

IBM

@server

iSeries

Windows environment on iSeries





@server

iSeries

Windows environment on iSeries

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 175.

Ninth Edition (August 2005)

This edition applies to version 5, release 3, modification 0 of IBM iSeries Integration for Windows Server (product number 5722-WSV) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 1998, 2005. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Windows environment on iSeries	1
Chapter 2. What's new for V5R3	3
Chapter 3. Print this topic	5
Chapter 4. Concepts	7
Hardware concepts	7
Software concepts	9
Networking concepts	10
Private networks	10
Virtual Ethernet networks.	11
External networks	13
I Windows console	14
Advantages	14
Considerations	15
Performance and capacity	16
User and group concepts	17
Types of user configurations	19
User enrollment templates	20
Password considerations.	21
Terminology	21
Chapter 5. Install and configure Windows environment on iSeries	23
Hardware requirements	23
Software requirements	25
Prepare for the installation of integrated Windows servers	26
Machine pool size requirements	27
Time synchronization	28
Configure OS/400 TCP/IP for integrated Windows servers	28
iSeries Access for Windows on integrated Windows servers	29
Enable iSeries NetServer	29
Create a guest user profile for iSeries NetServer	29
Install IBM iSeries Integration for Windows Server licensed program.	30
Plan for the installation of Windows server	30
Network server descriptions.	31
Installation worksheet for OS/400 parameters	31
Comparison of FAT, FAT32, and NTFS file systems	41
Tip: Find resource names when you have multiple integrated servers	42
Supported language versions	42
Install Windows 2000 Server or Windows Server 2003	43
Start the installation from the OS/400 console	44
Continue the installation from the integrated Windows server console	46
Complete the server installation	46
Upgrade the IBM iSeries Integration for Windows Server licensed program	47
Upgrade your server from Windows NT 4.0 to Windows 2000 Server	48
Upgrade the integrated Windows server side of the IBM iSeries Integration for Windows Server licensed program.	50
Migrate from 285x or 661x to 2890 Integrated xSeries Server hardware	51
Windows Cluster Service.	53
Install Windows Cluster service	54
Install Windows Cluster service on a new integrated Windows server	54
Install Windows Cluster service on an existing server	55

Prepare Windows before installing Windows Cluster service	55
Install Windows Cluster service on Windows	57
Install Windows Cluster service on Windows 2000 Server	57
Install Windows Cluster service on Windows Server 2003	58
Enabling QNTC access to Windows Server 2003 with Active Directory	59
l Install the ATI Radeon 7000M video device drivers for Windows 2000 on the 2892-002 or 4812-001	
l Integrated xSeries Server.	59
l Adjust hardware acceleration for Windows Server 2003 on the 2892-002 or 4812-001 Integrated	
l xSeries Server.	60
Respond to error messages during installation	60
Set an integrated Windows server to automatically vary on with TCP/IP	61
Code fixes	61
Types of code fixes.	62
Synchronize the integration software level using the integrated Windows server console	62
Synchronize the integration software level using iSeries Navigator	63
Synchronize the integration software level using a remote command	63
Chapter 6. Network integrated servers	65
Configure virtual Ethernet networks	65
Configure Inter-LPAR virtual Ethernet networks	66
Explore point-to-point virtual Ethernet networks	67
External networks	68
Create line descriptions for external network adapters	68
Add a TCP interface for a new shared network adapter	69
Install network adapter device drivers and add adapter address information to an integrated	
Windows server	69
Remove network adapters	70
Chapter 7. Administer integrated Windows servers	75
Start and stop an integrated server	75
Start and stop an integrated Windows server using iSeries Navigator	75
Start and stop an integrated Windows server using the character-based interface	76
Shutdown an integrated server from the Windows server console	76
How to safely shutdown your iSeries when integrated Windows servers are present	76
External host LAN issues	77
l Connect to the 4812 IXS virtual serial console	77
View or change integrated Windows server configuration information	78
Message logging.	78
Run integrated Windows server commands remotely	79
Guidelines for submitting remote commands	80
SBMNWSCMD and file level backup support for Kerberos v5 and EIM	81
Chapter 8. Manage storage	83
OS/400 storage management	83
Disk drives for integrated Windows servers	84
Predefined disk drives for integrated Windows servers	85
Administer integrated Windows server disk drives from OS/400	86
Access the OS/400 integrated file system from an integrated server	86
Obtain information about integrated server disk drives	86
Add disk drives to integrated Windows servers.	87
Create an integrated server disk drive	87
Link a disk drive to an integrated server	87
Format integrated server disk drives	89
Copy a disk drive	89
Unlink integrated Windows server disk drives	90
Delete integrated Windows server disk drives	90

Use Windows disk management programs with integrated Windows servers	91
Chapter 9. Share devices	93
Determine the device description and hardware resource names for iSeries devices	93
Use iSeries optical drives with integrated Windows servers	93
Use iSeries tape drives with integrated Windows servers	94
Format a tape on OS/400 for use with integrated Windows servers	95
Allocate the iSeries tape drive to an integrated Windows server	95
Return control of a tape drive from an integrated Windows server to the iSeries	96
Supported iSeries tape drives	96
Identify iSeries tape devices for applications	97
Transfer control of the iSeries tape and optical drives between integrated Windows servers	97
Print from an integrated Windows server to iSeries printers	98
Chapter 10. Administer integrated Windows server users from OS/400	99
Enroll a single OS/400 user to the Windows environment using iSeries Navigator	99
Enroll an OS/400 group to the Windows environment using iSeries Navigator	100
Enroll OS/400 users to the Windows environment using the character-based interface	100
Create user templates	100
Specify a home directory in a template	102
Changing the LCLPMDMGT user profile attribute	102
Enterprise Identity Mapping (EIM)	102
End user enrollment to the Windows environment	104
End group enrollment to the Windows environment	104
The QAS400NT user.	105
Preventing enrollment and propagation to an integrated Windows server.	107
Chapter 11. Back up and recover integrated Windows servers	109
Back up the NWSD and disk drives associated with an integrated Windows server	109
Back up the NWSD of an integrated Windows server	110
Back up predefined disk drives for integrated Windows servers created on V4R5 and later OS/400 systems.	110
Back up predefined disk drives for integrated Windows servers created on pre-V4R5 OS/400 systems.	111
Back up user-defined disk drives for an integrated Windows server.	112
Save and restore user enrollment information.	112
What objects to save and their location on OS/400.	113
Back up individual integrated Windows server files and directories	115
File-level backup restrictions	115
Preliminary administrator setup tasks	116
Create shares on integrated Windows servers	116
Add members to QAZLCSAVL file	117
Ensure iSeries NetServer and the integrated Windows server are in same domain	117
Save your files	118
Examples: How to address parts of an integrated Windows server	118
Windows Backup utility	119
Restore an integrated Windows server's NWSD and disk drives	119
Restore predefined disk drives for integrated Windows servers created on V4R5 and later systems	120
Restore predefined disk drives for integrated Windows servers created on pre-V4R5 systems	120
Restore user-defined disk drives for integrated Windows servers on iSeries	121
Restore integrated Windows server NWSDs	122
Recover integrated Windows server files	122
Chapter 12. Uninstall the Windows server operating system from the integrated server hardware	125
Delete an integrated Windows server's NWSD	125

Delete an integrated Windows server's line descriptions	126
Delete TCP/IP interfaces associated with an integrated Windows server	126
Delete controller descriptions associated with an integrated Windows server	126
Delete device descriptions associated with an integrated Windows server	127
Delete the IBM iSeries Integration for Windows Server licensed program	127
Chapter 13. Troubleshoot integrated Windows servers	129
Check message and job logs.	129
Monitor job	130
Problems with integrated Windows servers	130
Blue screen errors.	131
A full integrated server system drive	131
Remapping a full C drive; for integrated servers created pre-V4R5 only	132
Optical device problems	133
Locked optical device for a failed server.	133
Tape problems	133
Verify that the iSeries Tape Drive device driver is loaded	134
Problems starting an integrated Windows server	134
Vary-off failures.	136
NWSD configuration file errors	136
Repair the NWSD configuration file	136
Reset the NWSD configuration file parameter.	136
Use a previous version of the integrated server file	136
DASD in Integrated xSeries Adapter attached xSeries servers	137
HSL communication problems with the Integrated xSeries Adapter	137
Failures enrolling users and groups	137
User-enrollment authorization problems	138
Password problems	139
IBM iSeries Integration for Windows Server snap-in program	140
Virtual Ethernet connection problems	141
Both line description and icon are present	142
Line description is present and icon is missing	142
Line description is missing and icon is present	143
Both line description and icon are missing	143
Problems with external networks when using external host LAN	143
General problems with external networks	145
Manually update LAN drivers on the integrated Windows server	146
Begin the LAN driver installation or update.	146
Select the adapter to install or update	147
Complete the LAN driver installation or update	147
Private LAN IP address conflicts	148
Assign private LAN IP addresses	149
IP forwarding problems	150
TCP/IP failure between OS/400 and Windows	150
Problems accessing Windows Server 2003 shares using the QNTC file system	151
IFS access problems.	151
Problems with saving integrated Windows server files	151
Unreadable messages in the server message queue	152
Problems getting a Windows system memory dump	153
Reinstall an integrated Windows server	153
Collect integrated Windows server service data	154
Create an integrated Windows server memory dump on OS/400.	154
Use the network server description (NWSD) dump tool on OS/400	155
Chapter 14. Network server description configuration files	159
NWSD configuration file format	159

Create an NWSD configuration file	160
Example: NWSD configuration file	160
Remove lines from an existing integrated server file with CLEARCONFIG entry type	161
TARGETDIR keyword	161
TARGETFILE keyword	162
Change an integrated server file with ADDCONFIG entry type	162
VAR keyword	162
ADDSTR keyword	163
ADDWHEN keyword	163
ADDWHEN and DELETEWHEN expression operators	163
DELETEWHEN keyword	164
LINECOMMENT keyword	164
LOCATION keyword	164
LINESEARCHPOS keyword	164
LINESEARCHSTR keyword	164
LINELOCATION keyword	164
FILESEARCHPOS keyword (ADDCONFIG entry type)	164
FILESEARCHSTR keyword	165
FILESEARCHSTROCC keyword	165
REPLACEOCC keyword	165
TARGETDIR keyword	165
TARGETFILE keyword	165
UNIQUE keyword	166
VAROCC keyword	166
VARVALUE keyword	166
Change an integrated Windows server file with UPDATECONFIG entry type	166
FILESEARCHPOS keyword (UPDATECONFIG entry type)	167
FILESEARCHSTR keyword (UPDATECONFIG entry type)	167
FILESEARCHSTROCC keyword (UPDATECONFIG entry type)	167
Set configuration defaults with the SETDEFAULTS entry type	167
ADDWHEN	168
DELETEWHEN	168
FILESEARCHPOS keyword (SETDEFAULTS entry type)	168
FILESEARCHSTR keyword (SETDEFAULTS entry type)	169
TARGETDIR	169
TARGETFILE	169
Use substitution variables for keyword values.	169
Chapter 15. Related information	173
Appendix. Notices	175
Trademarks	176
I Terms and conditions for downloading and printing information	176

Chapter 1. Windows environment on iSeries

Windows® environment on iSeries™ is more of an idea than any one piece of hardware or software. It is a way for iSeries and Personal Computers (PCs) to work together, and what is more, to allow the iSeries to control PCs in order to make them easier to administer.

The first part of Windows environment on iSeries is the PC hardware which must be added to the iSeries. There are two basic ways of doing this.

- By using an *Integrated xSeries® Adapter (IXA)*, the iSeries can control IBM® xSeries servers. IBM calls its line of PCs *xSeries servers*.
- An *Integrated xSeries Server (IXS)* is an iSeries expansion card which contains Random Access Memory (RAM) and an Intel™ processor. It can be thought of as a PC which has been transplanted inside the frame of an iSeries.

The second part is the IBM iSeries Integration for Windows Server licensed program (5722–WSV) which is installed on the iSeries to give it the capability to control PCs. These PCs are then called integrated Windows servers.

Finally, it is necessary to install Microsoft's Windows 2000 Server or Windows Server 2003 software.

This document is divided into the following sections

Chapter 2, “What’s new for V5R3,” on page 3

Changes and improvements made this release.

Chapter 3, “Print this topic,” on page 5

Print a PDF of this document.

Chapter 4, “Concepts,” on page 7

Understand the Windows environment on iSeries solution.

Chapter 5, “Install and configure Windows environment on iSeries,” on page 23

Follow these instructions to install a new integrated Windows server from scratch.

Chapter 6, “Network integrated servers,” on page 65

Learn how to use the three different types of networks available to integrated servers.

Chapter 7, “Administer integrated Windows servers,” on page 75

Start and stop the server, run integrated server commands remotely, view and change configuration information, and monitor message and error logs.

Chapter 8, “Manage storage,” on page 83

Information about integrated server hard disks.

Chapter 10, “Administer integrated Windows server users from OS/400,” on page 99

Integrate OS/400® users into the Windows environment.

Chapter 9, “Share devices,” on page 93

Use iSeries devices on integrated servers.

Chapter 11, “Back up and recover integrated Windows servers,” on page 109

This section describes ways to back up integrated server files to tape drives or iSeries hard disks.

Chapter 12, “Uninstall the Windows server operating system from the integrated server hardware,” on page 125

Everything you need to know to remove integrated server software from your system.

Chapter 13, “Troubleshoot integrated Windows servers,” on page 129

Find answers to common questions.

Chapter 14, “Network server description configuration files,” on page 159

You can customize your integrated servers by creating your own configuration files.

Chapter 15, “Related information,” on page 173

Chapter 2. What's new for V5R3

For V5R3, Windows environment on iSeries has several new functions:



- Users enrolled to the Windows environment from OS/400 can now manage their passwords in Windows. See “Types of user configurations” on page 19.
- Enterprise Identity Mapping (EIM) user enrollment support allows easier setup for Windows single sign-on and also allows enrolled OS/400 user profiles to be different than Windows users profiles. See “Enterprise Identity Mapping (EIM)” on page 102.
- SBMNWSCMD and file level backup now provide limited support for kerberos v5 authentication. See “SBMNWSCMD and file level backup support for Kerberos v5 and EIM” on page 81.
- The maximum network server storage space size has been increased from 64,000 MB to 1,024,000 MB.
- The iSeries now automatically updates its system time for daylight savings time changes. See “Time synchronization” on page 28.
- A new NWSD attribute (SHUTDTIMO) allows you to specify how long integrated Windows servers are given to shut-down when they are varied off. See “Installation worksheet for OS/400 parameters” on page 31.
- The disk statistics displayed through the WRKNWSSTG command and through iSeries Navigator are now more accurate.
- Windows NT[®] 4.0 is no longer supported and should be upgraded to Windows 2000 Server. See “Upgrade your server from Windows NT 4.0 to Windows 2000 Server” on page 48. It is not possible to upgrade a Windows NT 4.0 server to Windows Server 2003. You must delete the existing Windows NT 4.0 server and install a new integrated server with Windows Server 2003.

| **What's new as of 18 October 2004**

- | • Support is added for the 4812–001 Integrated xSeries Server.
- | • Support is added for the 2689-002 Integrated xSeries Adapter.

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The  image to mark where new or changed information begins.
- The  image to mark where new or changed information ends.

To find other information about what's new or changed this release, see the Memo to Users.

Chapter 3. Print this topic

To view or download the PDF version of this document, select Windows environment on iSeries (about 1.4 MB).


You can view or print PDFs of related manuals and Redbooks™ from Chapter 15, “Related information,” on page 173.

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

You need Adobe Acrobat Reader to view or print these PDFs. You can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html)  .

Chapter 4. Concepts

In this document we will often use the term *integrated Windows server*, or just *integrated server*. With this term we are referring to an instance of Microsoft® Windows 2000 Server or Windows Server 2003 running on an Integrated xSeries Server or on an xSeries Server attached to an iSeries with an Integrated xSeries Adapter. Just as the term PC is often used to refer to Microsoft's Windows operating system software running on an Intel based microprocessor and associated hardware, we use the term integrated Windows server to refer to the combination of hardware and software which make up the entire product.


Read the following conceptual articles:

- "Hardware concepts"
- "Software concepts" on page 9
- "Networking concepts" on page 10
- "Windows console" on page 14
- "Advantages" on page 14
- "Considerations" on page 15
- "Performance and capacity" on page 16
- "User and group concepts" on page 17
- "Terminology" on page 21

Hardware concepts

Understand the essential difference between an Integrated xSeries Server (IXS), and an Integrated xSeries Adapter (IXA) attached xSeries server.

Comparison of IXS with IXA attached xSeries Server

<p>iSeries</p>  <p>IXS</p>	<p>An IXS is a PC server processor and memory 'transplanted' inside the frame of an iSeries.</p>
---	--

Comparison of IXS with IXA attached xSeries Server

iSeries

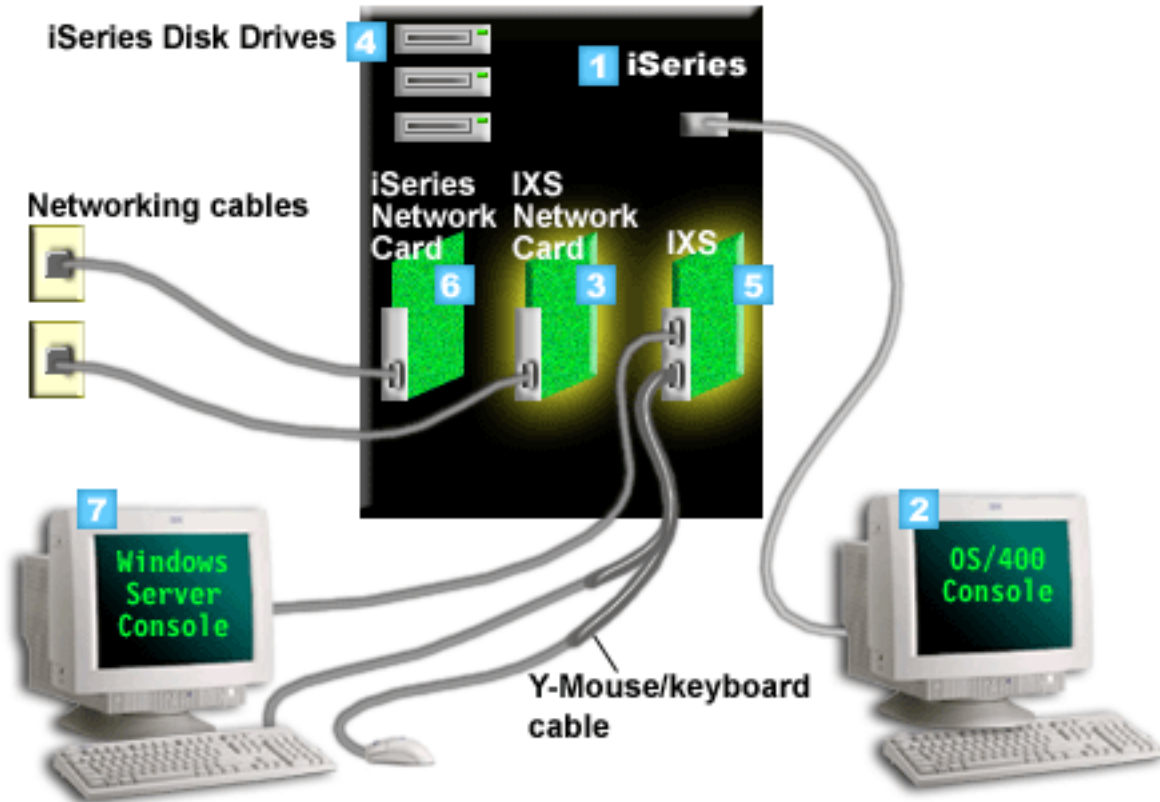


An IXA is a high-speed link (HSL) bus adapter plugged into a supported xSeries Server. The xSeries Server appears as an HSL attached expansion unit to the iSeries server.


IXA attached integrated servers are standard xSeries server models, containing processors, memory, and expansion cards, but no disks. All the disk space is housed in the iSeries and managed in the same way as for IXS models.

The installation procedure for an IXA attached integrated Windows server is almost identical to that for an IXS integrated server. The major difference between them is that since new xSeries servers are released more often than IXSs, updated capabilities are available more rapidly. Also, IXA attached xSeries servers have their own expansion slots, so they are far more expandable than IXSs. For example, some customers use these slots to attach devices like CD-ROM drives and modems.

The following graphic illustrates a typical IXS installation

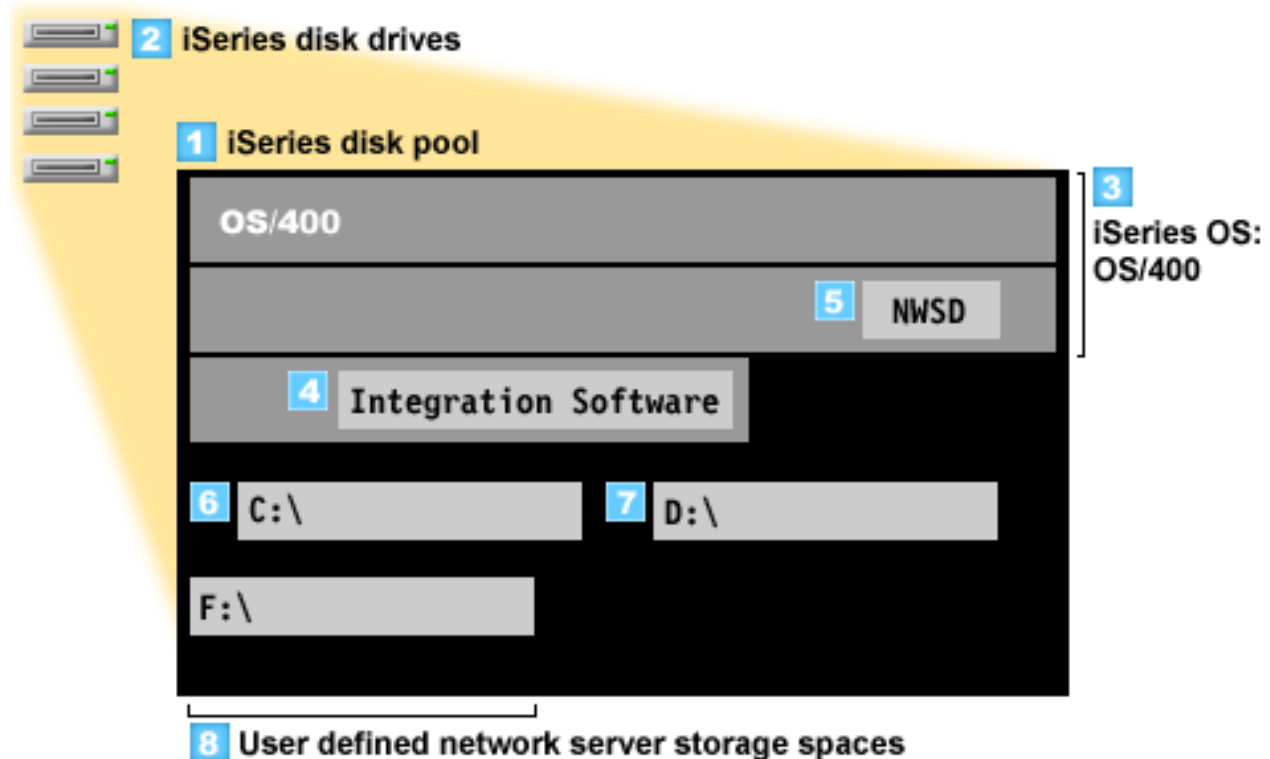


1. First you need a compatible iSeries. (See the “Hardware requirements” on page 23) section for compatibility information.)
2. The OS/400 console, from which you connect to the iSeries using iSeries Navigator or the character-based interface, is shown to make clear the distinction between it and the Windows console.
3. Depending upon the IXS type, there are different ways to provide network connectivity. Some types of IXSs can ‘take over’ adjacent PCI slots, allowing the IXS to control an iSeries network card (see “Hardware requirements” on page 23 for information about which network cards are supported). You can install up to three network cards in this way. Other types of IXSs have integrated network controllers and do not support network cards in adjacent slots.
4. An integrated server does not have its own hard disk drive. OS/400 emulates hard disk space for it to use from iSeries hard disk drives.
5. The IXS card itself is an Intel processor with its own RAM, mounted on a PCI board and plugged into an iSeries expansion slot. The IXS physically occupies two slots.
6. A typical iSeries will have a network card.
7. A Windows console allows you to interact with the integrated server. A Windows console may consist of a monitor, keyboard, and mouse directly attached to the IXS card. For more information about this and other types of Windows consoles, see “Windows console” on page 14.

For additional hardware information check the IBM Windows Integration  Web site. (www.ibm.com/servers/eserver/iseries/windowsintegration)

Software concepts

This graphic represents iSeries hard disk space and the different files and pieces of software which make Windows environment on iSeries work.



1. OS/400 combines all storage devices connected to the system into one or more disk pools.
2. An iSeries user never comes into direct contact with physical hard disks.

3. OS/400 itself is stored in objects within disk pool number 1.
4. In order for OS/400 to work with integrated servers, you must expand its capabilities by installing the IBM iSeries Integration for Windows Server licensed program.
5. A network server description (NWSD) object is created during the installation of an integrated server. An NWSD is a configuration object. It links an integrated server's software and hardware together.
6. During the installation process two default network server storage spaces are created in OS/400. One is the integrated server's C:/ drive, which is where Microsoft's Windows server software is installed. It also contains the part of the IBM iSeries Integration for Windows Server licensed program which runs on the integrated server.
7. The D:/ drive contains files used during installation.
8. The user can define up to 30 user created storage spaces (46 with Windows clustering service). These appear as hard disk drives to Windows server which can be used to store user data.

Networking concepts

There are two main types of networking available for integrated servers.

- **Virtual Networks**
 These networks are simulated inside of the iSeries and do not require networking cards or cables. They can be divided into two types.
 - “Private networks”
 These are the control networks which exist between integrated servers and the iSeries.
 - “Virtual Ethernet networks” on page 11
 These are networks created inside the iSeries between integrated servers, OS/400 partitions, and other partitions (such as Linux).
- “External networks” on page 13
 These are the normal Windows networks which all servers use, created by networking through physical network cards controlled by the integrated server.

Private networks

OS/400 needs a way to communicate with its integrated Windows servers. This communication takes place over a private network. When an integrated server is installed a special virtual network is created between it and a controlling OS/400 partition. This network is called private because it has only two endpoints, the integrated server and the iSeries, and also because, like a virtual Ethernet network, it is emulated within the iSeries and no physical network adapters or cables are used.

There are two types of private networks

- **Point-to-point virtual Ethernet**

| This is the newest type of private network. It is supported in newer IXSs (Type 2890, 2892, or 4812)
 | and in IXA (Type 2689) attached xSeries servers, and requires release V5R2 or later of IBM iSeries
 | Integration for Windows Server. In OS/400, it is configured as an Ethernet line description with Port
 | Number value *VRTETHPTP.

- **Virtual Token-ring Internal LANs (Internal LANs)**

This type of private network is available for Integrated Netfinity® servers (resource type 6617 or 2850), for Windows NT 4.0, or pre-V5R2 installations of IBM iSeries Integration for Windows server on any supported IXS or IXA attached xSeries server. It is configured as a token-ring line description with the port number value *INTERNAL.

When you run the Install Windows server (INSWNTSVR) command it will decide which type of network to configure based on the data you provide, saving you from having to decide which type of private network to create. The INSWNTSVR command will configure a point-to-point virtual Ethernet, the newest and preferred type, when possible.

You may wonder what makes a private network different from a virtual Ethernet network. The answer is that private networks are configured differently and can only have two endpoints: the iSeries and an integrated server. They only support the TCP/IP protocol, and use restricted IP addresses in private domains by default, so the addresses are not passed through gateways or routers. These addresses take the form of 192.168.xxx.yyy, where xxx is the hardware resource number. (Xxx and yyy can be from 1 to 3 digits.) For example, for an IXS that is defined with hardware resource number LIN03, the IP address will be 192.168.3.yyy. The OS/400 and Windows sides of the private network will receive the lowest odd/even unused yyy pair to complete the IP addressing. In our example, the OS/400 side of the private network will be given the IP address 192.168.3.1, and the Windows side has 192.168.3.2. As you define multiple line descriptions for the same hardware resource, yyy is incremented.

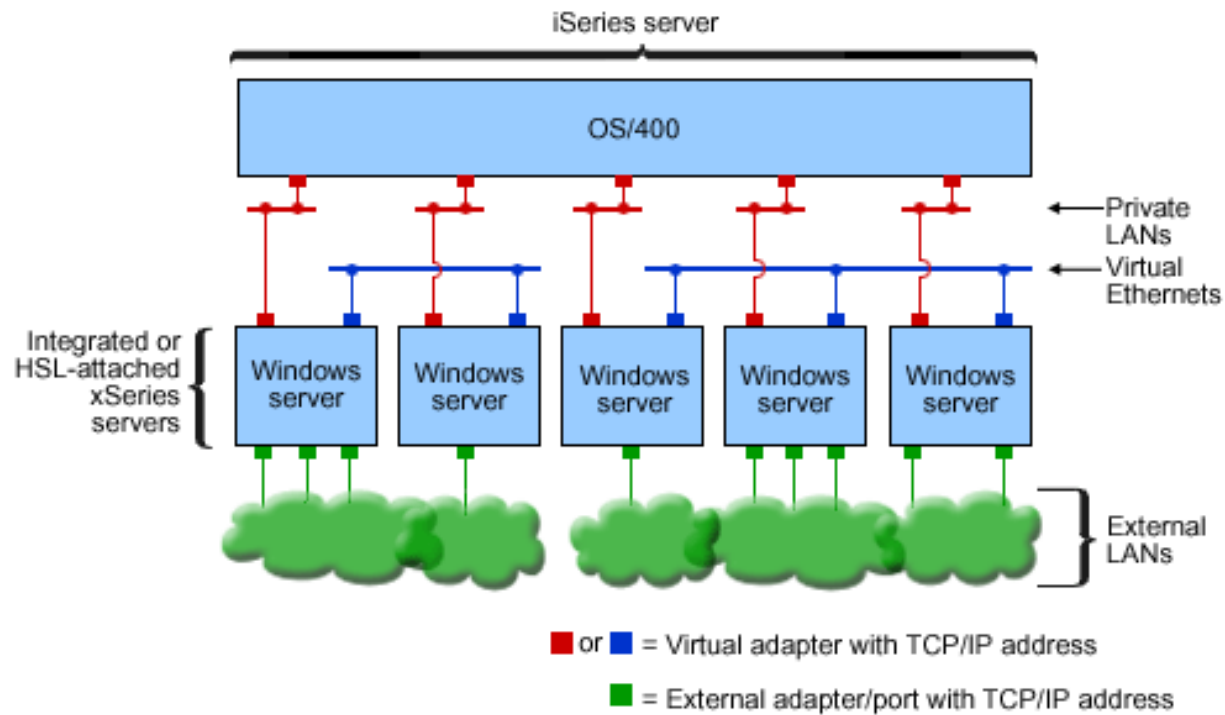
You can allow the INSWNTSVR command to automatically assign these IP addresses or manually configure them to prevent TCP/IP address collisions with other hosts on the system.

Virtual Ethernet networks

- | Virtual Ethernet networks are available on newer IXSs (Type 2890, 2892, or 4812) or on IXAs (Type 2689) using IBM iSeries Integration for Windows Server release V5R2 or later. They are flexible and can be configured in many different ways.

| Virtual Ethernet networks on systems with no logical partitions or one logical partition

For the procedure explaining how to create virtual Ethernet networks, see “Configure virtual Ethernet networks” on page 65.



Two isolated groups of integrated Windows servers on the same iSeries server. Each group has its own virtual Ethernet network.

The graphic above is intended to help you understand how virtual networks work within the iSeries. In it we see five separate integrated Windows servers. They are all connected to the single, controlling, OS/400 partition with private networks (in red). The green boxes on the bottom of the integrated servers represent physical network adapter cards which allow the machines to make external network connections. The

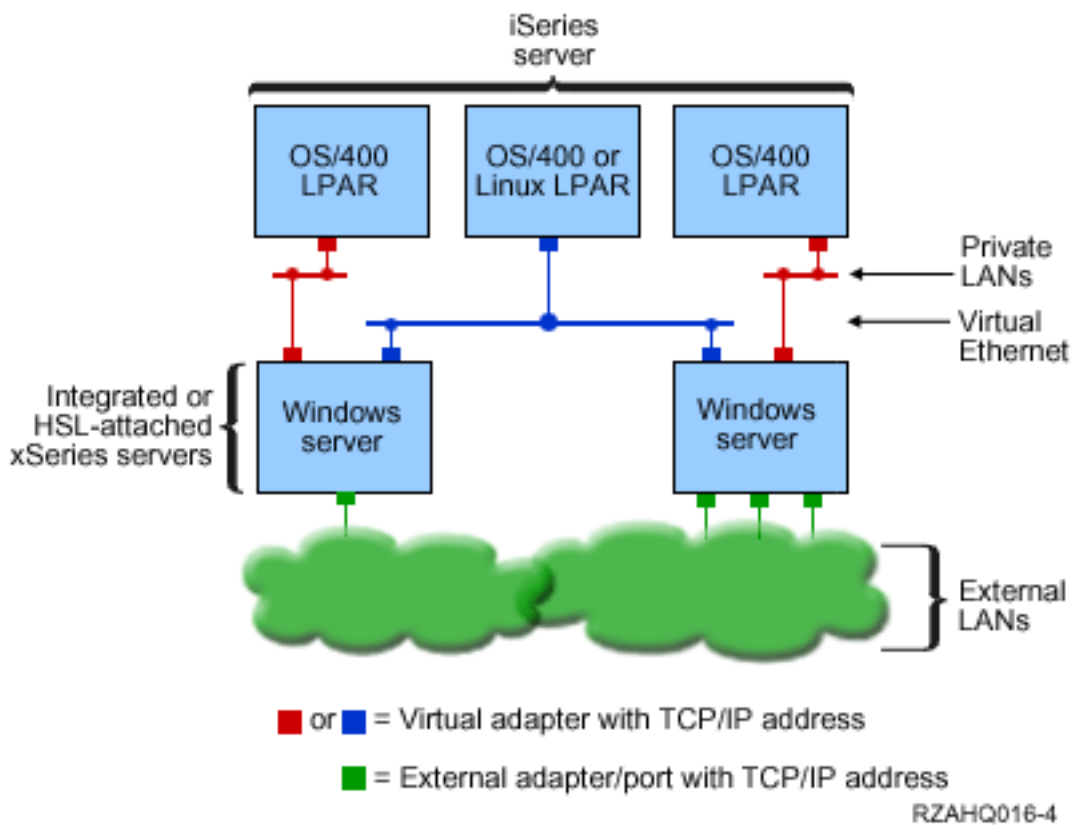
clouds to which they are connected represent external networks. Finally, there are two separate virtual Ethernet networks (in blue). Each integrated server can participate in up to four virtual Ethernet networks simultaneously.

This type of connection is required when configuring a group of integrated servers for clustering.

Like point-to-point virtual Ethernet, virtual Ethernet networks are configured through Ethernet line descriptions. An integrated server is connected to a virtual Ethernet network when its OS/400 configuration (NWSD) is configured to have an Ethernet line description port number with a value of *VRTETH0 through *VRTETH9. Integrated servers having NWSDs configured with the same port number values are connected to the same virtual Ethernet network. When installing a new integrated server, the Install Windows server (INSWNTSVR) command can automatically create the required line descriptions and assign them IP addresses. In the graphic, the OS/400 side of the line descriptions is not shown because, unlike Point-to-point virtual Ethernet, IBM recommends that you not configure a TCP/IP address on the OS/400 side of a line description that is used in a virtual Ethernet network.

I Virtual Ethernet networks on systems with more than one partition

For the procedure explaining how to create virtual Ethernet networks, see “Configure Inter-LPAR virtual Ethernet networks” on page 66.



A simple, inter-LPAR virtual Ethernet network.

Now the iSeries has been partitioned, creating three separate virtual OS/400 logical partitions inside the iSeries. Three virtual networks are represented in the graphic; two private networks (in red) and one virtual Ethernet network (in blue). Each integrated server has a private network for communicating with its controlling partition. In this example, the virtual Ethernet network has three participants: two integrated servers, each controlled by a different OS/400 partition, and a third partition running OS/400 or other operating system. This is called an inter-LPAR (for between logical partitions) Ethernet network.

In servers without HMCs, inter-LPAR connections exist between partitions using the same network number, and integrated servers are connected only if their controlling OS/400 partitions are connected. Network numbers 0-9 are pertinent to integrated servers. For example, if an OS/400 partition is configured for inter-LPAR connections on networks 1 and 5, then integrated servers controlled by that partition can participate in inter-LPAR communication on ports *VRTETH1 and *VRTETH5. The procedure to do this is in the iSeries Navigator online help. You can also refer to Logical partition concepts for an overview.

In servers with a Hardware Management Console (HMC), inter-LPAR connections exist between partitions or integrated servers using the same virtual LAN ID. Participating integrated servers do not support virtual LAN IDs directly. Instead, each participating integrated server needs an Ethernet line description that associates a port value such as *VRTETH1 with a virtual adapter having a virtual LAN ID. You create the virtual adapter using the HMC. See the Logical Partitions with an HMC topic for details. If you migrate inter-LPAR virtual Ethernet from a server without HMCs to a server with an HMC, you will need to create virtual Ethernet adapters using the HMC and additional Ethernet line descriptions to provide appropriate associations. Note that within the same partition, Windows servers can still communicate with each other by simply using the same virtual Ethernet port number.

Some additional ways that you can choose to use inter-LPAR networks include:

- Multiple integrated servers in a logical partition, connected to the same inter-LPAR virtual Ethernet network.
- Integrated servers using multiple virtual Ethernet networks to access different logical partitions. This would be useful when you want to keep your partitions as isolated as possible. On an iSeries server which uses the HMC, there is only one inter-LPAR "virtual switch", but the functionality of multiple, isolated virtual Ethernet networks may be achieved by using a different VLAN ID for each group of inter-LPAR communication participants. When multiple inter-LPAR networks are used to isolate network users, you need to create and configure more virtual Ethernet adapters. For example if an integrated server is to connect to two inter-LPAR networks, you need to create and configure two virtual Ethernet adapters.
- Integrated servers using one virtual Ethernet to reach an OS/400 partition, and a different virtual Ethernet to reach an integrated server running under that OS/400 partition. This would allow you to avoid creating a second virtual Ethernet path between the OS/400 partition and the integrated server running on it. The point-to-point virtual Ethernet connection between them is required. Adding a second virtual Ethernet path can make troubleshooting more difficult and can cause unpredictable results.

External networks

| An integrated Windows server can participate in external networks just as you can with a normal PC
| server. There are different ways to do this. In an IXA attached integrated server there are PCI expansion
| slots available, so you can use any onboard network adapter or install a network adapter card as you
| would in a PC. An IXS, on the other hand, is a PC server on a card which is installed in a PCI slot within
| the iSeries. It has no PCI expansion slots. Some IXSs can control the iSeries PCI slot adjacent to where it
| is installed, and in this way 'take over' an iSeries network adapter. In addition, type 2892 and 4812 IXS
| models contain an onboard Ethernet network adapter.

For the procedure explaining how to physically install network adapter cards for your IXS or IXA and how to configure them for use with integrated servers, see "External networks" on page 68.

External Host LAN

External host LAN is a method of sharing one LAN card between OS/400 and an integrated server. It is only available for Integrated Netfinity servers (INS, types 6617 and 2850). A problem with external host LAN is that when the INS shuts down, the LAN card is shut-down as well, causing OS/400 to lose network access. For this reason IBM suggests that you use two separate LAN cards; one for the iSeries and one for the INS.

External host LAN is unavailable for any of the following configurations:

- Your integrated server hardware is a model 2890, 2892, or 4812 Integrated xSeries Server or a model 2689 Integrated xSeries adapter.
- The IP forwarding function is enabled on the integrated server.
- The Integrated Netfinity hardware was migrated to a 50xx Migration expansion unit.

To configure external host LAN see “External networks” on page 68.

To remove external host LAN see “Remove network adapters” on page 70.

Windows console

You interact with your Integrated xSeries Server (IXS) or your Integrated xSeries Adapter (IXA) attached xSeries server using a Windows console. Depending on your configuration of hardware and software, you can use a monitor, keyboard, and mouse that is attached by one of the following methods:

Directly attached monitor, keyboard, and mouse

You can use a monitor, keyboard, and mouse that are directly attached to the IXS card or an IXA attached xSeries server, forming the integrated server console. You interact with the integrated server through these devices exactly as you would with a regular personal computer (PC).


Remote GUI desktop application

You can use an application such as Microsoft Terminal Services or another third party application to display the server’s graphical user interface (GUI) desktop on a remote workstation. Most administration tasks that are normally performed on the server’s directly attached console can be performed on the remote desktop. See the Microsoft Terminal Services or other third party application documentation for information on how to configure and use a remote desktop for the server console.

Virtual serial console

OS/400 provides the ability to connect to a virtual serial console for a type 4812 IXS. This is similar to the OS/400 virtual serial console support that is provided for iSeries logical partitions. It provides a text-mode console for the 4812 IXS server and can be used for various administration tasks that do not require access to a graphical user interface (GUI) desktop. See “Connect to the 4812 IXS virtual serial console” on page 77 for information on how to establish a session with the virtual serial console for a particular 4812 IXS.

The virtual serial console is currently supported for use with Windows Server 2003 only. It can be used to view server errors or to restore communication to the LAN. This console connection can be used prior to configuring TCP/IP on the server. See the Microsoft Emergency Management

Services document  (www.microsoft.com/whdc/system/platform/server/default.msp) for information about the tasks that can be performed using the virtual serial console. Note that:

- OS/400 does most of the configuration for the virtual serial console automatically, so some of the configuration tasks mentioned in the Microsoft documentation are unnecessary for the OS/400 virtual serial console.
- The iSeries implementation does not require any of the additional hardware, such as modems, concentrators, or cables, which are mentioned in the Microsoft documentation.

Advantages

Windows environment on iSeries provides most of the capabilities of running Microsoft Windows on a PC-based server and provides the following advantages over other computer systems.

Space savings

- There are fewer pieces of hardware to manage requiring less physical space.

Greater accessibility and protection for your data

- An integrated Windows server uses iSeries disk storage, which is generally more reliable than PC server hard disks.
- You have access to faster iSeries tape drives for integrated server backups.
- Integrated servers implicitly take advantage of superior data protection schemes which exist in OS/400 such as RAID or drive mirroring.
- You can add additional storage to integrated servers without varying the server off.
- It is possible to gain access to DB2[®] UDB for iSeries data through an enhanced Open Database Connectivity (ODBC) device driver using iSeries Access. This device driver enables server-to-server applications between integrated servers and OS/400.
- You have the ability to use an integrated server as a second tier in a three-tier client/server application.
- Virtual networking does not require LAN hardware and provides communications between iSeries logical partitions, Integrated xSeries Servers (IXSs), and Integrated xSeries Adapters (IXAs).

Simplified administration

- User parameters, such as passwords, are easier to administer from OS/400. You can create users and groups and enroll them from OS/400 to integrated servers. This makes updating passwords and other user information from OS/400 easy.
- Your computer system is less complicated thanks to the integration of user administration function, security, server management, and backup and recovery plans between the OS/400 and Microsoft Windows environments. You can save your integrated server data on the same media as other OS/400 data and restore individual files as well as OS/400 objects.

Remote management and problem analysis

- You can sign-on to OS/400 from a remote location and shut down or restart your integrated server.
- Since you can mirror integrated server event log information to OS/400 you can remotely analyze Microsoft Windows errors.

xSeries Server directly-attached with an Integrated xSeries Adapter (IXA)

- You have considerably more flexibility in configuring a full size xSeries than you have in configuring an IXS, an xSeries on a card. The full size xSeries can then be directly attached to the iSeries with an IXA.
- Full size xSeries models are released more often, meaning that you can get the most up-to-date Intel processors and other hardware.
- More PCI feature cards are available for full size xSeries than for IXSs.

Multiple servers

- Cluster service allows you to connect multiple servers into server clusters. Server clusters provide high-availability and easy manageability of data and programs running within the cluster.
- Without using LAN hardware, servers and logical partitions running on the same iSeries have high-performance, secure virtual networking communications.
- You can run multiple integrated servers on a single iSeries. Not only convenient and efficient, this also gives you the ability to easily switch to another up-and-running server if the hardware fails.
- If you have multiple integrated servers installed on your iSeries, you can define their Windows domain roles in a way that will simplify user enrollment and access. For example, you might want to set up one of these servers as a domain controller. Then you only have to enroll users to the domain controller and users can log on from any Microsoft Windows machine on that domain.
- An iSeries's optical and tape drives can be shared with integrated servers running on the iSeries.

Considerations

Although an integrated Windows server is much like a PC-based Windows server, here are a few differences that you need to consider:

- There may not be a diskette drive available. This means that you cannot use a startup diskette or an emergency repair diskette. However, you can use iSeries disk space to back up your files.
- iSeries tape and disk devices are available.
- LAN adapters, cables, hubs, or switches are not required for TCP/IP communication with the iSeries server or other integrated servers when using virtual networking.
- Installing the Microsoft Windows operating system with Windows environment on iSeries is different from a typical PC server installation. You first install the IBM iSeries Integration for Windows Server licensed program, then install Microsoft Windows. You enter much of the configuration information with the OS/400 Install Windows server (INSWNTSVR) command, so some of the typical installation panels do not appear. This command also includes some additional parameters that are specific to integrating the server with OS/400, such as synchronize date and time.
- On the OS/400 side of server management, an integrated Windows server is represented by a network server description (NWSD), and network interfaces are represented by line descriptions. You can stop and restart the server from OS/400 by varying the NWSD off and on.
- When you install applications, you do not need to install tape device drivers. The device drivers that allow integrated servers to use iSeries tape drives come with the IBM iSeries Integration for Windows Server licensed program.
- You can do a lot of your user administration tasks from OS/400, such as creating Windows users.
- Because OS/400 manages storage differently than a PC server (see “OS/400 storage management” on page 83), some techniques necessary to administer storage on a PC server are unnecessary. For example, defragmenting network server storage spaces with the Microsoft Windows utility will logically order the internal file structure of the storage space, but since the storage space may be spread across several iSeries physical hard disks, the overall effect on disk speed is unpredictable. Similarly, you do not need to partition high-growth databases or employ disk striping.




Performance and capacity

Integrated Windows server hardware (both the Integrated xSeries Server (IXS) and the Integrated xSeries Adapter (IXA) attached xSeries server), is similar to that of traditional PC servers. Both the IXS and IXA attached xSeries server have their own memory and a CISC processor. The only major difference is that integrated servers do not use standard disk drives. Instead they use simulated hard disk drives which are created using iSeries hard disk drive space. Therefore, while performing processor intensive work its performance should be similar to comparable PC servers, however, the disk performance of integrated servers is dependant on the iSeries.

You can monitor how well the iSeries is fulfilling the integrated server’s disk requirements by using the Work with Disk Status (WRKDSKSTS), Work with Network Server Storage Spaces (WRKNWSSTG), and Work with Network Server Status (WRKNWSSTS) commands.

For other performance considerations, realize that integrated servers are essentially PC-based Microsoft Windows servers. You can use Microsoft’s Windows Performance Monitor as you would on any PC server. See Windows documentation from Microsoft for information about using the Performance Monitor.

Use the following links to see more performance-related information:

- For supported hardware and detailed performance numbers, see the IBM Windows Integration Web site (www.ibm.com/servers/eserver/iseries/windowsintegration) .
- For more information about performance tools and IXS performance, see the iSeries Performance Management Web site  (www.ibm.com/eserver/iseries/perfmgmt).
- For more information about Integrated xSeries Server performance, see Chapter 17 of the iSeries Performance Capabilities Reference .

User and group concepts

One of the main advantages of using Windows environment on iSeries is the user administration function for OS/400 and Windows user profiles. The user administration function allows administrators to enroll existing OS/400 user and group profiles to Microsoft Windows. This section will explain the function in more detail.

Enrollment

Enrollment is the process by which an OS/400 user or group profile is registered with the integration software.

The enrollment process happens automatically when triggered by an event such as running the CHGNWSUSRA command to enroll a user or group, an enrolled Windows user updating their OS/400 user profile password or user attributes, or restarting the integrated server. If the integrated Windows server is active, the changes are made immediately. If the integrated server is varied off, the changes occur the next time the server is started.

Windows domains and local servers

Enrollment can be made to either a Windows domain or a local server. A Windows domain is a set of resources (applications, computers, printers) which are networked together. A user has one account across the domain and needs only to log onto the domain to gain access to all the resources. An integrated server can be a member server of a Windows domain and integrate OS/400 user accounts into the Windows domain.

On the other hand, if you enroll OS/400 users to an integrated server which is not part of a domain, it is called a **local server**, and user accounts will only be created on that integrated server.

Note: In Windows networking, groups of local servers can be loosely affiliated by using Windows workgroups. For example, if you open My Network Places and click Computers Near Me, you will see a list of the computers in the same workgroup as you. In iSeries Navigator, it will sometimes appear that you can enroll OS/400 users to these Windows workgroups, but attempting to do this will result in an error stating that a Windows domain controller could not be found.

Microsoft Windows OS/400 groups

Two groups of users are created in Microsoft Windows as part of the installation to an integrated server.

- **AS400_Users** (On a Windows domain this group is named **OS400_Users**.) Every OS/400 user, when first enrolled to the Windows environment, is placed in the AS400_Users group. You can remove a user from this group in the Windows environment, however, the next time an update occurs from the iSeries server, the user will be replaced. This group is a useful place to check which OS/400 user profiles are enrolled to the Windows environment.
- **AS400_Permanent_Users** (On a Windows domain this group is named **OS400_Permanent_Users**.) Users in this group cannot be removed from the Windows environment by the iSeries server. It is provided as a way to prevent Windows users from being accidentally deleted by actions taken within OS/400. Even if the user profile is deleted from OS/400, the user will continue to exist in the Windows environment. Membership in this group is controlled from the Windows environment, unlike the AS400_Users (or OS400_Users) group. If you delete a user from this group, it will not be replaced when an OS/400 update is performed.

Using the OS/400 user profile LCLPWDMGT attribute

There are two ways to manage user profile passwords.

- **Traditional user** You may choose to have OS/400 passwords and Windows passwords be the same. Keeping the OS/400 and Windows passwords the same is done by specifying the OS/400 user profile attribute value to be LCLPWDGMT(*YES). With LCLPWDGMT(*YES), enrolled Windows users manage their passwords in OS/400. The LCLPWDGMT attribute is specified using the OS/400 Create or Change user profile (CRTUSRPRF or CHGUSRPRF) commands.
- **Windows user** You may choose to manage enrolled Windows profile passwords in Windows. Specifying LCLPWDGMT(*NO) sets the OS/400 user profile password to *NONE. This setting allows enrolled Windows users to manage their password in Windows without OS/400 overwriting their password.

See “Types of user configurations” on page 19.

Using OS/400 Enterprise Identity Mapping (EIM)

There are 2 ways to take advantage of the OS/400 EIM support. You may decide to use the auto-creating of EIM associations function in the EIM Windows registry. Defining EIM associations allows OS/400 to support Windows single sign-on using an authentication method such as Kerberos. Auto-creation and deletion of Windows EIM source associations are done when the OS/400 Create, Change, or Delete user profile (CRTUSRPRF, CHGUSRPRF, or DLTUSRPRF) commands are used specifying the EIMASSOC parameter values of *TARGET, *TGTSRC, or *ALL.

You may decide to manually define EIM associations in the EIM Windows registry. When an EIM OS/400 target association and Windows source association is defined for an OS/400 user profile, the enrolled OS/400 user profile may be defined as a different user profile name in Windows. For more information see “Enterprise Identity Mapping (EIM)” on page 102.

Enrolling existing Windows user profiles

You can also enroll a user who already exists in the Windows environment. The password for the user must be the same on OS/400 as for the already existing Windows user or group. See “Password considerations” on page 21.

User enrollment templates

You can customize the authorities and properties a user receives during enrollment through the use of user enrollment templates. See “User enrollment templates” on page 20. If you do not use a template when you enroll users, they receive the following default settings:

- Users become members of the AS400_Users (or OS400_Users) group and either the Users group on a local integrated Windows server or the Domain Users group on a Windows domain.
- OS/400 keeps track of the user’s OS/400 password, password expiration date, description, and enabled or disabled status.

Enrolling OS/400 groups

Up to this point we have only discussed enrolling individual OS/400 user profiles to the Windows environment. You can also enroll entire OS/400 groups. Then, when you add users to those OS/400 groups that have been enrolled to the Windows environment, you automatically create and enroll those users in the Windows environment as well.

Enrolling to multiple domains

You may enroll users and groups to multiple domains, but typically this is unnecessary. In most Windows environments, multiple domains set up trust relationships with each other. In such cases, you only need to enroll the user in one domain because trust relationships automatically give the user access to other domains. See your Windows documentation for additional information about trust relationships.

Saving and Restoring enrollment information

Once you have defined your user and group enrollments, you will need to save the enrollment definitions. You may save the enrollment information using options 21 or 23 on the GO SAVE menu, by using the SAVSECDTA command, or by using the QSRSAVO API. Restoring the user profiles is done using the RSTUSRPRF command and specifying USRPRF(*ALL) or SECDTA(*PWDGRP) values.

Using the PRPDMNUSR parameter

If you have multiple servers which are members of the same domain, you may prevent duplicate domain enrollment from occurring on each member server. Use the Propagate Domain User (PRPDMNUSR) parameter in the Change Network Server Description (CHGNWD) or Create Network Server Description (CRTNWSD) commands. See “The QAS400NT user” on page 105 for more information.

Types of user configurations

It is helpful to think of integrated Windows users as fitting into three basic types:

- **Traditional user (password managed by OS/400)**

By default users are set to this type. This user works in both Windows and OS/400. The OS/400 password and Windows password will be synchronized. Each time that the integrated Windows server is restarted, the user's password will be reset to the OS/400 password. Password changes can only be made in OS/400. This user type is recommended for running File Level Backup and remote Windows commands. To set a Windows user to this configuration, use WRKUSRPRF to set the user profile attribute LCLPWDMGT to *YES.

- **Windows password-managed user**

This person does all or most of their work in Windows and may never, or rarely, sign-on to OS/400. If the user signs-on to OS/400, they must use an authentication method such as Kerberos to access OS/400. This is discussed in the next section: Windows user with Enterprise Identity Mapping (EIM) configured.

When the user profile attribute LCLPWDMGT(*NO) is defined for an OS/400 user, the OS/400 user profile password is set to *NONE. The OS/400 enrollment password is saved until Windows enrollment is successfully completed. After the OS/400 user is enrolled to Windows, the Windows user may change and manage their password in Windows without OS/400 overwriting their password. Using this method allows for a more secure environment because there are fewer passwords being managed. To read how to create a user of this type, see “Changing the LCLPWDMGT user profile attribute” on page 102.

- **Windows user with Enterprise Identity Mapping (EIM) associations automatically configured**

Specifying the user profile attribute of EIMASSOC to be *TGT, TGTSRC, or *ALL allows the integrated server to automatically define EIM Windows source associations. Using the automatic definitions of associations makes configuring EIM easier. To read how to create a user of this type, see “Enterprise Identity Mapping (EIM)” on page 102.

- **Windows user with Enterprise Identity Mapping (EIM) associations manually configured**

The user may choose to manually define EIM Windows source associations. This method may be used to set the OS/400 user profile to be enrolled to a different Windows user profile name. The user must manually define an OS/400 target association for the OS/400 user profile and also a Windows source association for the same EIM identifier.

Table 1. Types of user configurations

User type	Function provided	User profile definition
Traditional	<ul style="list-style-type: none"> • Both OS/400 and Windows fully functional. • Easy to configure. • Password is changed from OS/400. • OS/400 and Windows user ID and passwords will be identical. • Recommended for system administrators, users who frequently use OS/400, or for systems which use OS/400 for back up and restoration of user profiles. 	LCLPWDMGT(*YES) and no EIM Windows source associations defined.
Windows password-managed user	<ul style="list-style-type: none"> • Password can be changed from Windows. • Simple configuration. • Windows password administration makes this configuration more secure because the OS/400 password is *NONE. • OS/400 sign-on requires an authentication method such as iSeries Navigator provides with their support of OS/400 sign-on using Kerberos. 	LCLPWDMGT(*NO)
Windows user with Enterprise Identity Mapping (EIM) associations auto configured	Automatic creation of Windows source associations makes it easier to set up and configure to use Kerberos enabled applications.	For example: EIMASSOC(*CHG *TARGET *ADD *CRTEIMID)
Windows user with Enterprise Identity Mapping (EIM) associations manually configured	Allows the user to define EIM associations for enrolled OS/400 user profiles to be different user profiles in Windows.	Use iSeries Navigator to manually define EIM OS/400 target associations and Windows source associations.

User enrollment templates

A user enrollment template is a tool to help you enroll users from OS/400 to the Windows environment more efficiently. Rather than manually configure many new users, each with identical settings, use a user enrollment template to automatically configure them. Each template is a Windows user profile that defines user privileges, such as group membership, directory paths, and organizational unit containers.

When you enroll users and groups from OS/400 to the Windows environment, you can specify a user template on which to base the new Windows users. For example, you could create a user template and name it USRTEMP. USRTEMP could be a member of the Windows server groups NTG1 and NTG2. On OS/400 you could have a group called MGMT. You could decide to enroll the MGMT group and its members to Windows server. During the enrollment process, you could specify USRTEMP as the user template. During enrollment, you automatically add all members of the MGMT group to the NTG1 and NTG2 groups.

User templates save you from having to set up group memberships individually for each user. They also keep the attributes of enrolled users consistent.

You can make a user template a member of any Windows group, whether you enrolled that group from OS/400 or not. You can enroll users with a template that is a member of a group that was not enrolled from OS/400. If you do this, however, the users become members of that nonenrolled group as well. OS/400 does not know about groups that were not enrolled from OS/400. This means that you can only remove users from the group by using the User Manager program on Windows.

If you use a template to define a new user enrollment, and the template has a folder or directory **Path** or **Connect To** defined, the newly-created Windows user will have the same definitions. The folder definitions allow the user administrator to take advantage of folder redirection and to manage terminal service sign-on.


If you use a template when you define a new user enrollment, and the template is a user object in a Windows Active Directory organizational unit container, the newly created Windows user object will be in the same organizational unit container. An organizational unit provides a method to grant users administrative control to resources.

You can change existing user templates. Such changes affect only users that you enroll after you change the template.

You use templates only when you create a newly enrolled user in the Windows environment. If you perform enrollment in order to synchronize an existing Windows user with an OS/400 counterpart, Windows ignores the template.

For a detailed procedure see “Create user templates” on page 100.

Password considerations

1. The user should use OS/400 passwords containing only characters and password lengths allowed in Windows passwords if they want to enroll users. The password level of OS/400 can be set to allow for user profile passwords of 1 - 10 characters or to allow for user profile passwords of 1 - 128 characters. An OS/400 password level change of the system value QPWLVL requires an IPL.
2. The OS/400 password level of 0 or 1 supports passwords of 1 - 10 characters and limits the set of characters. At password level 0 or 1, OS/400 converts passwords to all lowercase for Windows.
3. The OS/400 password level of 2 or 3 supports passwords of 1 - 128 characters and allows more characters including uppercase and lowercase characters. At level 2 or 3, OS/400 preserves password case sensitivity for Windows.
4. When the OS/400 passwords of enrolled users expire, their Windows passwords also expire. Users can change their passwords on Windows, but they must remember to also change their passwords on OS/400. Changing the OS/400 password first automatically changes the Windows password.
5. If the OS/400 system value QSECURITY is 10, the Windows users that are created do not require passwords to sign-on. All other OS/400 QSECURITY levels require that a user object have a password to sign-on. You can find more information on security levels in the iSeries Security Reference .
6. Set QRETSVRSEC to 1. To successfully enroll, users must sign-on to OS/400 after this system value is set to 1.
7. If you are using a language other than English, be aware that using anything but invariant characters in user profiles and passwords can cause unpredictable results. The Globalization topic contains information about what characters are in the invariant character set. This statement is only true when QPWLVL is 0 or 1. When QPWLVL is 2 or 3, invariant characters can be used without causing any problems.

Terminology

The following are terms related to Windows environment on iSeries. For other iSeries terms and definitions, see the Information Center glossary.

Enterprise Identity Mapping (EIM). A mechanism for mapping/associating a person or entity to the correct user identities in various registries across multiple operating systems. User Administration function integrates user enrollment with EIM, by providing support for automatic creating of EIM Windows source associations. Also, enrolled OS/400 user profiles allow Windows user profiles to be different than the OS/400 user profile if the administrator has manually defined the EIM Windows source association.

EIM identifier. Represents an actual person or entity in EIM. When you create an EIM identifier you associate it with the user identity for that person.

EIM identity mapping association. A single sign-on environment is made possible by associating the user identity to an EIM identifier in a registry. There are 3 types of associations, source, target, and administrative. User enrollment integrates with EIM when a target OS/400 association and a source Windows association are defined. The associations may be defined either automatically using the user profile attribute, EIMASSOC, or by using iSeries Navigator to manually define the associations. Target associations are primarily used to secure existing data. Source associations are primarily used for authentication purposes.

external network. Networks accessed by integrated servers through a physical networking card, as distinct from virtual networks.

external host LAN. Feature of Integrated Netfinity servers which allowed OS/400 and Microsoft Windows to share one LAN adapter for network access.

IBM iSeries Integration for Windows server licensed program. Extension to the OS/400 operation system installed on the iSeries which allows it to work with integrated Windows servers. There is also a component of the licensed program which runs on the integrated server.

Integrated Netfinity Server (INS). The old term for IXS, in this document it refers to those models type 2850 and 6617. See IXS.

integrated Windows server. Also referred to as an *integrated server*, an instance of Windows 2000 Server or Windows Server 2003 running on an IXS or an IXA attached xSeries server.

Integrated xSeries Server (IXS). A PC (Intel-based computer) on a PCI expansion card that installs inside an iSeries server.

Integrated xSeries Adapter (IXA). A PCI expansion card that installs inside selected models of xSeries servers (IBM PCs), providing a high-speed link to an iSeries server.

Kerberos. A network security protocol created by MIT. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. iSeries Navigator provides Kerberos authenticated sign-on. User Administration supports the single sign-on environment by allowing OS/400 user profile passwords to be defined to be *NONE and to allow enrolled Windows users to set their passwords in Windows. This support is provided when an enrolled user profile attribute is specified as LCLPWDMGT(*NO).

Microsoft Windows Cluster Service. Service in Microsoft Windows which links individual servers so they can perform common tasks.

network server description (NWS D). An OS/400 object which describes an integrated Windows server. Basically, the configuration file of an integrated server.

network server storage space. OS/400 disk storage allocated to an integrated server.

point-to-point virtual Ethernet. A virtual Ethernet network configured between an iSeries and an integrated Windows server during its installation. It is the link that is used for communication between the iSeries and an integrated server. See **private network**.

private network. An internal token-ring or virtual Ethernet network existing solely between an iSeries and an integrated server, used for communication between the iSeries and an integrated server.


virtual network. A token-ring or Ethernet network emulated inside the iSeries to allow networks to be created between OS/400 logical partitions, Linux logical partitions, and integrated Windows servers. No physical networking hardware is used.

Windows server. Microsoft Windows 2000 Server or Windows Server 2003

Chapter 5. Install and configure Windows environment on iSeries

Setting up Windows environment on iSeries involves installing hardware and two separate pieces of software: the IBM iSeries Integration for Windows Server licensed program and the Windows 2000 Server or Windows Server 2003 operating system from Microsoft.

To install and configure Windows environment on iSeries, do the following:

1. Check the IBM iSeries Windows Integration  Web site. (www.ibm.com/servers/eserver/series/windowsintegration). Ensure that you are aware of late breaking news and information.
2. Check to make sure you have the correct hardware and software.
 - a. "Hardware requirements."
 - b. "Software requirements" on page 25.
3. Install hardware, if needed. Follow this link: [Install iSeries Features](#). Choose your model of iSeries and find the instructions labeled **Install PCI Card and Integrated xSeries Adapter Card**.
4. Install the IBM iSeries Integration for Windows Server licensed program.
 - a. "Prepare for the installation of integrated Windows servers" on page 26
 - b. "Install IBM iSeries Integration for Windows Server licensed program" on page 30
5. Install Microsoft Windows 2000 Server or Windows Server 2003 to the IXS or IXA.
 - a. "Plan for the installation of Windows server" on page 30
 - b. "Install Windows 2000 Server or Windows Server 2003" on page 43
6. Now that you have completed the installation, configure the integrated Windows Server.
 - a. "Code fixes" on page 61. These code fixes will correct any errors discovered in the licensed program since its release.
 - b. Chapter 6, "Network integrated servers," on page 65
 - c. "Set an integrated Windows server to automatically vary on with TCP/IP" on page 61

Hardware requirements


To run integrated Windows servers, you need the following hardware:


1. One of the following Integrated xSeries Servers (IXSs) or Integrated xSeries Adapters (IXAs).

Description	Feature code	Type-model
2.0 GHz Integrated xSeries Server	4811 ¹ 4812 ¹ 4813 ¹	4812-001
2.0 GHz Integrated xSeries Server	4710 ¹	2892-002
2.0 GHz Integrated xSeries Server	4810 ¹	2892-002
1.6 GHz Integrated xSeries Server	2792 ¹	2892-001
1.6 GHz Integrated xSeries Server	2892 ¹	2892-001
1.0 GHz Integrated xSeries Server	2799 ¹	2890-003
1.0 GHz Integrated xSeries Server	2899 ¹	2890-003
850 MHz Integrated xSeries Server	2791 ¹	2890-002
850 MHz Integrated xSeries Server	2891 ¹	2890-002
700 MHz Integrated xSeries Server	2790 ¹	2890-001

Description	Feature code	Type-model
700 MHz Integrated xSeries Server	2890 ¹	2890-001
333 MHz Integrated Netfinity Server	2865	2850-012 285A-003
333 MHz Integrated Netfinity Server	2866	2850-012 285A-003
333 MHz Integrated Netfinity Server	6618	6617-012
200 MHz Integrated PC Server	2854	2850-011 285A-003
200 MHz Integrated PC Server	2857	2850-011 285A-003
200 MHz Integrated PC Server	6617	6617-001
Integrated xSeries Adapter	0092 ^{1,2,3}	2689-001
Integrated xSeries Adapter	0092 ^{1,2,4}	2689-002

Notes[®]:

1. The hardware cannot serve as an external host LAN for your iSeries server.
2. The IXA requires an xSeries server. The xSeries server may have additional requirements, see the iSeries Windows integration Web site (www.ibm.com/servers/eserver/series/windowsintegration)  for details.
3. The hardware is ordered through AAS or WTAAS as machine type 1519-100.
4. The hardware is ordered through AAS or WTAAS as machine type 1519-200.

Note: If you have an IXS or an IXA that is not listed in the above table, see the IBM Windows Integration  web site for specifications.

For information on how to install hardware, see the “Install iSeries features” topic. For a description of IXSs and IXAs, see “Hardware concepts” on page 7.

2. A 64-bit RISC iSeries or AS/400[®] with sufficient free disk space, including 100 MB for the code of the iSeries Integration for Windows server software and 1,224 MB to 1 TB to be used for the Windows system drive or network server storage space.
3. One or more approved LAN ports or PCI adapters:

Description	Feature Code	Supported by IXS hardware type 4812	Supported by IXS hardware type 2892	Supported by IXS hardware type 2890	Supported by Integrated Netfinity Server hardware types 6617 and 2850
iSeries 1000/100/10 Mbps Ethernet Adapter (copper UTP)	5701		X		
iSeries Gigabit (1000 Mbps) Ethernet Adapter (fiber optic)	5700		X		

Description	Feature Code	Supported by IXS hardware type 4812	Supported by IXS hardware type 2892	Supported by IXS hardware type 2890	Supported by Integrated Netfinity Server hardware types 6617 and 2850
iSeries Gigabit (1000/100/10 Mbps) Ethernet Adapter (copper UTP)	2760			X	
iSeries Gigabit (1000 Mbps) Ethernet Adapter (fiber optic)	2743			X	
iSeries 2892 10/100 Mbps Ethernet port	2892		X		
IBM iSeries 10/100 Mbps Ethernet Adapter	2838			X	X
iSeries Ethernet Adapter 10 Mbps	2723				X
High-speed 100/16/4 Mbps Token-ring PCI Adapter	2744		X	X	
PCI Token-Ring Adapter 16/4 Mbps	2724				X
iSeries 4812 1000/100/10 Mbps Ethernet port	4812	X			

4. An SVGA compatible monitor, a mouse, and a keyboard. There is only a single keyboard/mouse port in an IXS, so you will also need a keyboard/mouse Y-cable to be able to attach both at the same time. If you have several integrated servers and plan to administer only one at a time, consider switching one set of I/O hardware between integrated servers.
5. At least 128 MB of random access memory (RAM), or at least 256 MB of RAM if you are using Windows 2003 Server. This memory is installed in the integrated server and must be ordered separately.


For additional hardware requirements, see


- “Machine pool size requirements” on page 27
- “Networking concepts” on page 10

Software requirements

You need this software:

1. OS/400 5722-SS1 Version 5 Release 3.
To check your release level:
 - a. On the OS/400 command line, type Go LICPGM and press Enter.
 - b. Type 10 in the option field to look at installed products.

- c. Look for 57xxSS1. The release shows beside that is your version. (On some releases, you may need to press F11 before the VRM number appears.)
2. IBM iSeries Integration for Windows Server (5722-WSV) V5R3 (the base licensed program and option 2).
3. TCP/IP Connectivity Utilities for OS/400 V5R3 (5722-TC1).
4. Microsoft Windows 2000 Server or Windows Server 2003.
5. Any required Microsoft Windows service packs. For the latest information about available service packs that IBM has tested with iSeries Integration for Windows Server, refer to the Applications topic on the IBM Windows Integration Web site  .

For additional information about the installation of required software, see the iSeries Software Installation manual  .

Prepare for the installation of integrated Windows servers

The installation will go smoothly if you perform some preliminary tasks.

1. Verify that you have the necessary authority to perform the installation. You must have *IOSYSCFG, *ALLOBJ, and *JOBCTL special authority on OS/400. *SECADM special authority is required to perform step 8 of this checklist. For information about special authorities, refer to the iSeries Security

Reference  .

2. Verify “Machine pool size requirements” on page 27.
3. If the Integrated xSeries Server has two LAN adapters on the same network, disconnect one of them from the network before installing the server. This way, Windows installation will not falsely detect a duplicate computer on the network. The simplest way to disconnect an adapter is to unplug its cable. Remember to reconnect the second adapter to the network after the installation is complete.
4. Ensure that time synchronization is correctly configured. See “Time synchronization” on page 28.
5. “Configure OS/400 TCP/IP for integrated Windows servers” on page 28.
6. Decide how many integrated Windows servers and subnets you need for your particular business.


If your organization uses fixed IP addresses (organizations that use DHCP may configure the integrated Windows server to be assigned an IP address automatically just like any standard PC server), obtain TCP/IP addresses from your network administrator. These include:

- IP addresses for all external TCP/IP ports
- Subnet mask
- Your domain name or workgroup name
- IP address for your Domain Name System (DNS) server, if you have one
- IP address of the default gateway for your local area network (LAN), if you have one




If you are running TCP/IP on your iSeries system, the last two items in the above list have already been supplied to the system. Specify *SYS for those parameters while performing the Install Windows server (INWNTSVR) command.

7. Decide whether you want to use iSeries Access for Windows, which allows you to use iSeries Navigator and run Open Database Connectivity (ODBC) as a Windows service. See the iSeries NetServer versus iSeries Access for Windows topic in the Information Center.
8. Enable NetServer and set up a guest user profile, so you can perform maintenance tasks on your integrated server. Refer to “Enable iSeries NetServer” on page 29 and “Create a guest user profile for iSeries NetServer” on page 29.

9. It’s possible to eliminate the need for a physical CD-ROM during installation (for example, to avoid the delay and expense of shipping the CD-ROM to a remote site if you need to reinstall a server). Store the image of the installation CD, then use the Windows source directory field during the

installation to specify the path name to that image. If you need directions, refer to the Redbook Microsoft Windows Server 2003 Integration with iSeries, SG24-6959 .

Note: Contents of the installation CD may be subject to licenses from their respective authors and distributors. Compliance with these licenses is your responsibility. By offering this function, IBM takes no responsibility for compliance with or enforcement of any CD license agreement.

10. You can customize the installation by using a configuration file to change the default values in the Windows unattended install setup script file (unattend.txt). See Chapter 14, “Network server description configuration files,” on page 159.
11. If the server will be installed on an external xSeries server using the 2689 Integrated xSeries Adapter, you need to prepare the xSeries server. Refer to
 - The chapter “Install Integrated xSeries Adapter for iSeries” in the iSeries PCI Card and Integrated xSeries Adapter Card Installation Instructions .
 - IXA install read me first .
12. If the server will be installed on an Integrated xSeries Server, refer to the IXS install read me first .
13. If you use logical partitions on your iSeries server, recall that you need to install the iSeries Integration for Windows Server licensed program only on the logical partition that you will use to vary on the server. There is no requirement to install the licensed program on all the logical partitions. For example, one logical partition might have the iSeries Integration for Windows Server licensed program and one or more integrated Windows servers installed while another logical partition has neither the iSeries Integration for Windows Server licensed program nor any integrated servers installed.
14. When you install a Windows server on OS/400, a network server description (NWSD) object is created containing configuration information such as the version of Windows and the hardware resource to be used. However, you can have only one NWSD varied on (running) for a given hardware resource at any given time.

Machine pool size requirements

The machine memory pool is used for highly-shared machine and operating system programs. The machine memory pool provides storage for jobs the system must run that do not require your attention. If you set the size for these storage pools too small, you will impair system performance. You cannot set QMCHPOOL to less than 256 KB. The size for this memory pool is specified in the machine memory pool size system value (QMCHPOOL). No user jobs run in this memory pool.

The following table provides the machine pool size requirements for the IBM iSeries Integration for Windows Server licensed program for the various integrated Windows server hardware:

Integrated xSeries Server or adapter	Minimum memory required	Additional memory required for network adapter card
6617	5400 KB	1800 KB for each 2838, 2723, or 2724 network adapter card that you install with the Integrated Netfinity Server.
2850	1800 KB	1800 KB for each 2838, 2723, or 2724 network adapter card that you install with the Integrated Netfinity Server.
2689, 2890, 2892, and 4812	856 KB	You do not need to consider network adapter cards that you install with these IXS models because they cannot serve as shared external host LAN adapters for iSeries.

You can display or change the machine pool size by using the Work With System Status (WRKSYSSTS) command. The first storage pool on the WRKSYSSTS display is the machine pool.

You can change the system value QPFRADJ so that the system automatically adjusts system pool sizes. However, because automatic performance adjustment can slow down a busy system, you probably want to limit its use to one of these times:

- The first couple days after the installation
- An hour or so at the time your system load changes from daytime (interactive emphasis) to nighttime (batch emphasis) and back

Time synchronization

To keep the time on OS/400 and the Windows environment synchronized, do the following:

1. Select *YES for synchronize date and time in the Install Windows server (INSWNTSVR) command or the CHGNWSD command. Selecting *YES will synchronize the time between OS/400 and the integrated Windows server every 30 minutes. Selecting *NO will synchronize the time only when the server is started.
2. Ensure that the iSeries time, date, and time zone are correct. Once these values are set they will automatically update themselves every six months for daylight savings time adjustments. The QTIMZON system value replaces the need to manually change the QUTCFFSET system value twice a year.
3. At the Windows console, click **Control Panel** → **Date/Time**, select the **Time Zone** tab and select your time zone from the drop-down list.
4. Select the **Automatically adjust clock for daylight savings changes** check-box. Then click OK.

If you have problems with time synchronization, check the OS/400 system value for LOCALE to make sure it is set properly.

Configure OS/400 TCP/IP for integrated Windows servers

When you install Windows environment for iSeries, you have the option of using values that you specified in the OS/400 TCP/IP configuration as default values to configure your integrated server. If you want to take this option and do not already have TCP/IP configured, you must configure it before installing the iSeries Integration for Windows Server licensed program. You also need to add your gateway address to OS/400. For more information about configuring TCP/IP, see the TCP/IP topic.

If you have iSeries Navigator installed, you can use it to configure your TCP/IP connections. The iSeries Navigator online help tells you how to configure TCP/IP. If you do not have iSeries Navigator installed, follow these steps:

1. On the OS/400 console, enter the command CFGTCP and press Enter. The Configure TCP/IP menu appears.
2. Select option 12 Change TCP/IP Domain information and press Enter. The Change TCP/IP Domain (CHGTCPDMN) display appears.
3. Specify the Local domain name from the "Installation worksheet for OS/400 parameters" on page 31.
4. In the Domain name server field, specify up to 3 IP addresses from the Windows server installation advisor or from the "Installation worksheet for OS/400 parameters" on page 31; then press Enter.
To add your gateway IP address to OS/400:
5. From the Configure TCP/IP menu, choose option 2 Work with TCP/IP routes. The Work with TCP/IP Routes display appears.
6. Type 1 in the Option field to add a TCP/IP route. The Add TCP/IP Route display appears.
7. Fill in the appropriate fields with the information for your gateway address.

iSeries Access for Windows on integrated Windows servers

IBM iSeries Access for Windows allows you to connect a personal computer (PC) to an iSeries server over a local area network (LAN), a twinaxial connection, or a remote link. It features a complete set of integrated functions that enable desktop users to use OS/400 resources as easily as their local PC functions. With iSeries Access, users and application programmers can quickly process information, applications, and resources for their entire company.

You can enable Open Database Connectivity (ODBC) to run as a Windows service by installing iSeries Access for Windows on your integrated server. This enables you to write server applications that call the ODBC device driver to access DB2 for iSeries.

To enable ODBC to be started from a Windows service, run the CWBCFG command with the /s option after you install iSeries Access.

As a single user signed-on to Windows, you have full support for all other iSeries Access features.

Additional information sources:

- You can read a [comparison](#) of iSeries Access for Windows with iSeries NetServer.

Enable iSeries NetServer

iSeries NetServer enables Windows clients to connect to OS/400 shared directory paths and shared output queues by way of TCP/IP. Before you can install service packs or perform file-level backups on an integrated Windows server, you must enable iSeries NetServer and set up a guest user profile.

If you plan to use iSeries NetServer only to perform maintenance tasks, you can set it up without iSeries Navigator. In that case, you can use the quickstart method found in the “Configure iSeries server for NetServer” topic. If you want the full capabilities of iSeries NetServer, you need iSeries Navigator, which requires setting up iSeries Access (see “iSeries Access for Windows on integrated Windows servers”) on a PC that you use for administration. Once you have set up either version, you need to set up a guest user profile. See “Create a guest user profile for iSeries NetServer.”

Create a guest user profile for iSeries NetServer

Before you can apply code fixes and system upgrades to the Windows environment on iSeries, you must set up a guest user profile for iSeries NetServer. You must have *SECADM special authority to perform this task.

If you have iSeries Navigator on your system, you can use the graphical interface to set up a guest user profile for iSeries NetServer with no special authorities and no password.

If you do not have iSeries Navigator, follow these steps to set up a guest user profile for iSeries NetServer:

1. On OS/400, create a user profile with no special authorities and no password:

```
CRTUSRPRF USRPRF(username) PASSWORD(*NONE) SPCAUT(*NONE)
```

Note:

See the iSeries Security Reference  for information about user profiles.

2. Enter the following command, where *username* is the name of the user profile that you created:

```
CALL QZLSCHSG PARM(username X'00000000')
```

3. To stop iSeries NetServer, enter the following command:

```
ENDTCPSVR SERVER(*NETSVR)
```

4. To restart iSeries NetServer, enter the following command:

```
STRTCPSVR SERVER(*NETSVR)
```


You can go back to “Enable iSeries NetServer” on page 29 or to the “Prepare for the installation of integrated Windows servers” on page 26.

Install IBM iSeries Integration for Windows Server licensed program

To install the IBM iSeries Integration for Windows Server licensed program, perform these steps on iSeries:

1. If you are upgrading IBM iSeries Integration for Windows Server from V5R1 or V5R2, refer to this topic, “Upgrade the IBM iSeries Integration for Windows Server licensed program” on page 47. Perform the steps under “Preparing to Upgrade” and then return here.
2. Insert the OS/400 CD containing 5722-WSV.
3. Type G0 LICPGM and press Enter.
4. Choose option 11 from the Work with Licensed Programs menu; then press Enter.
5. Page down the list of licensed programs until you see the description IBM Integration for Windows Server and Integration for Windows 2000 and 2003. (There are two parts to the licensed program.)
6. We want to install both of them, so enter a 1 in the Option field beside each description.
7. Press enter.
8. Enter the name of the Installation device in which you inserted the OS/400 CD.
9. Press Enter, and the system installs the integration software.
10. After installing IBM iSeries Integration for Windows Server, install the latest cumulative program temporary fix (PTF) package from IBM. Note that there should be no users on your iSeries when installing PTFs. If your system uses logical partitions, load the PTFs on the secondary partitions on which you are installing IBM iSeries Integration for Windows Server and set them for apply delay. Then load them on the primary partition. Refer to Install program temporary fixes on a system with logical partitions.
11. To install the latest PTF, complete the following steps:
 - a. On the OS/400 command line, type G0 PTF and press Enter.
 - b. To install the program temporary fix package, type 8 and press Enter.
 - c. In the Device field, enter the name of your optical device.
 - d. Use the default *YES for Automatic IPL unless your system uses logical partitions. Press Enter to install all PTFs. Unless you changed the value to *NO, your system automatically shuts down and restarts.

For more information about PTFs see Fixes in the **Get Started with iSeries** topic.

12. If you are upgrading IBM iSeries Integration for Windows Server from V5R1 or V5R2, go to “Upgrade the IBM iSeries Integration for Windows Server licensed program” on page 47. Perform the steps under “After upgrading OS/400” and return here.
13. If you are upgrading IBM iSeries Integration for Windows Server from V5R1 or V5R2, you need to upgrade existing integrated Windows servers to the new level. See “Upgrade the integrated Windows server side of the IBM iSeries Integration for Windows Server licensed program” on page 50.

Plan for the installation of Windows server

Before you install Windows 2000 Server or Windows Server 2003, you need to complete and save the command generated by the “Windows server installation advisor”. Alternatively, you may fill out the “Installation worksheet for OS/400 parameters” on page 31.

In addition:

- Make the first integrated Windows server on your network a domain controller and name it carefully. (To change its name, you must first change its role.) Domain controllers contain the master security database. Any domain controller can make changes which are then replicated to all other domain controllers.

- A member server is part of the domain, but it has no role in security administration. You can promote a server to a domain controller without reinstalling the server.

See “Install Windows 2000 Server or Windows Server 2003” on page 43 to continue.

Network server descriptions

Network server descriptions (NWSDs) represent an integrated Windows server on iSeries. The Install Windows server (INSWNTSVR) command automatically creates an NWSD for each integrated server that you install. The NWSD typically has the same name as the server. When you perform an action on the NWSD, you also take action on the server. For example, varying the NWSD on starts the server, and varying the NWSD off shuts down the server.

Installation worksheet for OS/400 parameters

Prior to installing Windows 2000 Server or Windows Server 2003, complete either the Windows server installation advisor or this installation worksheet.

This work sheet, completed, will help you to install and configure your system.

Field	Description and Instructions	Value
Network server description	<p>Defines the operating characteristics and communications connections of the network server that controls the integrated Windows server. See “Network server descriptions” for more information about network server descriptions.</p> <p>Use a name that is easy to remember. The name can have up to 8 characters. Use only the characters A - Z and 0 - 9 in the name, and use a letter for the first character. The network server description name is also the computer name and TCP/IP host name of the integrated server.</p>	
Install type	<p>Specifies the type of install to perform. Choose one of the following:</p> <p>*FULL Required when installing on an internal Integrated xSeries Server (IXS) and is optional when installing on an external xSeries server attached with an Integrated xSeries Adapter (IXA).</p> <p>*BASIC Optional install type when installing on an externally attached xSeries server attached with an IXA. With this option, the first part of the install process is controlled by the OS/400 Install Windows server INSWNTSVR command. Then the install is completed by the xSeries install process using the ServerGuide™ CD.</p>	

Field	Description and Instructions	Value
Resource name	<p>Identifies the Windows server hardware. To determine the name, enter DSPHDWRSC *CMN (Display Communication Hardware Resources) at the OS/400 command line. Most IXS types will have a resource name formatted as LINxx where xx is a number. These are described as File Server IOAs. The 6617 Integrated Netfinity Server will have a resource name formatted CCxx where xx is a number. These are described as File Server IOPs.</p> <p>“Tip: Find resource names when you have multiple integrated servers” on page 42</p>	
Domain role	<p>Specifies the role performed by the network server:</p> <p>*DMNCTL Signifies that this server is a domain controller, managing user access between servers and clients. To complete the installation of a *DMNCTL, you must promote the server using the Windows DCPROMO command after the INSWNTSVR command has completed.</p> <p>*SERVER Signifies that this server is a stand-alone or member server that provides services such as printing or e-mail to client computers but does not control access. To change the domain role to or from *SERVER, you promote or demote the server.</p>	
TCP/IP port configuration	<p>Use this parameter if you are installing Windows server and you do not want OS/400 to use external host LAN. Specify the Windows TCP/IP configuration values that are specific to each adapter port. Otherwise, skip this step and use the default value *NONE. If you plan to share the network adapters with the iSeries using external host LAN (on models that support doing so), use the parameters Port 1 and Port 2 as appropriate.</p>	<ul style="list-style-type: none"> • Port 1 <ul style="list-style-type: none"> – IP address – Subnet mask – Gateway • Port 2 <ul style="list-style-type: none"> – IP address – Subnet mask – Gateway • Port 3 <ul style="list-style-type: none"> – IP address – Subnet mask – Gateway • Port 4 <ul style="list-style-type: none"> – IP address – Subnet mask – Gateway

Field	Description and Instructions	Value
Virtual Ethernet port	<p>Specifies the TCP/IP configuration for the virtual Ethernet networks used by the file server.Notes:This parameter is only available for servers installing Windows server on an Integrated xSeries Server (models 2890, 2892, and 4812) or an Integrated xSeries Adapter (model 2689).</p> <p>A matching virtual Ethernet port is required to install the Windows Cluster service.</p> <p>Element 1: Port</p> <ul style="list-style-type: none"> • *NONE: Specifies that there is no virtual Ethernet port configuration. • *VRTETHx: The network server virtual Ethernet port <i>x</i> is configured, where <i>x</i> has a value of 0 through 9. <p>Element 2: Windows internet address The Windows internet address for the port in the form, nnn.nnn.nnn.nnn, where nnn is a decimal number ranging from 0 through 255.</p> <p>Element 3: Windows subnet mask The subnet mask for the Windows internet address in the form, nnn.nnn.nnn.nnn, where nnn is a decimal number ranging from 0 through 255.</p> <p>Element 4: Associated port The resource name that describes the port that is used to establish a connection between a Windows network server and the network.</p> <ul style="list-style-type: none"> • *NONE An associated port resource name is not associated with the line. • resource-name The resource name. 	<ul style="list-style-type: none"> • Virtual port 1 <ul style="list-style-type: none"> – *VRTETHx – IP Address – Subnet mask – Associated Port • Virtual port 2 <ul style="list-style-type: none"> – *VRTETHx – IP Address – Subnet mask – Associated Port • Virtual port 3 <ul style="list-style-type: none"> – *VRTETHx – IP Address – Subnet mask – Associated Port • Virtual port 4 <ul style="list-style-type: none"> – *VRTETHx – IP Address – Subnet mask – Associated Port
TCP/IP local domain name	Specifies the TCP/IP local domain name associated with the integrated server. You can specify *SYS to use the same value the OS/400 system uses.	
TCP/IP name server system	Specifies the Internet address of the name server used by the integrated server. You can specify up to three Internet addresses, or you can specify *SYS to use the same value the OS/400 uses.	
Server domain name	Applies only to domain controllers. Specifies the Windows domain on which the server will be a domain controller.	
To workgroup	Specifies the name of the Windows server workgroup in which the server participates.	
To domain	Specifies the name of the Windows domain in which the server participates.	

Field	Description and Instructions	Value
Server message queue and library	<p>Specify the name of the message queue and the library it will be located in. If the message queue does not already exist, the INSWNTSVR command creates it. The message queue is where all event logs and errors associated with this server are sent. You should specify a MSGQ name and library. You can also specify *JOBLOG to send nonsevere errors to the job log of the user administration monitor and severe errors to QSYSOPR. If you specify *NONE, nonsevere errors are not sent to OS/400, and severe errors are sent to QSYSOPR.</p>	<p>Queue: Library:</p>
Event log	<p>Specifies whether or not OS/400 receives event log messages from the integrated server. The choices are all, system, security, application, or none:</p> <p>*ALL OS/400 receives all event log messages.</p> <p>*NONE No event log messages are received.</p> <p>*SYS OS/400 receives system event log messages.</p> <p>*SEC OS/400 receives security event log messages.</p> <p>*APP OS/400 receives application event log messages.</p> <p>Note: If you have the integrated server send its security log to the iSeries (by specifying *ALL or *SEC), be sure to set up the message queue with the correct security.</p>	

Field	Description and Instructions	Value
Installation source and system drive sizes and auxiliary storage pool (ASP)	<p>Specify the size of the network server storage spaces for the installation source and system drives and in which ASP (1 - 255) you want them. An ASP device name can be specified in place of the ASP numbers 33-255 when the storage space should be created in an independent auxiliary storage pool. However, if a name is used, the ASP number field must be left as the default value of 1 or the place holder value of *N.</p> <p>The installation source drive (drive D) must be large enough to hold the contents of the I386 directory on the Windows server installation CD image and the IBM iSeries Integration for Windows Server code.</p> <p>The system drive (drive C) must be large enough to hold the Windows server operating system. When installing on Integrated Netfinity Servers 6617 and 2850, the limit is 1,024 to 8,000 MB. When installing Windows server on all other hardware types, the limit is 1,024 to 1,024,000 MB, depending on your resource capabilities. Consider these factors:</p> <ul style="list-style-type: none"> • Your version of Windows server (Refer to Microsoft documentation for operating system requirements.) • Primary usage (print/file serving) and number of Terminal Server users. • Free space on system drive. • Application resource requirements. • Need for crash dump file. <p>OS/400 creates and links the drive as a FAT or NTFS network server storage space, depending on the size.</p> <p>For more information about these drives, see "Predefined disk drives for integrated Windows servers" on page 85.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. The INSWNTSVR command automatically sets the system drive size if a size is specified that is smaller than the value listed as the minimum free system partition disk space (FreeSysPartDiskSpace in the TXTSETUP.SIF file). 2. When deciding the size of each drive, allow room for future needs such as new applications or upgrades to the Windows server product. 3. Support for independent ASPs (33 - 255) is provided through iSeries Navigator. For more information about working with independent ASPs, see Independent disk pools. Both the Information Center and iSeries Navigator refer to ASPs as disk pools. To use an independent ASP, the ASP device must be varied on prior to running the INSWNTSVR command. 	<p>Installation source drive:</p> <p>Size:</p> <p>ASP:</p> <p>ASPDEV:</p> <p>System drive:</p> <p>Size:</p> <p>ASP:</p> <p>ASPDEV:</p>

Field	Description and Instructions	Value
License mode	<p>Determines the license mode to install Microsoft Windows server.</p> <p>Element 1 License type:</p> <p>*PERSEAT Indicates that a client license has been purchased for each computer that accesses the server.</p> <p>*PERSERVER Indicates that client licenses have been purchased for the server to allow a certain number of concurrent connections to the server.</p> <p>Element 2 Client licenses:</p> <p>*NONE Indicates that no client licenses are installed. *NONE must be specified when *PERSEAT is specified.</p> <p>number-client-licenses: Specifies the number of client licenses purchased for the server being installed.</p> <p>Element 3 Windows Terminal Services:</p> <p>*TSENABLE For Windows 2000, install Windows Terminal Services and Terminal Services licensing.</p> <p>*PERDEVICE *PERDEVICE Installs and configures Windows 2003 Terminal Services to require that each connected device has a valid Windows Terminal Server access license. If the client has a Terminal Server access license, it can access more than one Terminal Server.</p> <p>*PERUSER Installs and configures Windows 2003 Terminal Server to provide one Terminal Server access license for each active user.</p> <p>*NONE There are no Terminal Server desktop licenses for this server.</p>	<p>License type:</p> <p>Client licenses:</p> <p>Terminal services:</p>
Propagate domain user (PRPDMNUSR)	<p>Specifies if this server should be used to propagate and synchronize users to the Windows domain or active directory.</p> <p>*YES Send user updates to the Windows domain or active directory through this server.</p> <p>*NO Do not send user updates to the Windows domain or active directory through this server.</p>	
Shutdown timeout (SHUTDTIMO)	<p>A value which determines how long OS/400 waits to allow programs to end before shutting down the IXS or IXA. The delay can be from 2 to 45 minutes. If you do not specify a value, it will be set to 15 minutes.</p>	Shutdown timeout:

Field	Description and Instructions	Value
Restricted device resources	<p>Restricts iSeries tape and optical devices from being used by the integrated server.</p> <p>*NONE Restricts no tape or optical devices from being used by the integrated server.</p> <p>*ALL Restricts all tape and optical devices from being used by the integrated server.</p> <p>*ALLTAPE Restricts all tape resources from being used by the integrated server.</p> <p>*ALLOPT Restricts all optical resources from being used by the integrated server.</p> <p>restricted-device Specify up to 10 device resources that you do not want the integrated server to use.</p>	
Time zone	(Optional) Records the time zone of the iSeries for use in the Windows server phase of installation. See "Time synchronization" on page 28.	
Internal LAN port (For Integrated Netfinity Servers)	<p>A local area network (see "Networking concepts" on page 10) exists between OS/400 and Windows server. Both the OS/400 side and the Windows server side of this LAN have IP addresses and subnet masks.</p> <p>Note: By default, the INSWNTSVR command sets up these addresses automatically. These addresses are in the form of 192.168.xx.yy. If your site uses class C addresses, it is possible for duplicate IP addresses to be generated.</p> <p>To avoid potential conflicts, you can also specify Internet addresses that you know will be unique across your system. Use addresses in the form a.b.x.y where a.b.x is the same value for both sides of the internal LAN and ensure that the internal LAN occupies its own subnet on OS/400. Use the Internal LAN port parameter under additional parameters of the INSWNTSVR command.</p> <p>The subnet mask is always 255.255.255.0.</p>	<p>OS/400-side IP address:</p> <p>Windows server-side IP address:</p>

Field	Description and Instructions	Value
Virtual Ethernet point-to-point (For Integrated xSeries Servers and adapters.)	<p>A local area network (see "Networking concepts" on page 10) exists between OS/400 and Windows server. Both the OS/400 side and the Windows server side of this LAN have IP addresses and subnet masks.</p> <p>Note: By default, the INSWNTSVR command sets up these addresses automatically. These addresses are in the form of 192.168.xx.yy. If your site uses class C addresses, it is possible for duplicate IP addresses to be generated.</p> <p>To avoid potential conflicts, you can also specify Internet addresses that you know will be unique across your system. Use addresses in the form a.b.x.y where a.b.x is the same value for both sides of the internal LAN and ensure that the internal LAN occupies its own subnet on OS/400. Use the Virtual PTP Ethernet port parameter under additional parameters of the INSWNTSVR command.</p> <p>The subnet mask is always 255.255.255.0.</p>	<p>OS/400-side IP address:</p> <p>Windows server-side IP address:</p>
Configuration file	<p>During the installation, creates and specifies a customized NWSD (see Chapter 14, "Network server description configuration files," on page 159).</p> <p>The default is *NONE. To specify a configuration file that you have created, substitute the name of the file and the library where it is stored (*LIBL, *CURLIB, or the name of the library).</p>	

Windows Cluster Service information

Notes:

Fill in this work sheet only when installing a clustered integrated server and your hardware model supports Windows Cluster service. (Integrated Netfinity Servers do not support Windows Cluster service.)

Network adapters are referred to as ports in OS/400.

Item	Description and Instructions	Value
Cluster name	<p>Specifies the name of the cluster. Administrators will use this name for connections to the cluster. The cluster name must be different from the domain name, from all computer names on the domain, and from other cluster names on the domain.</p> <p>The cluster name is also used to create the network server storage space that will be used as the Windows cluster quorum resource.</p> <p>*NONE: Do not form or join a Windows Cluster.</p> <p>cluster-name: Specify the name of the cluster.</p>	

Item	Description and Instructions	Value
Cluster configuration: (Elements 1 - 4)	<p>Specifies the parameters required to configure a new Windows Cluster.</p> <p>Notes: This parameter is used to verify the OS/400 cluster configuration. The Microsoft configuration wizards are used to install the Cluster service.</p> <p>This parameter is only required when forming a new Windows cluster using the Cluster name (CLU) parameter.</p> <p>Element 1: Cluster domain name Specifies the domain to which the cluster belongs. If the cluster already exists, the cluster will be joined, otherwise, the cluster will be formed. If forming a cluster, the Cluster configuration (CLUCFG) parameter must be specified.</p> <p>cluster-domain-name: Specify the domain name to which the cluster belongs when forming a new cluster.</p> <p>Element 2: Quorum resource size Specifies the size in megabytes of the storage space used as the Windows quorum resource.</p> <p>*CALC Specifies that the size should be calculated to be the default value based on the Windows server version (WNTVER) parameter.</p> <p>quorum-size Specifies the Windows quorum resource size in megabytes. The size must be at least 550 megabytes but no larger than 1024000 megabytes.</p> <p>Element 3: Quorum resource ASP Specifies the auxiliary storage pool for the storage space used as the Windows quorum resource. Specify one of the following values:</p> <p>1: The storage space is created in auxiliary storage pool 1, the system auxiliary storage pool (ASP).</p> <p>quorum-ASP: Specify a value ranging from 2 through 255 for the ASP identifier. Valid values depend on how many ASPs are defined on the system.</p> <p>Element 4: Quorum ASP device Specifies the independent auxiliary storage pool device name for the storage space used as the Windows quorum resource. Note: You cannot specify both a Quorum resource ASP and a Quorum ASP device value.</p>	<p>Cluster domain name:</p> <p>Quorum resource size:</p> <p>Quorum resource ASP:</p> <p>Quorum ASP device:</p>

Item	Description and Instructions	Value
Cluster configuration: (Elements 5-7)	<p>Element 5: Cluster connection port Specifies the connection port used for the Cluster service communication.</p> <p>*VRTETHx: The network server virtual Ethernet port x is configured, where x has a value of 0 through 9.</p> <p>Note: The virtual Ethernet port must be configured to match this value.Element 6: Cluster Internet Address Specifies the Internet address for the cluster.</p> <p>IP address: Specify the cluster internet address in the form, xxx.yyy.zzz.nnn, where xxx, yyy, zzz, and nnn are decimal numbers ranging from 0 through 255.</p> <p>Note: The Internet address selected must be unique across all NWSO objects and the OS/400 TCP/IP configuration.</p> <p>Element 7: Cluster Subnet Mask</p> <p>subnet-mask: Specifies the subnet mask for the cluster in the form, nnn.nnn.nnn.nnn, where nnn is a decimal number ranging from 0 through 255.</p>	<p>Connection port:</p> <p>Cluster Internet Address:</p> <p>Cluster Subnet mask:</p>

Integrated Windows server external host LAN networking information

Note: Fill in this work sheet only in these conditions:

- Your model of Integrated Netfinity Server supports external host LAN (the Integrated xSeries Server does not).
- You plan to use the LAN adapters installed in models of the Integrated Netfinity Server as external host LAN for your iSeries.

LAN adapters are referred to as "ports" in OS/400.

Item	Description and Instructions	Value
Line type	Identifies the type of network adapter that is installed and that will be shared by OS/400 and Windows server. This value can be one of four types: *ETH10M (10 Mbps Ethernet), *ETH100M (100 Mbps Ethernet), *TRN4M (4 Mbps token-ring), or *TRN16M (16 Mbps token-ring).	Port 1: Port 2:
Local adapter address	Identifies the IP address on OS/400. The values you can specify depend on the line type. Ethernet lines use values between 020000000000 and 7EFFFFFFF. The second character must be 2, 6, A, or E. Token-ring lines use values between 400000000000 and 7EFFFFFFF. Your network administrator can assign your local IP address. Every network adapter on the LAN must have a unique local adapter IP address.	Port 1: Port 2:

Item	Description and Instructions	Value
Maximum transmission unit	Specifies the maximum size (in bytes) of IP datagrams that are transmitted. Either take the default of 1492 or specify MTU to take the optimized value of your interface type. A larger size increases the efficiency of sending and receiving data. However, problems can arise if your network has bridges or routers that cannot accommodate larger sizes.	Port 1: Port 2:
OS/400 Internet address	Specify the OS/400 Internet address for each shared LAN adapter. (An Internet address consists of four numbers, each between 0 and 255, separated by periods.) All Internet address must be unique on the network. Your network administrator can give you the Internet addresses.	OS/400 Port 1: OS/400 Port 2:
OS/400 Subnet mask	Used in TCP/IP communications. A subnet mask consists of four numbers, each between 0 and 255, separated by periods. Your network administrator can give you the subnet mask.	OS/400 Port 1: OS/400 Port 2:
Windows server Internet address	Specify the integrated server Internet address for each shared LAN adapter. (An Internet address consists of four numbers, each between 0 and 255, separated by periods.) All Internet addresses must be unique on the network. Your network administrator can give you the Internet addresses.	Windows server Port 1: Windows server Port 2:
Windows server subnet mask	Used in TCP/IP communications. A subnet mask consists of four numbers, each between 0 and 255, separated by periods. Your network administrator can give you the subnet mask.	Windows server Port 1: Windows server Port 2:
Windows server gateway	Used in TCP/IP communications. Your network administrator can give you the gateway IP address.	Windows server Port 1: Windows server Port 2:

Comparison of FAT, FAT32, and NTFS file systems

Windows 2000 Server or Windows Server 2003 allow you to choose between NTFS, FAT, and FAT32 file systems. IBM iSeries Integration for Windows Server installs your system drives using an appropriate file system that depends on the hardware resource capabilities, Windows version and intended use. The installation command gives you the option of converting FAT or FAT32 drives to NTFS. In some cases, the conversion to NTFS is automatically performed based on the intended use of the server (for example, a domain role of *DMNCTL).

Note: Do not convert the D drive to NTFS. It must remain FAT.

You do have the option of converting the C drive. Here are some comparisons that might help you decide:

FAT	FAT32	NTFS
Volume from floppy diskette size up to 4 GB	Volumes from 512 MB to 2 terabytes (TB) (Size limited to 32 GB by Windows server and OS/400 CRTNWSSTG)	Volume 10 MB to 2 TB
Maximum file size 2 GB	Maximum file size 4 GB	File size limited by size of volume
Does not support Windows 2000 or Windows 2003 Active Directory	Does not support Windows 2000 or Windows 2003 Active Directory	Required to use Windows 2000 or Windows 2003 Active Directory or shared cluster drives

FAT	FAT32	NTFS
Allows access to files on the hard disk with MS-DOS.	Does not allow access to files on the hard disk with MS-DOS.	Does not allow access to files on the hard disk with MS-DOS.
Allows you to customize your server with NWSD configuration files	Allows you to customize your server with NWSD configuration files.	Cannot use NWSD configuration files.
Allows you to use the NWSD dump tool (QFPDMPLS) to retrieve files from the disk for service	Allows you to use the NWSD dump tool to retrieve files from the disk for service	Cannot use the dump tool to retrieve files from the disk

Tip: Find resource names when you have multiple integrated servers

You can have multiple integrated servers of the same type installed on your iSeries. If so, you may not be able to tell them apart on the Display Communication Resources display.

To find out which integrated server a resource name refers to, follow these steps:

1. If you are not already at the Display Communication Resources display, type DSPHDWRSC *CMN; then press Enter.
2. Type a 7 in the Opt field to the left of the resource name for a file server IOA or file server IOP. The Display Resource Detail display appears.
3. Look at the Card Position under the Physical Location heading.
4. Look at the labels on the slots of your iSeries. One slot should be labeled with the same number or combination of letters and numbers shown in the Card Position field. This slot contains the Integrated xSeries Server hardware to which the resource name refers.

Go back to “Installation worksheet for OS/400 parameters” on page 31.

Supported language versions

These languages are supported on the Language version parameter (LNGVER) of the Install Windows server (INSWNTSVR) command:

LNGVER	National Language
*PRIMARY	Uses the language version of the primary language that is installed on iSeries
2911	Slovenian
2922	Portuguese
2923	Dutch
2924	English upper/lowercase
2925	Finnish
2926	Danish
2928	French
2929	German
2931	Spanish
2932	Italian
2933	Norwegian
2937	Swedish
2938	English uppercase DBCS
2939	German MNCS
2940	French MNCS

LNGVER	National Language
2942	Italian MNCS
2950	English uppercase
2962	Japanese DBCS
2963	Dutch MNCS
2966	Belgian French
2975	Czech
2976	Hungarian
2978	Polish
2979	Russian
2980	Brazilian Portuguese
2981	Canadian French MNCS
2984	English upper/lowercase DBCS
2986	Korean DBCS
2987	Chinese, Traditional
2989	Chinese, Simplified
2994	Slovakian
2996	Portuguese MNCS


IBM iSeries Integration for Windows Server supports Windows Multi-Language User Interface.

Install Windows 2000 Server or Windows Server 2003

You will need the following:

- A CD that contains the Windows 2000 Server or Windows Server 2003 software (or an image of the CD).
- Your Windows license key (printed on the back of the installation CD jewel case or Certificate document).
- A completed and printed “Installation worksheet for OS/400 parameters” on page 31 or the command string generated by the installation advisor.

Note: Microsoft documentation tells you to disable disk mirroring and disconnect any uninterruptible power supply before installing or upgrading Windows server. Be aware that this does not apply to disk mirroring or an uninterruptible power supply that you have on your iSeries.

Note: If you have an Integrated xSeries Server or an Integrated xSeries Adapter that is not listed in the “Hardware requirements” on page 23 section, see the IBM Windows Integration  for installation instructions.

Do the following:

1. “Start the installation from the OS/400 console” on page 44.
2. “Continue the installation from the integrated Windows server console” on page 46.
3. “Complete the server installation” on page 46.

If you encounter any error messages during the installation, see “Respond to error messages during installation” on page 60.

Start the installation from the OS/400 console

To install Windows 2000 Server or Windows Server 2003 on iSeries, you need *IOSYSCFG, *ALLOBJ, and *JOBCTL special authority. You must have your Windows server license key available. In most cases, it is printed on the back of the installation CD jewel case.

1. When performing an installation type of *FULL, place the installation CD in the iSeries server optical drive (unless you plan to use an image of the installation CD).

When performing an Install type of *BASIC, place the ServerGuide CD in the attached xSeries server CD-ROM drive.

Note: If you are using an upgrade version of the installation CD, Windows server prompts you for a non-upgrade version during the text mode of the installation.

2. Use one of the following methods to begin the installation:
 - If the Install Windows server (INSWNTSVR) command generated by the Windows Server Installation Advisor is available:
 - a. Call QCMD at the OS/400 command line to start a command entry prompt and select F11=Display Full.
 - b. Paste the INSWNTSVR command generated by the Windows Server Installation Advisor at the OS/400 command line and press Enter to run the command.
 - c. The installation starts and can take up to an hour. You may be prompted to enter additional information. Afterward, go to “Continue the installation from the integrated Windows server console” on page 46.
 - Otherwise, begin the installation at the OS/400 command line by typing INSWNTSVR and pressing F4 to prompt the command.
3. In the Network server description field (see “Network server descriptions” on page 31 for more information), type the name for this server that you filled out in the advisor; press Enter.
4. In the Install type field, type the value (*FULL or *BASIC) that you filled out in the advisor.
5. In the Resource Name and Domain Role fields, type the information that you filled out in the advisor.
6. Choose the Windows server version you want to install.
7. Press F10 to see more parameters.
8. If you want to install the server from a stored image instead of the physical CD, specify the path to that image in the Windows source directory field.
9. In the Install option field, use the default *INSTALL.
10. If you want the installation to configure TCP/IP properties for any network adapters installed in the iSeries which will be ‘taken over’ by the new integrated server, specify the Windows TCP/IP configuration values from the “Installation worksheet for OS/400 parameters” on page 31. Otherwise, skip this step and use the default value *NONE. To install and configure a virtual Ethernet port, specify the Windows TCP/IP configuration values for the virtual Ethernet ports from the Installation work sheet for OS/400 parameters.
11. Type the value from the “Installation worksheet for OS/400 parameters” on page 31 for the TCP/IP local domain name.
12. Type the values from the “Installation worksheet for OS/400 parameters” on page 31 in these fields:
 - TCP/IP name server system
 - Server message queue
 - Library
 - In the Event log field, specify which event log messages you want OS/400 to receive from the server.
 - In the fields for Server storage space sizes, type the values from the “Installation worksheet for OS/400 parameters” on page 31. Increase the install source size from the default to at least 400[®] MB to hold the installation CD image. OS/400 creates and links the drives as network server storage spaces.

- If you want to choose a different auxiliary storage pool (ASP) for the install source and system drives, specify it in the corresponding element of either the Storage space ASP or Server storage ASP device fields.
 - For system drives up to 2047 MB, in the Convert to NTFS field, you can specify *NO to leave the integrated server's system drive formatted with the file allocation table (FAT) file system. If you want the system drive converted to the New Technology File System (NTFS) during the installation, specify *YES. For information that might help you decide, see "Comparison of FAT, FAT32, and NTFS file systems" on page 41. OS/400 automatically formats system drives larger than 2047 MB as NTFS if necessary, depending on hardware and software capabilities.
13. In the Full Name field, specify the name of the user who holds the Windows server license you are installing.
 14. In the Organization field, specify the name of the organization that holds the Windows server license you are installing.
 15. In the Language version field, specify *PRIMARY to have the IBM iSeries Integration for Windows Server licensed program use your primary language. To prevent problems with predefined names that cannot be enrolled, make sure that the integration licensed program and Windows server will be using the same language. If you need to know which languages the command supports, look at "Supported language versions" on page 42.
 16. In the Synchronize date and time field, specify *YES to have OS/400 synchronize the date and time with the integrated server every 30 minutes. If you want OS/400 to synchronize the date and time with the integrated server only when you vary it on, type *NO.
 17. In the Propagate domain user field, specify if this server should be used to propagate and synchronize users to the Windows domain or active directory.
 18. In the Shutdown timeout field, specify the integrated server's shutdown time-out value in minutes. This is used to limit the amount of time that the integrated server's operating system is given to shut down before the server is varied offline.
 19. In the Windows license key field, specify the CD key that Microsoft has provided, including the dash. In most cases, you can find this CD key printed on the back of the Windows installation CD jewel case.
 20. In the License type field, specify the type of Windows server license that you purchased.
 21. If you specified *PERSERVER in the License type field, then in the Client licenses field, specify the number of client licenses that you purchased.
 22. In the Restricted device resources field, type the value from the "Installation worksheet for OS/400 parameters" on page 31.
 23. Filling out additional parameters allows you to do the following:
 - Install a keyboard type on the integrated server other than the default. (Valid keyboard style identifiers are listed in the TXTSETUP.SIF file in the I386 directory of the Windows server installation source.)
 - Use your own IP addresses for the private LAN.
 - Use an NWSD configuration file. See Chapter 14, "Network server description configuration files," on page 159.
 - Use the Integrated Netfinity Server as an external host LAN (not supported for Integrated xSeries server or Integrated xSeries Adapter).
 - Configure a new or existing Windows Cluster configuration.
- Provide any other information that seems relevant for your needs and press Enter.

The integrated Windows server starts to install. The second stage of the installation process is "Continue the installation from the integrated Windows server console" on page 46. The process will take approximately 1 hour, depending on your hardware configuration.

Continue the installation from the integrated Windows server console

When the OS/400 phase of the installation completes, the integrated server starts. The Windows server phase of the installation begins. This phase of the installation is easy if you have completed the steps in “Prepare for the installation of integrated Windows servers” on page 26 and specified the installation attributes on the Install Windows server (INSWNTSVR) command.

To complete installation of Windows server, when not using ServerGuide, perform these tasks:

1. If the installation program prompts you for a non-upgrade version of the Windows server CD, insert the non-upgrade version. Then press Enter to continue with the installation.

Note: If the installation program prompts you again for the non-upgrade CD, just press Enter.

2. In the **License Agreement** step (in Windows Server Setup window), click on the **I accept this agreement** radio button. Then click on **Next**.
3. If you get error messages, click **OK**, and the installation program lets you correct the situation or provide the necessary information. For examples of these error messages and how to respond, see “Respond to error messages during installation” on page 60.

4. Enter and confirm the password in the **Computer Name and Administrator Password** window.

5. On the **Date/Time Settings** panel:

- a. Confirm that the OS/400 time zone is correct and matches the Time Zone system value given in Windows server installation advisor. See “Time synchronization” on page 28.
- b. If you are in an area that observes Daylight Savings Time, leave the **Automatically adjust clock** box checked.

If you know for sure that you do not observe Daylight Savings Time, clear the “Automatically adjust clock for daylight savings changes” check box.

6. On the Completing the Windows Setup Wizard panel, click **Finish**.
7. On the **Windows Setup** window, click the **Restart Now** button, or wait 15 seconds and the server automatically restarts.

Note: When installing a domain controller (DMNROLE of *DMNCTL) type of integrated Windows server, Active Directory should be installed at this time by running the DCPROMO command. Refer to the Microsoft documentation for more information on the Active Directory installation.


To complete the installation of Windows server when using ServerGuide, perform these tasks:

- Insert the ServerGuide CD in the local optical drive of the HSL attached server. (The IXA attached xSeries server.)
- Respond **G** to the message NTA100C “Insert ServerGuide CD-ROM into &2 optical device. (C G)”
- Follow the ServerGuide Wizard through the install process.

See “Complete the server installation.”

Complete the server installation

Perform a few final tasks after installing Windows 2000 Server or Windows Server 2003 on OS/400 to verify that it is correctly installed and ready.

1. It is recommended to install the latest supported Microsoft service pack. Refer to the Microsoft Service packs page for the latest supported service pack list on the Service Information page of the IBM Windows Integration Web site  .
2. If you want the integrated Windows server to automatically vary on when you start TCP/IP, see “Set an integrated Windows server to automatically vary on with TCP/IP” on page 61.
3. If you disconnected a LAN adapter before the installation, reconnect it now by plugging in the cable.
4. Change the QRETSVRSEC system value on OS/400 to ensure that OS/400 keeps passwords (this avoids delays when users sign-on):

- On the OS/400 command line, enter the command:
WRKSYSVAL SYSVAL(QRETSVRSEC)
 - To display the value, enter a 2 in the Option field and press Enter.
 - Change the value of Retain server security data to 1.
5. You can prevent the optical drive from changing drive letters whenever you link a user storage space to the server. Use **Disk Management** to assign the integrated server optical drive letter. (For example, you could make it drive X.)
 6. You can customize your servers by creating your own NWSD configuration file. See Chapter 14, “Network server description configuration files,” on page 159.
 7. If you want Windows clustering, see “Windows Cluster Service” on page 53.
 8. If your server is installed with Windows Server 2003 and has Active Directory installed (for example, it is a domain controller), see “Enabling QNTC access to Windows Server 2003 with Active Directory” on page 59.
 9. If you are using a 2892-002 or 4812-001 IXS hardware type with Microsoft Windows 2000 Server, you should install special video device drivers to take advantage of the ATI Radeon video chip which is on the 2892-002 and 4812-001 IXS. See “Install the ATI Radeon 7000M video device drivers for Windows 2000 on the 2892-002 or 4812-001 Integrated xSeries Server” on page 59.
 10. If you are using a 2892-002 or 4812-001 IXS hardware type with Microsoft Windows Server 2003, you should adjust the hardware acceleration settings to achieve optimal performance. See “Adjust hardware acceleration for Windows Server 2003 on the 2892-002 or 4812-001 Integrated xSeries Server” on page 60.

Attention: If you plan to use a firewall with the integrated server, be sure not to route the Internet addresses for the private LAN to a software common knowledge IR system (SOCKS) server acting as a firewall. Doing so causes connection failures. For information about setting up a firewall, see the topic Firewall: getting started.

Upgrade the IBM iSeries Integration for Windows Server licensed program


If you are upgrading OS/400 and IBM iSeries Integration for Windows Server to V5R3, you need the CD containing the 5722-WSV product. If you also plan to install new Integrated xSeries Server hardware, make sure you complete this software installation first. As you follow the upgrade procedure in the iSeries

Software Installation manual , take these additional steps:

Preparing to upgrade:

1. Ensure that you have the latest code fixes installed on all your existing integrated Windows servers, as well as on your OS/400. See “Code fixes” on page 61.
2. Ensure that you have a system backup available that includes the storage allocated to your integrated servers.
3. As a precaution, record the associated resources for your hardware:
 - a. On the OS/400 command line, type WRKCFGSTS *NWS and press Enter.
 - b. Type 8 in the option column next to the network server description. The Work with Network Server Descriptions display appears.
 - c. Type 5 in the option column next to the network server description.
 - d. Page down until you see the field Resource name and record the value for this network server (for example, CC07 or LIN05).
 - e. Press F12 twice to back out of this command.
 - f. On the OS/400 command line, type WRKHDWRSC TYPE(*CMN) and press Enter.

- g. Type 7 (Display resource detail) in the option column next to the resource name that you identified in step 3 d. The type column has the CCIN number for the Integrated xSeries Server hardware, and the text description should be File Server IOP or File Server IOA.
 - h. If you have multiple Integrated xSeries Servers of the same type installed on your iSeries, you may be able to identify the correct one by card position:
 - 1) look at the Card Position under the Physical Location heading.
 - 2) Look at the labels on the slots of your iSeries. One slot should be labeled with the same number or combination of letters and numbers shown in the Card Position field. This slot contains the Integrated xSeries Server to which the resource name refers.
 - i. Record the information that appears in the Type-model and Serial number fields.
 - j. Press F12 twice to back out of the command.
4. Vary off all of your integrated servers. See “Start and stop an integrated server” on page 75.

To install the new version of OS/400 on your iSeries, return to the procedure in the iSeries Software Installation manual  .

After upgrading OS/400, complete these additional steps:

1. Start the integrated server (see “Start and stop an integrated server” on page 75) and verify that it has the same resource name:
 - a. On the OS/400 command line, type WRKHDWRSC TYPE(*CMN) and press Enter.
 - b. Type 7 (Display resource detail) in the option column next to the resource name that you identified in step 3d on page 47. Verify that the information that appears in the Type-model and Serial number fields match what you recorded for this resource.
 - c. If these fields do not match what you recorded, do this:
 - 1) Press F12 to back out to the previous display.
 - 2) Use option 7 to display the resource details for other resource names in the list until you find the one whose Type-model and Serial number match those your recorded. Note the resource name that OS/400 now associates with this Integrated xSeries Server hardware. Press F12 to back out of this command.
 - 3) On the OS/400 command line, type WRKNWSD and press Enter. The Work with Network Server Descriptions display appears.
 - 4) Type 2 (change) in the option column next to the network server description and press Enter. The Change Network Server Description display appears.
 - 5) Change the resource name to the new correct resource name for this network server.
2. Install IBM iSeries Integration for Windows server on your existing integrated servers. See “Install IBM iSeries Integration for Windows Server licensed program” on page 30.

Upgrade your server from Windows NT 4.0 to Windows 2000 Server

The process for upgrading your integrated server from Windows NT 4.0 to Windows 2000 is different than it would be on a standalone PC server. You cannot upgrade your server starting from the integrated Windows server console. You must begin at the OS/400 console, just as you do for a fresh installation. Do not try to upgrade from the integrated server console. If you do, you will have to restore a recent backup of your system drive and possibly your user drives to recover. You might even have to reinstall.

Note: Upgrades from Windows NT 4.0 or Windows 2000 to Windows Server 2003 are not supported. You must perform a new install for Windows Server 2003.

To upgrade your server, you need *IOSYSCFG, *ALLOBJ, and *JOBCTL special authority. You must have your Windows server license key available. In most cases, it is printed on the back of the installation CD jewel case.

To upgrade from Windows NT 4.0 to Windows 2000, do this:

1. Back up all drives related to your integrated server. Otherwise, you will lose any user data that is stored on the D drive because the upgrade process re-creates that drive.
2. Ensure that you have installed the latest prerequisite program temporary fixes (PTF).
3. Verify that the server is inactive. See “Start and stop an integrated server” on page 75.
4. Place the Microsoft installation CD for the version you want to install in the optical drive (unless you plan to use an image of the installation CD).

Note: If you are using an upgrade version of the Windows server installation CD, Windows server may prompt you for a non-upgrade version. At that time, insert the non-upgrade Windows server CD and press Enter to continue the installation.

5. On the OS/400 command line, type the Install Windows server command: INSWNTSVR, and press F4.
6. In the Network server description field, type the name for the server that you are upgrading and press Enter. See “Network server descriptions” on page 31. Upgrade your primary domain controller first. OS/400 retrieves NWSD information about the existing server, and the Install Windows server display appears.

Note: If you are upgrading from a Windows NT 4.0 Backup Domain Controller, OS/400 considers the Domain role to be *SERVER. You can promote it to a domain controller after the upgrade.

7. In the Windows server version field, specify *WIN2000 for Windows 2000 Server and press F10 to see additional parameters.
8. Specify TCP/IP port configuration information in this menu unless you used the Port 1 and Port 2 parameters on your original installation (for sharing network adapters). In that case, use the Port 1 and Port 2 parameters instead.
9. Change the install source size from the default to at least 400.
10. You **cannot** change the size for the system server storage space during an upgrade. If your system drive is not large enough to hold the new version, you must do a fresh installation instead of an upgrade. An upgrade requires at least 1 GB of free space. Consult Microsoft documentation for recommendations for your specific configuration.

Note: More free space might be required if additional services or functions have been installed such as Terminal Server. These additional requirements might not be detected by the INSWNTSVR command and will only appear when the QUPGRADE.BAT file is run to start the Windows upgrade. Insufficient free space may not allow the upgrade to continue, requiring additional space on the system drive to be freed up or the upgrade to be canceled and a new server installed. Consult Microsoft documentation for recommendations for your specific configuration.

11. If you want to choose a different auxiliary storage pool (ASP) for the source drive, specify it in the Storage space ASP field.
12. Other values that you can change during an upgrade include:
 - Text description
 - To workgroup
 - To domain
 - Name
 - Organization
 - Language version
 - Windows license key
 - License mode
 - Shutdown timeout
 - Keyboard type
 - Message queue

- Event log processing
- Restricted devices
- NWSD configuration file
- Propagate domain user

If you want to change values for parameters that do not appear, press F10 to see all parameters. Make any of these changes that you want and press Enter to have OS/400 upgrade your server.

13. In inquiry message NTA103F: Windows server MYSERVER will be upgraded. (C G) will appear. Respond G to the inquiry message to have OS/400 continue with the upgrade or C to cancel it.
14. When OS/400 finishes copying files, the Windows NT 4.0 logon appears on the integrated server console. After you log on, go to the **Start** menu and click **Run**.
15. Type D:\QUPGRADE.BAT and click **OK** to continue the upgrade. The Windows server setup window appears. (If you remapped the install source drive, substitute the new drive letter.)
16. Click **I Accept** on the License agreement window. The upgrade goes through several phases that require no intervention.
17. Click **Yes** to restart the server. After the final restart, the new integrated Windows server display appears.
18. Use the **Configure your Server** window that appears to install applications such as Active Directory.
19. If you are installing or upgrading a domain controller that was not the primary domain controller, you need to promote the integrated server. You can do this by running the Windows server dcpromo program:
 - a. Go to the **Start** menu; click **Run**.
 - b. Type dcpromo and click **OK**.

Upgrade the integrated Windows server side of the IBM iSeries Integration for Windows Server licensed program

The IBM Integration for Windows Server licensed program is the software which couples together the iSeries and its integrated Windows servers. Think of it as a translation program. Half of the program runs on the iSeries to translate from the Windows language to the OS/400 language, and the other half runs on the integrated servers to translate from the OS/400 language to the Windows language.

New versions of the IBM iSeries Integration for Windows Server licensed program are installed to OS/400. Then the integrated server part of the licensed program needs to be copied over to the integrated server and installed.

You need to upgrade your existing integrated Windows servers' licensed program when you install:

- A new version of IBM Integration for Windows Server from IBM.
- A new version of Windows server from Microsoft.

New version of the IBM Integration for Windows Server licensed program

When you install a new version of the IBM Integration for Windows Server licensed program, you need to upgrade all your existing integrated servers to that level. If you have multiple integrated servers, you might want to upgrade those servers remotely from OS/400.

This procedure requires that you have the same userid and password on the integrated Windows servers and OS/400.

To upgrade an integrated server, follow these steps:

1. End any applications that are running.
2. Ensure that no users are logged on to the integrated server.

Attention: The integrated server automatically restarts after completion of the installation, so if you skip steps 1 and 2, you risk data loss.

3. From the **Start** menu, choose **Programs**, then **IBM iSeries Integration for Windows Server**, then **Software Level**.

Note: When a new level of the licensed program is available for installation, logging on to an integrated server as an administrator causes Software Level to start automatically.

4. Select the option to **Install Release from iSeries**.
5. Follow the user interface instructions to complete the installation.
6. **Tip:** Afterward, back up the predefined installation and system drives for this server. See “Back up predefined disk drives for integrated Windows servers created on V4R5 and later OS/400 systems” on page 110 for information about backing up these drives. Since it is safer to back up all storage spaces for the server at the same time, you should also back up the associated user-created storage (described in “Back up user-defined disk drives for an integrated Windows server” on page 112).

New version of Windows Server

Upgrade the Windows NT 4.0 primary domain controller (PDC) before upgrading any other machines. To upgrade your servers from Windows NT 4.0 to Windows 2000, see “Upgrade your server from Windows NT 4.0 to Windows 2000 Server” on page 48.

If the PDC is a stand-alone machine (not your Integrated xSeries Server), then you need to run QCONVGRP on all the servers connected to this domain. If the PDC is an Integrated xSeries Server, using the UPGRADE option of the Install Windows server (INSWNTSVR) command converts the groups on the PDC itself. However, you need to run QCONVGRP on all Windows NT 4.0 machines that are attached to this domain.

Migrate from 285x or 661x to 2890 Integrated xSeries Server hardware

Before migrating from 285x or 661x hardware to 2890 Integrated xSeries Server hardware, you must have the latest versions of OS/400 and IBM iSeries Integration for Windows Server installed, as well as the latest code fixes for the upgraded versions. See “Upgrade the IBM iSeries Integration for Windows Server licensed program” on page 47 and “Code fixes” on page 61. Look for information and follow any directions

you find at the IBM Windows Integration Web  site.

To migrate to new hardware, complete these steps:

1. If you did not already record the associated resources for your old Integrated xSeries Server hardware during the software installation, do this now:
 - a. On the OS/400 command line, type WRKNWSD and press Enter. The Work with Network Server Descriptions display appears.
 - b. Type 5 in the option column next to the network server description.
 - c. Page down until you see the field Resource name and record the value for this network server (for example, CC02 or LIN05).
If you have Integrated xSeries Servers of the same type installed on your iSeries, refer to “Tip: Find resource names when you have multiple integrated servers” on page 42.
 - d. On the OS/400 command line, type WRKHDWRSC TYPE(*CMN) and press Enter.
 - e. Type 7 (Display resource detail) in the option column next to the resource name that you identified in step 1c. (The text description should be File Server IOP or File Server IOA.)
 - f. Record the information that appears in the Type-model and Serial number fields.
2. Record the IP address for the internal LAN:
 - a. On the OS/400 command line, type CFGTCP and press Enter. The Configure TCP display appears.
 - b. Type 1 to Work with TCP/IP Interfaces.

- c. Identify the correct line description for the integrated Windows server and record the IP address. (The name of the line description begins with the NWSD name.)
 - d. Press F3 twice to exit from the command.
3. Remove the IBM AS/400 Protocol device driver (IBM AS/400 HostLAN Bridge device driver):
 - a. Click **Start, Settings, and Control Panel**.
 - b. Open **Network and Dial-up Connections**.
 - c. Double-click on any connection.
 - d. Click on the **Properties** button.
 - e. Select the **AS/400 Line Multi-Port Protocol Driver** and click the **Uninstall** button.
 - f. Answer **Yes** and click **Close** and **Close** to complete the removal.
4. Remove all network adapters from the Windows server except the IBM Internal LAN adapter. See “Remove network adapters” on page 70.
5. Remove the line description for the old adapter.

Attention: Do not remove the line description of the internal LAN. It has the name *nwsdname00*, where *nwsdname* is the name of the network server description.
6. Back up the NWSD and its associated disk drives. See “Back up the NWSD of an integrated Windows server” on page 110 and associated “Back up the NWSD and disk drives associated with an integrated Windows server” on page 109.
7. Vary off all your network servers. This step is not necessary if a full system save is done prior to the hardware upgrade. See “Start and stop an integrated server” on page 75.
8. If the new 2890 Integrated xSeries Server hardware is not already installed, follow the directions that come with the hardware to install it.
9. Restore the NWSD and its associated disk drives on the new Integrated xSeries. See “Restore integrated Windows server NWSDs” on page 122 and “Restore an integrated Windows server’s NWSD and disk drives” on page 119. To have OS/400 automatically relink restored storage spaces in the integrated file system to the appropriate NWSD, restore those storage spaces before you restore the NWSD.
10. Restore the line description:
 - a. To restore the line description, type RSTCFG on the OS/400 command line again and press F4.
 - b. In the Objects field, specify the name of the line description.
11. Supply a TCP/IP interface to allow OS/400 to communicate with the new Integrated xSeries Server:
 - a. On the OS/400 command line, type CFGTCP and press Enter. The Work with TCP/IP Interface display appears.
 - b. Type 1 on the command line to add an interface.
 - c. Type the IP address for the Internal LAN from the old system that you recorded in step 2c.
 - d. In the Line description field, specify the name of the line description that you restored in step 10a.
 - e. For the subnet mask, specify 255.255.255.0. Press Enter to complete the command.
12. Use the Work with Hardware Resources (WRKHDWRSC) command to determine the type of the new Integrated xSeries Server hardware and find the resource name:
 - a. On the OS/400 command line, type WRKHDWRSC TYPE(*CMN) and press Enter.
 - b. The 2890 Integrated xSeries Servers has Operational File Server IOA in the text field. (Other models have File Server IOA or File Server IOP.) To identify the hardware in the list, look for the number of the new Integrated xSeries Server in the Type column. “Hardware requirements” on page 23 lists these numbers for Integrated xSeries Servers.
 - c. Note the resource name for that Integrated xSeries Server (in the form LINxx).
13. Use the Change Network Server Description (CHGNWSD) command to change the resource name for the NWSD to the new resource name for the model 2890 Integrated xSeries Server:

- a. On the OS/400 command line, type CHGNWSD NWSD(nwsdname) and press F4.
 - b. In the Resource name field, specify the resource name for the new Integrated xSeries Server hardware that you identified in the previous step; press Enter.
14. “Create a guest user profile for iSeries NetServer” on page 29.
 15. Vary on the NWSD. A message appears to alert you to the possible need for manual intervention.
 16. On the first boot after the restore has completed the integrated server will freeze, so you must reboot at this time.
 17. After the integrated server reboot completes, the line description of the Internal LAN adapter will be in VARY-ON PENDING state and the corresponding icon at the integrated server console will have a red X, indicating the Cable is Disconnected. Ignore any Event Log messages listed for the device driver qvndhli.sys and perform an additional reboot of the integrated server.
 18. Let Windows plug-n-play detect your adapters. Then, manually configure the IP address by referring to the steps in “Install network adapter device drivers and add adapter address information to an integrated Windows server” on page 69.

Windows Cluster Service

Windows cluster service links individual servers so they can perform common tasks. Should any one server stop functioning, a process called failover automatically shifts its workload to another server to provide continuous service. In addition to failover, some forms of clustering also employ load balancing, which enables the computational workload to be distributed across a network of linked computers.


Windows 2000 Advanced Server supports a two-node cluster while Windows Server 2003 Enterprise Edition supports eight-node clusters. Datacenter versions of Windows are not supported.

Windows Cluster Service support is not supported for Integrated Netfinity servers. It is only supported for integrated Windows servers running either Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition.

Note: Windows clustered network server nodes must reside within a single iSeries partition in order to be clustered.

Although the traditional Windows clustered server solution requires a shared physical SCSI or Fibre Channel device, the integrated Windows server solution uses a virtual Fibre Channel bus to share the virtual disk devices between the nodes of a cluster.

In addition, the new support for virtual Ethernet enables high-performance, secure communication for the internal node-to-node communication between clustered nodes.

Detailed checklists for planning and creating a server cluster are available in the online Microsoft help for Server clusters and should be referred to prior to installing and configuring a Windows Cluster server. Additional information, including step-by-step guides to installing Cluster service, is available on the Microsoft Web site  .

For more information about Integration for Windows Server support for Windows Cluster service, see the following topics:

“Install Windows Cluster service” on page 54

Find out how to install and configure Windows Cluster service on the iSeries Integrated Windows Server and on Windows.

“Install Windows Cluster service on an existing server” on page 55

Find out how to create clusters on an existing integrated Windows server.

Install Windows Cluster service

Before installing the Cluster service, read all Microsoft checklists for installing server clusters to help you avoid future problems in planning and installation.

Note: During installation of Cluster service on the first node, vary off all other nodes participating in the cluster before you start Windows.

In the Server clusters information, any references to a shared SCSI or Fibre Channel device refers to the virtual Fibre Channel implementation used to access the shared network server storage spaces.

To install and run Windows Cluster service, complete the following tasks:

1. Install Windows Cluster service on the Integrated xSeries server
 - “Install Windows Cluster service on a new integrated Windows server”
 - “Install Windows Cluster service on an existing server” on page 55
2. “Install Windows Cluster service on Windows” on page 57

Install Windows Cluster service on a new integrated Windows server

The easiest way to install and configure the Windows Cluster server is to do so when you first configure an integrated server. Use the Install Windows server (INSWNTSVR) command with the following parameters that specify the cluster configuration information:

- Cluster name (CLU) parameter
- Cluster configuration (CLUCFG) parameter

For more information about installing the integrated server, see “Install Windows 2000 Server or Windows Server 2003” on page 43.

After you run the INSWNTSVR command (and the integrated Windows server install completes) and before you install the Windows Clustering service on the Windows side, you must perform additional configuration steps on the integrated server console. For more information, see “Prepare Windows before installing Windows Cluster service” on page 55.

Cluster name:

The Cluster name (CLU) parameter provides the name that the cluster will be known by. This is used by administrators to connect to the cluster and represents the group of independent network server nodes which will work together as a single system. The name entered for the cluster name is also used as the name of the network server storage space that is created and will serve as the quorum resource for the cluster.

Cluster configuration:

The Cluster configuration parameter (CLUCFG) is used to define the cluster and configure the quorum resource network server storage space. Additionally, this information is used to validate that any secondary nodes have the correct OS/400 configuration necessary to create the virtual cluster connections for the shared storage devices and the virtual Ethernet port that will be used for the private clustering interconnect. The cluster configuration value of *CLU will retrieve the cluster configuration from the existing quorum resource network server storage space specified on the CLU parameter,

Note: The clustering connection port requires configuration of a matching virtual Ethernet port. For more information about configuring a virtual Ethernet port, see “Configure virtual Ethernet networks” on page 65.

Install Windows Cluster service on an existing server

You can install Windows Cluster service on an existing Windows 2000 Advanced Server or a Windows Server 2003 Enterprise Edition server that runs on a supported file server resource with V5R2 (or later) Integration for Windows Server software.

If you installed the server before V5R2, ensure that the server's licensed program level is synchronized with OS/400. See "Upgrade the integrated Windows server side of the IBM iSeries Integration for Windows Server licensed program" on page 50. This ensures the availability of all server functions required to install the Windows Cluster service.

To install Windows Cluster service on an existing server, perform the following tasks:

- Create a storage space (quorum resource)
- Configure the virtual Ethernet connection port
- Link the quorum resource drive to the network server description

After you complete the steps above and before you install the Windows Clustering service on the integrated Windows server side, you must perform some additional configuration steps on the integrated Windows server console. For more information, see "Prepare Windows before installing Windows Cluster service."

Create a storage space (quorum resource):

The first step is to create a storage space to use as the quorum resource. To create a storage space, use the Create NWS Storage space (CRTNWSSTG) CL command and specify the special format *NTFSQR.

The name of the network server storage space should match the name of the cluster you are creating. The recommended size is 550 MB or larger. The command prompts for the following cluster information, which you need to provide:

- Cluster domain name
- virtual Ethernet connection port
- IP Address for the Windows cluster
- Subnet mask for the Windows cluster

Configure the virtual Ethernet connection port:

The next step is to configure the virtual Ethernet connection port that you want to use for the private cluster communication. See "Configure virtual Ethernet networks" on page 65. The virtual Ethernet port that you use must match the connection port you specify with the quorum resource network server storage space.

Link the quorum resource drive to the network server description:

Link the quorum resource storage space to the network server by using the Add Server Storage Link (ADDNWSSTGL) command, using ACCESS(*SHRUPD), DYNAMIC(*YES) and DRVSEQNBR(*QR).

Note: During installation of Cluster service on the first node, all other nodes must be varied off before starting the integrated server. Additional shared storage devices can be created and linked at this time. All shared storage spaces must be *NTFS and linked with ACCESS(*SHRUPD).

Prepare Windows before installing Windows Cluster service

After you install the integrated server, you need to prepare the server to install the Windows Cluster service.

To prepare Windows before you install the Windows Cluster service, perform the following tasks:

1. Format the quorum resource
2. Configure the private network adapter

When you complete these steps, Windows is ready for you to install the Windows Cluster service. For more information, see “Install Windows Cluster service on Windows” on page 57.

Format the quorum resource:

The first step to prepare Windows for a Windows Cluster installation is to format the quorum resource as NTFS. Formatting the quorum resource is not only required to install the Windows Cluster service, it is also the first step when installing the first node of a cluster. For more information, see “Format integrated server disk drives” on page 89.

The quorum resource appears as an unformatted disk drive typically with a logical device driver letter of E. The quorum resource’s location is bus number 1, target identifier 0 and Logical Unit Number (LUN) 0. You should format the volume and label it using the same name as the cluster, which is also the name of the quorum resource network server storage space name. Also format any other shared storage spaces at this time. It is also recommended that you assign a fixed drive letter to the quorum resource drive and any other shared storage drives.

Note: The drive letter assigned to all storage spaces on the shared storage bus must be the same on all nodes of the cluster.

Configure the private network adapter:

Next, configure the private network adapter for use by the Windows Cluster service by completing the following steps on the first node in your cluster:

1. On the integrated Windows server console, right-click **My Network Places** and select **Properties**.
2. Right-click the **Local Area Connection 2** icon.

Note: Which network adapter is private and which is public depends on how you configured the server. This information assumes the following:

- The first network adapter (Local Area Connection) is connected to the public network by using a physical LAN adapter under the Integrated Windows server
- The second network adapter (Local Area Connection 2) is the virtual Ethernet adapter configured as the cluster configuration connection port that you want to use as the private cluster network
- The third network adapter (Local Area Connection 3) is the private virtual Ethernet point-to-point connection to OS/400 and should not be enabled for any clustering use

The number and order of network adapters may not be the same, depending on the physical and virtual configuration of the server and the network.

3. Click **Status** to display the **Local Area Connection 2 Status** window, which shows the connection status, as well as the speed of connection.
4. In the **Local Area Connection 2 Status** window, click **Properties**.
5. In the **Properties** dialog box, make sure that the contents of the **Connect using** field contains IBM iSeries Virtual Ethernet x, where x matches the *VRTETHx that you specified for the cluster configuration connection port.
6. Click **Close**, then click **Close** again.

For clarity, you should rename your Local Area Network Icons. For example, you might want to change the name of Local Area Connection 2 to something like Private Cluster Connection.

Install Windows Cluster service on Windows

The actual installation of the Windows Cluster service depends on the version of Windows installed during the Windows environment for iSeries installation. For the most part, refer to the Microsoft documentation for instructions on installing the Windows Cluster service. This information highlights specific steps required to install the Windows Cluster service on an Integrated Windows server.

- “Install Windows Cluster service on Windows 2000 Server”
- “Install Windows Cluster service on Windows Server 2003” on page 58

Note: Make sure that Windows Cluster service is installed and running on one server before starting Windows on another server in the cluster. Starting the operating system on multiple servers before the Windows Cluster service is running on one server can damage the cluster storage. After you configure the first server, you can simultaneously install the remaining servers.

Install Windows Cluster service on Windows 2000 Server: Use the Cluster Service Configuration wizard to install the Windows Cluster service. You supply the wizard with all the initial cluster configuration information.

To install Windows Cluster service, perform the following tasks:

1. Start the Cluster Service Configuration wizard
2. Use the wizard to configure the cluster service

Start the Cluster Service Configuration wizard:

To start the Cluster Service Configuration wizard, complete the following steps:

1. From the Windows **Start** menu, click **Settings**, then click **Control Panel**.
2. In the **Control Panel** window, double-click **Add/Remove Programs**.
3. In the **Add/Remove Programs** window, click **Add/Remove Windows Components**.
4. In the **Windows Components Wizard** dialog box, select **Cluster Service**, then click **Next**.

Configure the Windows Cluster service:

After you have started the Cluster Service Configuration wizard, it prompts you through the installation of the Windows Cluster service. You supply the wizard with all the initial cluster configuration information, which is required in order to create the cluster.

When prompted for the quorum resource, select the drive that you formatted and labeled. Although this drive is typically the E: drive for a new installation, the Disk Manager may have fixed another letter to the drive.

Network connections require special consideration:

Note: The order in which the Cluster Service Configuration wizard presents the network configuration information may vary.

- Uncheck the box **Enable this network for cluster use** for the IBM iSeries virtual Ethernet Point-to-Point (typically Local Area Connection 3)
- Select the option **Internal cluster communications only** for the IBM iSeries virtual Ethernet xwhere x matches the *VRTETHx specified on the cluster configuration connection port (typically Local Area Connection 2)
- Configure the remaining network connections according to their need

Specify the IBM iSeries virtual Ethernet xadapter (typically Local Area Connection 2) as the primary network for the Internal Cluster Communication.

Install Windows Cluster service on Windows Server 2003: Use the Cluster Administrator to install Windows Cluster service on Windows Server 2003 and to join an existing cluster. Both installing the cluster service and joining an existing cluster require you to open the Cluster Administrator. Open the **Cluster Administrator** from the Windows **Start** menu by selecting **All Programs**, then **Administrative Tools**, then **Cluster Administrator**.

Install and configure the Windows Cluster service by completing the following steps.

1. Open the **Cluster Administrator**.
2. In the **Open Connection to Cluster** dialog box that appears, in **Action**, select **Create new cluster**.
3. Click **OK** to display the New Server Cluster wizard, which prompts you through the installation of the Cluster service for the first node.
4. Click **Next**.
5. Type the **Domain** (defaulted) and **Cluster name**.
6. Type the **Computer name** (defaulted).
7. Type the **IP Address** for the cluster management.
8. Type the **Cluster Service Account User name**, **Password** and **Domain**.
9. Verify the **Proposed Cluster Configuration**.

Join an existing cluster:

Join an existing cluster by completing the following steps:

1. Open the **Cluster Administrator**.
2. In the **Open Connection to Cluster** dialog box, in **Action**, select **Add nodes to cluster**.
3. Then in **Cluster or server name**, either type the name of an existing cluster, select a name from the list, or click **Browse** to search for an available cluster.
4. Click **OK** to display the Add Server Cluster wizard.
5. Select one or more computer names to add to the cluster, then click **Add**.
6. Enter the domain account password for the cluster service.
7. After Cluster service has finished installing, use the Cluster Administrator to locate and select the cluster that you just created.
8. Expand **Cluster Configuration, Network Interfaces**. This will open in the right panel with a list of all **Local Area Connections**.
9. Type the network name (Local Area Connection x) for the virtual IBM iSeries virtual Ethernet x where x matches the *VRTETHx specified on the Cluster configuration connection port. You need to identify this network later, so remember the name.
10. Identify the network name (Local Area Connection x) for the virtual IBM iSeries virtual Ethernet Point-to-Point. You need to identify this network later, so remember the name.
11. In the **Cluster Administrator** window, expand **Cluster Configuration, Networks**.
12. Right-click the network name (Local Area Connection x) for the virtual IBM iSeries virtual Ethernet x and select **Properties**.
13. Select the option **Internal cluster communications only** for this network.
14. Right-click the network name (Local Area Connection x) for the virtual IBM iSeries virtual Ethernet Point-to-Point and select **Properties**.
15. Uncheck the box **Enable this network for cluster use** for this network.

Configure the remaining network connections according to their need.

Enabling QNTC access to Windows Server 2003 with Active Directory

By default, file shares on a Windows Server 2003 server with Active Directory installed (for example, a domain controller) cannot be accessed via the OS/400 Network Client (QNTC) file system. This affects OS/400 commands such as Save (SAV), Restore (RST) and Work Link (WRKLNK). For example, the OS/400 SAV command cannot do a file-level backup of files on a Windows Server 2003 domain controller with the default settings.

Circumvention

QNTC is an OS/400 file system that utilizes the Server Message Block (SMB) protocol. By default, a Windows Server 2003 server installed with Active Directory requires digital signatures of SMB packets for increased security. Since QNTC does not yet perform this task, attempts at authenticating to the server using SMB are denied, making QNTC operations fail. If you are unable to save Windows Server 2003 data using the SAV command through QNTC file system, or are unable to view a list of shares defined using the WRKLNK command through QNTC, then you may need to perform the following steps on the Windows Server 2003 server to disable the requirement for digitally signed SMB communications.

1. Start Registry Editor (Regedt32.exe).
2. Locate and select the following key in the registry:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Service\lanmanserver\parameters
3. Double-click the RequireSecuritySignature value, type 0 in the Value data box, and then click OK.
4. Double-click the EnableSecuritySignature value, type 0 in the Value data box, and then click OK.
5. Quit Registry Editor.
6. Reboot the server for the Registry changes to take effect.

Note: You can edit the registry by using Registry Editor (Regedit.exe or Regedt32.exe). However, if you use Registry Editor incorrectly, you can cause serious problems that may require you to reinstall your operating system. Microsoft does not guarantee that problems that you cause by using Registry Editor incorrectly can be resolved. Use Registry Editor at your own risk. Before you change the registry, make sure to back up the registry, and make sure that you understand how to restore the registry if a problem occurs. For additional information about backing up and restoring the registry, click the following article

number to view the article in the Microsoft Knowledge Base: 322756  . HOW TO: Back Up, Edit, and Restore the Registry in Windows XP and Windows Server 2003.

Install the ATI Radeon 7000M video device drivers for Windows 2000 on the 2892-002 or 4812-001 Integrated xSeries Server

The 2892-002 and 4812-001 Integrated xSeries Server include an ATI Radeon 7000M video chip. The required drivers are not included in the Microsoft Windows 2000 Server distribution CD. You will need to install the ATI video display driver on the integrated Windows server to take full advantage of the ATI video chip's capabilities.

Your system must have DirectX 8.1, or later, installed before you can install the ATI video drivers.

To install the ATI video driver for Windows 2000, follow these steps:

1. Install DirectX version 8.1 or later. Windows 2000 ships with DirectX 7.0 but DirectX version 8.1 or later is required for the ATI video drivers and must be installed prior to installing the ATI video drivers. Microsoft maintains a website for DirectX information and downloads. Visit <http://www.microsoft.com/directx>.
2. Install the ATI video driver:
 - a. Close all programs.
 - b. Click the **Start** button and select the **Run** menu item.
 - c. Click the **Browse** button.
 - d. Browse to the %SystemDrive%\WSV directory where atidrivr.exe is located.

- e. Select `atidrvr.exe` and click OK to run the program.
 - f. Follow the installation instructions on the screen.
3. Optionally, the Advanced ATI Control Panel tabs can be installed.
 - a. Close all programs.
 - b. Click the **Start** button and select the **Run** menu item.
 - c. Click the **Browse** button.
 - d. Browse to the `%SystemDrive%\WSV` directory where `aticp.exe` is located.
 - e. Select `aticp.exe` and click OK to run the program.
 - f. Follow the installation instructions on the screen.

| **Adjust hardware acceleration for Windows Server 2003 on the 2892-002 or 4812-001 Integrated xSeries Server**

| If you are installing Windows Server 2003 on a 2892-002 or 4812-001 IXS, some additional setup is required for optimal video performance. To adjust performance, do the following:

- | 1. From the Windows **Start** menu, click **Settings -> Control Panel -> Display**.
- | 2. On the **Display Properties** panel, click the **Settings** tab.
- | 3. Click **Advanced**.
- | 4. Click the **Troubleshoot** tab.
- | 5. Adjust the **Hardware Acceleration** slider as desired.
- | 6. Click **Apply**.
- | 7. Click **OK**.
- | 8. Click **OK** again to accept the change.

Respond to error messages during installation

The integrated Windows server phase of the installation flags missing information that you did not provide during the OS/400 phase of the installation, then allows you to supply the information. This section contains some examples of those error messages and how to respond.

Duplicate name on network

If the Integrated xSeries Server has 2 LAN adapters that are connected to the same network, the installation program will indicate that the computer name already exists on the network. This is a limitation of the integrated Windows server installation process. To work around this limitation, do the following:

- Disconnect one of the Integrated xSeries Server LAN adapter cables from the network.
- On the integrated Windows server console, retype the same computer name.
- Press **OK** to continue with the installation.

After the installation is complete, you can reconnect the disconnected LAN adapter cable.

Error (Installing Server)

You may not have specified a value in the To workgroup or To domain fields of the Install Windows Server display on OS/400. If not, then you will see the following error message:

Error (Installing Server)

A setup parameter specified by your system administrator or computer manufacturer is missing or invalid. Setup must therefore ask you to provide this information now.

Once you have furnished the required information, unattended Setup operation will continue.

You may wish to inform your system administrator or computer manufacturer that the "JoinWorkgroup" value is missing or invalid.

Click **OK**.

The installation program then prompts you to make the computer a member of a workgroup or domain.

Set an integrated Windows server to automatically vary on with TCP/IP

You can set an integrated server to automatically vary on when you start TCP/IP. However, if multiple integrated servers use a single file server resource, configure only one of them to autostart. Only one network server can use the file server resource at a time. Configuration of multiple TCP/IP interfaces to autostart for network servers that share the same resource can cause unpredictable results.

To have an integrated server automatically vary on when you start TCP/IP, follow these steps:

1. On the OS/400 command line, enter the Configure TCP/IP (CFGTCP) command.
2. Choose Option 1 Work with TCP/IP interfaces and press Enter.
3. Specify 2 (change) in the Option field next to the interface for the private LAN (internal token-ring or virtual Ethernet point-to-point) line description for the server, and press Enter.

Note: The private LAN line description has a name that consists of the network server description (NWSD) name followed by '00' for the Internal token-ring or by 'PP' for the virtual Ethernet point-to-point LAN. For example, if the NWSD name is MYSVR, then the private LAN line description is MYSVR00.

4. Change the Autostart parameter value to *YES and press Enter. The integrated server automatically varies on when you start TCP/IP.

Note: Beginning in V5R1, TCP/IP can be automatically started by the system at IPL by changing the system's IPL attributes. A startup procedure is no longer necessary. Any TCP interfaces with the Autostart parameter set to *YES will be started along with TCP/IP at IPL.

Note: Be aware that an IP address entered at the integrated console for the private LAN overrides the value set in the NWSD for the TCPPRTCFG parameters *INTERNAL or *VRTETHPTP port. However, operations such as SBMNWSCMD use the value set in the NWSD to find the server. Both values must be consistent.

Code fixes

IBM iSeries Integration for Windows Server code fixes provide the most current and error-free code possible without requiring you to wait for the next software release. They update the iSeries Integration code that enables Microsoft Windows server to run on the IXS and are separate from the service packs for Windows itself, which you must get from Microsoft.

Read about the "Types of code fixes" on page 62.

The process of installing code fixes on your integrated servers is called synchronization. When you synchronize an integrated server, the integration software ensures that the Windows integration software on the integrated server is at the same service pack and release level as the OS/400 integration software. The level of code on the Windows side is dependant on the level of code on the OS/400 side. This is a change from past releases, where you could manually install and remove individual code fixes regardless what the level of code was on the OS/400 side.

When you use the integration software to synchronize an integrated server, there are potentially four actions which you may cause to occur 'under the covers'.

1. If OS/400 has been upgraded to a new release, for example, from V5R2 to V5R3, the software for the new release will replace that of the old release.

2. If a new IBM iSeries Integration for Windows Server service pack has been installed on OS/400, it will be copied over to the integrated server.
3. If an IBM iSeries Integration for Windows Server service pack has been removed from OS/400, it will be removed from the integrated server as well, and replaced with the code currently existing in OS/400.
4. If the OS/400 integration code and integrated server code are at the same level, the synchronization operation can still be performed. This allows for recovery of a deleted or damaged file on the integrated server.

In all cases the integrated server will be brought to the same level of software which exists in OS/400.



There are three ways to perform a synchronization

- “Synchronize the integration software level using the integrated Windows server console.”
- “Synchronize the integration software level using iSeries Navigator” on page 63.
- “Synchronize the integration software level using a remote command” on page 63.

If you have problems performing a synchronization, see “IBM iSeries Integration for Windows Server snap-in program” on page 140.

Types of code fixes

There are three types of code fixes

1. Code fixes applied to the OS/400 integration code, referred to as **regular program temporary fixes (PTFs)**.
 - To apply them all you have to do is install them to OS/400.
 - These code fixes are available from IBM Support or from the internet at www.iseries.ibm.com/windowsintegration/ (take service information link on the left navigation bar)  .
2. Code fixes which are copied to the integrated server’s drives and run on the integrated server, referred to as **service pack PTFs**.
 - The IBM iSeries Integration for Windows Server licensed program has an integrated server part which is copied over from the OS/400 side. When you apply an OS/400 Cumulative PTF package, it may contain a Windows Integration service pack which can be applied to the integrated server. You do this by synchronizing the integrated server.
 - These code fixes are also available from IBM Support or from the internet at www.iseries.ibm.com/windowsintegration/ (take the service information link on the left navigation bar)  .
3. Code fixes applied to Microsoft Windows server itself, referred to as **service packs**.
 - These come from Microsoft. You can download them from their Windows Update web site.
 - Do not apply any code fixes from Microsoft which might change portions of Windows server used by IBM iSeries Integration for Windows Server. For example, do not download any SCSI storage device drivers or LAN device drivers from Windows Update.
 - Other areas are generally safe, for example, USB device drivers may be downloaded from Windows Update at your own risk.

Synchronize the integration software level using the integrated Windows server console

To use the iSeries Integration for Windows Server snap-in to synchronize the software level, you must be a Windows system administrator. Before beginning the installation, end any applications that are running and make sure that no users are logged on to the integrated server. If you fail to do this, you risk data loss because the integrated server may require a restart after completing the installation.

1. Click **Start -> Programs -> IBM iSeries -> Integration for Windows Server**.
2. Click the integrated server's name, then **Software Level**.
3. The software level of the OS/400 integration software and of the Windows integration software is shown. Click **Synchronize** to bring the Windows integration software to the same level as the OS/400 integration software.
4. If the installation is performed successfully a confirmation message appears.

Note: If you log on as an administrator to the integrated Windows server console and there is a software level mismatch, you will automatically be asked to synchronize the software.

Synchronize the integration software level using iSeries Navigator

1. In iSeries Navigator, click **Network -> Windows Administration -> Integrated xSeries Servers**.
2. Right click the integrated server you want to synchronize and select **Synchronize iSeries Integration Software**. (If the OS/400 server you are accessing is not a V5R3 server, you will be presented with a list of legacy options, allowing you to install and uninstall service packs individually, or to perform a release update only.)
3. Click **Synchronize** to confirm the action.
4. You will receive a message indicating the synchronization is in progress followed by a completion message indicating that a reboot is about to take place. You will not be asked whether to reboot now or later.

To find out which levels of software are installed on OS/400 and the integrated server follow this procedure:

1. In iSeries Navigator, click **Network -> Windows Administration -> Integrated xSeries Servers**.
2. Right click the integrated server you are interested in and select **Properties**.
3. Click on the **Software** tab. The software levels will be displayed there.

Synchronize the integration software level using a remote command

Entering the command `lvlsync` at an integrated Windows server console command prompt will cause the integrated server to synchronize. The principle utility of this command-line program is that it allows you to synchronize an integrated server by remotely submitting a command. This functionality would be useful if you, for example, wanted to write a CL program to periodically synchronize your integrated servers. To learn more about remotely submitted commands, see "Run integrated Windows server commands remotely" on page 79.

Here is a simple procedure to remotely synchronize an integrated server by remotely submitting the `lvlsync` command from the OS/400 console.

1. At the OS/400 character-based interface, type `SBMNWSCMD` and press **F4**.
2. Enter `lvlsync` in the **Command** field and press **Tab**.
3. Enter the NWSD name of your integrated server in the **Server** field and press enter.

The `lvlsync` program allowed optional parameters in the past. These parameters no longer function, although their presence in the command will not affect its functionality.

`lvlsync` returns the following error codes:

lvlsync error codes

Error Code	Error
0	No errors
01	Must be an administrator to run <code>lvlsync</code>

Error Code	Error
02	Release level on integrated Windows server higher than on OS/400
03	Service pack level on integrated server higher than on OS/400
04	Cannot install release from OS/400 - language files not on OS/400
05	Syntax not valid
06	Cannot access service pack information on OS/400
07	Cannot map network drive
08	Cannot access service pack information in registry
09	Cannot open qvnacfg.txt file
10	No service pack installed on OS/400
11	NWSD not found
13	NWSD not active
20	No service pack available on OS/400
21	Cannot start InstallShield application
31	Unexpected error while starting lvlsync
44	Unexpected error during lvlsync

Note: The error message NTA0218 is a diagnostic (*DIAG) message for syntax, authorization, and NWSD not found errors.

Chapter 6. Network integrated servers

This section contains procedures to help you create and understand the three types of networks described in “Networking concepts” on page 10.

- “Configure virtual Ethernet networks”
- “Configure Inter-LPAR virtual Ethernet networks” on page 66
- “Explore point-to-point virtual Ethernet networks” on page 67
- “External networks” on page 68
- “Remove network adapters” on page 70

Configure virtual Ethernet networks

This section will describe how to configure a virtual Ethernet network between integrated servers. (Note that if you are installing an integrated server from scratch, the installation command (INSWNTSVR) can configure virtual Ethernet networks for you.) For information on how to extend virtual Ethernet networks to other iSeries logical partitions, see “Configure Inter-LPAR virtual Ethernet networks” on page 66. The procedure consists of the following basic steps

1. First you configure an Ethernet line description for the integrated server.
 - a. On OS/400, enter the Create Line Description (Ethernet) command, CRTLINETH, and press Enter.
 - b. In the Line Description field, enter the name of your network server description (NWSD), followed by V and a number (0 through 9) that corresponds to the virtual Ethernet network that you will use (for example, NWSDnameV0).
 - c. In the Resource Name field, enter *NWSD.
 - d. In the Network server description field, enter the name of the NWSD that will use the adapter.
 - e. Press Enter twice.
 - f. In the Port Number field, enter the port number that corresponds to the virtual Ethernet network that you will use. Virtual Ethernet network port values are *VRTETH0 through *VRTETH9.
 - g. In the Local Adapter Address field, *ADPT is required.
 - h. The Line Speed must be 1G and Duplex must be *FULL.
 - i. Press F10 to see more parameters. The Max frame size should be 8996 for virtual Ethernet.
 - j. (Optional) Page down to the Text 'description' field and write a brief description
 - k. (Optional) Page down to the Link Speed field and specify *MAX. Press enter.
 - l. Press Enter to create the Ethernet line description.
 - m. If you want this integrated server to be connected to more than virtual Ethernet network, repeat all of the above steps to create a line description for each network, using different port values in step 1f.
2. Then, you change the NWSD of the integrated server to use the Ethernet line description(s).
 - a. Enter the OS/400 command CHGNWSD and press Enter.
 - b. In the Network server description field, enter the name of your NWSD and press F4.
 - c. Page down to TCP/IP port configuration.
 - d. In the blank to the right of the words + for more values, type a + and press Enter.
 - e. In the Port field, enter the port number. (For example, *VRTETH0).
 - f. In the Internet address field, enter the IP address that the integrated server will use.
 - g. In the Subnet mask field, enter the subnet mask that the integrated server will use.
 - h. In the Max Transmission Unit field, enter 8996.
 - i. Press Enter.

3. Repeat the procedure for all the integrated servers you want to connect to the network, specifying the same virtual Ethernet port for each one.
4. Restart the integrated servers. A virtual Ethernet adapter device driver will be automatically installed and set to the Windows TCP/IP address that has been specified for it in the NWSD. However, an IP address entered at the integrated server console overrides the values that are set in the NWSD.
5. Test to see that the virtual Ethernet network is functioning, for example by pinging from one server to the IP addresses you specified for the other servers.

Configure Inter-LPAR virtual Ethernet networks

Inter-LPAR networks with the Hardware Management Console

If you want an integrated server to communicate with other logical partitions, or with integrated servers controlled by other OS/400 partitions, you need to configure one or more inter-LPAR networks. Inter-LPAR networks are configured differently on iSeries systems with the Hardware Management Console (HMC) than on other systems. In an iSeries HMC system, inter-LPAR connections exist between partitions or integrated servers using the same VLAN ID. Participating integrated servers do not support VLAN IDs directly. Instead, each participating integrated server needs an Ethernet line description that associates a port value such as *VRTETH1 with a virtual adapter having a VLAN ID. The configuration procedure consists of the following steps:

1. Use the Hardware Management Console (HMC) to create a virtual Ethernet adapter for each partition and each integrated server that will participate in the inter-LPAR network. See Logical Partitions with an HMC for more information. For each virtual adapter that will connect an integrated server or OS/400 partition to the inter-LPAR network, specify a consistent Port virtual LAN ID and uncheck **IEEE 802.1Q compatible adapter**.
2. In the OS/400 partition that controls the participating integrated server, use the WRKHDWRSC *CMN command to see the OS/400 view of the virtual adapter or adapters created in step 1. Note the port names having hardware type 268C. If there is more than one, move the cursor to the space in front of the resource name and press 7 to display resource details.
3. Create a line description as in step 1 of the “Configure virtual Ethernet networks” on page 65 article, except in the ASSOCPORT field, specify the name of the appropriate 268C resource. In the Port field, specify a value such as *VRTETH1. Alternatively, you can add ASSOCPORT to an existing line description, if that’s what your network topology calls for.
4. Continue with step 2 of the “Configure virtual Ethernet networks” on page 65 article (if you created a line description), step 3 (in all OS/400 partitions that control a participating integrated server), and step 4 (if you created a line description).
5. For a partition to fully participate, you will need to appropriately configure the protocol(s) within the partition. In each OS/400 partition, create an Ethernet line description on the appropriate dedicated 268C port resource. Configure an appropriate unique IP address in each partition that will participate in TCP/IP communications.
6. Test to see if the inter-LPAR network is functioning, for example by pinging between connected integrated servers and partitions.

Inter-LPAR networks without the Hardware Management Console

In a system other than an iSeries HMC system, Inter-LPAR connections exist between partitions using the same network number, and integrated servers are connected only if their controlling OS/400 partitions are connected. Network numbers 0-9 are pertinent to integrated servers. For example, if an OS/400 partition is configured for inter-LPAR connections on networks 1 and 5, then integrated servers controlled by that partition can participate in inter-LPAR communication on ports *VRTETH1 and *VRTETH5. The configuration procedure consists of the following steps:

1. Configure the network number that you want each partition to connect to. Refer to Logical Partition concepts and iSeries Navigator online help information. Keep in mind that integrated servers are connected only if their controlling OS/400 partitions are connected.

2. (The steps referred to are all located in the “Configure virtual Ethernet networks” on page 65 article.) Create a line description as in step 1, if one has not already been created for the port of interest (*VRTETH0 through *VRTETH9). Do not use the ASSOCPORT field in the line description as this field is for iSeries HMC systems only.
3. Continue with step 2 (if you created a line description), step 3 (in all OS/400 partitions that control a participating integrated server), and step 4 (if you created a line description).
4. If you want a partition to fully participate, you will need to appropriately configure the protocol(s) within the partition. In each OS/400 partition that you want to participate, use the WRKHDWRSC *CMN command to find the name of the appropriate port of hardware type 268C, which was automatically created in step 1 a. Then create an Ethernet line description on the 268C port resource. Configure an appropriate unique IP address in each partition that will participate in TCP/IP communications.
5. Test to see if the inter-LPAR network is functioning, for example by pinging between connected integrated servers and partitions.

Explore point-to-point virtual Ethernet networks

Each integrated server has a point-to-point virtual Ethernet network connection with the iSeries, which allows the iSeries to control the integrated server. Here you can learn how to view or change these connections, although they are automatically configured during installation.

View point-to-point Ethernet connections from OS/400

Point-to-point Ethernet connections in OS/400 are composed of a line description and an entry in an integrated server’s NWSD.

1. To view the line description issue the command WRKCFGSTS *NWS from the OS/400 character-based interface.
2. Find the cascade of entries corresponding to your integrated server. One of the entries in the Line Description column will have the same name as your NWSD and end with the characters PP. Enter 8 to its left and press enter.
3. Now you are in the Work with Line Descriptions menu. Enter a 5 to the left of your line description and press enter to display its information.
4. Press **F3** until you return to the base menu.
5. Now issue the command CFGTCP and select option 1, **Work with TCP/IP interfaces**.
6. One entry in the Line Description column should have the same name as your NWSD and end with the letters PP.
7. Option 5 will display the TCP/IP Interface information, while options 9 and 10 will allow you to enable and disable it. Note the internet address as we will use it later.
8. Now we will take a quick look at the entry in the integrated server’s NWSD. Issue the command WRKNWSD. Find your integrated server’s NWSD and enter 5 to display it. Press enter to page through the NWSD attributes.
9. One of the screens will be titled **Attached lines** and will display Port number *VRTETHPTP and the name of the line description that the network is using.
10. Back in the **Work with Network Server Descriptions** menu you can use option 2 to change this information.

View point-to-point Ethernet connections from the integrated Windows server console

1. At the console of your integrated server, click **Start** → **Settings** → **Control Panel**. Then select **Network and Dial-up Connections**.
2. One of the icons will be named **virtual Ethernet point-to-point**. Double-click it.
3. Click **Properties** in the dialog box which appears.
4. Double-click **Internet Protocol (TCP/IP)** in the next dialog box.

5. In this final dialog box you should see the IP address associated with the integrated server side of the point-to-point virtual Ethernet connection. It should be the OS/400's IP address augmented by one so as to be even instead of odd.
6. Close all of the windows that you opened, click **Start** → **Run**, and enter the command `cmd`. Press enter. This will start an instance of the Windows command prompt.
7. At the `C:\>` command prompt which appears, enter the command `ping` followed by the OS/400 IP address which you remember from the last step. For example `ping 192.168.3.1`. The command should return `Reply from`. That's good. The ping command sends a packet of data to a certain internet address and times how long it takes to make a round trip.
8. (optional) Return to the OS/400 character-based interface and enter the command `call qcml`. (This will increase the display space so that you can see the results of your commands.) Use the OS/400 command to ping the integrated server. For example, `ping '192.168.3.2'`. Congratulations! If all went correctly we have proved that you have a properly functioning point-to-point virtual Ethernet network.

External networks

You can install a new network adapter card in an open PCI slot. If you do this, you need to configure the new adapter on the integrated Windows server. Older models of Integrated Netfinity Server allow you to share the adapter between OS/400 and an integrated server. The Integrated xSeries Server, models 2890, 2892, and 4812, and the Integrated xSeries Adapter, model 2689, do not allow an adapter to be shared between OS/400 and an integrated server.

Refer to the [Install iSeries Features](#) topic for information about installing a new network adapter card. Choose your model of iSeries and find the instructions labeled **Install PCI Card and Integrated xSeries Adapter Card**.

Note: If you have an older 6617 model Integrated xSeries Server that has three available PCI slots, you can share only the first two with OS/400 when this 6617 is not installed on a 50xx Migration Tower.

To set up a new network adapter perform these tasks:

1. "Create line descriptions for external network adapters"
2. If you are configuring an external host LAN adapter, perform this step "Add a TCP interface for a new shared network adapter" on page 69.
3. "Install network adapter device drivers and add adapter address information to an integrated Windows server" on page 69

To create a virtual Ethernet connection, see "Configure virtual Ethernet networks" on page 65.

To remove a network adapter, see "Remove network adapters" on page 70.

Create line descriptions for external network adapters

After physically installing the network adapter, creating a line description is the first step in configuring a network adapter.

To create a line description, follow these steps:

1. On OS/400, type the appropriate command:
 - For token-ring ports, type `CRTLINTRN` and press Enter.
 - For Ethernet ports, type `CRTLINETH` and press Enter.
2. In the Line Description field, enter the name of your network server description (NWSD), followed by a 0, followed by the port number.
 - **Example:** For an adapter in port 1 that you want to share between OS/400 and an NWSD called NTSVR, name the line description `NTSVR01`.
3. In the Resource Name field, enter `*NWSD`.

4. In the Network server description field, enter the name of the NWSD that will use the adapter.
5. Enter Associated port resource name, if required to access LPAR network on select iSeries platforms.
6. In the Port Number field, enter the port number where you have plugged in the card.
7. In the Local Adapter Address field, enter a unique address for the adapter. *ADPT is not valid.
Note: Make note of this address. You will need it in a later step.
8. In the Line Speed field, enter the speed of the line that you have plugged into the adapter.
9. (Optional) Page down to the Link Speed field.
10. In the Link Speed field, enter the same value that you entered for the Line Speed.
11. (Optional) Page down to the Text 'description' field and type a brief description of the line description.
12. Press Enter.

If you are configuring an external host LAN network adapter, your next step is “Add a TCP interface for a new shared network adapter.”

Otherwise, skip directly to “Install network adapter device drivers and add adapter address information to an integrated Windows server.”

Add a TCP interface for a new shared network adapter

You can install a new network adapter card to share between OS/400 and an integrated Windows server. External host LAN is available only for the older hardware named Integrated Netfinity Servers. To do this, you must add a TCP interface for the port in which you installed the card. Before doing this, you must have created line descriptions for the port. See “Create line descriptions for external network adapters” on page 68.

To add a TCP interface, follow these steps:

1. On OS/400 enter the command ADDTCPIFC and press Enter.
2. In the Internet address field, enter the OS/400 Internet address for the port.
3. In the Line description field, enter the name of the line description for the port. Provided you followed the recommended naming conventions, this will be the name of your network server description (NWSD), followed by a 0, followed by the port number.
 - **Example:** For an adapter in port one that you want to share between OS/400 and an NWSD called NTSVR, the line description name is NTSVR01.
4. In the Subnet mask field, enter the OS/400 subnet mask for the port and press Enter.

Note: You can use a TCP route for the new port that is different from the one OS/400 uses. To do this, set a TCP route with the Add TCP/IP Route (ADDTCPRTE) command. For more information about

TCP routes, see the TCP/IP Configuration and Reference .

Install network adapter device drivers and add adapter address information to an integrated Windows server

Here you can install adapter device drivers and add adapter address information for the new adapters on an integrated Windows server.

The adapters and device drivers under Windows 2000 Server and Windows Server 2003 support Plug-n-Play. Once an adapter has been physically installed, reboot the integrated server by varying it on for the adapters to become available. Remember to configure the IP address for every adapter (connection).

If you are upgrading your Integrated xSeries Server from Windows NT 4.0 to Windows 2000 Server, remove the old adapter before adding the new one. See “Remove network adapters” on page 70.

Windows 2000 Server or Windows Server 2003 recognizes the new adapter. To configure the IP address for a given adapter:

1. Right-click on **My Network Places**; then click on **Properties** from the pull-down menu.
2. Double-click on the correct adapter (Local Area Connection) to configure the IP address.
3. Click the **Properties** button.
4. Select the **Internet Protocol (TCP/IP)**, then click the **Properties** button.
5. If it is not already selected, click the **Use the following IP address** radio button.
6. In the **IP Address** field, specify the IP address.
7. In the **Subnet Mask** field, specify the subnet mask.
8. In the **Default Gateway** field, specify the default gateway address.
9. Click **OK, OK, and Close** to complete the IP address setting.

Note: If Windows indicates that the IP address is already configured for another adapter, but you cannot find an adapter already using the address, Windows is probably aware of a previous hardware environment that used the address. To display a LAN adapter from a previous hardware environment so that you can free the IP address, see the Microsoft Knowledge Base article Q241257 Device Manager Does Not Display Devices Not Currently Present in

Windows 2000  .

If you want only the integrated server to use this network adapter, you are finished with the configuration. If you have a model of Integrated xSeries Server that supports external host LAN and want to share the new adapter with OS/400, perform these additional steps:

10. Click the **Adapters** tab.
11. Select the connection to be shared.
12. Click the **Configure** button.
13. Click the **Advanced** tab.
14. Select from the list the Network Address (Ethernet or token ring).
15. Select the correct radio button and type the Network Address that matches the iSeries Line Description and Local Administered Address field.
16. Select from the list the **Data Rate** and **Duplex** (token ring) and **External PHY** (Ethernet) and click the correct radio button. Ensure that these settings match the corresponding iSeries Line Description fields.
17. Click **OK, OK, and Close** for the settings to take effect.
18. You need to shutdown and restart for the changes to take effect.

Note: You will install the new external port at the level of the latest IBM iSeries Integration for Windows Server service pack. You do not need to reinstall the service pack after installing the port.

Remove network adapters

Before you remove a network adapter card from an integrated Windows server, you need to uninstall it. If the integrated server shares the network adapter card with OS/400 (external host LAN), you also need to uninstall it from OS/400. You also need to remove shared adapters if you are migrating to a 2890 Integrated xSeries Server, which does not support external host LAN. See “Migrate from 285x or 661x to 2890 Integrated xSeries Server hardware” on page 51.

Note: If you want to stop sharing an adapter with OS/400, but do not want to uninstall it from the integrated server, proceed directly to **Remove the network adapter device drivers from OS/400** (step 2).

To uninstall network adapters from an integrated server, follow these steps

1. **Uninstall the network adapter device drivers in Windows.**
 - a. For Windows 2000 Server or Windows Server 2003

- 1) Click on **Start**, then **Settings**, then **Control Panel**.
 - 2) Start the **Add/Remove Hardware** wizard and click **Next** on the opening panel.
 - 3) Click on **Uninstall/unplug a device**.
 - 4) On the **Choose a remove task** panel, click **Next** to take the default (Uninstall a device).
 - 5) Select the device from the list that you want to uninstall (for example, IBM PCI Token-ring adapter).
 - 6) Click **Yes** to confirm that you want to remove the adapter.
 - 7) Because Windows 2000 Server and Windows Server 2003 are Plug and Play operating systems, you must either physically remove the adapter from OS/400 or disable it before restarting the server. If you restart the integrated server with the adapter still plugged in, the operating system will detect it as new hardware and reinstall the device driver. If you want to disable the adapter rather than remove it, follow these steps:
 - a) From the **Control Panel**, select **Network and Dial-up Connections**.
 - b) Select the LAN adapter.
 - c) Right-click and select **Disable**.
 - 8) If the integrated server is the only user of the network adapter, then restart it to complete the procedure. If the integrated server shares the network adapter with OS/400, then do not restart it yet. Instead, proceed with step 2, **Remove the network adapter from OS/400**.
- b. For Windows NT 4.0:
- 1) Click on **Start**, then **Settings**, then **Control Panel**.
 - 2) Open the **Network** application.
 - 3) Click the **Adapters** tab.
 - 4) Click on the adapter that you want to remove. If you need to remove more than one adapter, repeat this procedure. If you are migrating to new Integrated xSeries Server hardware, you need to remove all but the IBM Internal LAN adapter.
 - 5) Click the **Remove** button.
 - 6) Click **Yes** to confirm that you want to remove the adapter.
 - 7) If the integrated server is the only user of the network adapter, then restart it to complete the procedure. If it shares the network adapter with OS/400, then do not restart yet. Instead, proceed with step 2, **Remove the network adapter from OS/400**.
- c. Removing an external host LAN adapter from an integrated server:
- 1) Click **Start**, **Settings**, and **Control Panel**.
 - 2) Open **Network and Dial-up Connections**.
 - 3) Double-click on any connection.
 - 4) Click on the **Properties** button.
 - 5) Select the **AS/400 Line Multi-Port Protocol Driver 1** and click the **Uninstall** button.
 - 6) Answer **Yes**, click **Close** and **Close** again to complete the removal.

2. Remove the network adapter from OS/400

- a. To record needed information and vary off the network server description (NWS) for the integrated server, type WRKCFGSTS *NWS and press Enter. The Work with Configuration Status display appears.

Figure 3. Work with Configuration Status display example

```

+-----+
|                                     Work with Configuration Status                                     |
|                                     SYSAS400                                     |
|                                     11/14/97 14:13:02                               |
| Position to . . . . . Starting characters                                         |
| Type options, press Enter.                                                       |
| 1=Vary on 2=Vary off 5=Work with job 8=Work with description                     |
| 9=Display mode status 13=Work with APPN status...                               |
+-----+

```

Opt	Description	Status	-----Job-----		
2	NTSVR	ACTIVE			
	NTSVR01	ACTIVE			
	NTSVRNET00	ACTIVE			
	NTSVR00	ACTIVE	QTCPIP	QTCP	007075
	NTSVRNET	ACTIVE			
	NTSVR00	ACTIVE	QTCPIP	QTCP	007075
	RAMP	VARIED OFF			
	RAMP01	VARIED OFF			
	RAMP00	VARIED OFF			
	RAMP0NET	VARIED OFF			
	RAMP0TCP	VARIED OFF			

Parameters or command
====>
F3=Exit F4=Prompt F12=Cancel F23=More options F24=More keys

While you have the Work with Configuration Status display, do the following:

- 1) Type a 2 in the Opt field to the left of the network server description you want to vary off (NTSVR in the example).
- 2) Record the line description. The line description name begins with the NWSD name followed by 01 or 02. The line description name depends on the port to which you attached it. In the example, the line description for NTSVR is NTSVR01.

Attention: Line description *nwsdname00* is the line description for the private LAN (private network). Do not record the line description for the private LAN.
- 3) Record the controller description, which appears directly under the line description for the port you are removing. The controller description name begins with the first five letters of *nwsdname* and includes 'NET'. In the example, the controller description is NTSVRNET00.

Attention: Be careful **not** to use the controller description for the private LAN (under the line description that ends in 00).
- 4) Record the device description. The device description name begins with the first five letters of *nwsdname* and includes 'TCP'. In the example, the device description is NTSVRTCP00.

Attention: Be careful **not** to use the device description for the private LAN (under the line description that ends in 00).
- 5) Press Enter. The integrated server shuts down.
 - b. If you configured a special route for the adapter, then remove the route by using the RMVTCPRTE command.
 - c. Enter the command RMVTCPIFC.
 - d. Press Enter.
 - e. In the Internet address field, specify the OS/400-side IP address for the adapter. You recorded this value in the integrated server networking information worksheet (See Integrated Windows server networking information) during installation.
 - f. Press Enter.
 - g. Enter the command WRKDEVD DEVD(*CMN) and press Enter.
 - h. Page down until you see the device description that you noted for the line of the adapter you are removing.
 - i. Place a 4 (Delete) in the Opt field to the left of the device description and press Enter.
 - j. Enter the command WRKCTLD CTLD(*CMN).

- k. Page down until you see the controller description that you noted for the line of the adapter you are removing.
 - l. Place a 4 (Delete) in the 0pt field to the left of the controller description and press Enter.
 - m. Enter the command WRKLIND.
 - n. Page down until you see the line description that you noted for the adapter you are removing.
 - o. Place a 4 in the 0pt field to the left of the line description and press Enter.
3. Follow the instructions in your hardware documentation to remove the adapter card.
 4. Vary on the integrated server (described in “Start and stop an integrated server” on page 75).

Chapter 7. Administer integrated Windows servers

The following sections will guide you through some common, everyday tasks performed on the integrated server.

- “Start and stop an integrated server”
 - “Start and stop an integrated Windows server using iSeries Navigator”
 - “Start and stop an integrated Windows server using the character-based interface” on page 76
 - “Shutdown an integrated server from the Windows server console” on page 76
 - “How to safely shutdown your iSeries when integrated Windows servers are present” on page 76
 - “External host LAN issues” on page 77
- “Connect to the 4812 IXS virtual serial console” on page 77
- “View or change integrated Windows server configuration information” on page 78
- “Message logging” on page 78
- “Run integrated Windows server commands remotely” on page 79
 - “Guidelines for submitting remote commands” on page 80
 - “SBMNWSCMD and file level backup support for Kerberos v5 and EIM” on page 81

Start and stop an integrated server

An integrated Windows server has no power button; its state is controlled by the iSeries. Normally you start and shut down integrated servers from iSeries Navigator or the character-based interface. You can partially shut down an integrated server using its own **Start** → **Shut Down** menu, but you cannot start it again without using iSeries Navigator or the character-based interface.

Ensure that integrated servers are varied off before shutting down your iSeries, otherwise, data corruption can occur. Some commands used to shutdown the iSeries will initiate a shutdown in attached integrated servers and wait a certain amount of time for them to power down before shutting down the iSeries. Other commands will shut down the iSeries immediately.

If you use the power off/on scheduling program QEZPWROFFP, you will need to configure it to work with your integrated server.

The following sections describe the start and shut down methods:

- “Start and stop an integrated Windows server using iSeries Navigator”
- “Start and stop an integrated Windows server using the character-based interface” on page 76
- “Shutdown an integrated server from the Windows server console” on page 76
- “How to safely shutdown your iSeries when integrated Windows servers are present” on page 76
- “External host LAN issues” on page 77

Start and stop an integrated Windows server using iSeries Navigator

1. To stop an integrated server in iSeries Navigator, select **Network** → **Windows Administration** → **Integrated xSeries Servers**.
2. Right-click the server you want to stop and select **Shut Down**. If you want to shutdown all integrated servers, right-click the Integrated xSeries Servers icon in the left navigation and select **Shut Down All**. The status changes to **Shutting down...**, **Partially shut down**, and eventually **Shutdown**.
3. To start an integrated server, right-click it and select **Start**. The status changes to **Starting** and eventually **Started**.

Start and stop an integrated Windows server using the character-based interface

1. To stop an integrated server using the character-based interface type the command `WRKCFGSTS *NWS`.
2. Find the integrated server to stop and enter 2 to cause a *vary off*.
3. The status changes from **ACTIVE** to **SHUT DOWN** to **VARIED OFF**. You can push **F5** to update the screen.
4. To start the integrated server use the same command `WRKCFGSTS *NWS`, and type 1 to *vary on* or start the integrated server.
5. To restart an integrated server you must manually vary it off and then back on. There is no command to automatically restart an integrated server from the character-based interface.

Shutdown an integrated server from the Windows server console

To shut down an integrated Windows server from its own console you select **Start** → **Shut Down** from the Windows start menu. However, this method is not recommended because it only causes an integrated server to partially shut down. The Windows operating system stops, leaving the screen *It is now safe to turn off your computer*, but to completely power down and restart you must *vary off* the server using iSeries Navigator or the character-based interface.

As opposed to shutting down, **restarting** an integrated server from its own console is one of the most efficient ways to do so.

Follow these steps

1. From the **Start** menu, choose **Shut down**.
2. Select **Restart** from the drop-down menu and click **Ok**.

How to safely shutdown your iSeries when integrated Windows servers are present

The easiest way to ensure your integrated servers will be shut-down safely is to always manually shut them down before shutting down the iSeries. You may grow tired of this tedious task, however. The CL command `PWRDWSYS *CNTRLD` will attempt to power-down each of the integrated servers, giving each of them a period of time (the `NWSD` attribute `SHUTDTIMO`, by default 15 minutes) in which to shut-down. Note that there is no guarantee that they will finish shutting down within this time period. Not recommended is the CL command `PWRDWSYS *IMMED`, which will power down the iSeries immediately, without attempting to shut down any integrated servers.

Table 2.

Action	Result
Shut down the integrated server manually.	The integrated server is varied off properly, with no risk of data loss.
Issue the CL command <code>pwrdwsys *cntrl</code> .	The integrated server is given the length of time specified in the shutdown timeout attribute of its <code>NWSD</code> in which to shut down, then the iSeries continues to power down.
Issue the CL command <code>pwrdwsys *immed</code> .	The iSeries powers down immediately and does not shut down any integrated servers. Data corruption may result.

If your OS/400 system uses the Power On/Off Schedule, the Power-Off exit program (QEZPWROFFP) should be changed to vary off all `NWSDs` prior to calling the `PWRDWSYS` command. Careful consideration must be given to scheduling as the number and activity of each server will determine the amount of time necessary to completely vary off each server. The scheduled power on must not occur before the system has a chance to vary off all servers and issue the `PWRDWSYS`. See the Schedule a system shutdown and restart topic.

External host LAN issues

When sharing a LAN card between OS/400 and an Integrated Netfinity Server (type 2850 or 6617) using external host LAN, varying off the INS causes the LAN card to shut down and causes OS/400 to lose access to the network as well. In that case you will receive an error message when you try to vary off the Integrated Netfinity Server. You can bypass the error message in three ways

- Respond G (for **Go**) to the error message CPA2614 "Network server *nwsdname* cannot be varied off at this time. (C G)". (This message appears in the QSYSOPR message queue if you vary off the server without first ending the external LAN interfaces.) This will ignore the error message and continue with the shut-down.
- Respond C (for **Cancel**) to the error message and first end the external LAN interface before trying to vary off the Netfinity Server again:
 1. At the OS/400 command line, type CFGTCP and select option 1 to get to the Work with TCP/IP Interfaces menu.
 2. Enter 10 on each external line description that is attached to the network server.

Attention: Be careful not to end the interface for the internal LAN (the line description that ends in 00) or OS/400 will not be able to communicate with the integrated server. For example, this user wants to end the shared external LAN interfaces for the NWSID named IF:

```
-----+-----
                        Work with TCP/IP Interfaces
                        System:  SYSAS400
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  9=Start  10=End

  Opt   Internet    Subnet       Line       Line
       Address     Mask         Description Type
-----+-----
10_    9.5.7.53       255.255.255.0  TRLINE    *TRLAN
       9.5.149.243  255.255.255.128  IF01      *ELAN
10_    9.5.149.245    255.255.255.128  IF02      *ELAN
       192.168.1.3   255.255.255.0   IF00      *TRLAN
-----+-----
```

- You can use the FRCVRYOFF(*YES) option of the Vary Configuration (VRYCFG) command to suppress any verification messages while shutting down the INS. At the OS/400 command line, type: VRYCFG CFGOBJ(*yourNWSID*) CFGTYPE(*NWS) STATUS(*OFF) FRCVRYOFF(*YES)

Connect to the 4812 IXS virtual serial console

The virtual serial console provides Windows console functions for a Windows Server 2003 server that is running on a 4812 Integrated xSeries Server (IXS). See "Windows console" on page 14 for more information about Windows consoles. This console connection can be used prior to configuring TCP/IP on the server.

Any Telnet client can be used as the virtual serial console. Multiple Telnet clients can share access to the same virtual serial console. To connect to a console, use Telnet to connect to port 2301 of the OS/400 partition that is sharing its resources. TCP/IP must be configured and running on the OS/400 logical partition.

To connect to a virtual serial console using the IBM Personal Communications client, do the following:

1. Click **Start -> Programs -> IBM Personal Communications -> Start or Configure Session**.
2. On the Customize Communication dialog, select **ASCII** in the **Type of Host** field.
3. Click **Link Parameters**.
4. On the TelnetASCII dialog, type the host name or the IP address of the OS/400 partition, where you want to connect, in the **Primary Host Name or IP Address** field.
5. Type 2301 in the **Primary Port Number** field.

6. Click **OK**.
7. Click **OK**. The session dialog opens.
8. On the OS/400 Virtual Consoles menu, select **Integrated xSeries Server Consoles**.
9. On the Integrated xSeries Server Consoles dialog, select the hardware resource name for the 4812 IOA that you want to connect as the console. To determine the 4812 IOA hardware resource name, display the Network Server Description (NWS) for the server and use the value of the Resource name parameter.
10. Type the OS/400 service tools ID and password to connect to the Integrated xSeries Server virtual console.

To connect to the virtual serial console using Telnet from a DOS command prompt, follow these steps:

1. On the Command Prompt dialog, type `telnet partitionname 2301`. Where *partitionname* is the name of the OS/400 partition where you want to connect.
2. Press the Enter key.
3. On the OS/400 Virtual Consoles menu, select **Integrated xSeries Server Consoles**.
4. On the Integrated xSeries Server Consoles dialog, select the hardware resource name for the 4812 IOA that you want to connect as the console. To determine the 4812 IOA hardware resource name, display the Network Server Description (NWS) for the server and use the value of the Resource name parameter.
5. Type the OS/400 service tools ID and password to connect to the Integrated xSeries Server virtual console.

View or change integrated Windows server configuration information

iSeries Navigator allows you to view and change most integrated server configuration information.

1. In iSeries Navigator, select **Network** —> **Windows Administration** —> **Integrated xSeries Servers**.
2. Right-click an integrated server and select **Properties**.

Using the character-based interface you can view and change all integrated server configuration information. The following table summarizes the relevant CL commands.

Table 3.

Tasks	CL Command
Vary on and off integrated servers, check the status of the integrated server and objects that are associated with the network server description (NWS).	WRKCFGSTS CFGTYPE(*NWS)
Manage your integrated server environment.	WRKNWSD
Manage line descriptions that are created when you install the integrated server.	WRKLIND
Manage TCP/IP interfaces that are created during server installation.	Work with TCP/IP Network Status, option 1: NETSTAT Configure TCP/IP, option 1 CFGTCP
Monitor network server storage spaces.	WRKNWSSTG

Message logging

Integrated Windows servers log information in different places. If there is a problem, this information may help determine the cause. The following sections describe the message logs.


The **monitor job log** is a key source of information when troubleshooting integrated server problems. It contains messages that vary from normal processing events to detailed error messages. The monitor job always runs in the QSYSWRK subsystem with the same name as the integrated server.

To find the job log in iSeries Navigator

1. Click **Work Management** → **Active Jobs**.
2. One of the jobs listed under the QSYSWRK section will have the same name as your integrated server. Right-click it and select **Job log**.
3. The integrated server job log window opens. Double-click on a message ID to see details.

To find the job log in the character-based interface

1. At an OS/400 command line enter WRKACTJOB SBS(QSYSWRK).
2. One of the jobs listed will have the same name as your integrated server. Select option 5 (Work with job).
3. Type 10 and press Enter to display the job log.
4. Press F10 to see the detailed messages.

| There are other relevant job logs that you may want to check as well. The redbook, Microsoft Windows
| Server 2003 Integration with iSeries, SG24-6959 , has an excellent section concerning integrated
| server event logs in OS/400 and at the Windows console.

Run integrated Windows server commands remotely

You can use OS/400 to remotely submit integrated server batch commands. Windows server commands that can run in batch mode without user interaction will work. Before submitting a remote command verify that the following is true:

- The server is an Integrated xSeries Server on this OS/400 and is active.
- Your user profile is enrolled to the integrated Windows server or domain, or you sign-on with the QSECOFR profile.
- You have authority to run SBMNWSCMD, which requires *JOBCTL special authority. You must also have at least *USE authority to the QSYS/SBMNWSCMD *CMD object.
- If the user profile *LCLPMDMGT value is *YES, then the system value, QRETSVRSEC, must be set to 1 and the user password must be changed or the user have signed-on after QRETSVRSEC was changed.
- If the user profile *LCLPMDMGT value is *NO, then network authentication (Kerberos) is used. The user must access the iSeries operation through Kerberos enabled applications (like iSeries Navigator single sign-on). See “SBMNWSCMD and file level backup support for Kerberos v5 and EIM” on page 81 for more information.
- The OS/400 user profile password, and Windows password must be equivalent. The easiest way to keep them consistent is to use User and Group enrollment.

You may also want to read these “Guidelines for submitting remote commands” on page 80.

To run integrated server commands from iSeries Navigator

1. In iSeries Navigator, select **Network** → **Windows Administration** → **Integrated xSeries Servers**.
2. Right-click on the server on which to run the batch command and select **Run Windows Command**.
3. On the Run Windows Command panel, type the Windows command to run (such as dir \).
Tip: You can select the command from a list of 10 commands that you have run previously on the server.
4. Click **OK** to run the command.

Note: A command using the Run Windows Command panel uses *PRIMARY as the authentication domain. For alternative domains use SBMNWSCMD.

To run integrated Windows server commands from the character-based interface

1. Type CALL QCMD and press Enter.
2. Type SBMNWSCMD and press F4.
3. Type the command you want to run on the remote server. Page down.
4. Enter the NWSD of the server you want to run the command on and press enter.
5. The OS/400 account which you are using must be enrolled to the integrated server in order to be granted authentication to run the remote command. The Authentication domain field allows you to specify where to attempt to authenticate your user ID.
6. The output returned from the command will be displayed on the console. Press F10 to see all messages.

Guidelines for submitting remote commands

To remotely submit integrated Windows server commands, keep these guidelines in mind:

Note: Many of the SBMNWSCMD parameters discussed in this section are not available when running Windows commands by using iSeries Navigator. If you need to use a parameter that iSeries Navigator does not support, then you must use Submit Network Server Command (SBMNWSCMD) directly.

- The requested command is run under the Windows console command "cmd.exe." SBMNWSCMD will not return control to its caller until the command has finished running on Windows and the cmd.exe program terminates.
- The authentication domain field of SBMNWSCMD indicates the Windows domain where your user ID is to be authenticated. The default, *PRIMARY, logs on to the primary domain of the server, if the server is a domain member. *LOCAL logs on to the server itself. The name of a trusted domain may also be specified.
- The QSECOFR user profile is handled differently than all other user profiles. User authentication is not performed on Windows when SBMNWSCMD is run by the QSECOFR profile. The requested Windows command is run under the Windows Local System Account. The Local System Account is used even if the QSECOFR profile is enrolled. The Local System Account does not have a password and lacks network access rights.
- Do not use the "/u" parameter with the Windows "cmd" command.
- SBMNWSCMD has limited support of Kerberos v5 authentication. Kerberos will only be used when the LCLPDMGT user profile attribute is *NO. See "SBMNWSCMD and file level backup support for Kerberos v5 and EIM" on page 81.
- The Remote Command service and SBMNWSCMD are able to distinguish between ASCII multi-byte and unicode output data and convert them as appropriate.
- You can combine integrated Windows server commands into a single command string by using features of the Windows "cmd.exe" command interpreter. For example, on the SBMNWSCMD command line, you can enter net statistics workstation && net statistics server to collect statistics. However, commands that you combine in a single SBMNWSCMD request should not return mixed data (for example, a combination of ASCII and Unicode data), or data in mixed codesets. If the commands return different types of data, SBMNWSCMD may end abnormally with a message which indicates "a problem occurred in the data output conversion." In that case, run the commands separately.
- Do not use characters that are not normally available from the integrated server keyboard. In rare cases, an EBCDIC character in the active jobs coded character set may not have an equivalent in the active code page on Windows. Each different Windows application will give different conversion results.
- The Submit Network Server Command does not completely initialize your logon environment. The user's environment variables are set, but may not be completely equal to those provided by an interactive logon. Thus, environmental variables that an interactive logon normally sets to user-specific values may not exist or may be set to system default values. Any scripts or applications that rely on user-specific environmental variables may not operate correctly.
- If the home directory for your user ID on the integrated server is mounted on the local server, the Submit Network Server Command sets the current directory to your home directory. Otherwise, it tries to use /home/default or the local system drive.

- If a user profile exists, SBMNWSCMD will attempt to load it. You can then use commands that use or alter profile dependencies. However, there is no indication of profile load failures, beyond event log messages that may be produced by Windows.
- You can use SBMNWSCMD to run integrated server applications as long as they do not require user intervention. The commands run in a background window, not on the integrated server console. If an application requests user intervention, such as popping up a message window, then SBMNWSCMD will hang, waiting for the command to complete - but no intervention is possible. If you end SBMNWSCMD on OS/400, it will attempt to end the hung Windows command. The background command stops whether GUI or console based.
- You can also run commands that require a **yes** or **no** reply to proceed. You do this by using input pipe syntax to provide the response. For example, `echo y|format f: /fs:ntfs` will let the format proceed after the **Proceed with Format** question raised by the format command. Note that the "y" and the pipe symbol "|" do not have a space between them.
- Not all Windows batch commands support the piping of input (for example, the "net" command). Attempts to pass a default response may not be possible.
- You can prevent SBMNWSCMD from logging the command. If the command string contains sensitive data, such as passwords, that you do not want logged in error messages, do the following:
 1. Specify *NOLOGCMD as the command string.
 2. When the Command (not logged) field appears, enter the command to run in this field.

Note, however, that the *NOLOGCMD option does not affect data that the command returns. If the command returns sensitive data, you can use the command standard output (CMDSTDOOUT) parameter to store the output in a secure location, such as an integrated file system file.

- You can direct standard output from the command to your job log (*JOBLOG), to a spool file (*PRINT), or to an integrated file system (IFS) object. Standard error data always goes to the job log.

When you specify *PRINT, the Work with Spool File (WRKSPLF) display shows SBMNWSCMD in the User Data field for the spooled file. If you select option 8 to display the attributes, the names of the specified integrated server and Windows command appear in the user-defined data field.

When you specify an integrated file system object, the path name must already exist. If the integrated file system object name does not exist, SBMNWSCMD creates it.
- In the Convert standard output field, you can specify (*YES) to convert output from the Windows code set to the coded character set identifier (CCSID) of the OS/400 job.

New IFS files will be created with the job CCSID. Output directed to an existing IFS object is converted to the IFS object CCSID. Output directed to a new member of an existing file in the /QSYS.LIB file system is converted to the existing file CCSID.
- If Convert standard output is (*NO), the Windows standard output will be written to the IFS object, or spool file, and will not be converted.

SBMNWSCMD and file level backup support for Kerberos v5 and EIM

File level backup operations to an integrated Windows server utilize the iSeries NetClient and Submit Network Server Command (SBMNWSCMD) functions. In V5R3, these functions provide limited Kerberos v5 support (also known as iSeries Network Authentication). Thus, there are some considerations to keep in mind if you desire to use network authentication with these functions.

1. In order to enable iSeries to use Kerberos authentication, you must configure these things on the iSeries server:
 - iSeries Navigator Security option
 - Network authentication service
 - Enterprise Identity Mapping (EIM)
 - Cryptographic Access Provider (5722-AC2 or AC3)
2. The iSeries NetServer should be configured to use Password/Kerberos v5 authentication and NetServer must be active.

3. The Kerberos KDC must be a Windows Active Directory domain controller (Windows 2000 Server or Windows Server 2003).
4. Kerberos authentication will only be used when the OS/400 job's user profile has the LCLPWDMGT attribute set to *NO. When LCLPWDMGT is set to *YES, then password authentication will always be used.
5. NetClient can only successfully authenticate using Kerberos to integrated servers that are members of the same Windows domain as the OS/400 default Kerberos realm. That is, the target integrated server cannot be in a different Windows domain (a Windows domain is equivalent to a Kerberos realm) than the OS/400's default Kerberos realm value.
6. User Enrollment supports using EIM to map a Windows user name to a different OS/400 profile name. Thus, user enrollment can look for an EIM registry which is named for the Windows Active Directory domain name, or for a EIM registry which is named for the integrated server name as appropriate. User enrollment will use the EIM mapping regardless of whether Kerberos authentication can be used. However, SBMNWSCMD and NetClient will **only** use an EIM mapped name when Kerberos authentication is used. So, user enrollment may create a local windows user with a different name than the OS/400 profile as specified by the EIM mapping. But, SBMNWSCMD and NetClient will only use the different windows name when Kerberos authentication is performed (When LCLPWDMGT = *NO). Otherwise, they attempt to authenticate with a Windows name equal to the OS/400 profile name.
7. For SBMNWSCMD submitted windows commands to be able to connect to other network servers when Kerberos authentication is used, the target windows server must be *trusted for delegation*. In Windows 2000, this is enabled by default for domain controllers. However, it is disabled by default for domain member servers. It may be enabled via the Administration Tool: **Active Directory User and Computers** on a domain controller. Within this tool, click **Computers** and select the correct computer. Then click **Computer properties** → **General**. Then check **Trust computer for delegation**.

Chapter 8. Manage storage

Instead of having their own hard disk drives, integrated Windows servers use OS/400 disk storage for storing client data and sharing network files. OS/400 disk storage allocated to an integrated server is called *network server storage space*. The integrated server equivalent of installing a new hard drive in a PC server is to create a network server storage space in OS/400 and link it to an integrated server. Realizing that integrated server disk storage is managed through OS/400 will influence your decisions about drive sizes, partitioning, and disk volumes. See “OS/400 storage management.” You can also read about “Predefined disk drives for integrated Windows servers” on page 85 and “Disk drives for integrated Windows servers” on page 84.

Windows environment for iSeries helps you handle data storage in the following ways:

- By allowing you to use OS/400 to “Administer integrated Windows server disk drives from OS/400” on page 86.
- By giving you the option to “Use Windows disk management programs with integrated Windows servers” on page 91.

OS/400 storage management

This brief overview of OS/400 storage management concepts is intended for administrators who are more familiar with how Windows servers manage storage. Because OS/400 handles storage management differently than a PC server, some techniques that you need in the PC server world are unnecessary in the Windows environment on iSeries.

OS/400 and disk drives

OS/400, the operating system that runs on an iSeries, does not need to deal directly with disk drives. Beneath the operating system a level of software (called System Licensed Internal Code (SLIC)) “hides” the disk drives and manages the storage of objects on those disk drives. A virtual address space is mapped over the existing disk space and used for addressing objects rather than disk drive IDs, cylinders, and sectors. Needed objects are copied (“paged in”) from this address space on disk into the address space of main memory.

Because of the way OS/400 manages disk data, you do not generally need to worry about partitioning high-growth databases, defragmenting disks, or disk striping on your Integrated xSeries Server. The Integrated xSeries Server uses device drivers to share the OS/400 disk drives. These device drivers send and receive disk data to the OS/400 storage management subsystem. OS/400 storage management handles the hard disks, including spreading the Windows disk drive images across multiple hard disk drives and applying RAID and file mirroring (if configured). Disk defragmentation software manages logical file fragmentation of the hard disk images. Because OS/400 storage management handles these tasks, running a defragmentation program on the Integrated xSeries Server helps only in cases where “critical file system structures” can be defragmented.

Disk pools (ASPs)

In OS/400 physical hard disk drives are pooled together into one storage space called a disk pool, also called an auxiliary storage pool (ASP). If your filesystem runs out of space, you can add a new hard disk drive to the disk pool, and the new storage space will be available immediately. Every system has at least one disk pool, the system disk pool. The system disk pool is always ASP 1. You can configure additional *user* disk pools, numbered 2 - 255. You can use disk pools to distribute your OS/400 data over different groups of disks. You can also use this concept to move less important applications or data to your older, slower disk drives. Support for independent ASPs (33-255) is provided through iSeries Navigator. Both the Information Center and iSeries Navigator refer to ASPs as Disk Pools.

Disk protection:

OS/400 disks can be protected in two ways:

- **RAID-5**

The RAID-5 technique groups several disks together to form an array. Each disk holds checksum information of the other disks in the same array. If a disk fails, the RAID-5 disk controller can re-create the data of the failing disk with the help of the checksum information on the other disks. When you replace a failing disk with a new one, OS/400 can rebuild the information from the failed disk on the new (and therefore empty) disk.

- **Mirroring**

Mirroring keeps two copies of data on two different disks. OS/400 performs write operations on both disks at the same time, and can simultaneously perform two different read operations on the two disks of a mirrored pair. If one disk fails, OS/400 uses information from the second disk. When you replace the failing disk, OS/400 copies the data from the intact disk to the new disk.

To further increase the level of protection, you can attach the mirrored disks to two different disk controllers. Then if one controller fails, and with it one set of disks, the other controller can keep the system up. On larger models of iSeries, you can attach controllers to more than one bus. Attaching the two disk controllers that form a mirrored pair to two different buses increases availability even more.

You can define disk pools on OS/400 to have different levels of protection or no protection at all. Then you can put applications and data into a disk pool with the right amount of protection, depending on how important their availability is. For more information about OS/400 disk protection and availability options, read Backup and Recovery.

Disk drives for integrated Windows servers

As stated earlier, integrated servers do not have their own disk drives. OS/400 creates network server storage spaces within its own file system and integrated servers use them as if they were normal PC server hard disk drives.

Network server storage spaces can reside in either the OS/400 system disk pool (ASP 1) or a user disk pool. You can statically link up to 16 disk drives. An additional 16 disk drives can be linked either while the server is shut down or linked dynamically while the server is active. You can copy one disk drive to another to move it to a different disk pool.

After a network server storage space has been created and linked to an integrated server, you must format it from the Windows console. You can choose from between three types of disk formats. You will probably choose NTFS since it is the newest format type and has the most features. Network server storage spaces formatted with NTFS can be up to 1,024,000 MB, except for the predefined system drive (C) of an older Integrated Netfinity Server (6617, 2850), which is limited to 8,000 MB. Another format type is FAT-32. Drives formatted with FAT-32 can be from 512 – 32,000 MB. The oldest format type is FAT. The maximum possible size for a FAT drive is 2,047 MB. The predefined installation source drive (D), which must be in FAT format, is therefore limited to 2,047 MB.

Network server storage spaces are one of the two types of network storage that integrated servers use. Integrated servers can also access resources on OS/400 that an administrator has shared with the network by using iSeries NetServer.

The IBM iSeries Integration for Windows Server installation process creates several disk drives that are used to install and run integrated Windows servers. See the topic on “Predefined disk drives for integrated Windows servers” on page 85.

Predefined disk drives for integrated Windows servers

IBM iSeries Integration for Windows Server installation process creates two disk drives (network server storage spaces) for installing and running integrated servers. See “Disk drives for integrated Windows servers” on page 84. (Earlier releases created server storage spaces in QUSRSYS.) By default, OS/400 creates these disk drives in the system disk pool (ASP), but you can choose a different location during the installation. OS/400 also uses these disk drives to load and start the integrated server.

Servers first installed on V4R5 and later systems have these predefined disk drives:

Boot and system drive (C)

This drive serves as the system drive. OS/400 names this drive *server1*, where *server* is the name of the network server description (NWSD). This disk drive resides in the integrated file system and is automatically linked as the first user-defined drive.

The C drive ranges from 1,024 to 1,024,000 MB, depending on the Windows version, server type, and install type. (Integrated Netfinity servers (6617, 2850) are limited to 8,000 MB.) You can choose to convert the drive to NTFS, which is required for Windows Active Directory. The C drive is automatically converted to NTFS, if required by the Windows version, hardware resource type or size of the storage space. However, if you plan to create NWSD configuration files, be aware that support for these files exists only for predefined disk drives that are formatted as FAT or FAT32. See Chapter 14, “Network server description configuration files,” on page 159. A system drive that has been converted to NTFS is not accessible for NWSD configuration files. For more information about the different file systems, see “Comparison of FAT, FAT32, and NTFS file systems” on page 41.

Installation source drive (D)

The D drive can be 200 - 2,047 MB and holds a copy of the Windows server installation code and the IBM iSeries Integration for Windows Server code. OS/400 names this drive *server2*, where *server* is the name of the NWSD. This disk drive resides in the integrated file system and is automatically linked as the second user-defined drive. OS/400 formats the D drive as a file allocation table (FAT) disk.

Attention: This drive must remain as a FAT drive. Do not make any changes to this drive. You use this drive to perform updates, and changing the drive can make performing updates impossible.

Servers upgraded from pre-V4R5 systems have these predefined disk drives:

Boot drive (C)

The boot drive contains the programs necessary to start the integrated server. This drive must remain a FAT drive to ensure that the integrated server can write configuration information to it when it is varied on. Do not convert this drive to NTFS. The C drive is 10 MB, and OS/400 names this drive *server1*, where *server* is the name of the network server description (NWSD). This storage space resides in the QUSRSYS library.

Note: If the C drive becomes full, see “Remapping a full C drive; for integrated servers created pre-V4R5 only” on page 132.

Installation source drive (D)

The source drive can be 200 to 1,007 MB and holds a copy of the Windows server installation code and the IBM iSeries Integration for Windows Server code. OS/400 names this drive *server2*, where *server* is the name of the NWSD. This disk drive resides in the QUSRSYS library. This drive must remain a FAT drive. Do not make any changes to this drive. You use this drive to perform updates, and changing the drive can make performing updates impossible.

System drive (E)

For servers first installed on pre-V4R5 systems, the E drive is the integrated server system drive. It can be 500 to 8000 MB and holds the installed copy of Windows server and the IBM iSeries Integration for Windows Server code. OS/400 names this drive *server3*, where *server* is the name of the NWSD.

A system drive less than or equal to 1,007 MB is created as a server storage space in QUSRSYS. Although you can convert this drive to the NTFS file system, leaving the drive as FAT increases the recovery options in case of a problem.

A system drive greater than 1,007 MB is created as a network server storage space in the integrated file system and automatically linked as the first user-defined drive. By default, OS/400 creates it in the system disk pool (ASP), but you can customize this when you install Windows server. System drives greater than 2,047 MB are too large to remain as FAT. During the installation, Windows server automatically converts them to NTFS and expands them to use all but the last cylinder of the disk image.

Note: If you plan to create your own NWSD configuration files, be aware that support for NWSD configuration files exists only for predefined disk drives that are formatted as FAT. A system drive that includes a network server storage object or that has been converted to NTFS is not accessible for NWSD configuration files. See Chapter 14, “Network server description configuration files,” on page 159.

Administer integrated Windows server disk drives from OS/400

Administering integrated server disk drives (network server storage spaces) from OS/400 includes these tasks:

- “Access the OS/400 integrated file system from an integrated server”
- “Obtain information about integrated server disk drives”
- “Add disk drives to integrated Windows servers” on page 87
- “Copy a disk drive” on page 89
- “Unlink integrated Windows server disk drives” on page 90
- “Delete integrated Windows server disk drives” on page 90

Access the OS/400 integrated file system from an integrated server

You can access the OS/400 integrated file system from an integrated server through IBM iSeries Support for Windows Network Neighborhood (iSeries NetServer). This allows you to easily work with file system resources on OS/400. For information about using iSeries NetServer, see:

- Create an iSeries NetServer file share
- Set up your PC client to use iSeries NetServer
- Access iSeries NetServer file shares with a Windows client

For more information, see “Enable iSeries NetServer” on page 29.

Obtain information about integrated server disk drives

If you want to know what percentage of an integrated server disk drive (network server storage space) is in use or what its format is, you can obtain the information from OS/400.

To obtain disk drive information, follow these steps:

1. In iSeries Navigator, select **Network**—> **Windows Administration** —> **Disk Drives**.
2. Select a disk drive from the list available
3. Right-click the disk drive and select **Properties** or click the appropriate icon on the iSeries Navigator toolbar

If you want to use the CL command, see Work with Network Server Storage Spaces (WRKNWSSTG).

Add disk drives to integrated Windows servers

Creating and formatting what the integrated server perceives as disk drives for your applications and data involves creating network server storage spaces on OS/400. For conceptual information about user-defined network server storage spaces, see “Disk drives for integrated Windows servers” on page 84. To add an integrated server disk drive (network server storage space), perform these tasks:

1. “Create an integrated server disk drive.”
2. “Link a disk drive to an integrated server.”
3. “Format integrated server disk drives” on page 89.

Create an integrated server disk drive

Creating an integrated server disk drive (network server storage space) is the first step toward adding disk space to an integrated Windows server. The time that you need to create a disk drive is proportional to the size of the drive. After creating the disk drive, you must link (See “Link a disk drive to an integrated server”) it to the network server description of your integrated server and format it. See “Format integrated server disk drives” on page 89.

To create an integrated server disk drive, follow these steps:

1. In iSeries Navigator, select **Network** —> **Windows Administration**.
2. Right-click the **Disk Drives** folder and select **New Disk** or click the appropriate icon on the iSeries Navigator toolbar.
3. Specify a disk drive name and description.
4. If you want to copy data from another disk, select **Initialize disk with data from another disk**. Then select the source disk to copy data from.
5. Specify the disk capacity. See the online help for details on valid disk sizes associated with a particular file system format.
6. Select a disk pool (auxiliary storage pool) to contain the disk.
7. Click **OK**.
8. Link the new disk drive (See “Link a disk drive to an integrated server”) to the network server description of your Windows server.

If you want to use the CL command, see CRTNWSSTG.

Notes:

Creating a disk drive creates a partition for the drive but does not format it.

Creating or starting a server with a disk drive in an independent disk pool (ASP) requires that the disk pool device be available.

Link a disk drive to an integrated server

In order for an integrated Windows server to recognize an integrated server disk drive (network server storage space) as a hard disk drive, you must link the two together. You must create a disk drive before you can link it. See “Create an integrated server disk drive.” After you create and link a new integrated server disk drive, it appears as a new hard disk drive to the integrated server. Then you must format it before you can use it. See “Format integrated server disk drives” on page 89.

Disk drives can be linked to servers in one of the following ways:

1. Static disk drive links allow disk drives to be linked to the server using user specified link sequence positions. The order that the server sees the drives is determined by the relative order of the link sequence positions. The server must be varied off when adding a static disk drive link. Up to 16 disk drives can be linked statically. The system defined drives created by the Install Windows server (INSWNTSVR) command are statically linked.

2. A cluster quorum resource disk drive link is used to link the cluster quorum resource disk drive to the servers in the cluster. This type of link is not allowed for the Integrated Netfinity Server (6617 or 2850) resource types.
3. Cluster shared disk drive links allow a disk drive to be shared among clustered integrated servers. This type of link is not allowed for the Integrated Netfinity Servers (6617 or 2850) resource types. Up to 15 disk drives can be linked as shared between the nodes that are clustered together. A shared drive can only be linked to nodes that share a common quorum resource drive. Drives of this type are available to all nodes that are joined together by the links of the cluster quorum resource. Each node has access to the shared drives under the control of Windows Cluster services running on each node.
Note: Drives that are linked as shared should be linked to ALL nodes that are clustered together.
4. Dynamic disk drive links allow additional disk drives to be linked to an integrated server using dynamically assigned link sequence positions. The disk link sequence position is assigned dynamically at the time that the disk drive is linked to an active server. The disk link sequence position can be specified, but it is not used until the server is restarted. The integrated server can either be shut down or active when adding a dynamic disk drive link. However, if adding a dynamic link to a server that is running on a type 2850 or 6617 Integrated Netfinity Server, then the server must be restarted in order to access the disk drive.

When an integrated server is started, it sees the disk drives in the following order:

1. Statically linked disk drives.
2. Cluster quorum resource disk drive.
3. Cluster shared disk drives.
4. Dynamically linked disk drives.

Within each of these link type categories, the disks appear in the order of their user specified link sequence positions. When dynamically linking a disk drive to an active server, the new disk drive appears following all other linked disk drives.

To link a disk drive to an integrated server, follow these steps:

1. If you are not linking a disk drive dynamically, then shut down your integrated server. See “Start and stop an integrated server” on page 75.
2. In iSeries Navigator, select **Network** —> **Windows Administration** —> **Disk Drives**.
3. Right-click an available disk drive and select **Add Link**, or select the drive and click the appropriate icon on the iSeries Navigator toolbar.
4. Select the server you want to link the disk to.
5. Select one of the available link types and the link sequence position.
6. Select one of the available data access types.
7. Click **OK**.
8. If you are not linking a disk drive dynamically, then start your integrated server. See “Start and stop an integrated server” on page 75.

If you want to use the CL command, see ADDNWSSTGL.

If the disk drive is new and has not previously been formatted, refer to “Format integrated server disk drives” on page 89.

Manage disk drives when running out of drive letters:

The maximum number of disk drives that can be linked to an integrated server 2003 is 32 disk drives (48 with cluster service). Since not all drives will have a drive letter, other options must be used to utilize all storage linked to the server. Here are two options to utilize all disk drives which are linked to a server.

1. A disk drive letter can be made up of multiple disk drives using a spanned volume set.

- a. From **Disk Management**, right-click on each disk drive number and select **Upgrade to Dynamic Disk...** from pop-up menu.
 - b. Right-click on a disk drive partition and select **Create Volume...** from pop-up menu.
 - c. Follow the create volume wizard to create a spanned volume, making sure to add the multiple disks. Note: This feature is nice because if the volume gets full, a disk can be dynamically added, and it will be immediately joined to the spanned volume without ever requiring to reboot the server.
2. A disk drive can be mounted over a subdirectory of an existing disk drive letter.
 - a. Create a directory on a disk drive letter that is formatted with NTFS. For example, MD C:\MOUNT1.
 - b. From **Disk Management**, click over disk drive partition you want to format and select **Format** from the pop-up menu.
 - c. Once drive is formatted, right-click over disk drive partition again and select **Change Drive Letter and Path...** from pop-up menu.
 - d. Select **Add**.
 - e. Select radio button **Mount in this NTFS folder:**
 - f. Use **Browse** button to find directory C:\MOUNT1 that was created in step 1.
 - g. Click **OK** to make that directory a mount point for this disk drive.

Format integrated server disk drives

In order to use integrated Windows server disk drives (network server storage spaces), you must format them. Before you can format them, you must first create (see “Create an integrated server disk drive” on page 87) and link (see “Link a disk drive to an integrated server” on page 87) the disk drives, then start the Windows server from OS/400 (see “Start and stop an integrated server” on page 75).

Note: Windows 2000 Server or Windows Server 2003 servers running on an Integrated xSeries Server or Adapter can dynamically link disk drives while the server is varied on using the dynamic storage link parameter.

To format disk drives, follow these steps.

1. On the integrated Windows server console, from the **Start** menu, select **Programs**, then **Administrative Tools**, then **Computer Management**.
2. Double-click **Storage**.
3. Double-click **Disk Management**.
4. Right-click the drive that you want to format and select **Format** from the pop-up menu.
5. Select the file system you specified when you created the disk drive.
6. Follow the prompts to format the new drive.

Copy a disk drive

You can create a new integrated Windows server disk drive (network server storage space) by copying data from an existing disk drive.

To copy a disk drive, follow these steps:

1. Expand **Network** —> **Windows Administration** —> **Disk Drives**.
2. Select a disk drive from the list available.
3. Right-click the disk drive and select **New Based On** or click the appropriate icon on the iSeries Navigator toolbar.
4. Specify a disk drive name and description.
5. Specify the disk capacity. See the online help for details on valid disk sizes associated with a particular file system format. If you want to increase the size of the disk while copying it, you can specify a larger size. The extended portion of the disk will be unpartitioned free space.

6. Select a disk pool (auxiliary storage pool) to contain the disk.
7. Click **OK**.

If you want to use the CL command, see Create Network Storage Space (CRTNWSSTG).

Unlink integrated Windows server disk drives

Unlinking integrated server disk drives (network server storage spaces) disconnects them from the integrated server, making them inaccessible to users.

To unlink a disk drive, follow these steps:

1. Shut-down your integrated server. See “Start and stop an integrated server” on page 75.
2. In iSeries Navigator, select **Network** —>**Windows Administration** —> **Disk Drives**.
3. Right-click an available disk drive and select **Remove Link**, or select the drive and click the appropriate icon on the iSeries Navigator toolbar.
4. Select a server from the list of linked servers.
5. If you are unlinking a disk drive that you plan to relink, uncheck the **Compress link sequence** check box. You need to relink the disk drive as the same link sequence number before you vary on the server. By preventing compression of the link sequence values, you avoid having to unlink and relink all the disk drives to get them in the correct sequence.
6. Click **Remove**.
7. If you are uninstalling Windows server from an Integrated xSeries Server, refer to “Delete integrated Windows server disk drives.” Otherwise, start the integrated server. See “Start and stop an integrated server” on page 75.

If you want to use the CL command, see RMVNWSSTGL.

Delete integrated Windows server disk drives

Deleting a disk drive (network server storage space) destroys the data on the disk drive and frees the iSeries disk storage so that it can be used for other purposes.

Before you can delete a disk drive, you must unlink it from the integrated server. See “Unlink integrated Windows server disk drives.” Once you have unlinked it, you can delete it.

To delete the disk drive, follow these steps:

1. In iSeries Navigator, select **Network** —>**Windows Administration** —> **Disk Drives**.
2. Select a disk drive from the list available.
3. Right-click the disk drive and select **Delete** or click the appropriate icon on the iSeries Navigator toolbar.
4. Click **Delete** on the confirmation panel.

If you want to use the CL command, see DLTNWSSTG.

Delete disk drives when removing an integrated server

When you manually remove an integrated server, you need to delete the disk drives (network server storage spaces) that are associated with the network server description (NWSD) for that server. Also delete user-created disk drives that you own.

The Delete Windows Server (DLTWNTSVR) command is provided to remove all objects created by the Install Windows server (INSWNTSVR) command. It removes the network server description (NWSD), line

descriptions (LIND), storage spaces (NWSSTG, SRVSTG), TCP interfaces, controller descriptions (CTLD), and device descriptions (DEVD). This is the recommended way to permanently remove an integrated server from the system.

You also need to delete any disk drives that OS/400 predefined as the system drive and installation drive for your server. For NWSDs that were created in V4R5 or later, you need to delete the system drive, named nwsdname1, and the installation drive, named nwsdname2. For NWSDs that were created before V4R5 with a system drive larger than 1007 MB, you need to delete the system drive, named nwsdname3.

To find out what disk drives are associated with your server, see the topic “Obtain information about integrated server disk drives” on page 86

Use Windows disk management programs with integrated Windows servers

You can use the Windows Disk Management program to administer your disk drives (network server storage spaces), just as if they were individual physical disk drives. Features such as assigning drive letters, partitioning, and volume set creation are fully functional.

When using Windows disk management programs, consider the following:

- When you link user-defined disk drives, you can assign relative positions for the drives or have OS/400 do it automatically. OS/400 also assigns sequence numbers to the predefined disk drives.
- Unless you use Windows Disk Management to assign the optical drive letter, the optical drive appears as the next available drive letter after all disk drives on the integrated server. If no user-defined disk drives are linked to your NWSD, the optical drive typically appears as drive E.
- It is possible to link up to 32 user-defined disk drives to each Windows 2000 Server or Windows Server 2003 (48 with cluster service).

Chapter 9. Share devices

One advantage integrated Windows servers have is the ability to use iSeries devices. You can use iSeries optical drives, tape drives, and printers from your Windows server.

Accessing iSeries devices includes these tasks:

- OS/400 and Windows server refer to devices by different names, so you first need to learn the appropriate device descriptions and hardware resource names you plan to use. See “Determine the device description and hardware resource names for iSeries devices.”
- To use an optical drive on an integrated server, vary it on from OS/400. See “Use iSeries optical drives with integrated Windows servers.”
- See this topic: “Use iSeries tape drives with integrated Windows servers” on page 94 for information about allocating drives to integrated Windows servers, formatting tapes, transferring drives between servers, and transferring drives back to OS/400.
- Read this topic: “Print from an integrated Windows server to iSeries printers” on page 98.

Determine the device description and hardware resource names for iSeries devices

When you refer to iSeries devices on OS/400, you need to use their device description name. When you refer to those devices from an integrated Windows server, you need to use their hardware resource name. If the names are different and you use the wrong name, you get the wrong device.

To determine the hardware resource name and see whether it is the same as the device description name, follow these steps:

1. On the OS/400 command line, type `DSPDEVD device_description_name` and press Enter.
2. The Resource name field has the hardware resource name for this device. Check to see if it has the same name as the Device description field. If the names are different, you must remember to use the appropriate name depending on whether you are working from the integrated Windows server or from OS/400.

Some tape devices report in under more than one device description. Tape libraries (3590, 3570, and so forth) report in as devices (TAPxx) as well as tape libraries (TAPMLBxx), where xx is a number. IBM iSeries Integration for Windows Server does not support tape libraries. Therefore, if your device has a tape library description, both the tape device and tape library device must be in a varied off state before locking the device on the Windows server.

Use iSeries optical drives with integrated Windows servers

Windows server can use an iSeries optical drive just as it does a local optical drive. The iSeries optical drive appears as a normal local optical drive in the **My Computer** folder on Windows server.

If you have logical partitions on your iSeries, the optical drive is allocated to a single partition. It cannot be shared by integrated servers that are in other partitions and the optical drive must be allocated (locked) to a NWSD to be used.

The optical drive must be varied on before you can allocate it to an integrated Windows server. If the optical drive is not varied on, follow these steps to vary it on:

1. At the OS/400 command line, type `WRKCFGSTS *DEV *OPT` and press Enter.
2. In the Opt column next to the correct optical device, typically OPT01, type 1 to vary on the optical drive.
3. Press Enter and the optical drive varies on.

To lock an optical drive, follow the steps below:

1. Click **Start**, then **Programs**, then **IBM iSeries**, then **Integration for Windows Server**.
2. Expand **Integration for Windows Server**.
3. Expand the Network Server Description name.
4. Select **iSeries Devices**.
5. Select the device name.
6. Right-click and select **All Tasks, Lock Device**.

If you have any problems using the iSeries optical drive from an integrated Windows server, see “Optical device problems” on page 133.

Note: If the integrated server fails before unlocking an optical device (or varying off the server), the optical device will be unavailable to OS/400 or other integrated servers. You will need to vary off the optical device using WRKCFGSTS *DEV *OPT and vary it back on to free the lock.

Return control of an optical device from an integrated server to iSeries

To use the optical drive from OS/400, you must first unlock it from the integrated server. To unlock the optical drive from the integrated server, you must either be the person who originally locked the drive or have Administrator or Backup Operator authority.

To transfer control of the iSeries optical drive from an integrated server to iSeries, follow these steps:

1. Click **Start**, then **Programs**, then **IBM iSeries**, then **Integration for Windows Server**.
2. Expand **Integration for Windows Server**.
3. Expand the **Network Server Description** name.
4. Select **iSeries Devices**.
5. Select the device that you want to unlock.
6. Right-click and select **All Tasks**, then **Unlock Device**.

Use iSeries tape drives with integrated Windows servers

iSeries tape drives can perform significantly faster than drives you normally attach to a PC server, and you can allocate them to integrated servers, therefore providing a faster tape access method than available to PC servers. See “Supported iSeries tape drives” on page 96.

Because multiple integrated servers in the same iSeries system can all access the same tape drive (although not at the same time), you need to allocate only one tape drive for multiple integrated servers.

Notes:

1. Although you can dedicate tape drives to the integrated server and to OS/400, both systems cannot simultaneously use the same tape drive. The two operating systems require different tape formats. You cannot use the same tape on an integrated server and on OS/400 without reformatting it.
2. If you have logical partitions on your iSeries, the tape drive is allocated to a single partition. It cannot be shared by integrated servers that are in other partitions.

To use an iSeries tape drive from an integrated server you must perform the following tasks:

- “Format a tape on OS/400 for use with integrated Windows servers” on page 95.
- Allocate an iSeries tape drive to an integrated server by varying off the tape drive from OS/400 and locking it on the integrated server. See “Allocate the iSeries tape drive to an integrated Windows server” on page 95.
- Transfer control of an iSeries tape drive to a different integrated server. See “Transfer control of the iSeries tape and optical drives between integrated Windows servers” on page 97.

- Return control a tape drive from an integrated server so that OS/400 can use it. Ensure that you have a correctly formatted tape. See “Return control of a tape drive from an integrated Windows server to the iSeries” on page 96.

If you have problems with an iSeries tape drive, see “Tape problems” on page 133.

Format a tape on OS/400 for use with integrated Windows servers

To use iSeries tape drives with integrated Windows servers, you must use a tape format that they recognize. To produce a non-labeled tape acceptable to Windows, use the OS/400 Initialize tape (INZTAP) command.

To format a tape, do the following:

- Put the tape you want to use in the iSeries tape drive.
- At the OS/400 command line, type:

```
INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED)
CHECK(*NO) DENSITY(*CTGTYPE) CODE(*EBCDIC)
```

where *tap01* is the name of your tape drive. Press Enter.

Allocate the iSeries tape drive to an integrated Windows server

To use an iSeries tape drive from the integrated Windows server console, you must vary it off on OS/400 and lock it onto the integrated server. You must lock the device before starting applications or their services.

Note: Some tape devices report in under more than one device description. Tape libraries (3590, 3570, and so forth) report in as devices (TAPxx) as well as tape libraries (TAPMLBxx), where xx is a number. IBM iSeries Integration for Windows Server does not support tape libraries. Therefore, if your device has a tape library description, you must vary off both the tape device and the tape library device before locking the device on the integrated server.

To transfer control of the iSeries tape drive to an integrated server, follow these steps:

1. Vary off the tape drive on OS/400:
 - To do this from iSeries Navigator
 - a. Click **Configuration and Service** → **Hardware** → **Tape Devices**.
 - b. Click **Stand-Alone Devices** or **Tape Libraries**.
 - c. Right-click a device or library and select **Make Unavailable**.
 - To do this from the OS/400 character based interface
 - a. At the OS/400 command line, type WRKCFGSTS *DEV *TAP, and press the Enter key. The Work with Configuration Status display appears.

Note: WRKCFGSTS *DEV *TAPMLB will bring up a list of the tape library devices.
 - b. In the Opt column next to the device name of your tape drive, type 2 to vary off the tape drive.
 - c. Press Enter. The tape drive varies off.
2. Lock the tape device on an integrated server:
 - a. From its Windows console, click **Start** → **Programs** → **IBM iSeries** → **Integration for Windows Server**.
 - b. Expand **Integration for Windows Server**.
 - c. Expand the network server description name.
 - d. Select **iSeries Devices**.
 - e. Select the tape object that you want to lock.
 - f. Right-click and select **All Tasks, Lock Device**.

3. If you need other information about the tape device to enable an application to recognize it, see “Identify iSeries tape devices for applications” on page 97. If you have problems, see “Tape problems” on page 133.

Return control of a tape drive from an integrated Windows server to the iSeries

To use a tape drive currently locked on an integrated server from OS/400, you must first unlock it from the integrated server and vary it on from OS/400. To unlock the tape drive from Windows server, you must either be the person who originally locked the drive or have Administrator or Backup Operator authority.

To transfer control of an iSeries tape drive from an integrated Windows server to iSeries, follow these steps:

1. Unlock the tape device from the integrated Windows server console.
 - a. Click **Start**, then **Programs**, then **IBM iSeries**, then **Integration for Windows Server**
 - b. Expand **Integration for Windows Server**
 - c. Expand the network server description name.
 - d. Select **iSeries Devices**.
 - e. Select the tape object that you want to lock.
 - f. Select **Action**, then **All Tasks**, then **Unlock Device**.
2. Make the device available to OS/400 from the OS/400 console.
 - From iSeries Navigator
 - a. Click **Configuration and Service** —> **Hardware** —> **Tape Devices**.
 - b. Click **Stand-Alone Devices** or **Tape Libraries**.
 - c. Right-click a device or library and select **Make Available**.
 - From the OS/400 command line interface
 - a. At the OS/400 command line, type `WRKCFGSTS *DEV *TAP`, and press Enter. The Work with Configuration Status display appears.
 - b. In the Opt column next to the tape drive device name (e.g., TAP01), type 1 to vary on the tape drive.
 - c. Press Enter and the tape drive varies on.
 - d. Change the tape to one formatted for OS/400.

Supported iSeries tape drives

Your ability to use iSeries tape drives from integrated Windows servers depends on tape device model, tape controller, and media type.

Refer to the iSeries Windows integration  web site to see which tape devices are supported.

Tape libraries are not supported as libraries, but they may be supported as single devices.

Manual and automatic modes are both supported on Auto Cartridge Facilities (ACF) and Auto Cartridge Loaders (ACL). If the ACL or ACF is in automatic mode the next tape will be loaded automatically if the backup application ejects the full tape. The Windows Backup Utility does this automatically with no user intervention. Veritas Backup Exec displays a dialog box that displays the following “Please remove the media from the drive, and respond OK.” Clicking **Respond OK** in this dialog box causes the backup to continue normally.

Identify iSeries tape devices for applications

Applications do not refer to tape devices by device description or hardware resource name as OS/400 does. Instead they show tape devices in one of three ways:

- Manufacture-feature-model number
- Device map
- Port-bus-target id-lun

If you need these values, do this:

1. On the integrated Windows server console, click **Start** —> **Programs** —> **Administrative Tools** —> **Computer Management**.
2. Click on **System Tools**.
3. Click on **Device Manager**.
4. Double-Click on **Tape Devices**.
5. Right-Click on a tape device.
6. Select **Properties**.
7. The properties box has two tabs, one marked **General** and one marked **Driver**. The General tab shows the OS/400 manufacture-feature-model number and the Bus Number, Target ID and LUN.

If all the tape devices on your iSeries are of different types, this information is enough to distinguish between them in Windows applications. If you have multiple tape devices of the same manufacture-feature-model number, you must experiment to determine which tape drive is which.

Transfer control of the iSeries tape and optical drives between integrated Windows servers

If you have multiple integrated servers only one at a time can use the iSeries tape or optical drive. To transfer control of tape and optical drives from one server to another, you must unlock it on one server and lock it on the other.

Note: If you have logical partitions on your iSeries, the tape and optical drive is allocated to a single partition and cannot be shared by integrated servers that are in other partitions.

To transfer control of an iSeries tape or optical drive between integrated servers, follow these steps:

On the integrated sever console that has control of the drive:

1. Click **Start**, then **Programs**, then **IBM iSeries**, then **Integration for Windows Server**
2. Expand **Integration for Windows Server**
3. Expand the network server description name.
4. Select **iSeries Devices**
5. Select the device that you want to unlock.
6. Select **Action**, then **All Tasks**, then **Unlock Device**


On the integrated server console that you want to give control, lock the tape or optical drive.

1. Click **Start**, then **Programs**, then **IBM iSeries**, then **Integration for Windows Server**
2. Expand **Integration for Windows Server**
3. Expand the **Network Server Description** name
4. Select **iSeries Devices**
5. Select the device that you want to lock.
6. Select **Action**, then **All Tasks**, then **Lock Device**.

Print from an integrated Windows server to iSeries printers

To send a print job to OS/400, you must set up the OS/400 printer for TCP/IP printing. You must also set up the integrated server to use that printer through the LPD/LPR protocol. Your integrated server must also have the **Microsoft TCP/IP Printing** Network Service installed. See the Windows documentation for more information about TCP/IP Printing.

To set up an integrated server to print to OS/400 printers, perform these tasks:

1. Set up the OS/400 printer for TCP/IP printing. For more information, see TCP/IP Configuration and Reference  .
2. Set up the integrated server to print to OS/400 printers:
 - a. From the **Start** menu on Windows 2000 Server or Windows Server 2003, click **Settings**, then **Printers**. The **Printers** window appears.
 - b. Double-click the **Add Printer** icon. The **Add Printer Wizard** starts.
 - c. Click the **Network Printer** button.
 - d. On the **Locate your Printer** panel, type the printer name or click **Next** to browse for the printer.

Chapter 10. Administer integrated Windows server users from OS/400


One of the main advantages of Windows environment on iSeries is synchronized, simplified user administration. Existing OS/400 user profiles and groups of profiles can be enrolled to integrated Windows servers, meaning that those users can log onto Windows server with the same user ID and password pair that they use to log onto OS/400. If they change their OS/400 password, their Windows password changes as well.

For conceptual information, read the article: “User and group concepts” on page 17.

Here are some tasks you can perform:

- “Enroll a single OS/400 user to the Windows environment using iSeries Navigator”
- “Enroll an OS/400 group to the Windows environment using iSeries Navigator” on page 100
- “Enroll OS/400 users to the Windows environment using the character-based interface” on page 100
- “Create user templates” on page 100
- “Specify a home directory in a template” on page 102
- “Changing the LCLPWDMGT user profile attribute” on page 102
- “Enterprise Identity Mapping (EIM)” on page 102
- “End user enrollment to the Windows environment” on page 104
- “End group enrollment to the Windows environment” on page 104
- “The QAS400NT user” on page 105
- “Preventing enrollment and propagation to an integrated Windows server” on page 107

Enroll a single OS/400 user to the Windows environment using iSeries Navigator


Create an OS/400 user profile for the user if one does not already exist. You can find information about creating OS/400 user profiles in the iSeries Security Reference .

To enroll a single user to the Windows environment, follow these steps:

1. In iSeries Navigator, expand **Network**—>**Windows Administration**—>**User Enrollment**.
2. Right-click an available Windows domain or server from the list and select **Enroll Users**.
Note: Do not select a Windows workgroup. Enrollment to a workgroup is not supported.
3. Select to enter the user name or choose the user name from the list.
4. (Optional) If you want to use a user template as a basis for user settings, specify a Windows user to use as a template when creating the user on Windows. Remember that if you change the user template after you enroll a user, the changes will not affect the user.
5. Click **Enroll**.

If you have problems enrolling users, see “Failures enrolling users and groups” on page 137.

Enroll an OS/400 group to the Windows environment using iSeries Navigator

This procedure enrolls all users in the OS/400 group to the Windows environment. You can find information about creating OS/400 user and group profiles in the iSeries Security Reference  .

To enroll an OS/400 group and its members to the Windows environment, follow these steps:

1. Expand **Network** —> **Windows Administration** —> **User Enrollment**.
2. Right-click an available Windows domain or server from the list and select **Enroll Groups**.
Note: Do not select a Windows workgroup. Enrollment to a workgroup is not supported.
3. Enter a group name or select an unenrolled group from the list.
4. (Optional) To use a template to create new users, specify a Windows user to use as a template when creating users in the group on Windows. If you change the user template after you enroll a user, the changes do not affect the user.
5. Select **Global** if the group is being enrolled in a domain and the group should be visible to the domain. Otherwise, select **Local** . Windows server local groups can contain users and Windows server global groups, while Windows server global groups can contain only users. See the Windows online help for more information about group types.
6. Click **Enroll**.

If you have problems enrolling groups, see “Failures enrolling users and groups” on page 137.

Enroll OS/400 users to the Windows environment using the character-based interface

Enroll users to the Windows environment

1. At the OS/400 character-based interface, type CHGNWSUSRA and press **F4**.
2. In the **User profile** field, type the name of the OS/400 user profile you want to enroll to the Windows environment.
3. Press **enter** twice. More fields should appear.
4. **Page down** and enter those Windows domains and Windows local servers you want to enroll the user to.
5. Press **enter** to accept the changes.

Table of relevant CL commands

Table 4.

WRKUSRPRF	Work with OS/400 user profiles.
WRKNWSENR	Work with OS/400 user profiles enrolled to the Windows environment.
CHGNSWUSRA	Enroll OS/400 users to the Windows environment.

Create user templates

A user enrollment template is a tool to help you enroll users from OS/400 to the Windows environment more efficiently. Rather than manually configuring many new users, each with identical settings, use a user enrollment template to automatically configure them. You can learn more about user enrollment templates at User Enrollment Templates.

Follow these steps to create a Windows template:

For a Windows 2000 Server or Windows Server 2003 domain:

1. At the integrated server console click **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Click the domain name.
3. Right-click **Users**, then select **New**→**User**.
4. In the **Username** and **Logon name** fields, enter a distinctive name for the template, such as *stduser* or *admtemp*. Click **Next**.
5. It is recommended that you also deselect the **User must change password at next logon** check box and select the **User cannot change password**, **Password never expires**, and **Account is disabled** checkboxes. This prevents anyone using the template account itself to access the integrated server.
6. Do not enter a password for a template account.
7. Click **Finish**.
8. To set up group memberships, double-click the template name in the list of domain users and groups that appear in the right pane. Click the **Member of** tab and then click **Add** to add the groups that you want.

For a Windows 2000 Server or Windows Server 2003 server:

1. From the integrated server console
 - In Windows 2000 Server click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
 - In Windows Server 2003 click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.
2. Select **System Tools** → **Local Users and Groups**.
3. Right-click **Users** and select **New User**.
4. In the **User name** field, enter a distinctive name for the template, such as *stduser* or *admtemp*.
5. It is recommended that you also deselect the **User must change password at next logon** check box and select the **Password never expires**, **User cannot change password**, and **Account is disabled** checkboxes. This prevents anyone using the template account itself to access Windows server.
6. Click **Create**, then **Close**.
7. Click **Users** or refresh to show the new user template.
8. To set up group memberships, double-click the template name in the list of domain users and groups that appears in the right pane. Click the **Member of** tab and then click **Add** to add the groups that you want.

You can make a user template a member of any Windows server group, whether you enrolled that group from OS/400 or not. You can enroll users with a template that is a member of a group that was not enrolled from OS/400. If you do this you can only remove users from the group by using the User Manager program on Windows server.

If you are creating a template that will be used to enroll administrators, you may want to make the template a member of the Windows server group *Administrators*. Likewise, if you want to protect Windows users from accidental deletion from OS/400, enroll the template in the *AS400_Permanent_Users* (or *OS400_Permanent_Users*) group.

Specify a home directory in a template

To allow Windows environment on iSeries to manage users in the most portable way possible, a home directory can be set up for each user to store user-specific information generated by applications. To minimize the amount of work that must be done, specify home directories in the template accounts so that each new profile created by the enrollment process has a home directory created for it automatically. To provide scalability, it is important not to lock home directories to a particular disk drive. Use the Universal Naming Convention (UNC) names to give portability.

To customize your template profiles to include a home directory, follow these steps from the integrated Windows server console:

1. Create the home directory folder on the appropriate server, and share it.
2. In a domain, click **Start->Programs->Administrative Tools->Active Directory Users and Computers** from the Windows server console. On a local server, click **Start->Programs->Administrative Tools-> Computer Management->Local Users and Groups**.
3. Double-click the template (model user) to display its properties.
4. Click the Profile tab.
5. In the Home folder segment, click **Connect**. Select a drive letter (such as Z:). Move to the **To:** dialogue, and enter the directory path of the home directory using a UNC name, for example: `\\iSeriesWin\homedirs\%username%`. In this example, **iSeriesWin** is the name of the server where the home directory folder resides, and **homedirs** is the name of the home directory folder. If you use the variable `%username%`, instead of the logon or user name, Windows server automatically substitutes the user's name in place of the variable name when each new Windows server account is created. It also creates a home directory for the user.

Changing the LCLPWDMGT user profile attribute

This article explains how to change the Local Password Management (LCLPWDMGT) user profile attribute. To read about the LCLPWDMGT attribute see "User and group concepts" on page 17 and "Types of user configurations" on page 19.

Follow this procedure in the OS/400 *character-based environment* to change the LCLPWDMGT user profile attribute.

1. Type CHGUSRPRF and the user profile name you want to change.
2. Press F4 to prompt.
3. Press **F9** to view all attributes and **F11** to view their abbreviations.
4. Find the attribute LCLPWDMGT and set it to *YES or *NO.
5. Press enter.

Enterprise Identity Mapping (EIM)

What is EIM?

Enterprise Identity Mapping (EIM) is a way to consolidate a user's various UserIDs and passwords together under a single account. Using it, a user can log on just once to a system, and then EIM will work together with other services behind the scenes to authenticate the user to all of his accounts.

This is called a single sign-on environment. Authentication still takes place whenever users attempt to access a new system; however, they will not be prompted for passwords. EIM reduces the need for users to keep track of and manage multiple user names and passwords to access other systems in the network. Once a user is authenticated to the network, the user can access services and applications across the enterprise without the need for multiple passwords to these different systems.

The Information Center has an entire topic devoted to EIM. See Enterprise Identity Mapping.

To learn the features of the different ways to enroll users to the Windows environment, see “Types of user configurations” on page 19.

The EIMASSOC user profile attribute

EIMASSOC is a user profile attribute specifically designed to aid in configuring EIM. At the OS/400 command prompt type CHGUSRPRF and the user profile name and then press F4 to prompt. Then page down to the very bottom and you will see a section labeled EIM association. Here is a summary of what the fields mean:

- **Element 1: EIM identifier** This is the UserID that EIM uses to identify you. Think of it as your Master ID under which all your other user IDs will be stored. If you specify *USRPRF the system will use your OS/400 user profile name as the EIM identifier. Alternatively, you can specify any valid character-string. If you enter *DLT in this field and press enter, you will be presented with a list of changed options for deleting EIM associations.
- **Element 2: Association type** This value specifies how the OS/400 user profile that you are editing will be associated with the EIM identifier. With Windows environment on iSeries, the values of *TARGET, *TGTSRC, or *ALL will allow auto-creation or deletion of OS/400 target and Windows source associations.
- **Element 3: Association action** The special values are:
 - *REPLACE The Windows source associations will be removed from all EIM identifiers that have an association for this user profile. For the enrolled user, a new Windows source association will be added to the specified EIM identifier.
 - *ADD For the enrolled user, a Windows source association will be added.
 - *REMOVE The Windows source association will be removed.
- **Element 4: Create EIM identifier** This value specifies whether the EIM identifier should be created if it does not already exist. The special values allowed are, *NOCRTEIMID, an EIM identifier will not be created, or, *CRTEIMID, an EIM identifier will be created if it does not exist.

Automatic and Manual EIM associations

In a typical EIM configured environment, which uses single sign-on, OS/400 target associations and Windows source associations are typically defined. With integrated Windows server user administration, the system administrator may decide to define enrolled Windows users to have EIM associations automatically defined. For instance, if an enrolled Windows user has EIMASSOC(*USRPRF *TARGET *ADD *CRTEIMID) specified, OS/400 will automatically create an OS/400 target and a Windows source association. The EIMASSOC information is not stored in the user profile. Also, this information is not saved or restored with the user profile. And, if the OS/400 system is not configured for EIM, then no association processing is done and the EIMASSOC information is ignored.

If OS/400 is configured to use EIM and EIMASSOC processing is defined for the enrolled user, integrated Windows server user administration will auto create or delete Windows source associations for the user in the Windows EIM registry. For a user enrolled locally to the Windows environment, the Windows EIM registry name is the fully qualified, local Domain Name System (DNS) name. The Windows EIM registry type is defined to be Windows 2000. For users enrolled to a Windows domain, the Windows registry name is the fully qualified domain DNS name and the Windows registry type is defined to be Kerberos - case ignore. If EIMASSOC is defined for a user, and OS/400 is configured to use EIM, and the Windows EIM registry doesn't exist, integrated Windows server user administration will create the Windows EIM registry.

Use EIM associations to allow different Windows user profile names

EIM provides a mechanism to associate user profiles in a directory system. EIM allows for an EIM identifier to have an OS/400 user profile target association defined and a Windows user profile source

association to be defined. It is possible for a user administrator to define a Windows source association using a different Windows user profile name than the OS/400 target association user profile name. Integrated Windows user administration will use the defined EIM Windows source association Windows user profile, if it exists, for Windows user enrollment. The OS/400 target association needs to be defined. Using the EIM identifier, the Windows source association needs to be defined by the administrator. The Windows source association needs to be defined for the same EIM identifier in the correct Windows EIM registry name and type. For a user enrolled locally to Windows, the Windows EIM registry name is the fully qualified, local domain name server (DNS) name. The Windows EIM registry type is defined to be EIM_REGTYPE_WIN2K. For users enrolled to a Windows domain, the Windows registry name is the fully qualified domain DNS name and the Windows registry type is defined to be EIM_REGTYPE_KERBEROS_IG.

End user enrollment to the Windows environment

To end the enrollment of a user to Windows environment domains and servers, follow these steps on the integrated Windows server console:

1. Expand **Network** —> **Windows Administration** —> **User Enrollment**.
2. Expand the domain or server that contains the user that you want to unenroll.
3. Select **Users**.
4. Right-click the user that you want to unenroll.
5. Select **Unenroll**.
6. Click **Unenroll** on the confirmation window.

Effects of ending user enrollment to the Windows environment

When you end user enrollment from the Windows environment, you also remove the user from the list of enrolled Windows server users, as well as from the Windows server group AS400_Users (or OS400_Users). Unless the user is a member of the Windows server group AS400_Permanent_Users (or OS400_Permanent_Users), you also delete the user from the Windows environment.

You cannot delete users who are members of the Windows server group AS400_Permanent_Users (or OS400_Permanent_Users) from Windows server by either ending enrollment or deleting them from OS/400. However, ending enrollment does remove the user from the list of enrolled Windows server users and from the Windows server group AS400_Users (OS400_Users).

You can keep users on the Windows environment after you have ended their enrollment on OS/400. We do not recommend this practice, however. This makes it possible to add these users to groups on OS/400 and change passwords on OS/400 without these updates ever appearing in the Windows environment. These discrepancies can make it difficult to keep track of users on either system.

You can end user enrollment in a number of ways. Actions that end user enrollment include the following:

- Intentionally ending enrollment for the user.
- Deleting the OS/400 user profile.
- Ending enrollment for all OS/400 groups to which the user belongs.
- Removing the user from an enrolled OS/400 group when the user does not belong to any other enrolled groups.

End group enrollment to the Windows environment

When you end enrollment of a group to the Windows environment, all users whose enrollment is limited to that group also have their enrollment ended. If the group has only members that were enrolled through it, the group is deleted from the Windows environment.

However, if the group has any members that were added from the Windows environment rather than enrolled from OS/400, the group is not deleted. The only members that the group can still have are nonenrolled users.

To end the enrollment of a group to Windows environment domains and servers, follow these steps in iSeries Navigator:

1. Expand **Network** —> **Windows Administration** —> **User Enrollment**.
2. Expand the domain or server that contains the group that you want to unenroll.
3. Select **Groups**.
4. Right-click the group that you want to unenroll.
5. Select **Unenroll**.
6. Click **Unenroll** in the confirmation window.

The QAS400NT user

You need to set up the QAS400NT user in order to successfully enroll an OS/400 user or group profile on a domain or local server in the following cases:

- You are enrolling on a domain through a member server.
- You are enrolling on a local server using a template which specifies a home directory path, as is discussed in the section “Specify a home directory in a template” on page 102).
- You are enrolling on a domain through an OS/400 partition which contains both domain controllers and member servers on the same domain.

You do not need to set up the QAS400NT user in order to successfully enroll an OS/400 user or group profile on a domain or local server in the following cases:

- You are enrolling on a domain through an OS/400 partition which contains a domain controller but no member servers on the same domain.
- You are enrolling on a local server (or locally on a member server) using a template which does not specify a home directory path.

If you need to set up the QAS400NT user, follow these steps:

1. Create the QAS400NT user profile on OS/400 with User class *USER. Take note of the password because you need it in the next step. Make sure that the password complies with the rules for Windows passwords if you are enrolling on a domain. See “Password considerations” on page 21.
2. Create the QAS400NT user account on the Windows console of the integrated Windows server you are enrolling through. Note that the OS/400 user profile password and Windows user account password must be the same for the QAS400NT user.

- a. Setting up QAS400NT on a domain controller

On the domain controller of the domain you are setting up enrollment for, create the QAS400NT user account as follows:

- 1) From the integrated server console

- a)

- In Windows 2000 Server click **Start** —> **Programs** —> **Administrative Tools** —> **Computer Management** —> **Local Users and Groups**.
- In Windows Server 2003 click **Start** —> **Programs** —> **Administrative Tools** —> **Computer Management** —> **System Tools** —> **Local Users and Groups**.

- b) Select **System Tools** —> **Local Users and Groups**.

- 2) Right-click the **Users** folder (or the folder that the user belongs to), and select **New** —> **User...**

- 3) Enter the following settings:

Full name: qas400nt
User logon name: qas400nt

4) Click Next. Enter the following settings:

Password: (the same password as you used for QAS400NT on OS/400)

Deselect: User must change password at next logon

Select: User cannot change password

Select: Password never expires

5) Click Next, then Finish

6) Right click the QAS400NT user icon and select Properties.

7) Click the **Member Of** tab and then Add.

8) Enter Domain Admins in the box and click OK, then OK again. This gives the QAS400NT user account sufficient rights to create users.

b. Setting up QAS400NT on a local server

On the local server (or member server if you are enrolling locally) you are setting up enrollment for, create the QAS400NT user account as follows:

1) From the integrated server console

- In Windows 2000 Server click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.

- In Windows Server 2003 click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.

2) Right-click the **Users** folder, and select **New User...**

3) Enter the following settings:

User name: qas400nt

Full name: qas400nt

Password: (the same password as you used for QAS400NT on OS/400)

Deselect: User must change password at next logon

Select: User cannot change password

Select: Password never expires

4) Click Create, then Close.

5) Right click the QAS400NT user icon and select Properties.

6) Click the Member Of tab and then Add.

7) Enter Administrators in the box and click OK, then OK again. This gives the QAS400NT user account rights to the User Administration Service.

3. Enroll the OS/400 QAS400NT user profile on the domain or local server using iSeries Navigator or the CHGNWSUSRA command. Refer to: "Enroll a single OS/400 user to the Windows environment using iSeries Navigator" on page 99, for a description of how to do this. Do not try to use a template when enrolling QAS400NT.

4. Use iSeries Navigator or the WRKNWSENK command to confirm that QAS400NT has been successfully enrolled. You may now enroll OS/400 user profiles through domain controllers or member servers on the domain.

Notes:

- You may change the QAS400NT password from OS/400 since it is now an enrolled user.
- If there are multiple integrated servers that belong to different domains on a single OS/400 partition, you must set up QAS400NT for each domain. All QAS400NT user accounts must have the same password as the OS/400 user profile. Alternatively, consider using Active Directory or trust relationships between domains, and enroll users on only a single domain.
- If you have multiple OS/400 partitions and multiple integrated servers, QAS400NT passwords on different OS/400 partitions can be different as long as each domain does not contain integrated servers on more than one OS/400 partition. The rule is, all OS/400 QAS400NT user profiles and corresponding Windows user accounts must have the same password for a single domain.
- Be sure not to delete the QAS400NT user profile on OS/400, or let the password expire. To minimize the risk of the QAS400NT password expiring on one of multiple OS/400 partitions on the same Windows domain, it is recommended that you allow only one OS/400 partition to propagate changes to

the QAS400NT user profile. Refer to “Preventing enrollment and propagation to an integrated Windows server,” for a description of how to do this.

- If you have multiple OS/400 partitions, each with an integrated Windows server on the same domain, failing to keep the QAS400NT password synchronized across all OS/400 partitions can cause enrollment problems. To minimize this problem, we recommend that you limit propagation of changes to the QAS400NT password to just one OS/400 partition, but still allow other partitions to keep sufficient authority to enroll users. Then, failure to change a password on one of the other partitions prevents user enrollment from that partition only. Refer to “Preventing enrollment and propagation to an integrated Windows server,” for a description of how to do this.

Preventing enrollment and propagation to an integrated Windows server

There are several reasons why you might want to prevent OS/400 user profile propagation to a particular integrated server:

- If there are multiple integrated servers that belong to the same domain, and they are all on the same OS/400 partition, user profile enrollment will, by default, go through all of the integrated servers in that partition. To reduce network traffic you can turn off enrollment to all integrated servers on the domain except one. This single integrated server would normally be the domain controller, if it is in the partition.
- If there are multiple integrated servers that belong to the same domain, but they are all on different OS/400 partitions, there is a risk of the QAS400NT passwords getting out of synchronization and causing problems with user profile enrollment. By preventing propagation of the QAS400NT user profiles from all OS/400 partitions except one, you can reduce the risk of enrollment problems. Notice that the other OS/400 partitions keep sufficient authority to enroll users. Then, failure to change a password on one of the other partitions prevents user enrollment from that partition only.

There are two methods to prevent OS/400 user profile propagation to a particular integrated server:

- Use the Propagate Domain User (PRPDMNUSR) parameter. See below for a description of how to do this.
- Create data areas with the Create data area (CRTDTAARA) command. See below for a description of how to do this.

Using the PRPDMNUSR parameter to prevent enrollment to a domain through a specific integrated server

The Propagate domain user (PRPDMNUSR) parameter of the Change network server description (CHGNWSD) command can be used to prevent user enrollment to a domain through a specific integrated server. You can also set this parameter when installing an integrated server using the Install Windows Server (INSWNTSVR) command. This option may be useful in the case where there is a single OS/400 partition which controls multiple integrated Windows servers that belong to the same domain, because it can turn off enrollment for all integrated servers except one.

To use the PRPDMNUSR parameter to prevent user enrollment, proceed as follows:

1. Using the Work with Network Server Description (WRKNWSD) command, select the integrated server you wish to stop enrollment on. (You do not need to vary off the server.)
2. Enter the command: CHGNWSD NWSD(nwsdname) PRPDMNUSR(*NO)

Notes:

- Do not turn enrollment off for all of the integrated servers on the domain. Otherwise all your users may go to update pending (*UPDPND) status, and no further propagation takes place.
- You may want to leave two integrated servers enabled for user enrollment so that you can still make changes if one of the servers is down.

Using the CRTDTAARA command to prevent enrollment of QAS400NT to a specific integrated server

The Create Data Area (CRTDTAARA) command can be used to prevent enrollment of the QAS400NT user profile only, for the specified integrated server. The propagation of other user profiles is not affected. This option may be useful in the case where there are multiple integrated servers that belong to the same domain, but they are all on different OS/400 partitions. You want to enroll user profiles from these different OS/400 partitions, but not have multiple QAS400NT user profiles propagating passwords to the domain. Follow these steps:

1. Choose one OS/400 partition that you wish to use for enrollment of QAS400NT on the domain. Ensure that QAS400NT is enrolled on this OS/400 partition.
2. If QAS400NT is enrolled on other OS/400 partitions follow these steps:
 - a. On the domain controller, add the QAS400NT user account to the OS400_Permanent_Users group to ensure that it is not deleted.
 - b. On the OS/400 partitions where you want to prevent enrollment of QAS400NT, delete the QAS400NT user profile.
3. On the OS/400 partitions where you want to prevent enrollment of QAS400NT, create a data area with this command:

```
CRTDTAARA DTAARA(QUSRSYS/nwsdnameAU) TYPE(*CHAR) LEN(10) VALUE( *NOPROP )
```

where **nwsdname** is the name of the network server description for the integrated server, and ***NOPROP** is the keyword that signals that QAS400NT user profile parameters (including the password) are not propagated from this OS/400 partition.

4. Create and enroll the QAS400NT user profile on each of the OS/400 partitions you created the data area on. Notice that you still need to keep the QAS400NT password current (not expired) on all these OS/400 partitions for enrollment of user profiles (other than QAS400NT) to occur. Because the QAS400NT password is not propagated, it does not matter what the password is, as long as it is not expired.


Chapter 11. Back up and recover integrated Windows servers

Because Windows environment on iSeries combines two operating systems (Windows 2000 Server or Windows Server 2003 with OS/400), you can use either OS/400 or Windows server utilities or a combination of both to manage backups. When you are planning your backup strategy, refer to the Backup and recovery topic, as well as Microsoft documentation.

To back up an integrated server on iSeries, you have these basic options:

- Do a full system backup on your OS/400. See the topic [Back up your server](#).
- Back up the network server description (NWSD) and the disk drives that are associated with the integrated server on iSeries. See “Back up the NWSD and disk drives associated with an integrated Windows server.”
- Back up individual integrated server files by using the OS/400 SAV and RST commands and OS/400 NetServer or a backup utility. See “Back up individual integrated Windows server files and directories” on page 115.

Your recovery options depend on how you backed up your system, as well as what you need to recover.

- If you need to recover your entire system, refer to the book [Backup and Recovery](#) .
- If you need to restore a network server description and its associated OS/400 disk drives, refer to “Restore an integrated Windows server’s NWSD and disk drives” on page 119.
- To restore integrated server data (files, directories, shares, and the Windows registry) that you backed up with the Save (SAV) command, see “Recover integrated Windows server files” on page 122.
- To restore files that you saved with Windows backup utilities or other utilities, use those utilities.

Back up the NWSD and disk drives associated with an integrated Windows server

When you install an integrated server, OS/400 creates a network server description and predefined disk drives for your server that you need to back up. See “Predefined disk drives for integrated Windows servers” on page 85. Some of the disk drives are system-related (the installation and system drives); others are user-related. Because Windows server considers them a unified system, you need to save all the disk drives and the network server description to restore properly.

The Microsoft Windows operating system and the files that are required to start the integrated server are located on the C and D drives of the server (or C, D, and E drives for servers created before V4R5). Windows environment on iSeries allows you to save and restore these drives as OS/400 network server storage space objects. These objects are saved as part of the OS/400 system when you perform a full OS/400 system backup. You can also specifically save the network server description and associated storage spaces. Daily backup of the system drive is a good idea.

Saving storage spaces is the fastest but least flexible method for backing up your integrated server because you cannot restore individual files. Alternatively, you can back up specific individual files and directories to eliminate the BOOT disk, RDISK, and registry backups that you would take with a PC-based Windows server. See “Back up individual integrated Windows server files and directories” on page 115.

To back up the network server description and the disk drives that are associated with integrated servers, see these topics:

- “Back up the NWSD of an integrated Windows server” on page 110.
- “Back up predefined disk drives for integrated Windows servers created on V4R5 and later OS/400 systems” on page 110.

- “Back up predefined disk drives for integrated Windows servers created on pre-V4R5 OS/400 systems” on page 111.
- “Back up user-defined disk drives for an integrated Windows server” on page 112.
- “Save and restore user enrollment information” on page 112.
- You can see a table of user objects and system objects that you “What objects to save and their location on OS/400” on page 113.

Back up the NWSD of an integrated Windows server

When you save the storage space objects that are associated with an integrated Windows server, you also need to save the Network Server Description (NWSD). Otherwise, Windows server may not be able to re-establish items such as Windows server File System permissions. To save an NWSD, you use the Save Configuration (SAVCFG) command:

1. On the OS/400 command line, type SAVCFG.
2. Press Enter to have OS/400 save the NWSD configuration.

Note: The Save Configuration (SAVCFG) command will save the objects associated with an NWSD and the current static network server storage spaces. It does not save the links associated with the dynamically added storage spaces. These will need to be added manually once the configuration and the dynamically linked storage spaces have been restored.

Back up predefined disk drives for integrated Windows servers created on V4R5 and later OS/400 systems

When you install an integrated server on V4R5 and later systems, OS/400 creates the system and installation source (C and D) drives as predefined drives that you need to save. See “Predefined disk drives for integrated Windows servers” on page 85.

Note: Treat a network server description (NWSD) of type *WINDOWSNT, its predefined disk drives, and any user-defined disk drives linked to it as a unit. Save and restore them at the same time. Together they constitute a complete system, and should be treated as such. Otherwise, the integrated server may not be able to re-establish items such as Windows server File System permissions.

To save disk drives (network server storage spaces) that are in the system disk pool (ASP) on OS/400, do this:

1. If you are saving to tape, ensure that you have mounted a tape that is formatted for OS/400.
2. Shut down the integrated server to prevent users from updating files during the backup. See “Start and stop an integrated server” on page 75.
3. On the OS/400 command line, type SAV and press F4.
4. If you are saving the storage space to tape, specify the name of your tape device (for example, /QSYS.LIB/TAP01.DEVD) in the *Device* field.

If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device. For example, to use a save file named MYSAVF in library WINBACKUP, you would specify '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' for the device.

5. In the Name field under Objects:, specify '/QFPNWSSTG/stgspc', where stgspc is the name of the network server storage space.
 - For the system (C) drive, use /QFPNWSSTG/nwsdname1.
 - To save the D drive, use /QFPNWSSTG/nwsdname2.
 - For storage spaces created in a user disk pool, use /QFPNWSSTG/stgspc and also dev/QASPnn/stgspc.UDFS, where stgspcis the name of the network server storage space and nnis the number of the user disk pool.

- For an independent disk pool, use /QFPNWSSTG/stgspc and also dev/independent ASP name/stgspc.UDFS, where independent ASP name is the name of the independent disk pool and stgspc is the name of the network server storage space.
6. Specify values for any other parameters that you want and press Enter to save the storage space.
 7. Then, start the integrated server. See “Start and stop an integrated server” on page 75.

You can read more here: “What objects to save and their location on OS/400” on page 113.

Back up predefined disk drives for integrated Windows servers created on pre-V4R5 OS/400 systems

Integrated Windows servers created on pre-V4R5 systems have C, D, and E as predefined drives. See “Predefined disk drives for integrated Windows servers” on page 85. The files that contain these drives are in library QUSRSYS. If the system drive (E drive) is larger than 1007 megabytes, that data goes into a user storage space, which you also need to back up. Even after you migrate your system to V4R5, these drives remain where they were created unless you reinstall Windows server.

Note: Treat a network server description (NWS) of type *WINDOWSNT, its predefined disk drives, and any user-defined disk drives linked to it as a unit. Save and restore them at the same time. To Windows server, they are a full system, and should be treated as such. Otherwise, Windows server may not be able to re-establish items such as Windows server File System permissions.

To save the disk drives for these NWSs, use the Save Object (SAVOBJ) command:

1. If you are saving to tape, ensure that you have mounted a tape that is formatted for OS/400.
2. Shut down the integrated server to prevent users from updating the files while you are saving them. See “Start and stop an integrated server” on page 75.
3. On the OS/400 command line, type SAVOBJ and press F4.
4. In the Objects field, specify the *nwsdname*.
5. In the Library field, specify QUSRSYS.
6. If you are saving the storage space to tape, specify the name of your tape device in the Device field (for example, TAP01). If you want to use a save file instead of tape, specify *SAVF as the device and enable the data compression option.
7. For Object type, specify *SVRSTG.
8. If you are using a save file, press F10 to see additional parameters.
9. In the Save file field, specify the path to your save file (for example *winbackup/svrstg3*).
10. If you are using a save file, page down twice and change the value for Data compression to *YES.

If the system drive (E drive) is larger than 1007 megabytes, to save the data that goes into a user storage space, you use the Save (SAV) command:

1. On the OS/400 command line, type SAV and press F4.
2. If you are saving the storage space to tape, specify the name of your tape device (for example, /QSYS.LIB/TAP01.DEVD) in the *Device* field.

If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device. For example, to use a save file named MYSAVF in library WINBACKUP, you would specify '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' for the device.

3. In the Name field under Objects:, specify '/QFPNWSSTG/nwsdname3', where *nwsdname* is the name of the network server storage space.
4. Specify values for any other parameters that you want and press Enter to save the storage space.
5. Start the integrated server. See “Start and stop an integrated server” on page 75.

Back up user-defined disk drives for an integrated Windows server

The disk drives that you create for your integrated servers are in the integrated file system. To save these storage spaces from the user disk pool (ASP) on OS/400, you use the Save (SAV) command.

Note: Treat a network server description (NWSD) of type *WINDOWSNT, its predefined disk drives, and any user-defined disk drives linked to it as a unit. Save and restore them at the same time. They constitute a full system and should be treated as such. Otherwise, the integrated server may not be able to re-establish items such as Windows server File System permissions.

To save disk drives in a user disk pool (ASP) on OS/400, do this:

1. If you are saving to tape, ensure that you have mounted a tape that is formatted for OS/400.
2. For network server storage spaces created in an independent disk pool, verify that the auxiliary storage pool (ASP) device is varied on prior to saving the 'dev/independent ASP name/stgspc.UDFS' object.
3. Shut down the integrated server by varying off the network server description to prevent users from updating files during the backup. See "Start and stop an integrated server" on page 75.
4. On the OS/400 command line, type SAV and press F4.
5. If you are saving the storage space to tape, specify the name of your tape device (for example, /QSYS.LIB/TAP01.DEVD) in the *Device* field.

If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device. (For example, to use a save file named MYSAVF in library WINBACKUP, you would specify: '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE') for the device.) Otherwise, use the name of your device (for example, /QSYS.LIB/TAP01.DEVD).


6. In the *Name* field under *Objects:*, specify '/QFPNWSSTG/stgspc' and also 'dev/QASPnn/stgspc.UDFS', where stgspc is the name of the network server storage space and xx is the number of the disk pool.
 - For storage spaces created in a user disk pool, use /QFPNWSSTG/stgspc and also dev/QASPnn/stgspc.UDFS, where stgspc is the name of the network server storage space and xx is the number of the user disk pool.
 - For an independent disk pool, use /QFPNWSSTG/stgspc and also dev/independent ASP name/stgspc.UDFS where independent ASP name is the name of the independent disk pool and stgspc is the name of the network server storage space.
7. Specify values for any other parameters that you want and press Enter to save the storage space.
8. Start the Windows server. See "Start and stop an integrated server" on page 75.

You can find more information about backing up system objects and the appropriate save commands in Backup, recovery, and availability.

The method that is described above allows you to back up and recover entire network server storage spaces. To back up and recover individual files, you can use the new function: "Back up individual integrated Windows server files and directories" on page 115.

Save and restore user enrollment information

In some situations, you may need to restore user profiles and their enrollment information. The following information describes the OS/400 commands and API to save and restore user profiles used for integrated Windows server enrollment. More OS/400 backup and recovery security information may be found in the

Backup and Recovery of Security Information section in the iSeries Security Reference .

User profiles may be saved using the SAVSECDTA command or the QSRSAVO API. The OS/400 system value QRETSVRSEC must be set to 1 for integrated Windows server enrollment support. User profiles saved with the SAVSECDTA command or QSRSAVO API may be restored using the RSTUSRPRF command and specifying the parameter USRPRF(*ALL). If the parameter USRPRF(*ALL) is not specified, then user profiles may be restored if the parameter and value SECDTA(*PWDGRP) is specified.

If you save user profiles using the QRSAGO API, and a previous target release value is used, the user profile enrollment definitions will not be restored. After restoring the user profiles, the enrollment needs to be defined. Use iSeries Navigator or the Change Network Server User Attributes (CHGNWSUSRA) command to define the enrollment.

User profiles need to be saved and restored using the above methods for integrated Windows server enrollment. User profiles saved and restored using other commands or API are not supported for Windows.

What objects to save and their location on OS/400

Many objects are created as a result of installing Windows environment for iSeries. Some of these objects are system-related, others user-related. You need to save them all if you want to restore properly. You can save these objects by using options of the OS/400 GO SAVE command. Option 21 saves the entire system. Option 22 saves system data. Option 23 saves all user data (which includes objects in QFPNWSSTG).

If you want to save a particular object, use one of the following tables to see the location of that object on OS/400 and the command to use. The topic "Manually saving parts of your system" has more information about using the save commands. In addition to saving the entire drive (storage space), you can also save and restore individual files and directories. See "Back up individual integrated Windows server files and directories" on page 115.

For integrated Windows servers created on V4R5 and later systems

Object content	Object name	Object location	Object type	Save command
Integrated server boot and system drive	nwsdname1	/QFPNWSSTG	Predefined network server storage spaces in system disk pool (ASP)	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/nwsdname1') DEV('/QSYS.LIB/TAP01.DEVD')
Integrated server boot and system drive	nwsdname1	/QFPNWSSTG	Predefined network server storage spaces in user disk pool	SAV OBJ('/QFPNWSSTG/nwsdname1') ('/dev/QASPnn/nwsdname1.UDFS')) DEV('/QSYS.LIB/TAP01.DEVD')
Integrated server installation source drive	nwsdname2	/QFPNWSSTG	Predefined network server storage space in system disk pool	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/nwsdname2') DEV('/QSYS.LIB/TAP01.DEVD')
Integrated server installation source drive	nwsdname2	/QFPNWSSTG	Predefined network server storage spaces in user disk pool	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/nwsdname2') ('/dev/QASPnn/nwsdname2.UDFS')) DEV('/QSYS.LIB/TAP01.DEVD')
Integrated server installation source drive	nwsdname2	/QFPNWSSTG	Predefined network server storage spaces in an independent disk pool (ASP)	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/nwsdname2') ('dev/independent ASP name/nwsdname2.UDFS')) DEV('/QSYS.LIB/TAP01.DEVD')

For integrated Windows servers created on pre-V4R5 systems

Object content	Object name	Object location	Object type	Save command
Integrated server boot drive	nwsdname1	QUSRSYS	Predefined server storage space	GO SAVE, option 21 or 23 SAVOBJ OBJ(nwsdname1) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*SVRSTG)
Integrated server installation source drive	nwsdname2	QUSRSYS	Predefined server storage space	GO SAVE, option 21 or 23 SAVOBJ OBJ(nwsdname2) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*SVRSTG)
Integrated server system drive	nwsdname3	QUSRSYS	Predefined server storage space	GO SAVE, option 21 or 23 SAVOBJ OBJ(nwsdname2) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*SVRSTG)

Object content	Object name	Object location	Object type	Save command
Integrated server system drive	nwsdname3	/QFPNWSSTG	Predefined network server storage space used for system drives larger than 1007 MB	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/nwsdname3') DEV('/QSYS.LIB/TAP01.DEVD')

For all integrated Windows servers

Object content	Object name	Object location	Object type	Save command
User data and applications	Various	/QFPNWSSTG	User-defined network server storage spaces in system disk pool	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/stgspc') DEV('/QSYS.LIB/TAP01.DEVD')
User data and applications	Various	/QFPNWSSTG	User-defined network server storage spaces in user disk pool	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/stgspc') ('/dev/QASPnn/stgspc.UDFS')) DEV('/QSYS.LIB/TAP01.DEVD')
User data and applications	Various	/QFPNWSSTG	User defined network server storage spaces in an independent disk pool	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/stgspc') ('dev/independent ASP name/stgspc.UDFS')) DEV('/QSYS.LIB/TAP01.DEVD')
Messages from the integrated server	Various	Various	Server message queue	GO SAVE, option 21 or 23 SAVOBJ OBJ(msgq) LIB(qlibrary) DEV(TAP01) OBJTYPE(*MSGQ)
OS/400 config objects for integrated servers	Various	QSYS	Device config objects	GO SAVE, option 21, 22, or 23 SAVCFG DEV(TAP01)
Various	Various	All QUSRSYS	Various	GO SAVE, option 21 or 23 SAVLIB LIB(*NONSYS) or LIB(*ALLUSR)
OS/400 based IBM iSeries Integration for Windows Server code	QNTAP	QSYS	Library	GO SAVE, option 21 or 22 SAVLIB LIB(*NONSYS) or LIB(*IBM)

Object content	Object name	Object location	Object type	Save command
Windows-based IBM iSeries Integration for Windows Server code	NTAP and subdirectories	/QIBM/ProdData/NTAP	Directory	GO SAVE, option 21 or 22 SAV
Windows server file shares	QNTC and subdirectories	/QNTC/servername/sharename	Directory	GO SAVE, option 21 or 22 SAV
OS/400 TCP interfaces	QATOCIFC	QUSRSYS	physical file	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*MSGQ)
OS/400 TCP interfaces	QATOCLIFC	QUSRSYS	logical file	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*MSGQ)

Back up individual integrated Windows server files and directories

IBM iSeries Integration for Windows Server allows you to save integrated server data (files, directories, shares, and the Windows registry) to tape or disk along with other OS/400 data and restore the data on an individual basis. However, you should not use this approach as your primary backup procedure. You should still periodically save your entire system and the NWSD associated with your Windows server for disaster recovery. Then you can choose to do daily backups of only the integrated server files that have changed. See “Back up the NWSD and disk drives associated with an integrated Windows server” on page 109.

For information on the new file-level backup function, see these topics:

- First read “File-level backup restrictions.”
- To do file-level backup of your integrated server, you must first refer to: “Preliminary administrator setup tasks” on page 116.
- “Save your files” on page 118

You can also use a utility such as the Backup program that comes with Windows (see “Windows Backup utility” on page 119) or the Tivoli® Storage Manager to back up your integrated server files. You can find information about Tivoli Storage Management Solutions on the Tivoli Storage Management Solutions Web

Page. 

File-level backup restrictions

When you use the file-level backup, you need to be aware of the following limitations and restrictions:

Limitations:

- This support is not available to a network-connected Windows servers because the code comes packaged with IBM iSeries Integration for Windows Server.
- This method does not back up files that are part of the IBM iSeries Integration for Windows Server code.
- You cannot stop users from signing-on and accessing data on the server while the Save (SAV) or Restore (RST) command is running. IBM iSeries Integration for Windows Server can save a file that is in use as long as it can read the file. Consequently, you should back up integrated server files when you expect few users to be accessing the system. A note telling users to avoid accessing the server would be a good precaution.

- The QSECOFR user profile should not be used to perform a file-level backup. Even if enrolled to the integrated server, QSECOFR will not be used to back up the files. The Windows Local System Account will be used instead. It may not have the necessary authority to back up all of the requested files.
- If the user profile *LCLPWDMGMT value is *YES, then the system value, QRETSVRSEC, must be set to 1 and the user password must be changed or the user have signed-on after QRETSVRSEC was changed.
- If the user profile *LCLPWDMGMT value is *NO, then network authentication (kerberos) is used. The user must access the iSeries operation through an EIM enabled application (like iSeries Navigator single-signon). See “SBMNWSCMD and file level backup support for Kerberos v5 and EIM” on page 81 for more information.

Requirements:

- The integrated server must be active and have a working TCP/IP private (Internal or virtual Ethernet Point-to-Point) LAN connection with OS/400. You must back up your integrated server files either before putting the system into restricted state to back up the rest of the OS/400 files or after completing restricted state operations.
- This procedure requires that you have the same userID and password on the integrated server and OS/400.
- Your integrated server user account must be a member of the Administrators group.
- File-level backup uses the QNTC file system (NetClient) to build the list of files to be saved. QNTC uses iSeries NetServer to locate servers in the domain. You need to have the iSeries NetServer in the same domain (see “Ensure iSeries NetServer and the integrated Windows server are in same domain” on page 117) as the integrated server from which you are going to save files.
- Be careful about trying to restore all files on all drives that you previously saved through the QNTC file system. Certain Windows system files (for example, files in the Recycle Bin) can cause unexpected results after you restore them.
- On Windows 2000 Server or Windows Server 2003, you need to give special consideration to System File Protection when you are backing up and recovering Windows system files. Refer to Microsoft documentation.

Preliminary administrator setup tasks

Before you can back up your integrated Windows server files at file-level, you must do some preliminary setup tasks:

1. Ensure that the person who is saving and restoring files has the same password on OS/400 and the integrated server. The easiest method is found at “Enroll a single OS/400 user to the Windows environment using iSeries Navigator” on page 99. Also ensure that the user is a member of the Administrators group. Refer to “Create user templates” on page 100.
2. Create shares for each drive or volume that you want to save when you request to save all the files on a Windows server. IBM iSeries Integration for Windows Server accesses the file system and translates these shares into path-names. See “Create shares on integrated Windows servers.”
3. Add members to the QAZLCSAVL file in QUSRSYS that lists the share names that you want to be able to save. See “Add members to QAZLCSAVL file” on page 117.
4. Ensure that iSeries NetServer is in the same domain as the integrated server for which you want to save files. See “Ensure iSeries NetServer and the integrated Windows server are in same domain” on page 117.

Create shares on integrated Windows servers

To enable file-level backup and restoration of integrated server files on OS/400, create a share over each directory that contains data you want to save. To create shares on integrated servers, do this from the integrated server console:

1. Open the **My Computer** icon to bring up **Windows Explorer**.
2. Right-click on the drive or volume that you want.

3. From the pop-up menu, select **Sharing**.
4. Click **Share this folder**. Provide a **Share Name** (characters in the share name must be in the more restrictive code page 500 character set). The default share name is the same as the last part of the directory name. Share names can be no longer than 12 characters and can include embedded blanks.
5. You can choose unlimited access or limit the number of users who can access the share at one time. You can also use the **Permissions** button to set up the level at which you want to share (No Access, Read, Change, or Full Control).
6. Click on **Apply** to create the share.

Add members to QAZLCSAVL file

To enable file-level backup and recovery from OS/400, add a member for each integrated Windows server to the QAZLCSAVL file in QUSRSYS. For the member name, use the NWSD name of the server (*nwsdname*).

To add a member, do this:

1. On the OS/400 command line, type:


```
ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(nwsdname)
      TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE)
```
2. In the file member that you just created, list all the shares that you want to be able to save. List each share name that you defined for the server on a separate line. The maximum length that the Windows share name can be is 12 characters. Share names can have embedded blanks. For example, if you defined cshare, dshare, eshare, fshare, gshare, and my share as shares on WINSVR1, your member name WINSVR1 would look like this:

```

                                QUSRSYS/QAZLCSAVL
                                WINSVR1

0001.00  cshare
0002.00  dshare
0003.00  eshare
0004.00  fshare
0005.00  gshare
0006.00  my share
```

Note: If you specify multiple share names that point to the same integrated server directory, OS/400 saves the data multiple times for a "save all" request. To avoid duplicating data when you save it, do not include multiple shares that include the same directory or data.

Ensure iSeries NetServer and the integrated Windows server are in same domain

To save integrated server files for file-level backup, you must have iSeries NetServer in the same domain as the files you want to save.

1. Check the domain for your integrated server:
 - a. In iSeries Navigator, select **Network**—> **Windows Administration** —> **Integrated xSeries Servers**.
 - b. Find your integrated server in the list in the right pane; then look in the Domain column to find the domain for that server.
2. Check the domain for iSeries NetServer:
 - a. In iSeries Navigator, select **Network** —> **Servers** —> **TCP/IP**.
 - b. Find iSeries NetServer in the list of TCP/IP servers.
 - c. Right-click on **iSeries NetServer**, and pick **Properties** (or double-click on **iSeries NetServer**, then select **File**, then **Properties**). The domain name for iSeries NetServer appears under the **General** information file tab.
3. If iSeries NetServer is not in the same domain as the integrated server, change the domain for iSeries NetServer:
 - a. Click the **Next Start** button.
 - b. In the **Domain name** field, type the name of the Windows server domain.

- c. Stop and start iSeries NetServer (right-click on iSeries NetServer and pick **Stop**, then **Start**.)

Save your files

After you finish the necessary preliminaries (see “Preliminary administrator setup tasks” on page 116), you are ready to back up integrated server files on OS/400. To be able to restore a directory or file by share name, you must specify that file or share name specifically on the SAV command.

Note: To avoid duplicating data, be careful specifying what you want to save on the SAV command. If you specify multiple share names that point to the same directory on the integrated server, OS/400 saves the data multiple times.

To specify what you want OS/400 to save, do this:

1. Ensure that the integrated server is active (described in “Start and stop an integrated server” on page 75). Also ensure that the QSYSWRK subsystem, QSERVER, and TCP/IP are active (you can do this by using the Work with Active Jobs (WRKACTJOB) command).
2. On the OS/400 command line, type SAV and press F4.
3. In the Device field, specify the device on which you want OS/400 to save the data. For example, 'QSYS.LIB/TAP01.DEVD' saves the data to tape.
4. In the Object field, specify what you want OS/400 to save in the form '/QNTC/*servername*/*sharename*'. You can use wildcard characters. Refer to “Examples: How to address parts of an integrated Windows server” for how to specify particular parts of the integrated server.
5. Use the Directory subtree field to specify whether you want to save subtrees under a directory. The default is to save all directories.
6. To specify that you want to save changes since the last save, specify *LASTSAVE in the Change period field. You can also specify a specific range of dates and times.
7. Press Enter to save the shares that you specified.

Examples: How to address parts of an integrated Windows server

These examples show how to refer with the SAV or RST commands to specific parts of an integrated server for a server that is named *server1*:

To save or restore this:	Specify this:
All integrated server objects.	OBJ('/QNTC/*') SUBTREE(*ALL)
All objects for <i>server1</i> .	OBJ('/QNTC/ <i>server1</i> /*') SUBTREE(*ALL)
All objects for <i>server1</i> that changed since you last saved the files.	OBJ('/QNTC/ <i>server1</i> /*') SUBTREE(*ALL) CHGPERIOD(*LASTSAVE)
All objects for <i>server1</i> that changed during a certain period (in this case between 10/19/99 and 10/25/99).	OBJ('/QNTC/ <i>server1</i> /*') SUBTREE(*ALL) CHGPERIOD('10/19/99' '00:00:00' '10/25/99' '23:59:59')
All directories, files, and shares to which a particular share (for example, 'fshare') refers. OS/400 does not save and restore the directory over which the share is built.	OBJ('/QNTC/ <i>server1</i> /fshare/*') SUBTREE(*ALL)
Only files to which the specified share (for example, 'fshare') refers that match the specified pattern (<i>pay*</i>). OS/400 does not save directories nor shares.	OBJ('/QNTC/ <i>server1</i> /fshare/ <i>pay*</i>)
Only directories and shares (no objects) for 'fshare' and its immediate children.	OBJ('/QNTC/ <i>server1</i> /fshare') SUBTREE(*DIR)

To save or restore this:	Specify this:
Directories, shares, and files for 'terry' and its subtrees (not directory 'terry').	OBJ('/QNTC/server1/fdrive/terry/*') SUBTREE(*ALL)
Only the specific file 'myfile.exe'.	OBJ('/QNTC/server1/gdrive/myfile.exe')
The integrated server registry.	OBJ('/QNTC/server1/\$REGISTRY')

Windows Backup utility

You can use the Windows Backup utility and an iSeries tape drive to do backups from the integrated Windows server. See “Use iSeries tape drives with integrated Windows servers” on page 94.

To start the Backup utility:

1. On the integrated server console, click on **Start**
2. Select **Accessories** → **System Tools** → **Backup**.

For information about backup or recovery by using LAN-connected mass storage devices, refer to in your Windows server documentation from Microsoft.

Restore an integrated Windows server's NWSD and disk drives

One method of restoring your integrated server data is to restore the Network Server Description (NWSD) and disk drives that OS/400 associates with that server. It is the fastest method for restoring large amounts of data. If you used file-level backup, you can also restore specific integrated server files.

When you restore saved objects from OS/400, you need to be aware of these considerations:

Notes:

1. Treat a network server description (NWSD) of type *WINDOWSNT, its predefined disk drives (see “Predefined disk drives for integrated Windows servers” on page 85), and any user-defined disk drives that are linked to it as a unit. Restore them at the same time. Otherwise, the integrated server may not be able to re-establish items such as Windows server File System permissions.
2. To have OS/400 automatically relink restored disk drives in the integrated file system to the appropriate NWSD, restore the NWSD after you restore the disk drives.
3. If you restore an NWSD of type *WINDOWSNT before restoring the predefined and user-defined disk drives in the integrated file system, you need to relink those disk drives. You can do this by using the Add Network Server Storage Link (ADDNWSSTGL) command for each disk drive that is associated with the NWSD:

```
ADDNWSSTGL NWSSTG(Storage_Name) NWSD(NWSD_Name)
```

4. When you restore a domain controller, ensure that the domain database held on the server is synchronized with the other domain controllers. When restoring shared drives used by a Windows cluster node, it may be necessary to manually relink the shared drives. Begin by linking the shared quorum resource drive first. You can use the following command to link the shared quorum resource drive:

```
ADDNWSSTGL NWSSTG(Quorum_name) NWSD(NWSD_Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*QR)
```

Once the quorum resource has been relinked, the remaining shared drives can then be re-linked as well. Use the following command to relink the remaining shared drives:

```
ADDNWSSTGL NWSSTG(Shared_name) NWSD(NWSD_Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*CALC)
```

Follow normal Windows procedures to do this and refer to documentation from Microsoft as necessary.

5. Restoring NWSD installed on certain hardware types to different hardware type may be restricted. For more information, see “Restore integrated Windows server NWSDs” on page 122.

To restore an integrated server's NWSD and disk drives, refer to these pages:

- “Restore predefined disk drives for integrated Windows servers created on V4R5 and later systems”
- “Restore predefined disk drives for integrated Windows servers created on pre-V4R5 systems”
- “Restore user-defined disk drives for integrated Windows servers on iSeries” on page 121
- “Restore integrated Windows server NWSDs” on page 122

Restore predefined disk drives for integrated Windows servers created on V4R5 and later systems

For integrated servers that you create on V4R5 or later systems, disk drives that contain the Windows operating system and registry are in the integrated file system. You restore these predefined disk drives just as you do user-defined disk drives. To restore disk drives in the integrated file system on OS/400, use the Restore (RST) command:

1. If you are restoring from save media, ensure that you have mounted your media.
2. If there are no network server storage spaces that currently exist on the system (none appear when you use the WRKNWSSTG command), you must create the /QFPNWSSTG directory before you can restore network server storage spaces that you saved beneath that directory. To create the /QFPNWSSTG directory, complete these steps:
 - a. On the OS/400 command line, type CRTNWSSTG to create a server storage space and press F4.
 - b. Provide a name for the storage space.
 - c. Use the minimal size allowed and specify the appropriate disk pool (ASP).
 - d. Press Enter to create the storage space. OS/400 creates the storage space in the /QFPNWSSTG directory.
3. To restore the storage spaces, type RST and press F4.
4. In the Name field under Objects:, specify '/QFPNWSSTG/stgspc' and 'dev/QASPnn/stgspc.UDFS', where *stgspc* is the name of the network server storage space and *nn* is the number of the disk pool.

Note: To restore the .UDFS object to an independent disk pool, the disk pool device must be varied on. Specify *dev/independent ASP name/stgspc.UDFS* where *independent ASP name* is the name of the independent disk pool and *stgspc* is the name of the network server storage space.

To restore the system (C) drive, use /QFPNWSSTG/nwsdname1. To restore the D drive, use /QFPNWSSTG/nwsdname2.
5. Specify values for any other parameters that you want and press Enter to restore the storage space.
6. You also need to restore any user defined disk drives that are associated with the server and restore the NWSD. See “Restore user-defined disk drives for integrated Windows servers on iSeries” on page 121. When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Restore predefined disk drives for integrated Windows servers created on pre-V4R5 systems

Earlier versions of IBM iSeries Integration for Windows Server created disk drives for the C, D, and E drives in the QUSRSYS library. Those disk drives contain the Windows operating system and registry, boot and system drives. Even after you upgrade your system to V4R5, these storage spaces remain where OS/400 created them unless you reinstall Windows. You restore those storage spaces with the Restore Object (RSTOBJ) command. System drives that are larger than 1007 megabytes also have data in a network storage space that you need to restore.

To restore server storage spaces, you use the Restore Object (RSTOBJ) command:

1. On the OS/400 command line, type RSTOBJ and press F4.
2. If you are restoring from save media, ensure that you have mounted your media.

3. In the Objects field, specify the name the storage space. (If you want to restore all the predefined storage spaces, first type + and press Enter.)
 - To restore the C drive, specify the name of the NWSD followed by 1.
 - To restore the D drive, specify the name of the NWSD followed by 2.
 - To restore the E drive, specify the name of the NWSD followed by 3.
4. In the Save Library field, specify QUSRYS.
5. In the Device field, specify either the name of the device that contains the save media or specify *SAVF if you are restoring from a save file.
6. In the Object types field, specify *SVRSTG.
7. If you are restoring from a save file, specify the name and library for the save file.
8. Press Enter to restore the storage spaces.
9. If your system drive (E) is not larger than 1007 megabytes, go directly to step 10. If your system drive is larger than 1007 megabytes, you need to restore data that you saved from an additional disk drive in the integrated file system:
 - a. If there are no network server storage spaces that currently exist on the system (none appear when you use the WRKNWSSTG command), you must create the /QFPNWSSTG directory before you can restore network server storage spaces that you saved beneath that directory. To create the /QFPNWSSTG directory, complete these steps:
 - 1) On the OS/400 command line, type CRTNWSSTG to create a disk drive and press F4.
 - 2) Provide a name for the storage space.
 - 3) Use the minimal size allowed and specify the appropriate disk pool (ASP).
 - 4) Press Enter to create the storage space. OS/400 creates the it in the /QFPNWSSTG directory.
 - b. To restore the storage space, type RST and press F4.
 - c. If you saved the storage space to a save file instead of to tape, use *SAVF for the device. Otherwise, specify the device name.
 - d. In the Name field under Objects:, specify '/QFPNWSSTG/nwsdname3', in which nwsdname3 is the name of the storage space for the E drive.
 - e. Specify values for any other parameters that you want and press Enter to restore the storage space.
10. You also need to restore any user-defined disk drives that are associated with the server and restore the NWSD. See "Restore user-defined disk drives for integrated Windows servers on iSeries". When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Restore user-defined disk drives for integrated Windows servers on iSeries

Although you can now back up individual files and directories (see "Back up individual integrated Windows server files and directories" on page 115), the fastest way to restore large amounts of data is to restore the entire storage space. If you back up your user storage space from the \QFPNWSSTG directory, you can restore only the entire storage space. See "Back up user-defined disk drives for an integrated Windows server" on page 112. You cannot restore individual files from this backup.

To restore disk drives in the integrated file system, do this:

1. If you are restoring from save media, ensure that you have mounted your media.
2. If there are no network server storage spaces currently exist on the system (none appear when you use the WRKNWSSTG command), you must create the /QFPNWSSTG directory before you can restore network server storage spaces that you saved beneath that directory. To create the /QFPNWSSTG directory, complete these steps:
 - a. On the OS/400 command line, type CRTNWSSTG to create a server storage space and press F4.
 - b. Provide a name for the storage space.

- c. Use the minimal size allowed and specify the appropriate disk pool (ASP).
 - d. Press Enter to create the storage space. OS/400 creates the storage space in the /QFPNWSSTG directory.
3. To restore the storage spaces, type RST and press F4.
 4. In the Objects: name field, specify '/QFPNWSSTG/stgspc' and 'dev/QASPnn/stgspc.UDFS', where stgspc is the name of the network server storage space and nn is the number of the disk pool.

Note: To restore the .UDFS object to an independent disk pool, the disk pool device must be varied on. Specify 'dev/independent ASP name/stgspc.UDFS' where independent ASP name is the name of the independent disk pool and stgspc is the name of the network server storage space.
 5. Specify values for any other parameters that you want and press Enter to restore the storage space.
 6. You also need to restore any predefined disk drives that are associated with the server and restore the NWSD. See "Restore integrated Windows server NWSDs." When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Restore integrated Windows server NWSDs

In a disaster recovery situation, you would restore all the configuration objects, one of which is the integrated Windows server's network server description (NWSD). In some situations, for example when you migrate to new Integrated xSeries Server hardware, you need to specifically restore the NWSD. To have OS/400 automatically relink disk drives within the integrated file system to the restored NWSD, restore those disk drives first. To restore the NWSD, you use the Restore Configuration (RSTCFG) command:

1. On the OS/400 command line, type RSTCFG and press F4.
2. In the Objects field, specify the name of the NWSD.
3. In the Device field, specify the device name if you are restoring from media. If you are restoring from a save file, specify *SAVF and identify the name and library for the save file in the appropriate fields.
4. Press Enter to have OS/400 restore the NWSD.
5. When you are done restoring the NWSD and all its associated storage spaces, start the integrated server. See "Start and stop an integrated server" on page 75.

Note: When you restore a NWSD, you must also restore any line, controller, and device description objects that are associated with the NWSD. You must also restore any line descriptions that had TCP/IP interfaces defined.

Recover integrated Windows server files

IBM iSeries Integration for Windows Server supports file-level backup and recovery of your files. You can recover a particular file from your OS/400 backup without restoring the entire disk drive. Before using this method, however, consider the amount of data you need to restore. For large amounts of data, restoring an entire disk drive object is much faster than restoring all the individual files in the disk drive. To restore a smaller amount of data, this method works great.

You should restore the directory first, then files, then the registry, then reboot for new registry entries to take effect. To restore files that you saved by this method, use the RST command:

1. Ensure that the integrated Windows server and TCP/IP are running.
2. On the OS/400 command line, type RST and press F4.
3. In the Device field, specify the device on which the data is available. (For example, 'QSYS.LIB/TAP01.DEVD' restores the data from tape.)
4. In the Object field, specify what you want OS/400 to restore in the form '/QNTC/servername/sharename'

You can use wildcard characters. Refer to “Examples: How to address parts of an integrated Windows server” on page 118 for how to specify particular parts of an integrated Windows server. Avoid restoring Windows system files by this method because the restored files may behave unpredictably.

5. In the Name field, specify the path name of the object to restore.
6. You can use the Include or omit field to include or omit objects with the pattern that you specify in the Name portion of the Object parameter.
7. In the New object name field, leave the object name the same or specify a new path name. The new path name must be referenced by a share name that exists on the integrated Windows server.
Note: When you save a directory that has shares defined over it, OS/400 saves the share information with the directory. If you specify a new object name when you restore the directory, OS/400 does not re-create these shares.
8. Use the Directory subtree field to specify whether you want to restore subtrees under a directory. The default is to restore all directories.
9. To specify that you want to restore files that were saved during a particular period, specify starting and ending dates and times in the Change period field.
10. Provide any other information that you want OS/400 to use to restore the files and press Enter.
11. When the files are restored, reboot the integrated server for new registry entries to take effect.

Chapter 12. Uninstall the Windows server operating system from the integrated server hardware

You can use the Delete Windows Server (DLTWNTSVR) command to uninstall Windows server from an Integrated xSeries Server. Prior to running the Delete Windows Server command, shut down your integrated Windows server from OS/400. See “Start and stop an integrated server” on page 75.

The Delete Windows Server (DLTWNTSVR) command deletes the specified Windows network server description and all associated objects that were created by the Install Windows server (INSWNTSVR) command. These objects include the network server description, line descriptions, TCP/IP interfaces, server storage spaces and system created network server storage spaces. The network server must be varied offline before this command is issued.

To manually uninstall Windows server from an Integrated xSeries Server, do the following:

1. Shut down the integrated server, see “Start and stop an integrated server” on page 75.
2. “Unlink integrated Windows server disk drives” on page 90.
3. “Delete integrated Windows server disk drives” on page 90.
4. “Delete an integrated Windows server’s NWSD.”
5. “Delete an integrated Windows server’s line descriptions” on page 126.
6. “Delete TCP/IP interfaces associated with an integrated Windows server” on page 126.
7. “Delete controller descriptions associated with an integrated Windows server” on page 126.
8. “Delete device descriptions associated with an integrated Windows server” on page 127.
9. (Optional) If you remove all your Windows servers from OS/400 and plan not to install any more, you can delete IBM iSeries Integration to free up the storage the product uses. See “Delete the IBM iSeries Integration for Windows Server licensed program” on page 127.

Delete an integrated Windows server’s NWSD

Before you delete a network server description (NWSD), you need to unlink its disk drives (see “Unlink integrated Windows server disk drives” on page 90) and delete storage spaces that are associated with that NWSD (see “Delete integrated Windows server disk drives” on page 90). Then you can delete the NWSD.

For NWSDs created before V4R5:

1. To unlink the storage space object for NWSDs created before V4R5, on the OS/400 command line, type `RMVNWSSSTGL NWSSTG(nwsdname3) NWSD(nwsdname)` and press Enter.
2. To delete the network server storage space object, type the command `DLTNWSSTG NWSSTG(nwsdname3)` and press Enter.

For NWSDs created at V4R5 and later:

1. To unlink the storage space for the system drive for NWSDs created at V4R5 and later, on the OS/400 command line, type `RMVNWSSSTGL NWSSTG(nwsdname1) NWSD(nwsdname)`. Press Enter.
2. To unlink the storage space for the install source drive, type `RMVNWSSSTGL NWSSTG(nwsdname2) NWSD(nwsdname)` and press Enter.
3. Any user defined storage spaces that have been linked to the NWSD can also be removed at this time using the command as often as needed `RMVNWSSSTGL NWSSTG(nwsstgname) NWSD(nwsdname)` and press Enter.
4. To delete the network server storage space object for the system drive, type the command `DLTNWSSTG NWSSTG(nwsdname1)` and press Enter.

5. To delete the network server storage space object for the install source drive, type `DLTNWSSTG NWSSTG(nwsdname2)` and press Enter.
6. Remove any additional storage spaces that are no longer needed by typing the `DLTNWSSTG NWSSTG(nwsstgname)` command and pressing Enter.

To delete an integrated server's network server description (NWSD), follow these steps:

1. On OS/400, type the command `WRKNWSD` and press Enter.
2. Type 8 in the Opt field to the left of the Network Server; press Enter. The Work with Configuration Status display appears.
3. If the status of the NWSD is not varied off, type 2 in the Opt field to the left of the Network Server; press Enter. Otherwise, go to the next step.
4. Press F3 to return to the previous dialog.
5. Enter a 4 in the Opt field to the left of the Network Server and press Enter.
6. On the Confirm Delete of Network Server Descriptions display, press Enter.

Delete an integrated Windows server's line descriptions

To delete all of an integrated server's line descriptions, follow these steps:

1. On OS/400, type the command `WRKLIND` and press Enter.
2. Page down until you see the line description that you want to delete.
Note: The name of the line description should be the name of the network server description (NWSD) followed by 00, 01, 02, PP, V0, V1, V2, V3, V4, V5, V6, V7, V8 or V9. This depends on the port number to which you attached it.
3. Place a 4 in the Opt field to the left of the line description and press Enter. Repeat this step for any other line descriptions that are associated with the NWSD.

Note: An alternate method to steps 1 and 2 is to use the `WRKLIND nwsdname*` command, where `nwsdname` is the name of the associated network server description.

Delete TCP/IP interfaces associated with an integrated Windows server

To delete TCP/IP interfaces that are associated with an integrated server, follow these steps:

1. On the OS/400 console, enter the `CFGTCP` command.
2. Choose option 1. Work with TCP/IP interfaces from the Configure TCP/IP menu.
3. Type a 4 in the Opt field next to the TCP/IP interface you want to remove, then press Enter.
You can identify the TCP/IP interfaces that are associated with the network server description (NWSD) by looking at the name of the attached line description. This name consists of the NWSD name, followed by a number.
4. Repeat step 3 for each TCP/IP interface that is associated with the NWSD.

Delete controller descriptions associated with an integrated Windows server

To delete all of the controller descriptions for an integrated server, follow these steps:

1. On OS/400, type the command `WRKCTLD` and press Enter.
2. Page down until you see the controller description that you want to delete.
Note: The name of the controller description starts with the first five characters of the NWSD name, followed by 'NET' and a two-digit number. For example, if the NWSD name is MYSERVER, the controller name might be MYSERVERNET01.

3. Place a 4 in the Opt field to the left of the controller description and press Enter. Repeat this step for any other controller descriptions that are associated with the NWSD.

Note: An alternate method to steps 1 and 2 is to use the WRKCTLD MYSER* command, where MYSER is the first 5 characters of the NWSD name.

Delete device descriptions associated with an integrated Windows server

To delete all of the device descriptions for an integrated server, follow these steps:

1. On OS/400, type the command WRKDEVD and press Enter.
2. Page down until you see the device description that you want to delete.

Note: The name of the device description starts with the first five characters of the NWSD name, followed by 'TCP' and a two-digit number. For example, if the NWSD name is MYSERVER, the device name might be MYSERTCP01.

3. Place a 4 in the Opt field to the left of the device description and press Enter. Repeat this step for any other device descriptions that are associated with the NWSD.

Note: There may be many devices on a system. Use the WRKDEVD MYSERTCP* or WRKDEVD *NET commands to get the complete list of network devices that need to be deleted.

Delete the IBM iSeries Integration for Windows Server licensed program

If you remove all integrated Windows servers from your iSeries and do not plan to reinstall others, you may also want to remove the IBM iSeries Integration for Windows Server licensed program from OS/400. Removing the program frees the storage space it occupied on OS/400.


Note: Removing the program does not automatically delete existing network server descriptions or user-defined disk drives. However, it does render them unusable. You can find information on deleting network server descriptions and disk drives in Chapter 12, "Uninstall the Windows server operating system from the integrated server hardware," on page 125.

To delete IBM iSeries Integration for Windows Server, follow these steps:

1. On OS/400, type the command GO LICPGM and press Enter.
2. Choose option 12 from the Work with Licensed Programs menu and press Enter.
3. Page down the list of licensed programs until you see the description Integration for Windows Server
4. Type 4 in the Option field to the left of the base program. Press Enter, and OS/400 deletes the licensed program and its optional parts.

Chapter 13. Troubleshoot integrated Windows servers

If your integrated server is not functioning properly, follow these steps to attempt to correct the problem:

1. Try restarting the integrated server. See “Start and stop an integrated server” on page 75.
2. Display information about the NWSD and its associated lines, controllers, and devices. See “View or change integrated Windows server configuration information” on page 78.
3. If the problem persists, look for helpful information in the logs. See “Check message and job logs”.
4. Next look for the specific problem in the section “Problems with integrated Windows servers” on page 130.
5. Also check the Informational APARs for the latest tips and service information. You can find these at the IBM Windows Integration web site .
6. If the integrated server becomes damaged, you may be able to preserve installed applications and user data by reinstalling it. See “Reinstall an integrated Windows server” on page 153.
7. If you need information about collecting service data to send to support personnel, see “Collect integrated Windows server service data” on page 154.

Other options to resolve problems

If a solution to the problem you are having is not addressed by the troubleshooting sections in this chapter, other service options may help resolve the problem.

- For problems with specific applications, contact the application provider for support.
- For Integrated xSeries Server or Integrated Netfinity Server hardware errors or server installation problems, contact IBM Service.
- For unrecoverable server errors (for example, blue screens), there may be pertinent information at websites www.ibm.com/eserver/series/support or support.microsoft.com relating to the problem.

If additional assistance is required, under IBM service contracts, IBM service will assist in determining the correct path for problem resolution. Contact the IBM Support Line for assistance.

Check message and job logs

Information about integrated Windows servers is logged in several places. If you have a problem, this information may help determine its cause.

Monitor job log

The Monitor job log (see the topic “Monitor job” on page 130) contains messages that vary from normal processing events to detailed error messages. To check this log, do this:

1. At the OS/400 command line, use the Work with active job (WRKACTJOB) command and find the job in the QSYSWRK subsystem with the same name as your network server. If the job does not appear on this display, the job has either ended or has not started.
2. If you find the job, use option 5 to work with the job and option 10 to display the job log.
3. Press F10 for detailed messages.
4. If you find useful information in the log, write down the job ID (all three parts: Name, User, and Number). Then print the log with this command: `DSPJOBLOG JOB(number/user/name) OUTPUT(*PRINT)`.

Note: If the problem caused your monitor job to end or you are debugging a problem that happened before the present monitor job, search for a spooled file that contains information in the previous job log. To find spooled files that deal with your network server, use this command: `WRKSPLF SELECT(QSYS *ALL *ALL nwsd_name)`.

QVNAVARY job log

The QVNAVARY job log contains messages that deal with the vary on and vary off of the network server description when you shut down and restart from Windows server. To check this log for shutdown and startup errors, do this:

1. At the OS/400 command line, use the Work with active job (WRKACTJOB) command and find the QVNAVARY job in the QSYSWRK subsystem.
2. Use option 5 to work with the job and option 10 to display the job log.

You can also use WRKJOB JOB(QVNAVARY).

Job log of the job that initiated a vary on or off

If a batch job or interactive user initiated a vary on or off of the NWSD from OS/400, the log for that job might provide helpful information. For example, if you used a VRYCFG or WRKCFGSTS command, you can use the Display job (DSPJOB) command and option 10 to look at the job log.

Server message queue

If during the installation you specified a message queue for your network server, that message queue can provide helpful information.

1. If you need to verify whether you specified a message queue, at the OS/400 command line, type DSPNWSN NWSD(nwsd_name) and press Enter. If it is set to *none, only serious messages go to the QSYSOPR message queue.
2. If a message queue is specified, use this command on OS/400 to display the messages: DSPMSG MSGQ(library/queue)

System operator's message queue

The integrated server updates the system operator's message queue (QSYSOPR) with normal startup and shutdown messages in addition to failure messages. To display these messages from the character-based interface, enter DSPMSG QSYSOPR.

Profile synchronization job log

The profile synchronization job log contains EIM and user profile enrollment messages. To check this log, enter WRKJOB QPRFSYNCH.

Monitor job

Every active integrated Windows server has a monitor job that starts when you start the server. The monitor job runs in the QSYSWRK subsystem under the QSYS user profile. The job name is the name of the network server description that it is monitoring.

When the monitor job starts, OS/400 sends an informational message, CPIA41B, to the QSYSOPR message queue. This message contains the job ID of the monitor job. You can use this job ID with the Work with Job (WRKJOB) command to find the monitor job log and other job-related information for the monitor job.

Problems with integrated Windows servers



If your integrated Windows server is not working correctly, check to see if your problem fits into this list:

- "Blue screen errors" on page 131
- Problems using Software maintenance program. See "IBM iSeries Integration for Windows Server snap-in program" on page 140.

- **Drive problems**
 - “A full integrated server system drive”
- **Device problems**
 - “Optical device problems” on page 133
 - “Tape problems” on page 133
- **Starting/stopping problems**
 - “Problems starting an integrated Windows server” on page 134
 - “Vary-off failures” on page 136
 - “NWSD configuration file errors” on page 136
- **Externally attached xSeries servers**
 - “DASD in Integrated xSeries Adapter attached xSeries servers” on page 137
 - “HSL communication problems with the Integrated xSeries Adapter” on page 137
- **User and group enrollment problems**
 - “Failures enrolling users and groups” on page 137
 - “User-enrollment authorization problems” on page 138
 - “Password problems” on page 139
- **Networking problems**
 - “Virtual Ethernet connection problems” on page 141
 - “Problems with external networks when using external host LAN” on page 143
 - “General problems with external networks” on page 145
 - “Manually update LAN drivers on the integrated Windows server” on page 146
 - “Private LAN IP address conflicts” on page 148
 - “IP forwarding problems” on page 150
 - “IFS access problems” on page 151
 - “TCP/IP failure between OS/400 and Windows” on page 150
 - “Problems accessing Windows Server 2003 shares using the QNTC file system” on page 151
- “Problems with saving integrated Windows server files” on page 151
- “Unreadable messages in the server message queue” on page 152
- “Problems getting a Windows system memory dump” on page 153

Blue screen errors

When you get blue screen errors, take the following actions to try to determine the cause of the errors and how to correct the errors:



1. On the OS/400 command line, type DSPMSG QSYSOPR.
2. Press Enter. The QSYSOPR message queue appears.
3. Look through the messages for any that may help you determine what caused the blue screen.
4. Restart the integrated server by varying it off, then back on, from OS/400 (see “Start and stop an integrated server” on page 75).
5. Inspect the Event log on Windows for errors, type of stop code, and other diagnostic information.
6. If the problem still persists, check the technical information databases at the  **server** IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

A full integrated server system drive

The system drive contains the Windows server operating system and may contain applications and data as well. If this drive fills up, it can cause such errors as full drive messages and paging file errors.

To keep the system drive from filling up, take one or more of these steps:

- Increase the size of the system drive during the installation of Windows server.
- When you install applications, install them on a user-defined storage space instead of taking the default of installing them to your system drive.
- If your integrated server was created pre-V4R5, see the section “Remapping a full C drive; for integrated servers created pre-V4R5 only.”
- Move your Windows server paging file to a user-defined storage space instead of defaulting to the system drive. If you move your paging file, you will not be able to collect a system-memory dump if a STOP error or blue screen occurs. However, if you want to do this, follow these steps:
 1. Right-click on the **My Computer** icon and select **Properties**.
 2. Select the **Advanced** tab.
 3. Click the **Performance** options button.
 4. Click the **Change** button for **Virtual Memory**.
 5. Select a user-defined storage space that has the amount of free space that you need.
 6. Click **OK**.
- Move your Windows server memory dump to a user-defined storage space instead of defaulting to the system drive. To do this, follow these steps:
 1. Go to **Start**, then **Settings**, then **Control Panel**.
 2. Click the **Startup/Shutdown** tab.
 3. Select the **Write debugging information to** box in the **Recovery** section of the panel.
 4. Select a user-defined storage space that has enough free space (about 12 MB larger than your RAM size). Refer to the Windows documentation for additional recommendations and requirements for page size.
 5. Click **OK**.

Note: If you move your Windows server memory dump to a user-defined space, you will have to copy the dump file to tape to send it to technical support.
- If the problem still persists, check the technical information databases at the  IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.


Remapping a full C drive; for integrated servers created pre-V4R5 only

If your C drive is too small to hold Windows server applications that require the C drive during installation, you can remap the C drive. With Windows server Administrator authority, you can use the Disk Manager to remap the current C drive (which is the first physical drive) to another available drive letter. Then you can map a larger network storage space as the new C drive. Windows server on iSeries can still locate control files after you reassign the drives. To do this, follow these steps:

1. On OS/400, vary off the network server description (NWSD) for your Windows server. See “Start and stop an integrated server” on page 75.
2. On OS/400, use the Create Network Server Storage Space (CRTNWSSTG) command to create a network storage space.
3. On OS/400, use the Add Network Server Storage Link (ADDNWSSTGL) command to link that storage space to the Windows server.
4. Vary on the network server description (NWSD) for your Windows server. See “Start and stop an integrated server” on page 75.
5. On the Windows server, use **Disk Manager** to do this:
 - a. Map the current C drive to another available letter
 - b. Map the new network storage space to the C drive
 - c. Format your new network storage space
6. Install the Windows server application.

Optical device problems

If the OS/400 optical device does not work with an integrated Windows server, take these actions:

1. Make sure that you have varied on the optical device on OS/400. Find out how to vary on the optical device in “Use iSeries optical drives with integrated Windows servers” on page 93.
2. Make sure the optical drive is allocated to the integrated server.
3. Make sure that there is optical media in the drive.
4. If your system has logical partitions, make sure that you have allocated the optical device to the same partition as the integrated server.
5. Look in the event log for optical device errors.
6. Make sure that the optical device shows up in **My Computer** on the integrated Windows server.
7. Recovery steps for optical devices:
 - a. Close the IBM iSeries Integration for Windows Server snap-in program
 - b. Vary off the optical device on the iSeries
 - c. Vary the optical device on
 - d. Reallocate the device to the integrated server
8. If the problem still persists, check the technical information databases at the [@server IBM iSeries Support Web page](#) .
9. If you cannot find the solution there, contact your technical support provider.

If an integrated server fails before unlocking an optical device, the device will be unavailable to OS/400 or to other integrated servers. For more information, see “Locked optical device for a failed server.”



Locked optical device for a failed server

If the integrated server fails before unlocking an optical device (or varying off the server), the optical device will be unavailable to OS/400 or other Windows Servers. You will need to vary off the optical device using WRKCFGSTS *DEV *OPT and vary it back on to free the lock.

Tape problems

If the iSeries tape drive does not work with an integrated Windows server, take these actions:

1. Verify that you have varied off the tape drive on OS/400 and locked it on an integrated server. See “Allocate the iSeries tape drive to an integrated Windows server” on page 95. Devices may fail to lock for one of these reasons:
 - The tape device or its tape library is varied on.
 - The device driver is not loaded.
 - The tape device is not supported.
 - If you have problems with locking the device, verify that the device driver is loaded on the integrated server. This typically happens automatically. See “Verify that the iSeries Tape Drive device driver is loaded” on page 134.
 - Verify that your tape drive is supported. See “Supported iSeries tape drives” on page 96.
2. More advanced applications might lock devices to services that continue after the application interface is dismissed. This prevents other applications from being able to use the device. These services may restart automatically after a system restart, locking the device to the application. To see services of an application (such as Seagate and Computer Associates), do this:
 - a. Click on **Start, Programs, Administrative Tools**, then **Component Services**.
 - b. Double-click on **Services**.
 - c. If necessary, you can stop services from the **Services** window.

3. You may have multiple integrated servers. If so, verify that the tape drive is unlocked on all of them except the one on which you want to use it. See “Transfer control of the iSeries tape and optical drives between integrated Windows servers” on page 97.
4. If your system has logical partitions, ensure that you allocated the tape drive to the same partition as the integrated server.
5. Verify that the drive contains a properly formatted tape. See “Format a tape on OS/400 for use with integrated Windows servers” on page 95.
6. Verify that the drive is not on the list of restricted devices on OS/400 by using the Display NWSD command (DSPNWSD).
7. Look in the event log for tape errors.
8. See if the tape device shows up in the Device List:
 - a. Click on **Start, Programs, Administrative Tools**, then **Computer Management**.
 - b. Select **System Tools**, then **Device Manager**.
 - c. Verify that the tape drive shows up in **Device List**.
9. If the problem still persists, check the technical information databases at the  **server** IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

Verify that the iSeries Tape Drive device driver is loaded

Before applications running on an integrated server can use the iSeries tape drive, the IBM iSeries Tape Drive device driver must be loaded on the integrated server. This is typically automatic. To ensure that the tape device driver is loaded, follow these steps.

1. On the Windows server task bar, click **Start**, then **Programs**, then **Administrative Tools**.
2. Click **Computer Management**, then **System Tools**, then **Device Manager**.
3. Expand the icon with your computer’s name on it. If a tape device is loaded, a Tape Device icon appears.
4. Expand the **Tape device** icon to see the loaded tape device drivers.
5. If you need to manually load a tape device driver, complete these steps.
 - a. Click on **Start**, then **Settings**, then **Control Panel**.
 - b. Click on **Add/Remove Hardware**.
 - c. On the Add/Remove Hardware Wizard, click **Next**.
 - d. Select **Add/Troubleshoot a device** and click **Next**.
 - e. On the **Choose a Hardware Device** section of the Add/Remove Hardware Wizard window, choose **Add a new device** and click **Next**.
 - f. From the **Find New Hardware** section of the Add/Remove Hardware Wizard window, choose “No, I want to select the hardware from a list,” and click **Next**.
 - g. On the Hardware Type section, scroll down the combo box to **Tape drives**, select it, and click **Next**.
 - h. In the Manufacturers pane of the Select a Device Driver section, select **IBM**. In the Models pane, select **IBM iSeries Tape Drive** and click **Next**.
 - i. Click **Next** on the “IBM iSeries Tape Drive” section of this window.
 - j. If the “Files Needed” box appears, enter c:\WINNT\System32\drivers, where C: is your system drive, into the “Copy files from” box. Click **OK**.
 - k. On the “Completing the Add/Remove Hardware Wizard” section of the Add/Remove Hardware Wizard window, click **Finish**. All the tape devices should load.
 - l. After restarting your computer, repeat steps 1 – 4 to confirm that your devices are loaded.

Problems starting an integrated Windows server

If your integrated server will not start, perform these steps to determine the problem.

1. Check the status of the server. Verify that the current status of the NWSD is VARIED OFF. If it is not, vary off the NWSD; then retry starting the server. See “Start and stop an integrated server” on page 75. If the status of the server is VARY ON PENDING even though the integrated server did not start, there may be a device driver problem.
2. Look for error messages and possible corrective actions in the job log where the vary on of the NWSD was performed.
3. Look in the QSYSOPR message queue for failure messages and possible corrective actions.
4. If you created a server configuration file that might be causing problems, try repairing or resetting the server configuration file. See “NWSD configuration file errors” on page 136.
5. If you initiated a restart from the integrated server, perform these steps.
 - a. On OS/400, enter the command WRKACTJOB SBS(QSYSWRK).
 - b. Press Enter.
 - c. Locate the job QVNAVARY.
 - d. Select option 5 to work with the job.
 - e. If the job is active or on the job queue, select option 10 to display the job log. Look for failure messages and possible corrective actions.
 - f. If you have ended the job, enter WRKSPLF SELECT(*CURRENT *ALL *ALL QVNAVARY) to display the spooled file.
6. Enter the command WRKPRB to see logged problems.

Emergency Repair

If the problem persists due to a failing system drive but you have a successful backup of that drive, try this emergency repair. To recover lost data and return the system to a functioning state, follow these steps.

Note: These examples use the NWSD name *ERS* with a system drive named *ERS1*.

1. Unlink the failing system drive (typically the C: drive) by using this command: `RMVNWSSSTGL NWSSTG(ERS1) NWSSTG(ERS)`.
2. Copy the failing system drive to a new name by using this command: `CRTNWSSTGL NWSSTG(ERS1BKP) FROMNWSSTG(ERS1)`.
3. Restore your latest backup of the system drive.
4. Link in the restored system drive by using this command: `ADDNWSSTGL NWSSTG(ERS1) NWSSTG(ERS)`.
5. Link in the failing system drive from step 1 by using this command: `ADDNWSSTGL NWSSTG(ERS1BKP) NWSSTG(ERS)`
6. Vary on the NWSD by using this command: `VRYCFG CFGOBJ(ERS) CFGTYPE(*NWS) STATUS(*ON)`.
7. Copy any key files, such as data files, from the failing system drive which have changed from the latest backup.
8. Install any applications that you added or upgraded since the latest backup.
9. Vary off the NWSD by using this command: `VRYCFG CFGOBJ(ERS1) CFGTYPE(*NWS) STATUS(*OFF)`.
10. Unlink the failing system drive from step 5 by using this command: `RMVNWSSSTGL NWSSTG(ERS1BKP) NWSSTG(ERS1)`.
11. Until you are sure you have removed all data from the failing system drive, you can relink the drive (step 5) and copy additional files to the restored drive. Once you are sure that you have removed all data from the failing system drive, make a new backup of all storage spaces. Refer to “Back up predefined disk drives for integrated Windows servers created on V4R5 and later OS/400 systems” on page 110 for steps to backup storage spaces. Then delete the failing system drive by using this command: `DLTNWSSTGL NWSSTG(ERS1BKP)`.

Vary-off failures

If you get a blue screen and an error message that says ECONREFUSED (3425) when you are trying to vary off an integrated server, look to see if the internal OS/400 Internet addresses are routed to a software common knowledge IR system (SOCKS) server that is acting as a firewall. Routing the private LAN through a firewall causes communications failure. For information about setting up a firewall, see the page Firewalls.

NWSD configuration file errors

If you suspect that an NWSD configuration file that you created is causing an error, try resetting the NWSD configuration file parameter to *NONE. See “Reset the NWSD configuration file parameter.” If the error disappears, your NWSD configuration file most likely has a problem.

If the NWSD configuration file is causing errors, you have these options.

- Continue without using your own NWSD configuration file.
- “Use a previous version of the integrated server file”
- “Repair the NWSD configuration file”

Repair the NWSD configuration file

If you want to repair your NWSD configuration file to eliminate the errors, consider these options.

1. Check the logs for error and recovery information. See “Check message and job logs” on page 129.
2. Edit the NWSD configuration file.
3. Restart. See “Start and stop an integrated server” on page 75.

Reset the NWSD configuration file parameter

You can set the Configuration file parameter of the NWSD to *NONE to prevent the changes that are causing errors from being made to the integrated server file. To prevent OS/400 from using your NWSD configuration file, follow these steps.

1. On the OS/400 command line, type WRKNWSD to work with your network server descriptions (NWSD).
2. On the line by the network server that is having problems, choose option 2 (Change).
3. In the Configuration file field, select *NONE.
4. Vary on the network server and see if the error has gone away.

Note: Existing modifications to any files that are processed by a configuration file will remain unchanged. A .BKU file exists with the file contents prior to the last modification performed by varying on the server. This file can be used to replace the changed version or the file can be restored from a previous backup if one is available.

Use a previous version of the integrated server file

If you have a working version of the integrated server file, you can change the file back to this working version. To change it follow these steps.

1. Reset the configuration file parameter of the NWSD to *NONE to prevent the changes that are causing errors from being made to the integrated server file. See “Reset the NWSD configuration file parameter.”
2. Choose the file that you want to reset to a previous version.
3. If the server is functional and varied on, log on to the server or run a remote command (see “Run integrated Windows server commands remotely” on page 79) from the OS/400 console to rename the files:
 - Rename the file that is causing problems to another name.
 - Rename the previous version of the file to the original name.
4. Vary the integrated server off and back on to use the previous version of the file.

DASD in Integrated xSeries Adapter attached xSeries servers

Local hard disk drives are not supported in an xSeries server when it is direct attached to the iSeries with the Integrated xSeries Adapter. In most cases, the local hard disk drive will not show up. If the drive does happen to appear, and it is used, unpredictable results may occur. When using an xSeries server in the direct attach mode, make sure any hard disk drives are removed.

HSL communication problems with the Integrated xSeries Adapter

The preferred way to shut down a direct attach server with Integrated xSeries Adapter is to vary it off from the iSeries server. The shut down process on the xSeries server from Windows 2000 or Windows Server 2003 causes the server to power off. This appears to the iSeries server as an I/O tower powering off and leaving the loop. This causes the iSeries server to go into recovery mode. Powering off multiple external servers could cause problems for other non-Integrated xSeries Server towers on the high speed link (HSL) loop (e.g. a tower between two external servers that are powered off could become isolated from the iSeries).

Failures enrolling users and groups

If you cannot enroll groups or users to the Windows environment on iSeries, follow this procedure to determine the problem.

From OS/400:

- Check for errors in the message log for this network server description (NWSD) (designated during server installation to be QSYSOPR, a user-defined message log, or the user job log). Follow the error message Recovery actions to correct the problem. You can also find error codes on the Work with NWS Enrollment (WRKNWSEN) display.
- If the message log has User Admin error NTA0282, see “User-enrollment authorization problems” on page 138.
- Make sure that the status of the server is VARIED ON.
- Check enrollment status (see “Enroll a single OS/400 user to the Windows environment using iSeries Navigator” on page 99) and look for error messages. Press F5 to refresh the status.
- Verify that OS/400 is set to keep passwords (QRETSVRSEC is set to 1). Also verify that users who are trying to enroll sign-on to OS/400 **after** this value is set.
- Specify and create a message queue for the NWSD; check the queue for messages.
- On OS/400, enter the WRKACTJOB command. Check the QPRFSYNCH job in the QSYSWRK subsystem. Check the job log by pressing F10 for more detailed messages.
- On OS/400, enter the WRKJOB *nwsdname* command, where *nwsdname* is the name of the NWSD for your integrated server. If the job is active, display the job log (Press F10 for more detail messages). If you end the job, display the spooled file.

From the integrated Windows server:

You can also try the following steps to determine the problem.

- See if the User Administration Service is running.
 1. From the integrated server’s **Start** menu, select **Programs**, then **Administrative Tools**, then **Component Services**.
 2. Select **System Tools**, then **Services**.
 3. See if **iSeries User Administration** appears in the list of services.
 4. If the **iSeries User Administration** service is listed, but the status does not show that it is started, Right-click on **iSeries User Administration** and select **Start** from the menu.
 5. If **iSeries User Administration** is not listed, do the following to reinstall it:
 - a. From the **Start**, select **Run**, and type command to open a command prompt window.

- b. Go to the C: drive (or the current Windows drive).
- c. Type `C:\winnt\as400wsv\admin\qvnadaem /install` and press Enter.
- d. Close the **Services** window.
- e. Re-open **Services**.
- f. If you have not started **iSeries User Administration**, click **Start**.

If you get an error message stating that a Windows domain controller cannot be found, it may be that you are trying to enroll users to a Windows workgroup. In Windows networking, groups of local servers can be loosely affiliated by using Windows workgroups. For example, if you open My Network Places and click Computers Near Me, you will see a list of the computers in the same workgroup as you. In iSeries Navigator, it will sometimes appear that you can enroll OS/400 users to these workgroups, but attempting to do this will result in an error. There is no separate list of Windows workgroup users like there is for a Windows domain.

User-enrollment authorization problems



If you get an error (NTA0282) that indicates insufficient authorization to create and update integrated server users, take action as appropriate.

- If you are trying to enroll users and groups to a domain for the first time, ensure that you set up a QAS400NT user ID to provide the necessary authorization. The topic, “The QAS400NT user” on page 105, tells you how. Also ensure that the user is configured as a traditional user, which means that the user must specify an iSeries password and have local password management enabled. See “Types of user configurations” on page 19.
- If you have been successfully enrolling users and groups for awhile, check to see if the OS/400 password for the QAS400NT user has expired. When the QAS400NT user password expires, the account on the integrated server also expires. To correct this situation, do the following.
 1. Enable the integrated server account.
 - On a domain controller:**
 - a. Open **Start** → **Programs** → **Administrative Tools**.
 - b. Select **Active Directory Users and Computers**.
 - c. Right-click on **Users**, then double-click on **QAS400NT**.
 - d. Click on the **Account** tab at the top of the **User Properties** window.
 - e. Change the **Account expires** date to a date in the future and click on **Never**.
 - On a local integrated Windows server:**
 - a. Open **Start**, **Programs**, **Administrative Tools**.
 - b. Select **Computer Management**.
 - c. Expand **System Tools**; then expand **Local Users and Groups**.
 - d. Right-click on **QAS400NT** from the list.
 - e. Click on the **Account** tab at the top of the **User Properties** window.
 - f. Change the **Account expires** date to a date in the future and click on **Never**.
 2. On OS/400, use the Change user profile (CHGUSRPRF) or Change password (CHGPWD) command to change the QAS400NT user password.
 3. Restart the iSeries User Administration Service.
 - a. Click on **Start**, then **Programs**, then **Administrative Tools**, then **Component Services**.
 - b. Click on **Services**.
 - c. Click on **iSeries User Administration**, then right-click on **Stop** to stop the service.
 - d. Click on **iSeries User Administration**, then right-click on **Start** to restart the service.


Restarting the service automatically retries the enrollment of the users and groups.

To avoid this problem, be sure to change the QAS400NT password periodically on your OS/400 system to prevent the password from expiring.

If you have more than one iSeries with multiple integrated servers that participate in a Windows domain, you can minimize password expiration problems by implementing the steps described here: “The QAS400NT user” on page 105.

- If the problem still persists, check the technical information databases at the IBM  iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

Password problems

Previously, all characters that were allowed in OS/400 passwords were also allowed in Windows passwords. Now, OS/400 allows longer passwords and more characters than Windows supports. You should use OS/400 passwords containing only characters and password lengths allowed in Windows passwords if you want to enroll users. More OS/400 password level security information may be found in the Planning Password Level Changes section of the iSeries Security Reference  .


If a password keeps expiring each day after being changed from the integrated server console, it means that the user forgot that the password must be changed from OS/400. Changing the OS/400 password eliminates the problem.

If the OS/400 and Windows server passwords do not match, perform these tasks to determine why.

1. Check to see if the user is configured as a Windows user. See “Types of user configurations” on page 19.
 - a. On the OS/400 command line, type WRKUSRPRF.
 - b. Type in the correct UserID.
 - c. Check to see if the attribute LCLPDMGT (Local password management) is set to *NO. If so the user is configured to have an OS/400 password of *NONE and the OS/400 and Windows passwords will not be the same.
2. Check to see that OS/400 is set to store passwords:
 - a. On the OS/400 command line, type WRKSYSVAL SYSVAL(QRETSVRSEC).
 - b. Enter a 2 in the Option field; press Enter.
 - c. Verify that Retain server security data is set to 1. If it is not, change it to 1.
3. On the integrated Windows server, make sure that the User Administration Service is running. See “Failures enrolling users and groups” on page 137 for related information.
4. Check to see the OS/400 password support level:
 - a. On the OS/400 command line, type WRKSYSVAL SYSVAL(QPDDLVL).
 - b. Enter a 5 in the Option field; press Enter.

The password level of OS/400 can be set to allow user profile passwords from 1 - 10 characters or to allow user profile passwords from 1 - 128 characters. The OS/400 password level of 0 or 1 supports passwords from 1 - 10 characters and limits the set of characters. At level 0 or 1, OS/400 will convert passwords to all lowercase for Windows server. The OS/400 password level of 2 or 3 supports passwords from 1 - 128 characters and allows more characters including upper and lower case characters. At level 2 or 3, OS/400 will preserve password case sensitivity for Windows server. A change to the OS/400 password level takes effect following an IPL.

5. Check the enrollment status of the user. Make sure the user did not already exist in the Windows environment with a different password before you attempted to enroll the user (see “Enroll a single OS/400 user to the Windows environment using iSeries Navigator” on page 99). If the user did exist with a different password, enrollment will have failed. Change the Windows password to match the OS/400 password; then perform the enrollment procedure again.

6. If the problem still persists, check the technical information databases at the [@server](#) IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

IBM iSeries Integration for Windows Server snap-in program

You may experience an error when trying to run the IBM iSeries Integration for Windows Server snap-in program. The program may not start, may provide unexpected information, or an error could occur during use.


If the IBM iSeries Integration for Windows Server snap-in display never appears the following steps can help you determine the problem.

- Check to see if there is already an instance of IBM iSeries Integration for Windows Server snap-in or the Lvlsync program on the system. You can only run one instance of these programs at a time. If there is already an instance of either program in operation, then a new call to either program will return. Finish using the current program before trying to start a new instance.
- Ensure that the user has administrator-level access and special authorities. The IBM iSeries Integration for Windows Server Snap-in programs require these authorizations. Retry starting the program with administrator authority.
- Ensure that you have started iSeries NetServer. iSeries NetServer starts automatically with the QSERVER subsystem on OS/400. Start iSeries NetServer if OS/400 has not already started it.
- Ensure that you have enabled the guest user profile on iSeries NetServer. If not, then enable the guest user profile so that guests can access the iSeries NetServer (see “Create a guest user profile for iSeries NetServer” on page 29). When you have enabled guest access, first stop and then restart iSeries NetServer and then retry running the IBM iSeries Integration for Windows Server snap-in program.
- Check the system event log on the Windows server for any messages pertaining to the IBM iSeries Integration for Windows Server snap-in program.

The IBM iSeries Integration for Windows Server snap-in display may appear, but the information that OS/400 displays may not be what you expected. If so, the following steps can help you determine the problem.

- Verify that the latest service pack PTF is available and in an active state on OS/400. You can use the Display PTF (DSPPTF) command to do this.
- Verify that the service pack you believe that you have installed is actually installed on the integrated server.
- Check the system and application event log on the integrated server for any messages pertaining to the Integration for Windows Server snap-in program.

When you perform an action with the IBM iSeries Integration for Windows Server snap-in program, problems can occur. The following list helps you solve problems that can occur after you click the **OK** button.

- A drive letter must be available for the IBM iSeries Integration for Windows Server snap-in program to proceed. This drive letter need only be available temporarily. If all drive letters are in use, try freeing a drive letter for use with IBM iSeries Integration for Windows Server snap-in and retry the program.
- The IBM iSeries Integration for Windows Server snap-in program takes the specified action. The system may or may not be restarted depending on the set of files updated. It may take a short time for the system shutdown and start up to occur.
- Check the system and application event log on the integrated server for any messages pertaining to the IBM iSeries Integration for Windows Server snap-in program.
- If the problem still persists, check the technical information databases at the [@server](#) IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

Virtual Ethernet connection problems

For the purposes of this section, the virtual Ethernet Point-to-Point (Private LAN) and the virtual Ethernet Ports 0-9 are all considered virtual Ethernet Adapters or virtual Ethernet Ports.

There are two kinds of virtual Ethernet device drivers, virtual Ethernet Adapter (VE) and a virtual Ethernet Data Transport (DT).

- The virtual Ethernet Adapter corresponds to the driver that appears as the adapter, called 'virtual' because no NIC hardware is associated with it.
- The virtual Ethernet Data Transport is the driver that provides a connection to the system bus connecting all the virtual Ethernet networks.

When a VE port cannot communicate across the system bus, it reports that the cable for the port is unplugged (cable disconnected). This is an important concept for troubleshooting virtual Ethernet errors.

The virtual Ethernet Ports under Windows are automatically installed and uninstalled by the virtual Ethernet Utility (VEU). The utility receives signaling through a configuration file from the NWSD. For example, when a user creates a Line Description under the NWSD for a given virtual Ethernet Port the VEU installs the corresponding VE port. Rebooting the Windows server configures the VE port address.

The following virtual Ethernet components use the listed driver.

- virtual Ethernet Adapter: qvndvemp.sys
- virtual Ethernet Data Transport: qvndvedt.sys
- virtual Ethernet Install Utility: qvndveu.exe

Troubleshooting virtual Ethernet problems

When the communication between any VE ports is not functioning, you need to perform two general tasks to troubleshoot the problem.

1. Determine the status of the VE ports.
2. Match the observed results to the following troubleshooting cases.

Determine VE port status

To determine the status of the VE ports.

- Use the iSeries console to determine if a line description for the VE port is created under the NWSD.
- Use the the Windows console to open the **Network and Dial Up Connections** folder and determine if the VE port icon is present.

Match port status with troubleshooting cases

Match results of your determination of the status of the VE ports to one of the following troubleshooting cases.

- "Both line description and icon are present" on page 142.
- "Line description is present and icon is missing" on page 142.
- "Line description is missing and icon is present" on page 143.
- "Both line description and icon are missing" on page 143.

In each case, you must first verify the OS/400 side then verify the Windows side. To verify the Windows side, you may need to open the Event Log and the Device Manager.

- To open the Event Log, from the Windows **Start** menu, select **Programs**, then **Administrative Tools**, then **Event Viewer**.

- To open the Device Manager, from the Windows **Start** menu, select **Settings**, then **Control Panel**, then **Administrative Tools**, then **Computer Management**, then **Device Manager**.

Both line description and icon are present

Verify the OS/400 side

Check the line description. When the line description is in the FAIL state, perform the following steps.

1. Collect PAL[®] entries and VLOGs
2. Contact support
3. Verify the Windows side

Otherwise, when the line description is in the VARY-ON PENDING, VARY-ON, or RCYPND state, verify the Windows side.

Verify the Windows side

Open the **Network and Dialup Connections** window and check the VE icon.

- When the VE icon appears functional and the line description is in the VARY-ON state, verify that the IP addresses are properly configured. If the problem persists, contact support.
- When the VE icon appears functional and the line description is in VARY-ON PENDING or RCYPND state, verify for entries in the PAL and contact support.
- When the VE icon has a red X (cable disconnected), open the Event Log and locate entries for the qvndvemp.sys driver.
 - When you find entries for qvndvemp.sys, record them and contact support. Driver initialization is likely to have failed, and an IOP dump may be required to determine the problem.
 - When you do not find any entries for qvndvemp.sys, contact support and indicate the state of the line description. The problem is likely to be related to an OS/400 LIC problem.

Line description is present and icon is missing

Verify the OS/400 side

Check the line description. When the line description is in the FAIL state, perform the following steps.

1. Collect PAL entries and VLOGs
2. Contact support
3. Verify the Windows side

Otherwise, when the line description is in the VARY-ON PENDING, VARY-ON, or RCYPND state, verify the Windows side.

Verify the Windows side

Open the **Device Manager**, click **Network Adapters** to list the installed adapters, and locate the entry for the VE port.

- When the VE port has a yellow bang, complete the following steps.
 1. Open the Event Log, locate any entries for the qvndvemp.sys driver and record them.
 2. Contact support. The driver failed to initialize, which requires assistance to diagnose the cause.
- When the VE port has a red X, complete the following steps.
 1. Right-click the VE port and select **Enable**.
 2. Open the **Network and Dialup Connections** window and locate the VE icon.
 3. If the VE port icon is missing or it remains gray, open the **Event Log**.

4. Locate entries for the qvndvemp.sys driver, record any that you find, and contact support. The VE port failed to load or start.

Line description is missing and icon is present

Verify the OS/400 side

Verify that no line description is currently present for the VE port under the NWSD, then verify the Windows side.

Verify the Windows side

Open the **Network and Dialup Connections** window and check the VE icon. When the installation VEU failed to remove the VE port, reboot the integrated server to clear this condition. If the problem persists, complete the following steps.

1. Use the VEU to manually remove the VE port by using the following command.

```
qvndveu -a -R -x [port_id]
```

where [port_id] is either a decimal (0-9) that corresponds to the port being removed or p, for Point-to-Point (Private LAN).

2. After running the command, if the VE port icon is no longer present, the process has completed. However, if the VEU failed to uninstall and remove the VE port, continue with the remaining steps.
3. Collect the VEU log file (D:\as400nt\qvndveu.log).
4. Open the **Event Log**, locate any entries for the qvndvemp.sys driver and record them.
5. Contact support. Ensure that you have the following at hand.
 - Any entries that you recorded for qvndvemp.sys
 - The VEU log file that you previously collected

Both line description and icon are missing

Verify the OS/400 side

You must have a line description in the NWSD for a VE port to be installed. Use the instructions found here, "Configure virtual Ethernet networks" on page 65, to create a line description.

Note: To add a line description, the NWSD needs to be varied off. Once you have created the line description and rebooted the integrated Windows server, the installation VEU automatically creates the VE port under Windows.

When a VE port problem persists after you successfully create a line description and reboot the integrated server, come back to this troubleshooting section and follow the instructions for the newly matched failing case.

Verify the Windows side

When no OS/400 line description is present, a VE port should not be listed under Windows. Install the line description as described in "Configure virtual Ethernet networks" on page 65 and restart the integrated server to see if this fixes the problem.

Problems with external networks when using external host LAN

External networks are networks accessed by integrated servers through a physical networking card. Although the networking card is inserted in an iSeries slot, the integrated server has control of it, and OS/400 is not involved. OS/400 is involved, however, when you share the networking card between an integrated server and OS/400 using external host LAN.

This section gives you steps to troubleshoot external network problems from OS/400. If you are using external host LAN and are experiencing problems, then follow the steps in this section to troubleshoot them. For steps to troubleshoot external network problems from an integrated server, see “General problems with external networks” on page 145.

Note: Integrated Netfinity servers support external host LAN. Integrated xSeries Servers do not. When you upgrade to an Integrated xSeries Server, you need to manually remove any line descriptions and TCP/IP interfaces that are associated with external host LAN. See “Delete an integrated Windows server’s line descriptions” on page 126 and “Delete TCP/IP interfaces associated with an integrated Windows server” on page 126.

From OS/400:

- Ensure that you have started TCP/IP services on OS/400 by using the Start TCP/IP (STRTCP) command.
- Review the QSYSOPR message queue for any TCP/IP errors.
- Ensure that you have properly configured the OS/400 TCP/IP address and that this address is unique on the network. You can use option 1 of the Configure TCP/IP (CFGTCP) command to do this.
- Ensure that the line description to which the OS/400 TCP/IP address is bound is the appropriate TCP/IP address for the 6617 or 2850 adapter card.
- If you added a line description for a network adapter on OS/400 after installing the server, ensure that the integrated server Internet address configured in OS/400 matches the one you configured on the integrated server for that adapter.
- Ensure that the TCP/IP interface status is active. To do this, follow these steps.
 1. Use option 1 of the CFGTCP command.
 2. Press F11 to view the interface status.
 3. Type a 9 next to the appropriate network service to start the TCP/IP interface.
 4. Press F5 to refresh the view. The appropriate TCP/IP service should now be active.
- Test the communication link by using the PING command.
 - If you can PING local addresses (those on your network), but not remote addresses, use option 2 (Work with TCP/IP routes) of the Change TCP/IP domain information (CFGTCP) command. Ensure that a *DFTRROUTE entry exists for the local gateway system.
 - If you can PING systems by their IP addresses but not by their system names, use option 12 of the CFGTCP command. Ensure that the name of the system, the domain, and the domain name server addresses are correct.
- If sharing adapters with OS/400, also ensure that you have set the **Network Address** to the same value that appears in the Adapter address field for the corresponding line description of OS/400. To review this, follow these steps.
 1. Click on **Start**, then **Programs**, then **Administrative Tools**, then **Computer Management**, then **System Tools**.
 2. Double-click **Device Manager**.
 3. Expand **Network Adapters**, right-click on the adapter in the list, and select **Properties** from the menu.
 4. Select the **Advanced** tab. From the list of parameters, find the **Network Address** and click to select. Ensure that the **Values** box is filled with the matching iSeries Line Description Local Adapter Address value.
 5. Find and select the **External Phy** parameter. Ensure that the value is set to match the Line Speed and Duplex set in the iSeries Line Description.
 6. On OS/400, use the WRKLIND command and select option 5 on the corresponding line to view the Local Adapter Address, Line Speed, and Duplex values.

- For token-ring networks, ensure that the **Data Rate**, **Duplex**, and **Locally Administered Address** settings match the values on the corresponding line description of OS/400: Line Speed, Duplex, and Adapter Address. To review this, follow these steps.
 1. Select **Control Panel**, then **Network**, then the **Adapters** tab and press the **Properties** button.
 2. Select the **Advanced** tab. From the list of parameters, find the Network Address (LAA) and click to select. Ensure that the Value Box is filled with the matching iSeries Line Description Local Adapter Address value.
 3. Find the Data Rate and Duplex parameters. Select each and ensure that the value is set to match the Line Speed and Duplex set in the iSeries Line Description.
 4. On OS/400, use the WRKLIND command and select option 5 on the corresponding line to view the Line Speed, Duplex, and Local Adapter Address values.
- Ensure that the **IP Address**, **Subnet Mask**, and **Default gateway** values are correct and that each adapter present has a unique IP address. To do this, do the following.
 1. Click on **Start**—>**Settings**—>**Control Panel**, then choose **Network and Dial-up Connections**.
 2. Right-click on **Local Area Connections** and select **Properties** from the menu.
 3. Select **TCP/IP Protocol** from the list of installed protocols and press the **Properties** button.
 4. Check the values for the **IP Address**, **Subnet Mask**, and **Default gateway**. Also ensure that each adapter present has a unique IP address.
- Ensure that all **iSeries Line Multi-Port Protocol Driver** entry is present and enabled under all network adapters. To verify, open **Network and Dial-up Connections**, double-click on each connection, click on the **Properties** button, and ensure that the **iSeries Line Multi-Port Protocol Driver** is listed and selected.
- Test the communication link by using the PING command. You should be able to ping external systems as well as the external LAN port of OS/400 that shares the same physical network adapter.

If the problem has not yet been resolved, continue troubleshooting from the integrated server. See “General problems with external networks”.

General problems with external networks

If you have a problem with an integrated server’s external network

- Review the integrated Windows server event log for either communication errors or device driver errors. You can use the Windows **Event Viewer** to do this. Event logs associated with external adapters supported by 2890, 2892, and 4812 Integrated xSeries Servers may have one of the following in the event log Source field: IBMTRP, PCNET, ALTND5, E100B, or E1000. If you can not find text in event logs for the IBMTRP token-ring service, you need to make changes in the Windows Registry.



Note: If you are not familiar with the process for making changes in the Windows Registry, contact a service representative.

If you are familiar with this process, to make the text in the event logs viewable, complete the following steps.

 1. From the Windows **Start** menu, click **Run**.
 2. Type regedit.
 3. In the Registry Editor, go to
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\IBMTRP
 4. Select **EventMessageFile**.
 5. From the Registry Editor **Edit** menu, select **Modify**.
 6. Type %SystemRoot%\System32\netevent.dll;%SystemRoot%\System32\ibmsgnet.dll
 7. Close the Registry Editor and restart the integrated server.
- When sharing adapters with OS/400, ensure that the drivers **IBM iSeries Line Device Driver Port 1** and **iSeries Line Device Driver Port 2** are listed and have a status of **Enabled**.


1. From Windows, click on **Start**, then **Programs**, then **Administrative Tools**, then **Computer Management**.
 2. Select **System Tools**; then click **Device Manager**.
 3. At the top menu bar, select **View** and from the drop-down menu, select **Show Hidden Devices** to list all drivers.
 4. Expand the **Non-Plug and Play Drivers** entry and locate in the list the **iSeries Line Device Driver Port 1** and **iSeries Line Device Driver Port 2**.
 5. Double-click on each driver and verify that the **Device Usage** is set to **Enable**.
 6. Verify that the **Device Status** window indicates that *This Device is working properly*.
 7. Click **Cancel** to terminate the verification.
- For Ethernet adapters, ensure that a driver with **iSeries** or **AMD PCNET Family Ethernet Adapter (PCI)** in its name is listed and has a status of **started**.
 1. Click on **Start**, then **Administrative Tools**, then **Computer Management**, then **System Tools**, then **Device Manager**, then **Network Adapters**.
 2. Ensure that a driver with **iSeries** or **AMD PCNET Family Ethernet Adapter (PCI)** in its name is listed and has a status of **started**.
 - For token-ring networks, also in **Device Manager**, ensure that you have started the **IBM High-Speed 100/16/4 Token-Ring PCI Adapter** or **IBM PCI Token-Ring Adapter**.

Note: The start up setting should be **Enable**.

- For token-ring networks, ensure that the Network Data Rate setting is appropriate for your network.
- For Ethernet networks, ensure that the Link Speed and Duplex settings are appropriate for your switch or hub. If your 4812 or 5701 does not connect at speeds greater than 100 million bits per second, check your switch's specifications for compliance with the IEEE 802.3ab standard. Windows LAN drivers for 4812 or 5701 gigabit Ethernet ports may be limited to 100 million bits per second when connected to some early model non-compliant switches.
- The 10/100 Mbps Ethernet port on the 2892 Integrated xSeries Server does not support direct connection to certain 10 Mbps hubs and routers that lack **auto-polarity** functionality. If you are having difficulty getting your 2892 10/100 port to work at all with a 10 Mbps hub or router, check its specifications for **auto-polarity** support. Also, see if your 2892 10/100 port works with other devices.
- If the problem still persists, check the technical information databases at the  IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

Manually update LAN drivers on the integrated Windows server

Windows 2000 Server and Windows Server 2003 generally automatically install LAN drivers that are appropriate for your LAN adapters and ports. However, if you have a special situation you can manually install or update a LAN driver.

To manually install or update a LAN driver for an adapter other than virtual Ethernet in an externally attached Netfinity or xSeries server, go to the IBM Personal computing support Web site  and select **Servers**, then **Device driver file matrix**.

To manually install or update a LAN driver for an adapter or port in an Integrated xSeries Server or for virtual Ethernet, complete the following tasks.

1. "Begin the LAN driver installation or update."
2. "Select the adapter to install or update" on page 147.
3. "Complete the LAN driver installation or update" on page 147.

Begin the LAN driver installation or update

To begin the manual installation or update of the LAN driver or port in an Integrated xSeries Server or for virtual Ethernet, complete the following steps.

1. From the Windows **Start** menu, select **Settings**, then **Control Panel**.
2. Double-click **System**.
3. In the **System Properties** window, select the **Hardware** tab.
4. If the new LAN driver is not digitally signed, or if you are unsure whether or not the LAN driver is digitally signed, ensure that the driver signing policy is set to Ignore.
 - a. In the **System Properties** window, click **Driver Signing**.
 - b. Note the current setting, then click **Ignore**, and then click **OK**.
5. Click **Device Manager**.
6. "Select the adapter to install or update."

Select the adapter to install or update

After you complete the steps to begin the installation or update (see "Begin the LAN driver installation or update" on page 146) of the LAN driver or port in an Integrated xSeries Server or for virtual Ethernet, you will need to select the adapter.

To select the adapter that you want to install or update, complete the following steps.

1. In the **Device Manager** window, open **Network Adapters**.
2. Under **Network Adapters**, right-click the adapter that you want to update and select **Properties**.
3. In the **Properties** windows for the adapter, click the **Driver** tab.
4. Click **Update Driver** or **Install Driver** (only one will display).
5. In the **Update Device Driver Wizard** dialog, click **Next**.
6. "Complete the LAN driver installation or update."

Complete the LAN driver installation or update

Ensure that you have completed the first two tasks required to manually install or update the LAN driver or port in an Integrated xSeries Server or for virtual Ethernet.

- "Begin the LAN driver installation or update" on page 146.
- "Select the adapter to install or update."

To complete the LAN driver or port installation or update, use one of the following procedures that fits your situation.

- You are using Windows Server 2000 or have been directed to install the LAN driver from a specific folder for Windows 2003 Server.
- You are using Windows 2003 Server and have not been directed to install the LAN driver from a specific location.

If you are using Windows Server 2000, or if you have been directed to install the LAN driver from a specific location for Windows 2003 Server.

To complete the LAN driver installation or update, perform the following steps.

1. Select **Display a list of the known drivers for this device so that I can choose a specific driver** and click **Next**.
2. Click **Have Disk** to open the **Install From Disk** dialog and specify the location of the driver.
 - If you were directed to install the driver from a specific drive and folder, click **Browse** to specify the location, then click **Open**.
 - Otherwise, click **Browse** to specify the location on the system drive (typically C:) of the driver that corresponds to the adapter that you are installing or updating. Use the following list to locate the folder that contains the driver for your specific hardware.
 - \wsv\ibm for hardware types 2724 and 2744
 - \wsv\alt for hardware types 2743 and 2760

- | – \wsv for virtual Ethernet
 - | – \wsv\amd for hardware types 2723 and 2838 in Windows 2000
 - | – \windows\inf for hardware types 2723 and 2838 in Windows Server 2003
 - | – \wsv\it1 for hardware type 2892 in Windows 2000
 - | – \wsv for hardware type 2892 in Windows Server 2003
 - | – \wsv\alt for hardware types 4812, 5700, and 5701 in Windows 2000
 - | – \wsv\itg for hardware type 4812, 5700, and 5701 in Windows Server 2003
3. Click **OK**.
 4. In the **Update Device Driver Wizard** dialog, if the appropriate driver is not already highlighted, select it from the list, then click **Next**.
 5. Click **Next** again.
 6. If there is a Ret Code 22 when the Update Driver procedure completes, the adapter may be disabled. To enable the adapter in this case, in the **Device Manager** window, right-click the disabled adapter and select **Enable**.
 7. If you want to install or update more adapters, see “Select the adapter to install or update” on page 147.
- Note:** If Windows indicates that a restart is needed after any driver update, defer it until there are no more adapters to update.
8. If you changed the driver signing policy when you began the installation or update (see “Begin the LAN driver installation or update” on page 146), restore the original policy.

If you are using Windows 2003 Server and you have not been directed to install the LAN driver from a specific location.

To complete the LAN driver installation or update, perform the following steps.

1. Select **Search for a suitable driver for my device** and click **Next**.
 2. Click **Next** to show compatible hardware.
 3. Deselect all **Optional search locations**, click **Next**, then click **Next** again.
 4. If there is a Ret Code 22 when the Update Driver procedure completes, the adapter may be disabled. To enable the adapter in this case, in the **Device Manager** window, right-click the disabled adapter and select **Enable**.
 5. If you want to install or update more adapters, see “Select the adapter to install or update” on page 147.
- Note:** If Windows indicates that a restart is needed after any driver update, defer it until there are no more adapters to update.
6. If you changed the driver signing policy when you began the driver installation or update (see “Begin the LAN driver installation or update” on page 146), restore the original policy.

Private LAN IP address conflicts

IBM iSeries Integration for Windows Server uses IP addresses in the range of 192.168.x.y for the integrated server’s private local area network (LAN). By default, the actual addresses are selected by the OS/400 Install Windows server (INSWNTSVR) command. For details and examples, see “Assign private LAN IP addresses” on page 149. Depending on your network, there could be conflicts with addresses that are already in use. To avoid potential conflicts you can use the VRTPTPPORT parameter for an Integrated xSeries Server or Integrated xSeries Adapter attached xSeries server, and the INTLANPORT parameter for the Integrated Netfinity Server.

If a conflict requires you to change the addresses, you must ensure that the private LAN occupies its own subnet on OS/400. The subnet mask that is used is 255.255.255.0. To ensure that the private LAN is on

its own subnet, use IP addresses of the form a.b.x.y, where a.b.x is the same value for both sides of the internal LAN. Also verify that the value of a.b.x is unique on your network.

To change the private LAN addresses because of a conflict, take the following action.

1. At the OS/400 console, enter the command `DSPNWSN NWSN(name) OPTION (*PORTS)`. Make a note of the Attached line for the port number `*VRTETHPTP` or `*INTERNAL`, which is also known as the line description.
2. Use the Configure TCP (CFGTCPIP) command and option 1 to display the TCP interfaces. Make a note of the IP address and the subnet mask associated with the line description that you found in step 1.

Note: An IP address entered at the Windows console for the private LAN overrides the values that are set in the NWSN for the TCPPRTCFG parameters `*INTERNAL` or `*VRTETHPTP`.

1. Click on **Start**—>**Settings**—>**Control Panel**, then **Network and Dial-up Connections**.
2. Right-click on the correct **Local Area Connection** for the private LAN and select **Properties** from the menu.
3. Select **TCP/IP Protocol** from the list of installed protocols and press the **Properties** button to display the TCP/IP properties.
4. Change the IP address for the new value that you have selected.
5. Click **OK**, then **Close** to close the application.
6. Shut down the integrated Windows server without doing a restart.
7. On OS/400, vary off the NWSN.
8. Use the Remove TCP/IP interface (RMVTCPIFC) command with the IP address you recorded in step 2.
9. Use the Add TCP/IP interface (ADDTCPIFC) command to add the new interface. Use the IP address that you selected for the OS/400 side of the private LAN. You also need to enter the subnet mask and line description that you recorded in steps 1 and 2.
10. On the OS/400 command line, type `CHGNWSN NWSN(name)`, and press F4.
 - a. Page down to the section labeled TCP/IP port configuration.
 - b. Change the IP address in the Internet address field for the port `*VRTETHPTP` or `*INTERNAL` to the value that you used in step 3. Press Enter for the change to take effect.
 - c. Vary on the NWSN.

Note: If you are installing multiple servers, to avoid further conflicts, assign private LAN IP addresses (see “Assign private LAN IP addresses”) instead of letting the INSWNTSVR command generate them. The Internal LAN port parameter allows you to enter IP addresses that you know to be unique on your system.

Assign private LAN IP addresses

By default, the Install Windows server (INSWNTSVR) command assigns private LAN IP addresses of the form 192.168.x.y. To avoid potential conflicts, you can use the INTLANPORT or VRTPTPPORT parameter on this command to assign IP addresses that you know are unique on your system.

If you let the command assign addresses and then discover a conflict, you can change the IP addresses. The command assigns to x a value that is based on the resource number of the Integrated xSeries Server. The command looks for a pair of values y and y+1 (starting with y=1), with addresses that are not in use on that OS/400. The command assigns the lower number of the pair to the OS/400 side of the private LAN and the higher number to the Windows server side.

For example, suppose you have a 2892 Integrated xSeries Server with a resource name of LIN03. After running the Install Windows Server (INSWNTSVR) command you might end up with the following addresses for the internal LAN.

192.168.3.1 (OS/400 side)
192.168.3.2 (Windows server side)


In case of a conflict on a server that you have installed, verify that a particular substitute value (for example, 192.168.17) is not used on your network and change the IP addresses to that value.

192.168.17.1 (OS/400 side)

192.168.17.2 (Windows server side)

Be aware that an IP address entered at the Windows console for the private LAN overrides the value set in the NWSD for the TCPPOPTCFG parameters *INTERNAL or *VRTETHPTP port .

If the problem still persists, check the technical information databases at the  IBM iSeries

Support Web page  . If you cannot find the solution there, contact your technical support provider. If the problem persists, contact IBM for service.

IP forwarding problems



By default IP forwarding is disabled for Windows 2000 Server and Windows Server 2003. When the IP forwarding function is enabled, OS/400 should not use the LAN adapters on the Integrated xSeries Server. This means that you should not create a line description for the adapters. However, a line description for the *INTERNAL or *VRTETHPTP line is always required. Not observing this restriction can cause a TCP/IP packet storm. Note that this restriction applies only when IP forwarding is enabled for Windows server, not when IP Forwarding is enabled for OS/400.

To verify or change the setting of the IP forwarding function for an integrated Windows server, do the following.

On Windows 2000 Server or Windows Server 2003, IP forwarding is a registry entry. Refer to Microsoft documentation on how to disable IP forwarding.

If IP forwarding on an integrated Windows server is required, do one of the following.

- If you are installing a new integrated server, install it without creating line descriptions for the external ports. To do that, use the Install Windows server (INSWNTSVR) command to define ports 1 and 2 as (*NONE).
 1. At the OS/400 command line, enter INSWNTSVR PORT1(*NONE) PORT2(*NONE).
- If the server is already installed, remove the line descriptions for the external ports. Perform the following steps.
 1. At the OS/400 command line, enter the Display NWSD (DSPNWSD) command, and look at the attached lines. Note the names of the attached lines for ports 1 and 2.
 2. Enter the Work with Line Descriptions (WRKLIND) command.
 3. In the Opt column next to the line descriptions for the external ports of the NWSD that you noted, type option 4 (delete) and press Enter.

Attention: The line description for the *INTERNAL line is always required, so be careful not to delete it.
- If the problem still persists, check the technical information databases at the  IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

TCP/IP failure between OS/400 and Windows

1. Verify that the private LAN (internal token ring or virtual Ethernet point-to-point) IP Address was configured and that the default DHCP is not being used. If during the install the Private LAN IP Address was set, not all the following steps are required.
 - a. Click **Start** —> **Settings** —> **Control Panel**.
 - b. Open **Network and Dial-up Connections** .
 - c. Find the IBM Private LAN Adapter connection and double-click to open.
 - d. Click on the **Properties** button.

- e. Select the Internet Protocol (TCP/IP)
- f. Click on the **Properties** button. If the **Use the Following IP Address** is selected and the IP address from the OS/400 console is displayed, you do not need to proceed any further. If the Obtain an IP address automatically is selected, continue with the next step.
- g. Select the radio button: **Use the Following IP Address**.
- h. On an OS/400 command line, type the following command, where 'nwsd' is the name of the NWSD for your server, then press Enter; DSPNWSD NWSD(nwsd) OPTION(*TCPIP)
 - On the DSPNWSD dialog, find the port named *INTERNAL. This shows the IP address and subnet mask values for the Private LAN.
 - On the integrated server console, type the Private LAN IP address and subnet mask values that were shown by the DSPNWSD command.
- Note:** An IP address entered at the integrated server console for the private LAN overrides the values set in the NWSD for the TCPPRTCFG parameters *INTERNAL or *VRTETHPTP port.
- i. Click OK.
- j. Click OK.
- k. Click Close.

The process is complete and the Private LAN should now be active.

Attention: If you plan to use a firewall with an integrated server, be sure not to route the Internet addresses for the private LAN to a software common knowledge IR system (SOCKS) server acting as a firewall. Doing so causes connection failures. For information about setting up a firewall, see the topic Firewall: getting started.

Problems accessing Windows Server 2003 shares using the QNTC file system

If you cannot use the OS/400 QNTC file system to access shares on a Windows Server 2003 server that has Active Directory installed (for example, it is a domain controller), then you may need to do some additional setup. See “Enabling QNTC access to Windows Server 2003 with Active Directory” on page 59.

IFS access problems

When you try to access the OS/400 integrated file system (IFS) from an integrated Windows server through iSeries NetServer, the access may fail in the following situation.

- If you are using a Universal Naming Convention (UNC) name with an IP address in it and
- Both private and external LAN paths exist between the integrated Windows server and OS/400

Either change the UNC name to use the iSeries NetServer name instead, or disable the external LAN path and then retry the operation that failed.

Problems with saving integrated Windows server files

If you have problems with doing file-level backup of your integrated server files, check the Windows event log and OS/400 QSYSOPR message queue for messages.

- If you get a session initialization error (CPDB050) or session communication error (CPDB055) when you try to save files, do this.
 1. Ensure that OS/400 NetServer is in the same domain (see “Ensure iSeries NetServer and the integrated Windows server are in same domain” on page 117) as the integrated server for which you want to save files.
 2. Ensure that you complete the steps “Create shares on integrated Windows servers” on page 116 and “Add members to QAZLCSAVL file” on page 117.
 3. Ensure that the QSERVER subsystem is running.

4. Ensure that TCP/IP is active:
 - a. Use option 1 of the CFGTCP command.
 - b. Press F11 to view the interface status.
 - c. Type a 9 next to the appropriate network service to start the TCP/IP interface.
 - d. Press F5 to refresh the view. The appropriate TCP/IP service should now be active.
5. Then try saving your files again.
- If you get an error message that indicates a problem with exchanging security information (CPDB053) or logging on to the server (NTA02AE), do this:
 1. Ensure that you are enrolled on the integrated server as part of the Administrators group.
 2. Ensure that you have the same password on OS/400 and on the integrated server.
 3. Then try saving your files again.
- If you get an error message (CPDB058) that indicates a problem with processing the share file member, ensure that the QAZLCSAVL file is set up correctly.
 1. Check that you have completed this step: “Create shares on integrated Windows servers” on page 116.
 2. As well as this step: “Add members to QAZLCSAVL file” on page 117. Also you must have listed in that file the share that you specified on the Save (SAV) command.
- If you get an error message (NTA02A3) that indicates a problem communicating with NTSAV, verify that the Remote Procedure Call service is running.
 1. On the integrated server task bar, click **Start** —> **Programs** —> **Administrative Tools**.
 2. Double-click **Services**.
 3. Verify that the Remote Command Service is running.
- The following errors may appear when doing a SAV.
 - CPFA09C Not authorized to object
 - CPD3730 Cannot save directory /qntc/(server)/(share)/System Volume Information



These errors indicate that the directory, **System Volume Information**, was not saved. This is a hidden, system directory that can be accessed only by the Windows SYSTEM account. If you ignore this message, the directory and its contents will not be saved (it contains intermediate log files used when encrypting files). Otherwise, you can add permissions for the user who is running SAV to this directory. To set the permissions, you will need to make the directory visible (don't hide hidden files, and don't hide protected operating system files). Refer to the Windows 2000 Server or Windows Server 2003 help for information on setting folder permissions.

You may also see a CPFA09C error if you run file-level backup as QSECOFR, whether QSECOFR is enrolled to the server or not. Use a different enrolled user profile that has a backup on the integrated server.

Unreadable messages in the server message queue

Windows event log messages do not display correctly if the message queue coded character set identifier (CCSID) is set to *HEX (65535). If you get unreadable messages in the server message queue (identified by the MSGQ parameter of the NWSD), take the following action.

1. At the OS/400 console, enter the command CHGMSGQ to change the server message queue CCSID to something other than *HEX (65535), for example *MSG.

For example, if the message queue name is MYSVRQ in library MYLIB, then you can use the following command on OS/400 to change the message queue CCSID: CHGMSGQ MSGQ(MYLIB/MYSVRQ) CCSID(*MSG).
2. If the problem still persists, check the technical information databases at the  **server** IBM iSeries Support Web page  . If you cannot find the solution there, contact your technical support provider.

Problems getting a Windows system memory dump


If sufficient space is available on the system drive, your integrated Windows server is automatically configured to collect a system memory dump when a STOP error or blue screen occurs. If a system memory dump is not collected, do the following.

1. Select **Start**, then **Programs**, then **Administrative Tools**.
2. Click on **Computer Management**.
3. In the **Action** menu, click on **Properties**.
4. Select the **Advanced** tab
5. Click the **Startup/Recovery** button.
6. Check the **Write debugging information to:** box. The default path to the memory.dmp file that is created when a blue screen occurs is %SystemRoot%, which is C:\WINNT (E:\WINNT for servers installed prior to V4R5) for Windows 2000 Server and C:\WINDOWS for Windows Server 2003.

Other problems that can prevent a system-memory dump from being taken include.

- Insufficient paging file size specified. The paging file size must be large enough to hold all of physical RAM, plus 12 MB. To verify the amount of physical RAM on your machine, do the following.
 1. Select **Start**, then **Settings**, then **Control Panel**.
 2. Double-click on **System**. The value listed under **Computer** on the **General** page indicates the amount of physical RAM you have on your system.

To verify or change the paging file size, do the following.

1. Select the **Advanced** tab, and click on the **Performance Options** button of the **Virtual Memory** section. The **Virtual Memory** part of the window shows the current paging file size.
 2. If you need to change the paging file size, click the **Change** button.
- The paging file is not located on the system drive. A system memory dump is not collected unless the paging file is located on the system drive. The system drive for V4R5 and later releases of Windows environment on iSeries is the C: drive; for earlier releases it is the E drive. To verify or change this, do the following.
 1. Select the **Advanced** tab, and click on the **Performance Options** button of the **Virtual Memory** section.
 - Insufficient space is available on the drive you specified as the path to the memory.dmp file. The default path for the memory.dmp file is the system drive, but you may change it to another drive. Verify that sufficient free space exists on the system drive or the drive you chose if you changed it. The free space needed is equal to the size of physical RAM, plus 12 MB.
 - If the problem still persists, check the technical information databases at the [@server IBM iSeries Support Web page](#) . If you cannot find the solution there, contact your technical support provider.

Reinstall an integrated Windows server

If an integrated Windows server becomes damaged, you may be able to preserve installed applications and user data by reinstalling it. Try either logging on or starting up with DOS by using the Boot menu of the NT loader (NTLDR). (This is only possible if the boot drive is still formatted as FAT.) You can then reinstall Windows server. Doing this returns the system to the base level code of Windows server originally installed. You must then reapply any Microsoft service packs that you had installed. You should also reinstall the latest IBM iSeries Integration for Windows Server service pack.

To reinstall Windows server, try this.

1. “Start and stop an integrated server” on page 75
2. At the boot menu, select to boot PC-DOS or Windows server, whichever is working.
3. If you selected Windows server, open an MS-DOS window.
4. In the DOS window, enter this:


```
D:
cd \i386
winnt /s:D:\i386 /u:D:\unattend.txt
```

5. Press Enter.

Note: The network drives may become so damaged that you cannot log on to the integrated Windows server or start up with DOS. In this case, try restoring all predefined and user-defined storage spaces from usable backups. See “Back up predefined disk drives for integrated Windows servers created on V4R5 and later OS/400 systems” on page 110 and “Back up user-defined disk drives for an integrated Windows server” on page 112.

Windows 2000 Server and Windows Server 2003 also provide the Windows Recovery Console, which is a command-line console that provides limited access to the system to perform many administrative tasks or repair the system. Refer to the Windows 2000 Server or Windows Server 2003 documentation for additional information.

You may also have to reinstall from the very beginning by following this procedure: “Start the installation from the OS/400 console” on page 44.

Collect integrated Windows server service data

If you need to supply service data to support personnel, first consult the OS/400 logs (see “Check message and job logs” on page 129) and the Windows event log. You can also make a copy of the Windows event logs on OS/400 (see “Message logging” on page 78) and make Windows server dumps for remote troubleshooting. These topics help you create dumps to collect further diagnostic information.

1. “Create an integrated Windows server memory dump on OS/400.”
2. To find out how this dump can tell you which configuration and log files to look at first, refer to “Use the network server description (NWSD) dump tool on OS/400” on page 155

Create an integrated Windows server memory dump on OS/400

You can create a Windows memory dump file on OS/400 to help you solve integrated server problems. When you install Windows server on iSeries, by default the dump goes to the system drive.

- C:\WINDOWS\Memory.Dmp for Windows Server 2003.
- C:\WINNT\Memory.Dmp for Windows 2000 servers installed on V4R5 or later.
- E:\WINNT\Memory.Dmp for Windows 2000 servers installed prior to V4R5.

Note: For Windows to successfully create a complete memory dump the pagefile must reside on the system drive and be at least equal to the memory size plus one megabyte. The memory contents are written into the pagefile during the dump. This is the first step in the memory dump process. During the second step the data from the pagefile is written to the actual dump file. This step occurs when the system is booted again after the dump. The drive that contains the memory dump file (memory.dmp by default) must have free space at least as large as the amount of installed memory.

The memory dump is enabled by default if the system drive has enough room for the paging file. To verify that the memory dump support is enabled or to write the memory.dmp file to a different drive, follow these steps.

1. Go to **Start**, then **Settings**, then **Control Panel**.
2. Open the **System** application.
 - Click the **Advanced** tab, then the **Startup and Recovery** button.
3. Click on the **Write Debugging Information To** check box.
4. Change the location of the dump file if necessary.
5. If you want the system to overwrite the file every time a Kernel STOP Error occurs, click on the **Overwrite any Existing File** check box.

6. Select the appropriate type of memory dump (Small Memory Dump, Kernel Memory Dump, or Complete Memory Dump) based on the size of the page file and the amount of free space available on the system drive.
7. Click **OK**.

Use the network server description (NWS) dump tool on OS/400

You can use the network server description (NWS) dump tool (QFPDMPLS) to dump the different configuration and log files that are used with your integrated Windows server. To do this you need *ALLOBJ special authority.

To do this, take these steps:

1. Vary off the *WINDOWSNT NWS (see “Start and stop an integrated server” on page 75).

Attention: If you do not vary off the NWS before running QFPDMPLS, you risk possible data corruption of the predefined storage spaces for the network server.

2. At the OS/400 command line, type

```
CALL QFPDMPLS PARM(nwsdname)
```

where nwsdname is the network server description name.

The program creates a database file QGPL/QFPNWSMPL with multiple members. Each database file member name has the NWS name followed by two digits (01 - 99). For example, for an NWS named MYSERVER, the first member name would be MYSERVER01.

3. Display the member to see the contents of the different files associated with your server description. Different files are important for problem analysis, depending on which installation step is causing a problem.
4. Refer to the following table to note the importance of each file during a particular installation step. If a file is marked 1, refer to it first during problem analysis, 2 second, and 3 last. Files that are not marked are not relevant to installation, but may be relevant at other times. Some members are not created until the post-installation phase.

Note: You cannot use QFPDMPLS to retrieve files on the system drive if you convert the drive to NTFS.

You may not find all the files listed below on some servers. If a particular file is not found, the file will not be retrieved by the QFPDMPLS API and the corresponding database member will not be created.

NWS configuration and log files

Member Name	Data Type	File Name	Windows Directory	Install	Post-Install
nwsdname01	Txt	CONFIG.SYS	C:\	3	3
nwsdname02	Txt	AUTOEXEC.BAT	C:\	2	2
nwsdname03	Txt	BOOT.INI	C:\		
nwsdname04	Txt	HOSTS	C:\ or D:\		3
nwsdname05	Txt	QVNI.CFG	C:\ or D:\		
nwsdname06	Txt	QVNACFG.TXT	C:\ or D:\		
nwsdname07	Txt	QVNADAEM.LOG	C:\ or D:\		
nwsdname08	Bin	HOSTLANI.CFG	C:\ or D:\		
nwsdname09	Bin	HOSTLAN1.CFG	C:\ or D:\		
nwsdname10	Bin	HOSTLAN2.CFG	C:\ or D:\		
nwsdname11	Txt	DUMPFIL.C01	C:\		
nwsdname12	Bin	DUMPFIL.C01	C:\		
nwsdname13	Txt	DUMPFIL.C02	C:\		
nwsdname14	Bin	DUMPFIL.C02	C:\		
nwsdname15	Txt	UNATTEND.TXT	D:\	1	

Member Name	Data Type	File Name	Windows Directory	Install	Post-Install
nwsdname16	Txt	INSWNTSV.LNG	D:\	2	
nwsdname17	Txt	INSWNTSV.VER	D:\	2	
nwsdname18	Txt	QVNADAEM.LOG	D:\		
nwsdname19	Txt	QVNARCMD.LOG	D:\		
nwsdname20	Txt	QVNDT400.LOG	D:\		
nwsdname21	Txt	QVNDHLE1.LOG	D:\AS400NT		
nwsdname22	Txt	QVNDHLE2.LOG	D:\AS400NT		
nwsdname23	Txt	QVNDVSTP.LOG	D:\		
nwsdname24	Txt	QVNDVSCD.LOG	D:\		
nwsdname25	Txt	QVNDVSDD.LOG	D:\		
nwsdname26	Txt	EVENTSYS.TXT	D:\		
nwsdname27	Txt	EVENTSEC.TXT	D:\		
nwsdname28	Txt	EVENTAPP.TXT	D:\		
nwsdname29	Txt	PERFDATA.TSV	D:\		
nwsdname30	Txt	REGSERV.TXT	D:\		
nwsdname31	Txt	REGIBM.TXT	D:\		
nwsdname32	Txt	REGIBMCO.TXT	D:\		
nwsdname33	Txt	DUMPFIL.E.D01	D:\		
nwsdname34	Bin	DUMPFIL.E.D01	D:\		
nwsdname35	Txt	DUMPFIL.E.D02	D:\		
nwsdname36	Bin	DUMPFIL.E.D02	D:\		
nwsdname37	Txt	HOSTS	(for V4R5) C:\WINNT\SYSTEM32\DRIVERS\ETC (prior releases) E:\WINNT\SYSTEM32\DRIVERS\ETC		3
nwsdname38	Txt	LMHOSTS	(for V4R5) C:\WINNT\SYSTEM32\DRIVERS\ETC (prior releases) E:\WINNT\SYSTEM32\DRIVERS\ETC		3
nwsdname39	Bin	MEMORY.DMP	(for V4R5) C:\WINNT (prior releases) E:\WINNT		
nwsdname40	Txt	VRMFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\VRM		
nwsdname41	Txt	PTFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname42	Txt	PTFUNIN.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname43	Txt	A4EXCEPT.LOG	D:\		
nwsdname44	Txt	DUMPFIL.E.E01	E:\		
nwsdname45	Bin	DUMPFIL.E.E01	E:\		
nwsdname46	Txt	DUMPFIL.E.E02	E:\		
nwsdname47	Bin	DUMPFIL.E.E02	E:\		
nwsdname48	Txt	CMDLINES.TXT	D:\386\SOEM\$	2	
nwsdname49	Txt	QVNABKUP.LOG	D:\AS400NT		
nwsdname50	Txt	QVNADAEM.LOG	D:\AS400NT		
nwsdname51	Txt	QCONVGRP.LOG	D:\AS400NT		
nwsdname52	Txt	SETUPACT.LOG	C:\WINNT	1	
nwsdname53	Txt	SETUPAPI.LOG	C:\WINNT	1	
nwsdname54	Txt	SETUPERR.LOG	C:\WINNT	1	
nwsdname55	Txt	SETUPLOG.TXT	C:\WINNT	1	
nwsdname56	Txt	VRMFLOG.TXT	D:\AS400NT		
nwsdname57	Txt	PTFLOG.TXT	D:\AS400NT		
nwsdname58	Txt	PTFUNIN.TXT	D:\AS400NT		
nwsdname59	Txt	VRMLOG.TXT	C:\WINNT\AS400WSV\SERVICE\VRM		

Member Name	Data Type	File Name	Windows Directory	Install	Post-Install
nwsdname60	Txt	PTFLOG.TXT	C:\WINNT\AS400WSV\SERVICE\SERVPACK		
nwsdname61	Txt	PTFUNIN.TXT	C:\WINNT\AS400WSV\SERVICE\SERVPACK		
nwsdname62	Txt	QVNDHLIU.LOG	D:\AS400NT		
nwsdname63	Txt	QVNDHLI.LOG	D:\AS400NT		
nwsdname64	Txt	QVNDHLM.PLOG	D:\AS400NT		
nwsdname65	Txt	QVNDHLP1.LOG	D:\AS400NT		
nwsdname66	Txt	QVNDHLP2.LOG	D:\AS400NT		
nwsdname67	Txt	QVNDVEU.LOG	D:\AS400NT		
nwsdname68	Txt	SERVICE.LOG	D:\AS400NT		
nwsdname69	Txt	LVDELOEM.LOG	D:\AS400NT		
nwsdname70	Txt	INVOKINF.LOG	D:\AS400NT		
nwsdname71	Txt	LVMASTER.LOG	D:\AS400NT		

Chapter 14. Network server description configuration files

You can customize your integrated Windows servers by creating your own configuration files. For example, you might want to change screen resolution or suppress installation of the IPX protocol. You can do this by following these steps.

1. Create an NWSD configuration file. See “Network server descriptions” on page 31.
2. Specify this file with the `Configuration file` parameter when you install a server or create or change a network server description.

Each time the network server starts, OS/400 uses the configuration file to change the specified integrated server file on the server’s C or D drive.

When the Install Windows server (INSWNTSVR) command activates the integrated server, it generates a Windows unattended installation setup script file (UNATTEND.TXT). By specifying your configuration file on the INSWNTSVR command, you can use this file during the installation to modify the UNATTEND.TXT file.

Attention: Be careful what you change with configuration files. Avoid removing device drivers from UNATTEND.TXT, for example, or changing the OEM section or the section that installs TCP. Otherwise, your changes could prevent your server from starting. If you are creating a configuration file to modify an installed server, first make a backup copy of whatever files you plan to change.

- To see how your system drive is formatted, you can use the Work with Network Server Storage Spaces Command (WRKNWSSTG) command.
- Before creating a configuration file, read “NWSD configuration file format.” This section tells you how to use each entry type.
- You should also read this topic, “Use substitution variables for keyword values” on page 169, to see what variables are available for you to use and how to create your own list.
- You might also want to read: “Example: NWSD configuration file” on page 160.
- Then you are ready to follow this procedure: “Create an NWSD configuration file” on page 160.

If you have problems starting a server after you create a configuration file, see “NWSD configuration file errors” on page 136.

NWSD configuration file format

An NWSD configuration file consists of multiple occurrences of **entry types**, each with a different function. The entry types are:

“Remove lines from an existing integrated server file with CLEARCONFIG entry type” on page 161

Use this entry type if you want to remove all lines from the integrated server file.

“Change an integrated server file with ADDCONFIG entry type” on page 162

Use this entry type to add, replace, or remove lines in the integrated server file.

“Change an integrated Windows server file with UPDATECONFIG entry type” on page 166

Use this entry type to add or remove strings within lines in the integrated server file.

“Set configuration defaults with the SETDEFAULTS entry type” on page 167

Use this entry type to set the default values for certain keywords. OS/400 uses the defaults only when processing ADDCONFIG and UPDATECONFIG entries in the current file member.

An **entry** is one occurrence of an entry type. Each entry contains a series of keywords that are followed by equal signs (=) and values for those keywords.

Format guidelines

- Source physical file record length must be 92 bytes.
- A line can have only one entry, but an entry can occupy multiple lines.
- You can use blank spaces between the entry type and the keyword, around the equal sign, and after the commas.
- You can use blank lines between entries and between keywords.

Keywords

- You can put entry keywords in any order.
- Use a comma after all keyword values except the last one in the entry.
- Enclose keyword values in single quotation marks if they contain commas, blank spaces, asterisks, equal signs, or single quotation marks.
- When you use keyword values that contain single quotation marks, use two single quotation marks to represent a quotation mark within the value.
- Keyword value strings can have a maximum length of 1024 characters.
- Keyword values can span lines, but you must enclose the value in single quotation marks. The value includes leading and trailing blanks in each line.

Comments

- Begin comments with an asterisk (*).
- You can put a comment on its own line or on a line with other text that is not part of the comment.

Create an NWSD configuration file

Before creating a configuration file, read the topics “NWSD configuration file format” on page 159 and “Use substitution variables for keyword values” on page 169. You might also want to read “Example: NWSD configuration file.”

To create an NWSD configuration file, do this:

1. Create a source physical file.
 - a. At the OS/400 command line, type CRTSRCPF and press F4.
 - b. Supply a name for the file, any text you want to describe it, and a member name and press Enter to create the file.
2. Use an available editor to add syntactically correct entries to the file that fit the NWSD. See “NWSD configuration file format” on page 159. For example, you can use the Work with members using PDM (WRKMBRPDM) command:
 - a. At the OS/400 command line, type WRKMBRPDM file(*yourfilename*) mbr(*mbrname*) and press Enter.
 - b. Type 2 next to the file you want to edit.

Example: NWSD configuration file

This example configuration file:

- Sets a default file path
- Deletes the time zone and uses a configuration variable to add it back
- Sets default search values that cause the display configuration lines to be added before the UserData section
- Adds lines that configure the display

```
+-----+
| ***** Beginning of data ***** |
| ***** |
| * Update D:\UNATTEND.TXT |
| ***** |
| * |
| ***** |
+-----+
```



```

* Set default directory and file name values.
=====
SETDEFAULTS TARGETDIR = 'D:\', TARGETFILE = 'UNATTEND.TXT'
*
=====
* Delete and use a substitution variable to re-add TimeZone line.
=====
ADDCONFIG VAR      = 'TimeZone', ADDWHEN = 'NEVER', DELETEWHEN = 'ALWAYS'
ADDCONFIG ADDSTR = 'TimeZone="%TIMEZONE%"',
FILESEARCHSTR = '%FPA_L_BRACKET%GuiUnattended%FPA_R_BRACKET%'
*
* Add lines to configure the display.
=====
* Set default search values to add new statements to the file
* before the UserData section header line.
SETDEFAULTS FILESEARCHSTR = '%FPA_L_BRACKET%UserData%FPA_R_BRACKET%',
FILESEARCHPOS = 'BEFORE'
*
* Add the display statements to the file.
ADDCONFIG ADDSTR = '%FPA_L_BRACKET%Display%FPA_R_BRACKET%',
UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'ConfigureAtLogon = 0', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'BitsPerPel = 16', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'XResolution = 640', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'YResolution = 480', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'VRefresh = 60', UNIQUE = 'YES'
ADDCONFIG ADDSTR = 'AutoConfirm = 1', UNIQUE = 'YES'
*
-----

```

Remove lines from an existing integrated server file with CLEARCONFIG entry type

You can use the CLEARCONFIG entry type to remove all lines from an existing integrated server file.

Attention: Removing all lines from the integrated server file may result in your being unable to vary on the network server. If you have problems, see “NWSD configuration file errors” on page 136.

To clear an integrated server file, create an NWSD configuration file that contains the CLEARCONFIG entry type as follows.

```

CLEARCONFIG
LINECOMMENT = '<"REM "|<comment_string>>', (optional)
TARGETDIR = '<BOOT|path>', (optional)
TARGETFILE = '<file_name>' (required)

```

For a detailed explanation of the CLEARCONFIG keywords, use the following keyword links. You can also go back to “NWSD configuration file format” on page 159, or on to “Change an integrated server file with ADDCONFIG entry type” on page 162.

- “LINECOMMENT keyword” on page 164
- “TARGETDIR keyword”
- “TARGETFILE keyword” on page 162

TARGETDIR keyword

Use TARGETDIR to specify the path for the integrated server file to be cleared.

Note: When changing a file, OS/400 uses only the first directory for that file. It ignores any other entries that specify a different target directory.

TARGETFILE keyword

Use TARGETFILE to specify the integrated server file to be cleared.

Change an integrated server file with ADDCONFIG entry type

You can use the ADDCONFIG entry type to change an integrated Windows server file in these ways:

- Add a line to the beginning or end of the file.
- Add a new line before or after a line that contains a specific string.
- Delete a line in the file.
- Replace the first, last, or all occurrences of a line in the file.
- Specify in which directory to change the file.

To change an integrated server file, create an NWSD configuration file that contains the ADDCONFIG entry type as follows:

```
ADDCONFIG
VAR           = '<variable_name>',           (conditionally required)
ADDSTR        = '<line to process>',         (optional)
ADDWHEN       = '<ALWAYS|NEVER|<expression>>', (optional)
DELETEWHEN    = '<NEVER|ALWAYS|<expression>>', (optional)
LINECOMMENT   = '<"REM "|<comment_string>>', (optional)
LOCATION        = '<END|BEGIN>',              (optional)
FILESEARCHPOS = '<AFTER|BEFORE>',            (optional)
FILESEARCHSTR = '<search_string>',           (conditionally required)
FILESEARCHSTROCC = '<LAST|FIRST>',          (optional)
REPLACEOCC    = '<LAST|FIRST|ALL>',         (optional)
TARGETDIR     = '<BOOT|path>',              (optional)
TARGETFILE    = '<CONFIG.SYS|<file_name>>', (optional)
UNIQUE        = '<NO|YES>'                  (optional)
```

For a detailed explanation of the ADDCONFIG keywords, use the following keyword links. You can also go back to “NWSD configuration file format” on page 159 or on to the “Change an integrated Windows server file with UPDATECONFIG entry type” on page 166.

- “VAR keyword”
- “ADDSTR keyword” on page 163
- “ADDWHEN keyword” on page 163
- “DELETEWHEN keyword” on page 164
- “LINECOMMENT keyword” on page 164
- “LOCATION keyword” on page 164
- “FILESEARCHPOS keyword (ADDCONFIG entry type)” on page 164
- “FILESEARCHSTR keyword” on page 165
- “FILESEARCHSTROCC keyword” on page 165
- “REPLACEOCC keyword” on page 165
- “TARGETDIR keyword” on page 165
- “TARGETFILE keyword” on page 165
- “UNIQUE keyword” on page 166

VAR keyword

VAR specifies the value on the left side of the equal sign that identifies the line you want to add to or delete from the file. For example:

```
ADDCONFIG
VAR = 'FILES'
```

OS/400 requires the keyword if you do not specify REPLACEOCC,

ADDSTR keyword

Use ADDSTR to specify the string that you want to add to the integrated Windows server file. For example:

```
ADDCONFIG
  VAR = 'FILES'
  ADDSTR = '60'
```

ADDWHEN keyword

Use ADDWHEN to specify when during processing you want OS/400 to add the new line or string to the integrated Windows server file.

You can specify:

- ALWAYS if you want OS/400 to add the line or string every time it processes the configuration file. (ALWAYS is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)
- NEVER if you want OS/400 to never add the line or string.
- An expression that directs OS/400 to add the line or string when the specified condition is true. Expressions are composed of operators (see “ADDWHEN and DELETEWHEN expression operators”) and must equate to either TRUE or FALSE.

Note: If you do not want OS/400 to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to add a line when the NWSD type is *WINDOWSNT, you could use this:

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

ADDWHEN and DELETEWHEN expression operators

You can use these operators for expressions:

Operator	Description
==	Returns TRUE if operands are equivalent, FALSE if they are not.
!=	Returns FALSE if operands are equivalent, TRUE if they are not.
>	Returns TRUE if the operand on the left is greater than the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
<	Returns TRUE if the operand on the left is less than the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
>=	Returns TRUE if the operand on the left is greater than or equal to the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
<=	Returns TRUE if the operand on the left is less than or equal to the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
&&	Logical AND. Returns TRUE if both operands have a value other than 0. Operands must be integers.
	Logical OR. Returns TRUE if either operand has a value other than 0. Operands must be integers.
+	If the operands are both integers, the result is the sum of the integers. If the operands are both strings, the result is the concatenation of the two strings.
-	Subtracts integers.
*	Multiplies integers.
/	Divides integers.
()	Parentheses force an evaluation order.
!	Logical NOT. Returns TRUE if the value of a single operand is 0. Returns FALSE if it is not 0.

Operator	Description
ALWAYS	Always returns TRUE.
NEVER	Always returns FALSE.

DELETEWHEN keyword

Use DELETEWHEN to specify when during processing you want OS/400 to delete a line or string from the file. You can specify:

- ALWAYS if you want OS/400 to delete the line or string every time it processes the configuration file.
- NEVER if you want OS/400 to never delete the line or string. (NEVER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member)
- An expression that directs OS/400 to delete the line or string when the specified condition is true. Expressions are composed of operators (see “ADDWHEN and DELETEWHEN expression operators” on page 163) and must equate to either TRUE or FALSE.

Note: If you do not want OS/400 to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to delete a line when the NWS type is *WINDOWSNT, you can use this:

```
DELETEWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

LINECOMMENT keyword

LINECOMMENT specifies the prefix string that identifies comments in a file. Use the default value if you want LINECOMMENT to use 'REM' to identify comments. You can specify a different value. For example, to use a semicolon to identify comments, use LINECOMMENT = ';' within the **first** entry that refers to that file. (OS/400 ignores the LINECOMMENT keyword on any other entry.)

LOCATION keyword

LOCATION specifies where in the file to add the new line. The default value END directs OS/400 to add the line at the end of the file. If you want OS/400 to add the line at the beginning of the file, specify BEGIN.

LINESEARCHPOS keyword

Use LINESEARCHPOS to specify whether to add the string you specify with the ADDSTR keyword value AFTER (the default) or before

LINESEARCHSTR keyword

Specifies the string to search for within the lines.

Note: Only the right side of the equal sign is searched for the LINESEARCHSTR value.

LINELOCATION keyword

Use LINELOCATION to specify where in the line to add the string that you specify with the ADDSTR keyword value.

Use the default value of END if you want OS/400 to add the string at the end of the line. If you want OS/400 to add the string at the beginning of the line instead, specify BEGIN.

FILESEARCHPOS keyword (ADDCONFIG entry type)

Specify where to locate a line relative to the file search string. You can specify:

- AFTER if you want OS/400 to add the line after the line that contains the file search string. (AFTER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)

- BEFORE if you want OS/400 to add the line before the line that contains the search string.

FILESEARCHSTR keyword

Use FILESEARCHSTR with the REPLACEOCC keyword to specify the line to replace. You must specify the entire line as the value.

When you are adding a new line, FILESEARCHSTR can be any part of a line you want to find.

There is no default value, unless you defined a default value by using a SETDEFAULTS entry in the member.

FILESEARCHSTROCC keyword

Specifies which occurrence of a string that appears multiple times in the file to use for positioning the new line.

The default value of LAST specifies the last occurrence of the search string. If you want OS/400 to use the first occurrence of the search string, specify FIRST.

REPLACEOCC keyword

Specifies which occurrence of a line you want to replace:

- Use LAST if you want OS/400 to replace the last occurrence of the FILESEARCHSTR.
- Use ALL if you want OS/400 to replace all occurrences of the FILESEARCHSTR.
- Use FIRST if you want OS/400 to replace the first occurrence of the FILESEARCHSTR.

Use FILESEARCHSTR to specify the entire line that you want to replace.

OS/400 deletes the line that matches the FILESEARCHSTR and adds the specified VAR and ADDSTR to the file at this location.

Note: REPLACEOCC has precedence over LOCATION and FILESEARCHPOS. If OS/400 does not find the FILESEARCHSTR value used with a REPLACEOCC keyword, it adds a new line based on the value of the LOCATION keyword but does not replace a line.

TARGETDIR keyword

Use TARGETDIR to specify the path for the integrated server file to be changed.

Unless you first use a SETDEFAULTS entry to change the default, you need to specify the path for UNATTEND.TXT or your own integrated server file. (This keyword defaults to BOOT, which directs OS/400 to change the file in the root directory of the E drive.)

Notes:

1. Support for NWSD configuration files exists only for predefined disk drives that are formatted as FAT. Storage spaces that are converted to NTFS are not accessible for configuration files. See “Predefined disk drives for integrated Windows servers” on page 85.
2. When changing a file, OS/400 uses only the first directory for that file. It ignores any other entries that specify a different target directory.

TARGETFILE keyword

TARGETFILE specifies the integrated server file to be changed. The value of UNATTEND.TXT directs OS/400 to change the integrated server unattended install setup script file.

Unless you first use a SETDEFAULTS entry to change the default, you need to specify UNATTEND.TXT or your own integrated server file. (This keyword defaults to CONFIG.SYS.)

UNIQUE keyword

Specify YES if you want to allow only one occurrence of a line in the file.

The default value of NO specifies that multiple occurrences are

VAROCC keyword

Use VAROCC to specify which occurrence of the variable you want to change.

If you want to change the last occurrence of the variable, you can use the default value. Otherwise, specify FIRST to change the

VARVALUE keyword

Use VARVALUE if you want to change a line only if it has this particular value for the variable you specify.

You can specify all or part of the string on the right side of an expression that you want to change.

Change an integrated Windows server file with UPDATECONFIG entry type

You can use the UPDATECONFIG entry type to change an integrated server file in these ways:

- Add strings to lines in the file.
- Add new strings before or after a specified string.
- Delete strings from lines in the file.
- Specify in which paths to change the file.

To change an integrated server file, create an NWSD configuration file that contains the UPDATECONFIG entry type as follows:

```
UPDATECONFIG
VAR           = '<variable_name>',           (required)
ADDSTR       = '<line to process>',         (required)
ADDWHEN      = '<ALWAYS|NEVER|<expression>>', (optional)
DELETEWHEN  = '<NEVER|ALWAYS|<expression>>', (optional)
LINECOMMENT  = '<"REM "|<comment_string>>', (optional)
LINELOCATION  = '<END|BEGIN>',               (optional)
LINESEARCHPOS = '<AFTER|BEFORE>',           (optional)
LINESEARCHSTR = '<string within a line>',    (optional)
FILESEARCHPOS = '<AFTER|BEFORE>',           (optional)
FILESEARCHSTR = '<search string>',          (optional)
FILESEARCHSTROCC = '<LAST|FIRST>',          (optional)
TARGETDIR    = '<BOOT|<path>>',             (optional)
TARGETFILE   = '<CONFIG.SYS|<file_name>>', (optional)
VAROCC       = '<LAST|FIRST>',             (optional)
VARVALUE     = '<variable value>'          (optional)
```

For a detailed explanation of the UPDATECONFIG keywords, use the following keyword links. You can also go back to “NWSD configuration file format” on page 159 or on to “Set configuration defaults with the SETDEFAULTS entry type” on page 167.

- “VAR keyword” on page 162
- “ADDSTR keyword” on page 163
- “ADDWHEN keyword” on page 163
- “DELETEWHEN keyword” on page 164
- “LINECOMMENT keyword” on page 164
- “LINELOCATION keyword” on page 164
- “LINESEARCHPOS keyword” on page 164

- “LINESEARCHSTR keyword” on page 164
- “FILESEARCHPOS keyword (UPDATECONFIG entry type)”
- “FILESEARCHSTR keyword (UPDATECONFIG entry type)”
- “FILESEARCHSTROCC keyword (UPDATECONFIG entry type)”
- “TARGETDIR keyword” on page 165
- “TARGETFILE keyword” on page 165
- “VAROCC keyword” on page 166
- “VARVALUE keyword” on page 166

FILESEARCHPOS keyword (UPDATECONFIG entry type)

You can use FILESEARCHPOS to specify which occurrence of the variable you want OS/400 to find relative to a line that contains the search string. Use the value:

- AFTER if you want OS/400 to find the first occurrence of the variable on or after the line that contains the search string. (AFTER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)
- BEFORE if you want OS/400 to find the first occurrence of the variable on or before the line that contains the search string.

Note: If OS/400 does not find the search string, it determines the line to change from the VAROCC keyword.

FILESEARCHSTR keyword (UPDATECONFIG entry type)

Use FILESEARCHSTR to provide a search string for OS/400 to use to locate the occurrence of the variable to replace.

There is no default value, unless you defined a default value by using a SETDEFAULTS entry in the member.

FILESEARCHSTROCC keyword (UPDATECONFIG entry type)

Use FILESEARCHSTROCC to specify which occurrence of a string that appears multiple times in the file to use for finding the lines to be modified.

Use the default value of LAST if you want OS/400 to use the last occurrence of the search string. If you want OS/400 to use the

Set configuration defaults with the SETDEFAULTS entry type

You can set default values for certain keywords on the ADDCONFIG and UPDATECONFIG entry types by using SETDEFAULTS. You can set defaults to:

- Add and delete lines.
- Search for lines.
- Identify the file name and path to change.

To set the defaults, create an NWSD configuration file that contains the SETDEFAULTS entry type as follows:

```
SETDEFAULTS
ADDWHEN      = '<ALWAYS|NEVER|<expression>>', (optional)
DELETEWHEN  = '<NEVER|ALWAYS|<expression>>', (optional)
FILESEARCHPOS = '<AFTER|BEFORE>', (optional)
FILESEARCHSTR = '<search_string>', (optional)
TARGETDIR   = '<path>', (optional)
TARGETFILE  = '<file_name>' (optional)
```


For a detailed explanation of the SETDEFAULTS keywords, use the following keyword links.

- “ADDWHEN”
- “DELETEWHEN”
- “FILESEARCHPOS keyword (SETDEFAULTS entry type)”
- “FILESEARCHSTR keyword (SETDEFAULTS entry type)” on page 169
- “TARGETDIR” on page 169
- “TARGETFILE” on page 169

ADDWHEN

Use ADDWHEN with the SETDEFAULTS entry type to set the default value for the ADDWHEN keyword on ADDCONFIG and UPDATECONFIG entry types.

Set the default for when during processing you want OS/400 to add the new line or string to the file. You can specify:

- ALWAYS if you want OS/400 to add the line or string every time it processes the configuration file. (ALWAYS is the default unless you defined a different default.)
- NEVER if you want OS/400 to never add the line or string.
- An expression that directs OS/400 to add the line or string when the specified condition is true. Expressions are composed of operands (see “ADDWHEN and DELETEWHEN expression operators” on page 163) and must equate to either TRUE or FALSE.

Note: If you do not want OS/400 to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to add a line when the NWSD type is *WINDOWSNT, you could use this:

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

DELETEWHEN

Use DELETEWHEN with the SETDEFAULTS entry type to set the default value for the DELETEWHEN keyword on ADDCONFIG and UPDATECONFIG entry types.

Specify when during processing you want OS/400 to delete the line or string from the file.

You can specify:

- ALWAYS if you want OS/400 to delete the line or string every time it processes the configuration file.
- NEVER if you want OS/400 to never delete the line or string. (NEVER is the default unless you defined a different default.)
- An expression that directs OS/400 to delete the line or string when the specified condition is true. Expressions are composed of operands (see “ADDWHEN and DELETEWHEN expression operators” on page 163) and must equate to either TRUE or FALSE.

Note: If you do not want OS/400 to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to delete a line when the NWSD type is *WINDOWSNT, you can use this:

```
DELETEWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

FILESEARCHPOS keyword (SETDEFAULTS entry type)

Use FILESEARCHPOS with the SETDEFAULTS entry type to set the default value for the FILESEARCHPOS keyword on ADDCONFIG and UPDATECONFIG entry types.

Specify where to locate a line relative to the file search string. You can specify:

- AFTER if you want the line located after the line that contains the file search string. (AFTER is the default unless you defined a different default.)

- BEFORE if you want OS/400 to add the line before the line that contains the search string.

FILESEARCHSTR keyword (SETDEFAULTS entry type)

Use FILESEARCHSTR with the SETDEFAULTS entry type to set the default value for the FILESEARCHSTR keyword on ADDCONFIG and UPDATECONFIG entry types.

The FILESEARCHSTR value can be any part of the line you want to find.

TARGETDIR

Use TARGETDIR with the SETDEFAULTS entry type to set the default value for the TARGETDIR keyword on ADDCONFIG and UPDATECONFIG entry types.

A path specifies the directory that contains the file to be processed.

For example, to set the default TARGETDIR value for a file on drive D, you could use this:

```
SETDEFAULTS TARGETDIR = 'D:\'
```

TARGETFILE

Use TARGETFILE with the SETDEFAULTS entry type to set the default value for the TARGETFILE keyword on ADDCONFIG and UPDATECONFIG entry types.

A name specifies the file to be processed.

For example, to set the default TARGETFILE value for file UNATTEND.TXT on drive D, you could use this:

```
SETDEFAULTS
  TARGETDIR = 'D:\',
  TARGETFILE = 'UNATTEND.TXT'
```

Use substitution variables for keyword values

You can use substitution variables for keyword values. The NWSD configuration file substitutes the correct values for the variables. These substitution variables are configured using the values stored in the NWSD or the hardware that is detected on the NWSD.

OS/400 supplies these variables:

Substitution variable	Description
%FPALANDRIVER00%	Device driver name (Port *INTERNAL)
%FPALANDRIVER01%	Device driver name (Port 1)
%FPALANDRIVER02%	Device driver name (Port 2)
%FPALANDRIVER03%	Device driver name (Port 3)
%FPAMACADDR00%	MAC address (NWSD Port *INTERNAL) *
%FPAMACADDR01%	MAC address (NWSD Port 1) *
%FPAMACADDR02%	MAC address (NWSD Port 2) *
%FPAMACADDR03%	MAC address (NWSD Port 3) *
%FPAIPADDR00%	TCP/IP address (NWSD Port *INTERNAL) *
%FPAIPADDR01%	TCP/IP address (NWSD Port 1) *
%FPAIPADDR02%	TCP/IP address (NWSD Port 2) *
%FPAIPADDR03%	TCP/IP address (NWSD Port 3) *
%FPASUBNET00%	TCP/IP subnet address (NWSD Port *INTERNAL) *

Substitution variable	Description
%FPASUBNET01%	TCP/IP subnet address (NWSD Port 1) *
%FPASUBNET02%	TCP/IP subnet address (NWSD Port 2) *
%FPASUBNET03%	TCP/IP subnet address (NWSD Port 3) *
%FPAMTU00%	TCP/IP interface MTU (NWSD Port *INTERNAL)*
%FPAMTU01%	TCP/IP interface MTU (NWSD Port 1) *
%FPAMTU02%	TCP/IP interface MTU (NWSD Port 2) *
%FPAMTU03%	TCP/IP interface MTU (NWSD Port 3) *
%FPAPORTTYPE00%	Adapter port type (Port *INTERNAL - 2B00)
%FPAPORTTYPE01%	Adapter port type (Port 1 - ex.2723,2724,2838, 2744,2743,2760)
%FPAPORTTYPE02%	Adapter port type (Port 2 - ex.2723,2724,2838, 2744,2743,2760)
%FPAPORTTYPE03%	Adapter port type (Port 3 - ex.2723,2724,2838,2744,2743,2760)
%FPATCPHOSTNAME%	TCP/IP host name
%FPATCPDOMAIN%	TCP/IP domain name
%FPATCPDNSS%	TCP/IP DNS's, separated by commas
%FPATCPDNS01%	TCP/IP Domain Name Server 1
%FPATCPDNS02%	TCP/IP Domain Name Server 2
%FPATCPDNS03%	TCP/IP Domain Name Server 3
%FPANWSDTYPE%	The type of the NWSD that you are varying on (*WINDOWSNT)
%FPANWSDNAME%	The name of the NWSD that you are varying on
%FPACARDTYPE%	The resource type of the NWSD that you are varying on (ex. 6617, 2850, 2890, 2892, 4812, 2689)
%FPAINSMEM%	The amount of installed memory detected
%FPAUSEMEM%	The amount of useable memory detected
%FPACODEPAGE%	The ASCII codepage used to translate from EBCDIC
%FPALANGVERS%	The OS/400 Language version used on the NWSD
%FPASYSDDRIVE%	The drive letter used for the system drive (C, E when server was installed with V4R4 or earlier)
%FPA_CARET%	The caret symbol (^)
%FPA_L_BRACKET%	The left bracket symbol ([)
%FPA_R_BRACKET%	The right bracket symbol (])
%FPA_PERCENT%	The percent symbol (%) NOTE: Since the percent symbol is used as the substitution variable delimiter, this substitution variable should be used when a string contains a percent symbol that should NOT be interpreted as a substitution variable delimiter.
%FPABOOTDRIVE%	This is always drive E for the Integrated xSeries Server
%FPACFGFILE%	The name of the NWSD configuration file being processed
%FPACFGLIB%	The library that contains the NWSD configuration file being processed
%FPACFGMBR%	The name of the NWSD configuration file member being processed
* Values are retrieved from the NWSD	

You can configure additional substitution variables by creating a file in QUSRSYS and giving it the same name as the NWSD followed by the suffix 'VA'. You must create the file as a source physical file with a minimum record length of 16 and maximum record length of 271.

For example, at the OS/400 command line, type this:

```
CRTSRCPF FILE(QUSRSYS/nwsdnameVA) RCDLEN(271)
  MBR(nwsdname) MAXMBRS(1)
  TEXT('Configuration file variables')
```

The member 'nwsdname' contains data in fixed columns formatted as:

- A variable name in column 1-15 padded with blanks and
- A value that starts in column 16

For example:



```
Columns:
12345678901234567890123456789012345678901234567890...
myaddr          9.5.9.1
```

where %myaddr% is added to the list of available substitution variables and has a value of "9.5.9.1".

Chapter 15. Related information

Listed below are the iSeries manuals and IBM Redbooks (in PDF format), Web sites, and Information Center topics that relate to the Windows Environment on iSeries topic. You can view or print any of the PDFs.





Manuals

- iSeries Performance Capabilities Reference 
- Backup and Recovery 
- Hardware installation instructions. See the “Install iSeries features” topic.

Redbooks (www.redbooks.ibm.com)

- | [Microsoft Windows Server 2003 Integration with iSeries, SG24-6959](#) 

Web Sites

- Latest product and service information: IBM Windows Integration 
(www.ibm.com/servers/eserver/series/windowsintegration)
- iSeries Performance Management 
(www.ibm.com/eserver/series/perfmgmt)
- IXA install read me first 
(www.ibm.com/servers/eserver/series/windowsintegration/ixareadme)
- | • IXS install read me first 
| (www.ibm.com/servers/eserver/series/windowsintegration/ixsreadme)

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

- | IBM Director of Licensing
- | IBM Corporation
- | North Castle Drive
- | Armonk, NY 10504-1785
- | U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

- | IBM World Trade Asia Corporation
- | Licensing
- | 2-31 Roppongi 3-chome, Minato-ku
- | Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

- | The licensed program described in this information and all licensed material available for it are provided by
- | IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM
- | License Agreement for Machine Code, or any equivalent agreement between us.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

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

AS/400
DB2
IBM
iSeries
Netfinity
Operating System/400
OS/400
PAL
Redbooks
ServerGuide
Tivoli
xSeries

Pentium® is a trademark or a registered trademark of Intel Corporation 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.

Other company, product, and service names may be trademarks or service marks of others.

| Terms and conditions for downloading and printing information

- | Permissions for the use of the information you have selected for download are granted subject to the
- | following terms and conditions and your indication of acceptance thereof.

- | **Personal Use:** You may reproduce this information for your personal, noncommercial use provided that all
- | proprietary notices are preserved. You may not distribute, display or make derivative works of this
- | information, or any portion thereof, without the express consent of IBM.

- | **Commercial Use:** You may reproduce, distribute and display this information solely within your enterprise
- | provided that all proprietary notices are preserved. You may not make derivative works of this information,
- | or reproduce, distribute or display this information or any portion thereof outside your enterprise, without
- | the express consent of IBM.

- | Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either
- | express or implied, to the information or any data, software or other intellectual property contained therein.

- | IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of
- | the information is detrimental to its interest or, as determined by IBM, the above instructions are not being
- | properly followed.

| You may not download, export or re-export this information except in full compliance with all applicable
| laws and regulations, including all United States export laws and regulations. IBM MAKES NO
| GUARANTEE ABOUT THE CONTENT OF THIS INFORMATION. THE INFORMATION IS PROVIDED
| "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING
| BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND
| FITNESS FOR A PARTICULAR PURPOSE.

All material copyrighted by IBM Corporation.

| By downloading or printing information from this site, you have indicated your agreement with these terms
| and conditions.



Printed in USA