IBM Software Group
Enterprise Networking Solutions (ENS) and Transaction Processing Facility (TPF)

Configuring Telnet and FTP Workloads with Application Transparent Transport Layer Security (AT-TLS)

Alfred B Christensen - alfredch@us.ibm.com
IBM Software Group, Enterprise Networking Solutions, Raleigh

IBM Systems

Trademarks and notices

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

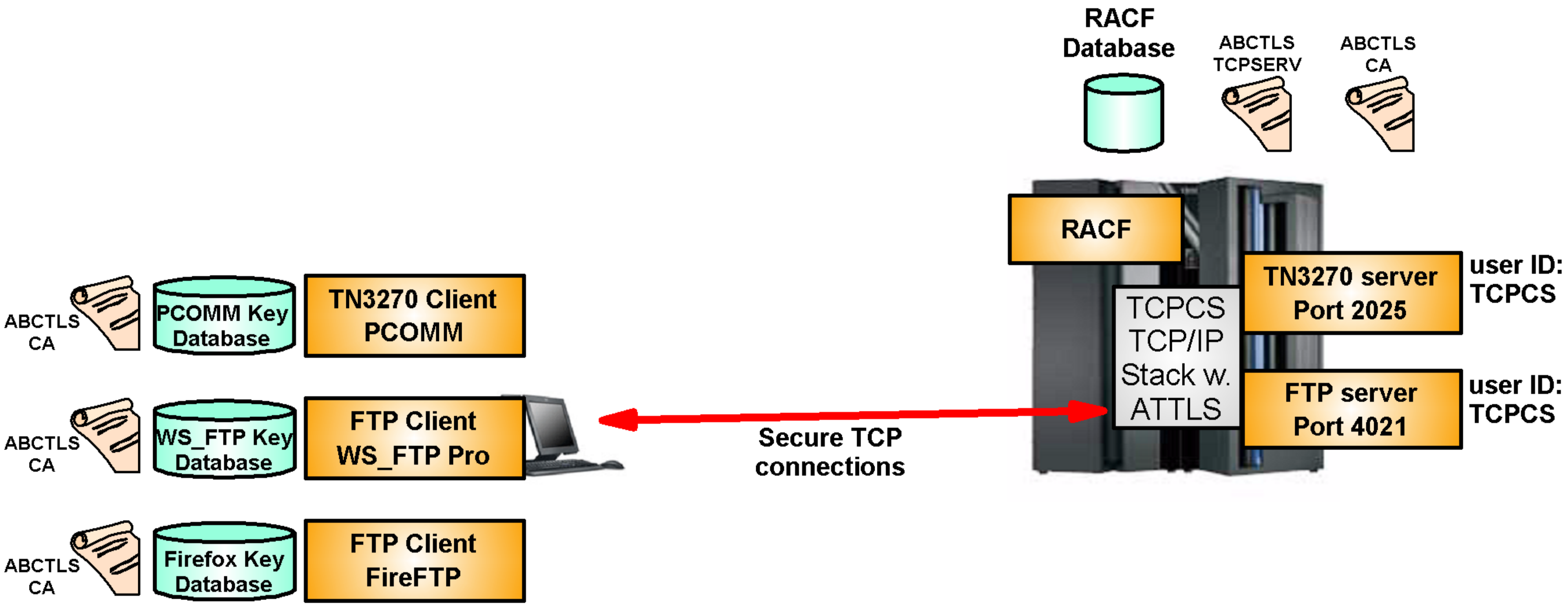
- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM (logo)®
- IBM®
- IMS
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x
- System z
- System z9
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Refer to www.ibm.com/legal/us for further legal information.

ATTLS sample scenario overview

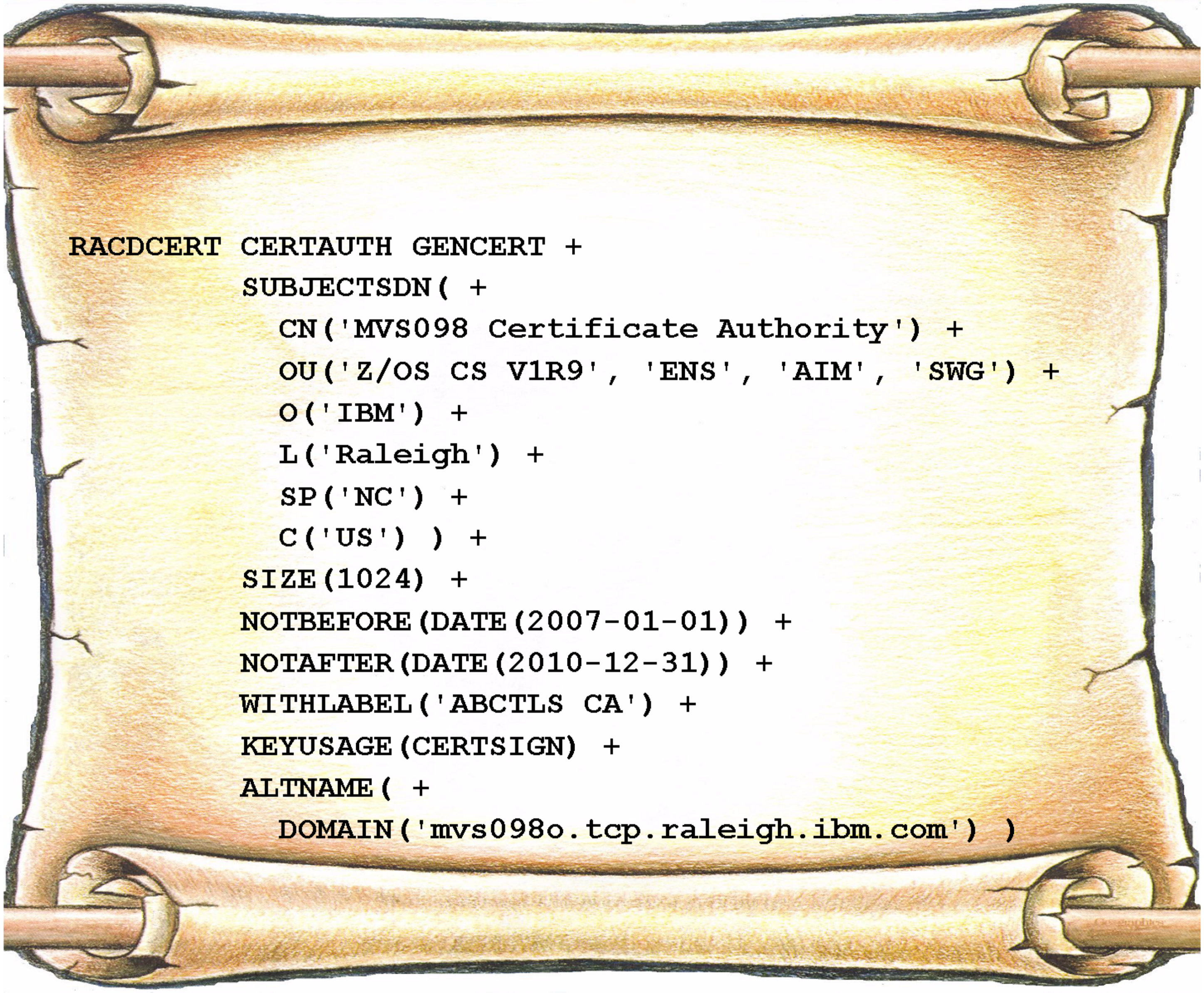


- **Scenario scope:**
  - All SSL/TLS processing done by ATTLS
  - Server authentication only
  - Server certificate signed by self-signed root certificate
  - PCOMM used as secure TN3270 client
  - Ipswitch WS_FTP Pro 2007 used as secure FTP client
  - FireFTP secure FTP client also used as secure FTP client

Task outline

1. Create self-signed root certificate in RACF
2. Create server key-ring and certificate signed by the root certificate
3. Distribute root certificate to client key rings
4. Define ATTLS policy with the Configuration Assistant
5. Transfer policy definition file to z/OS and enable Policy Agent
6. Set up the TN3270 server port as a TTLSPORT
7. Set up the FTP server port with TLSMECHANISM ATTLS
8. Set up TN3270 client keyring and configure a secure TN3270 connection
9. Set up WS_FTP Pro client keyring and configure a secure FTP session
10. Set up Firefox client keyring and configure a secure FireFTP FTP session

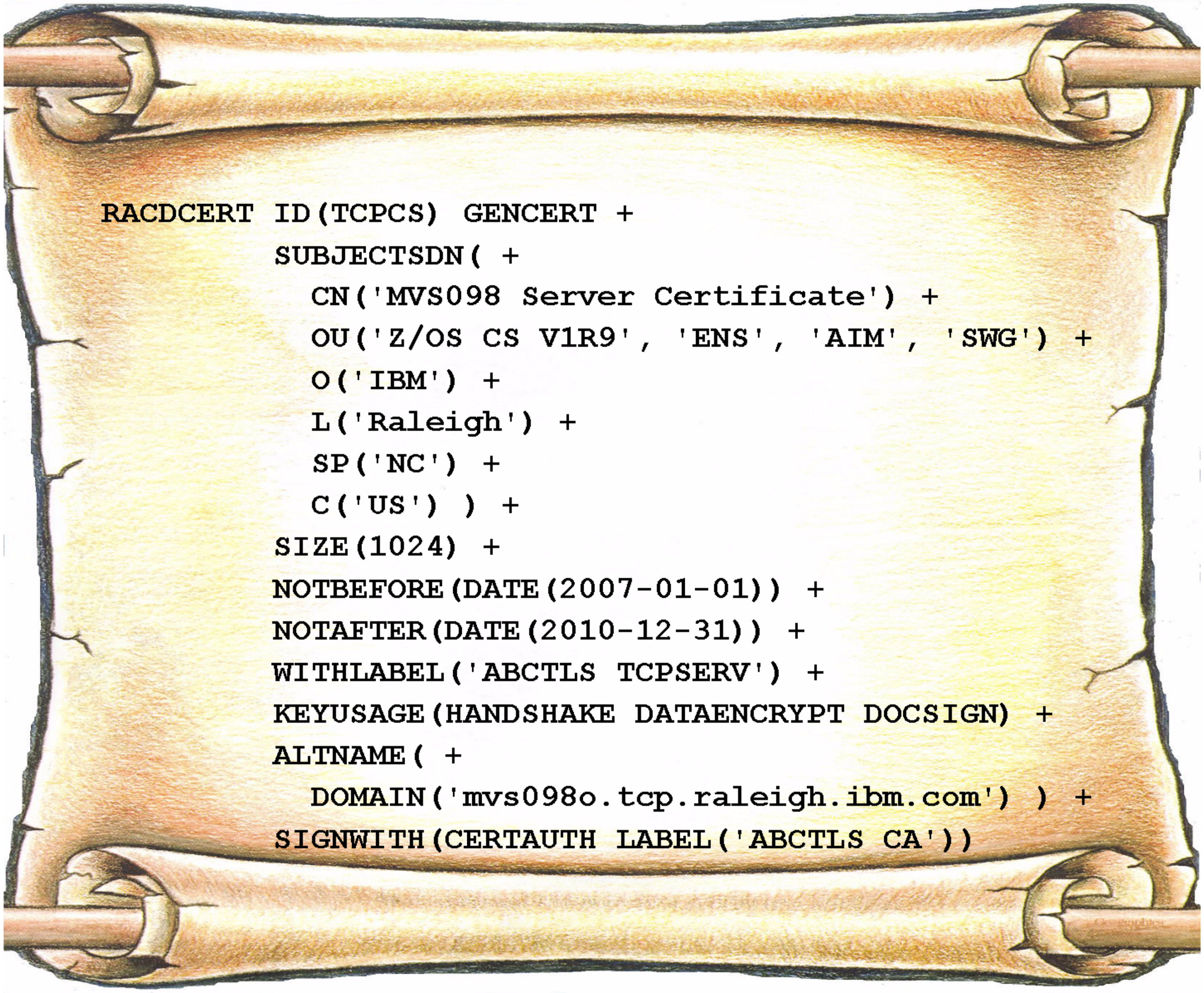
Prepare RACF - part 1/3



```
RACDCERT CERTAUTH GENCERT +
         SUBJECTSDN( +
           CN('MVS098 Certificate Authority') +
           OU('Z/OS CS V1R9', 'ENS', 'AIM', 'SWG') +
           O('IBM') +
           L('Raleigh') +
           SP('NC') +
           C('US') ) +
         SIZE(1024) +
         NOTBEFORE(DATE(2007-01-01)) +
         NOTAFTER(DATE(2010-12-31)) +
         WITHLABEL('ABCTLS CA') +
         KEYUSAGE(CERTSIGN) +
         ALTNAME( +
           DOMAIN('mvs098o.tcp.raleigh.ibm.com') )
```

- Create a Certificate Authority (CA) key pair and self-signed certificate - also known as a root certificate.
- If you are not setting yourself up as a Certificate Authority, you can skip this step

Prepare RACF - part 2/3



```
RACDCERT ID(TCPCS) GENCERT +
         SUBJECTSDN( +
           CN('MVS098 Server Certificate') +
           OU('Z/OS CS V1R9', 'ENS', 'AIM', 'SWG') +
           O('IBM') +
           L('Raleigh') +
           SP('NC') +
           C('US') ) +
         SIZE(1024) +
         NOTBEFORE(DATE(2007-01-01)) +
         NOTAFTER(DATE(2010-12-31)) +
         WITHLABEL('ABCTLS TCPSERV') +
         KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN) +
         ALTNAME( +
           DOMAIN('mvs098o.tcp.raleigh.ibm.com') ) +
         SIGNWITH(CERTAUTH LABEL('ABCTLS CA'))
```

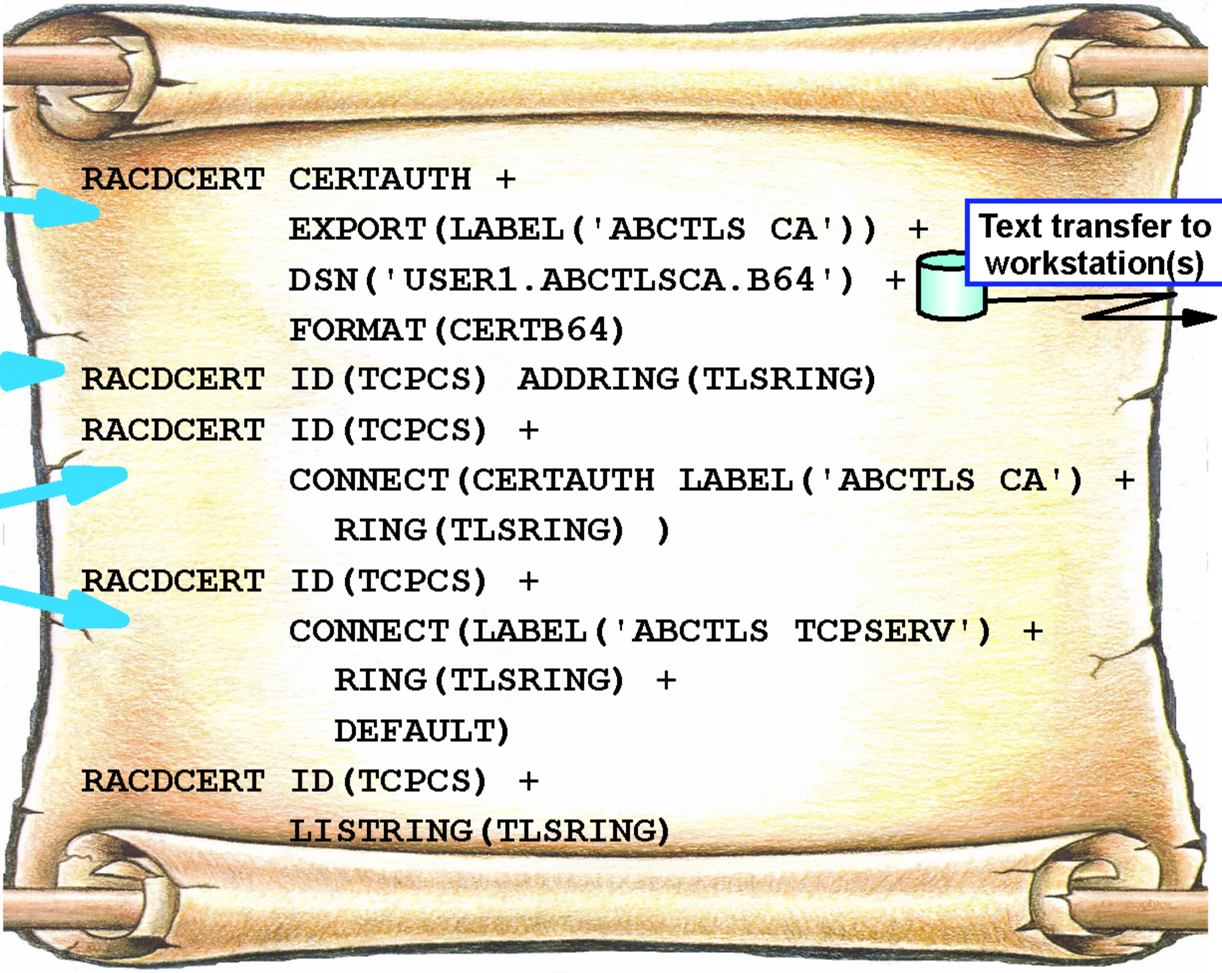
- Create a key pair and a server certificate - signed by your root certificate.
- Or, if you are using another CA, create a key pair and a certificate request, send it to your CA, and receive the signed certificate into RACF

Prepare RACF - part 3/3

- Export the root certificate into a transportable Base64-encoded file

- Create a server keyring under the server started task user ID

- Connect both the root certificate and the server certificate to that keyring



```
RACDCERT CERTAUTH +
         EXPORT(LABEL('ABCTLS CA')) +
         DSN('USER1.ABCTLSCA.B64') +
         FORMAT(CERTB64)
RACDCERT ID(TCPCS) ADDRING(TLSRING)
RACDCERT ID(TCPCS) +
         CONNECT(CERTAUTH LABEL('ABCTLS CA') +
           RING(TLSRING) )
RACDCERT ID(TCPCS) +
         CONNECT(LABEL('ABCTLS TCPSERV') +
           RING(TLSRING) +
           DEFAULT)
RACDCERT ID(TCPCS) +
         LISTRING(TLSRING)
```

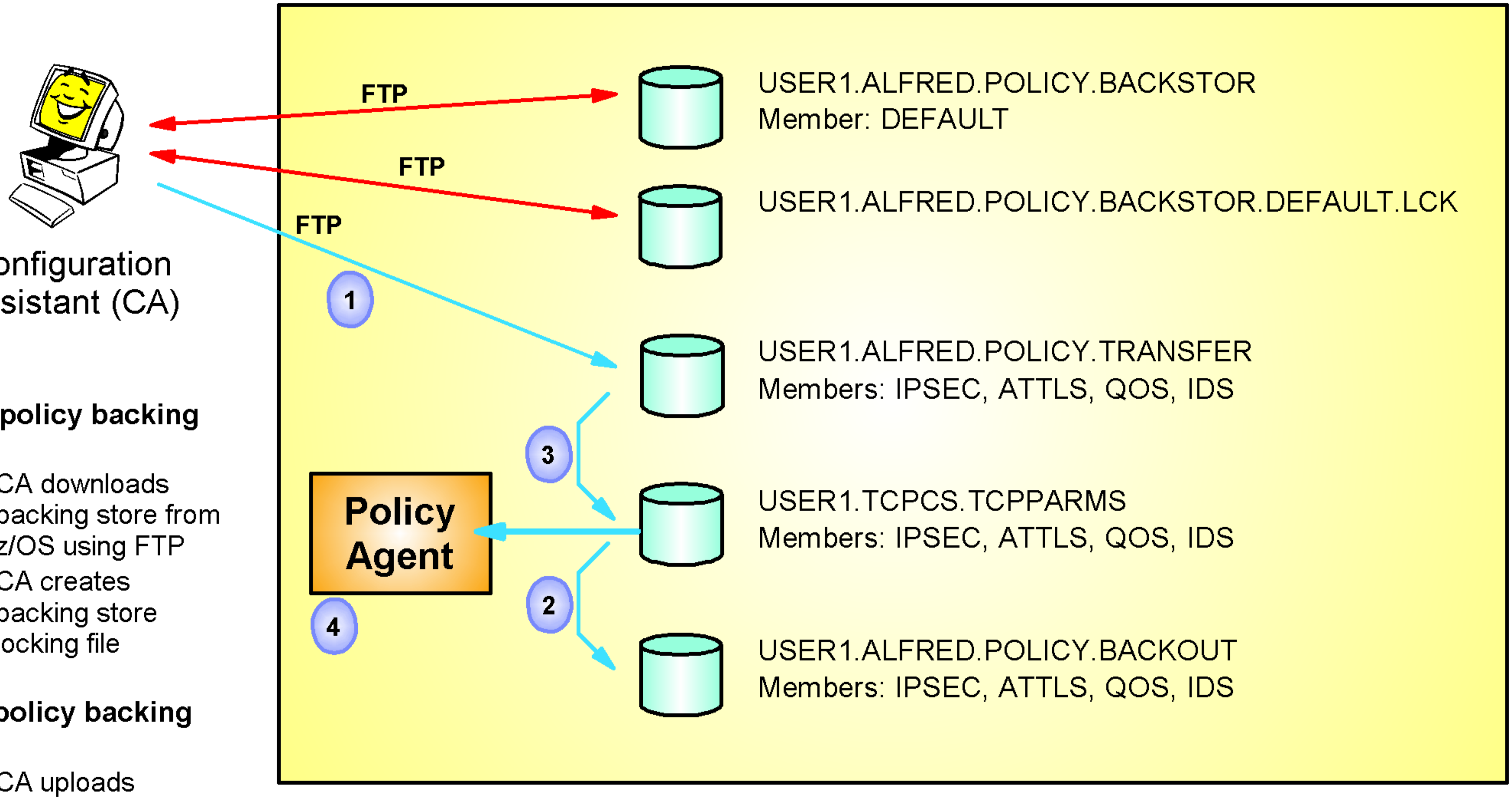
Text transfer to workstation(s)

```
Digital ring information for
user TCPCS:

  Ring:
       >TLSRING<
  Certificate Label Name                Cert Owner     USAGE      DEFAULT
  --------------------------------      ------------   --------   -------
  ABCTLS CA                             CERTAUTH       CERTAUTH     NO

  ABCTLS TCPSERV                        ID(TCPCS)      PERSONAL     YES
```

Configuration Assistant and Policy Agent - one example of a data set structure to support a policy environment


Configuration Assistant (CA)
FTP
FTP
FTP
1
USER1.ALFRED.POLICY.BACKSTOR
Member: DEFAULT
USER1.ALFRED.POLICY.BACKSTOR.DEFAULT.LCK
USER1.ALFRED.POLICY.TRANSFER
Members: IPSEC, ATTLS, QOS, IDS
3
USER1.TCPCS.TCPPARMS
Members: IPSEC, ATTLS, QOS, IDS
Policy Agent
4
2
USER1.ALFRED.POLICY.BACKOUT
Members: IPSEC, ATTLS, QOS, IDS

Open policy backing store:

1. CA downloads backing store from z/OS using FTP
2. CA creates backing store locking file

Save policy backing store:

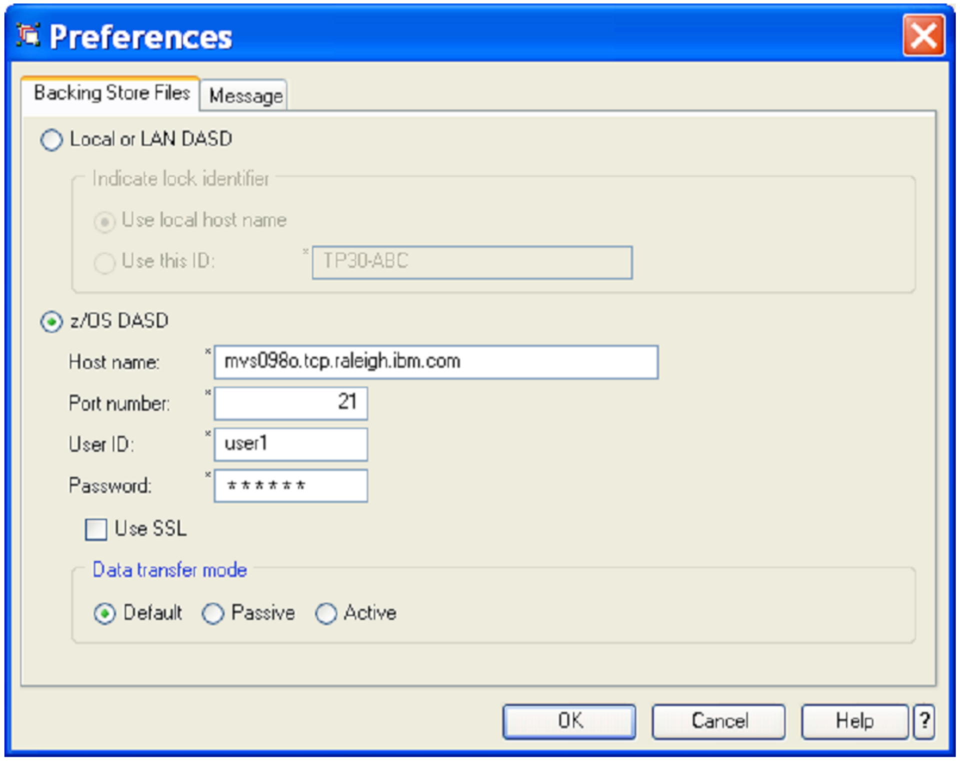
1. CA uploads updated backing store to z/OS using FTP
2. CA removes backing store locking file

1. Generate new policy flat file in CA and FTP it to z/OS (staging library)
2. Backup current production policy flat file
3. Copy new policy flat file into production
4. Modify Policy Agent for REFRESH

Policy backing store file on z/OS as a member of a PDS(E)

Select

1. "File"
2. "Preferences"



Preferences

Backing Store Files | Message

○ Local or LAN DASD

Indicate lock identifier

● Use local host name

○ Use this ID: * TP30-ABC

● z/OS DASD

Host name: * mvs098o.tcp.raleigh.ibm.com

Port number: * 21

User ID: * user1

Password: * ******

□ Use SSL

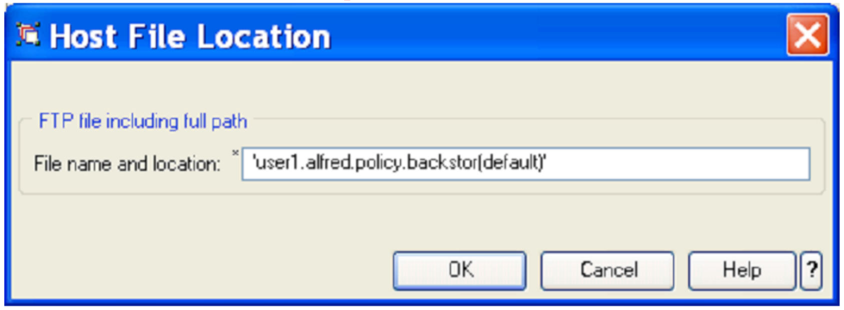
Data transfer mode

● Default ○ Passive ○ Active

The configuration assistant can be configured to access the backing store file via FTP transfers during open and save operations.

Select

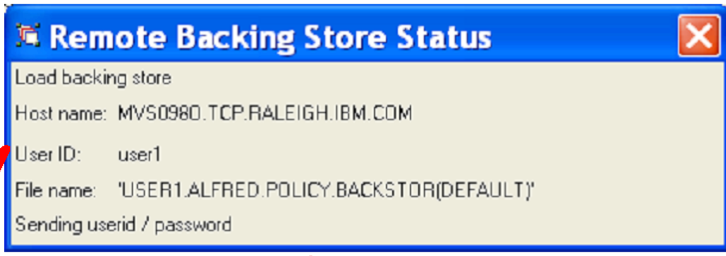
1. "File"
2. "Open"
3. "Open Existing Backing Store"



Host File Location

FTP file including full path

File name and location: * 'user1.alfred.policy.backstor(default)'



Remote Backing Store Status

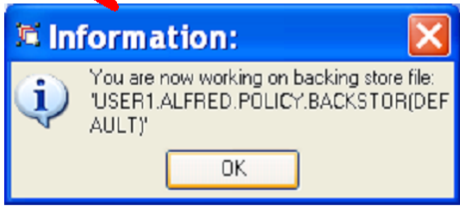
Load backing store

Host name: MVS098O.TCP.RALEIGH.IBM.COM

User ID: user1

File name: 'USER1.ALFRED.POLICY.BACKSTOR(DEFAULT)'

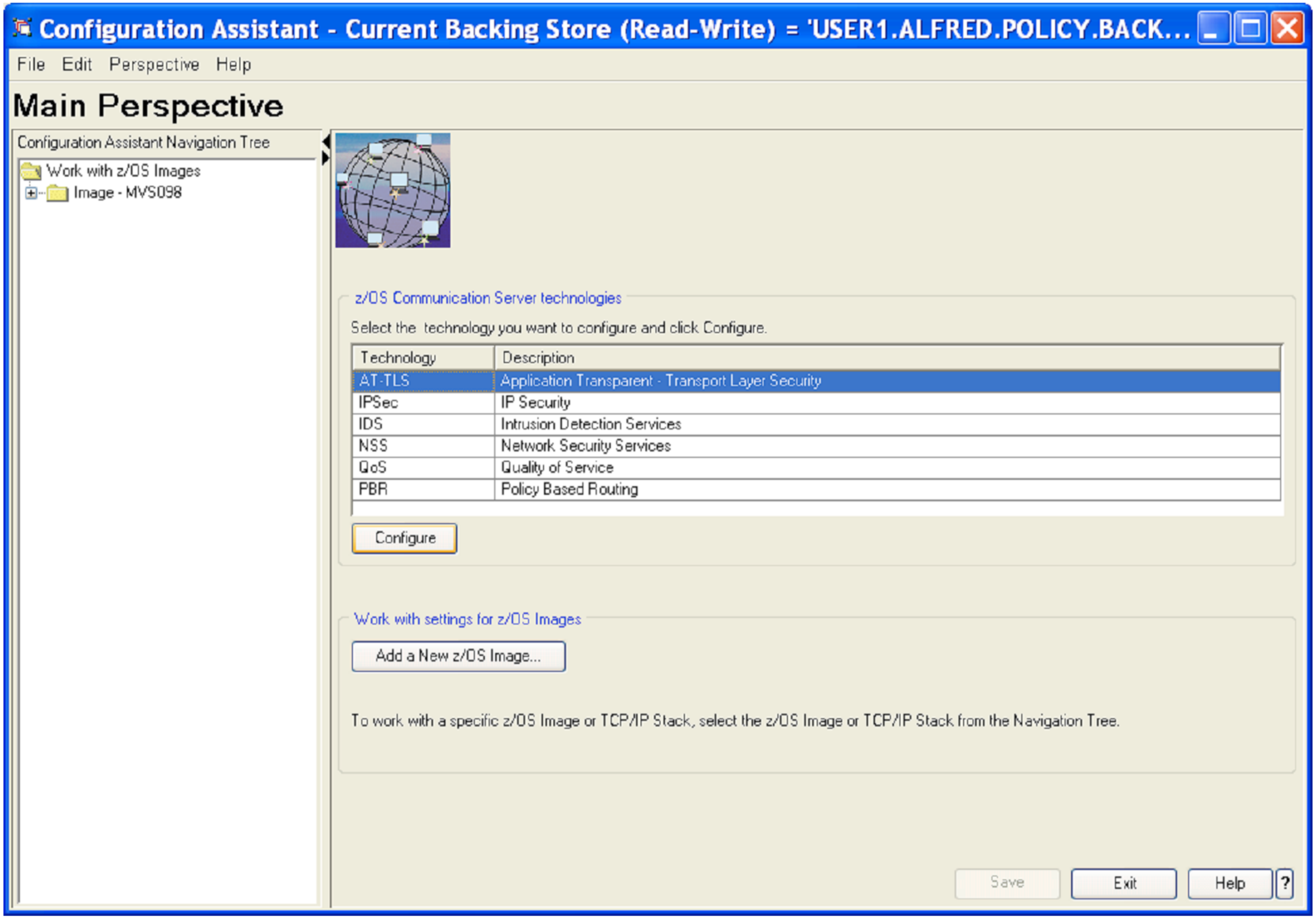
Sending userid / password



Information:

You are now working on backing store file: 'USER1.ALFRED.POLICY.BACKSTOR(DEFAULT)'

Start configuring AT-TLS


Configuration Assistant - Current Backing Store (Read-Write) = 'USER1.ALFRED.POLICY.BACK...
File Edit Perspective Help
Configuration Assistant Navigation Tree
Work with z/OS Images
Image - MVS098
Configure
Add a New z/OS Image...
Save
Exit
Help
?

Main Perspective

z/OS Communication Server technologies

Select the technology you want to configure and click Configure.

Technology	Description
AT-TLS	Application Transparent - Transport Layer Security
IPSec	IP Security
IDS	Intrusion Detection Services
NSS	Network Security Services
QoS	Quality of Service
PBR	Policy Based Routing

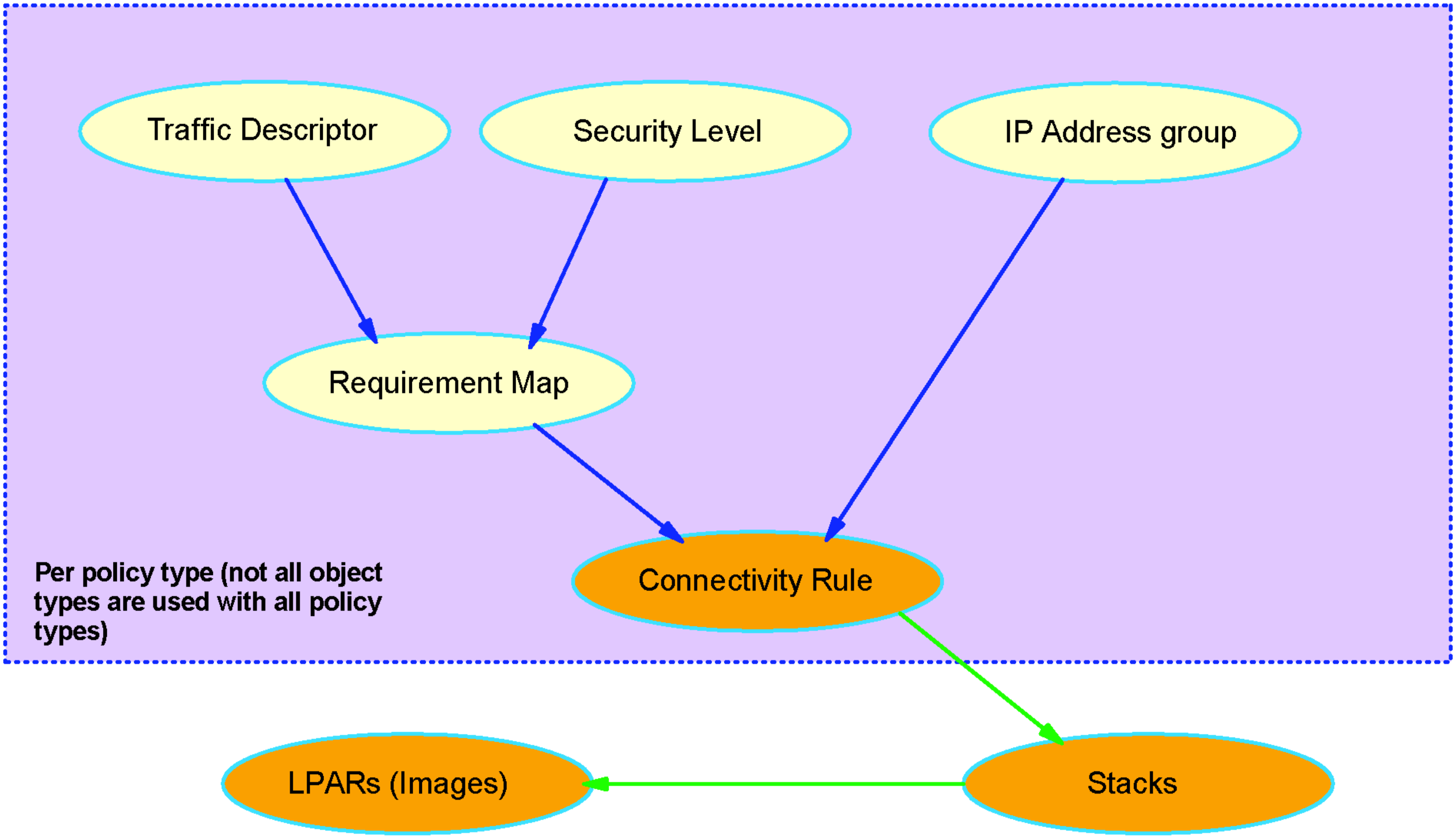
Work with settings for z/OS Images

To work with a specific z/OS Image or TCP/IP Stack, select the z/OS Image or TCP/IP Stack from the Navigation Tree.

I will not go through all aspects of a CA dialog, but will focus on how to configure AT-TLS policies.

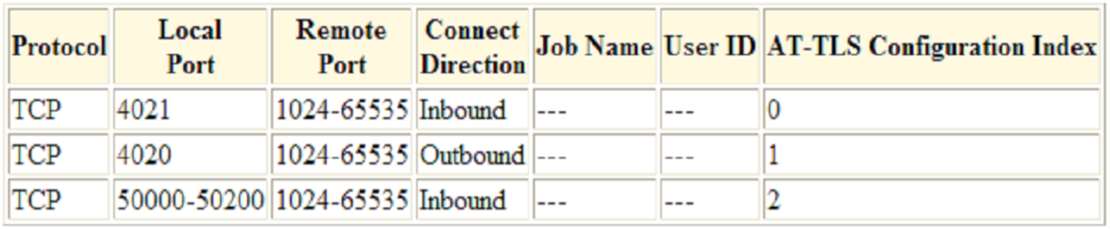
- **Steps not shown:**
  - Create an image (an LPAR)
  - Create a stack on that image

Quick Guide to working with the Configuration Assistant objects - ATTLS example

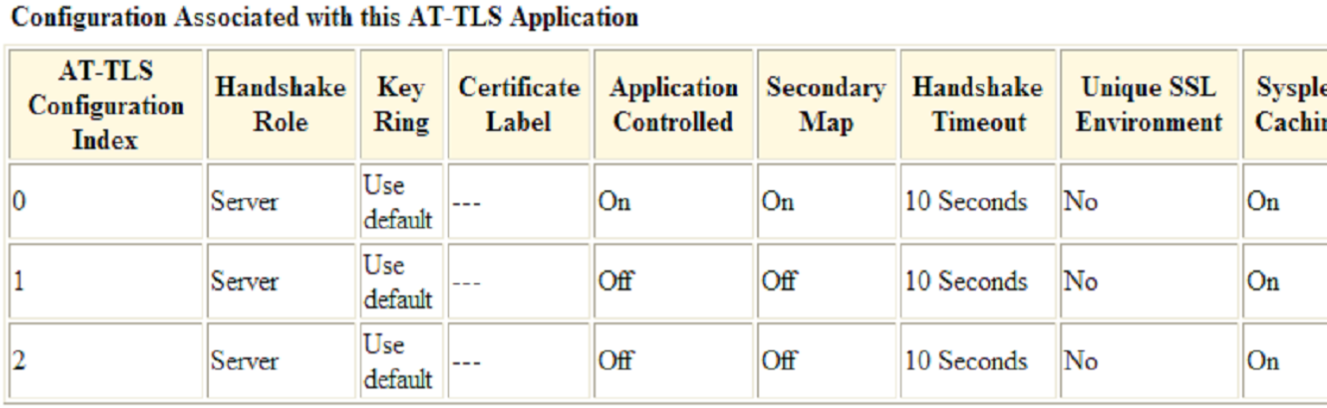


Quick Guide to working with the Configuration Assistant objects - ATTLS example

- **Traffic Descriptor:**
  - Identifies a specific type of application network traffic
  - Based on protocol (TCP/UDP), local and/or remote ports, connection direction, z/OS jobname, etc.
  - A traffic descriptor does not refer to IP addresses
  - IBM provides a long list of traffic descriptors for different types of network traffic
  - Reuseable across LPARs and stacks in the same backing store file
    - But not reuseable across policy technologies
    - Each policy technology has unique attributes per traffic descriptor



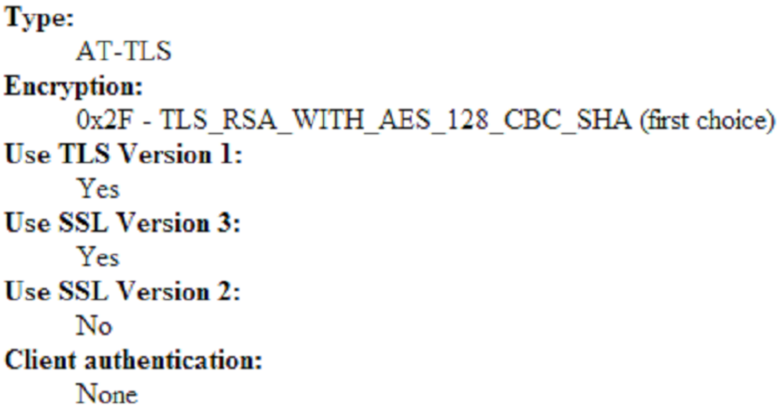
Protocol	Local Port	Remote Port	Connect Direction	Job Name	User ID	AT-TLS Configuration Index
TCP	4021	1024-65535	Inbound	---	---	0
TCP	4020	1024-65535	Outbound	---	---	1
TCP	50000-50200	1024-65535	Inbound	---	---	2



Configuration Associated with this AT-TLS Application

AT-TLS Configuration Index	Handshake Role	Key Ring	Certificate Label	Application Controlled	Secondary Map	Handshake Timeout	Unique SSL Environment	Sysple Cachi
0	Server	Use default	---	On	On	10 Seconds	No	On
1	Server	Use default	---	Off	Off	10 Seconds	No	On
2	Server	Use default	---	Off	Off	10 Seconds	No	On

- **Security Level:**
  - Identifies the SSL/TLS security requirements, such as ciphersuites, allowed protocol versions (SSLv2, SSLv3, TLSv1), etc.
  - Reuseable across LPARs and stacks in the same backing store file
    - But not reuseable across policy technologies

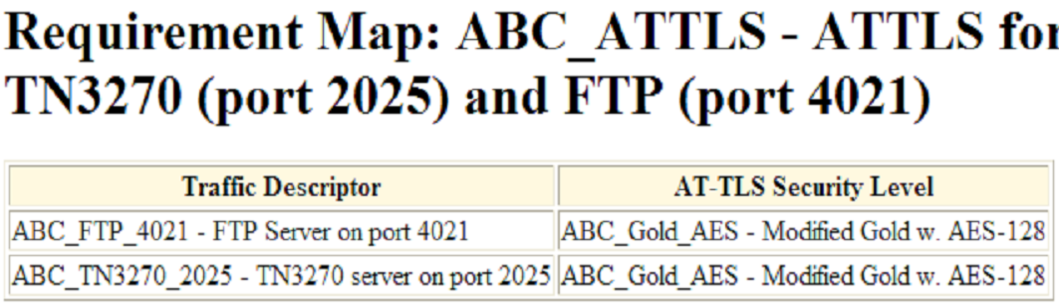


Type:
AT-TLS
Encryption:
0x2F - TLS_RSA_WITH_AES_128_CBC_SHA (first choice)
Use TLS Version 1:
Yes
Use SSL Version 3:
Yes
Use SSL Version 2:
No
Client authentication:
None

Quick Guide to working with the Configuration Assistant objects - ATTLS example

Requirement Map

- Identifies what type of processing you want applied to your traffic descriptors
- Specific requirements are policy-type dependent
  - For ATT-TLS policies, you define security levels and then you use a requirement map to tie your traffic descriptors to those security levels
  - Reuseable across LPARs and stacks in the same backing store file
    - But not reuseable across policy technologies

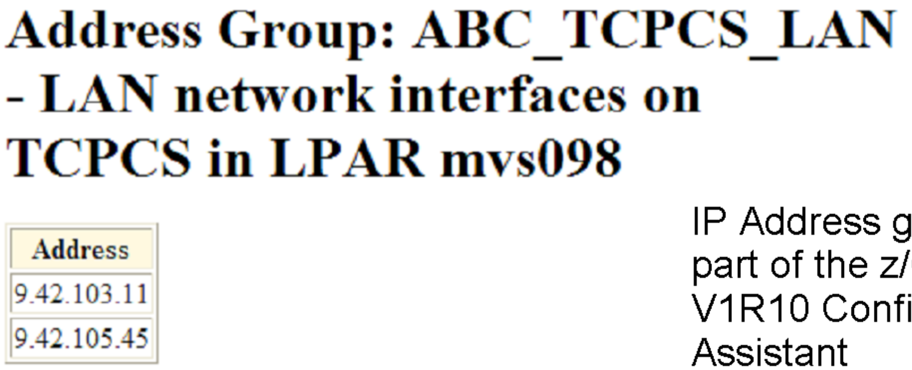


Requirement Map: ABC_ATTLS - ATTLS fo TN3270 (port 2025) and FTP (port 4021)

Traffic Descriptor	AT-TLS Security Level
ABC_FTP_4021 - FTP Server on port 4021	ABC_Gold_AES - Modified Gold w. AES-128
ABC_TN3270_2025 - TN3270 server on port 2025	ABC_Gold_AES - Modified Gold w. AES-128

IP Address Groups

- Group IP addresses that need the same treatment
  - For example all VIPA addresses, or all real network interface addresses
- Simplifies creation of connectivity rules
- Reuseable across LPARs and stacks in the same backing store file
  - But not reuseable across policy technologies



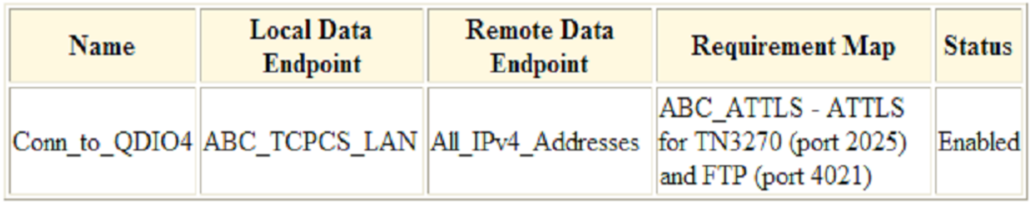
Address Group: ABC_TCPCS_LAN - LAN network interfaces on TCPCS in LPAR mvs098

Address
9.42.103.11
9.42.105.45

IP Address groups ar part of the z/OS V1R10 Configuration Assistant

Connectivity Rule

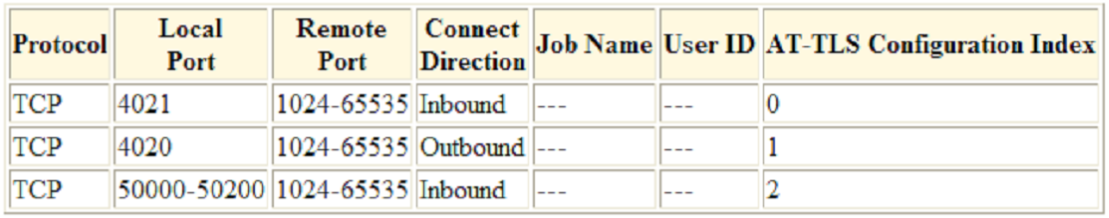
- Here is where IP addresses come into the picture
- Connectivity rules are stack-specific and ties IP addresses to requirement maps
  - And by that, type of processing to traffic descriptors
- Either individual IP addresses or groups of IP addresses



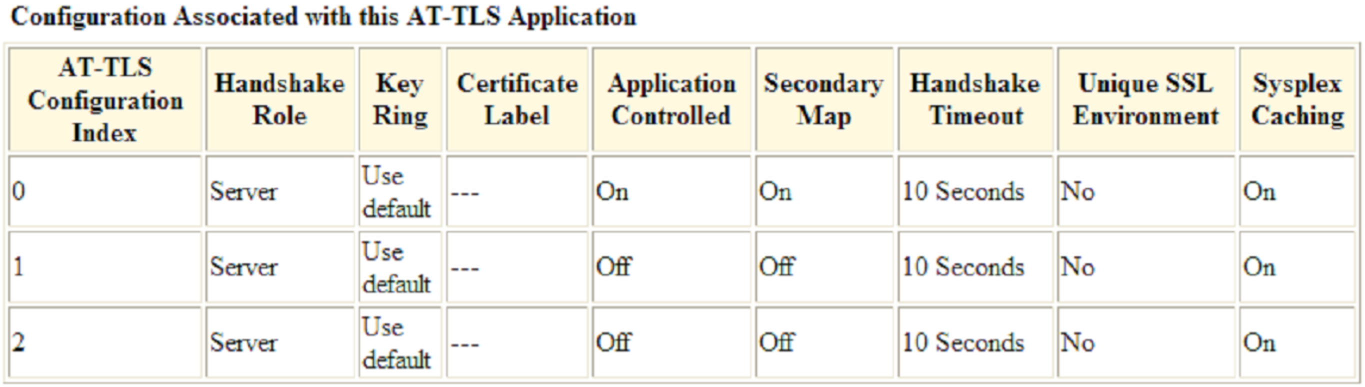
Name	Local Data Endpoint	Remote Data Endpoint	Requirement Map	Status
Conn_to_QDIO4	ABC_TCPCS_LAN	All_IPv4_Addresses	ABC_ATTLS - ATTLS for TN3270 (port 2025) and FTP (port 4021)	Enabled

Some basic concepts for defining AT-TLS policies

- **Traffic Descriptor:**
  - Identifies certain types of traffic by means of transport protocol (TCP or UDP), local and remote port numbers, for TCP the direction of the connection setup, etc.
  - Specific AT-TLS attributes for this type of application
  - A traffic descriptor does not include references to IP addresses in any form!



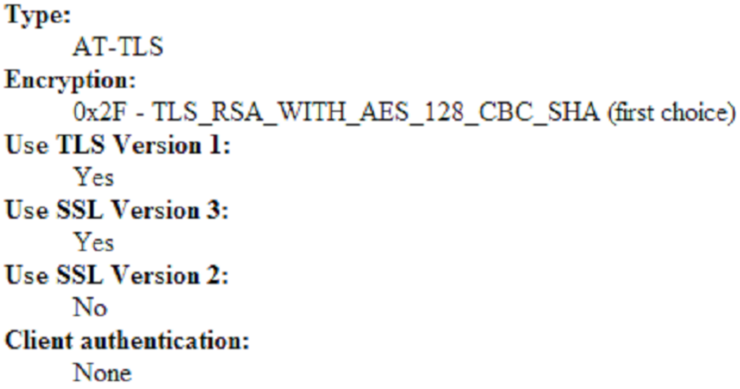
Protocol	Local Port	Remote Port	Connect Direction	Job Name	User ID	AT-TLS Configuration Index
TCP	4021	1024-65535	Inbound	---	---	0
TCP	4020	1024-65535	Outbound	---	---	1
TCP	50000-50200	1024-65535	Inbound	---	---	2



Configuration Associated with this AT-TLS Application

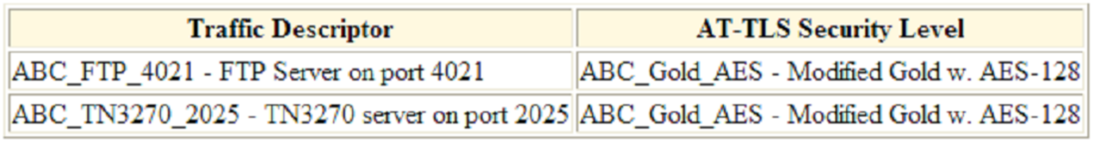
AT-TLS Configuration Index	Handshake Role	Key Ring	Certificate Label	Application Controlled	Secondary Map	Handshake Timeout	Unique SSL Environment	Sysplex Caching
0	Server	Use default	---	On	On	10 Seconds	No	On
1	Server	Use default	---	Off	Off	10 Seconds	No	On
2	Server	Use default	---	Off	Off	10 Seconds	No	On

- **Security Level:**
  - Identifies the SSL/TLS security requirements, such as ciphersuites, allowed protocol versions (SSLv2, SSLv3, TLSv1), etc.



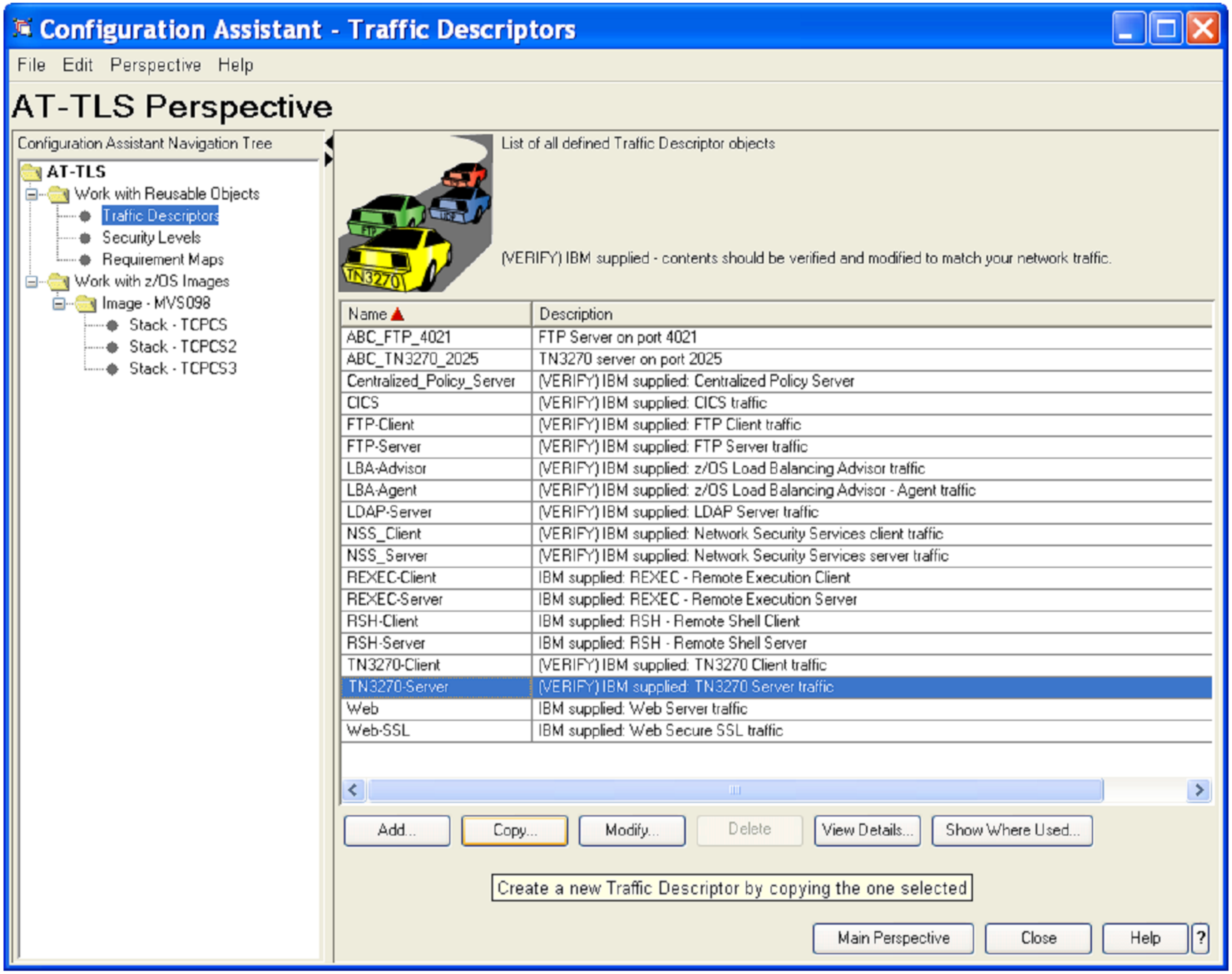
Type:
AT-TLS
Encryption:
0x2F - TLS_RSA_WITH_AES_128_CBC_SHA (first choice)
Use TLS Version 1:
Yes
Use SSL Version 3:
Yes
Use SSL Version 2:
No
Client authentication:
None

- **Requirement Map:**
  - Links traffic descriptors to security levels.



Traffic Descriptor	AT-TLS Security Level
ABC_FTP_4021 - FTP Server on port 4021	ABC_Gold_AES - Modified Gold w. AES-128
ABC_TN3270_2025 - TN3270 server on port 2025	ABC_Gold_AES - Modified Gold w. AES-128

Start working with your traffic descriptors



List of all defined Traffic Descriptor objects

(VERIFY) IBM supplied - contents should be verified and modified to match your network traffic.

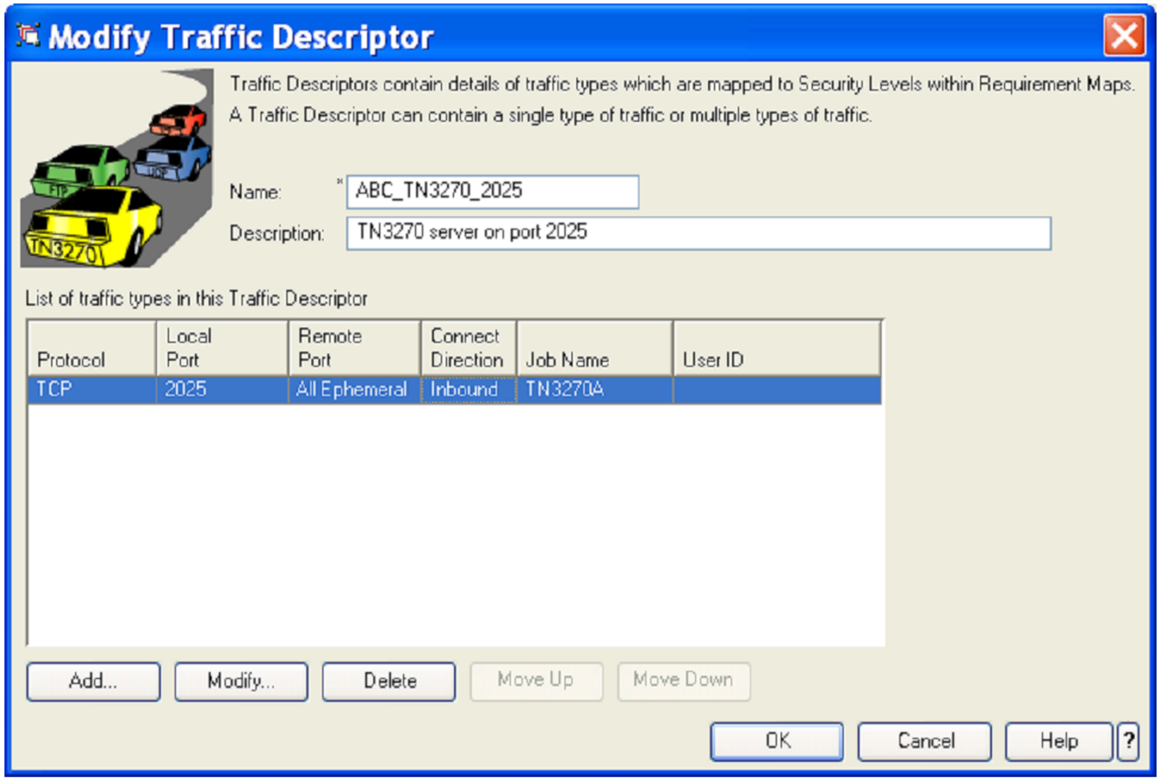
Name ▲	Description
ABC_FTP_4021	FTP Server on port 4021
ABC_TN3270_2025	TN3270 server on port 2025
Centralized_Policy_Server	(VERIFY) IBM supplied: Centralized Policy Server
CICS	(VERIFY) IBM supplied: CICS traffic
FTP-Client	(VERIFY) IBM supplied: FTP Client traffic
FTP-Server	(VERIFY) IBM supplied: FTP Server traffic
LBA-Advisor	(VERIFY) IBM supplied: z/OS Load Balancing Advisor traffic
LBA-Agent	(VERIFY) IBM supplied: z/OS Load Balancing Advisor - Agent traffic
LDAP-Server	(VERIFY) IBM supplied: LDAP Server traffic
NSS_Client	(VERIFY) IBM supplied: Network Security Services client traffic
NSS_Server	(VERIFY) IBM supplied: Network Security Services server traffic
REXEC-Client	IBM supplied: REXEC - Remote Execution Client
REXEC-Server	IBM supplied: REXEC - Remote Execution Server
RSH-Client	IBM supplied: RSH - Remote Shell Client
RSH-Server	IBM supplied: RSH - Remote Shell Server
TN3270-Client	(VERIFY) IBM supplied: TN3270 Client traffic
TN3270-Server	(VERIFY) IBM supplied: TN3270 Server traffic
Web	IBM supplied: Web Server traffic
Web-SSL	IBM supplied: Web Secure SSL traffic

Create a new Traffic Descriptor by copying the one selected

Use the predefined traffic descriptors to create your own

Select one (for example the TN3270-server) and press COPY

Create a new TN3270 server traffic descriptor based on an existing TN3270 server traffic descriptor



Modify Traffic Descriptor

Traffic Descriptors contain details of traffic types which are mapped to Security Levels within Requirement Maps. A Traffic Descriptor can contain a single type of traffic or multiple types of traffic.

Name: * ABC_TN3270_2025

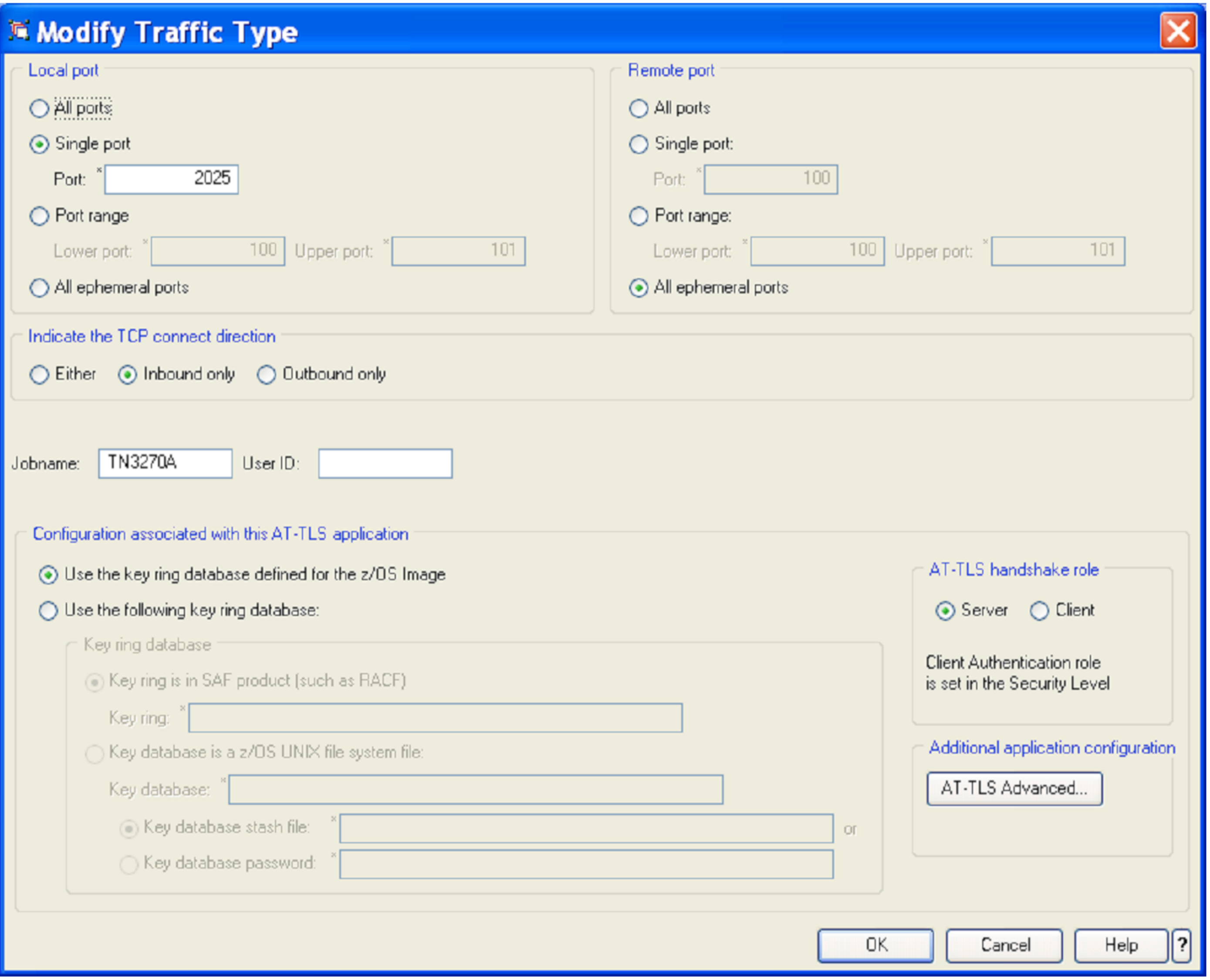
Description: TN3270 server on port 2025

List of traffic types in this Traffic Descriptor

Protocol	Local Port	Remote Port	Connect Direction	Job Name	User ID
TCP	2025	All Ephemeral	Inbound	TN3270A	

- When you copy an existing traffic descriptor, you are required to enter a new name and a description.
- All the attributes of the traffic descriptor you copied are copied into your new traffic descriptor.
- To change these copied attributes, highlight the traffic type and press MODIFY

Add your information to the new TN3270 server traffic descriptor



Modify Traffic Type

Local port

○ All ports
● Single port
Port: * 2025
○ Port range
Lower port: * 100 Upper port: * 101
○ All ephemeral ports

Remote port

○ All ports
○ Single port:
Port: * 100
○ Port range:
Lower port: * 100 Upper port: * 101
● All ephemeral ports

Indicate the TCP connect direction

○ Either ● Inbound only ○ Outbound only

Jobname: TN3270A User ID:

Configuration associated with this AT-TLS application

● Use the key ring database defined for the z/OS Image
○ Use the following key ring database:

Key ring database

● Key ring is in SAF product (such as RACF)
Key ring: *
○ Key database is a z/OS UNIX file system file:
Key database: *
● Key database stash file: * or
○ Key database password: *

AT-TLS handshake role

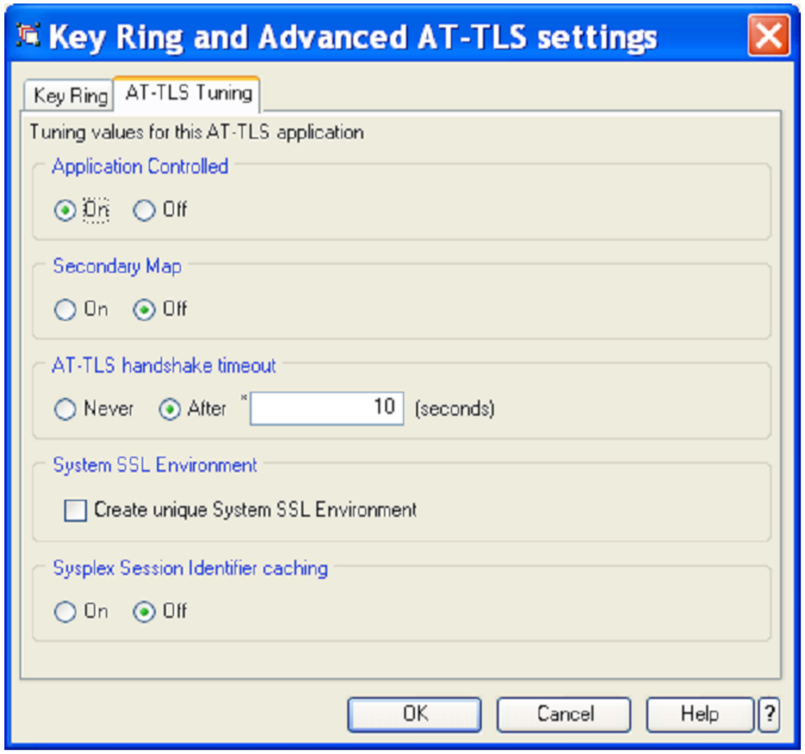
● Server ○ Client

Client Authentication role
is set in the Security Level

Additional application configuration

- Change the server port number to your server port number (2025)
- This policy is for inbound connections to TN3270 server port 2025.
- Server jobname is TN3270A (optional)
- Use the keyring information we've added for the TCP/IP stack
- Server handshake role
- Select Advanced

Application Controlled



Key Ring and Advanced AT-TLS settings

Key Ring | AT-TLS Tuning

Tuning values for this AT-TLS application

Application Controlled: ● On ○ Off

Secondary Map: ○ On ● Off

AT-TLS handshake timeout: ○ Never ● After * 10 (seconds)

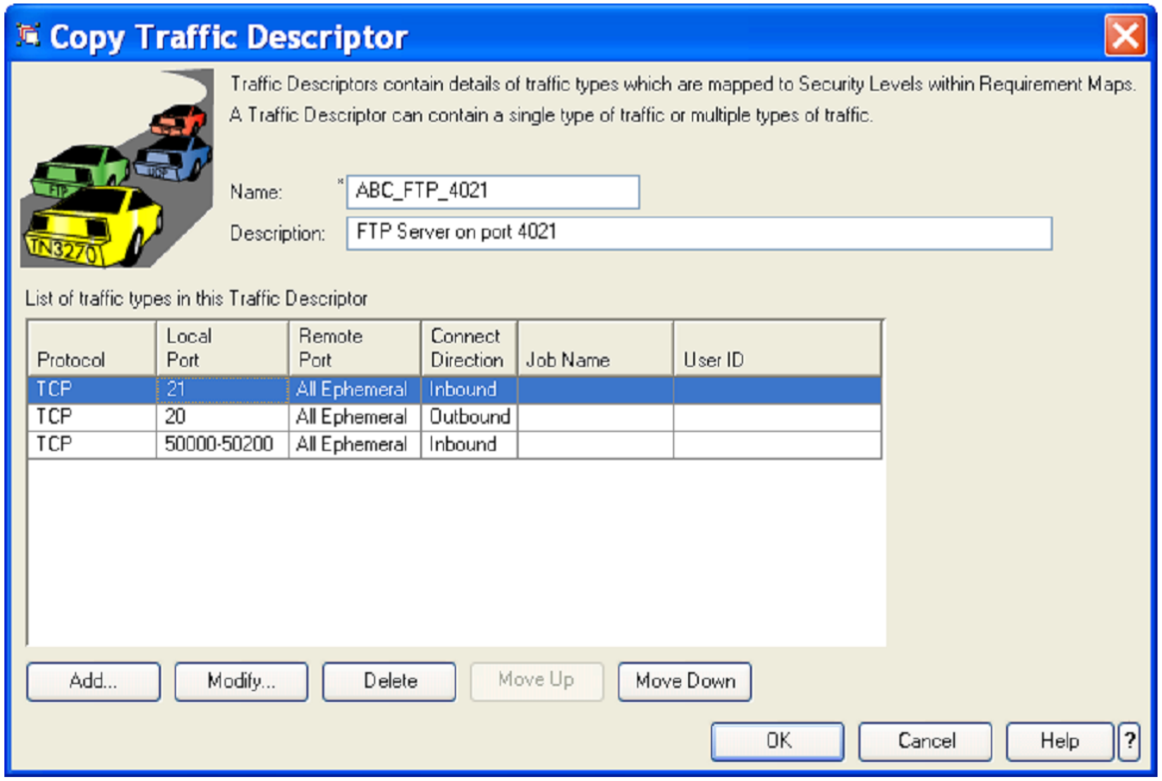
System SSL Environment: □ Create unique System SSL Environment

Sysplex Session Identifier caching: ○ On ● Off

- For a TN3270 server port that is defined as a TTLSPORT, you need to enable TN3270 server control of ATTLS operations
  - The TN3270 server has to be able to tell ATTLS when to start the SSL/TLS handshake - if at all

- Sysplex-caching can improve performance of SSL/TLS handshake in a Sysplex where connections are distributed to multiple LPARs

Create a new FTP server traffic descriptor based on an existing FTP server traffic descriptor



Traffic Descriptors contain details of traffic types which are mapped to Security Levels within Requirement Maps. A Traffic Descriptor can contain a single type of traffic or multiple types of traffic.

Name: * ABC_FTP_4021

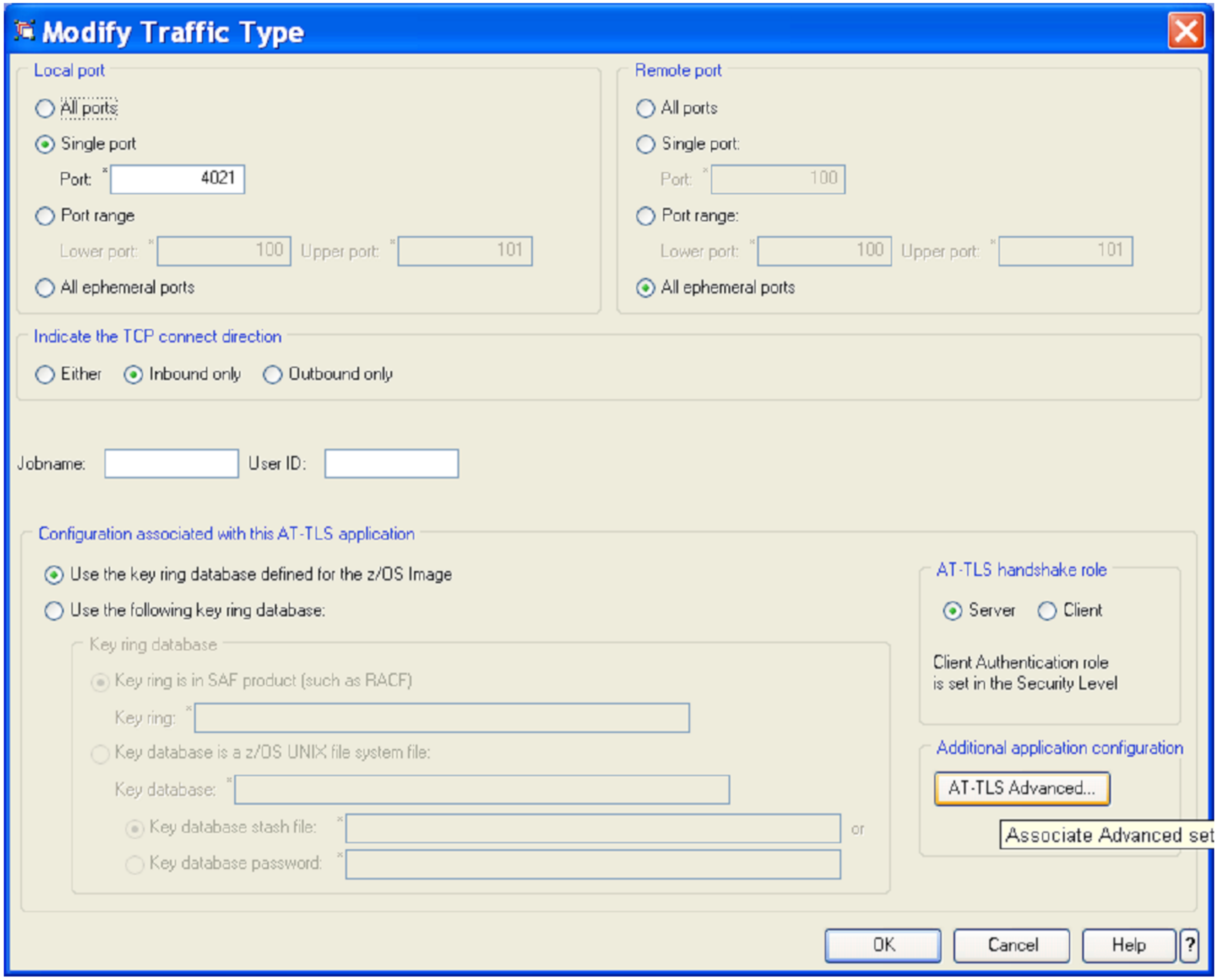
Description: FTP Server on port 4021

List of traffic types in this Traffic Descriptor

Protocol	Local Port	Remote Port	Connect Direction	Job Name	User ID
TCP	21	All Ephemeral	Inbound		
TCP	20	All Ephemeral	Outbound		
TCP	50000-50200	All Ephemeral	Inbound		

- FTP server traffic is more complex than TN3270 server traffic. For FTP, we have three traffic types we need to define policies for:
  - The inbound control connection
  - The outbound active mode data connection
  - The inbound passive mode data connection

The inbound FTP control connection traffic type



Modify Traffic Type

Local port

○ All ports
● Single port
Port: * 4021
○ Port range
Lower port: * 100 Upper port: * 101
○ All ephemeral ports

Remote port

○ All ports
○ Single port:
Port: * 100
○ Port range:
Lower port: * 100 Upper port: * 101
● All ephemeral ports

Indicate the TCP connect direction

○ Either ● Inbound only ○ Outbound only

Jobname: User ID:

Configuration associated with this AT-TLS application

● Use the key ring database defined for the z/OS Image
○ Use the following key ring database:

Key ring database

○ Key ring is in SAF product (such as RACF)
Key ring: *
○ Key database is a z/OS UNIX file system file:
Key database: *
○ Key database stash file: * or
○ Key database password: *

AT-TLS handshake role

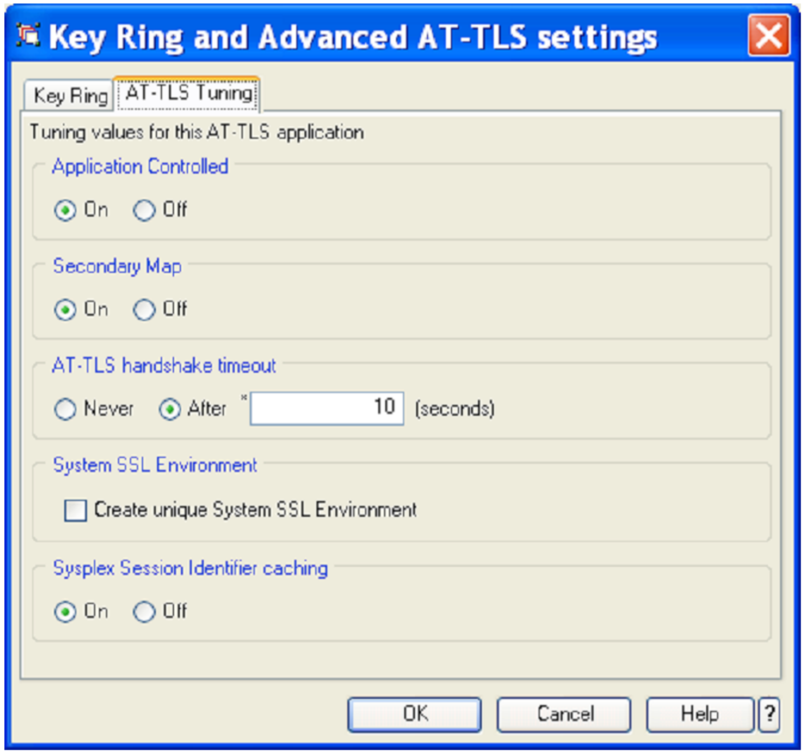
● Server ○ Client

Client Authentication role is set in the Security Level

Additional application configuration

- Server port number for the control connection is port 4021
- Inbound connections
- Use image keyring
- Server handshake role
- Here we also need to set some of the advanced AT-TLS options

Advanced AT-TLS options for inbound control connections to our FTP server



Tuning values for this AT-TLS application

Application Controlled
● On ○ Off

Secondary Map
● On ○ Off

AT-TLS handshake timeout
○ Never ● After * 10 (seconds)

System SSL Environment
□ Create unique System SSL Environment

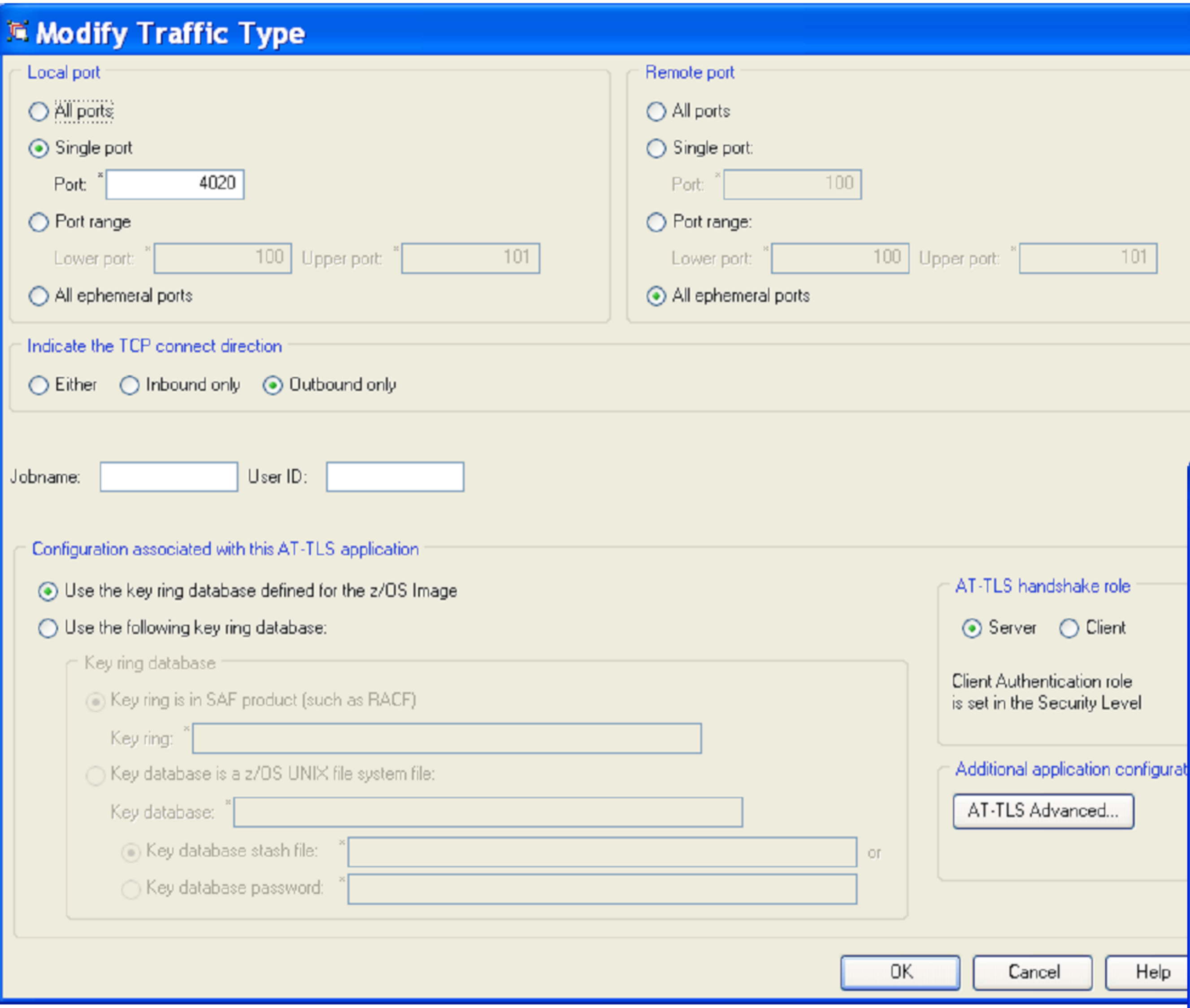
Sysplex Session Identifier caching
● On ○ Off

- FTP in this setup uses the AUTH TLS command exchange to determine if SSL/TLS is to be used. Not all connections to port 4021 need to use SSL/TLS.
  - FTP must tell AT-TLS if/when a connection switches into SSL/TLS mode - AT-TLS use is application controlled

- FTP uses multiple connections per session (one control connection and one or more data connections). Secondary map allows AT-TLS to "tie" them together from an AT-TLS perspective
  - Only one traffic type in a traffic descriptor can use this option

- Sysplex-caching can improve performance of SSL/TLS handshake in a Sysplex where connections are distributed to multiple LPARs

The outbound active mode FTP data connection



Modify Traffic Type

Local port
○ All ports
● Single port
Port: * 4020
○ Port range
Lower port: * 100 Upper port: * 101
○ All ephemeral ports

Remote port
○ All ports
○ Single port:
Port: * 100
○ Port range:
Lower port: * 100 Upper port: * 101
● All ephemeral ports

Indicate the TCP connect direction
○ Either ○ Inbound only ● Outbound only

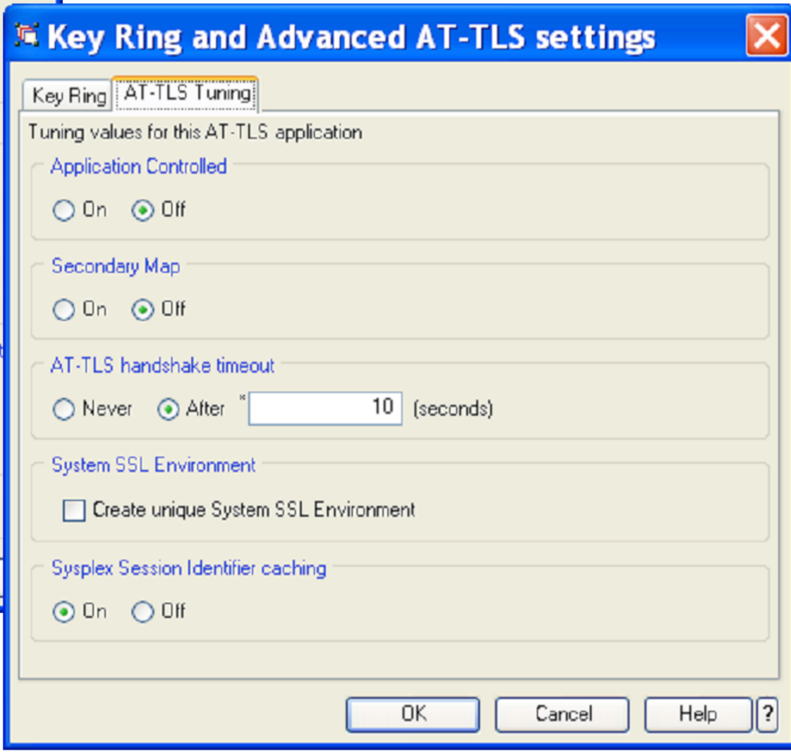
Jobname: User ID:

Configuration associated with this AT-TLS application
● Use the key ring database defined for the z/OS Image
○ Use the following key ring database:
Key ring database
● Key ring is in SAF product (such as RACF)
Key ring: *
○ Key database is a z/OS UNIX file system file:
Key database: *
● Key database stash file: * or
○ Key database password: *

AT-TLS handshake role
● Server ○ Client
Client Authentication role is set in the Security Level

Additional application configurat

The active mode data connections are outbound and come from port 4020.



Key Ring and Advanced AT-TLS settings

Tuning values for this AT-TLS application

Application Controlled
○ On ● Off

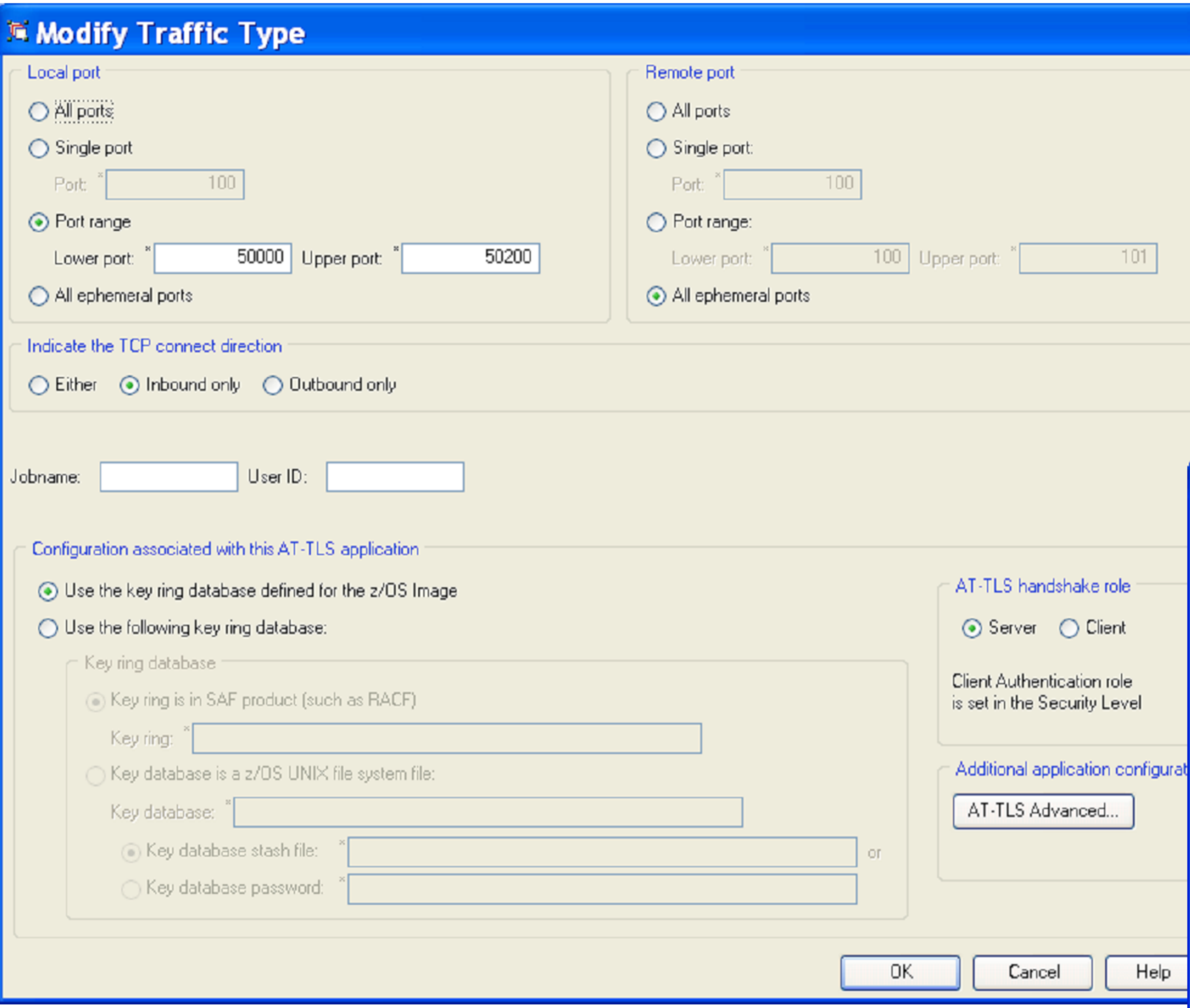
Secondary Map
○ On ● Off

AT-TLS handshake timeout
○ Never ● After * 10 (seconds)

System SSL Environment
□ Create unique System SSL Environment

Sysplex Session Identifier caching
● On ○ Off

The inbound passive mode FTP data connection



Modify Traffic Type

Local port
- ○ All ports
- ○ Single port
  - Port: * 100
- ● Port range
  - Lower port: * 50000 Upper port: * 50200
- ○ All ephemeral ports

Remote port
- ○ All ports
- ○ Single port:
  - Port: * 100
- ○ Port range:
  - Lower port: * 100 Upper port: * 101
- ● All ephemeral ports

Indicate the TCP connect direction

○ Either ● Inbound only ○ Outbound only

Jobname: User ID:

Configuration associated with this AT-TLS application
- ● Use the key ring database defined for the z/OS Image
- ○ Use the following key ring database:
  - Key ring database
    - ● Key ring is in SAF product (such as RACF)
      - Key ring: *
    - ○ Key database is a z/OS UNIX file system file:
      - Key database: *
      - ● Key database stash file: * or
      - ○ Key database password: *

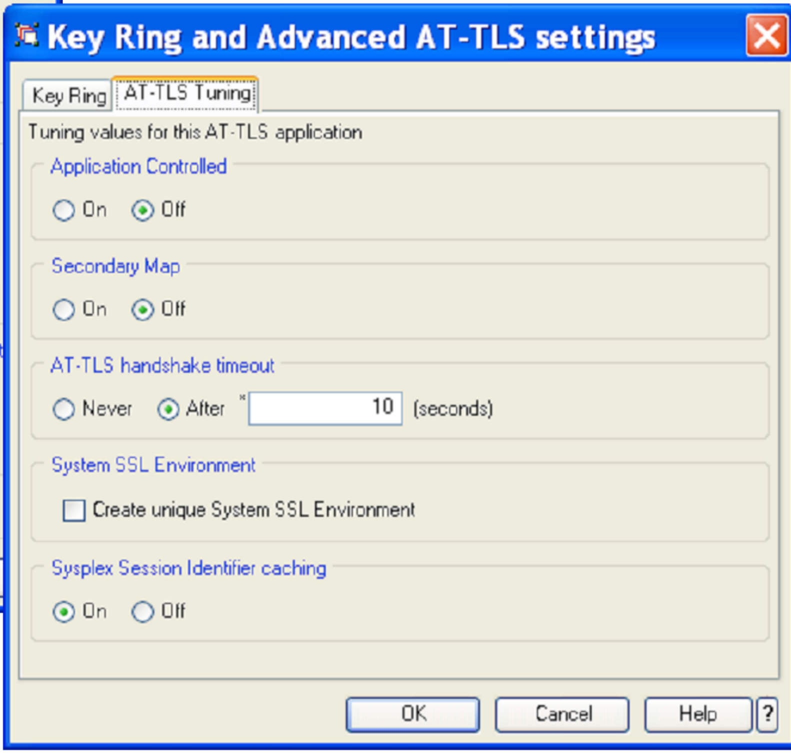
AT-TLS handshake role

● Server ○ Client

Client Authentication role is set in the Security Level

Additional application configurat

In this setup, I use the PASSIVEDATAPORTS FTP.DATA option to control the range of port numbers that can be used for passive mode data connections.



Key Ring and Advanced AT-TLS settings

Tuning values for this AT-TLS application

Application Controlled

○ On ● Off

Secondary Map

○ On ● Off

AT-TLS handshake timeout

○ Never ● After * 10 (seconds)

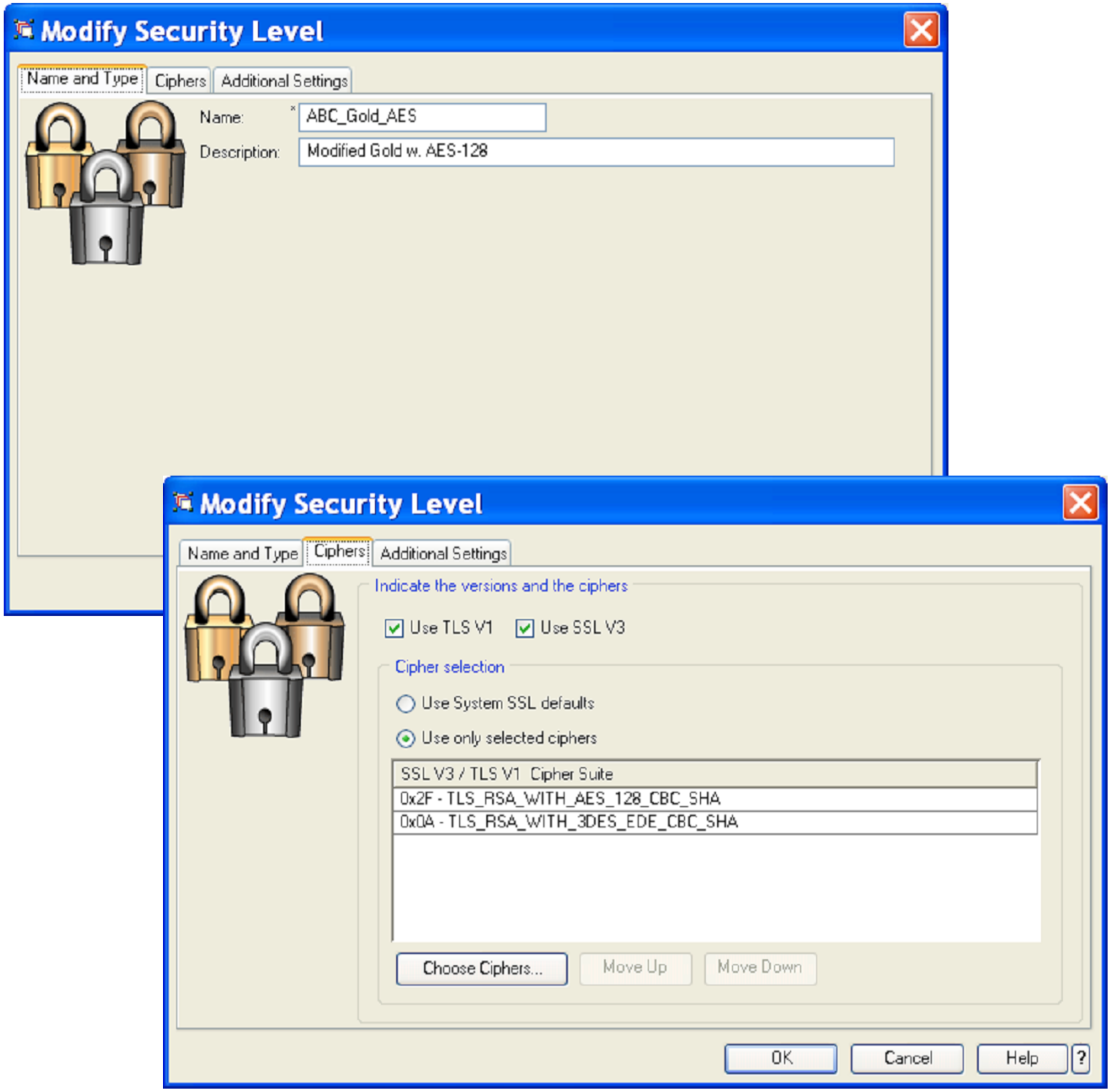
System SSL Environment

☐ Create unique System SSL Environment

Sysplex Session Identifier caching

● On ○ Off

A new security level



Name: ABC_Gold_AES

Description: Modified Gold w. AES-128

Indicate the versions and the ciphers

☑ Use TLS V1 ☑ Use SSL V3

Cipher selection

○ Use System SSL defaults

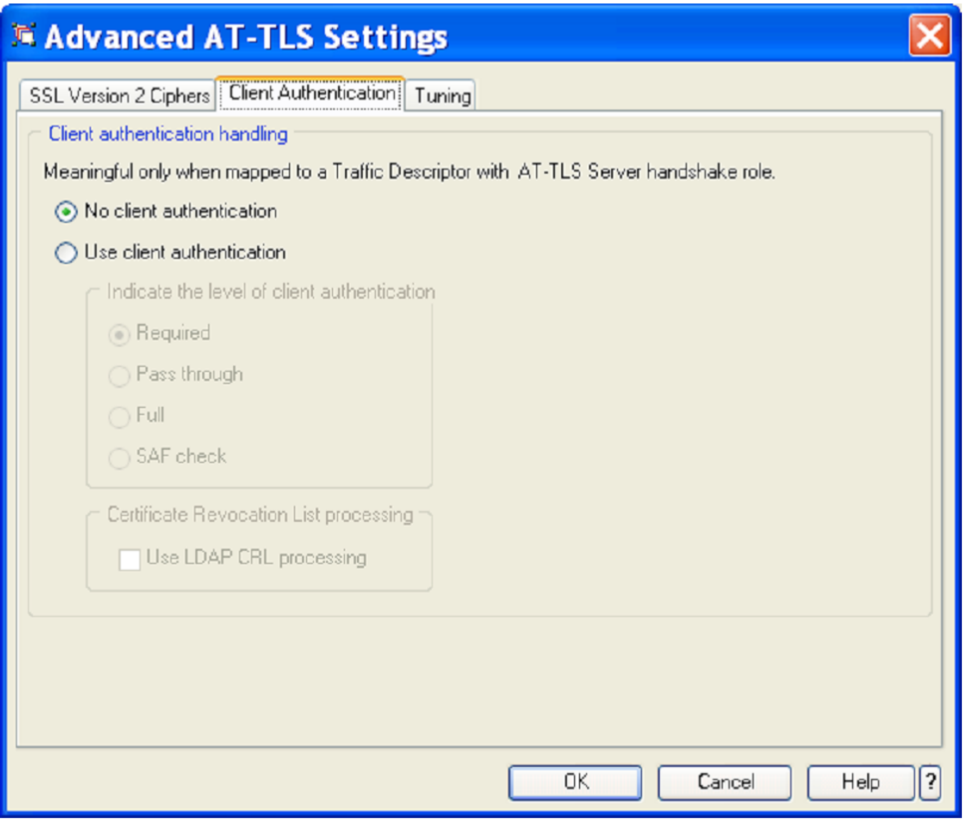
● Use only selected ciphers

SSL V3 / TLS V1 Cipher Suite
0x2F - TLS_RSA_WITH_AES_128_CBC_SHA
0x0A - TLS_RSA_WITH_3DES_EDE_CBC_SHA

- Start by copying a security level and then apply your changes.
- Give the new security level a name and a description
- Select your ciphers and arrange them in preferred order (most preferred at the top of the list)

Advanced security level settings for AT-TLS

- SSLv2 is by default disabled, but you can enable it and choose SSLv2 Ciphers - if needed (not recommended!)
- If you need SSL/TLS client authentication, this is where you will specify what level of client authentication you require
- You would normally not need to change the information under the tuning tab, but you can



Advanced AT-TLS Settings

SSL Version 2 Ciphers | Client Authentication | Tuning

Client authentication handling

Meaningful only when mapped to a Traffic Descriptor with AT-TLS Server handshake role.

● No client authentication

○ Use client authentication

Indicate the level of client authentication

● Required

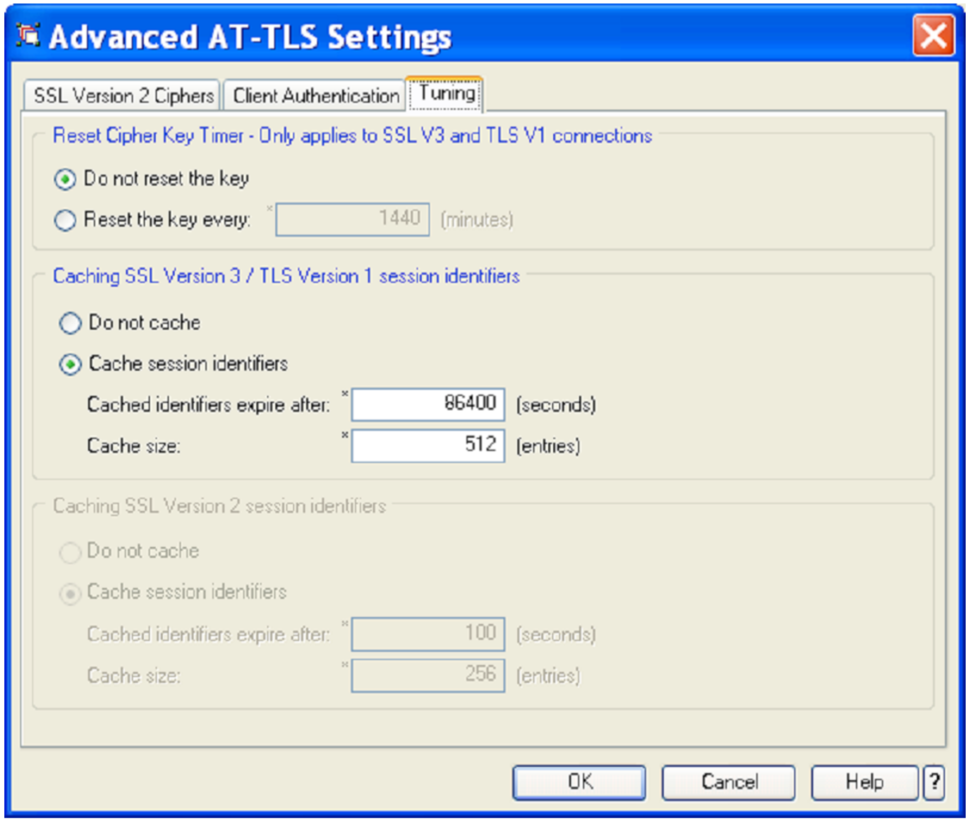
○ Pass through

○ Full

○ SAF check

Certificate Revocation List processing

□ Use LDAP CRL processing



Advanced AT-TLS Settings

SSL Version 2 Ciphers | Client Authentication | Tuning

Reset Cipher Key Timer - Only applies to SSL V3 and TLS V1 connections

● Do not reset the key

○ Reset the key every: * 1440 (minutes)

Caching SSL Version 3 / TLS Version 1 session identifiers

○ Do not cache

● Cache session identifiers

Cached identifiers expire after: * 86400 (seconds)

Cache size: * 512 (entries)

Caching SSL Version 2 session identifiers

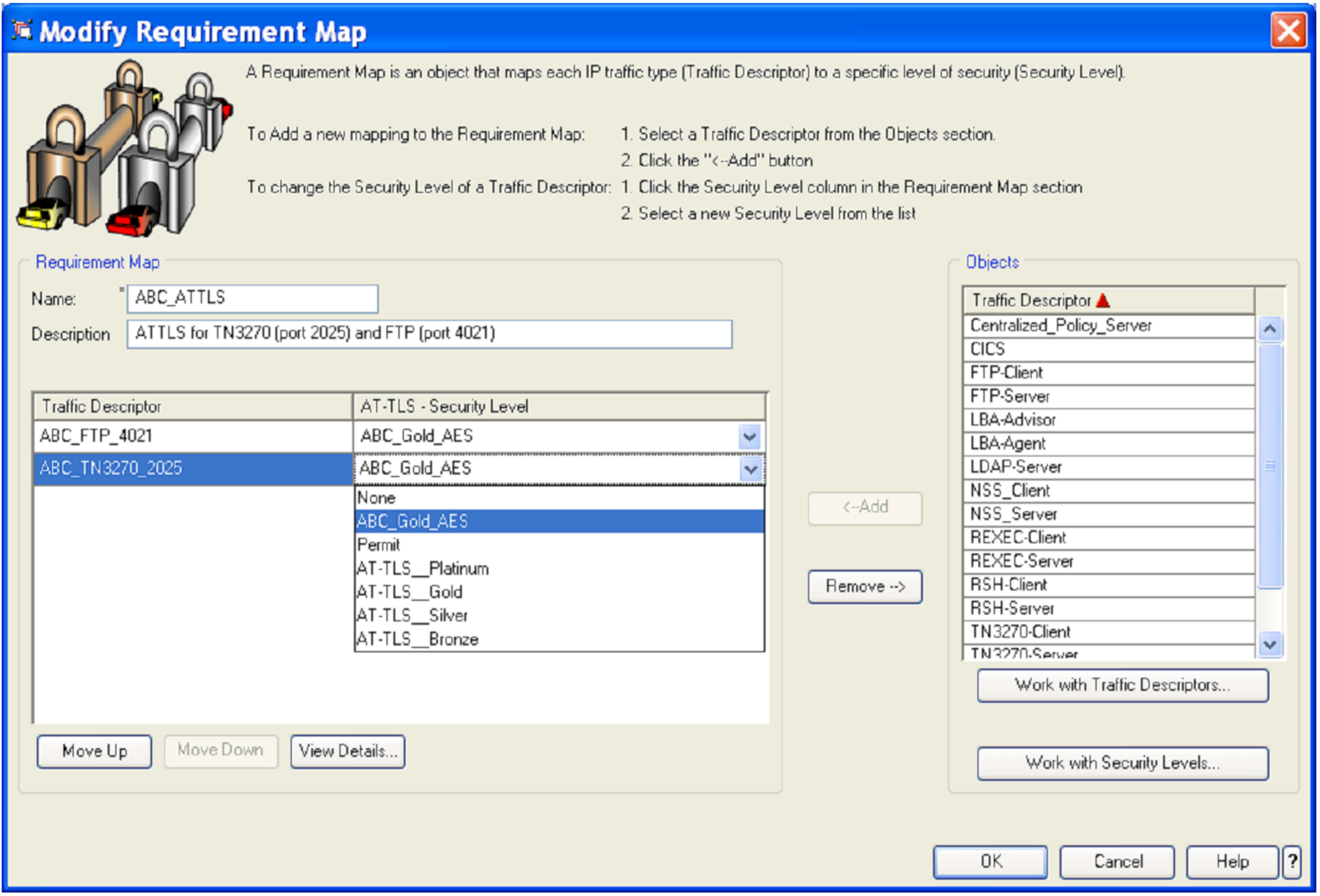
○ Do not cache

● Cache session identifiers

Cached identifiers expire after: * 100 (seconds)

Cache size: * 256 (entries)

Requirement map for AT-TLS



A Requirement Map is an object that maps each IP traffic type (Traffic Descriptor) to a specific level of security (Security Level).

To Add a new mapping to the Requirement Map: 1. Select a Traffic Descriptor from the Objects section. 2. Click the "<--Add" button

To change the Security Level of a Traffic Descriptor: 1. Click the Security Level column in the Requirement Map section 2. Select a new Security Level from the list

Requirement Map

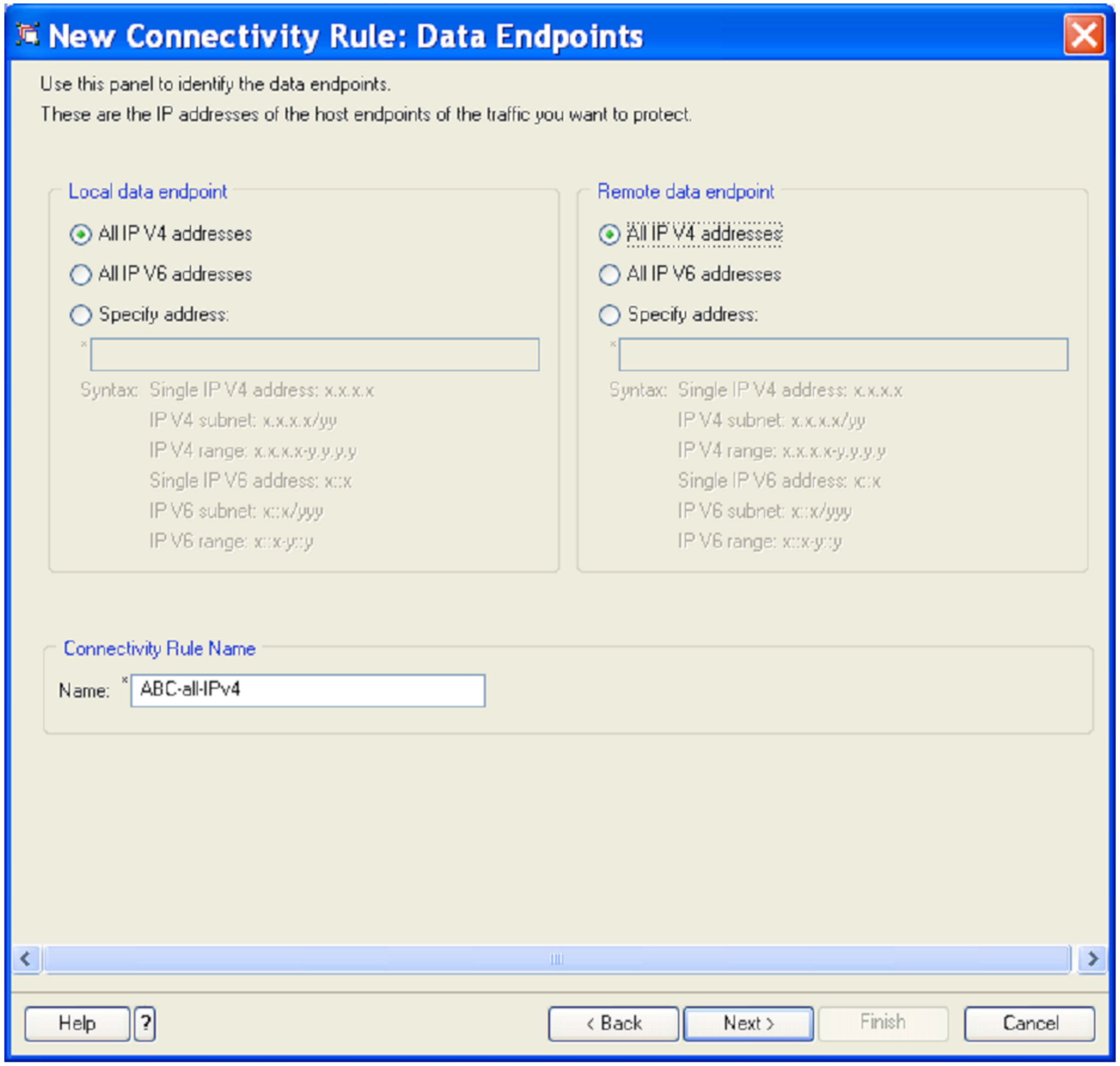
Name: * ABC_ATTLS

Description ATTLS for TN3270 (port 2025) and FTP (port 4021)

Traffic Descriptor	AT-TLS - Security Level
ABC_FTP_4021	ABC_Gold_AES
ABC_TN3270_2025	ABC_Gold_AES

- Create a new requirement map
- Add desired traffic descriptors from the right and click the "add" button
- Click the drop-down box in the security level column and select security level for the traffic

Now is time to add IP addresses per stack in a connectivity rule



Use this panel to identify the data endpoints.
These are the IP addresses of the host endpoints of the traffic you want to protect.

Local data endpoint

- ● All IP V4 addresses
- ○ All IP V6 addresses
- ○ Specify address:

Syntax: Single IP V4 address: x.x.x.x
IP V4 subnet: x.x.x.x/yy
IP V4 range: x.x.x.x-y.y.y.y
Single IP V6 address: x::x
IP V6 subnet: x::x/yyy
IP V6 range: x::x-y::y

Remote data endpoint

- ● All IP V4 addresses
- ○ All IP V6 addresses
- ○ Specify address:

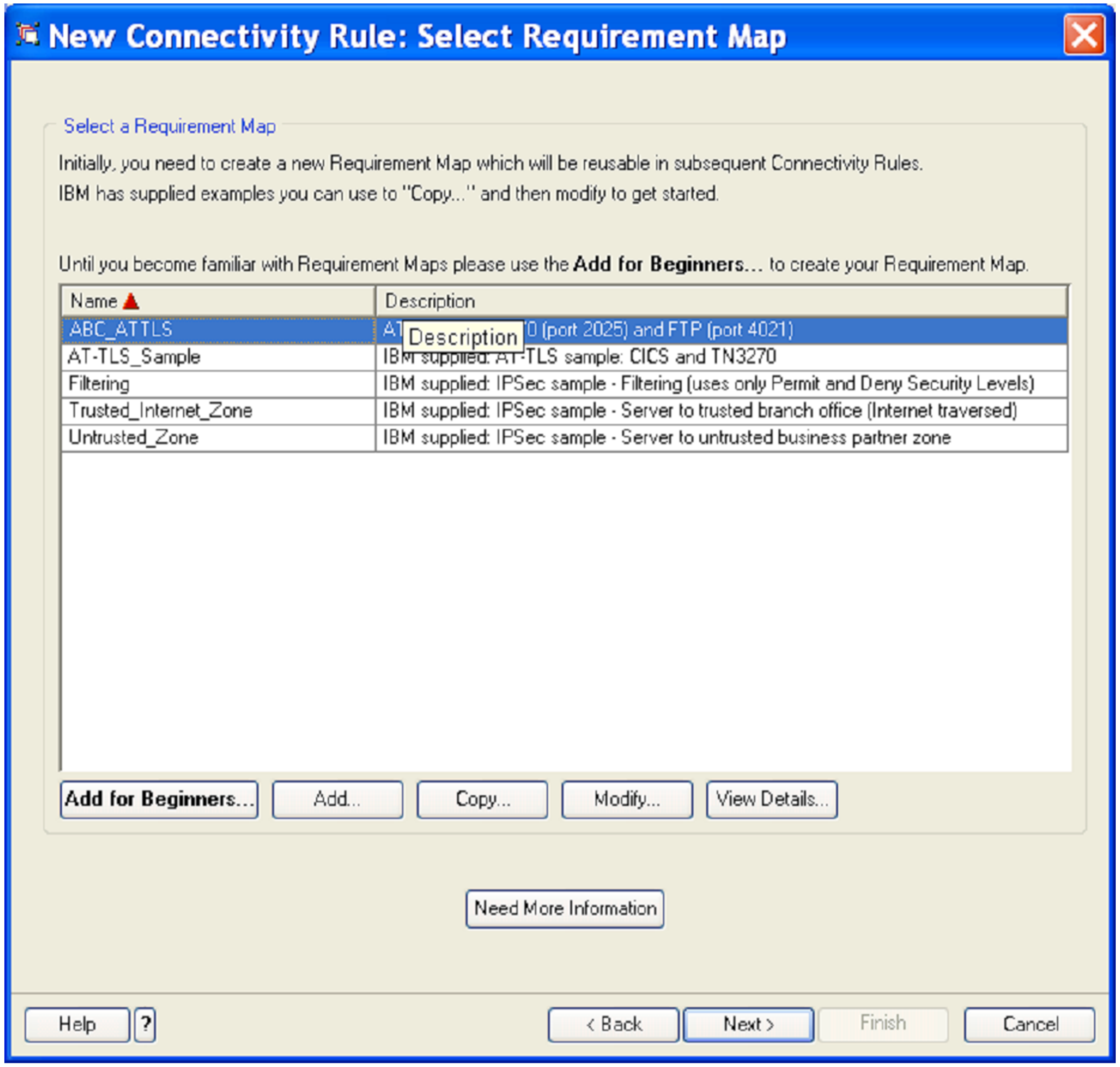
Syntax: Single IP V4 address: x.x.x.x
IP V4 subnet: x.x.x.x/yy
IP V4 range: x.x.x.x-y.y.y.y
Single IP V6 address: x::x
IP V6 subnet: x::x/yyy
IP V6 range: x::x-y::y

Connectivity Rule Name

Name: * ABC-all-IPv4

- So far, all policy definitions are generic for ATT-TLS and can be (re)used on many stacks on many LPARs.
  - You would most typically share all these across all the stacks in a Sysplex
- Per stack, we now need to create a connectivity rule that ties the requirement maps to the IP addresses of that stack
- In our example, we want anyone who connects to our secure servers on any of the stack's home IP addresses to use AT-TLS security

Tie the requirement map into the connectivity rule



Select a Requirement Map

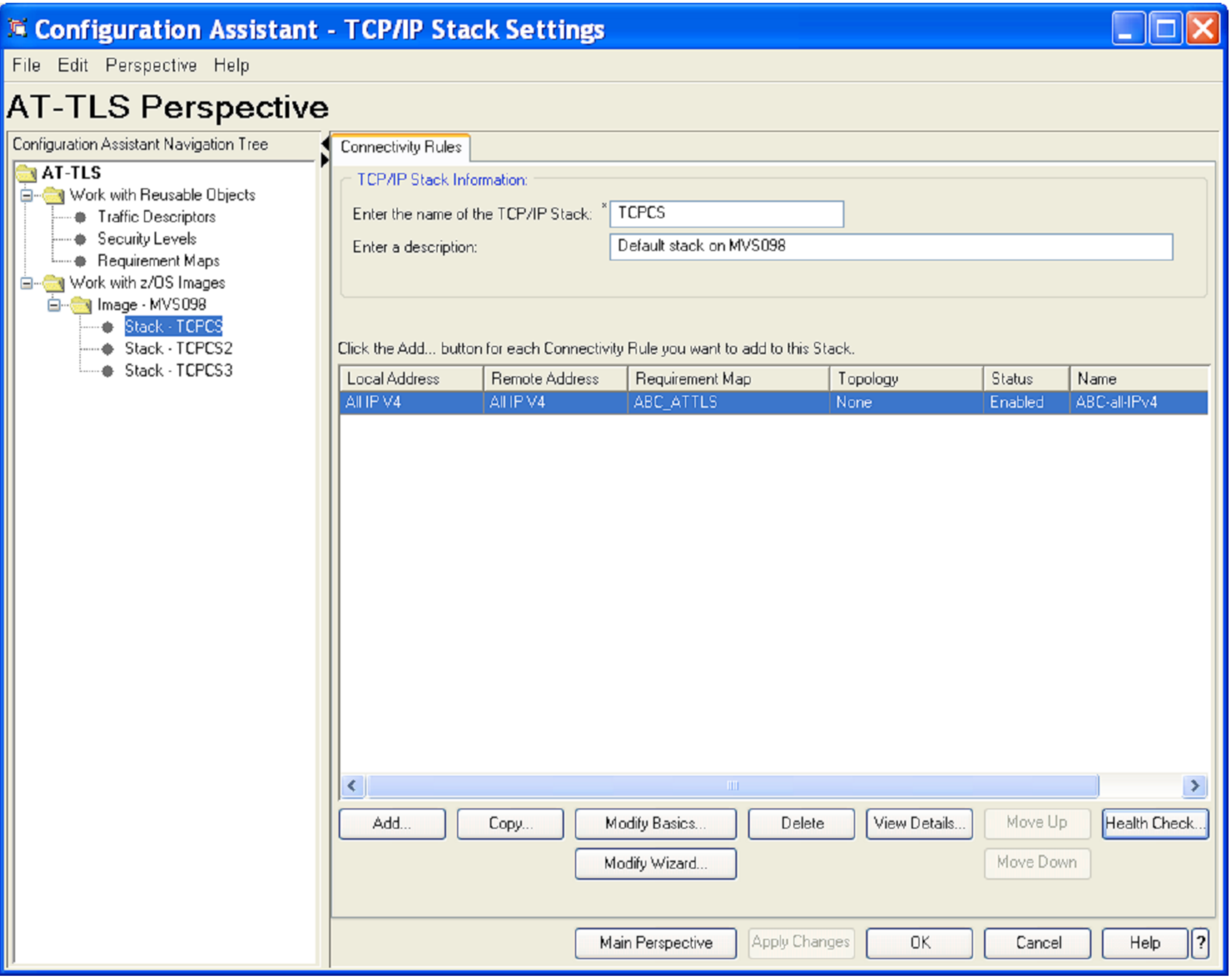
Initially, you need to create a new Requirement Map which will be reusable in subsequent Connectivity Rules. IBM has supplied examples you can use to "Copy..." and then modify to get started.

Until you become familiar with Requirement Maps please use the **Add for Beginners...** to create your Requirement Map.

Name ▲	Description
ABC_ATTLS	AT Description 0 (port 2025) and FTP (port 4021)
AT-TLS_Sample	IBM supplied: AT-TLS sample: CICS and TN3270
Filtering	IBM supplied: IPSec sample - Filtering (uses only Permit and Deny Security Levels)
Trusted_Internet_Zone	IBM supplied: IPSec sample - Server to trusted branch office (Internet traversed)
Untrusted_Zone	IBM supplied: IPSec sample - Server to untrusted business partner zone

- We use the requirement map we created earlier on in our new connectivity rule

Run HealthChecker on your definitions



AT-TLS Perspective

TCP/IP Stack Information:

Enter the name of the TCP/IP Stack: * TCPCS

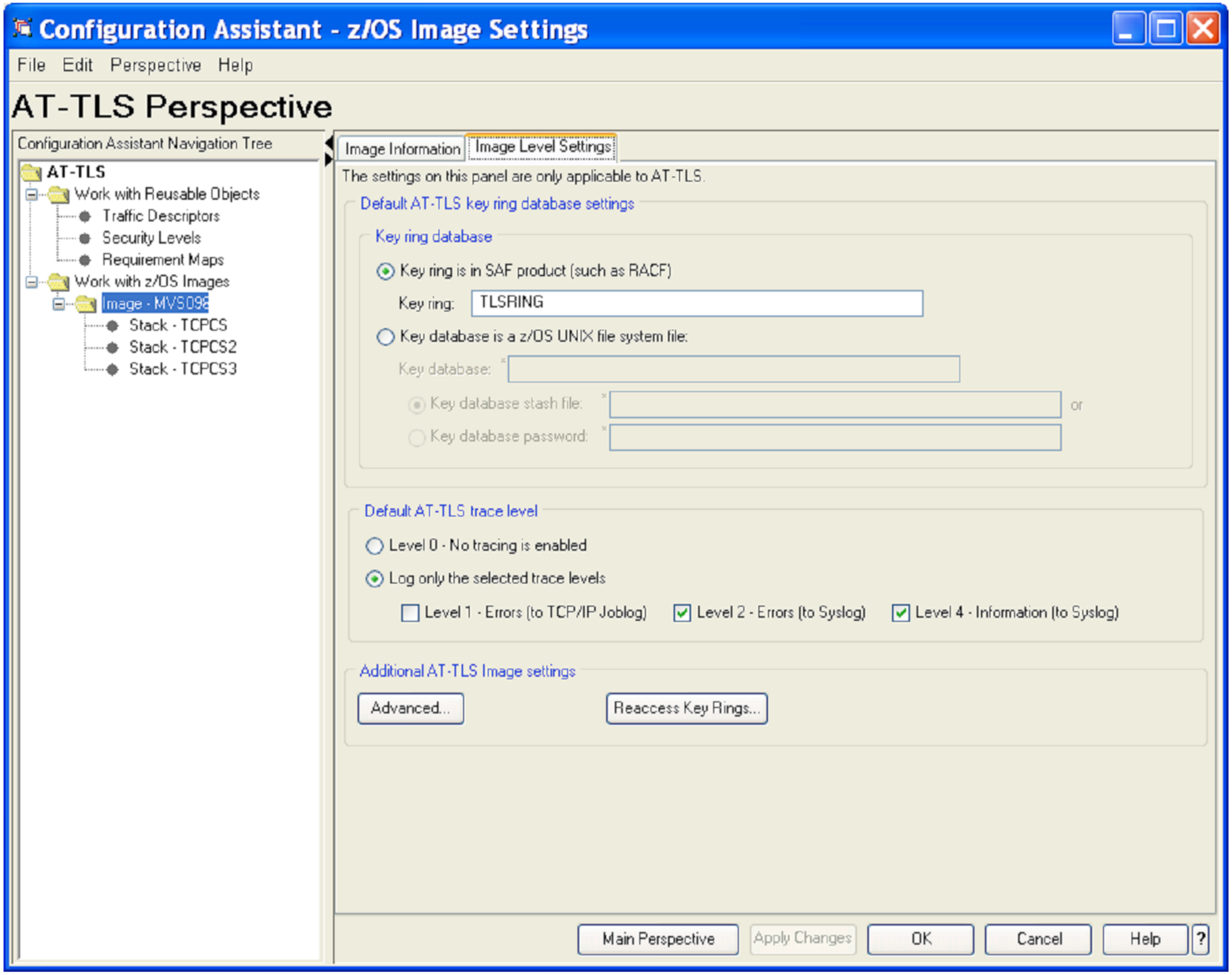
Enter a description: Default stack on MVS098

Click the Add... button for each Connectivity Rule you want to add to this Stack.

Local Address	Remote Address	Requirement Map	Topology	Status	Name
All IP V4	All IP V4	ABC_ATTLS	None	Enabled	ABC-all-IPv4

- Now would be a good time to let the CA try and see if all your definitions are consistent - run the HealthChecker
- HealthChecker output is a help panel that will identify any mistakes or missing elements.

Image-wide keyring information



The settings on this panel are only applicable to AT-TLS.

Default AT-TLS key ring database settings

Key ring database

● Key ring is in SAF product (such as RACF)

Key ring: TLSRING

○ Key database is a z/OS UNIX file system file:

Key database: *

● Key database stash file: * or

○ Key database password: *

Default AT-TLS trace level

○ Level 0 - No tracing is enabled

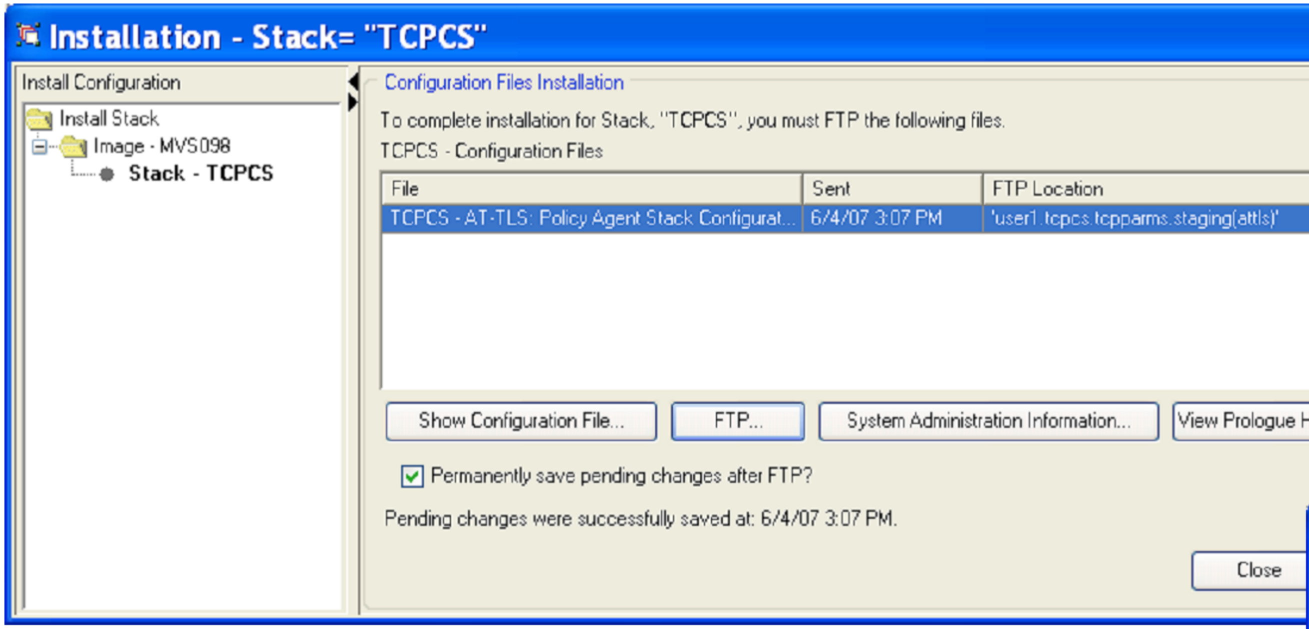
● Log only the selected trace levels

□ Level 1 - Errors (to TCP/IP Joblog) ☑ Level 2 - Errors (to Syslog) ☑ Level 4 - Information (to Syslog)

Additional AT-TLS Image settings

- Keyring information can be specified at two levels:
  - At the image level – shared by all stacks on that image
  - At the individual traffic descriptor level – used by that traffic descriptor only

Transfer policy flat file to z/OS



Installation - Stack= "TCPCS"
Install Configuration
Install Stack
Image - MVS098
Stack - TCPCS
Configuration Files Installation
Show Configuration File...
FTP...
System Administration Information...
View Prologue History...
Close

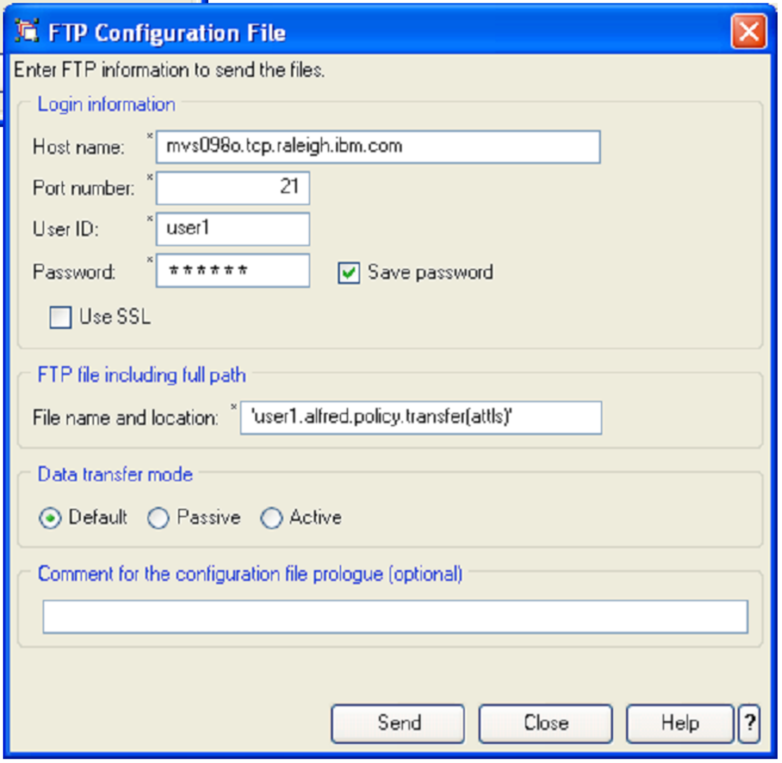
To complete installation for Stack, "TCPCS", you must FTP the following files.

TCPCS - Configuration Files

File	Sent	FTP Location
TCPCS - AT-TLS: Policy Agent Stack Configurat...	6/4/07 3:07 PM	'user1.tcpcs.tcpparms.staging(attls)'

☑ Permanently save pending changes after FTP?

Pending changes were successfully saved at: 6/4/07 3:07 PM.



FTP Configuration File
Login information
FTP file including full path
Data transfer mode
Comment for the configuration file prologue (optional)
Send
Close
Help
?

Enter FTP information to send the files.

Host name: * mvs098o.tcp.raleigh.ibm.com

Port number: * 21

User ID: * user1

Password: * ****** ☑ Save password

□ Use SSL

File name and location: * 'user1.alfred.policy.transfer(attls)'

● Default ○ Passive ○ Active

- Transfer the policy flat file to your z/OS system
- In this example, we transfer the ATTLS policies to USER1.ALFRED.POLICY.TRANSFER member ATTLS

USER1.ALFRED.POLICY.TRANSFER(ATTLS) after upload

```
##
## AT-TLS Policy Agent Configuration file for:
##    Image: MVS098
##    Stack: TCPCS
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 1 Release 9
## Backing Store = 'USER1.ALFRED.POLICY.BACKSTOR(DEFAULT)'
## FTP History:
## 2007-06-05 09:39:25  user1 to mvs098o.tcp.raleigh.ibm.com
##   Added application control for TN3270 server port 2025
## 2007-06-04 03:07:05  user1 to mvs098o.tcp.raleigh.ibm.com
##   Modified a few details
## 2007-06-01 02:24:55  user1 to mvs098o.tcp.raleigh.ibm.com
## 2007-06-01 01:36:13  user1 to mvs098o.tcp.raleigh.ibm.com
##   Added FTP port 4021 to ATTLS configuration
## 2007-06-01 12:54:27  user1 to mvs098o.tcp.raleigh.ibm.com
##   Support for TN3270 server port 2025 (only ATTLS port in this config)
##
TTLSRule                          ABC-all-IPv4~1
{
  LocalAddrSetRef                 addr1
  RemoteAddrSetRef                addr1
  LocalPortRangeRef               portR1
  RemotePortRangeRef              portR2
  Direction                       Inbound
  Priority                        255
  TTLSGroupActionRef              gAct1
 ++++
 ++++ Many, many more lines.....
```

- Note the transfer history section:
  - For every transfer, the CA will prompt for a log entry, which will be included in the header comment lines in the flat file

Policy Agent

```
//PAGENT   PROC P='-d 0'
//PAGENT   EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
//       PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/&P'
//*
//STDENV   DD DSN=USER1.TCPCS.TCPPARMS(PAGTENV),DISP=SHR
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
//SYSOUT   DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

Policy Agent start JCL procedure

```
##
## USER1.TCPCS.TCPPARMS(PAGTCONF)
##
##    Image: mvs098
##
TcpImage TCPCS  FLUSH 600
##
TTLSConfig //'USER1.TCPCS.TCPPARMS(ATTLS)' FLUSH NOPURGE
QoSConfig //'USER1.TCPCS.TCPPARMS(QOS)' FLUSH NOPURGE
IDSConfig //'USER1.TCPCS.TCPPARMS(IDS)' FLUSH NOPURGE
IPSecConfig //'USER1.TCPCS.TCPPARMS(IPSEC)'
```

Policy Agent "root" configuration data

```
F PAGENT,REFRESH
EZZ8443I PAGENT MODIFY COMMAND ACCEPTED
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : IDS
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : QOS
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : TTLS
```

Policy Agent refresh command to read in updated policies

TN3270 server definitions

```
;
; Set TN3270(E) server port 2025 options
;
; TTLS port - secured via ATTLS
;
TelnetParms
    TTLSPort 2025                 ; Port number 2025 (security via TTLS)
    Conntype Any                  ; We'll use it for both secure and clear
    Expresslogon                  ; Express logon is supported
    Debug detail console
EndTelnetParms
```

FTP server definitions

```
EXTENSIONS        AUTH_TLS          ; Enable TLS authentication

TLSMECHANISM      ATTLS             ; Server-specific or ATTLS
                                    ; ATTLS - use ATTLS
                                    ; FTP - server-specific (D)

SECURE_FTP        ALLOWED           ; Authentication indicator
                                    ; ALLOWED         (D)
                                    ; REQUIRED

SECURE_LOGIN      NO_CLIENT_AUTH    ; Authorization level indicator
                                    ; for TLS
                                    ; NO_CLIENT_AUTH (D)
                                    ; REQUIRED
                                    ; VERIFY_USER

SECURE_PASSWORD   REQUIRED          ; REQUIRED (D) - User must enter
                                    ;     password
                                    ; OPTIONAL - User does not have to
                                    ;     enter a password
                                    ; This setting has meaning only
                                    ; for TLS when implementing client
                                    ; certificate authentication

SECURE_CTRLCONN   CLEAR             ; Minimum level of security for
                                    ; the control connection
                                    ; CLEAR           (D)
                                    ; SAFE
                                    ; PRIVATE

SECURE_DATACONN   CLEAR             ; Minimum level of security for
                                    ; the data connection
                                    ; NEVER
                                    ; CLEAR           (D)
                                    ; SAFE
                                    ; PRIVATE
```

CIPHERSUITE, KEYRING, and TLSTIMEOUT in FTP.DATA are ignored when TLSMECHANISM is set to ATTLS.

```
PASSIVEDATAPORTS   (50000,50200)
    ; Assign a range of ports to be
    ; used for passive data ports
    ; lowest valid port = 1024
    ; highest valid port = 65535
    ; There are no default values.
```

Remember the EZB.INITSTACK SERVAUTH profile before enabling TTLS on TCPConfig!

```
CLASS       NAME
-----       ----
SERVAUTH    EZB.INITSTACK.*.* (G)

LEVEL  OWNER       UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------    ----------------  -----------  -------
 00    USER1            NONE              ALTER      NO

.....

USER       ACCESS
----       ------
USER1      ALTER
TCPCS      READ
```

- **When TCP/IP starts with TCPCONFIG TTLS specified, it will issue the following message**
  - EZZ4248E TCPCS WAITING FOR PAGENT TTLS POLICY
- **From then on and until PAGENT has been started and installed the TTLS policies into the TCP/IP stack, the TCP/IP stack will only allow users permitted to the EZB.INITSTACK.system.stack SERVAUTH profile to establish connections.**
  - Make sure all your pertinent server address spaces (including PAGENT and OMPROUTE) run under user IDs that are permitted to this profile.

Netstat connection report with TTLS filter to see all ATTLS connections

```
ALLCONN APPLDATA TCP TCPCS STACK TITLES ( CONNT TTLSP

MVS TCP/IP NETSTAT CS V1R9       TCPIP Name: TCPCS           17:00:13
User Id  Conn     State
-------  ----     -----
FTP40211 00000683 Establsh
  Local Socket:   ::ffff:9.42.105.45..4021
  Foreign Socket: ::ffff:9.65.192.113..1543
FTP40211 0000068B Establsh
  Local Socket:   ::ffff:9.42.105.45..4021
  Foreign Socket: ::ffff:9.49.152.174..2346
FTP40211 00000428 Establsh
  Local Socket:   ::ffff:9.42.105.45..4021
  Foreign Socket: ::ffff:9.49.148.71..1178
TN3270A  0000067E Establsh
  Local Socket:   ::ffff:9.42.105.45..2025
  Foreign Socket: ::ffff:9.65.192.113..1541
  Application Data:  EZBTNSRV TCPABC83 TSO10002 ET B
USER1    00000687 TimeWait
  Local Socket:   9.42.105.45..50118
  Foreign Socket: 9.65.192.113..1544
```

Netstat TTLS report for specific connection that is protected by ATTLS

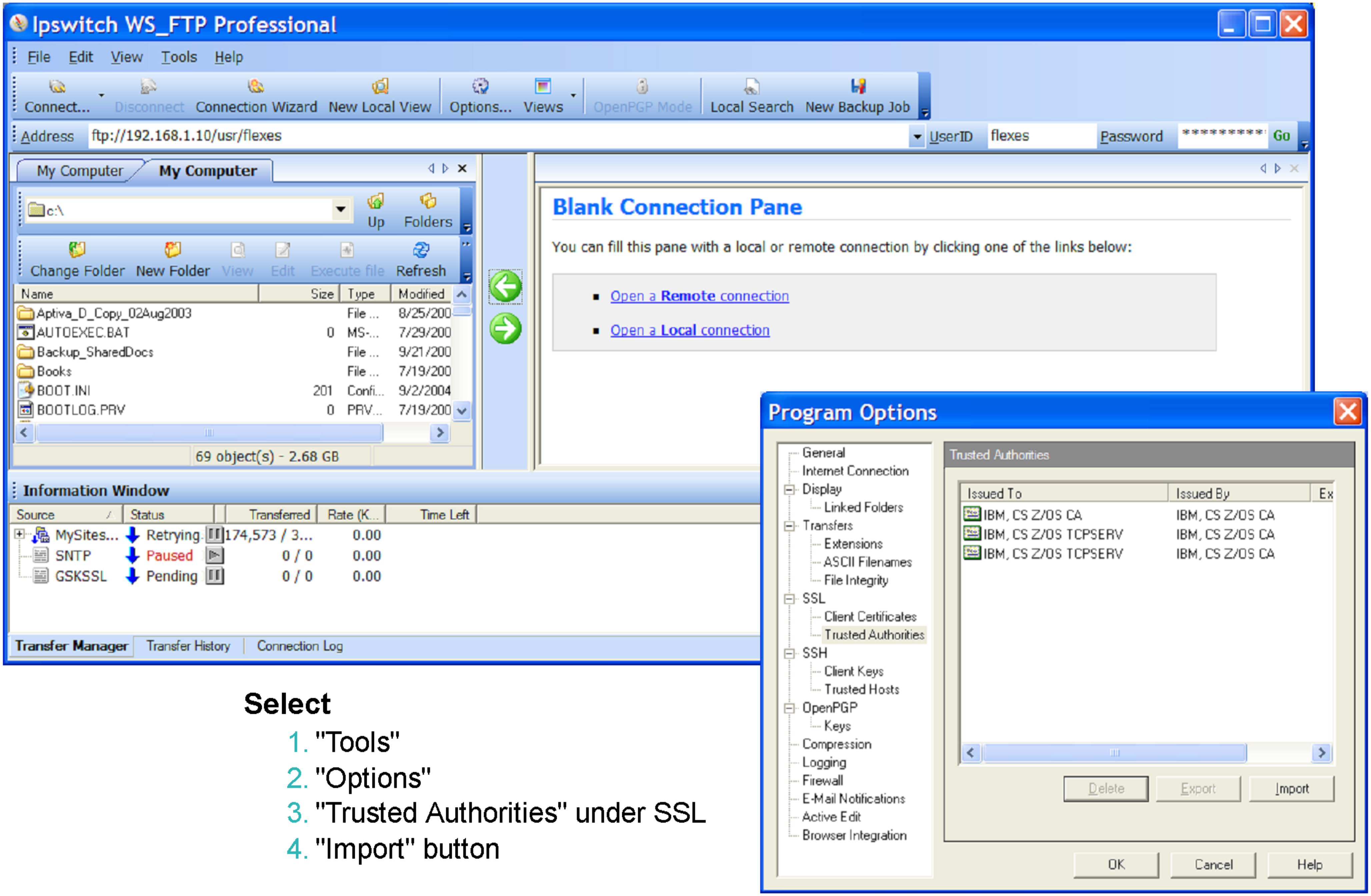
```
TTLS CO 683 DETAIL TCP TCPCS STACK TITLES

MVS TCP/IP NETSTAT CS V1R9       TCPIP Name: TCPCS           17:01:31

ConnID: 00000683
  JobName:       FTP40211
  LocalSocket:   ::ffff:9.42.105.45..4021
  RemoteSocket:  ::ffff:9.65.192.113..1543
  SecLevel:      TLS Version 1
  Cipher:        2F TLS_RSA_WITH_AES_128_CBC_SHA
  CertUserID:    N/A
  MapType:       Primary
TTLSRule: ABC-all-IPv4~1
  Priority:        255
  LocalAddr:       0.0.0.0/0
  LocalPort:       4021
  RemoteAddr:      0.0.0.0/0
  RemotePortFrom: 1024               RemotePortTo: 65535
  Direction:       Inbound
  TTLSGrpAction:   gAct1
    GroupID:                    00000006
    TTLSEnabled:                On
    CtraceClearText:            Off
    Trace:                      6
    SyslogFacility:             Daemon
    SecondaryMap:               Off
  TTLSEnvAction:   eAct1~ABC_FTP_4021
    EnvironmentUserInstance:    0
    HandshakeRole:              Server
    Keyring:                    TLSRING
    SSLV2:                      Off
    SSLV3:                      On
    TLSV1:                      On
    ResetCipherTimer:           0
    ApplicationControlled:      Off
    HandshakeTimeout:           10
    ClientAuthType:             Required
    GSK_SYSPLEX_SIDCACHE:       On

TTLSConnAction: cAct1~ABC_FTP_4021
  HandshakeRole:              Server
  V3CipherSuites:             2F TLS_RSA_WITH_AES_128_CBC_SHA
                              0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
  Trace:                      6
  ApplicationControlled:      On
  SecondaryMap:               On
    GSK_SYSPLEX_SIDCACHE:       On
```

WS_FTP Pro import CA certificate part 1/2



Address ftp://192.168.1.10/usr/flexes UserID flexes Password ********* Go

c:\

Name	Size	Type	Modified
Aptiva_D_Copy_02Aug2003		File ...	8/25/200
AUTOEXEC.BAT	0	MS-...	7/29/200
Backup_SharedDocs		File ...	9/21/200
Books		File ...	7/19/200
BOOT.INI	201	Confi...	9/2/2004
BOOTLOG.PRV	0	PRV...	7/19/200

69 object(s) - 2.68 GB

Blank Connection Pane

You can fill this pane with a local or remote connection by clicking one of the links below:

- Open a **Remote** connection
- Open a **Local** connection

Source	Status	Transferred	Rate (K...	Time Left
MySites...	Retrying	174,573 / 3...	0.00	
SNTP	Paused	0 / 0	0.00	
GSKSSL	Pending	0 / 0	0.00	

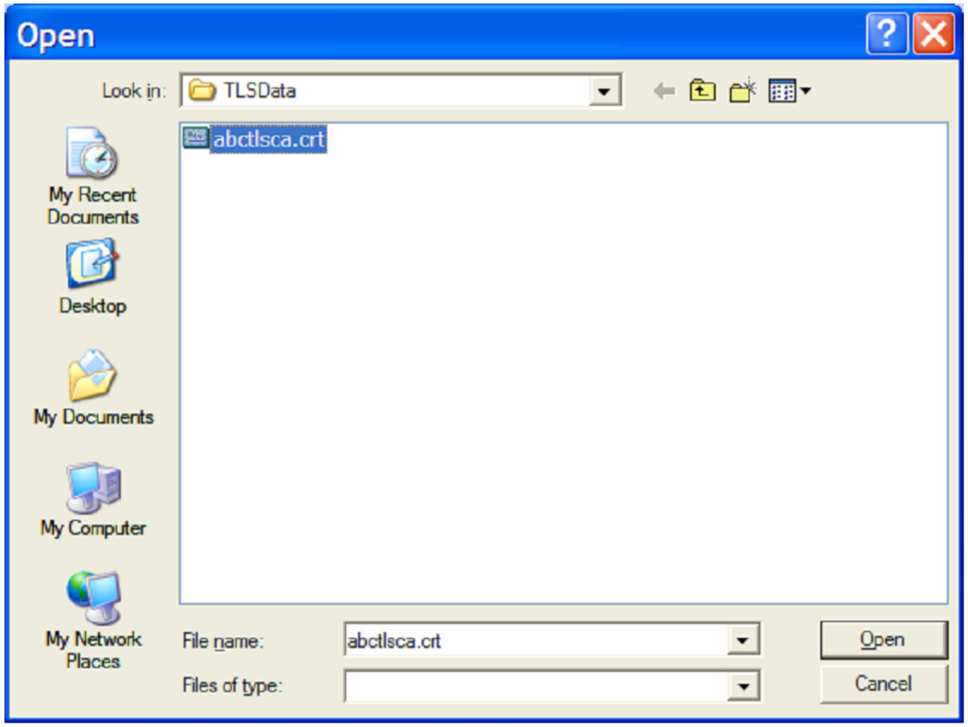
Trusted Authorities

Issued To	Issued By	Ex
IBM, CS Z/OS CA	IBM, CS Z/OS CA	
IBM, CS Z/OS TCPSERV	IBM, CS Z/OS CA	
IBM, CS Z/OS TCPSERV	IBM, CS Z/OS CA	

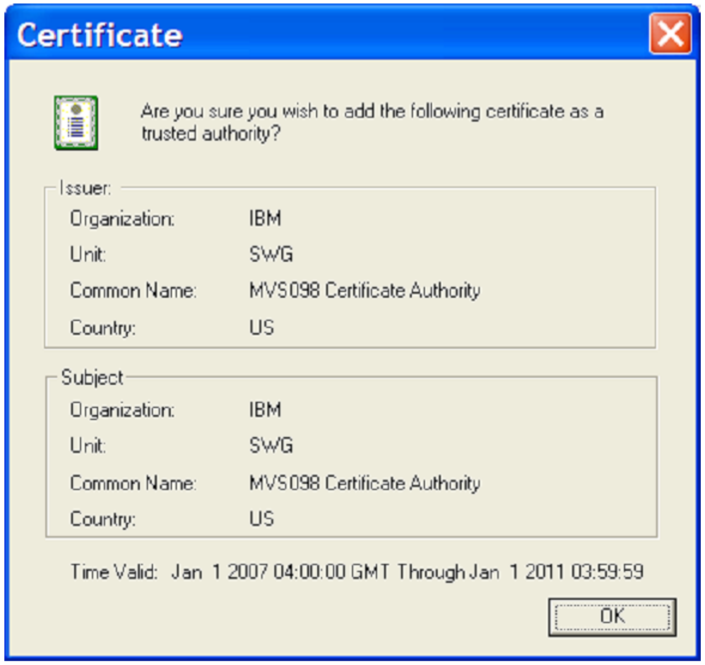
Select

1. "Tools"
2. "Options"
3. "Trusted Authorities" under SSL
4. "Import" button

WS_FTP Pro import CA certificate - part 2/2



Find your downloaded Base64-encoded Certificate Authority certificate



Are you sure you wish to add the following certificate as a trusted authority?

Issuer:

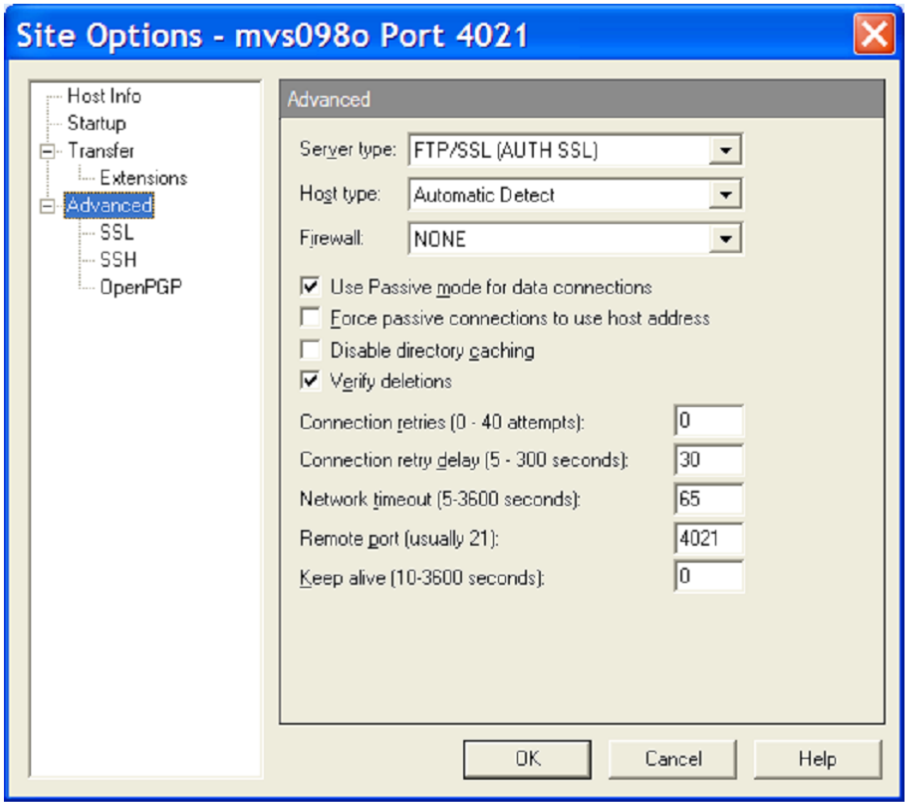
Organization:	IBM
Unit:	SWG
Common Name:	MVS098 Certificate Authority
Country:	US

Subject

Organization:	IBM
Unit:	SWG
Common Name:	MVS098 Certificate Authority
Country:	US

Time Valid: Jan 1 2007 04:00:00 GMT Through Jan 1 2011 03:59:59

WS FTP Pro site manager - site options for SSL/TLS



Site Options - mvs098o Port 4021

Advanced

Server type: FTP/SSL (AUTH SSL)

Host type: Automatic Detect

Firewall: NONE

☑ Use Passive mode for data connections

☐ Force passive connections to use host address

☐ Disable directory caching

☑ Verify deletions

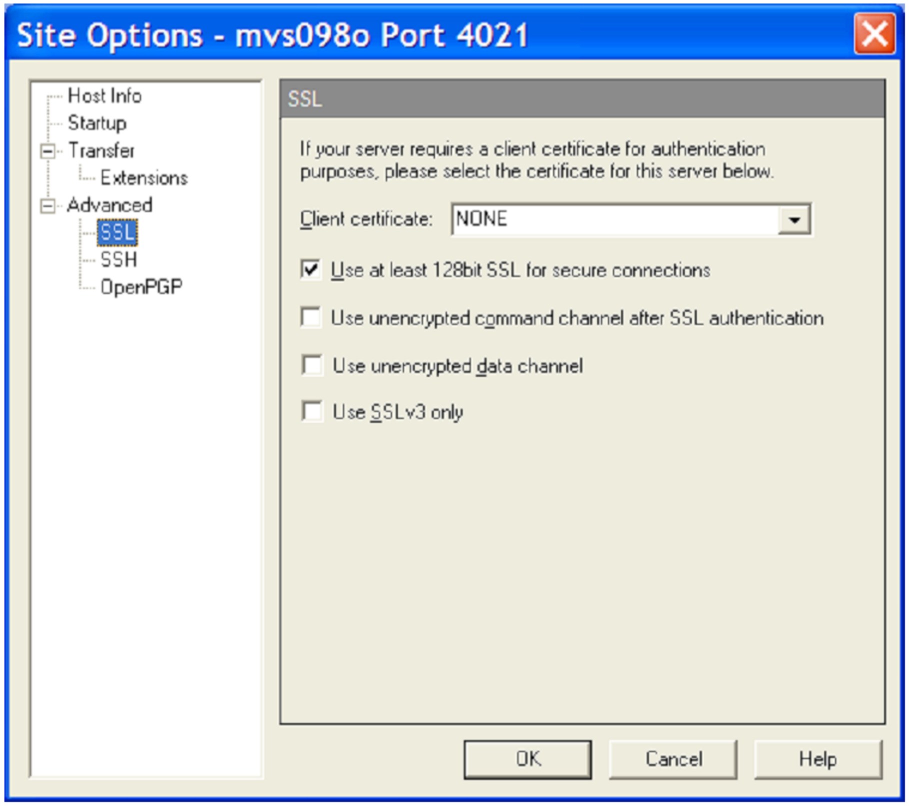
Connection retries (0 - 40 attempts): 0

Connection retry delay (5 - 300 seconds): 30

Network timeout (5-3600 seconds): 65

Remote port (usually 21): 4021

Keep alive (10-3600 seconds): 0



Site Options - mvs098o Port 4021

SSL

If your server requires a client certificate for authentication purposes, please select the certificate for this server below.

Client certificate: NONE

☑ Use at least 128bit SSL for secure connections

☐ Use unencrypted command channel after SSL authentication

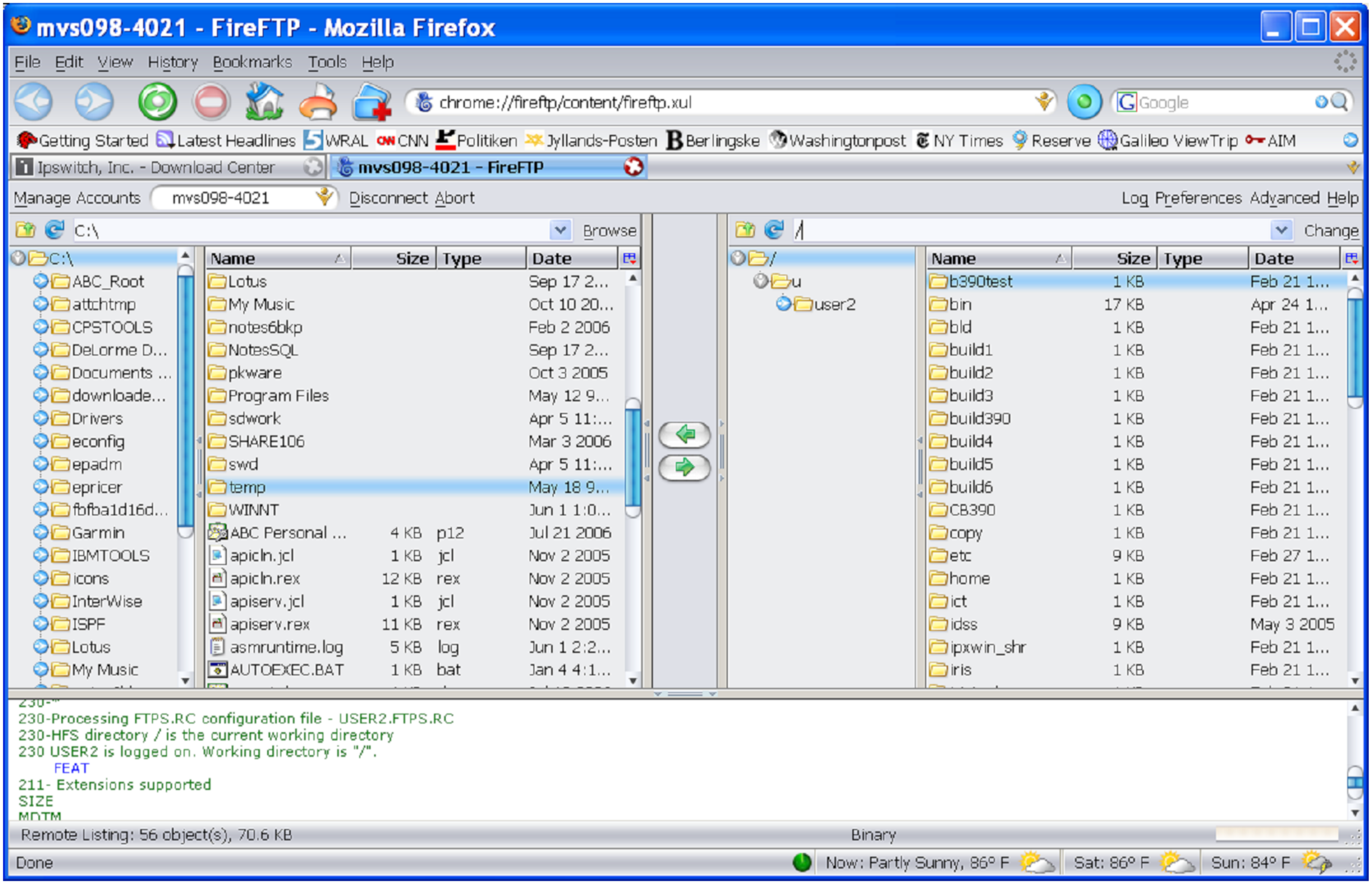
☐ Use unencrypted data channel

☐ Use SSLv3 only

WS FTP Pro sample FTP session log

```
Finding Host mvs098o.tcp.raleigh.ibm.com ...
Connecting to 9.42.105.45:4021
Connected to 9.42.105.45:4021 in 0.031250 seconds, Waiting for Server Response
Initializing SSL Session ...
220-FTP40211 IBM FTP CS V1R9 at MVS098.tcp.raleigh.ibm.com, 15:37:30 on 2007-06-01.
220-*
220-* Welcome to the FTP server on MVS098.tcp.raleigh.ibm.com
220-* This system is used by Alfred for testing purposes.
220-* Any issues should be reported to
220-* Your host name is sig-9-65-198-155.mts.ibm.com
220-*
220 Connection will not timeout.
AUTH TLS
234 Security environment established - ready for negotiation
SSL session NOT set for reuse
SSL Session Started.
Host type (1): IBM MVS
USER user1
331 Send password please.
PASS (hidden)
230-*
230-* USER1 - welcome to the FTP server on MVS098.tcp.raleigh.ibm.com
230-* Login time and date is Fri Jun  1 15:37:32 2007
230-* The current working directory is USER1.
230-*
230 USER1 is logged on.  Working directory is "USER1.".
Host type (I): IBM MVS
PBSZ 0
200 Protection buffer size accepted
PROT P
200 Data connection protection set to private
PWD
257 "'USER1.'" is working directory.
USER1.  loaded from [Directory Listing Cache]DIR3C.tmp
```

FireFTP (Firefox browser secure FTP client plug-in)


mvs098-4021 - FireFTP - Mozilla Firefox
File Edit View History Bookmarks Tools Help
chrome://fireftp/content/fireftp.xul
Google
Getting Started Latest Headlines WRAL CNN Politiken Jyllands-Posten Berlingske Washingtonpost NY Times Reserve Galileo ViewTrip AIM
Ipswitch, Inc. - Download Center
mvs098-4021 - FireFTP
Manage Accounts mvs098-4021 Disconnect Abort
Log Preferences Advanced Help
C:\
Browse
/
Change

C:\
- ABC_Root
- attchtmp
- CPSTOOLS
- DeLorme D...
- Documents ...
- downloade...
- Drivers
- econfig
- epadm
- epricer
- fbfba1d16d...
- Garmin
- IBMTOOLS
- icons
- InterWise
- ISPF
- Lotus
- My Music

Name	Size	Type	Date
Lotus			Sep 17 2...
My Music			Oct 10 20...
notes6bkp			Feb 2 2006
NotesSQL			Sep 17 2...
pkware			Oct 3 2005
Program Files			May 12 9...
sdwork			Apr 5 11:...
SHARE106			Mar 3 2006
swd			Apr 5 11:...
temp			May 18 9...
WINNT			Jun 1 1:0...
ABC Personal ...	4 KB	p12	Jul 21 2006
apicln.jcl	1 KB	jcl	Nov 2 2005
apicln.rex	12 KB	rex	Nov 2 2005
apiserv.jcl	1 KB	jcl	Nov 2 2005
apiserv.rex	11 KB	rex	Nov 2 2005
asmruntime.log	5 KB	log	Jun 1 2:2...
AUTOEXEC.BAT	1 KB	bat	Jan 4 4:1...

/
- u
  - user2

Name	Size	Type	Date
b390test	1 KB		Feb 21 1...
bin	17 KB		Apr 24 1...
bld	1 KB		Feb 21 1...
build1	1 KB		Feb 21 1...
build2	1 KB		Feb 21 1...
build3	1 KB		Feb 21 1...
build390	1 KB		Feb 21 1...
build4	1 KB		Feb 21 1...
build5	1 KB		Feb 21 1...
build6	1 KB		Feb 21 1...
CB390	1 KB		Feb 21 1...
copy	1 KB		Feb 21 1...
etc	9 KB		Feb 27 1...
home	1 KB		Feb 21 1...
ict	1 KB		Feb 21 1...
idss	9 KB		May 3 2005
ipxwin_shr	1 KB		Feb 21 1...
iris	1 KB		Feb 21 1...

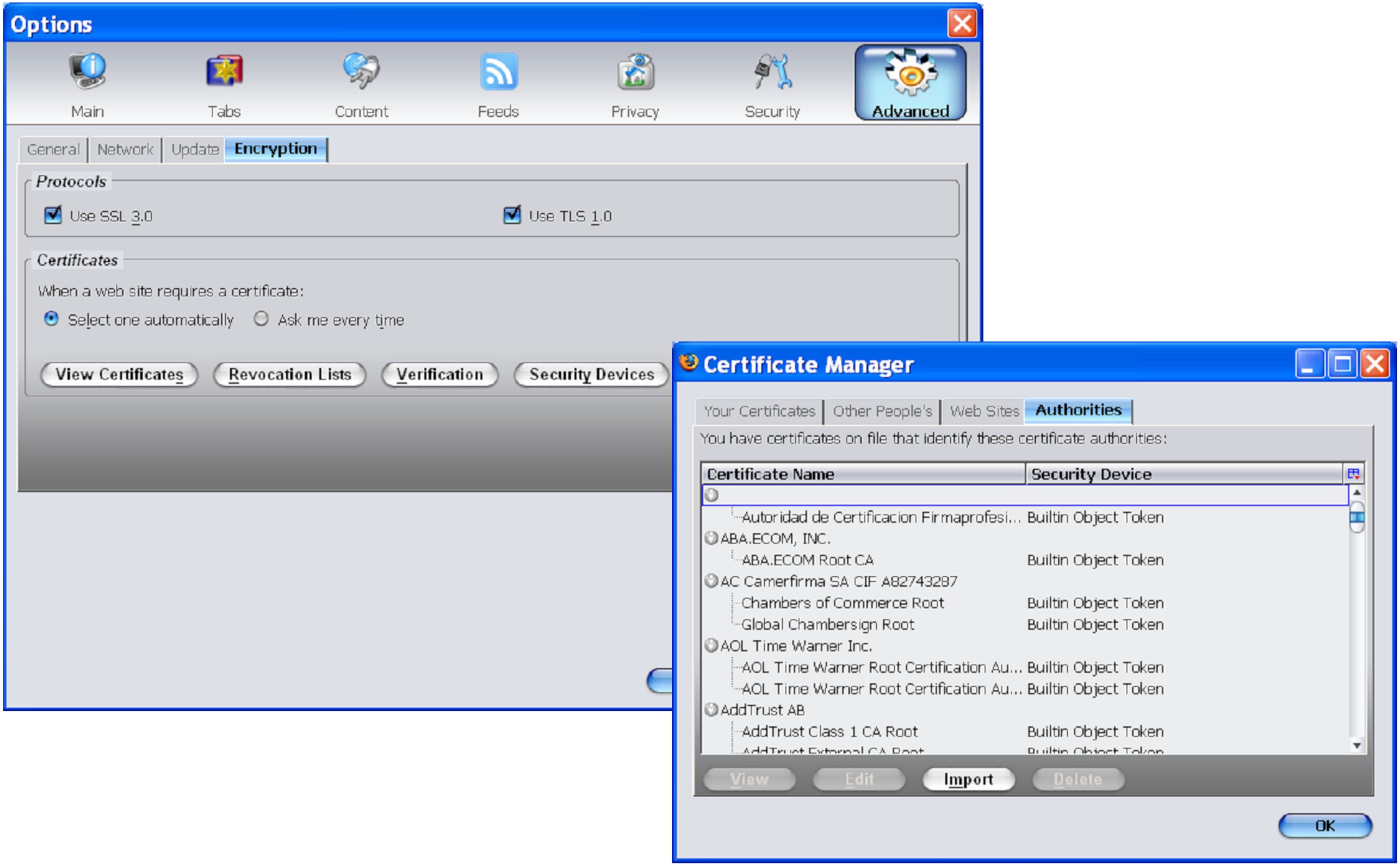
```
230-
230-Processing FTPS.RC configuration file - USER2.FTPS.RC
230-HFS directory / is the current working directory
230 USER2 is logged on. Working directory is "/".
    FEAT
211- Extensions supported
SIZE
MDTM
```

Remote Listing: 56 object(s), 70.6 KB   Binary

Done   Now: Partly Sunny, 86° F   Sat: 86° F   Sun: 84° F

FireFTP does not understand MVS data sets, but only HFS files.

Firefox import CA certificate - part 1/2



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

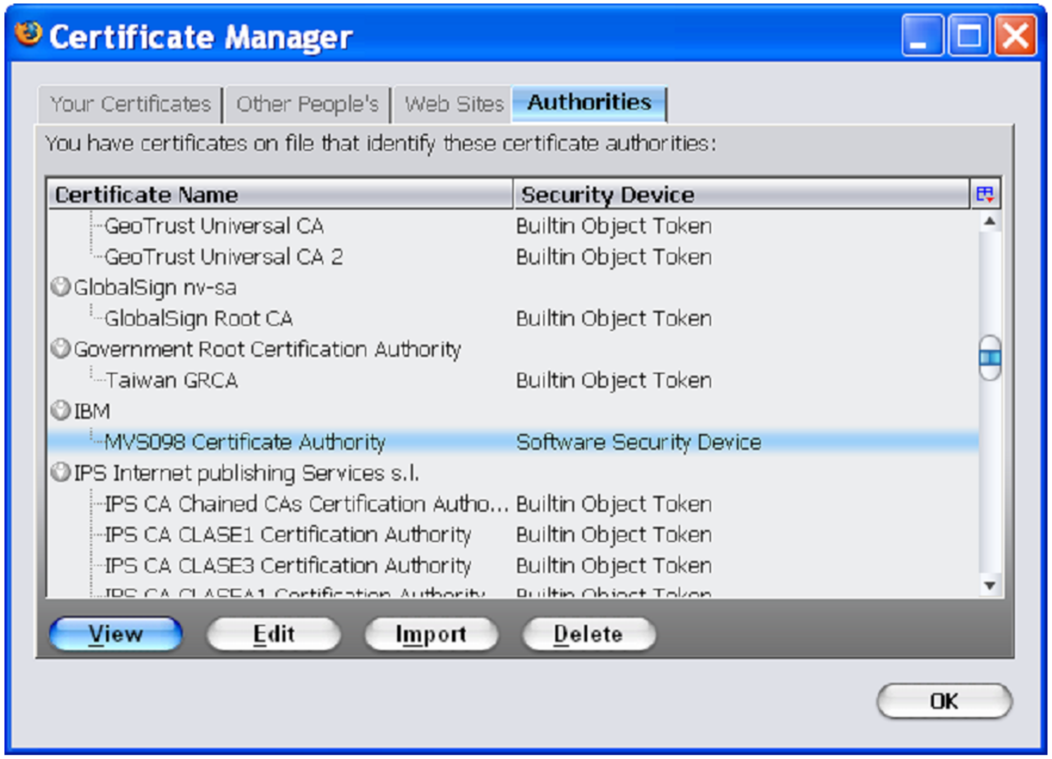
When a web site requires a certificate:

● Select one automatically ○ Ask me every time

You have certificates on file that identify these certificate authorities:

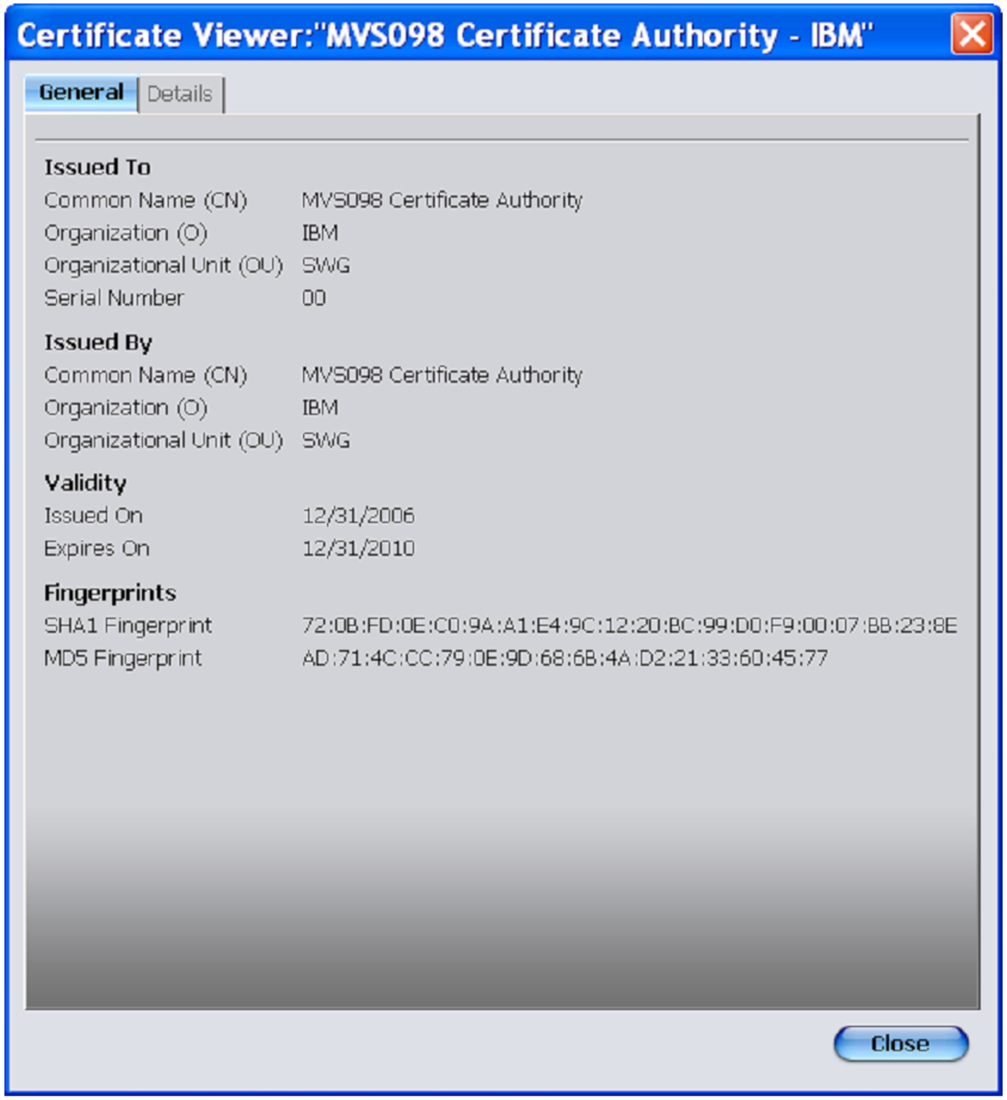
Certificate Name	Security Device
Autoridad de Certificacion Firmaprofesi...	Builtin Object Token
ABA.ECOM, INC.	
ABA.ECOM Root CA	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
AOL Time Warner Inc.	
AOL Time Warner Root Certification Au...	Builtin Object Token
AOL Time Warner Root Certification Au...	Builtin Object Token
AddTrust AB	
AddTrust Class 1 CA Root	Builtin Object Token
AddTrust External CA Root	Builtin Object Token

Firefox import CA certificate - part 2/2



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
GeoTrust Universal CA	Builtin Object Token
GeoTrust Universal CA 2	Builtin Object Token
GlobalSign nv-sa	
GlobalSign Root CA	Builtin Object Token
Government Root Certification Authority	
Taiwan GRCA	Builtin Object Token
IBM	
MVS098 Certificate Authority	Software Security Device
IPS Internet publishing Services s.l.	
IPS CA Chained CAs Certification Autho...	Builtin Object Token
IPS CA CLASE1 Certification Authority	Builtin Object Token
IPS CA CLASE3 Certification Authority	Builtin Object Token
IPS CA CLASEA1 Certification Authority	Builtin Object Token



Issued To

Common Name (CN)	MVS098 Certificate Authority
Organization (O)	IBM
Organizational Unit (OU)	SWG
Serial Number	00

Issued By

Common Name (CN)	MVS098 Certificate Authority
Organization (O)	IBM
Organizational Unit (OU)	SWG

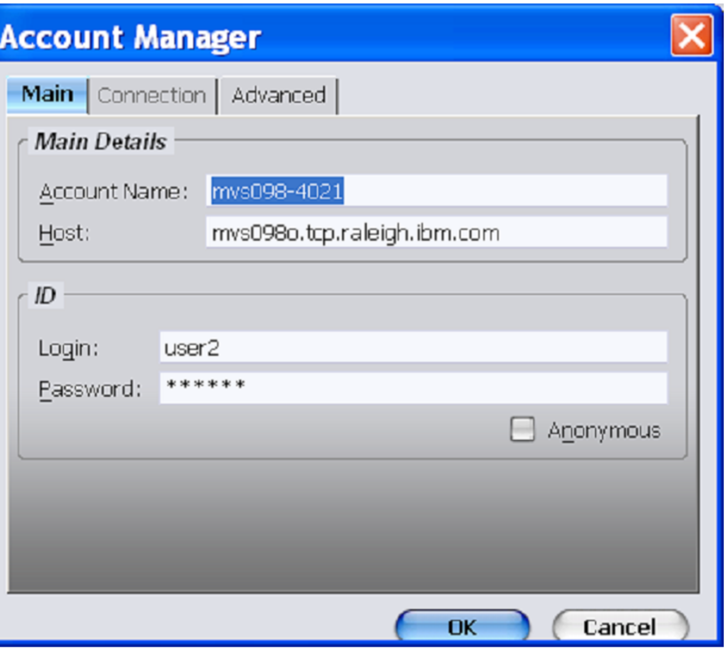
Validity

Issued On	12/31/2006
Expires On	12/31/2010

Fingerprints

SHA1 Fingerprint	72:0B:FD:0E:C0:9A:A1:E4:9C:12:20:BC:99:D0:F9:00:07:BB:23:8E
MD5 Fingerprint	AD:71:4C:CC:79:0E:9D:68:6B:4A:D2:21:33:60:45:77

FireFTP connection setup and sample log



Main Details

Account Name: mvs098-4021

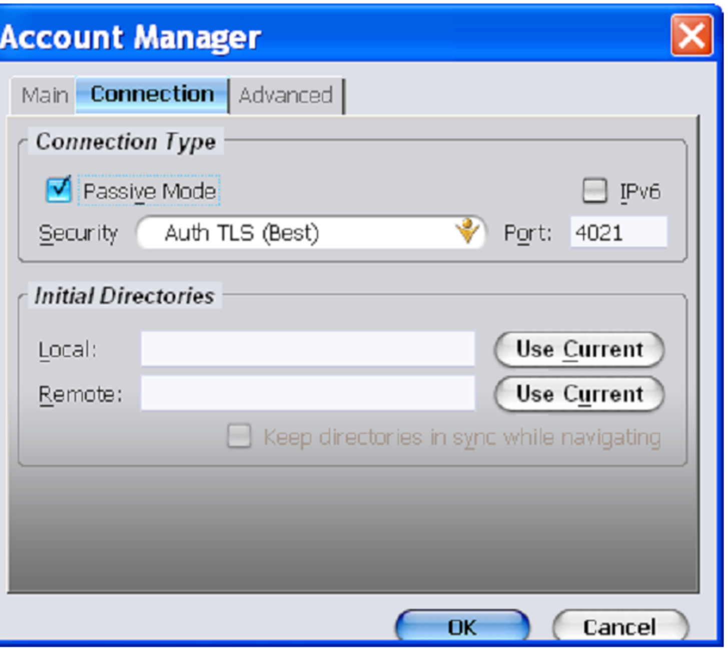
Host: mvs098o.tcp.raleigh.ibm.com

ID

Login: user2

Password: ******

□ Anonymous



Connection Type

☑ Passive Mode □ IPv6

Security: Auth TLS (Best) Port: 4021

Initial Directories

Local:

Remote:

□ Keep directories in sync while navigating

```
220-FTP40211 IBM FTP CS V1R9 at MVS098.tcp.raleigh.ibm.com, 16:07:23 on 2007-06-01.
220-*
220-* Welcome to the FTP server on MVS098.tcp.raleigh.ibm.com
220-* This system is used by Alfred for testing purposes.
220-* Any issues should be reported to
220-* Your host name is sig-9-49-152-174.mts.ibm.com
220-*
220 Connection will not timeout.
       AUTH TLS
234 Security environment established - ready for negotiation
       PBSZ 0
200 Protection buffer size accepted
       USER user2
331 Send password please.
       PASS (password not shown)
230-*
230-* USER2 - welcome to the FTP server on MVS098.tcp.raleigh.ibm.com
230-* Login time and date is Fri Jun 1 16:07:26 2007
230-* The current working directory is USER2.
230-*
230-Processing FTPS.RC configuration file - USER2.FTPS.RC
230-HFS directory / is the current working directory
230 USER2 is logged on. Working directory is "/".
       FEAT
211- Extensions supported
SIZE
MDTM
REST STREAM
UTF8
LANG en*
AUTH TLS
PBSZ
PROT
211 End
       PWD
257 "/" is the HFS working directory.
```

For more information....

URL	Content
http://www.ibm.com/systems/z/	IBM Mainframe
http://www.ibm.com/systems/z/hardware/networking/index.html	IBM Mainframe Networking
http://www.ibm.com/software/network/commserver/	Communications Server product overview
http://www.ibm.com/software/network/commserver/zos/	z/OS Communications Server overview
http://www.ibm.com/software/network/commserver/z_lin/	Communications Server for Linux on system z
http://www.ibm.com/software/network/ccl/	Communication Controller for Linux on system z
http://www.ibm.com/software/network/commserver/library/	Communications Server products - white papers, product documentation, etc.
http://www.ibm.com/systems/z/os/zos/bkserv/	z/OS Internet library - PDF versions of z/OS manuals (including z/OS CS)
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/support	Communications Server technical Support
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from ATS (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp	IBM education assistant