commands. They are flags within the started proc, to tell DCAS what its initial state should be.

- Use **ping** and **netstat** to verify connectivity to the TN3270 Server.
- Check the */tmp/dcas.log* file for messages.
- Check the DCAS job log for messages.
- Check the MVS system console for RACF messages.
- Review suggestions in *IP Diagnosis for OS/390*.

Further troubleshooting steps can be taken at the HOD client and at the TN3270 Server. See other troubleshooting sections of this document for details.

If these tips don't help, collect the appropriate traces and contact IBM Support.

Return to Part 5: Troubleshooting Tips
Return to Contents

5.1.2 Host ELF Return Codes

Return codes in Reply (offset 3) from DCAS to client (TN3270)

- X'00' positive (request was successful- user ID and passticket returned)

- X'FF' Client Authentication1 failed.
Client authentication was requested (CLIENTAUTH= LOCAL2). RACF checked the client certificate from the SSL handshake and this failed for some reason. Client is terminated. The extended return code information will the return code information is returned by RACF for the Initacee query- Safrc, Racfrc, Racfrsn.

- X'FE' Client Authentication2 failed.
Client authentication was requested (CLIENTAUTH= LOCAL2). RACF verified that a valid user ID was associated with the certificate from the SSL handshake and that the SERVAUTH class was defined and active, but the user ID does not have access to the SERVAUTH class resource EZA.DCAS.cvtsysname. Client is terminated. The extended information will be the return code information that is returned by RACF for the Racroute Fastauth macro.

- X'FD' Invalid Input to the Server.
Extended return code information:
10 - Bad certificate length
11 - Invalid request format
12 - Invalid request opcode

- X'FC' RACF certificate check failed.
The certificate received in the request received from the client was sent to RACF to find a valid userid and this failed. The extended information will be the return code information is returned by RACF for the Initacee query- Safrc, Racfrc, Racfrsn.

- X'FB' Passticket generation failed.
One possible cause is that the APPLID from the HOD macro is not defined in a RACF PTKTDATA profile.

- X'FA' Internal Server Error

Return to Part 5: Troubleshooting Tips
Return to Contents

5.2 Communications Server ELF Troubleshooting

The following three sections contain some troubleshooting tips for the TN3270 Servers when configuring ELF.

5.2.1 Communications Server ELF Troubleshooting for OS/2 (CS/2)

This section contains a few troubleshooting tips for CS/2 when implementing ELF.

- Try to ping your CS/2 server IP address from your HOD client.
- Verify TCP/IP protocol is configured in MPTS.
- Verify **tcpcfg** or **tcpcfg2** is complete.
- Make sure the latest MPTS is installed on the CS/2 server.
- Make sure the HOD client is able to connect to the CS/2 TN3270 Server using SSL client authentication.
  Queries can be done on either CS/2 or HOD to make sure the session is SSL client-authenticated.
- Make sure the HOD client is able to get an active LU (i.e. the USS MSG10 appears).
- If the steps above work, the problem is on the session between CS/2 and DCAS. Here are steps to debug that connection:
  - Try to ping your DCAS IP address from OS/2.
  - Use '**netstat -s**' to see if the IP connection to DCAS is up.
  - Check the *Message Log Formatter* for messages.
  - Make sure all certificates are created and stored in the correct places.
  - Make sure there are no port mismatches or conflicts.

Further troubleshooting steps can be taken at the HOD client and at the DCAS host. See other troubleshooting sections of this document for details.

If these tips don't help, collect the appropriate traces and contact IBM Support.

Return to Part 5: Troubleshooting Tips
Return to Contents

5.2.2 Communications Server ELF Troubleshooting for AIX (CS/AIX)

This section contains a few troubleshooting tips for CS/AIX when implementing ELF.

- Try to ping your CS/AIX server IP address from your HOD client.
- Make sure the HOD client is able to connect to the CS/AIX TN3270 Server using SSL client authentication.
  Queries can be done on either CS/AIX or HOD to make sure the session is SSL client-authenticated.
- Make sure the HOD client is able to get an active LU (i.e. the USS MSG10 appears).
- If the steps above work, the problem is on the session between CS/AIX and DCAS. Here are steps to debug that connection:
  - Try to ping your DCAS IP address from AIX.
  - Use '**netstat -an | grep 8990**' to see if the IP connection to DCAS is up.
  - Check the */var/sna/sna.err* file for messages.
  - Check the */var/sna/sna.aud* file for messages (after enabling audit logging).
    Turn on audit logging with the command '**snaadmin set_global_log_type, audit=YES**'
  - Make sure all certificates are created and stored in the correct places.
  - Make sure there are no port mismatches or conflicts.

Further troubleshooting steps can be taken at the HOD client and at the DCAS host. See other troubleshooting sections of this document for details.

If these tips don't help, collect the appropriate traces and contact IBM Support.

1. Turn on CS/AIX TN3270 Server trace with the command '**snaadmin set_tn_server_trace, trace_flags=ALL**'.
2. Recreate the problem.
3. Collect the problem determination data with the command '**snagetpd**'.

Return to Part 5: Troubleshooting Tips
Return to Contents

5.2.2.1 CS/AIX ELF Return Codes

This section contains a few of the more common return codes that may be seen in the CS/AIX */var/sna/sna.err* file.

Message #	Return Code	Cause
4102-72		HOD client ran an ELF macro, but CS/AIX does not have ELF enabled
4102-115	69	tTCP/IP route or interface to DCAS is down
4102-115	78	(Informational) AnyNet Sockets-over-SNA used to access DCAS
4102-115	79	DCAS is down or not reachable (e.g., IP routing problem)
4102-115	404	CS/AIX TN3270 Server certificate defined in RACF but not DCAS
4102-115	406	DCAS cannot accept any new TN3270 Server socket connections
4102-115	414	DCAS's certificate not defined in CS/AIX's key database
4102-115	420	CS/AIX TN3270 Server certificate not defined in RACF
4102-119	-1	DCAS's certificate not defined in CS/AIX's key database
4102-119	251	APPLID in ELF macro not defined to RACF
4102-119	253	HOD client ran an ELF macro on a session which is not SSL client-authenticated

Use the **snahelp** command to see the associated text for each message. For example 'snahelp 4102-119'.

Return to Part 5: Troubleshooting Tips
Return to Contents

5.2.3 Communications Server ELF Troubleshooting for NT (CS/NT)

This section contains a few troubleshooting tips for CS/NT when implementing ELF.

- Try to ping your CS/NT server IP address from your HOD client.
- Make sure the HOD client is able to connect to the CS/NT TN3270 Server using SSL client authentication.
  Queries can be done on either CS/NT or HOD to make sure the session is SSL client-authenticated.
- Make sure the HOD client is able to get an active LU (i.e. the USS MSG10 appears).
- If the steps above work, the problem is on the session between CS/NT and DCAS. Here are steps to debug that connection:
  - Try to ping your DCAS IP address from NT.
  - Use '**netstat -an**' to see if the IP connection to DCAS is up.

- Check the *Log Viewer* for messages.
- Make sure all certificates are created and stored in the correct places.
- Make sure there are no port mismatches or conflicts.

Further troubleshooting steps can be taken at the HOD client and at the DCAS host. See other troubleshooting sections of this document for details.

If these tips don't help, collect the appropriate traces and contact IBM Support.

Return to Part 5: Troubleshooting Tips
Return to Contents

5.3 Host On-Demand (HOD) ELF Troubleshooting

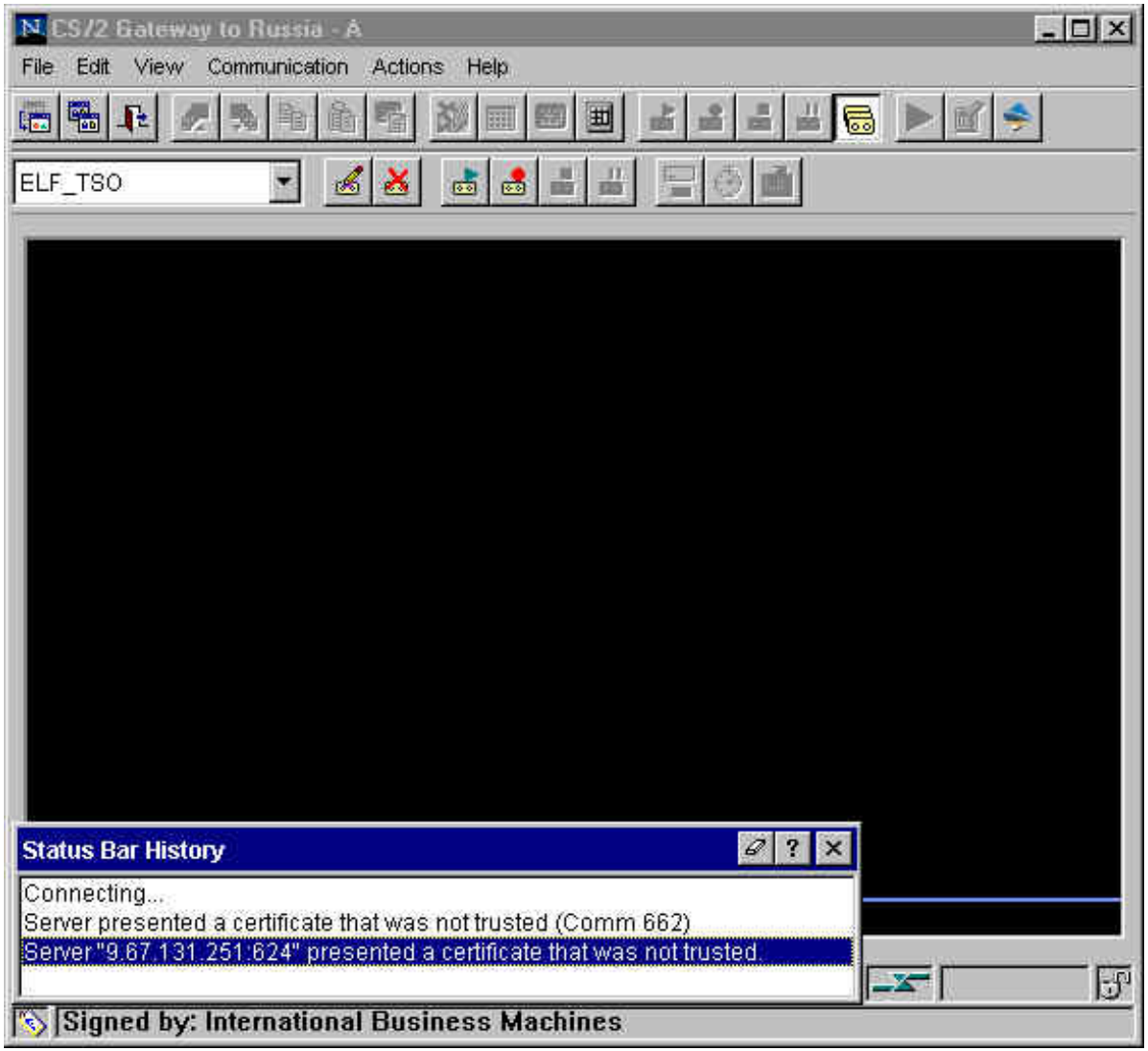
This section contains a few troubleshooting tips for HOD when implementing ELF.

5.3.1 HOD Common Connection Problems

Most of the HOD problems that are encountered for ELF are due to setup problems with SSL. The most common problems deal with not having the proper certificates for each platform in the proper places (the HOD client, the intermediate TN3270 Server, the CS/390 MVS host).

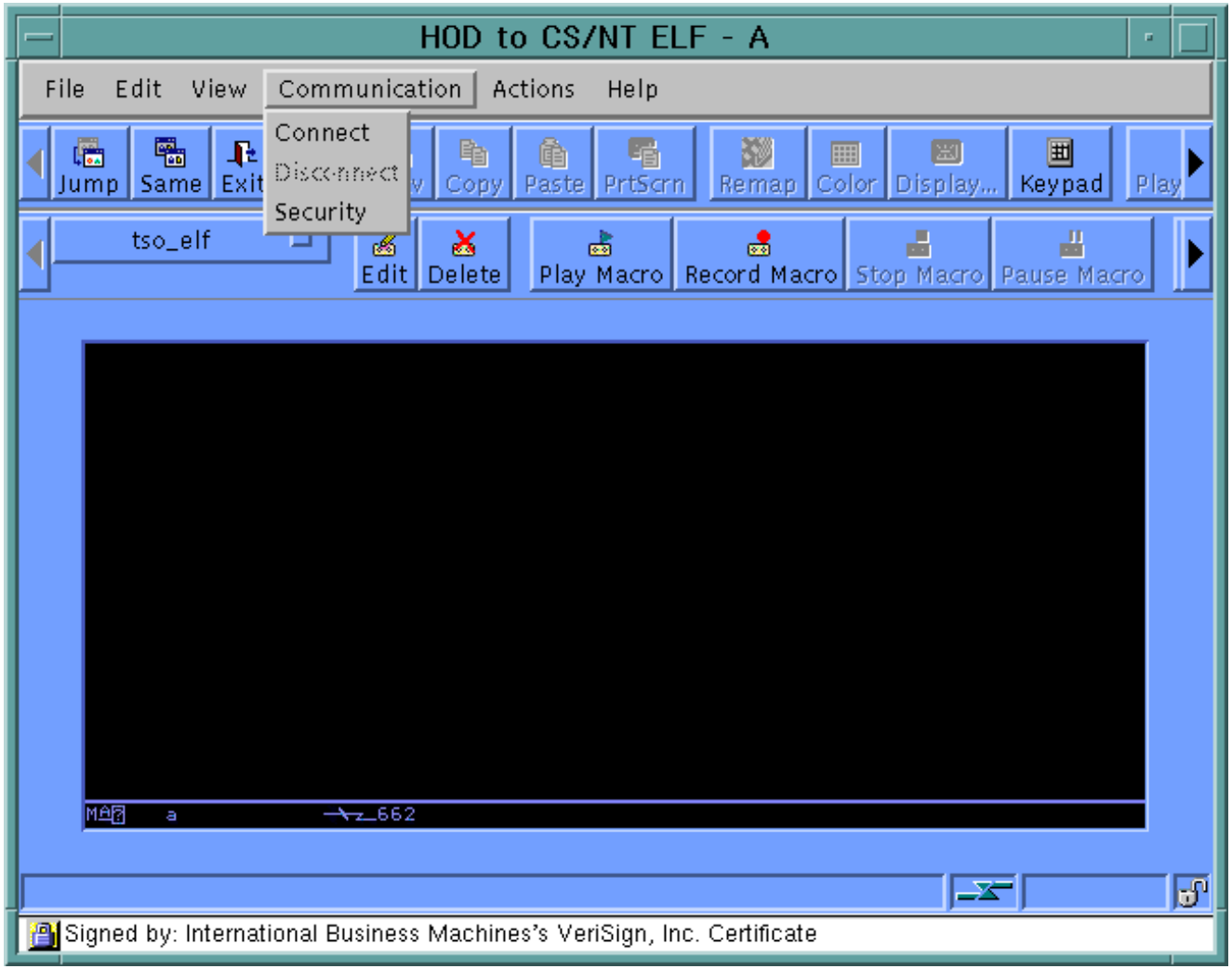
Following is an example of a scenario in which the certificate for the intermediate TN3270 Server is not in the HOD CustomizedCA.class file. CustomizedCAs.class resides in the \hostondemand\HOD directory, for download clients, or \hostondemand\lib, for a locally installed client. For HOD on AIX the directory names are /usr/opt/hostondemand/HOD and /usr/opt/hostondemand/lib respectively.

The screen below has the Status Bar History expanded, as the error messages are only displayed temporarily in the Status Bar area. The messages state that the server was not trusted.



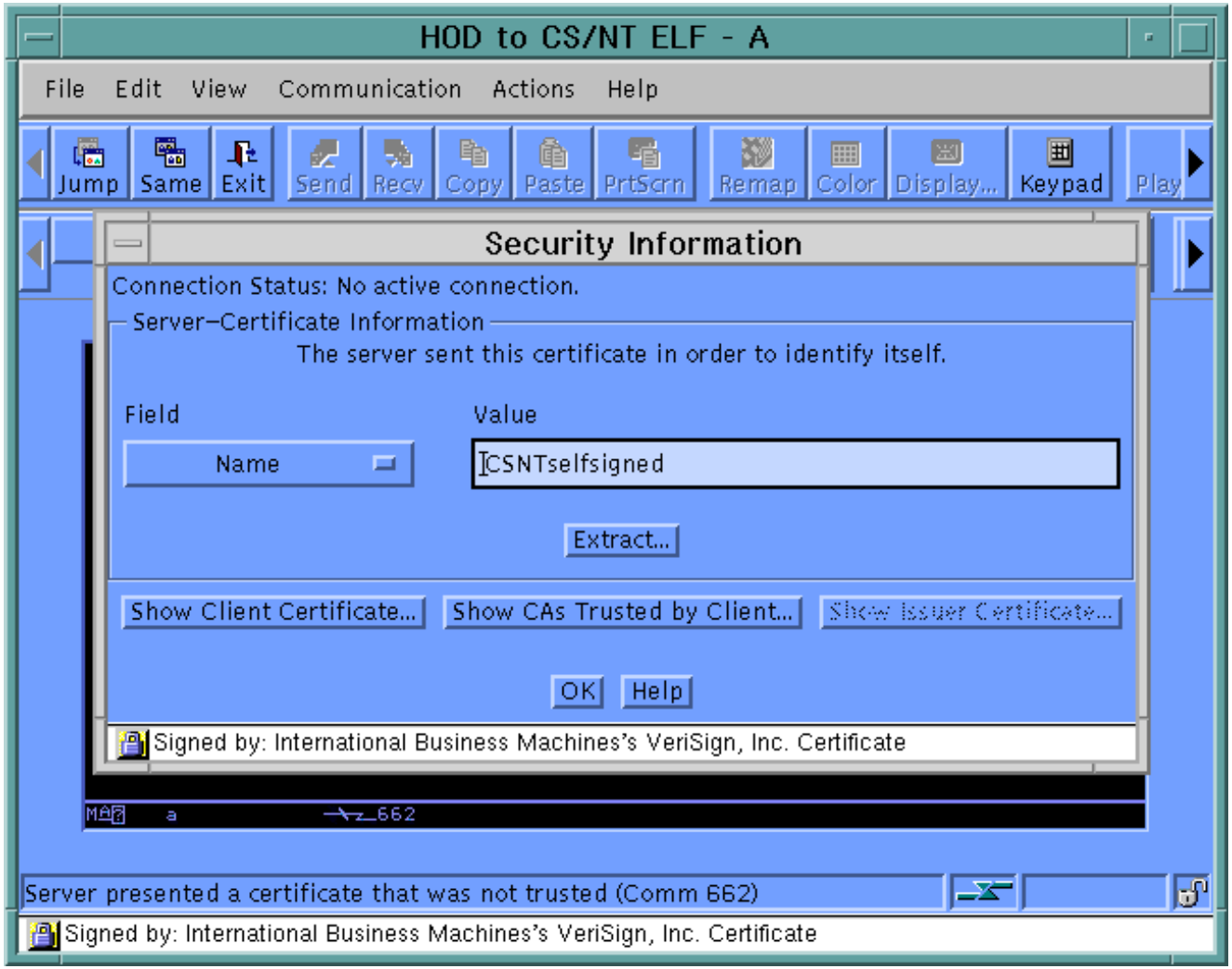
Intermediate TN3270 Server Not Trusted

Although the connection has failed, it is still possible to view the server certificate that was sent to the HOD client, and also to extract this certificate. This process in initiated by clicking on Security from the Communication pulldown.



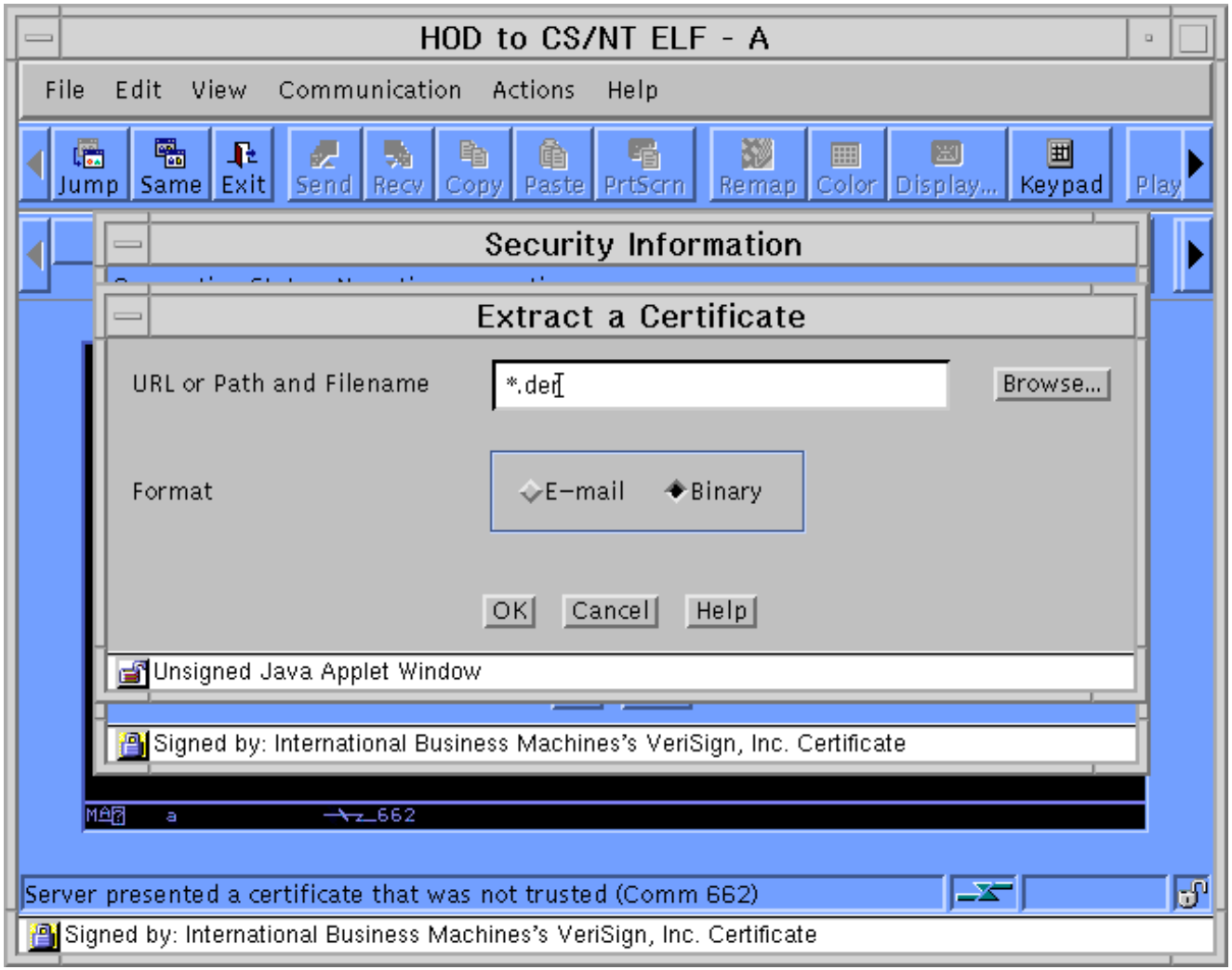
Access the Security Menu

The Security Information window displays the name of the server that sent the certificate (that was not accepted) to the HOD client.



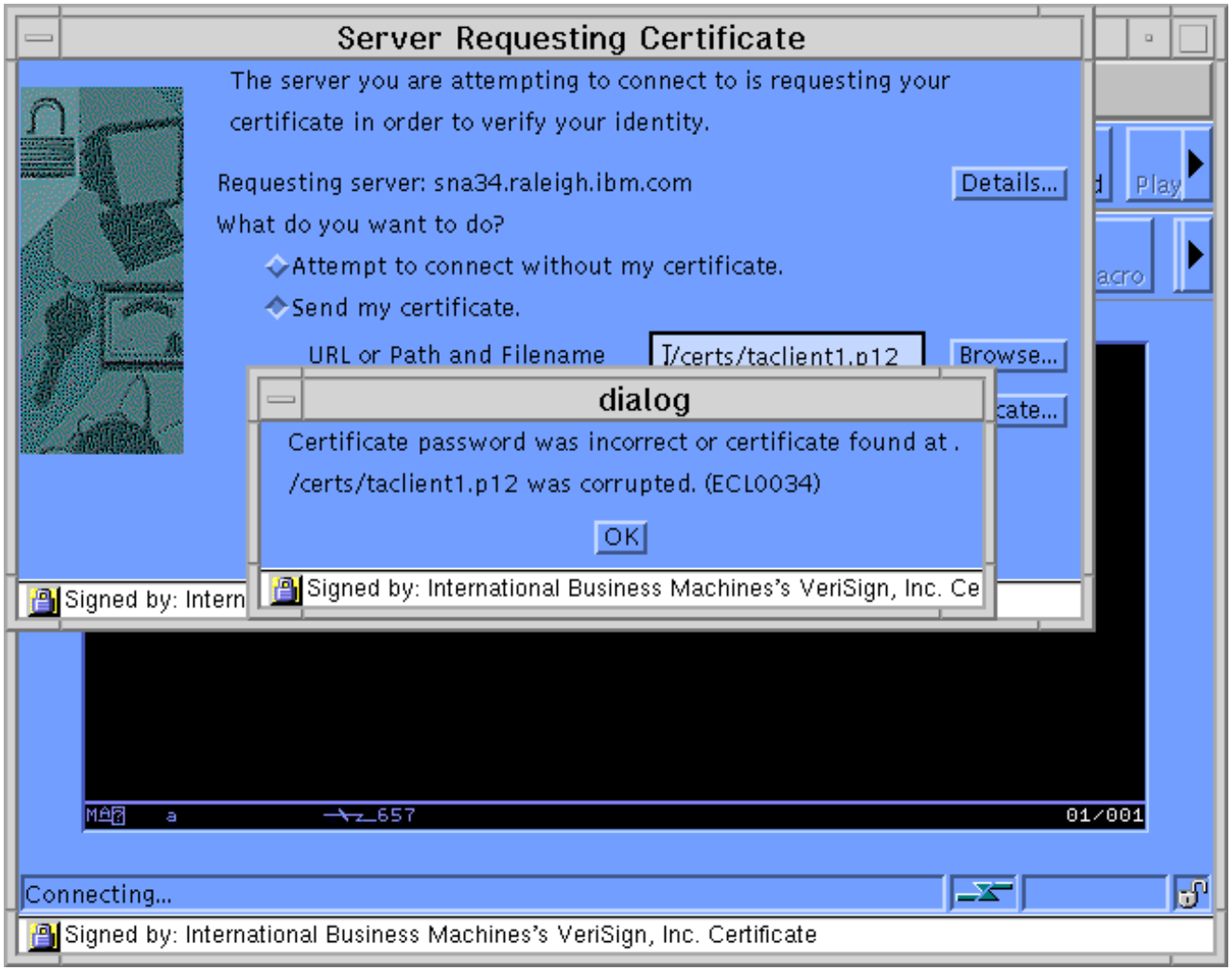
Security Information window

Clicking on the Extract button will bring up the Extract a Certificate dialog window. The server's certificate can then be extracted to either an ARM (ascii) file or a DER (binary) file. After the server's certificate has been extracted, it may then be added to the CustomizedCA.class file, using HOD Certificate Management Utility. However, for the session to activate, the client must use the new copy of CustomizedCAs.class. This can usually be accomplished by stopping and then restarting the browser.



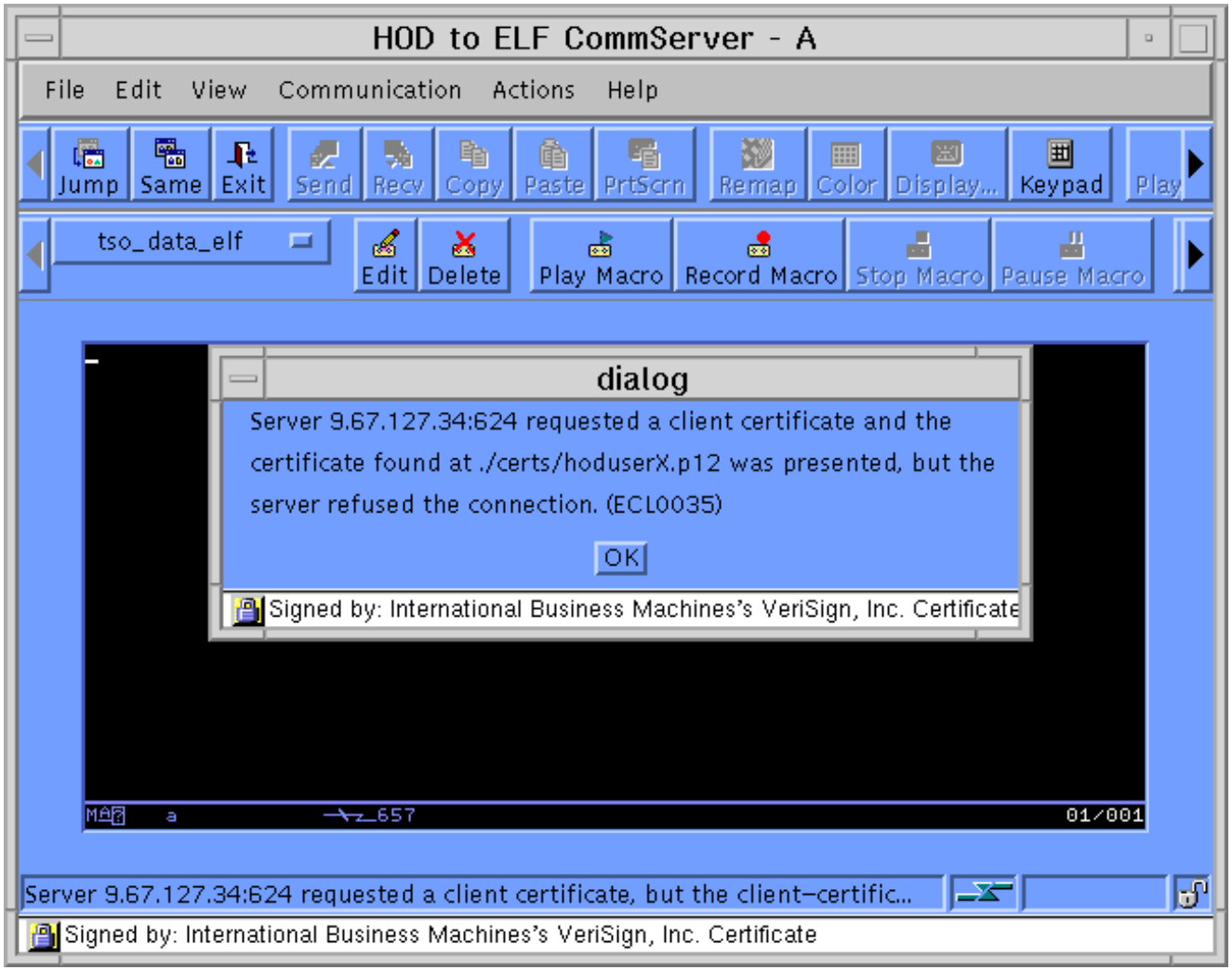
Extracting a Server Certificate

Sometimes an incorrect password is used to open the HOD Client P12 file when the intermediate TN3270 Server requests the client certificate. In this case, the error takes place at the HOD client, and the certificate is never sent. Following is the error message displayed for this situation.



Incorrect Password For The HOD Client Certficate (P12 file).

Another common SSL failure is due to the TN3270 Server not accepting the HOD Client Certificate. That is due to the HOD client Root Certificate not being in the intermediate TN3270 Server's key database. Following is the error message that is displayed by the HOD client when its certificate is refused.

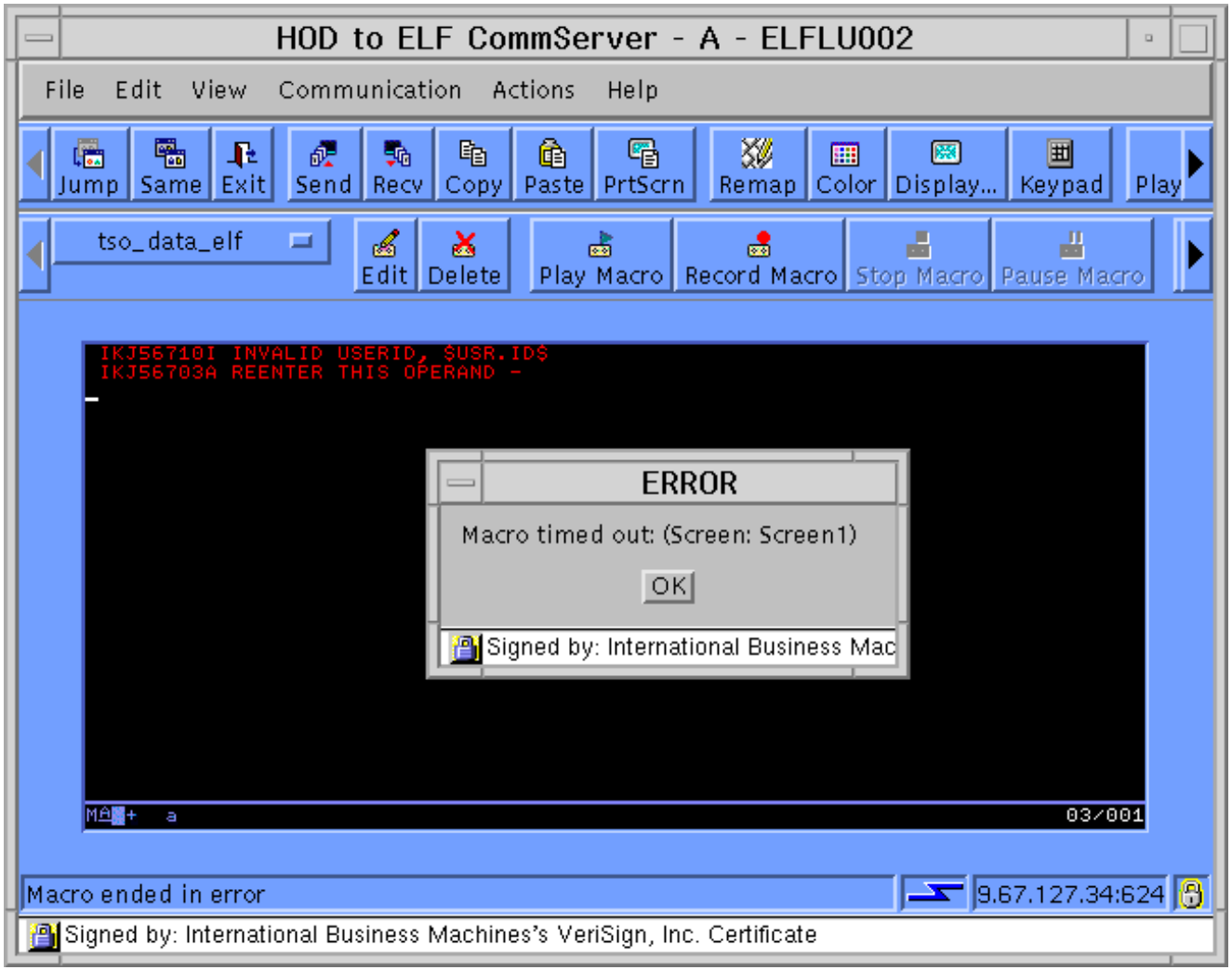


HOD Client Certificate is Refused

Once the SSL session has been established the ELF macro can be run. If a host message like "$USR.ID$ not found" is seen, that means the ELF part of the macro failed. There are many possible causes for this:

- TN3270 Server is not ELF enabled
- DCAS is not available at the host
- HOD client certificate not defined to RACF
- HOD macro used an APPLID that is not defined to RACF

Use the TN3270 Server and DCAS logs to determine what is the actual cause. Following is a typical error message for these scenarios.



ELF macro fails ($USR.ID$ not found)

Return to Part 5: Troubleshooting Tips
Return to Contents

5.3.2 Additional HOD Debugging Tips

Sometimes the HOD connection error is not apparent from the error messages that are displayed to the client. It is not uncommon for information for security errors to be rather sparse, by design. Checking the log files on the TN3270 Server and the host is usually a good idea in these cases.

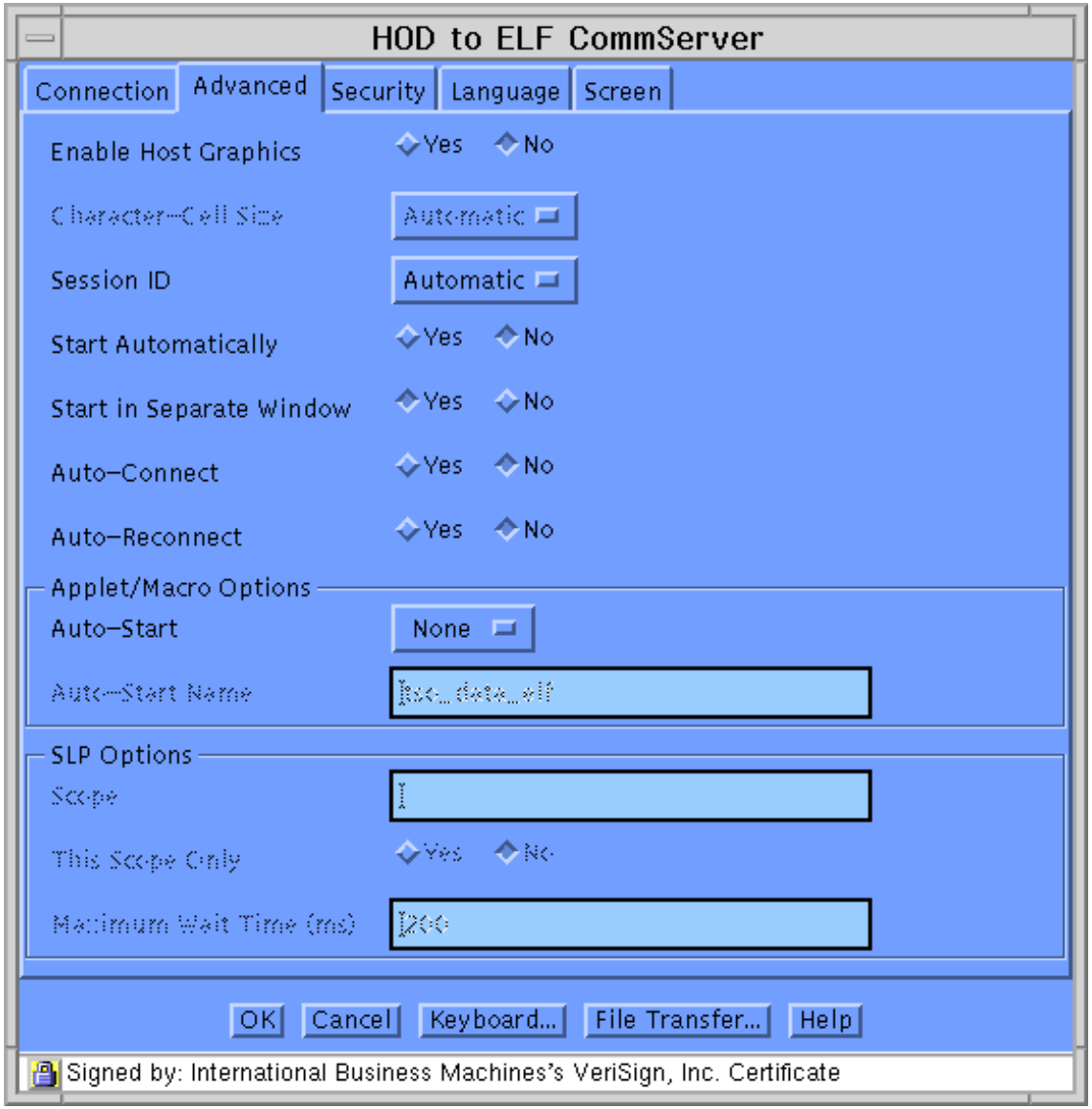
Following are instructions for collecting HOD traces, if more extensive debugging is required.

To gather HOD traces, the HOD Debug Client must be run (HODDebug.html). Point the web browser to this page instead of the normal (HOD.html or HODCached.html)

pages.

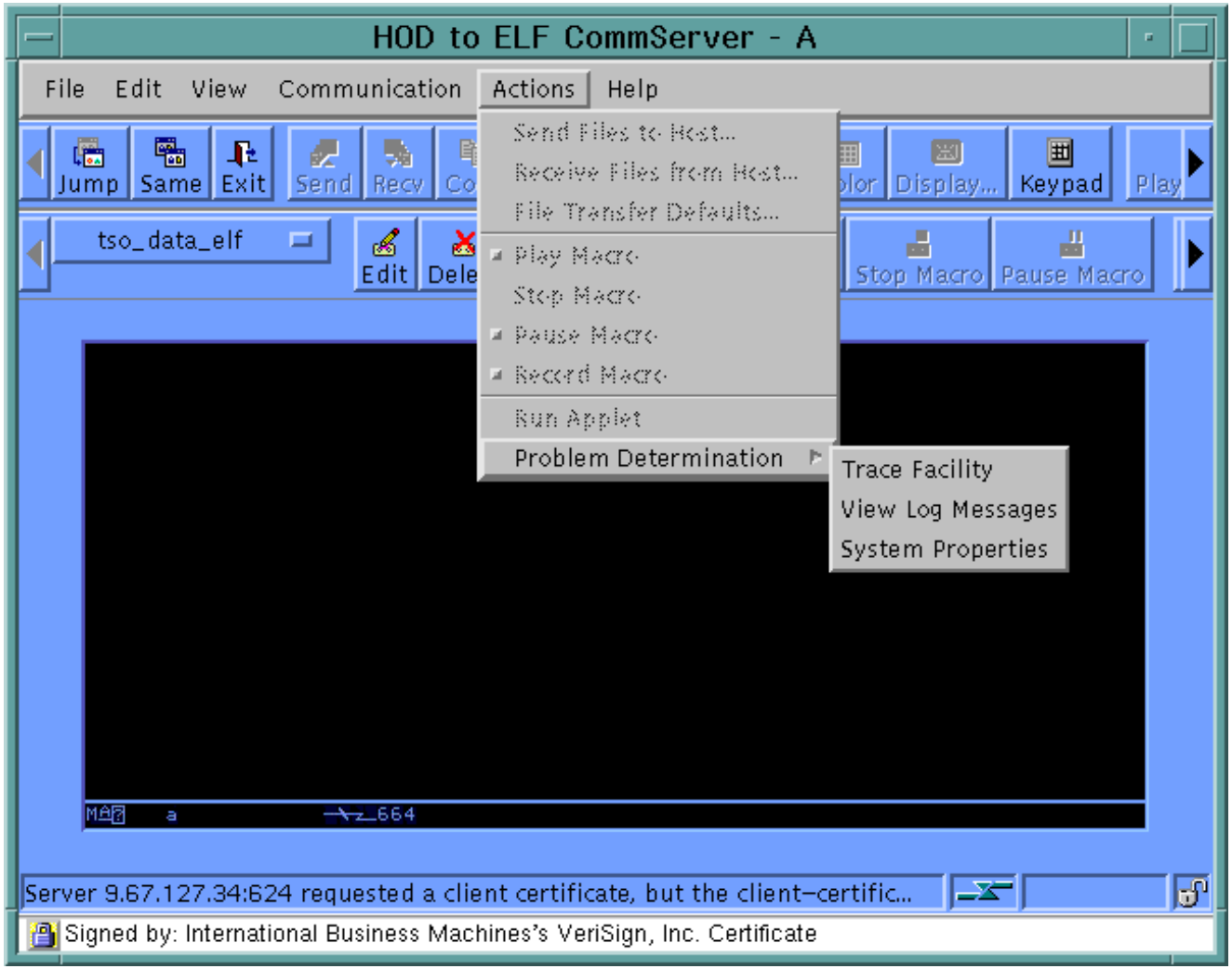
Log on to the debug client using the same User ID and Password as would be used for the normal HOD client. The same ELF session icons should be displayed.

If the error is encountered during the activation of the session, it is usually best to alter the Session Properties (on the Advanced tab) to turn Auto-connect and Auto-Reconnect to No and to also turn the Macro Auto-Start to None. This allows the trace to be started prior to the connection attempt.



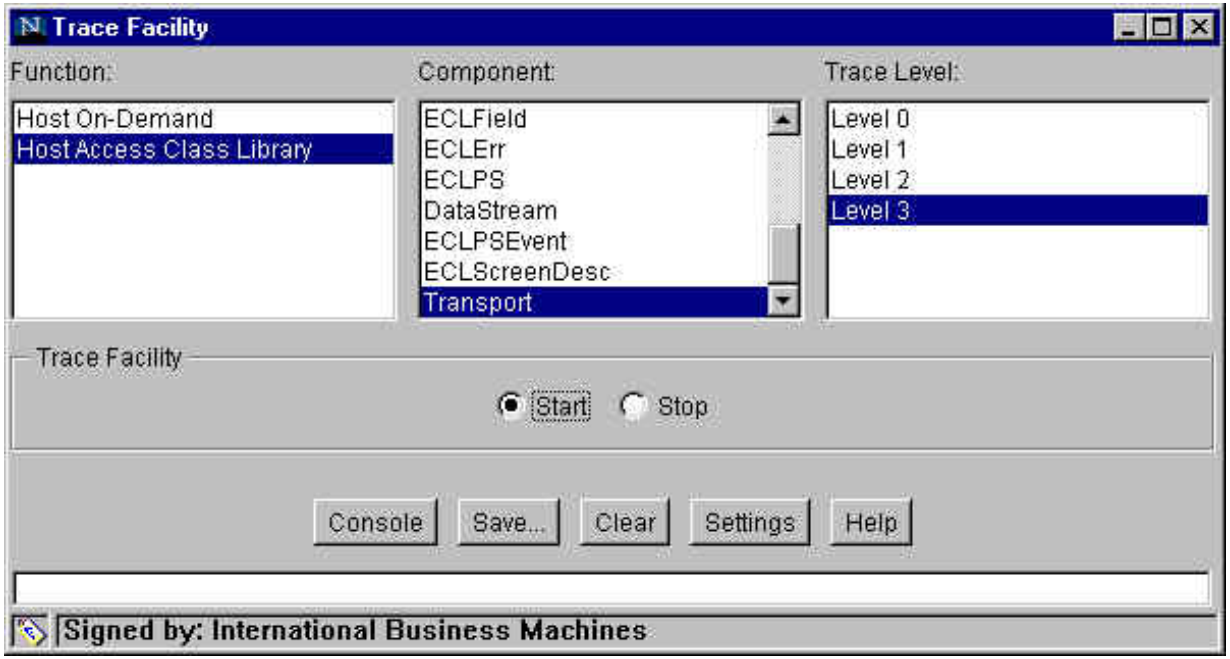
Session Properties Window

HOD tracing is activated from the Actions pulldown, which is located on the Main Menu bar.



Start the Trace Facility

This will initialize the main Trace Facility window.
Notice there are Start and Stop radio buttons which are used to start and stop the HOD trace. From this window you can set the trace levels for the various HOD and HACL Components. Level 0 is for no tracing, and Level 3 is the highest (most detailed) level of tracing.

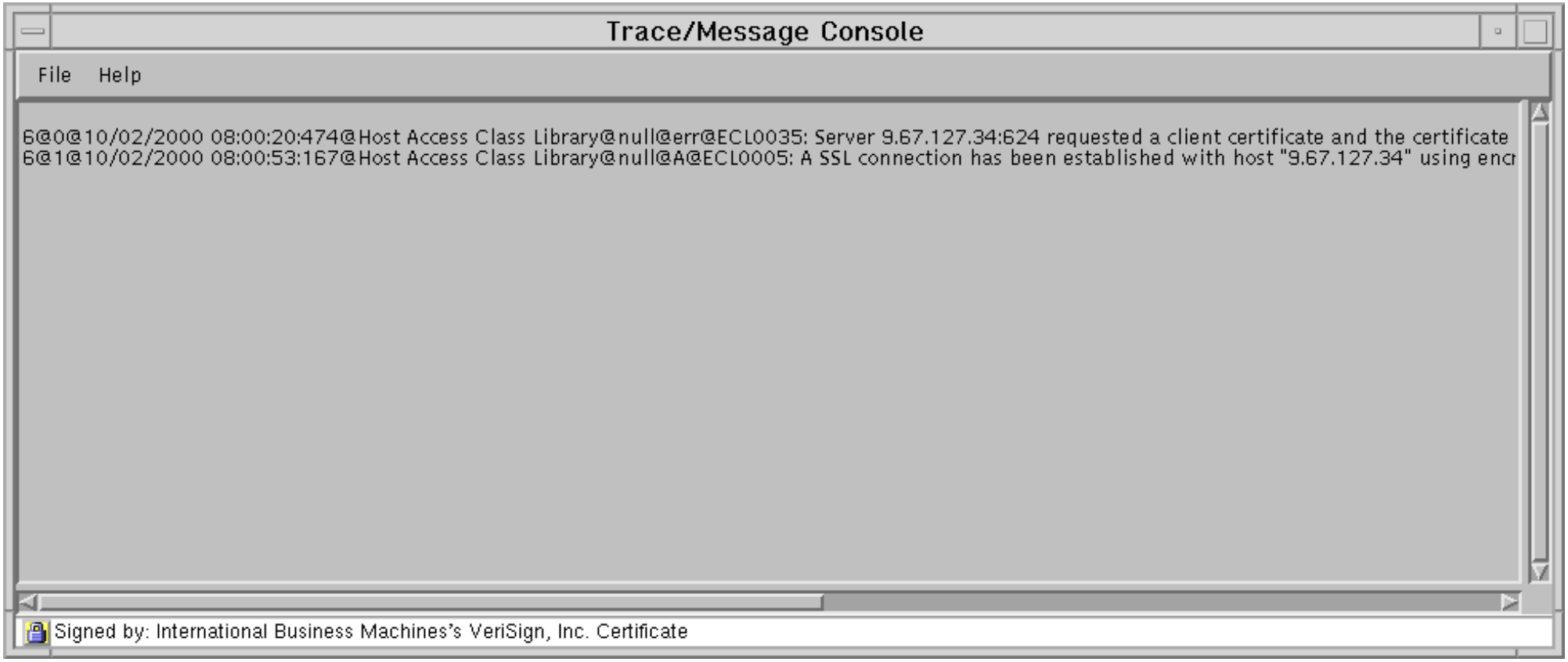


Trace Facility Window

Clicking on the Settings button will allow you to change global trace values.

Trace Settings Window

Clicking on the Console button will activate a separate window, the Trace/Message Console window. This will display the trace messages, but will dramatically slow down the performance of the HOD client.



HOD Trace/Message Window

Return to Part 5: Troubleshooting Tips
Return to Contents

References

Communications Server for AIX references:

IBM Communications Server for AIX V6, *README* file at /usr/lpp/sna/README

IBM Communications Server for AIX, Quick Beginnings, Version 6, GC31-8583-01 at:
http://www.ibm.com/software/network/commserver/library/publications/csaix_60/dysl1mst.htm

IBM Communications Server for AIX, Administration Guide, Version 6, SC31-8586-01 at:
http://www.ibm.com/software/network/commserver/library/publications/csaix_60/dyvl1mst.htm

IBM Communications Server for AIX, Administration Command Reference, Version 6, SC31-8587-01 at:
http://www.ibm.com/software/network/commserver/library/publications/csaix_60/dywl1mst.htm

Redbook *IBM Communications Server for AIX, V6 New Features and Implementation Scenarios*, SG24-5947-00, 'Chapter 2. Secure Sockets Layer support' at: http://www.redbooks.ibm.com/abstracts/sg245947.html

Whitepaper *"SSL with CS/AIX v5.0.4.0 TN3270 Server"* at:
http://www.ibm.com/software/network/commserver/library/whitepapers/sslhow-to.html

Communications Server for OS/2 references:

IBM Communications Server for OS/2 Warp Version 6.1 has information available on the distribution CD in the Information Folder within the IBM Communications Server Folder:

What's New in Version 6.1
Overview
TN3270 Enhancements
Express Logon Feature
Documentation Updates

IBM Communications Server for OS/2 Warp Publications web page: http://www.ibm.com/software/network/commserver/library/publications/csos2.html

Communications Server for NT and Windows 2000 references:

IBM Communications Server for Windows NT 6.1.1, *Readme* file

IBM Communications Server for Windows NT and Windows 2000 Publications web page: http://www.ibm.com/software/network/commserver/library/publications/csnt.html

Communications Server for OS/390 references:

OS/390 IBM Communications Server: IP Migration, Version 2 Release 10, (SC31-8512-05) at http://www.ibm.com/s390/os390/bkserv

OS/390 IBM Communications Server Express Logon Feature User's Guide, Version 2 Release 10 at
http://www.ibm.com/software/network/commserver/library/whitepapers/csos390.html

OS/390 references:

OS/390 System Secure Sockets Layer Programming Guide and Reference, (SC24-5877-03) at http://www.ibm.com/s390/os390/bkserv

OS/390 SecureWay Security Server (RACF) Security Administrator's Guide, (SC28-1915-07) at http://www.ibm.com/s390/os390/bkserv

OS/390 SecureWay Security Server (RACF) Command Language Reference, (SC28-1919-07) at http://www.ibm.com/s390/os390/bkserv

Host On-Demand references:

IBM WebSphere® Host On-Demand V5, online help

IBM WebSphere Host On-Demand product web page: http://www.ibm.com/software/webservers/hostondemand

IBM WebSphere Host On-Demand product library web page: http://www.ibm.com/software/webservers/hostondemand/library.html

Return to Contents

Notices, Copyright, and Trademarks

This document may refer to products that are announced but currently unavailable in your country. This document may also refer to products that have not yet been announced in your country. IBM does not make a commitment to make available any unannounced products referred to herein. The final decision to announce products is based on IBM's business and technical judgment.

Every effort has been made to present a fair assessment of the product families discussed in this paper. The opinions and recommendations expressed in this paper are those of the authors, not necessarily those of IBM.

IBM, AIX, CICS, IMS, NetView, OS/2, OS/390, RACF, S/390, SecureWay, and VTAM are trademarks or registered trademarks of International Business Machines Corporation and/or its subsidiaries.

Java is a trademark of Sun Microsystems, Inc.

Netscape is a trademark of Netscape Communcations Corporation.

Windows and Windows NT are trademarks of Microsoft® Corporation.

All other product names are trademarks or registered trademarks of their respective owners.

Return to Contents