



Session: 403971/ 22CS

# iSeries. mySeries.

## iSeries Access for Windows: Security and Communications Tips

*Jeff Van Heuklon*

<http://www.ibm.com/servers/eserver/series/access/>

© Copyright IBM Corporation, 2004. All Rights Reserved.  
This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.

**iSeries. mySeries.**



## Agenda

- Connections with iSeries Access for Windows
  - Connection types supported
  - Configuration
  - Troubleshooting
- Using iSeries Access in an Internet Environment
  - Firewalls
    - Includes new info on Windows XP SP2
  - NAT
  - VPNs
  - Other Security Considerations
- Using iSeries Access with Terminal Services
  - Functions supported
  - iSeries Access restrictions
  - Windows 2000 considerations
- Appendix A: Example of terminal services install and config
- Appendix B: Example of internet connection through firewall

© 2004 IBM Corporation

**iSeries. mySeries.**



## Connection Types Supported

© 2004 IBM Corporation

**iSeries. mySeries.**



## iSeries Access for Windows Connectivity

- Windows 95/98/NT/2000/XP/2003 TCP/IP
  - LAN
  - PPP
  - SLIP
  - Twinax (requires separate TCP/IP driver)
- Any 32-bit Winsock 2.x or higher provider

Note: Windows XP support requires V5R1M0 version of Client Access Express and service pack SI01907. See Info APAR II12900 for information on restrictions

Windows 2003 requires V5R2M0 of iSeries Access for Windows and service pack SI07765 (for 32-bit) or SI08894 (for 64-bit). See Info APAR II13465 for information on restriction.

© 2004 IBM Corporation

**iSeries. mySeries.**



## LAN Connections

- LAN connections supported:
  - Token Ring (4M and 16M)
  - Ethernet
  - 100 M Ethernet
  - 1 Gig Ethernet
  - ATM
- If Windows supports a specific LAN card, it should work with iSeries Access for Windows



## Dial-up connections

- Windows PPP and SLIP direct to iSeries
  - Requires iSeries V4R2 or later
  - See TCP/IP Configuration and Reference (SC41-5420) for details



## TCP/IP over Twinax

- iSeries Access configuration is same as a LAN TCP/IP connection.
- However, the TCP/IP over twinax drivers are not shipped with iSeries Access.
- They can be obtained from the following URL:  
<http://www.networking.ibm.com/525tcpip/index.html>
- iSeries Access support statement is located in Info APAR ii11022.
- All 5250 Express cards are supported, some non-Express cards are supported.
- For Windows XP support, make sure the latest driver is obtained. There is no driver available for Windows Server 2003.



## Configuring and Managing Connections



## Managing Connections

- Managing of connections is integrated into iSeries Navigator
- iSeries Navigator can be used to create, delete, and change properties of connections.
- Connections can also be created by simply specifying the iSeries system name in the desired applications.

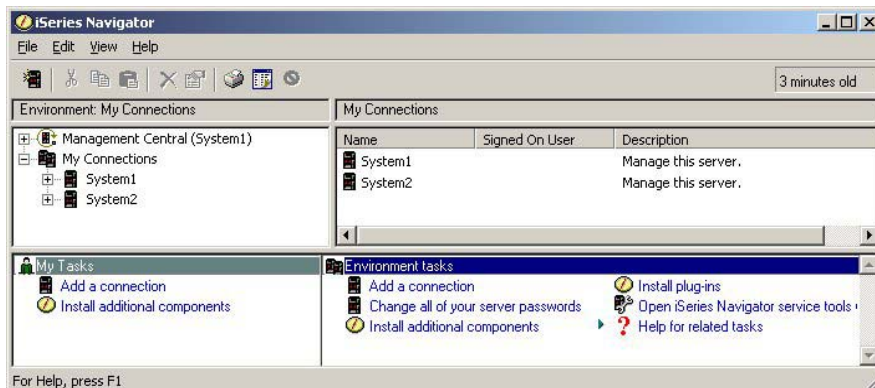
© 2004 IBM Corporation

**iSeries. mySeries.**



## iSeries Navigator Main Windows

- Left Window shows active environment and configured systems.
- Right Window shows contents of current selection.



© 2004 IBM Corporation

**iSeries. mySeries.**

## Creating a new connection

- Adding a new connection
  - Click on "Add Connection" icon on toolbar

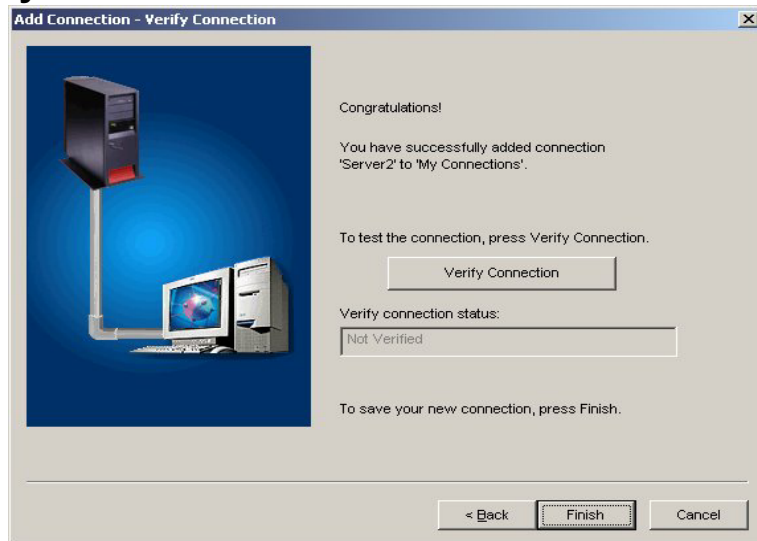
**Enter System Name or IP address**

## Sign-on Options

- Enter appropriate signon option



## Verify Connection



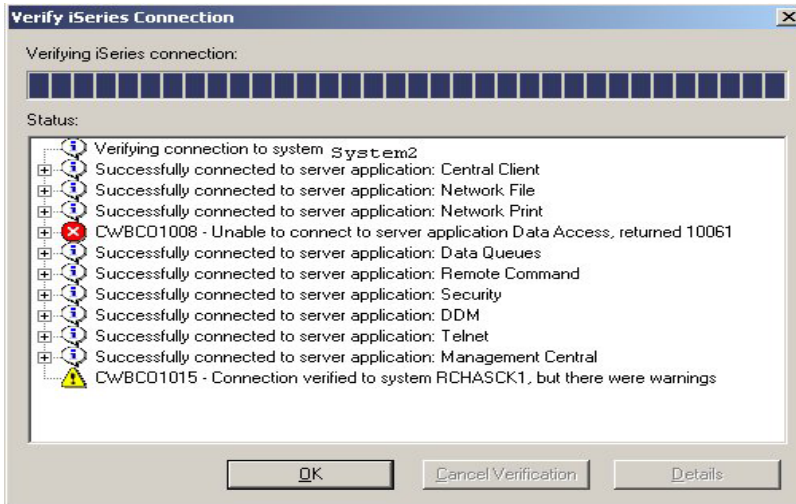
© 2004 IBM Corporation

**iSeries. mySeries.**



## Verification

- Verification screen allows detailed messages to be displayed when the "+" is clicked on.

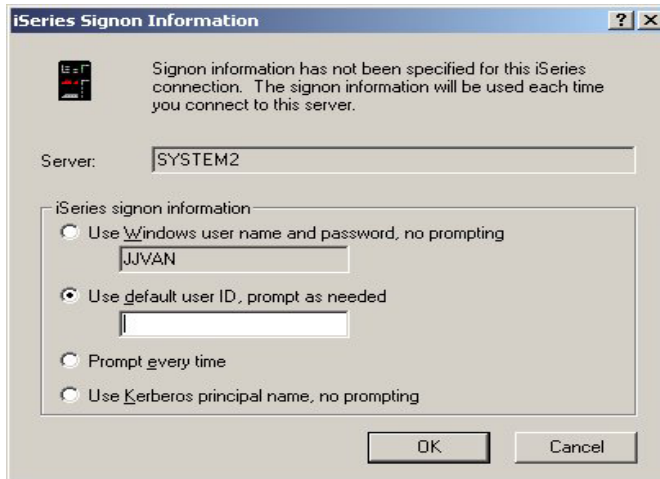


© 2004 IBM Corporation

**iSeries. mySeries.**

## Config-free connection

- Simply start up an application (like Data Transfer), specify a new system name, and you'll be prompted for signon option.

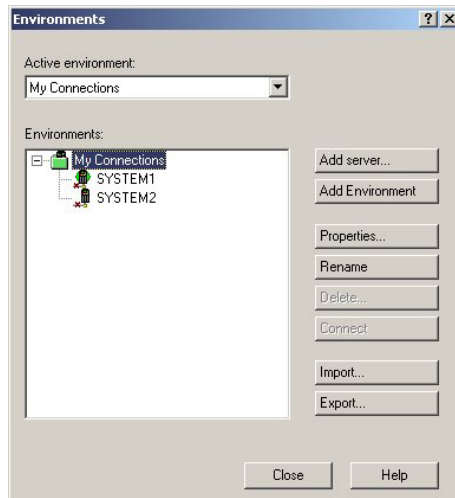


## Managing Environments & Connections

The Environments View offers a lot more interaction with the environments and connections.

The Environments View is opened from Operations Navigator by selecting [Connections to Servers - > Environments](#) from the File menu.

This will bring up the screen shown, which allows the user to manage all defined environments and iSeries connections. One can also define new ones.







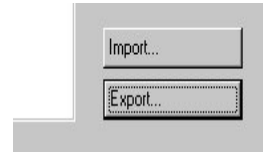
## Importing & Exporting Environments

The Export option allows the user to save the environment definition, including all connections it contains.

The environment will save the environment as a \*.ENV file. The default name of the file will be the name of the environment.

Then the Import option can be used to restore the environment, and the connections.

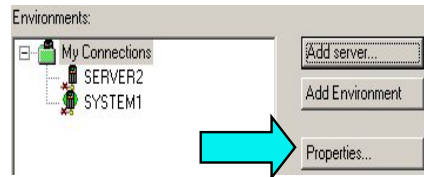
This can be useful to distribute common connection definitions to several PCs. The connections can be defined on one PC and then exported to a location where the other PCs can import the environment.



## Importing & Exporting Environments

Even though iSeries Access for Windows allows environments to be created with names that contain the characters \ / : \* ? " < > and |, the Windows operating systems will not accept these characters as part of a file name. So environments that contain these characters will not be able to be exported or imported.

## Properties



Selecting the Properties button allows the user to view or change the properties of either connections or environments.

Whatever connection or environment that is highlighted when the Properties button is selected will be displayed.

The only property of an environment is the default system.

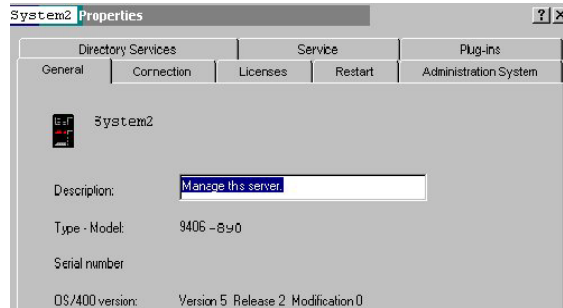
- The default system will specify which of the connections within the environment will be used to download a language conversion table from if the table isn't on the PC, if this environment is set to the active environment.
- The default system will also be the default system name presented when configuring a new PC5250 or Data Transfer session.

## System Connection Properties

## Properties

The properties of a connection display a lot more information.  
The following property tabs are available.

- General
- **Connection**
- **Secure Sockets**
- Licenses
- Restart
- Directory Services
- Plug-ins



Some of these properties will not be able to be interacted with if the connection isn't currently active. So the user might be prompted to signon to the system while interacting with the properties.

Note: Properties can also be accessed by right-clicking on the system name in iSeries Navigator

## More on Properties

- Changing Connection and Secure Sockets properties does not change active connections (including the iSeries Navigator session).
- After changing any properties, end any applications that are using a connection to that iSeries.
- Individual iSeries Access applications each can set their own connection properties, which may take precedence over the global properties set in iSeries Navigator.

## Connection Properties

- The Connection tab allows the user to modify the iSeries Signon Information and Performance preferences of the connection. Each of these will be discussed.

**System1 Properties**

General | **Connection** | Licenses | Restart | Directory Services | Service | Plug-ins

Signon information

Use Windows user name and password, no prompting

Use default user ID, prompt as needed

Prompt every time

Use Kerberos principal name, no prompting

Time-out for signon:  
 seconds (1-3600)

Performance

IP address lookup frequency:  IP address:

Where to lookup remote port:

Note: These values are used as defaults by other applications connecting from this PC to this server.

OK Cancel Help

## Connection Timeout Value -

- Rather than wait for a significant number of minutes for a connection attempt to timeout, shorten the timeout period for this PC.
- If the network is slow, you can give yourself a longer period of time to connect.
- The default is 30 seconds. If you have a slow connection, try increasing this value if you have trouble connecting.

General | **Connection** | Secure Sockets | Licenses | Restart | Directory Services | Service

Signon information

Use Windows user name and password, no prompting

Use default user ID, prompt as needed

**Prompt every time**

Time-out for signon:  
 seconds (1-3600)

## Performance Properties

- IP address lookup options

- Always
- One hour
- One day
- One week
- Never - Specify an IP address (host file entry needed for PC5250)
- After startup of PC

- Depending on your network, IP address resolution may take several seconds.

- Less frequent lookups improve performance.

- If IP address given as system name, no lookup occurs and no host file entry needed for PC5250

Performance

IP address lookup frequency:  IP address:

Where to lookup remote port:

Note: These values are used as defaults by other applications connecting from this PC to this AS/400 system.

## Performance Properties

- "Where to lookup remote port" options

- Server
  - Server mapper is always used for port resolution
- Local
  - Use the local Services file on PC to resolve. Note: All Client Access servers must then be added manually into this file.
- Standard
  - Always use the default port, no lookup

- Local and Standard will result in better performance, since server mapper does not have to be contacted first.

Performance

IP address lookup frequency:  IP address:

Where to lookup remote port:

Note: These values are used as defaults by other applications connecting from this PC to this AS/400 system.

## Performance properties

Performance

IP address lookup frequency: Always

Where to lookup remote port: Server

IP address: 9.9.9.9

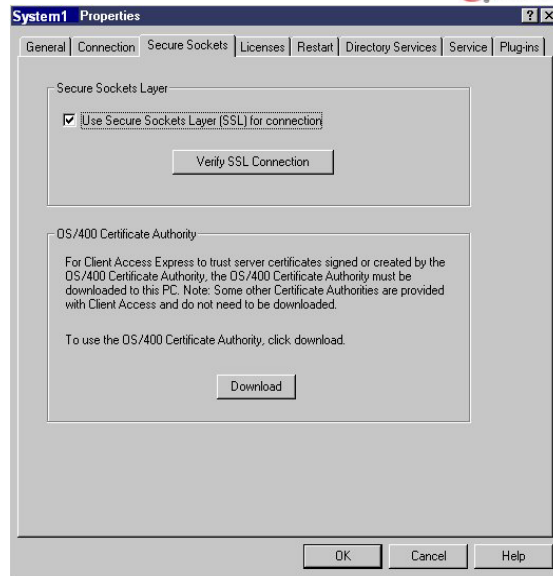
- IP Address
  - Lists last IP address used to access this iSeries
  - Cannot be changed from properties page, unless IP address lookup is changed to "Never".
- Note: iSeries Access for Windows does not update the Hosts file on your PC.

## Secure Sockets Properties and Support



## SSL Properties

- Secure Sockets
  - Enable/Disable SSL
  - Verify SSL Connections
  - Download Certificate Authority



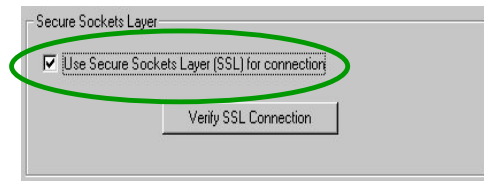
© 2004 IBM Corporation

**iSeries. mySeries.**



## Security Properties

- Specify if SSL should be used or not.
- SSL stands for Secure Sockets Layer, and specifies that encryption will be used for the sessions.
- Only SSL server authentication is supported. The exception is that client authentication has been added for PC5250 only in V5R1 and later.
- This option will be greyed out unless the 5769-CE1, CE2, or CE3 LPP is installed on the iSeries and the PC. The user must have access to: QIBM/ProdData/CA400/Express/SSL/SSLxxx, where xxx is 40, 56, or 128.
  - CE1 = 40-bit encryption (**no longer available in V5R1**)
  - CE2 = 56-bit encryption (**no longer available in V5R2**)
  - CE3 = 128-bit encryption



© 2004 IBM Corporation

**iSeries. mySeries.**



## SSL Information



- SSL is the current standard for World Wide Web security.
- When it is turned on, all data flows are encrypted, with the exception of the port mapper handshake.
- When it is turned off, all data flows unencrypted, with the exception of the connection password. If the emulator is being used, the password does flow in the clear as part of the telnet session (unless bypass signon is used).
- Always use encryption when communicating via the Internet to your iSeries.



## SSL InformationSSL Information

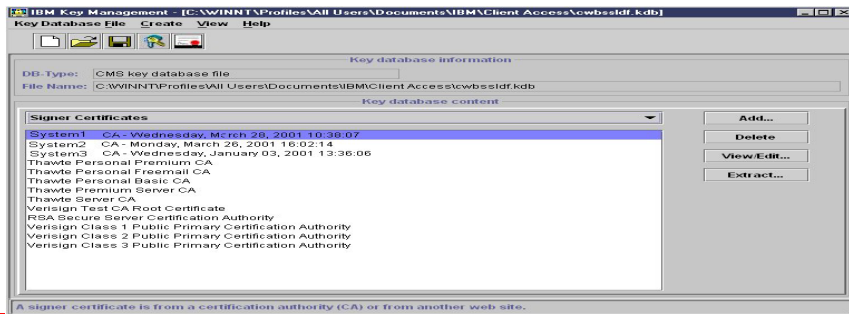
- Before making an SSL connection to an iSeries, the following must be true:
  - 5769-AC1, AC2, or AC3 must be installed on the iSeries (this is the iSeries side of SSL).
    - The encryption level (40, 56, or 128-bit) will be negotiated between the PC and the iSeries to the highest level supported by both.
  - A certificate must be available on the iSeries, and assigned to the iSeries Access Servers through the iSeries Digital Certificate Manager.
    - Note: Once certificate is available on iSeries, host servers will automatically be SSL-enabled.
  - The matching signer certificate or Certificate Authority must be available on the PC.





## Certificate Management

- IBM Key Management utility is included as part of installing CE1,2, or 3 on the PC.
- Can be accessed through Control Panel, under iSeries Access for Windows properties for Secure Sockets
- Recommend that a certificate by a well-known certificate authority (such as VerisignR) be used.
- A number of well-known certificate authorities are already stored in the key database.
- Using any other type of certificate will require transferring certificate authorities from other sources.



© 2004 IBM Corporation

**iSeries. mySeries.**



## Downloading Certificate Authorities

- Button is available to download CA from the iSeries
- The CA is automatically imported into the iSeries Access key database and the Java key database (required by iSeries Navigator).
- Previously, a separately downloadable utility had to be downloaded from the web to do this.

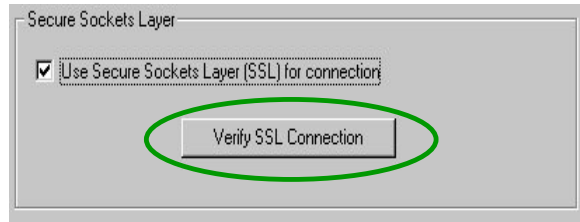


© 2004 IBM Corporation

**iSeries. mySeries.**

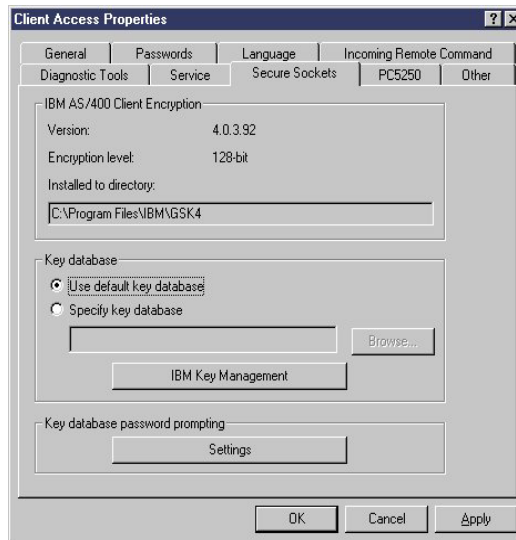
## Verify SSL Connections

- A verify button is included on the Secure Sockets properties page.
- This allow you to check if the iSeries Access servers are enabled for SSL.



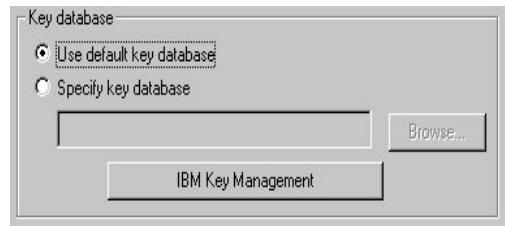
## PC5250 Client Authentication

- SSL client authentication can be enabled for the OS/400 Telnet server.
- iSeries Access for Windows PC5250 support has been enhanced to take advantage of this.
- SSL server authentication must always be configured before client authentication will work.
- No settings are required on the client to enable client authentication, but some preferences can be set.



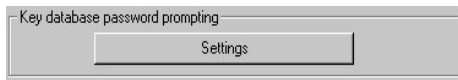
## Key Database Selection

- User can select which key database to use on their PC.
- For most users, keeping the default key database selection selected is fine.
- The IBM Key Management Utility can also be invoked from here to view the contents of key databases on your PC.



## Client Authentication Prompting modes

- Users can choose how often they are prompted for access to the key database.
- Its important to authenticate that the user has access to the key database before the certificate is sent up to the iSeries. Otherwise, someone could simply move the key database file to another PC and have access to the certificate.



Note: A policy can be used by an administrator to force one of these.





## Certificate Selection

- PC5250 configuration allows user to choose if they want to be prompted with a list of certificates to choose from to send to iSeries.

Configure PC5250

System name: [System] [Properties]

Workstation ID

Use Computer name  Add prefix to indicate printer or display

Use Windows user name  Avoid duplicate names on this workstation

Specify workstation ID  Avoid duplicate names with other workstations

[Text Field]

Connection

User ID signon information

[Use Operations Navigator default]

User ID: [Text Field]

Security

Current security: Not secured

Use Operations Navigator default

Not secured

Use Secured Sockets Layer (SSL)

Client certificate to use:

Select certificate when connecting

Use default

OK Cancel Help

Recommend just using the default.

© 2004 IBM Corporation



## Kerberos added to V5R2 version

iSeries Signon Information

Signon information has not been specified for this iSeries connection. The signon information will be used each time you connect to this server.

Server: [MYISERIESSYSTEM]

iSeries signon information

Use Windows user name and password, no prompting

[CMINER]

Use default user ID, prompt as needed

[Text Field]

Prompt every time

Use Kerberos principal name, no prompting

OK Cancel

- Support for Kerberos authentication of users
  - Kerberos ticket can replace the sending of userid and password from a PC to the iSeries.
  - Kerberos authentication as a new connection property to select

© 2004 IBM Corporation

**iSeries. mySeries.**



## Kerberos role in Single Sign-on

- Uses Kerberos protocol for authentication.
  - Network authentication protocol invented by MIT.
  - Freely available from MIT.
  - Ticket based, third party authentication scheme.
- Uses EIM (Enterprise Identity Mapping) to manage users in an enterprise.
  - Uses LDAP technology to keep track of who users are in an enterprise.

Did NOT implement a user ID and password synchronization tool.



## Overview of Kerberos signon process

- When you authenticate using Kerberos you get a Ticket-Granting-Ticket
- Services that use Kerberos authentication require the caller to provide an appropriate Service-Ticket (ST).
- iSeries Navigator client code requests a ST for krbsvr400/<host name> when using Kerberos
- The ST is what is sent to the iSeries at connect time in place of a userid and password.



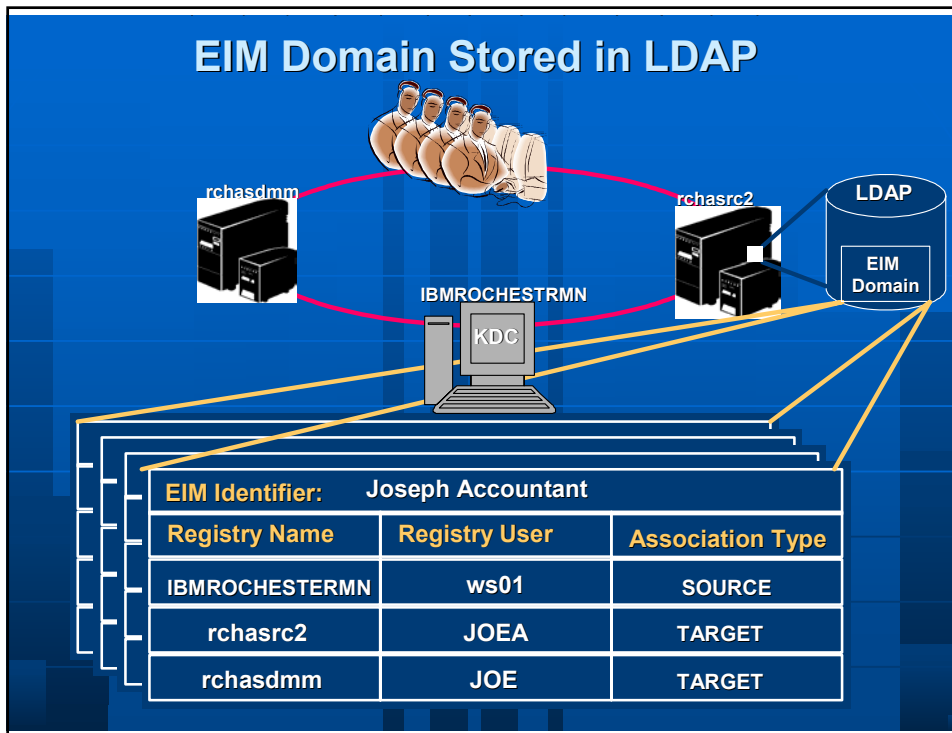


## EIM's role in Single Sign-on

- At this point, for Single Sign-On, Kerberos authentication is complete.
- However, Single Sign-On is not.
- iSeries System1 knows they received a valid ST from ws01 in the domain IBMROCHESTERMN
- What iSeries OS/400 profile should be used to complete the iSeries Navigator "open connection" for System1?
- EIM will provide that answer!

© 2004 IBM Corporation

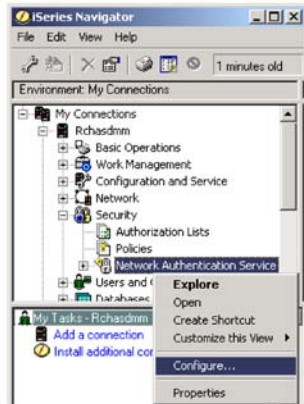
**iSeries. mySeries.**



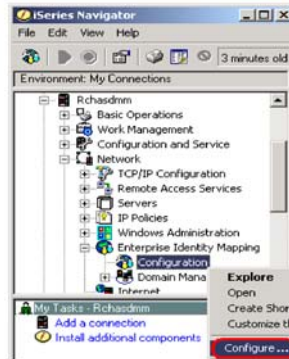


## Wizards available for configuring both Kerberos and EIM

### 1. Launch point



### Launch Point for EIM wizard



© 2004 IBM Corporation

**iSeries. mySeries.**



## More Info

- For more info On configuring SSL, recommend getting handouts for:
  - Session 25CS - Configuring iSeries Access to use SSL
- For mor info on configuring Kerberos and EIM:
  - Session 36CL - Kerberos: Single Sign-on Authentication

© 2004 IBM Corporation

**iSeries. mySeries.**



## Other Communication Support

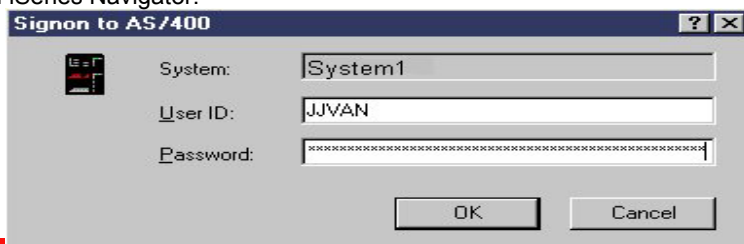
© 2004 IBM Corporation

**iSeries. mySeries.**



## Long Password Support

- Connections to V5R1 or later iSeries servers can be done with 128-character passwords, for better security.
- The Password Level (QPWDLVL) must be set to 2 or 3 for these long passwords to be used.
  - A value of 0 is the default and allows 1 to 10-character passwords.
  - A value of 1 allows 1 to 10-character passwords and iSeries Netserver passwords for Windows 95,98,Me will be removed from the system.
  - A value of 2 enables 1 to 128-bit passwords.
  - A value of 3 enables 1 to 128-bit passwords, and iSeries Netserver passwords for Windows 95,98,Me will be removed from the system.
- Password level can be modified in green screen, or through Security ->Policies within iSeries Navigator.



© 2004 IBM Corporation

**iSeries. mySeries.**





## Long Password Support (continued)

- Long passwords can have mixed case and can use virtually any character that can be keyed on the keyboard (including spaces that aren't trailing).
  - Be careful when using multiple languages, since it's possible to set a password on one PC, and not be able to enter it on another if they have different character sets.
- When making iSeries Netserver connections, be aware that by default, only Windows NT, 2000, XP, and 2003 PCs will be able to make that connection.

### Possible Password:

This password is so long that there is no way that I'll be able to remember it, so I'm going to make it a phrase I can recall.



## Data Compression -

- V5R1 and later iSeries Access communications supports data compression.
- This reduces network traffic and improves performance of data flows.
- Unicode data is also handled.
- Data compression is used by ODBC and remote command. This enables ODBC applications, iSeries Access Data Transfer, and iSeries Navigator to use compression.



## Troubleshooting

© 2004 IBM Corporation

**iSeries. mySeries.**



## Problem Diagnosis

If the connection fails to one of the servers with the message CWBCO1003 rc=10061, that is most likely because the server isn't active.

This can be verified from the NETSTAT \*CNN screen on the iSeries system to verify the server is in a \*Listen status. The server names are listed in the table on the next page.

If a server isn't listed the STRHOSTSVR command should be ran.

All Winsock/TCP/IP connection messages to iSeries Access for Windows will be displayed using the CWBCO1003 message. Check the online help message file for the meaning of the return codes associated with the message. This will be the same for SSL communications, which will display its return codes with the CWBCO1034 message.

© 2004 IBM Corporation

**iSeries. mySeries.**



## Tools for Troubleshooting

- CWBPING
  - Checks to see if iSeries can be connected to.
  - Checks to see if host servers are up.
  - If problems, messages indicate what is wrong.
- CWBCOTRC
  - Traces communications flows. Output can be sent into IBM Service personnel.

© 2004 IBM Corporation

**iSeries. mySeries.**



## CWBCOSSL tool

- One stop shop for working with SSL
  - CWBCOSSL.EXE installed into Client Access install directory.
- Makes it easier to debug problems with SSL connections.



© 2004 IBM Corporation

**iSeries. mySeries.**



## iSeries Access in an Internet Environment

- Getting through firewalls
- NAT
- VPNs (vs. SSL)
- Other security tips



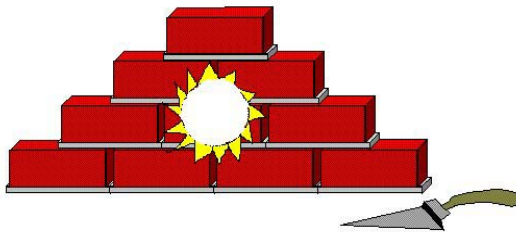
## Firewalls with iSeries Access

- Firewalls selectively filter TCP/IP traffic
- iSeries Access for Windows creates a challenge for firewalls.
- Different ports on the iSeries are used depending on what iSeries Access function is being used.
- Although all firewalls are different, what they have in common is that they can be configured to allow traffic through specific ports.



## IP Packet Filtering

- Firewall must be configured to allow specific ports to be opened.
- Use of IP packet filtering allows administrator to control this.
- This is so that each of the iSeries Access Servers on the iSeries can be reached (Telnet Server, Database Server, etc.).



© 2004 IBM Corporation

**iSeries. mySeries.**



## Servers and ports used

The following servers are used by iSeries Access for Windows. In addition to the servers listed, the Port Mapper (Port 449) is also used by all functions. However, if the user changes the Connection properties for an iSeries connection so that "Where to look up Remote Port" is set to 'Standard' or 'Local', then the Port Mapper will not be used. In addition, if a DNS server is to be accessed, Port 53 should be made available to the client.

Servers	Ports	Description
Port Mapper	449	Port mapper returns the port number for the requested server
Sign-on	8476 (9476)	Sign-on server is used for every iSeries Access connection to authenticate users and to change passwords
Central	8470 (9470)	Central server is used when an iSeries Access license is required, and also for downloading translation tables
Data Queue	8472 (9472)	Data Queue server allows access to the OS/400 data queues, used for passing data between applications
Database	8471 (9471)	Database server is used for accessing the OS/400 database
Remote Command	8475 (9475)	Remote command server is used to send commands from a PC to an iSeries and for program calls
File	8473 (9473)	File Server is used for accessing any part of the OS/400 file system
Print	8474 (9474)	Print Server is used to access printers known to the iSeries

© 2004 IBM Corporation

**iSeries. mySeries.**



## Servers and Ports Used (continued)

Servers	Ports	Description
Web Admin	2001 (2010)	Used to access web applications served by the iSeries
DDM	446 (448)	DDM server is used to access data via DRDA and for record level access
Telnet	23 (992)	Telnet server is used to access 5250 emulation
Netserver	137, 138, 139, 8474	iSeries Netserver allows access to iSeries integrated file system from Windows PCs
USF	8480	Ultimedia services is used for multimedia data
LDAP	389 (636)	Provides a network directory service
Mgmt Central	5555 5544 5577 (5566)	Management Central server is used to manage multiple iSeries in a network



## Notes on ports and servers

Note 1: the port number in parenthesis is the one used to connect to the server via SSL (encrypted session).

Note 2: Ports 449, 8xxx, and 9xxx can be started with the STRHOSTSVR \*ALL command. The others need to be started individually, or can be set to autostart when TCP/IP is started (as can 449, 8xxx, and 9xxx).

Note 3: Although 8474 is listed next to Netserver, it is only used internally, so does not have to be set in your firewall IP filtering. However, that server (Print server) must be started for Netserver to work properly.

Note 4: If any applications are registered under Application Administration, then the remote command server will be required in addition to what is listed below.



## Servers used by specific functions

iSeries Access Function	Servers Used
PC5250 display and printer emulation	Sign-on, Central, Telnet
Data Transfer	Sign-on, Central, Database
Base iSeries Navigator support	Sign-on, Remote Command
All Operations Navigator functions	Sign-on, Remote Command, File, Print, Database, Web Admin, Mgmt Central, USF, Netserver, LDAP, Data Queue
ODBC	Sign-on, Database
OLE DB	Sign-on, Database, DDM, Remote Command, Data Queue
AFP Viewer	Sign-on, Print
iSeries Access Install	Netserver
Incoming Remote Command	Uses no specific server, and iSeries port will vary. PC-side port is 512.
Fax support	Sign-on, Print

© 2004 IBM Corporation

**iSeries. mySeries.**



## Firewalls and Windows XP Service Pack 2

- By default, once Windows XP SP2 is installed, the Windows Firewall is automatically configured to prevent some incoming connections into the PC. This can affect the following iSeries Access for Windows functions:
  - Incoming Remote Commands
  - Operations Console
  - Management Central
- If you are using these functions, and they stop working once Windows XP SP2 is installed, here are steps you can take...

© 2004 IBM Corporation

**iSeries. mySeries.**



## Incoming Remote Command

- This uses port 512 by default
- Typical error messages would be:
  - CPE3447 "A remote host did not respond within the timeout period"
  - rexec:connect:Connection timed out
  - rexec: can't establish connection
- Solution:
  - Configure a port exception to allow incoming TCP connections on port 512:

```
C:\> netsh firewall add portopening TCP 512 "rexecd server (exec service, port 512)"
```

- OR -

Configure an application exception to allow the iSeries Access for Windows Remote Command service (cwbrxd.exe) to accept any incoming connection, regardless of port number or protocol:

```
C:\> netsh firewall add allowedprogram %windir%\cwbrxd.exe "iSeries Access Incoming Remote Command server"
```



## Operations Console

- Use ports 67 and 2112 for local (async and LAN) connections
- Can use any one of a number of different ports for RCS -> LCS connections
- Typical failures are:
  - When connecting an LCS (local connection), the status may not progress beyond "connecting console".
  - When connecting an RCS (remote connection) to an LCS that has not had all needed firewall exceptions configured, it may fail to connect; or it may connect, but fail to authenticate. The failure reason noted at the RCS may be that the local system is not configured to receive calls.





## Operations Console Continued

- Steps to correct:
- Configure a port exception to allow incoming UDP connections on port 67:
  - C:\> netsh firewall add portopening UDP 67 "bootp server (bootps service, port 67)"
- Configure a port exception to allow incoming TCP connections on port 2112 from the local PC (127.0.0.1) only:
  - C:\> netsh firewall add portopening TCP 2112 "Internal Op Console worker server (port 2112)" ENABLE CUSTOM 127.0.0.1
- Configure an application exception to allow the Operations Console program to accept any incoming connection, regardless of port number or protocol:
  - C:\> netsh firewall add allowedprogram <INSTALL>\cwbopcon.exe "iSeries Access Operations Console (cwbopcon)"



## Management Central

- Refer to:
- For V5R3:  
<http://publib.boulder.ibm.com/infocenter/iseries/v5r3/ic2924/info/experience/mcfirewall.pdf>
- For V5R2:  
<http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/experience/mcfirewall.pdf>



## Info on Web

- The preceding information on Windows XP SP2 is also available on the web at:
  - <http://www-1.ibm.com/servers/eserver/iseries/access/supportedos.htm>
  - Then click on the appropriate link in the Windows XP Professional section

© 2004 IBM Corporation

**iSeries. mySeries.**



## The iSeries Access for Web Alternative

Depending on your needs, if you don't want to mess with all the ports, iSeries Access for Web may be a solution:

- All traffic goes through a single HTTP port.
- SSL will also work using a single HTTPS port.
- All functions run as servlets on the iSeries
- No code to download to the client
- Good set of functions designed for end users:
  - Database access
  - File/Share access
  - printer and print output access
  - Messages
  - 5250 support
  - Customizable user interface
  - Commands

**Messages**

Access messages on your iSeries server with iSeries Access for Web.

[Display messages](#)

Display, answer and manage the messages in the message queue for the logged on user.

[Send message](#)

Send a message to users and message queues.

[Operator messages](#)

Operator messages

Display, answer and manage the messages in the system operator message queue.

[Message queues](#)

List message queues on the iSeries server. Select a message queue from this list and display messages.

© 2004 IBM Corporation

**iSeries. mySeries.**



## NAT (Network Address Translation)

- Configured through iSeries Navigator
  - Using the same interface used for setting IP packet filtering
- Primary use is to hide addresses when the iSeries is acting as the security gateway (no firewall).
- 3 forms of implementation on the the iSeries
  - Masquerade, or hide, NAT
  - Static, or map, NAT
  - Masquerade, or hide "port-mapped", NAT



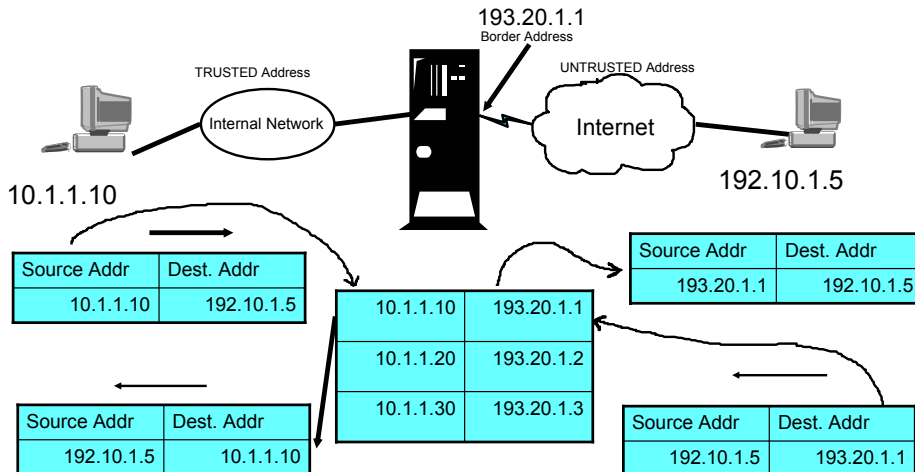
© 2004 IBM Corporation

**iSeries. mySeries.**



## Static NAT

- Used to enable systems on the internet to access servers in your internal network by translating actual internal server address to a public address.

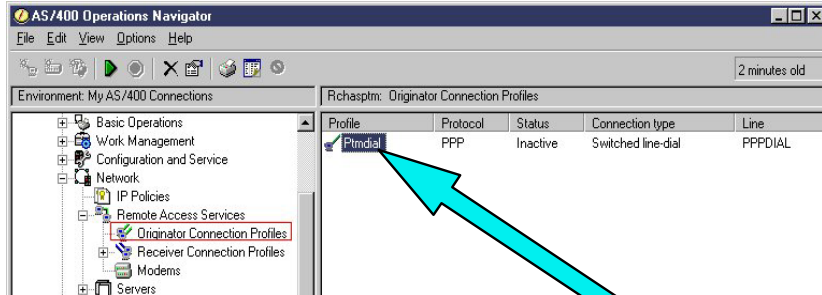


© 2004 IBM Corporation

**iSeries. mySeries.**

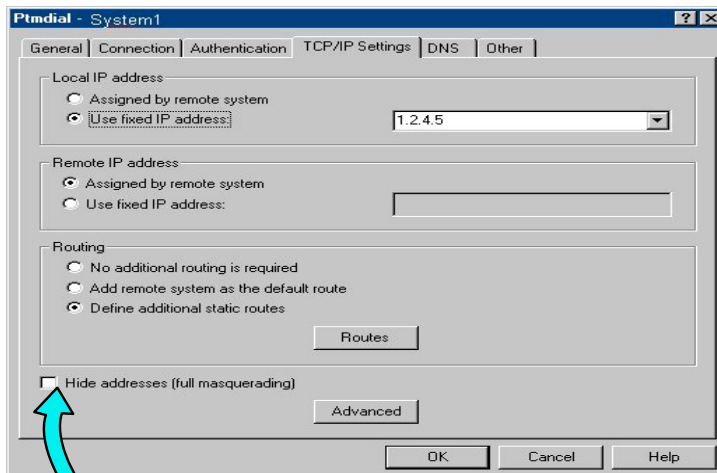
## Configuring NAT

- All configuration is done using iSeries Navigator



Right-click here and go to properties

## Configuring NAT

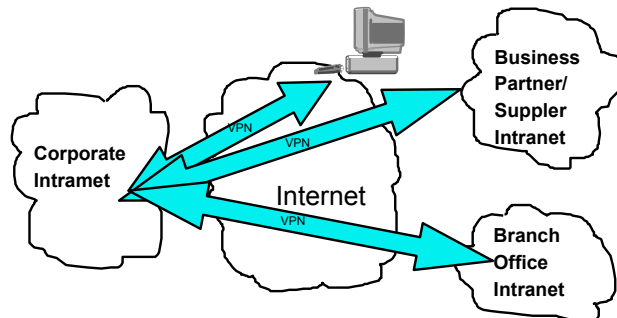


Click here to turn on hiding

## VPN Support

## VPNs (Virtual Private Networks)

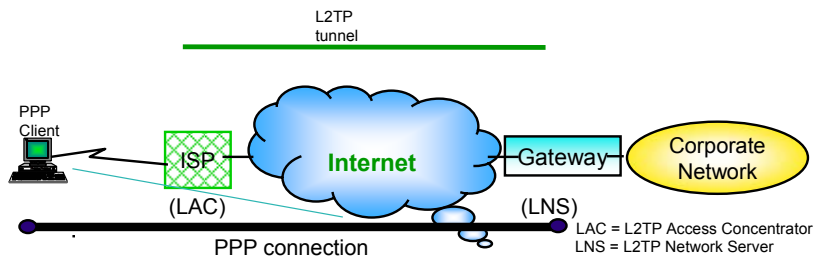
- VPNs use a combination of a tunneling protocol and encryption to ensure secure communications from a specific client to a specific server.
- A dedicated "pipe" is assigned for all client/server communications.



## VPN and encryption

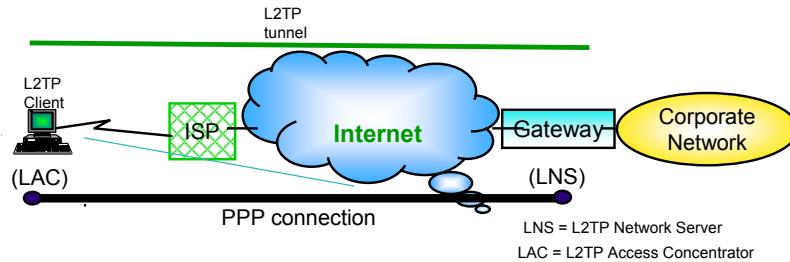
- IPSec is the standard encryption used by VPN.
- The IPSec support is usually built into the VPN client support, which is a separately purchasable and installable program. It is built into Windows 2000 and XP

## L2TP Compulsory Tunnel



- 1 The remote user initiates a PPP connection to an ISP.
- 2 The ISP accepts the connection and the PPP link is established.
- 3 The ISP now undertakes a partial authentication to learn username.
- 4 ISP maintained database maps users to services and LNS tunnel endpoint.
- 5 LAC then initiates L2TP tunnel to LNS.
- 6 If LNS accepts connection, LAC then encapsulates PPP with L2TP, and forwards over the appropriate tunnel.
- 7 LNS accepts these frames, strips L2TP, and processes them as normal incoming PPP frames.
- 8 LNS then uses PPP authentication to validate user and then assigns IP address.

## L2TP Voluntary Tunnel

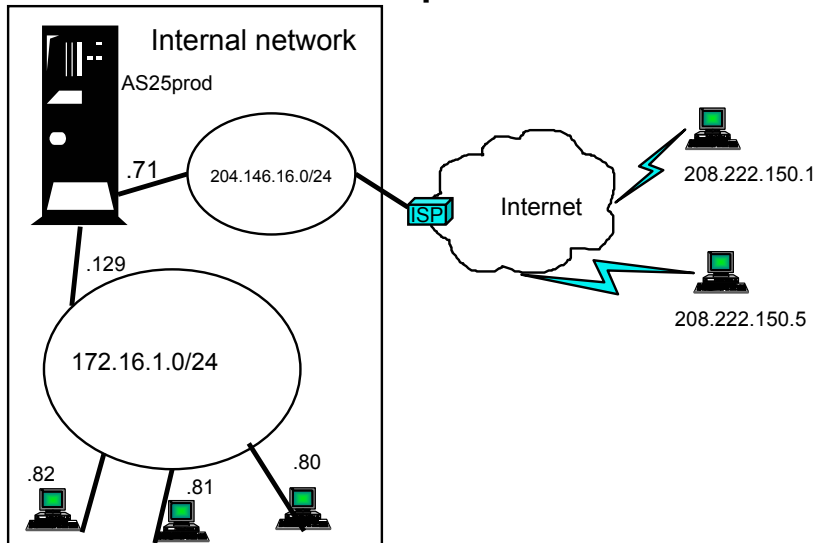


- The remote user has pre-established connection to an ISP.
- L2TP Client(LAC) initiates L2TP tunnel to LNS.
- If LNS accepts connection, LAC then encapsulates PPP and L2TP, and forwards over tunnel.
- LNS accepts these frames, strips L2TP, and processes them as normal incoming frames.
- LNS then uses PPP authentication to validate user and then assign IP address.

## Windows 2000 VPN Support

- Windows 2000, 2003 and XP have IPSec and L2TP built-in
- RSA signature mode authentication uses digital certificates rather than preshared keys (passwords) for IKE authentication. RSA Signature mode authentication allows us to support Windows 2000/XP clients with dynamically assigned IP addresses.

## Windows 2000 VPN Example



## Windows 2000: Implementation tasks

1. Verifying the IP connectivity
2. Assigning the Certificate Authority (CA) trust to the OS/400 VPN Key Manager using the OS/400 Digital Certificate Manager (DCM)
3. Creating a server certificate using DCM
4. Creating a VPN connection using the VPN connection wizard
5. Verifying the system-wide responding policy
6. Creating an L2TP Receiver Connection Profile for the iSeries
7. Reviewing the IP packet rules created by iSeries Navigator
8. Obtaining the certificates for the Windows 2000 workstation
9. Configuring the IP Security Architecture for Microsoft Windows 2000
10. Configuring L2TP for Microsoft Windows 2000
11. Start the VPN connection
12. Verifying connectivity on the Windows 2000 workstation
13. Verifying connectivity on the iSeries system





## VPN comparison to SSL

Feature	SSL	VPN
Data Confidentiality	Yes	Yes
Authentication	Server Mandatory. Client Optionally	Yes (VPN Server)
Requires application support	Yes	No
Requires host support	Yes	Yes
Services	SSL-enabled servers and clients	All
Client Configuration	Required for each application	Required for VPN server.
Filter Configuration	Individual filter by service (more complex)	IKE+IPSec filters (simpler configuration)
Availability for Windows clients	<b>Most iSeries SSL-enable servers have a corresponding SSL-enabled SSL client</b>	Standard in Windows 2000  Lack of support on 95/98/NT

© 2004 IBM Corporation

**iSeries. mySeries.**



## Session on VPNs

- 33CM - iSeries VPN Technologies and Solutions
- 32CM - iSeries TCP/IP Remote Access

© 2004 IBM Corporation

**iSeries. mySeries.**



## Prestart jobs

© 2004 IBM Corporation

**iSeries. mySeries.**



## Using prestart jobs for IP security

- Prestart jobs for sockets run by default in QUSRWRK
- A user can make these prestart jobs run in different subsystems (daemon jobs will continue to run in QUSRWRK).
- This was done so that prestart jobs don't clutter us QSYSWRK.
- Administrators can better control who can connect

© 2004 IBM Corporation

**iSeries. mySeries.**



## Configuring where prestart jobs run

- Configuration is done in iSeries Navigator
- Right-click on server name, and go to its properties. Click on "Add".
- Specify where the prestart job should run (or not run) for any client IP address, or range of IP addresses.
- Can specify that if the subsystem entered cannot be started, that the job will either be rejected, or will try to run in QUSRWRK.



## Prestart job config screen

Client information

Description:

Client:

IP address:

IP address range:  ..

Subnet mask:

Subsystem:

Alternate action:



## Other Security Tips

© 2004 IBM Corporation

**iSeries. mySeries.**



## General Security Tips

- Only start the TCP/IP servers that are really needed
- Use non-routable private IP addresses in internal network
- Prevent application from using well-known ports
- Turn IP Source Routing off
- Allow IP datagram forwarding only when needed
- Do not leave PPP or SLIP line waiting in answer state.
- Use IP packet filtering on your iSeries
- Use NAT if possible
- Prevent unauthorized use of well-known ports by preventing the users that can use the ports.
- Use iSeries auditing and journaling
- Use exit programs to control access to servers

© 2004 IBM Corporation

**iSeries. mySeries.**



## Telnet security considerations

- Limit the number of signon attempts (QMAXSIGN system value)
- Set QAUTOVRT to automatically create enough virtual devices. Then set QAUTOVRT to 0.
- Use inactivity time-out (INACTTIMO) parameter on the Telnet configuration to reduce the exposure when a user leaves a telnet session unattended.
- Restrict powerful user profiles from access a telnet session



## Terminal Server Environment



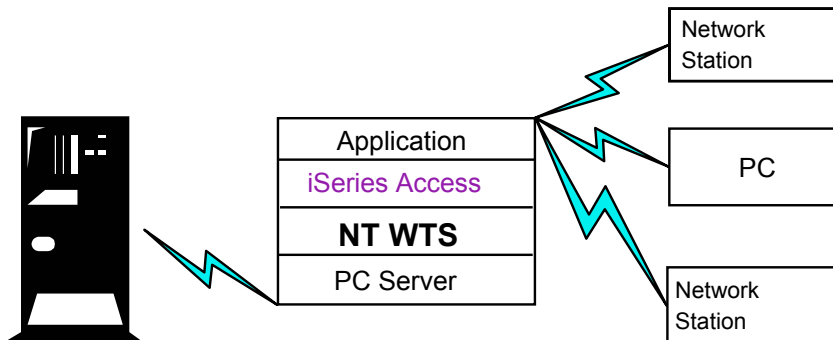
## What is Terminal Server<sub>R</sub>?

- A multi-user version of NT 4.0, Windows 2000, and Windows 2003
- Allows multiple, simultaneous client sessions to be run on a single server
- End-users can use Windows<sub>R</sub>, DOS<sub>R</sub>, network stations, Unix, or Macs<sub>R</sub>.
- Follow-on from NCD's WinCenter<sub>R</sub> and Citrix's WinFrame<sub>R</sub> from NT 3.51<sub>R</sub>.
- Most standard Windows-based applications don't need modification to run on Terminal Server.



## Where iSeries Access fits in

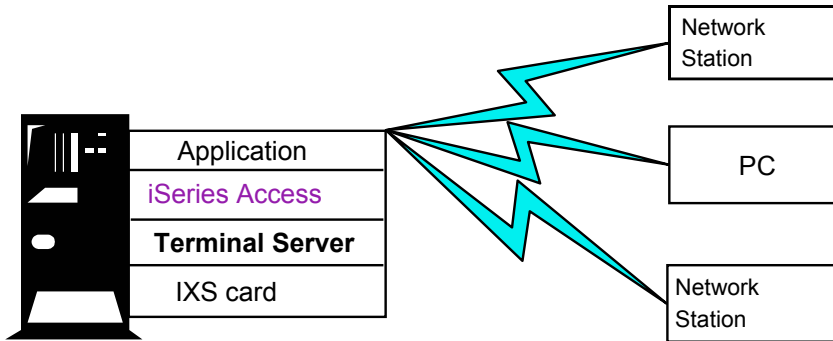
- iSeries Access<sub>R</sub> for Windows can run on Terminal Server, either on a standalone server.....





## Where Client Access fits in

- Or on an Integrated XSeries Server card in the iSeries



© 2004 IBM Corporation

**iSeries. mySeries.**



## Citrix Metaframe

*Metaframe Application Server for Windows*

- Thin-Client/Server Computing
  - Applications are deployed, managed, supported, and executed completely on a server
  - Requirements
    - Multi-user operating system
    - Remote presentation services (MetaFrame = ICA)
    - Centralized applications and client management

© 2004 IBM Corporation

**iSeries. mySeries.**



## Metaframe Heterogeneous Computing Environment Extensions

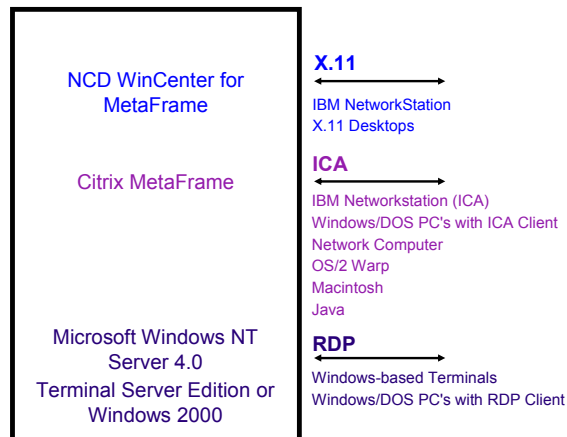
- Clients
  - Hardware
    - Intel 286,386,486, Pentium
    - Windows-based Terminals
    - Network Computers
    - Through OEM Partners:
    - X.11 based devices
  - Operating Systems
    - Windows 3.1
    - Windows for Workgroups 3.11
    - Windows 95/98
    - Windows NT 3.51/4.0
    - Windows 2000/XP/2003
    - Windows CE
    - DOS
    - UNIX
    - OS/2 Warp
    - Macintosh
    - Java
    - Browser client
- Network Protocol
  - TCP/IP
  - IPX/SPX
  - NetBIOS / NetBEUI
  - SLIP/PPP
  - Direct Asynch

© 2004 IBM Corporation

**iSeries. mySeries.**



## Multi-User NT Summary



© 2004 IBM Corporation

**iSeries. mySeries.**





## iSeries Access for Windows Installation

- Use the Add/Remove Programs applet in the control panel to invoke the iSeries Access for Windows Setup program.
- Switch to Install Mode using the chgusr command (chgusr /install) prior to invoking setup from the command line. After completing the install, switch back to execute mode using chgusr (chgusr /execute).



## Support Position with iSeries Access for Windows

- Client Access Express and iSeries Access have been tested with most of its functions.
- Functions are supported on Windows clients (thru RDP) as well as through Citrix Metaframe.
- Functions include:



## iSeries Access functions supported

- -PC5250 emulation
- ODBC
- - iSeries Navigator
- - Data Transfer
- - PC5250 Print Emulation
- - Data Queue APIs
- - Database APIs
- - Remote Command APIs
- - NLS APIs
- - DPC
- - Transforms
- - Policies
- - Directory Update
- - Properties
- - Command Line Remote Command



## Non-support of Incoming Remote Command

- This function, which allows PC commands to be initiated by the iSeries, is not supported on Terminal Server.
- The current implementation does not allow the routing of the PC command to the proper client workstation.



## Use of NTFS with iSeries Access

- In V5R1, problems accessing directories and registry entries with the NTFS file system were addressed.
- Strategy was to store most user-writable files in " My Documents" directory where it made sense. That is the Microsoft-recommended way to handle.
- Tried not to move existing files when upgrading from an older release to V5R1.



## Windows NT, 2000, and 2003 NTFS Users

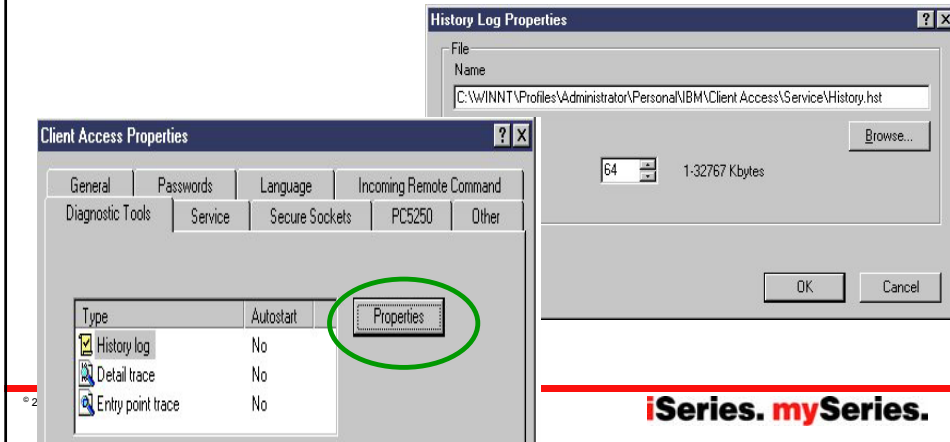
- By default, PC5250 files still go into the Client Access Install directory.
- Recommend changing to "My documents".
- Always should be writable.
- User can specify any path, but there is no guarantee that it will be writable.



**New NT File System (NTFS) support**

## Service Locations

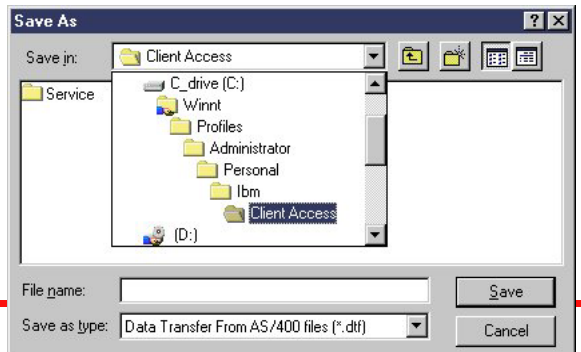
- Service
  - History Log
    - Personal or My Documents location (different for each operating system)
  - Detail and Entry Point Trace files
    - Personal or My Documents location (different for each operating system)
  - Change the locations from Control Panel->Client Access, Diagnostics Tools page



**iSeries. mySeries.**

## Data Transfer Requests

- Save and Open locations
- Default location
  - Personal or My Documents location (different for each operating system)
- If users have saved to or opened from a different location before, that location will displayed.
- Data Transfer "remembers" this location. This way, users on upgraded systems that have saved transfer requests will continue to see them where they saved before.





## Summary

© 2004 IBM Corporation

**iSeries. mySeries.**



## Summary

- iSeries Access for Windows is supported in a number of different TCP/IP environments
- Can be configured for improved performance and security.
- Access through firewalls requires ports to be opened.
- VPNs are supported on Windows 2000, XP, and 2003 clients
- There are other methods of improving security of your connections
- Terminal Server environment is supported

© 2004 IBM Corporation

**iSeries. mySeries.**



## References

- Client Access web site: <http://www.ibm.com/eserver/series/clientaccess/>
- COMMON Session 25CS, "Configuring the iSeries Access Servers to Use SSL"



## Appendix: Firewall/NAT example with Client Access



## Firewall Configuration Example

- The following information shows how IP Forwarding can be used to configure an iSeries Access connection to an iSeries through a firewall.
- Shows how to permit mobile users on the Internet to access your iSeries behind the Firewall using iSeries Access and Telnet. Since the users are mobile, their IP address is unknown.
- IP filtering is used.
- Assume:
  - 192.168.2.1 is your iSeries Server's IP address
  - 5.5.5.5 is the public IP address that represents your iSeries on the Internet.



## Example - Using NAT to map iSeries address

- From a client behind the firewall, point a web browser at the iSeries, port 2001. For example, if the iSeries is named myas400.priv.abc.com then point the web browser at
  - <http://myas400.priv.abc.com:2001>
  - Select the "IBM Firewall for AS/400" link
  - Select "Configuration" in the left frame
  - To configure the NAT settings, select "NAT" in the right frame
  - Click on the "Insert" button
  - Choose "MAP" from the list of actions, and then click on the OK button
  - After configuring the NAT settings (as shown below), select "Configuration" in the left frame
  - To configure the filter rules (settings), select "Filters" in the right frame
  - After configuring the filter settings, select "Administration" in the left frame
  - Select "Status" in the right frame
  - Restart both NAT and Filters
- If 5.5.5.5 is NOT the non-secure IP address of your Firewall, then you can do this with 1 simple NAT setting:
  - MAP 192.168.2.1 0 5.5.5.5 0



## Using NAT (continued)

- MAP 192.168.2.1 23 5.5.5.5 23 (For telnet)
  - MAP 192.168.2.1 449 5.5.5.5 449 (Port Mapper)
  - MAP 192.168.2.1 8470 5.5.5.5 8470 (Central server - Needed whenever PC5250 or Data Transfer is used)
  - MAP 192.168.2.1 8471 5.5.5.5 8471 (Database server)
  - MAP 192.168.2.1 8472 5.5.5.5 8472 (DataQueues server)
  - MAP 192.168.2.1 8473 5.5.5.5 8473 (File server)
  - MAP 192.168.2.1 8474 5.5.5.5 8474 (Print server)
  - MAP 192.168.2.1 8475 5.5.5.5 8475 (Remote command server)
  - MAP 192.168.2.1 8476 5.5.5.5 8476 (Signon server)
  - MAP 192.168.2.1 8480 5.5.5.5 8480 (Ultimedia server)
  - MAP 192.168.2.1 9480 5.5.5.5 9480 (Ultimedia server with SSL on)
  - MAP 192.168.2.1 5555 5.5.5.5 5555 (Management Central server)
  - MAP 192.168.2.1 5556 5.5.5.5 5556 (Management Central server with SSL on)
- 
- MAP 192.168.2.1 446 5.5.5.5 446 (DDM server - Sometimes used by Client Access OLE DB support)
  - MAP 192.168.2.1 448 5.5.5.5 448 (DDM server with SSL on)
  - MAP 192.168.2.1 5110 5.5.5.5 5110 (MAPI server - Needed if these Mail APIs are being used)
  - MAP 192.168.2.1 992 5.5.5.5 992 (Telnet with SSL on)
  - MAP 192.168.2.1 9470 5.5.5.5 9470 (Central Server with SSL on)
  - MAP 192.168.2.1 9471 5.5.5.5 9471 (Database Server with SSL on)
  - MAP 192.168.2.1 9472 5.5.5.5 9472 (DataQueues server with SSL on)
  - MAP 192.168.2.1 9473 5.5.5.5 9473 (File Server with SSL on)
  - MAP 192.168.2.1 9474 5.5.5.5 9474 (Print Server with SSL on)
  - MAP 192.168.2.1 9475 5.5.5.5 9475 (Remote command server with SSL on)
  - MAP 192.168.2.1 9476 5.5.5.5 9476 (Signon server with SSL on)

If 5.5.5.5 is the non-secure IP address of your Firewall, then you will need to add these NAT settings. In addition, your router must be configured so that all traffic destined to 5.5.5.5 with subnet mask 255.255.255.255 is routed to the non-secure IP address of your firewall.



## More port info

- The only required ports are 8476 and 449. The other ports will only need to be opened if you are using a function that they support. Most users will want to open 23, 449, and 8470 thru 8476.
- Also, be aware that parts of iSeries Navigator, which is part of iSeries Access, also use port 2001 (and 2010 for SSL) to access the Web Admin server. A mapping rule like those above for the scenario when 5.5.5.5 is the non-secure IP address cannot be used for those 2 ports, since this would cause the firewall not to work (it uses those ports). If you need to use those functions of iSeries Navigator from outside of the firewall, then you need to set up your network so that 5.5.5.5 is NOT the non-secure IP address of your Firewall.
- This means acquiring an additional publicly registered IP address that is NOT the same as the firewall's public IP address.
- Then, add the following Filter settings:









## Example of setting filter rules

**0010: action(permit) from(1.2.3.\*) to (10.10.10.\*) protocol(all any 23/any 23)**

 <a href="#">Configuration</a>  <a href="#">Administration</a>	Action:	<input type="text" value="permit"/>	From Address:	<input type="text" value="10.10.10.0"/>	From Mask:	<input type="text" value="255.255.255.0"/>		
	To Address:	<input type="text" value="1.2.3.0"/>	To Mask:	<input type="text" value="255.255.255.0"/>	Protocol:	<input type="text" value="all"/>		
	From Operation:	<input type="text" value="any"/>	Port/ICMP Type:	<input type="text" value="23"/>	To Operation:	<input type="text" value="any"/>	Port/ICMP Code:	<input type="text" value="23"/>
	Interface:	<input type="text" value="both"/>	Routing:	<input type="text" value="both"/>	Direction:	<input type="text" value="both"/>	IP Fragments:	<input type="text" value="(y) Match all"/>
	IP Packet Logging:	<input type="text" value="no"/>	VPN:	<input type="text" value="0"/>	Description:	<input type="text" value="telnet"/>		

© 2004 IBM Corporation

**iSeries. mySeries.**



## Trademarks and Disclaimers

© IBM Corporation 1994-2004. All rights reserved.  
References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:  
*Instruction: Refer to the following URL: <http://www.ibm.com/legal/copytrade.shtml>. Edit the list below, IBM subsidiary statement, and special attribution companies which follow so they coincide with your presentation.*

AS/400	e-business on demand	i5/OS
AS/400e	IBM	OS/400
eServer	IBM (logo)	
	iSeries	

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.  
Linux is a trademark of Linus Torvalds 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.  
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.  
Other company, product or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

© 2004 IBM Corporation

**iSeries. mySeries.**