

iSeries Access for Windows V5R2

Hot Topics:

Tailored Images, Application Administration, SSL, and Kerberos



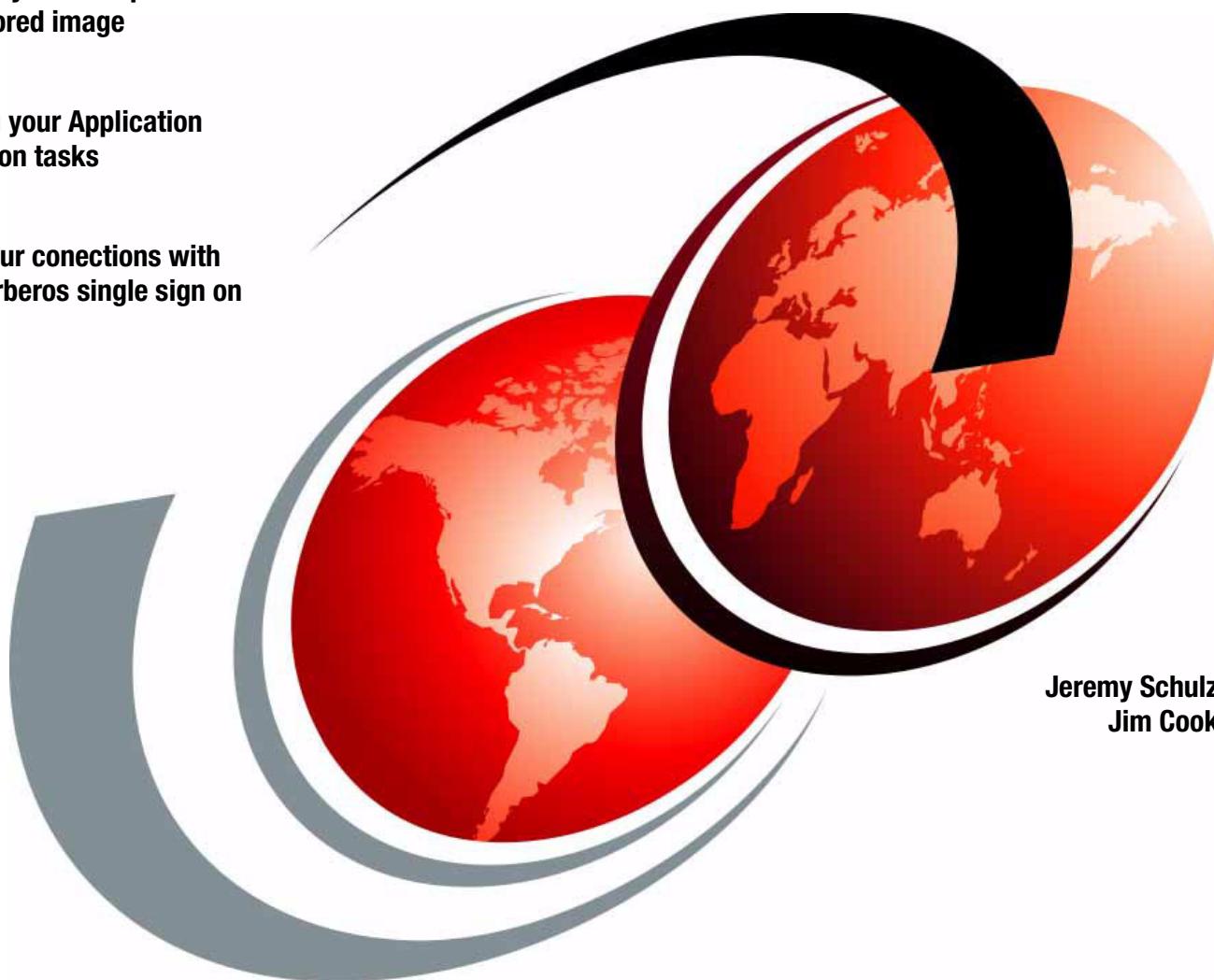
Speeding up your multiple workstation install using a tailored image



Centralizing your Application Administration tasks



Securing your connections with SSL and Kerberos single sign on



Jeremy Schulz
Jim Cook

Redbooks



International Technical Support Organization

**iSeries Access for Windows V5R2 Hot Topics: Tailored
Images, Application Administration, SSL, and
Kerberos**

February 2004

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (February 2004)

This edition applies to Version 5, Release 2, Modification 0 of OS/400, 5722-SS1 and iSeries Access for Windows, 5722-XE1, with Service Pack level available with PTF SI09809.

© Copyright International Business Machines Corporation 2004. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	v
Trademarks	vi
Preface	vii
The team that wrote this redbook	viii
Become a published author	viii
Comments welcome	ix
Summary of changes	xi
March 2004, Update	xi
Chapter 1. Overview	1
1.1 iSeries Access for Windows overview	2
1.2 Topics by chapter	3
Chapter 2. Installing iSeries Access for Windows	5
2.1 Introduction	6
2.2 Tailored installation image	7
2.3 Combining a service pack with your install image	15
2.3.1 Merging the service pack with the install image on the iSeries server	15
2.3.2 Using PTFFORM.EXE to merge a service pack and an install image	16
2.4 Distributing and installing the merged installation image	20
2.5 Silent install	22
2.5.1 Creating a response file	23
2.5.2 Starting a silent installation	24
2.5.3 Example response file: setup.iss	24
2.5.4 Installing upgrades and service packs silently	27
Chapter 3. Application Administration: Administration system and Central Settings	29
3.1 Administration system and Central Settings overview	30
3.2 Application Administration concepts	31
3.3 Implementing Central Settings	32
3.3.1 Choosing an administration system	32
3.3.2 Customizing the administration of users	36
3.3.3 Configuring Central Settings	37
3.4 Registering Central Settings	37
3.5 Managing Central Settings	39
3.5.1 Managing Central Settings: Basic customization	41
3.5.2 Managing Central Settings: Advanced customization	43
3.6 Client discovery of the administration system	50
3.6.1 Administration system discovery: Manual	52
3.6.2 Administration system discovery: Signon	52
3.6.3 Administration system discovery: Install	53
Chapter 4. Secure Sockets Layer (SSL)	55
4.1 Introduction	56
4.1.1 iSeries Access for Windows SSL utility program	56
4.2 SSL prerequisites	58
4.3 Server authentication	58

4.3.1	Creating the system certificate	58
4.3.2	Certificate authority (CA).	60
4.4	Client authentication	66
4.4.1	Creating a user certificate for client authentication	67
4.4.2	Importing the user certificate.	80
4.5	Configuring iSeries Access for Windows to use SSL	84
4.5.1	Installing the Secure Sockets Layer	84
4.5.2	Downloading the certificate authority	86
4.5.3	Verifying the SSL connection	87
4.5.4	Configuring PC5250 emulation to use SSL.	89
4.6	Viewing a certificate authority certificate	91
Chapter 5.	iSeries Access for Windows in a Kerberos environment	97
5.1	Using Kerberos authentication with iSeries Access for Windows functions	98
5.2	Kerberos overview	99
5.2.1	Kerberos concepts	101
5.3	Kerberos protocol components	102
5.3.1	Kerberos tickets	103
5.3.2	Principals and realms	103
5.3.3	Key Distribution Center	104
5.4	Kerberos and Microsoft: Implicit support by Microsoft.	106
5.5	Kerberos commands	106
5.6	Setting up an operational Kerberos realm example	109
5.6.1	General TCP/IP network host name resolution considerations.	110
5.6.2	Coordinating the time used on all network servers	113
5.6.3	KDC server setup	116
5.6.4	Setting up an iSeries server to perform Kerberos functions	123
5.6.5	Verifying Network Authentication Service setup	130
5.7	Enterprise Identity Mapping	132
5.7.1	EIM overview and components	133
5.7.2	EIM authorities	142
5.7.3	Simple EIM setup example for iSeries Access for Windows users	142
5.7.4	Setting up Kerberos authentication for an iSeries Navigator session	154
5.7.5	Setting up Kerberos authentication for an iSeries Access PC5250 session.	156
5.7.6	Verifying iSeries Access for Windows with single signon	157
Appendix A.	Coming attractions for iSeries Access for Windows	161
	iSeries Access for Windows: Beyond V5R2 overview	162
	New database provider	162
	Data transfer	162
	ODBC	162
	OLE DB	163
	Incoming Remote Command (IRC)	163
	PC5250	163
	Configuration	163
Related publications	165
	IBM Redbooks	165
	Other publications	165
	Online resources	165
	How to get IBM Redbooks	166
Index	167

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 give 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.

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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

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

AIX®
AS/400®
Distributed Relational Database
Architecture™
Domino®
DB2 Universal Database™
DB2®

DRDA®
@server®
IBM®
ibm.com®
iSeries™
Lotus®
Lotus Notes®

OS/400®
Redbooks™
Redbooks (logo) ™
xSeries®
z/OS®

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks 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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM® Redbook covers the “hot topic tasks” (according to client feedback) related to running the following iSeries™ Access for Windows, 5722-XE1, capabilities:

- ▶ iSeries Access for Windows installation, focusing on tailored and silent installation
- ▶ iSeries Access for Windows Application Administration, focusing on the new starting in Version 5 Release 2, Central Settings support
- ▶ Setting up iSeries Access for Windows functions to use Secure Sockets Layer (SSL) support
- ▶ iSeries Access for Windows functions using Kerberos and IBM Enterprise Identity Mapping (EIM) network authentication capabilities

This information should get you up and running quickly using these capabilities.

This book also includes a summary of what is coming in the next release of iSeries Access for Windows by describing what is available as Beta code from the iSeries Access Web site at:

<http://www.ibm.com/eserver/iseries/access/windows>

The information in this book is generally available through sets of information located at the following Web sites, but is documented here all in one place and with actual examples to speed up your deployment of these capabilities:

<http://www.ibm.com/eserver/iseries/access/windows>

<http://www.ibm.com/eserver/iseries/infocenter>

Select your geographical region and your V5R2 language. In the Information Center, select **Connecting to iSeries** → **What to connect with** → **iSeries Access**.

Note that iSeries Access for Windows, 5722-XE1, includes a wide range of TCP/IP-based functions not covered in this book that use client PC workstations running a variety of Microsoft® Windows® operating systems when connected to one or more iSeries systems. iSeries Access for Windows offers an all-inclusive client solution for accessing and using resources from your Windows desktop.

The primary components of iSeries Access for Windows are:

- ▶ iSeries Navigator, which provides interfaces to the system for:
 - Work management
 - Configuration and service (hardware, software, fixes, system value, logical partition management and performance data collection)
 - Network management (TCP/IP configuration and status and manage servers)
 - User and group profile management
 - Database access
 - OS/400® Integrated File System (IFS) management
 - Management Central functions for managing one or more iSeries systems, including software and fixes, system values, performance data collection, performance metrics and job monitoring, and task scheduling
 - And more

- ▶ Middleware for using and developing client applications to access OS/400 resources and that uses iSeries NetServer for working with the OS/400 Integrated File System and printers
- ▶ 5250 emulation (PC5250)
- ▶ Data transfer access to DB2® Universal Database™ (UDB) to your iSeries server

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Rochester Center.

Jim Cook is a Senior Software Engineer at the International Technical Support Organization, Rochester Center. He leads teams that produce iSeries Announcement presentation sets that are maintained on the IBM @server® iSeries Web site (<http://www.ibm.com/eserver/iseries/support>) and presented at ITSO iSeries Forums internationally. Jim also produces Redbooks™ about various OS/400 topics.

Jeremy Schulz is a Staff Software Engineer in Rochester, Minnesota in the U.S. He has five years of experience in the client support field. He has worked at IBM for five years. His areas of expertise include iSeries Access for Windows, iSeries Access for Web, and the Telnet Server.

Thanks to the following people for their key contributions to this project:

IBM Rochester Development

Yvonne Griffin
 Gordie Grout
 Linda Hirsch
 Jeff Van Hueklon
 Steve Mervosh
 Carole Miner
 Tim Mossing
 Sharee Oesterlin
 Jill Shepherd
 Mark Vanderwiel

iSeries Support, Rochester (Support Line)

Gary Lakner, especially for his Kerberos and Enterprise Identity Mapping assistance

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners or clients, or both.

Your efforts will help increase product acceptance and client satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

ibm.com/redbooks

- Send your comments in an Internet note to:

redbook@us.ibm.com

- Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, Minnesota 55901-7829

Summary of changes

This section describes the technical changes made in this update of *iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos*, SG24-6939-00, as updated March 2004. This update might also include minor corrections and editorial changes that are not identified.

March 2004, Update

This revision reflects the addition, deletion, or modification of new and changed information described in the following sections.

New information

Section 5.7, “Enterprise Identity Mapping” on page 132, now includes expanded Enterprise Identity Mapping (EIM) overview information and simple EIM configuration examples. This information is required because iSeries support of Kerberos authentication requires basic EIM configuration to map between a Kerberos principal and an OS/400 user profile.

The previous edition indicated EIM configuration was not required when the Kerberos principal name and OS/400 user profile were identical.

Changed information

- ▶ The “Preface” on page vii and Chapter 1, “Overview” on page 1 now contain text that includes the new information in the Enterprise Identity Mapping topic.
- ▶ In Chapter 5, “iSeries Access for Windows in a Kerberos environment” on page 97, the topics about setting up iSeries Access for Windows iSeries Navigator and PC5250 Emulation to use Kerberos are moved to the end of the chapter.



Overview

This chapter provides an overview of:

- ▶ iSeries Access for Windows
- ▶ Topics covered in each chapter of this redbook

1.1 iSeries Access for Windows overview

iSeries Access for Windows, 5722-XE1, includes a wide range of TCP/IP-based functions that use client PC workstations running a variety of Microsoft Windows operating systems when connected to one or more IBM @server iSeries systems. iSeries Access for Windows offers an all-inclusive client solution for accessing and using resources from your Windows desktop.

The primary components of iSeries Access for Windows are:

- ▶ iSeries Navigator, which provides a Windows operating system-based graphical user interface (GUI) to an iSeries system with the following major functional areas:
 - Work management (view and manage jobs, subsystems, job queues, spool output queues, and more)
 - Configuration and service (multiple system management of hardware, software, software fixes, OS/400 system values, and user inventory, installing software and fixes, search results for user profile usage attributes, system-wide performance data collection, logical partition management, and more)
 - Network management (TCP/IP configuration, IP policies, and status, OS/400 “servers” such as Telnet and Management Central, and more)
 - User and group profile management
 - Database access (primarily through SQL-based functions)
 - OS/400 Integrated File System (IFS) management (including file shares)
 - Security (view and manage authorization lists, security policies, and Network Authentication Services (Kerberos usage))
 - Windows administration (view, start, stop, and install fixes for a Windows operating system installed on either the Integrated xSeries® server (IXS) or the Integrated xSeries Adapter (IXA) for iSeries, configure and manage virtual disks to that Windows operating system, propagate OS/400 users to users on the Windows network domain, and more)
 - Support for properly set up products to appear as “plug-ins” in the function hierarchy tree on the PC workstation (includes IBM products, such as Lotus® Domino®, Backup Recovery and Media Services, Advanced Job Scheduler, and Performance Tools for iSeries)
 - Management Central (an underlying component that provides multiple system support, scheduling of specific iSeries Navigator functions, such as performance data collection, performance monitoring, job and message monitoring, and all of the configuration and service functions)
 - And more
- ▶ Middleware for using and developing client applications to access OS/400 resources and that uses iSeries NetServer for working with the OS/400 Integrated File System and printers
- ▶ 5250 emulation (PC5250), which provides 5250 display and printer emulation
- ▶ Data transfer access to DB2 Universal Database (UDB) to your iSeries server, which provides SQL-based selection of file data exchange between the iSeries server and the iSeries Access for Windows client workstation

This book is not intended to provide additional details about these capabilities, but rather useful information about underlying support, such as installation options and specifically

tailored image installation, iSeries Access function administration (Application Administration), and SSL-based and Kerberos-based security when using these functions.

For details about iSeries Access for Windows capabilities, see the following information resources:

- iSeries Information Center:

<http://www.ibm.com/eserver/iseries/infocenter>

Select your geographical region, your V5R2 language, and the **Connecting to iSeries** link.

- iSeries Access Web site:

<http://www.ibm.com/eserver/iseries/access>

- iSeries Access for Windows online help information

- iSeries IBM Redbook volumes about V5R1 Operations Navigator (renamed iSeries Navigator in V5R2):

<http://www.ibm.com/redbooks>

Search the iSeries domain with “Operations AND Navigator” or the following manual numbers. Although based on V5R1, this series of books gives moderate detail level information with examples of the major iSeries (Partitions) Navigator capabilities. These Redbook titles are:

- *Managing OS/400 with Operations Navigator V5R1, Volume 1: Overview and More*, SG24-6226
- *Managing OS/400 with Operations Navigator V5R1, Volume 2: Security*, SG24-6227
- *Managing OS/400 with Operations Navigator V5R1, Volume 3: Configuration and Service*, SG24-5951
- *Managing OS/400 with Operations Navigator V5R1, Volume 4: Packages and Products*, SG24-6564
- *Managing OS/400 with Operations Navigator V5R1, Volume 5: Performance Management*, SG24-6565
- *Managing OS/400 with Operations Navigator V5R1, Volume 6: Networking*, SG24-6566

With all these functional capabilities, there are underlying iSeries Access functions that span this entire set of capabilities that provide installing these functions, controlling who can use specific functions (Application Administration, an iSeries Access for Windows function), and using Secure Sockets Layer (SSL)-based application authentication and data encryption, and using Kerberos-based network sign on (authentication).

1.2 Topics by chapter

The following chapters take information located in several sources and integrate that information into this book according to the following highest-level topics:

- Chapter 2, “Installing iSeries Access for Windows” on page 5

This chapter gives a brief overview of all of the iSeries installation options and focuses on the tailored installation option to provide images that contain only certain iSeries Access for Windows functions. Each tailored image can be used for installation on a specific set of PC client workstations.

- Chapter 3, “Application Administration: Administration system and Central Settings” on page 29

This chapter describes how to allow or deny usage of iSeries Access for Windows functions explicitly using the new for V5R2 *Central Settings* along with *Local Settings*, which in previous releases were the only way to implement Application Administration.

- Chapter 4, “Secure Sockets Layer (SSL)” on page 55

This chapter describes how to set up all or selected iSeries Access for Windows functions to use the security capabilities of SSL under OS/400. This includes the setting up and assignment of digital certificates using the iSeries browser-based interface to the iSeries Digital Certificate Manager (DCM).

- Chapter 5, “iSeries Access for Windows in a Kerberos environment” on page 97

This chapter describes iSeries Access for Windows basic usage of Kerberos and IBM Enterprise Identity Mapping (EIM) network secure authentication. Overviews of Kerberos and EIM are presented along with basic Kerberos and EIM setup examples.

This enables several iSeries Access for Windows functions to use the industry-standard Kerberos Authentication and Authorization System network authentication. Note that Kerberos is an architecture that enables implementation of an encryption-based security system that provides both mutual authentication between the users and the servers in a network environment and encrypted data exchange. iSeries Access for Windows uses only the authentication function under Kerberos. SSL is used for data encryption.

You can set up Kerberos usage on an iSeries server through the Network Authentication Service interface under the iSeries Navigator Security component.

You set up EIM usage on an iSeries server through the Enterprise Identity Mapping interface under the iSeries Navigator Network component.

Note, for V5R2 functions such as those available with iSeries Access for Windows (licensed program 5722-XE1) 5250 emulation and iSeries Navigator, use of Enterprise Identity Mapping and iSeries Network Authentication Service are both required for the target iSeries to map the Kerberos principal (“user”) to an OS/400 user profile. This is required even when the user IDs and passwords are identical on the client and server and network Kerberos support has authenticated the user.



Installing iSeries Access for Windows

This chapter describes the following:

- ▶ Creating a tailored installation image including SSL
- ▶ Servicing your tailored installation image
- ▶ Silent installation

2.1 Introduction

iSeries Access for Windows offers four installation types:

- ▶ Typical: Installs the components containing the most common functions.
- ▶ PC5250 User: Installs the minimum support needed for printer emulation and PC5250 display emulation.
- ▶ Custom: Allows you to select which components you want to install.
- ▶ Full: Installs all iSeries Access for Windows components available in the source directory.

For a complete explanation of these installation types, refer to the online help text when installing iSeries Access for Windows.

Most administrators are well versed in the typical installation procedures of iSeries Access for Windows. However, a common problem administrators have is how to control which components the users install. These four installation types might not be the set of components that is desired. One way to resolve this problem is to use a tailored installation image so that your users can only install the components that you include in that image. Therefore, the focus of this chapter will be on administering a tailored installation image.

An administrator needs to take the following steps to manage a tailored install image. The result will be an installation image of exactly the components you want, all at the latest fix level, ready to be used for initial installation on a workstation.

To manage a tailored install image:

1. Decide if Secure Sockets Layer (SSL) will be included in the tailored installation image.

Note, it is common to first install iSeries Access for Windows functions, begin using them, and later decide to use SSL with these functions. We put this choice of selecting to use SSL first in our series of steps. This is because, if selected, your install image will contain the supporting SSL code, and you will not have to rebuild an install image later when you decide to use SSL with your iSeries Access for Windows functions.

Selecting SSL during installation does not make it immediately “in use.” As described later in this book, you have several digital certificate setup steps, certificate assignment to an application, and some iSeries Access for Windows-related steps to perform before SSL is actually used.

From an iSeries Access for Windows installed on a client workstation viewpoint, if the SSL component has been installed, SSL will be displayed in the Component Selection List.

SSL will not be included in the tailored image unless selected.

Important:

- ▶ SSL will only be available in the Component Selection List if you are using the source image from the iSeries (or an image you copied from the iSeries) and have both iSeries Access for Windows, 5722-XE1, and the no charge Client Encryption 128-bit, 5722-CE3, installed on your iSeries.

Note that no charge Cryptographic Access Provider 128-bit for AS/400®, 5722-AC3, must also be installed on the iSeries for iSeries encryption/decryption support.

- ▶ SSL is controlled by U.S. export regulations. You are responsible to ensure that the new installation image is properly controlled to meet the U.S. export regulations.
- ▶ See also Chapter 4, “Secure Sockets Layer (SSL)” on page 55 for more information.

2. Create a tailored installation image.
3. Apply the latest iSeries Access for Windows service pack to the tailored image.
4. Distribute the tailored image to your users and perform the actual installation.

The following topics in this chapter expand on these steps for using a tailored installation image.

2.2 Tailored installation image

You can create one or more tailored iSeries Access for Windows installation images, each one containing a specific set of functions. For example, you could enable user workstations A, B, and C to install from image ONE and user workstations X, Y, and Z to install from image TWO.

At the appropriate time, you can apply the latest iSeries Access for Windows service pack to an install image. The result will be an installation image of exactly the components you want that includes the latest fix level. This keeps any new installs with the simplest install process you had set up previous to the availability of the new service pack/new software level.

The tailored installation image wizard is started by running the batch program **cwbinimg**. This program can be found in the following locations:

- iSeries Access Setup and Operations CD

Select the **Additional information and Tools** option, followed by the option **Create tailored installation image for iSeries Access for Windows**.

- On the network drive, specifying:

`\\your-iSeries-server-name\QIBM\ProdData\Access\Windows\Install\Image`

The Licensed Program Product (LPP) 5722-XE1 must be installed on this server. From this directory path, run the **cwbinimg** batch program.

If you will be running this wizard from the iSeries server and plan to use the iSeries for the source of your service packs, you should first apply the latest PTF, as described in 2.3.1, “Merging the service pack with the install image on the iSeries server” on page 15. Users who then install from this image will be at the latest fix level upon initial install.

If you will be running this wizard from the iSeries server, and your connection is low speed, you can copy the entire Windows folder from the iSeries server to the root drive of your PC. The Windows folder can be found in `\QIBM\ProdData\Access`, as shown in Figure 2-1 on page 8.

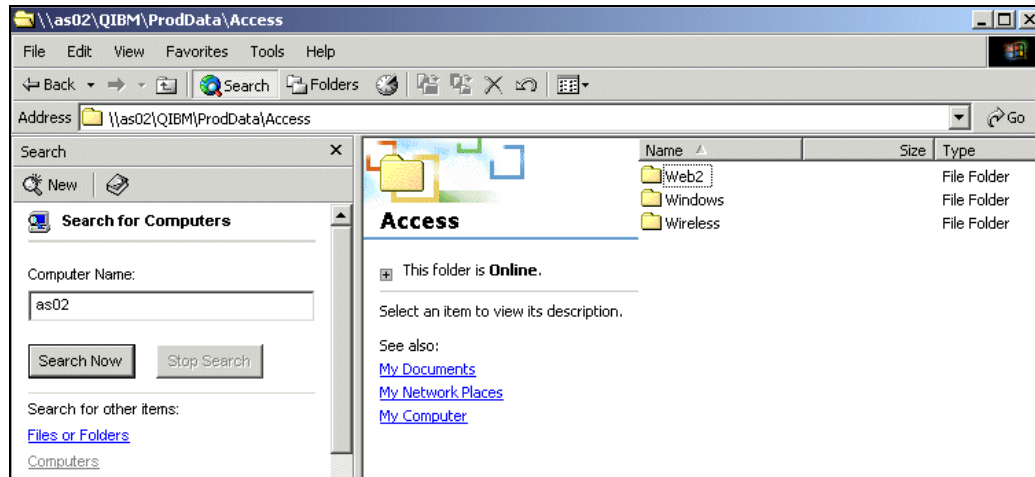


Figure 2-1 Windows folder on iSeries

Note: We recommend that you copy the Windows folder to the root directory (typically c:). In some cases when a different directory has been used, the cwbinimg.bat file has not always run satisfactorily.

Figure 2-2 shows the Windows folder copied to a PC workstation's C drive. Notice that the Windows folder contains an Install, MRI (language-specific Machine Readable Image), and SSL folder. The SSL folder will be present only if you have installed 5722-CE3 (Client Encryption, 128-bit) on an iSeries server.

The cwbinimg.bat file is located in the Windows\Install\Image directory.

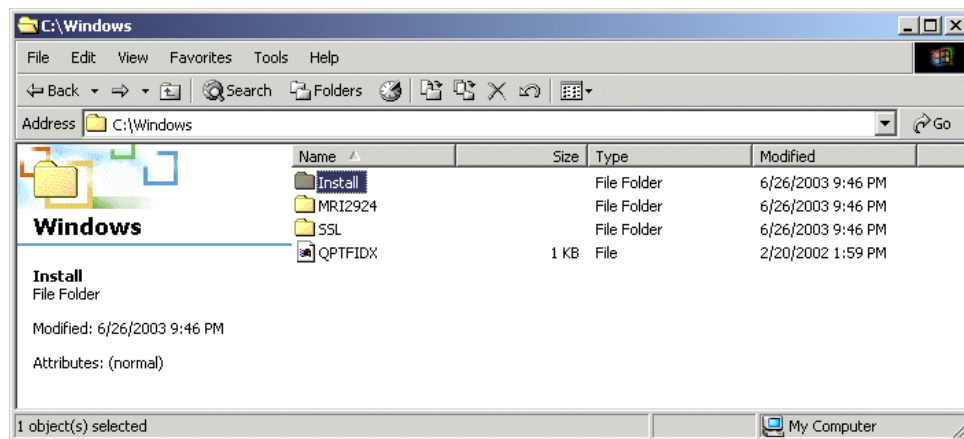


Figure 2-2 Windows directory

Another option is to run the wizard directly from the iSeries. A drive must be mapped to the iSeries, as shown in Figure 2-3 on page 9.

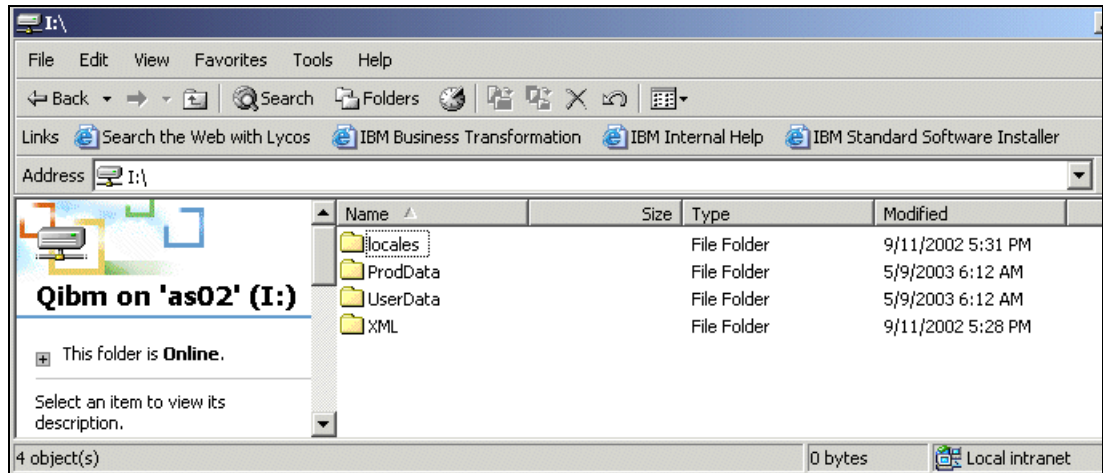


Figure 2-3 The I drive mapped to Qibm

Run the cwbinimg.bat file from the \QIBM\ProdData\Access\Windows\Install\Image directory to start the wizard.

Important: If you are creating a tailored installation image from a NetServer share, you cannot use the Universal Naming Convention (UNC) share name of \\NetServerName\QIBM\ProdData\Express\Install\Image. Windows cannot run a .bat file using a UNC name. Therefore, you need to map a network drive to this location and run cwbinimg.bat from the mapped drive.

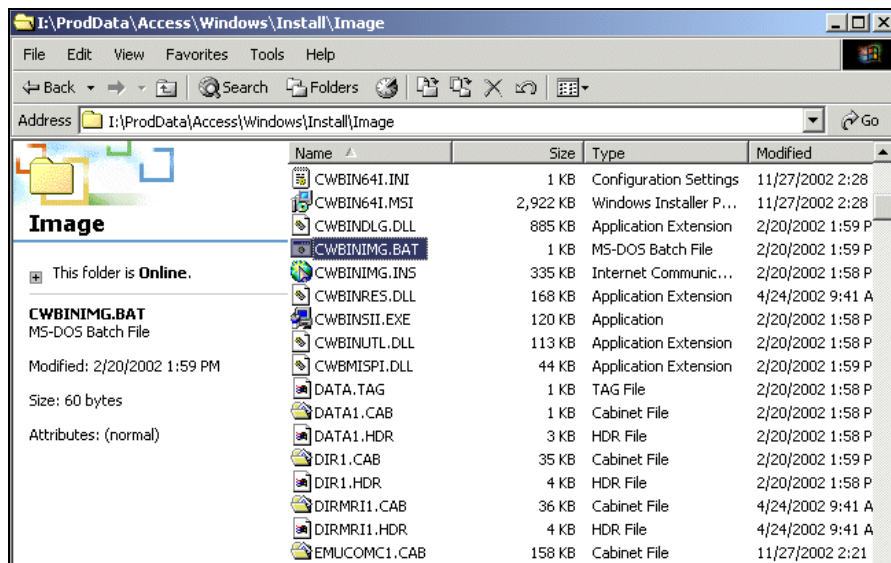


Figure 2-4 Directory path to the iSeries Access for Windows install image

To create a tailored installation image:

1. Figure 2-5 on page 10 shows the first installation wizard window. Select **Next**.

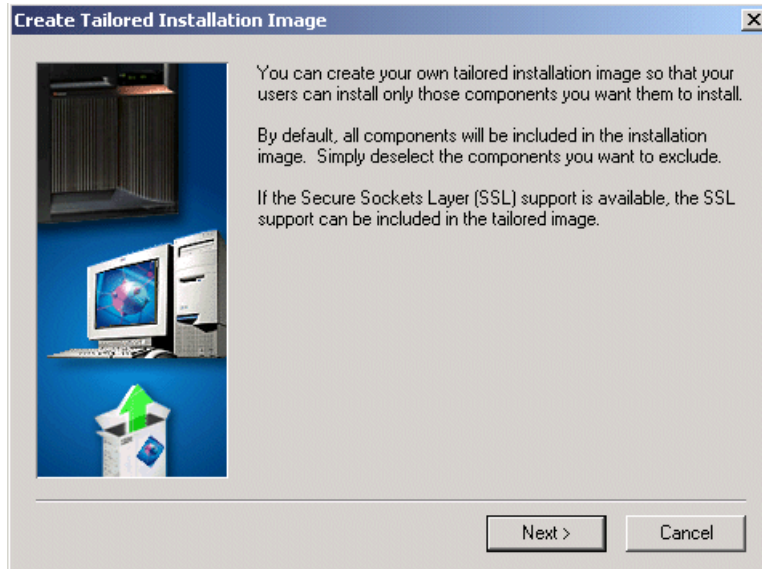


Figure 2-5 Tailored installation image wizard

This opens the Select Language window.

Important: If you are installing from an iSeries server and this server has multiple iSeries Access for Windows secondary languages installed, you can use any of the installed secondary languages or the primary language on the iSeries server as the primary language for the new installation image. This is not available if you are running the wizard from the CD, because the CD does not contain any secondary languages.

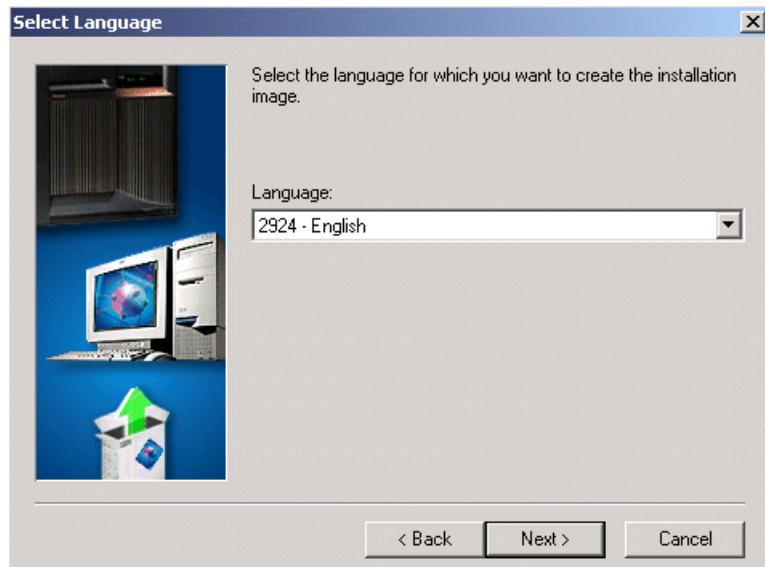


Figure 2-6 Select Language

2. As you see in the Select Language window, each wizard window has the Back (go back and review or change previous selection), Cancel (to stop the wizard and discard any selections already made), and Next (continue to the next step) buttons. In this example, after specifying the appropriate language, click **Next**. The Select Destination Directory window opens with the default destination folder (to be created) already selected.

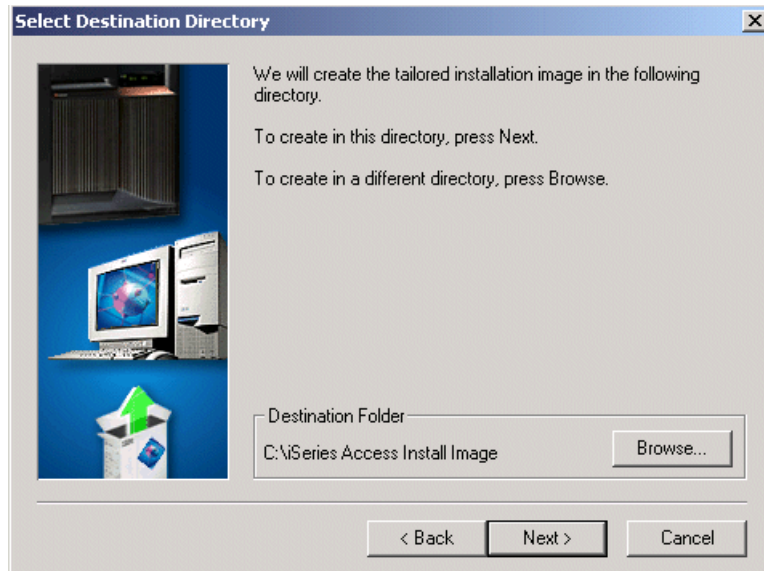


Figure 2-7 Select Destination Directory

3. By default, your tailored image will be created in a new directory called iSeries Access Install Image, as shown in Figure 2-7. The Browse button can be used to select a different directory if more than one image is going to be created or you want to use a different naming convention.

This location *must* be an empty directory. You cannot overwrite a previous installation image.

After you specify the appropriate directory, click **Next**. This opens the Component Selection window.

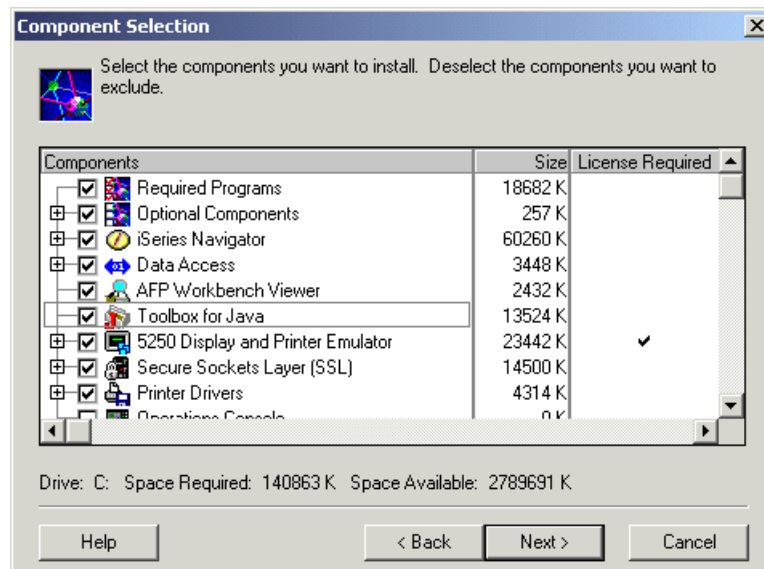


Figure 2-8 Component Selection

4. By default, all components are selected, as shown in Figure 2-8 on page 11. Notice that we show SSL in this figure. As stated earlier, SSL will only be available in the Component Selection list if you are using the source image from the iSeries and have 5722-CE3 installed as a licensed program product (LPP).

Deselect any components you do not want included in the installation image. If you deselect a component that other components depend on, a message displays indicating that these components will also have to be removed.

After you are satisfied with the components selected, click **Next**. Because we selected SSL, the SSL Selection Confirmation window opens. Review the window text. In this example, we comply with import and export requirements for SSL usage and click **Next**.



Figure 2-9 SSL Selection Confirmation

5. The Start Copying Files window opens, showing the components you selected. This is the last window before the copying files portion of install starts. After you are satisfied with the components selected, click **Next**.

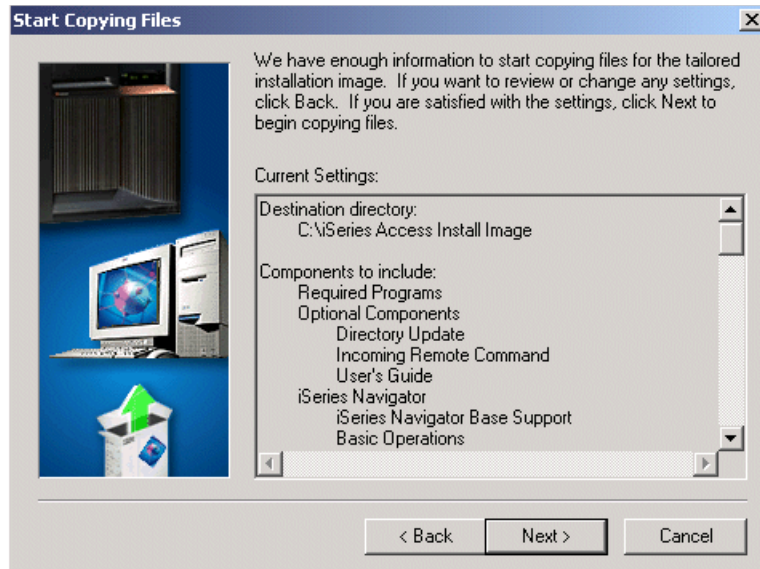


Figure 2-10 Start Copying Files

After clicking Next, the files are copied of files, and the tailored installation completes, as shown in the window in Figure 2-11.

6. Click **Finish** in this Tailored Installation Image Completed window.

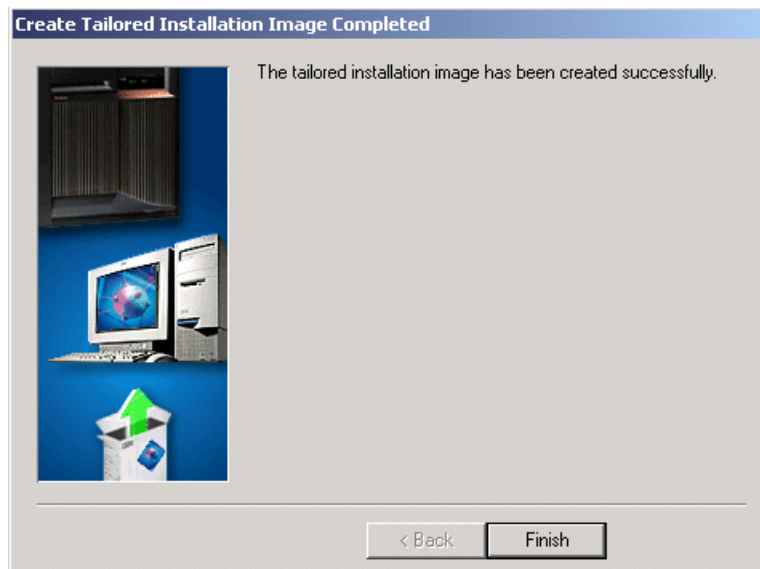


Figure 2-11 Successful creation of image

Assuming a successful tailored image completion, a new folder (directory) named iSeries Access Install Image (as shown in Figure 2-12 on page 14), or an image name you provided should have been created. Note that the SSL component will be in a subdirectory in this folder.

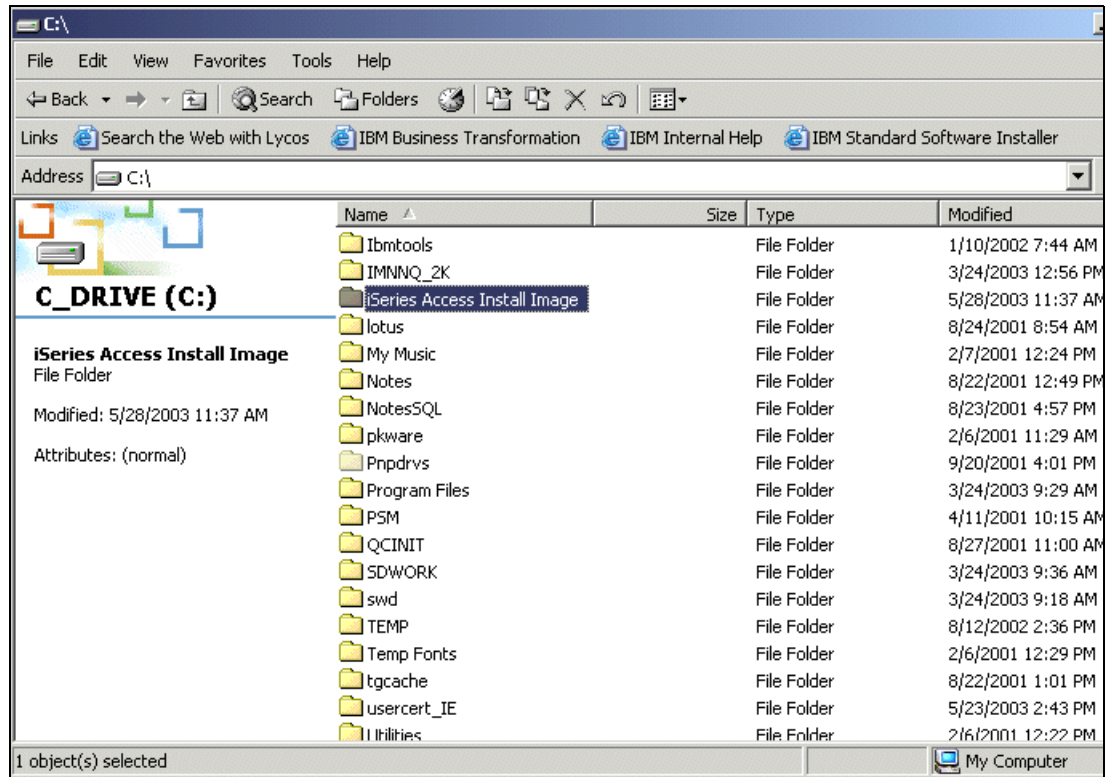


Figure 2-12 iSeries Access Install Image

The tailored installation wizard is not copied to this tailored install image. Therefore, you cannot create a tailored image from an image that was already tailored. Also, the tailored installation wizard is not installed onto the user's PC as part of the installation. You can only run this wizard from a complete installation image.

Prior to using this install image, it would be prudent to merge the latest service pack with it, as described in 2.3, "Combining a service pack with your install image" on page 15. Users who then install from this image will be at the latest fix level upon initial install.

Notes and tips:

- ▶ If a PC workstation is upgrading from a previous release using your tailored installation image and that PC contains components that are not contained in your tailored image, those components will be automatically uninstalled.
- ▶ An administrator might want to exclude users via OS/400 Work with Links (iWRKLNK) command or the iSeries Navigator File Permissions function, from accessing the original install image. This would prevent users from installing any restricted components.

You may also want to restrict users from these components through Application Administration (Chapter 3, "Application Administration: Administration system and Central Settings" on page 29) so that even if a user does install a restricted component, they are unable to use it.

- ▶ If you want one group of workstations to have a set of iSeries Access for Windows components and functions and another group of workstations to have a different set of component and functions, you can create different tailored installation images. Each set of workstations install from a specific image.

2.3 Combining a service pack with your install image

Combining a service pack with your install image enables you to continue the ease of maintaining client workstations by minimizing the steps necessary to have each workstation at the latest iSeries Access for Windows software level. This topic describes ways to build the combined image.

This topic is based on V5R1 Client Access for Windows or V5R2 iSeries Access for Windows, or later.

iSeries Access for Windows service packs are fixes for client code, meaning they do not contain any fixes or enhancements for the server. They are available either as a PTF (fix) or as a download from the Web. Sometimes, there may be “co-requisite iSeries server fixes” required for fixes in the iSeries Access for Windows service packs, but they are not included in the actual iSeries Access for Windows service pack.

Prior to V5R1M0, you were unable to combine service packs with your installation image, and therefore, your initial installation of client PCs typically was a two-step process: install the base release and then install the latest service pack.

There are two methods to update your installation image with the latest service pack so that the installation is a one step process:

1. Merge occurs on the iSeries server.
2. Merge occurs on a network drive.

We provide additional details about each of these methods in the next subtopics in this redbook.

If a later service pack becomes available, you can repeat the process described here with the new service pack to get another, new install image.

An image that has been merged with the service pack has numerous uses, such as:

- ▶ It can be used to install a new release on a client (and will automatically contain the merged service pack level).
- ▶ It can be used to upgrade to a new release (and will contain the merged service pack level).
- ▶ It can be used to selectively install a new component (and that component will automatically contain the merged service pack level).
- ▶ It can be used to install or reinstall a service pack (if the PC already has that release level of base code and only needs the service pack update).

2.3.1 Merging the service pack with the install image on the iSeries server

This section describes integrating the base release and a fix pack into a single image within an iSeries server's Integrated File System (IFS). It is not necessary to install service packs for iSeries Access for Windows on your iSeries server but there is a *significant* benefit to do so.

The first step is to order the PTF (for example, use the Send PTF Order (SNDPTFORD) command). Then apply the PTF to the iSeries. This updates the QIBM\ProdData\Access\Windows\Install\Image directory, which contains the client installation code.

This directory now contains the merge of both the base release and this service pack.

You can then use this directory as the source of the installation image, copy this directory to another location, or follow the instructions in 2.2, “Tailored installation image” on page 7 to create a tailored installation image.

Important: If you apply a new PTF at a later date, your tailored installation image must be re-created from the iSeries. An easy way to re-create a tailored installation image with the same components is to create a silent install response file for the tailored install, as described in 2.5, “Silent install” on page 22.

The only exception to these directions is to add “-fcwbining.ins” to the command line.

2.3.2 Using PTFFORM.EXE to merge a service pack and an install image

PTFFORM.EXE is a utility that enables you to merge the latest service pack to your existing tailored installation image.

Note: PTFFORM.EXE should only be used for merging a service pack with a copy of the original install image. Do not use PTFFORM against the original licensed product install image located on the iSeries server. You should use LODPTF/APYPTF so that DSPPTF and PTF requisite checking are accurate.

To merge the service pack within the install image on a network drive using the PTFFORM.EXE utility:

1. You can access the latest service pack and the PTFFORM.EXE utility from the iSeries Access Web site:

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

Select the **Service Packs (Fixes)** link for information about the latest service pack, in addition to the ability to immediately download the service pack. This leads to a window similar to the one shown in Figure 2-13 on page 17.

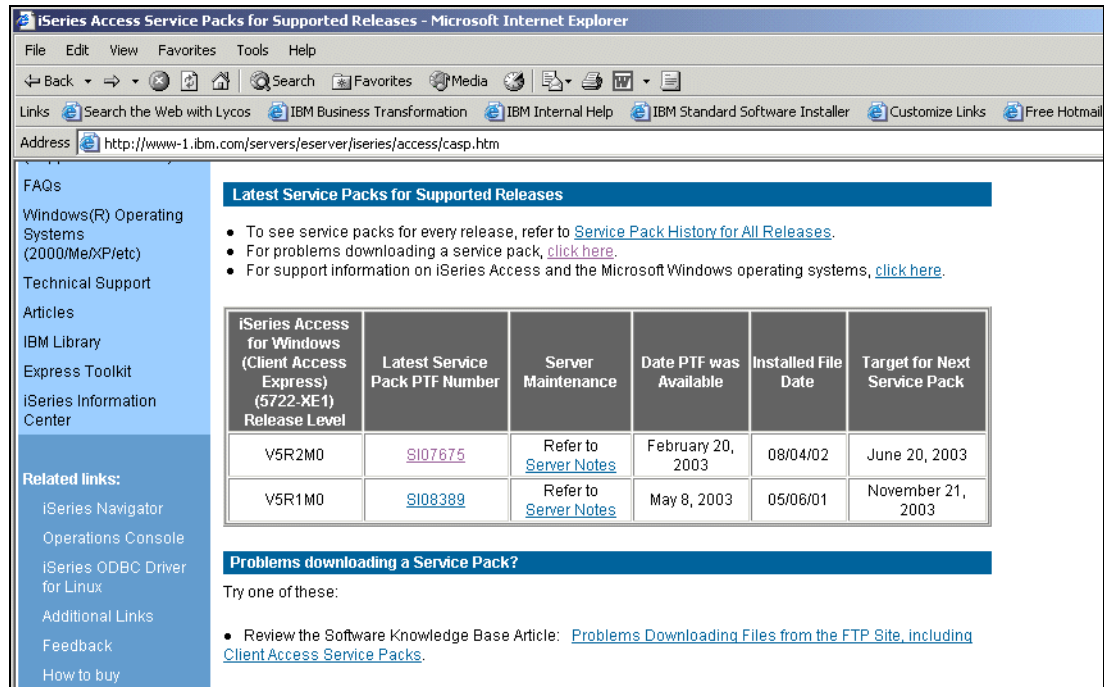


Figure 2-13 iSeries Access for Windows service packs available for download

- Notice in Figure 2-13 that the latest service pack for the different supported release levels are displayed. Select the appropriate service pack according to your release level and then select the tailored directory, which will appear in the next window (not shown).

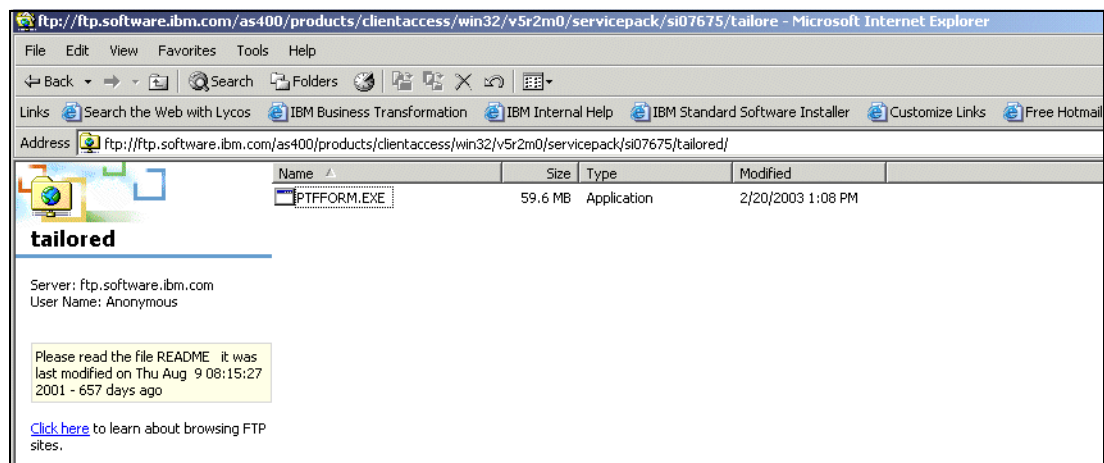


Figure 2-14 PTFFORM.EXE within the tailored directory

- The PTFFORM.EXE utility found in the tailored directory is the latest service pack with additional code that enables a merge with your install image. Select **PTFFORM.EXE** and select to download. This opens a window similar to the one shown in Figure 2-15 on page 18.

Tip: You might want to create a temporary folder on your PC prior to downloading software related to the service pack so that the download can be directed to this location. The key is to always download service packs to an empty folder.

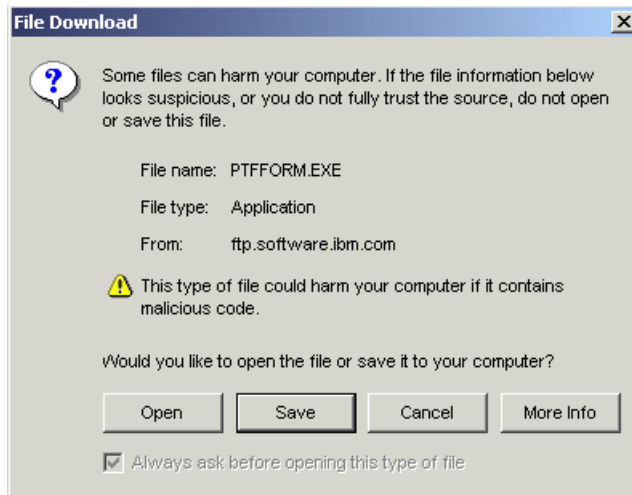


Figure 2-15 Downloading the service pack

4. In the File Download window, select the **Save** option to direct the download to a temporary folder. We chose to create a folder called v5R2servicepack in this example. Figure 2-16 shows PTFFORM.EXE downloaded to c:\v5R2servicepack.

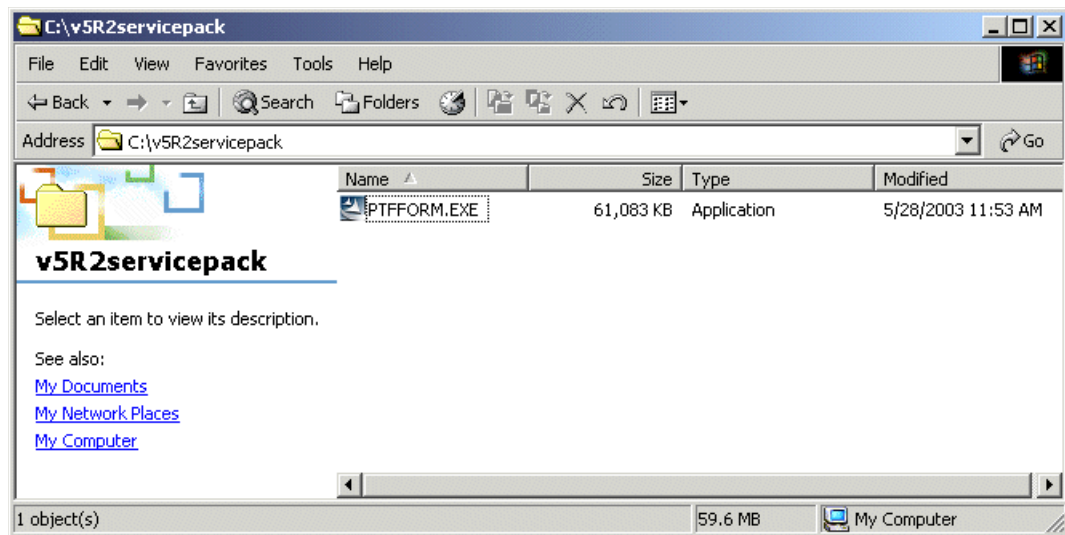


Figure 2-16 PTFFORM.EXE downloaded to a temporary folder

5. Select the PTFFORM executable to begin the update (merge) install image wizard, as shown in Figure 2-17 on page 19.

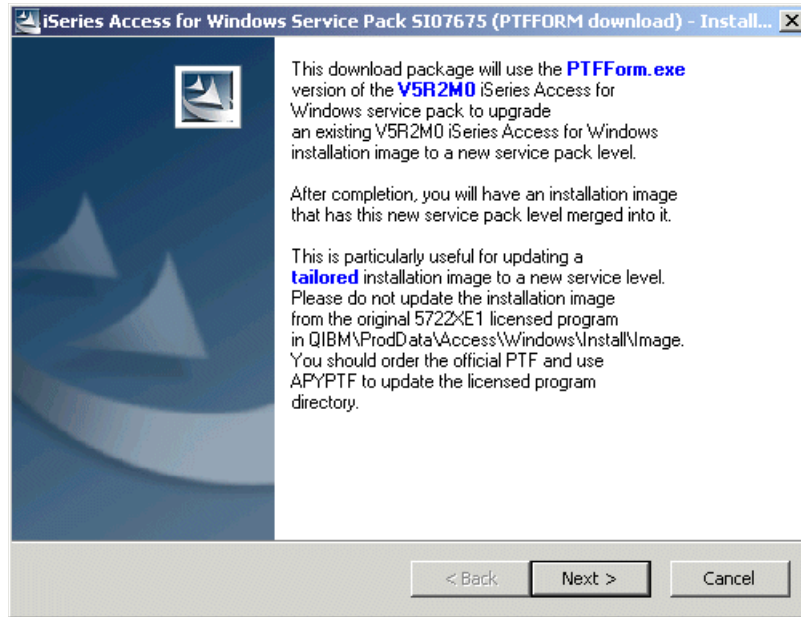


Figure 2-17 Running PTFFORM.EXE

6. Review the window text, especially the last paragraph regarding updating the iSeries code. Select **Next** to bring up the install image to new service level window, as shown in Figure 2-18.

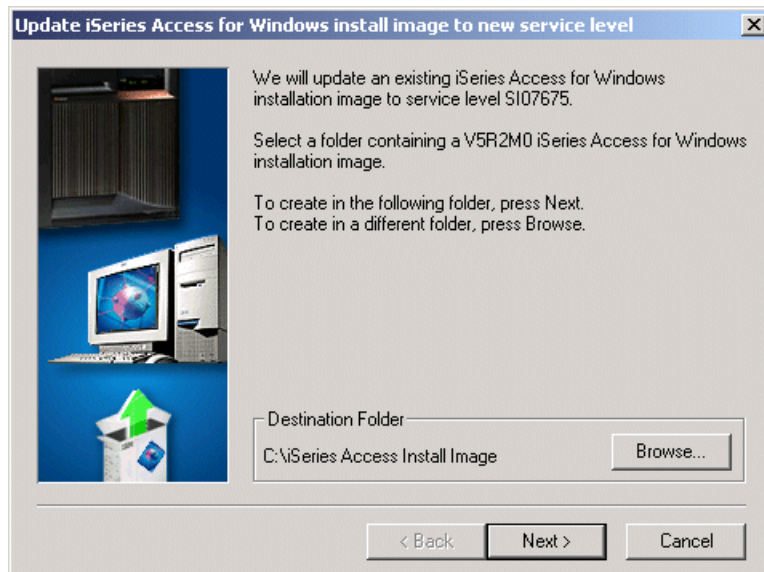


Figure 2-18 Destination Folder

7. Notice in Figure 2-18 that the Destination Folder (this should be the location of your install image) defaults to iSeries Access Install Image, which is the default folder name when creating a tailored installation image. Select **Next** to update the installation image with this service pack.
8. After the update image process completes, a window opens, as shown in Figure 2-19 on page 20. Select **Finish**.

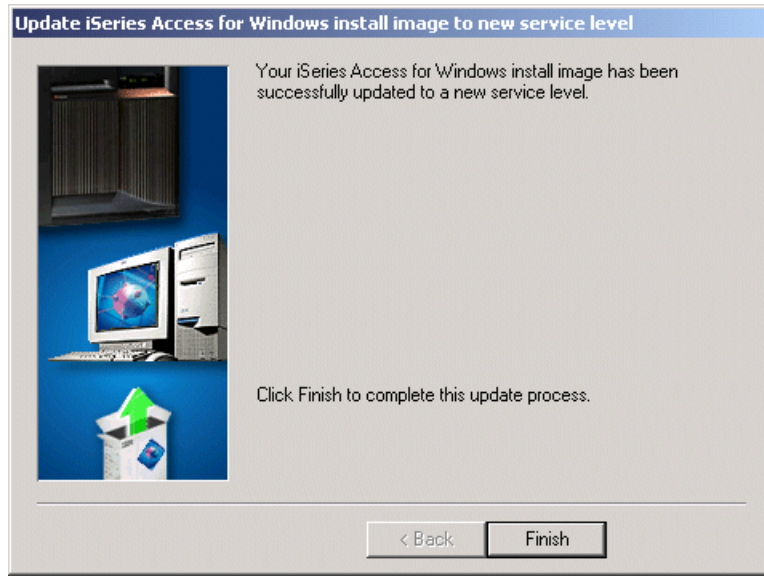


Figure 2-19 Update complete

This directory now contains the updated tailored installation image that includes this service pack.

2.4 Distributing and installing the merged installation image

Your new tailored and updated installation image can now be copied to a CD or shared on your network for installation. If you copy this install image to a CD, iSeries Access for Windows will run automatically when the CD is inserted into the PC workstation CD drive.

In the following description, we use an image located in the iSeries Access Install Image directory on the PC workstation.

To distribute and install the merged installation image:

1. Setup.exe, the primary installation program, is located in your installation directory, as shown in Figure 2-20 on page 21. Double-click **setup.exe** to begin the installation.

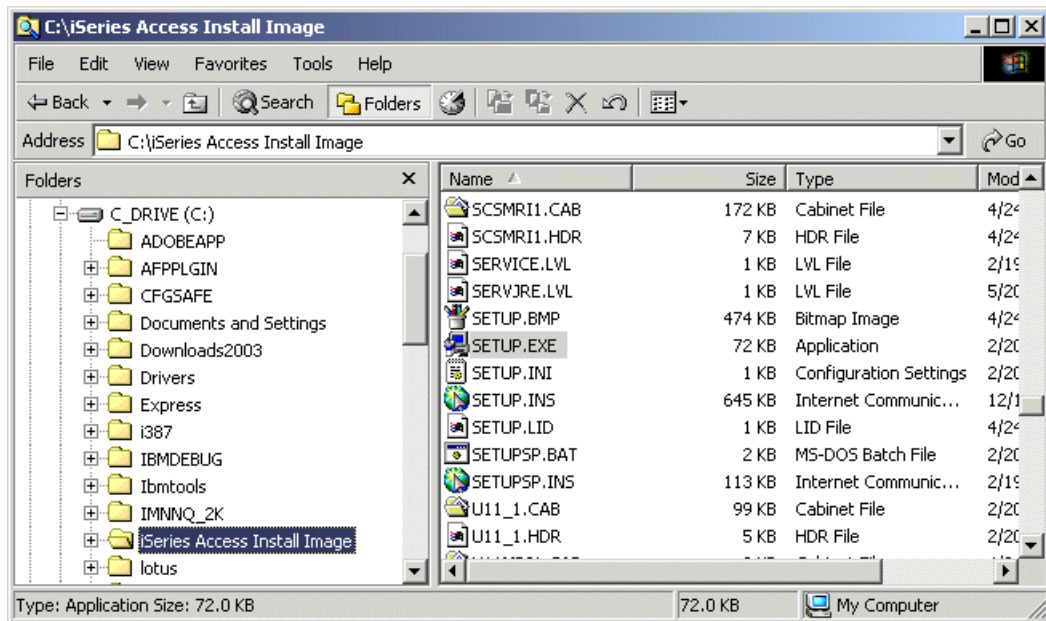


Figure 2-20 *SETUP.EXE*

This opens the window shown in Figure 2-21, where you can select the type of installation you want to perform.

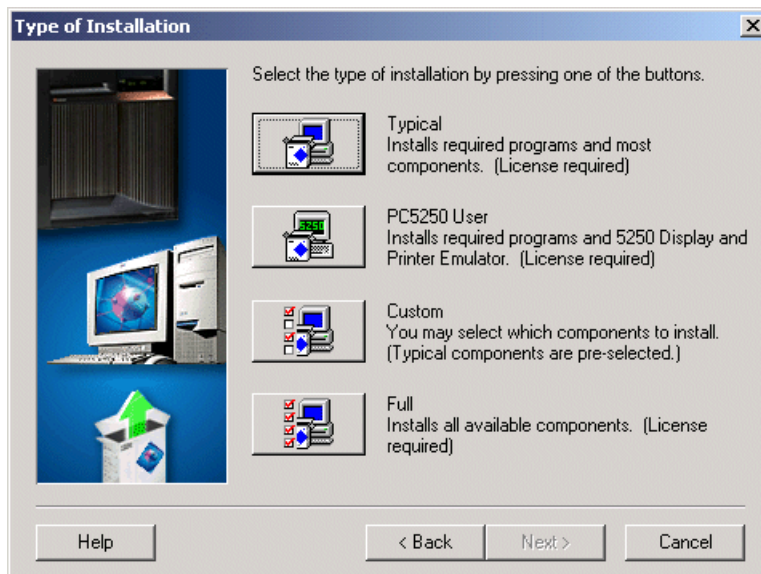


Figure 2-21 *Type of Installation*

- Remember that a Full install in this environment includes only the components in your tailored install image. If you want to install a subset of components from your tailored image, select the Custom button. If you select a Typical install, only the components that are identified as typical components in the original install that exist in your tailored install image are installed. If you select a PC5250 User install, only the components that are identified as PC5250 components in the original install that exist in your tailored install image are installed.
- After the iSeries Access for Windows setup program begins, follow the straightforward instructions and online help in the program until the program completes.

4. After the installation has completed, open iSeries Access for Windows on the desktop and then open iSeries Access for Windows Properties to see the service level, as shown in Figure 2-22.

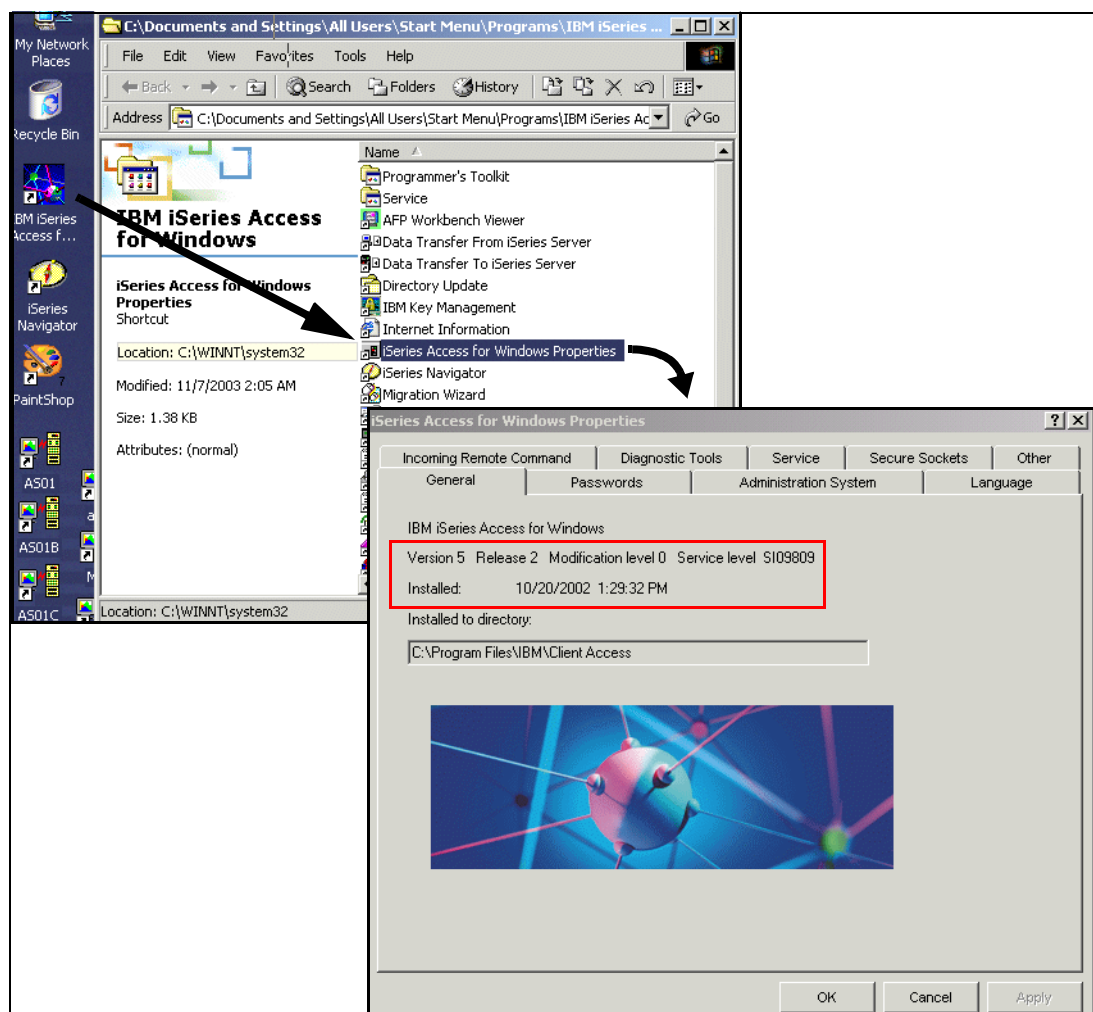


Figure 2-22 iSeries Access for Windows Properties

You can also use **Start → Program Files → IBM iSeries Access for Windows → iSeries Access for Windows Properties** to see this service level information.

Note: If the current release is already installed on the PC, you do not need to reinstall to get the latest service pack from your merged tailored image. You can use setupsp.bat, the Install Service Pack shortcut, or the Check Service Level shortcut to install just the service pack.

2.5 Silent install

An additional way to distribute your tailored install image, or any install image, is with a silent installation.

Note, the information presented here is a consolidation of information available in V5R2 iSeries Information Center located at the following URL:

<http://publib.boulder.ibm.com/series/v5r2/ic2924/index.htm>

You can find the Information Center information by selecting **Connecting to iSeries → What to connect with → iSeries Access → iSeries Access for Windows → Administration → Installing or migrating on multiple PCs → Installing or migrating silently**.

Silent installation eliminates the need for any user interaction during the iSeries Access for Windows setup process. A response file provides all the installation information so that no dialog boxes display while installing iSeries Access for Windows. To perform a silent installation:

1. Create your response file.

The response file contains the installation options that the system would normally prompt you for during the installation process. In the following text we describe how to create the response file.

2. Start the silent installation.
3. Check the log file return codes to see if your installation was successful.

The silent install has a progress indicator. The Silent Install Indicator is an icon in the task tray that appears when a silent install is launched and remains in the task tray as long as the install is executing. Passing the cursor over the icon will cause the Silent Install Indicator to display the percent of the install that is complete. The Silent Install Indicator can also be expanded to expose more information. When the install completes successfully, the icon will disappear from the task tray. If the install fails, the icon will remain, and a small red triangle appears on the icon to indicate the failure. Click the red triangle to see the failure message.

Tip: If the Silent Install Indicator displays a given percentage of completion longer than you would expect, you might want to check the log file for errors. You specify the name and location of the log file when you start the silent installation. You can also see additional information about failures in `silent.txt` in the target directory, or in `cwbsilent.txt` in the Windows directory (Windows or WinNT) if the target directory is not yet set.

Important: Often the best way to debug a silent install failure is to start the install in non-silent mode on the user PC, and see if there are any unexpected dialog boxes that appear prior to the Component Confirmation panel. Most silent install failures occur due to unexpected dialog boxes that appear prior to the actual component installation file transfers.

2.5.1 Creating a response file

A response file records the selections made in response to the prompts in the installation process. During a silent installation, the setup program uses the response file to get the information necessary to complete the installation.

To create a response file, follow these steps:

1. At the PC workstation DOS command line, set the current directory to the iSeries Access for Windows installation image directory. To run an installation and record the responses, enter:

```
setup -r -f1d:\dir\file.iss
```

Where:

- `-f1` is an optional parameter used to indicate an alternate response file name. If you do not use this parameter, the `setup.iss` file records all of the installation choices. `Setup.iss` resides in the Windows directory, for example, `C:\Windows` or `C:\Winnt` depending on your PC operating system.
 - `d:\dir\` is the drive and directory where you want to create the response file. If you use the `-f1` parameter, you must specify the drive and directory along with the response file name that you want to create.
 - `file.iss` is the name of the response file that you want to create. The file extension must always be `iss`.
2. Complete the setup program, providing the responses you want to use during the silent installations.

2.5.2 Starting a silent installation

Silent installations use a response file (`setup.iss` or your alternate response file) for the responses to prompts during the installation process. This eliminates the need for any user interaction during the installation process, and allows you to quickly and easily copy duplicate installations across your network. Information about the status of the silent installation can be recorded in a log file (`file.log`).

To start a silent installation, type the following at a command line prompt in the iSeries Access for Windows installation image directory:

```
setup -s -f1d:\dir\file.iss -f2d:\dir\file.log
```

Where:

- ▶ `-f1` is an optional parameter where you can specify the response file (`file.iss`) to use. If you do not use this parameter, the installation attempts to use a default response file named `setup.iss`. It looks for this file in the directory containing `setup.exe`. `d:\dir` is the drive and directory that contains the response file that you want to use. If you use the `-f1` parameter, you must specify the drive and directory along with the response file name.
- ▶ `-f2` is an optional parameter where you can specify the location and name for the log file that the silent installation creates. If you do not use this parameter, the installation creates a log file named `setup.log` and places it in the directory containing `setup.exe`. `d:\dir` is the drive and directory that contains the log file. If you use the `-f2` parameter, you must specify the drive and directory along with the log file name. `file.log` is the name of the log file that you want to create.

2.5.3 Example response file: `setup.iss`

The response file shown Example 2-1 on page 25 is from a Custom installation with all the components selected. Your file will differ depending on the installation type, the components you select, and your national language version.

Tip: In the sample response file, note that `BootOption=3` (located toward the end of the example response file). This means that the PC automatically reboots when the installation completes. If you do not want this to happen, set `BootOption=0`.

Example 2-1 Example response file

```
[InstallShield Silent]
Version=v5.00.000
File=Response File

[DlgOrder]
Dlg0=SdWelcome-0
Count=9
Dlg1=SdLicense-0
Dlg2=SdOptionsButtons-0
Dlg3=SdAskDestPath-0
Dlg4=CwbComponentDlg-0
Dlg5=SdShowDlgEdit1-0
Dlg6=SdStartCopy-0
Dlg7=SdAskOptions-0
Dlg8=SdFinishReboot-0

[SdWelcome-0]
Result=1

[SdLicense-0]
Result=1

[SdOptionsButtons-0]
Result=103

[SdAskDestPath-0]
;Note - This is the directory where iSeries Access for Windows will be installed.
szDir=F:\Program Files\IBM\Client Access
Result=1

[CwbComponentDlg-0]
CAOptional-type=string
CAOptional-count=4
CAOptional-0=CAOptional\DirUpdate
CAOptional-1=CAOptional\IRC
CAOptional-2=CAOptional\MAPI
CAOptional-3=CAOptional\OUG
Unity-type=string
Unity-count=14
Unity-0=Unity\Base
Unity-1=Unity\BasicOp
Unity-2=Unity\AppDevWorkManagement
Unity-3=Unity\SysConfig
Unity-4=Unity\Network
Unity-5=Unity\Security
Unity-6=Unity\UserGroups
Unity-7=Unity\Database
Unity-8=Unity\FileSys

Unity-10=Unity\Backup
Unity-11=Unity\AppDev
Unity-12=Unity\Commands
Unity-13=Unity\Packages
Unity-14=Unity\Monitors
Unity-15=Unity\LogicalSystems
Unity-16=Unity\AFPManger
Unity-17=Unity\ManCentral
Unity-18=Unity\Admin
DataAccess\FileTransfer-type=string
```

```

DataAccess\FileTransfer-count=3
DataAccess\FileTransfer-0=DataAccess\FileTransfer\DataXfer
DataAccess\FileTransfer-1=DataAccess\FileTransfer\Excel
DataAccess\FileTransfer-2=DataAccess\FileTransfer\WK4
DataAccess-type=string
DataAccess-count=3
DataAccess-0=DataAccess\FileTransfer
DataAccess-1=DataAccess\ODBC
DataAccess-2=DataAccess\OLEDB
Emulators\Standard\PCFont-type=string
Emulators\Standard\PCFont-count=1
Emulators\Standard\PCFont-0=Emulators\Standard\PCFont\Latin2
Emulators\Standard-type=string
Emulators\Standard-count=3
Emulators\Standard-0=Emulators\Standard\Base
Emulators\Standard-1=Emulators\Standard\PdfPdt
Emulators\Standard-2=Emulators\Standard\PCFont
Emulators-type=string
Emulators-count=1
Emulators-0=Emulators\Standard
PrinterDrivers-type=string
PrinterDrivers-count=1
PrinterDrivers-0=PrinterDrivers\AFP
Toolkit-type=string
Toolkit-count=2
Toolkit-0=Toolkit\Base
Toolkit-1=Toolkit\VBW
Component-type=string
Component-count=13
Component-0=Install
Component-1=Base
Component-2=CAOptional
Component-3=Unity
Component-4=DataAccess
Component-5=MDAC
Component-6=AFPViewer
Component-7=JRE
Component-8=JAVATB
Component-9=Emulators
Component-10=PrinterDrivers
Component-11=OpCon
Component-12=Toolkit
Result=1

[SdShowDlgEdit1-0]
szEdit1=IBM iSeries Access for Windows
Result=1

[SdStartCopy-0]
Result=1

[Application]
Name=iSeries Access for Windows
Version=CurrentVersion\Selectively_Installable_Components\Toolkit VB
Wizard
Company=IBM

[SdAskOptions-0]
Component-type=string
Component-count=1

```



```
Component-0=Add program folder shortcut to desktop
Result=1

[SdFinishReboot-0]
Result=1
BootOption=3
;Note - Setting BootOption to 3 means that the silent install will
;       automatically reboot the PC. If you do not want to reboot
;       automatically, set BootOption to 0.
```

2.5.4 Installing upgrades and service packs silently

Using Figure 2-23 as an example, select the **Perform silent installation** check box on the Service tab of iSeries Access for Windows Properties window to do service level checks and service pack installation silently, without any user interaction.

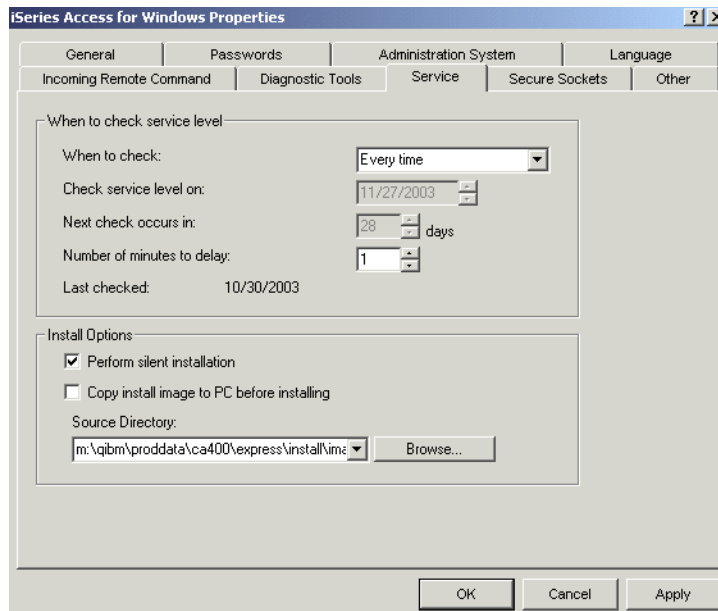


Figure 2-23 iSeries Access for Windows Properties: Silent service pack install


The silent service pack installation utility uses information from a response file to answer prompts automatically.

The response file is identical to the one used in the silent installation, except you must specify the following name:

- ▶ SLTSP.ISS - For service packs (this file must reside in the same directory as your service pack setup.exe does).
- ▶ SLTSP.ISS - For upgrades (this file must reside in the same directory as your installation setup.exe does).

When you create your response file, you can set a parameter to reboot automatically (BootOption=3). If you set this to yes, you should set SCHEDCHECK in a scheduled job so that the silent check service version runs during the night. See the online *iSeries Access for Windows User's Guide* for more information about SCHEDCHECK.

If your response file automatic reboot is set to no, a message box opens (if a reboot is determined to be necessary) asking the user to select **OK** to restart the system.



Application Administration: Administration system and Central Settings

This chapter describes how to use the iSeries Navigator function of Application Administration to use the new V5R2 Central Settings function, including:

- ▶ The configuration of an Administrative System with Central Settings
- ▶ The registration of Central Settings to be managed
- ▶ The management of settings for users or groups, or both
- ▶ Client discovery of the administration system and the Central Settings

3.1 Administration system and Central Settings overview

You can restrict iSeries Access for Windows functions on a client workstation by the following primary methods:

- ▶ Do not include a specific component or set of functions during the iSeries Access for Windows installation process.
- ▶ User exit programs called during client workstation signon to the iSeries server.
- ▶ The iSeries Access for Windows Application Administration component.

These capabilities are thoroughly described in the Information Center and the IBM Redbook *Managing your iSeries System with Operations Navigator V5R1: Overview and More*, SG24-6226.

This chapter specifically addresses the *Central Settings* support within Application Administration, which is new in V5R2.

Application Administration is an optionally-installable component of iSeries Navigator. With Application Administration, administrators can control the iSeries Access for Windows functions or applications available to users and groups on a specific server. This includes controlling the functions available to users that access their server through clients. If you access a server from a Windows client, the OS/400 user profile, and not the Windows user, determines which functions are available.

Application Administration controls access to any application that has a defined *administrable function* on your server. iSeries Navigator and iSeries Access for Windows are examples of applications that have defined administrable functions. For example, you can grant or deny access to the Printer Output function in Basic Operations, and grant or deny access to the entire Basic Operations or Work Management administrable function in iSeries Navigator.

These administrable functions can be specifically managed from an iSeries Navigator client workstation with the Application Administration component installed. You specify accessibility to the specific component or component subfunctions on a specific iSeries server.

Starting with V5R2, Application Administration adds support for *Central Settings*. The Central Settings support in Application Administration provides the ability to manage most of the functions iSeries Access for Windows controls through the following policy templates:

- ▶ Runtime Restrictions (caerestr.adm)
- ▶ Mandated Connection Properties (config.adm)
- ▶ Configuration Policies (caecfg.adm)

As shown in Figure 3-1 on page 31, the administration system is a central system that is used to manage many of the properties used by iSeries Access for Windows clients. It is important to know that:

- ▶ *Central Settings* can only control iSeries Access for Windows functions. They cannot control iSeries Navigator or the function of other applications.
- ▶ You must use *Local Settings* to control the use of iSeries Navigator functions and other applications. In previous releases of Application Administration, restrictions had to be set up for each system (now referred to as Local Settings) that users connected to.
- ▶ The introduction of an administration system with Central Settings allows an administrator to set up restrictions on one system for users/groups that is then applied to all systems.

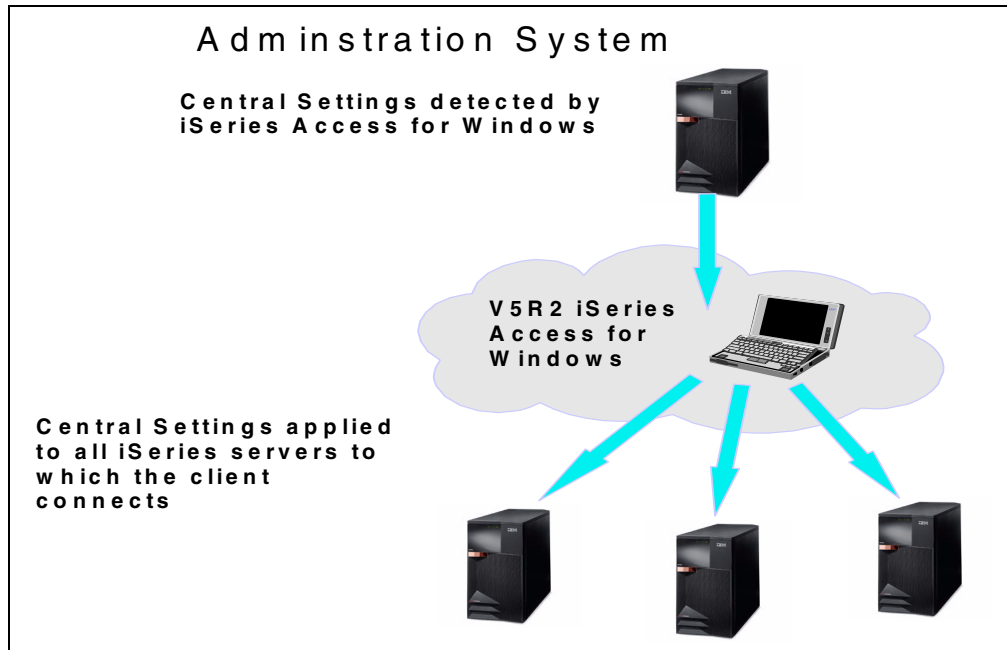


Figure 3-1 Sample scenario implementing Central Settings

The administration system is any V5R2 or later iSeries that has been configured to serve Central Settings to client PCs. By default, all iSeries are configured to not be an administration system. A system administrator must use Application Administration to configure an iSeries server before it can act as an administration system. Typically, a network will have only one iSeries system acting as the administration system. This administration system will be used by iSeries Access for Windows clients as the source for their administration system settings. Although a network can have multiple iSeries systems defined as the administration system, iSeries Access for Windows clients will only use a single administration system for their Central Settings.

An administrator can work with users and groups using Application Administration on a local server, but the administration system provides additional ways to manage users and groups. An administrator can use the Advanced Settings of an administration system to control what environments are available to specific users and groups and set password, connection, service, and language settings.

Important: You must have security administrator (*SECADM) and all object (*ALLOBJ) special authorities to work with the Advanced Settings on an administration system. This differs from other Local Settings in Application Administration that only require security administrator (*SECADM) special authorities to make changes.

3.2 Application Administration concepts

In order to support the functionality previously only available through iSeries Access for Windows policies templates, Application Administration introduced several new concepts in V5R2:

- **Administration system:** The administration system is any V5R2 or later iSeries that has been configured to serve Central Settings to client PCs. By default, all iSeries are configured to not be an administration system.

- ▶ **Local Settings:** Local Settings can reside on any iSeries and were the only type of administrative settings supported by Application Administration prior to V5R2. They are called Local Settings because each iSeries maintains its own set of Application Administration settings. When an iSeries Access for Windows client accesses multiple iSeries servers, it will use a different set of Local Settings for each server.

Information about the configuration of Local Settings can be found at:

- iSeries V5R2 Information Center:

<http://publib.boulder.ibm.com/series/v5r2/ic2924/index.htm>

Select **Connecting to iSeries** → **What to connect with** → **iSeries Access** → **iSeries Access for Windows** → **Administration** → **Setting restrictions using policies and Application Administration**.

- The IBM Redbook *Managing your iSeries System with Operations Navigator V5R1: Overview and More*, SG24-6226.

- ▶ **Central Settings:** Central Settings are new in V5R2 and can only be supported by V5R2 or later iSeries servers that are configured as an administration system.

Important: Only V5R2 or later iSeries Access for Windows clients will retrieve Central Settings from an administration system. The Central Settings affect iSeries Access for Windows properties that apply to all iSeries servers that the client may access. The main difference between Central Settings and Local Settings is that the Central Settings are retrieved from a single central server, and Local Settings are retrieved from each iSeries being accessed by the PC.

3.3 Implementing Central Settings

To take advantage of the Central Settings support in iSeries Navigator, perform the following steps:

1. Configure an iSeries to be an administration system. This system is where the Central Settings will be managed.
2. Register the Central Settings that you want to manage from the administration system.
3. Determine the properties you want to manage through Central Settings and modify them as you see fit.
4. Choose the mechanism that client PCs will use to discover their administration system.

3.3.1 Choosing an administration system

The first step in implementing Central Settings is to select an iSeries system in your network that will act as the administration system.

Important: Remember that your administration system must be at V5R2 or a later release.

To configure an iSeries as your administration system:

1. Open the iSeries system properties in iSeries Navigator.

To open the system properties, right-click your system name under the **My Connections** folder and select **Properties**. See Figure 3-2 on page 33.

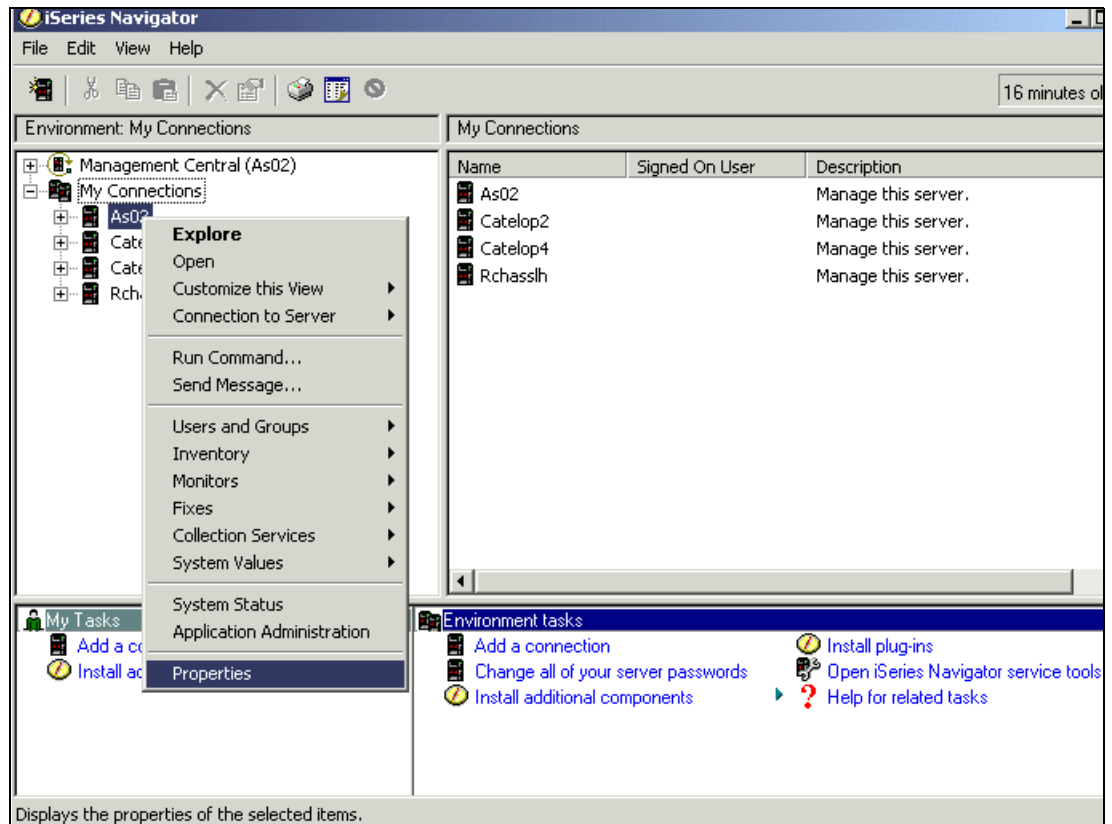


Figure 3-2 iSeries system properties

2. Select the Administration System tab on the Properties window, as shown in Figure 3-3 on page 34. Notice that by default the system is not an administration system.

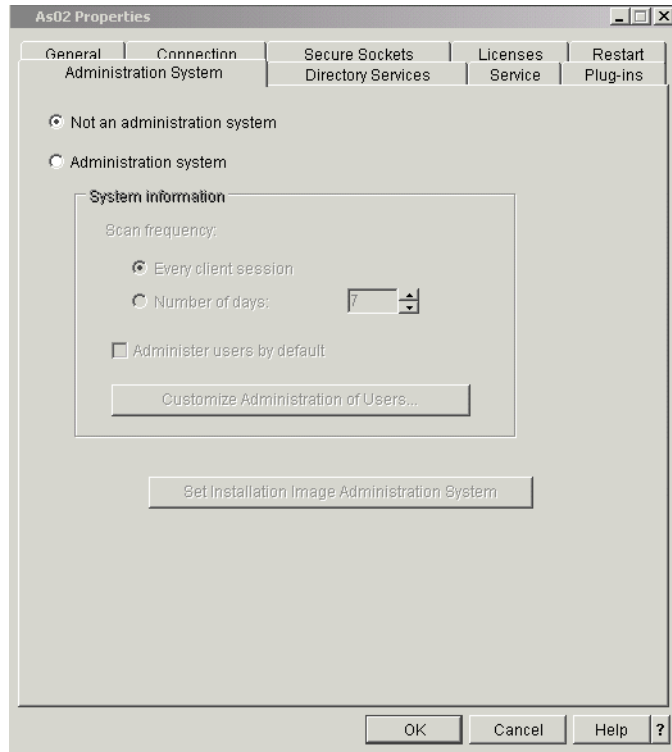


Figure 3-3 Administration System tab within the properties of your iSeries system

3. Select the **Administration system** radio button to select this iSeries system as your administration system to store your Central Settings. Notice in Figure 3-4 on page 35 that the additional parameters and buttons previously not available are now available for modification, including Scan frequency and the Customize Administration of Users and Set Installation Image Administration System buttons.

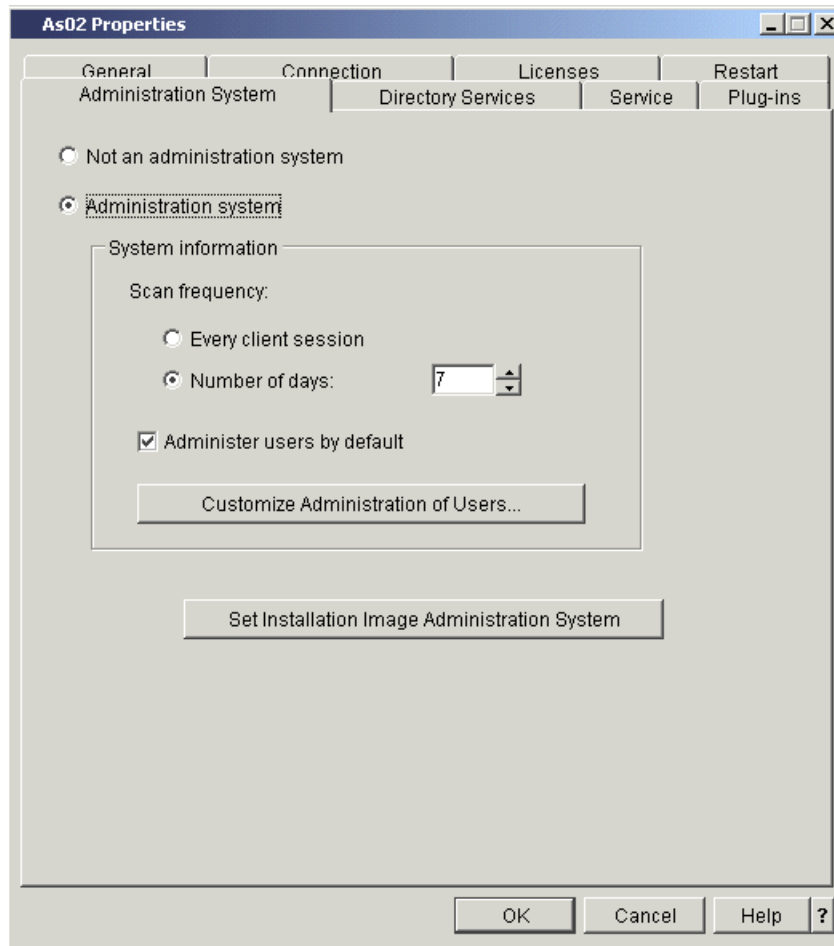


Figure 3-4 Administration system selected

The options include:

- **Customize Administration of Users button:** An administrator can determine exactly which users will or will not be administered by the administration system.

Tip: In the simplest configuration, an administration system will either administer all users or none of them. If Administer Users by Default is selected, it does not mean that all users have restrictions. It simply means that all users will check the administration system for any Central Settings that apply to their user profile. The setting of restrictions will actually be done through the Central Settings configuration. There can be cases where an administrator will want only some of the users on the system to use it as their administration system. In that case, the Customize Administration of Users panel must be used.

- **Scan frequency:** This set of controls indicates how frequently the client PC will automatically download its Central Settings from the administration system. It can range from once every client session to once every 1 to 14 days.
- **Set Installation Image Administration System:** This button allows an administrator to set up an initial administration system in the iSeries Access for Windows install image on the given iSeries. Doing this causes every client that installs with the image to have its initial administration system defined by the install image.

- Customize Administration of Users button: This will display the window shown in Figure 3-5 in the following section.

3.3.2 Customizing the administration of users

This topic shows how to set up the central administration of users or groups.

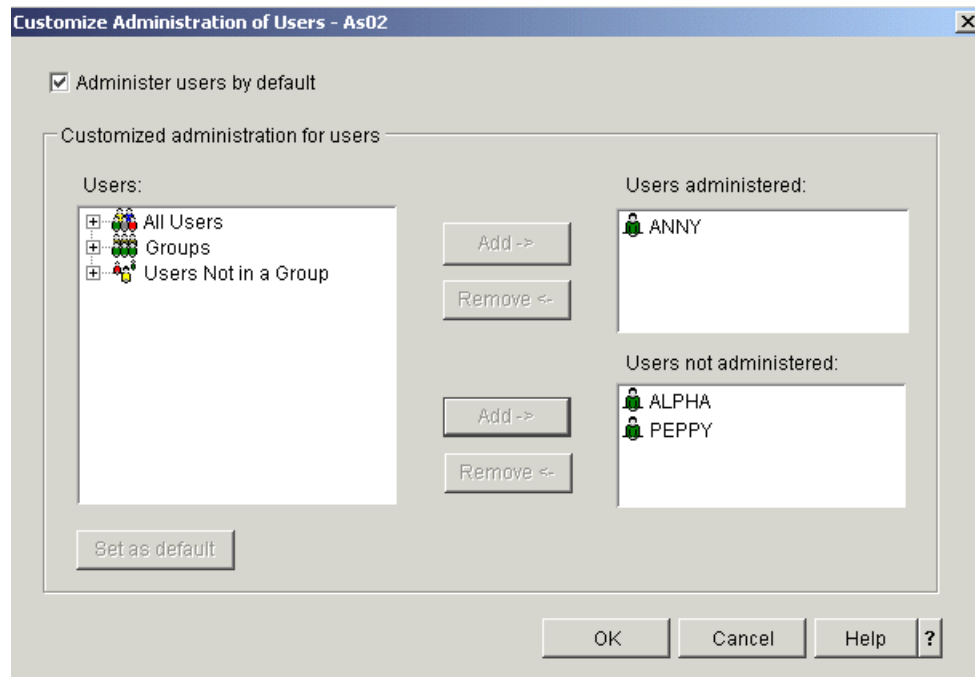


Figure 3-5 Customize Administration of Users

The Customize Administration of Users window is grouped into the following categories:

- Administer users by default: This is the same field that is on the Administration System properties panel. It indicates whether the iSeries can serve as an administration system for all users on this system, unless specifically indicated otherwise in the Customize Administration of Users window.
- Users administered: This list contains the users that will be administered, regardless of the value of the “Administer users by default” setting.
- Users not administered: This list contains the users that will not be administered, regardless of the value of the “Administer users by default” setting.
- Users: This contains the list of all users and groups on the system. Selected users and groups can be added to either the “Users administered” or “Users not administered” lists.

Note: Groups can be selected, but if they are moved to the “Users administered” or the “Users not administered” lists, only their member users are moved and not the group itself. (This is done because if the user is a member of multiple groups, and some of these groups are administered and some are not, it is unclear whether the user should be administered.)

- Set as default: This button removes the selected users from the “Users administered” and the “Users not administered” lists and returns them to the “Users” list. It causes the selected profile to use the value of the “Administer users by default” field.

3.3.3 Configuring Central Settings

After an iSeries has been configured as an administration system, the Application Administration context menu (displayed when right-clicking a system in iSeries Navigator) will contain a submenu with the following choices, as displayed in Figure 3-6:

- ▶ Central Settings: This is used to launch the Central Settings panels.
- ▶ Local Settings: This menu provides support for managing the “Local Settings” in Application Administration.

If the iSeries is not an administration system, the Application Administration context menu will not have the submenu, and selecting Application Administration will launch the panels for managing only Local Settings.

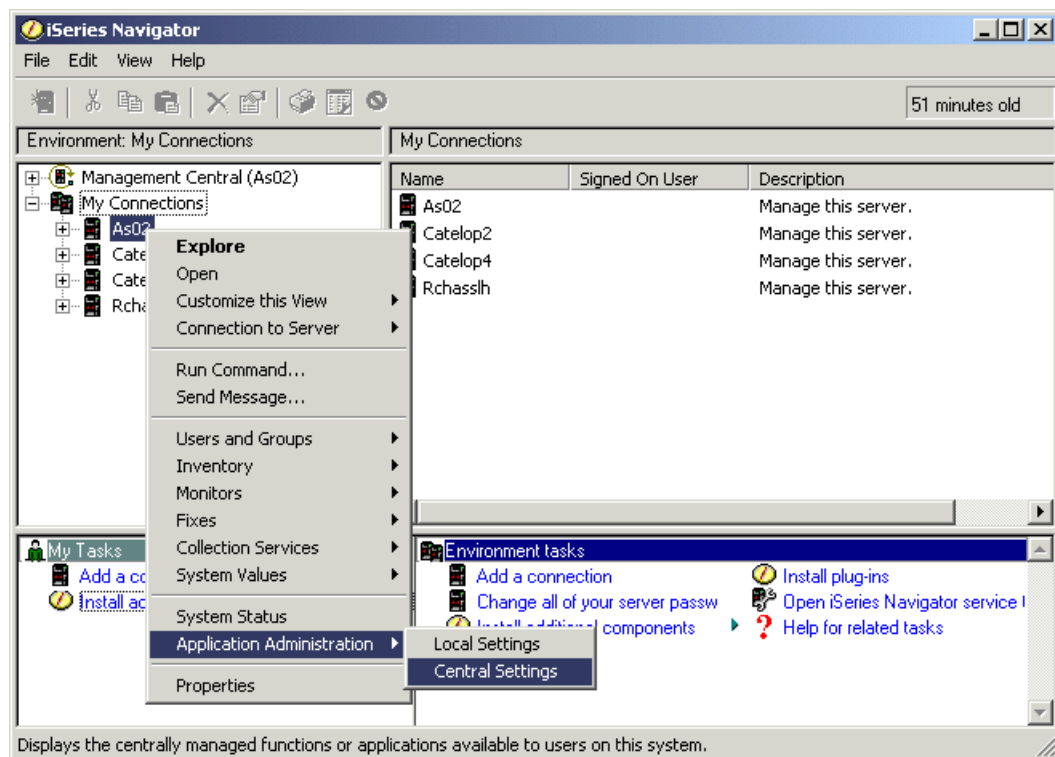


Figure 3-6 Submenu for Application Administration showing Central Settings

3.4 Registering Central Settings

After an iSeries has been configured as an administration system, the administrator has to register the Central Settings that are to be managed. There are two types of Central Settings in V5R2:

- ▶ iSeries Access for Windows: These are the basic Central Settings for iSeries Access for Windows and only support denying or allowing users access to specific functions.
- ▶ Advanced Settings for iSeries Access for Windows: The Advanced Settings provide the administrator with the ability to control more complex settings than the typical “allow” or “deny” setting values that are supported in Application Administration Local and Central Settings. An administrator can use Advanced Settings to define a set of environments and server connections that will be automatically downloaded to an iSeries Access for Windows client. The environments and server connections are always mandated values;

the client cannot modify them. In addition, Advanced Settings can be used to configure default settings or restrict clients to using specific settings for many of the password, connection, service, and language attributes used by iSeries Access for Windows clients.

To register the Central Settings, use the following steps on a system configured to be an administration system:

1. Right-click the system name and select **Application Administration** → **Central Settings**, as shown in Figure 3-6 on page 37.
2. On the next window (not shown) select **Applications** on the Application Administration (Central Settings) panel. This launches the Applications (Central Settings) window, as shown in Figure 3-7.

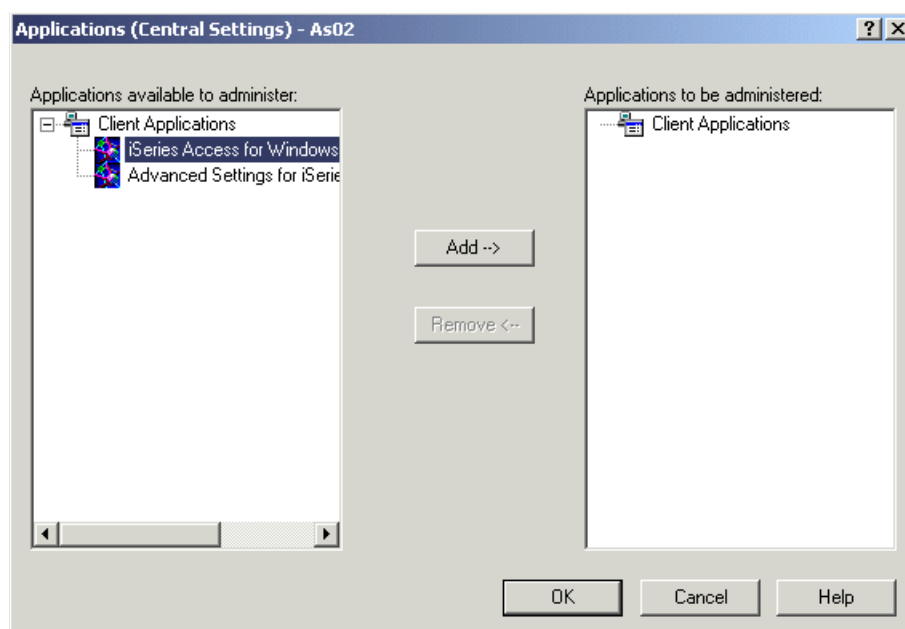


Figure 3-7 Applications available to administer

3. In the Applications (Central Settings) window, select the Central Settings that are to be managed on the administration system.

Applications can have their Central Settings registered on the administration system by adding them (**Add** button), which places them in the Applications to be administered list. Applications can have all of their Central Settings removed from the administration system by moving them (**Remove** button) to the Applications available to be administered list.

In Figure 3-8 on page 39, we added iSeries Access for Windows and Advanced Settings for iSeries Access for Windows.

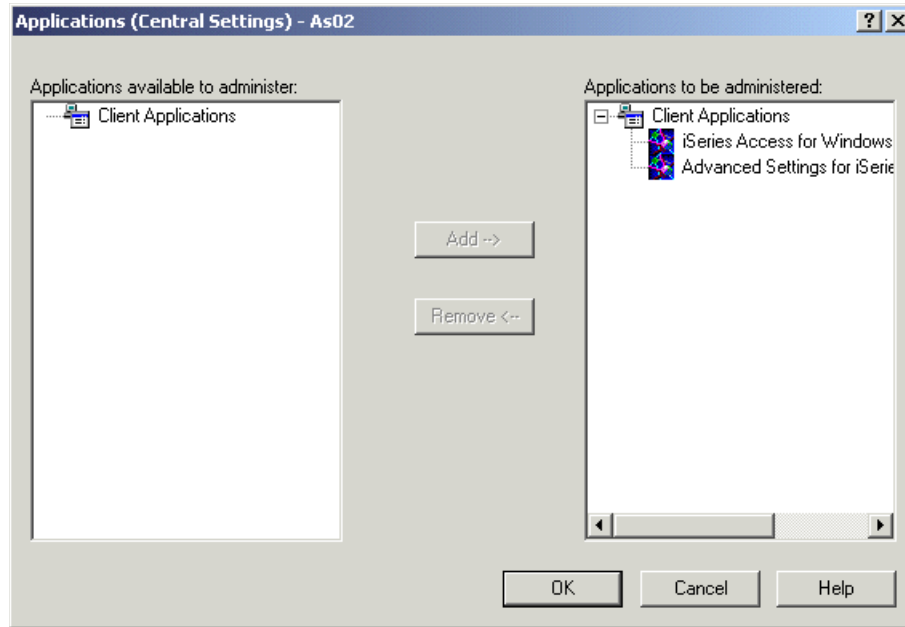


Figure 3-8 Applications to be administered

4. Click **OK** when you are finished with your selections. This registers your Central Settings.

3.5 Managing Central Settings

After the Central Settings have been registered on the administration system, the administrator can manage the settings for each user.

Figure 3-9 on page 40 displays the basic Central Settings, identified by iSeries Access for Windows on the Applications (Central Settings) panel shown in Figure 3-8. If iSeries Access for Windows was not registered in the prior step, this window would be empty.

To get this window, use the main iSeries Navigator window. Right-click the administration system. In the context menu, select **Application Administration** → **Central Settings** to get a window similar to the one shown in Figure 3-9 on page 40.

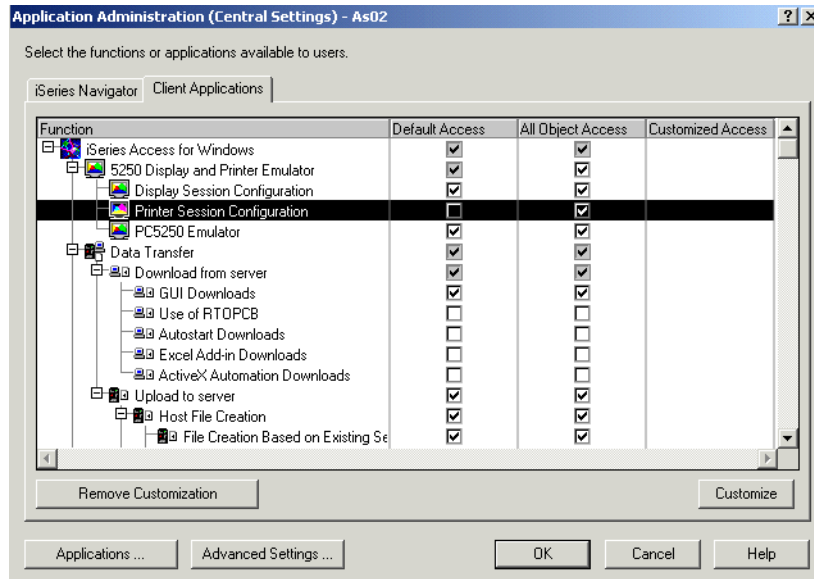


Figure 3-9 Client applications available to be managed: Printer Session example

In this example, we use the Client Applications tab panel, expanded items under **iSeries Access for Windows** → **5250 Display and Printer Emulator**, and selected **Printer Session Configuration**. Default Access is not selected and All Object Access is selected. There is no Customization (no “x” under the Customized Access column). The settings under these headings work very similarly in their behavior as the corresponding setting values using pre-V5R2 Application Administration functions:

- Each function has a Default Access, All Object Access, and a Customized Access setting:

- Default Access: When selected, any user, by default, has access to the function. When unchecked, and no customization has been specified, by default, only users with All Object Access (assuming the All Object Access column is selected for this function) have access to Printer Session Configuration. If All Object Access is also not selected, and there is no customization, no user has access to this function.

You can select this function, clear either Default Access or All Object Access columns, and use the Customize button to explicitly deny or allow users and groups to access this function. We show an example of this in 3.5.1, “Managing Central Settings: Basic customization” on page 41.

- All Object Access: When selected, this means a user with all object authority (*ALLOBJ in 5250 command interface or all object access system privilege in iSeries Navigator interface), by default, has access to the function. If All Object Access has been specified (selected) a user with *ALLOBJ authority has access to the function, regardless of the Default Access setting or any optional customization.

If the current iSeries Navigator session user has at least security administration system privilege (*SECADM), they can use the Customize button functions.

- Customized Access: This means additional customization is done by clicking the Customize button and explicitly allowing or denying one or more users or groups access to the function.
- The same rules are used for both Local Settings and basic Central Settings when determining a user's access to a specific function. If you are denied access, the function might not appear or be unavailable on workstation windows that support the specific function.

- The only difference is that these settings can only be managed from the administration system.

3.5.1 Managing Central Settings: Basic customization

You might want to restrict one or more users from using an iSeries Access for Windows function specifically using the Central Settings. To do this, you must understand the Default Access and All Objects Access settings shown in Figure 3-9 on page 40 and described in the text following the figure.

In our example, we want to set some access restrictions on the iSeries Access for Windows GUI download function available under the Data Transfer function.

In Figure 3-10, we expanded **iSeries Access for Windows** → **Data Transfer** → **Download from Server** and selected **GUI Downloads**. We leave **Default Access** and **All Object Access** selected.

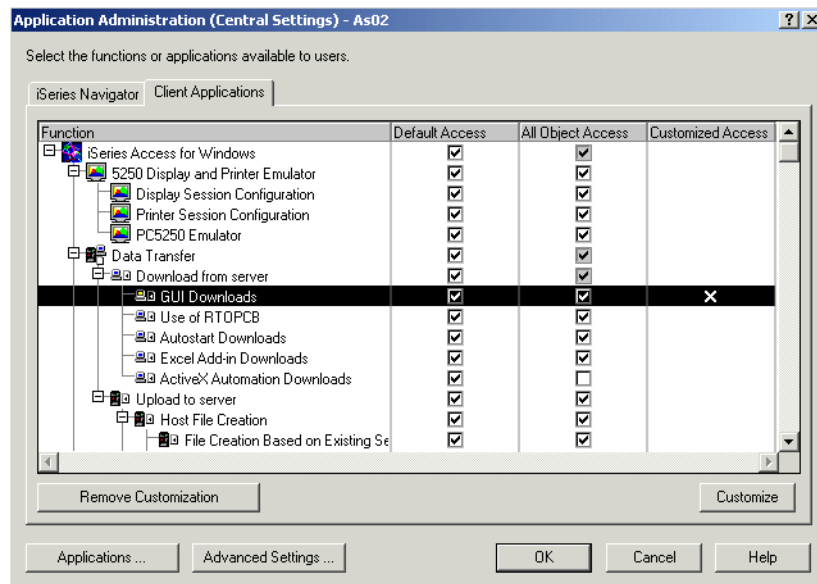


Figure 3-10 Client applications to be managed: Customized access example

As shown, all users, by default, have access to the GUI Downloads function unless they are “denied” using the Customize function. Click **Customize**, which opens the window shown in Figure 3-11 on page 42.

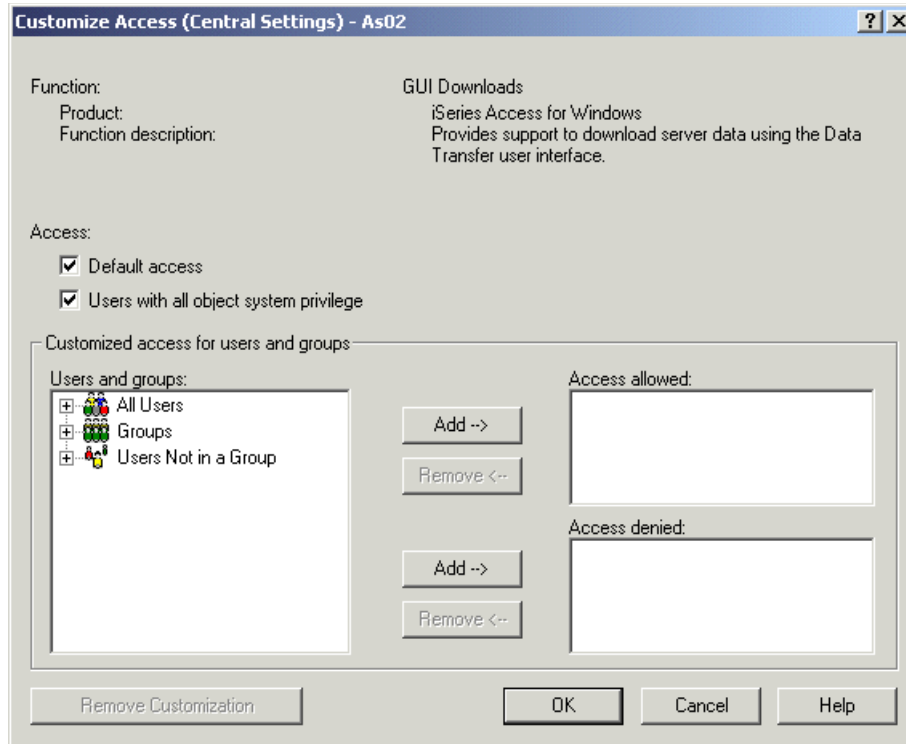


Figure 3-11 Customize Access: Basic

By expanding All Users, Groups, or Users Not in a Group, you get a list of users or groups within the expanded category. By selecting one or more of the users or groups, you can select the **Add** button next to the Access denied box. In our example, we expanded **All Users**, selected user **Anya**, and clicked the **Add** button next to Access denied box, as shown in Figure 3-12 on page 43.

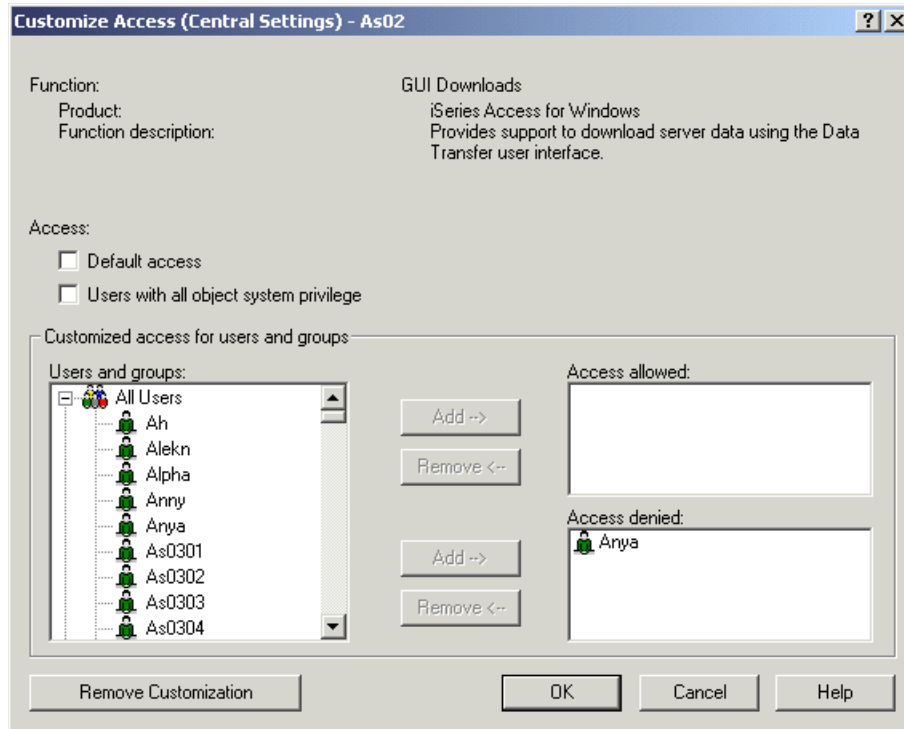


Figure 3-12 Customize Access: Basic

The user Anya is now restricted from using the Data Transfer GUI Downloads function of iSeries Access for Windows to all systems. With the Default Access and All Object Access settings both selected, there is no need to explicitly add a user or group to the Access allowed box.

If you cleared the Default Access setting and kept All Object Access selected, users without all object authority that you want to be able to use the GUI Downloads function would need to be added to the Access allowed box.

The settings take effect immediately, but the user still needs to discover the Central Settings, which is discussed in 3.6, “Client discovery of the administration system” on page 50.

3.5.2 Managing Central Settings: Advanced customization

There are advanced Central Settings. Using the window in Figure 3-10 on page 41 as a reference, click the **Advanced Settings** button to get the initial Application Administration (Central Settings) - Advanced window shown in Figure 3-13 on page 44.

The window includes the Connections, Passwords, Language, Service, and Environments tabs.

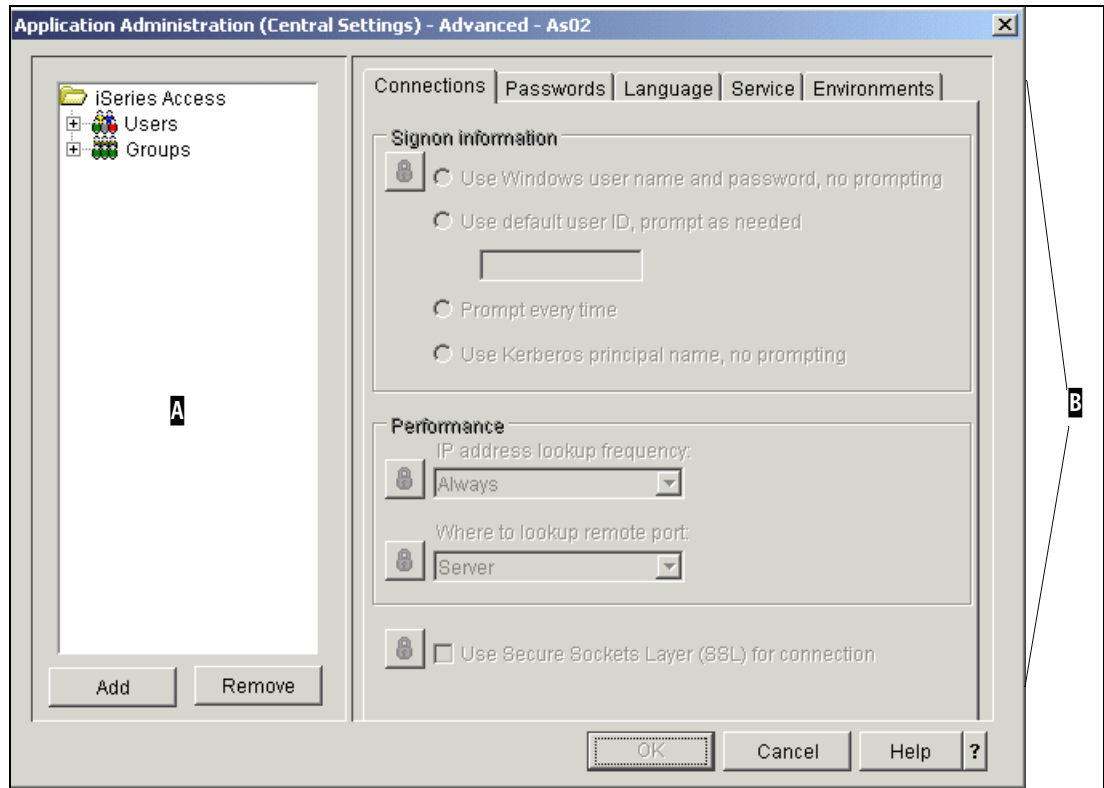


Figure 3-13 Managing Central Settings: Advanced

As shown, the parameters on the right side of this panel are not available, because on initial use of the Advanced Settings button, Advanced Settings are not yet specified. You also see only the Users and Groups folders that can be expanded to show a list users and groups for which advanced customization can be done.

The Connections panel displayed in Figure 3-13 is split into left and right sections.

- ▶ The list on the left (area **A**) contains the profiles that can have customized Advanced Central Settings defined. The following profile categories can have custom Advanced Settings defined:
 - Default User: The default user Advanced Settings are only used if a user does not have their own custom Advanced Settings and they do not belong to a group that has custom Advanced Settings.
 - Users: Each user profile on the system can have its own custom Advanced Settings.
 - Groups: Each group profile on the system can have its own custom Advanced Settings.
- ▶ The tabs on the right (area **B**) contain the custom advanced Central Settings for the profile currently selected in the left list area.

Important: The following rules are used to determine the custom Advanced Settings for a specific user:

- ▶ If the user has custom Advanced Settings, use them. Otherwise, continue.
- ▶ Check the user's groups (if any). Use the custom Advanced Settings for the first group that has them defined. If no group has custom Advanced Settings, continue.
- ▶ If Default User has custom Advanced Settings, use them. Otherwise, the user has no custom Advanced Settings.

On the initial Advanced Settings panel shown in Figure 3-13 on page 44, click **Add**, which opens the Application Administration Advanced Settings - Add Profile panel (shown in Figure 3-14). You can then either type in a profile name in the “User or group name” field, or expand one of the folders in the “Select one or more users or groups” field and select one or more entries in the expanded list. This enables the tabs and parameters on the right side of the Advanced panel. You are ready to define custom settings for the selected profile or profiles.

In our example, we already entered user profile Jeremys.

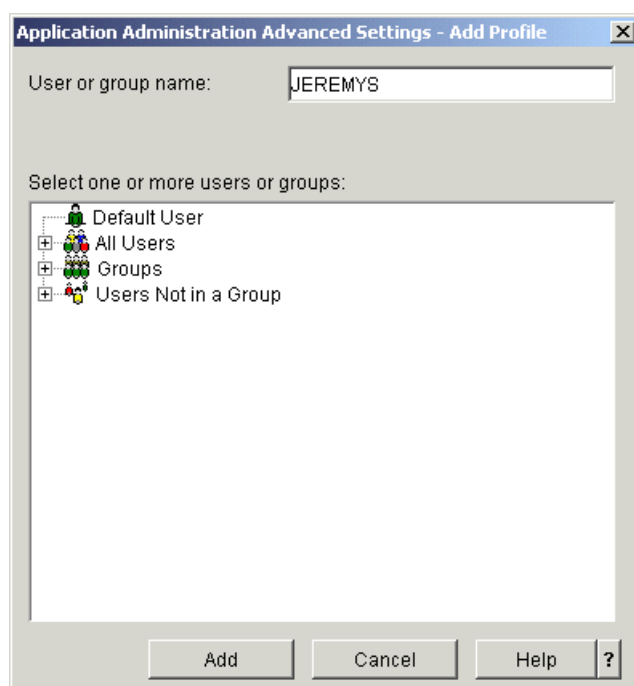


Figure 3-14 Advanced Settings: Add Profile

The following applies to the Application Administration Advanced Settings - Add Profile panel:

- ▶ Multiple profiles can be selected at once. When the Add button is clicked, all selected profiles will have default custom Advanced Settings created (and they will be added to the left side of the Applications Administration (Central Settings) - Advanced panel.
- ▶ The Application Administration Advanced Settings - Add Profile panel only displays those profiles that do not have custom Advanced Settings created. For example, if Default User has advanced custom settings, and the Add button is selected from left area of the panel (A) of the Applications Administration (Central Settings) - Advanced panel shown in Figure 3-13 on page 44, the Application Administration Advanced Settings - Add Profile panel will be presented, but it will not contain the “Default User.”

The advanced Central Settings can be either mandated or suggested by an administrator. Padlock icons next to a function represent either a mandated or suggested state. See “Mandated and suggested settings example” on page 46 for more information.

The padlock icons can be seen in Figure 3-15 on page 46.

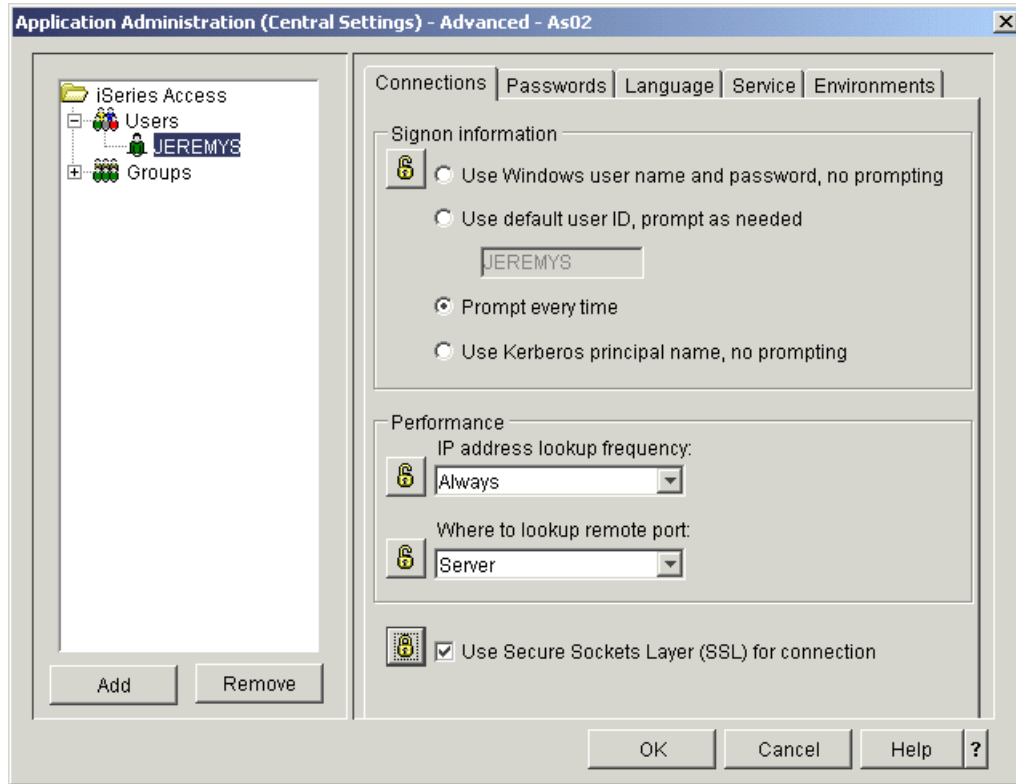


Figure 3-15 Connections tab

A locked padlock icon represents a status of mandated (see the SSL padlock). If a function has a status of mandated, this means that the system administrator has made the value of this function mandatory and unalterable; the system administrator defined the value of this function, and the client user cannot alter or override that value.

An unlocked padlock icon represents a status of suggested. If a function has a status of suggested, this means that the system administrator has made a suggestion as to what the value of a function should be; the system administrator defined the value of this function, but the client user can alter or override that value.

To remove the custom advanced Central Settings for a profile, select one or more profiles and then click the **Remove** button in the Applications Administration (Central Settings) - Advanced panel shown in Figure 3-13 on page 44.

Mandated and suggested settings example

The administrator indicates that a client user must use Secure Sockets Layer (SSL) when connecting to the server. If the administrator suggests that the client user use SSL, the client user can override the suggested value, and connect without using SSL. But, if the administrator mandates that the client user use SSL, all existing connections already defined on the client would be changed to use SSL. New connections would also use SSL, and the client user would not be able to override this value.

The Connections tab shown in Figure 3-15 allows an administrator to control several connection-related items of iSeries Access for Windows:

- Signon information: Allows an administrator to define how a user is chosen for an iSeries Access for Windows connection.

- **Performance:** Allows an administrator to control how the client connects to the server. You can specify how often the client should look up an iSeries server's IP address and where to look up the remote port.
- **SSL:** Allows an administrator to specify whether or not communication with the iSeries server is encrypted using Secure Sockets Layer (SSL).

The Passwords tab shown in Figure 3-16 allows an administrator to control several password-related items of iSeries Access for Windows:

- **Password expire warning:** Allows an administrator to specify whether or not to notify users before their passwords expire and the number of warning messages to send before the password expires. (This is the setting iSeries Access users see on their iSeries Access for Windows Properties panel, under the Passwords tab.)
- **Allow caching of server passwords:** Allows an administrator to specify whether or not passwords are stored internally. If you do not want users to be prompted for their password every time they sign on, select this option so that the system remembers their password. If you want users to be prompted for their password every time they sign on, do not select this option.
- **Allow all incoming remote commands when password caching is disabled:** Allows an administrator to specify whether or not to allow commands run from remote servers to be processed when password caching is disabled. When all incoming remote commands are allowed, users, or groups are able to run commands remotely.

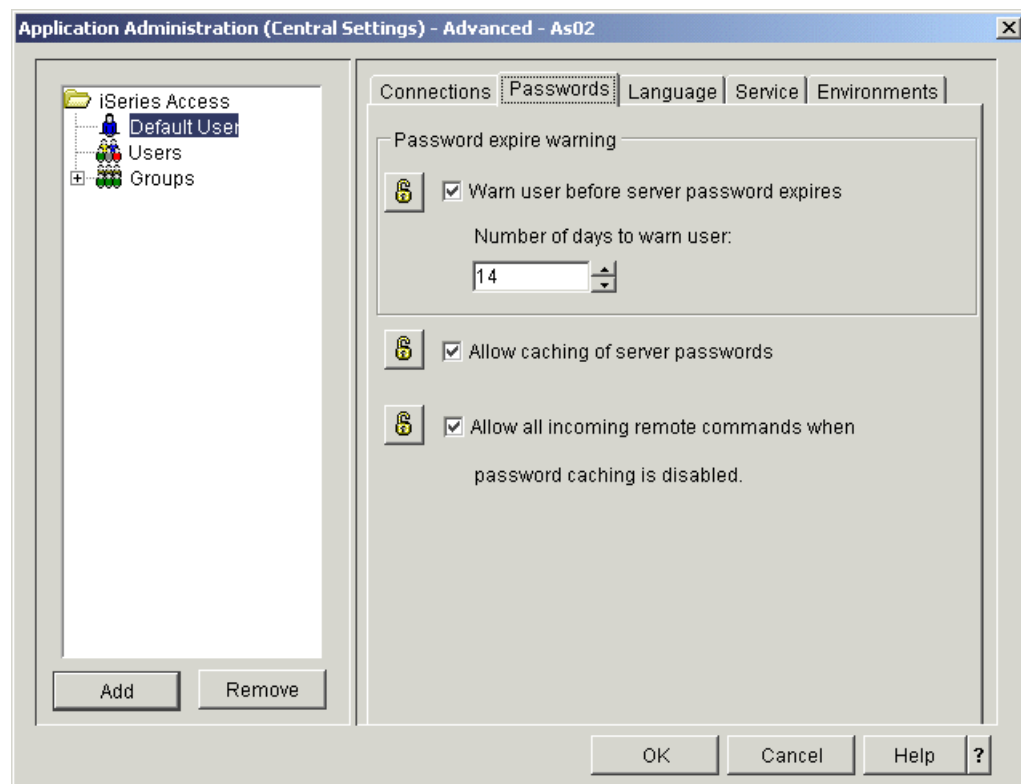


Figure 3-16 Passwords tab

The Language tab (not shown) allows an administrator to control several language related items of iSeries Access for Windows:

- ▶ Character conversion overrides: Allows you to specify the client code page and OS/400 coded character set identifier (CCSID) to be used for iSeries Access for Windows character conversions. Specified values override the current client code page or the associated server CCSID.
 - ANSI code page: Specifies the ANSI code page number from 0 to 65535 that should be used to override the current client ANSI code page. Type in a code page number or select Default from the list to instruct iSeries Access for Windows to use the client's default ANSI code page.
 - OEM code page: Specifies the original equipment manufacturer (OEM) code page number from 0 to 65535 that should be used to override the current client OEM code page. Type in a code page number or select Default from the list to instruct iSeries Access for Windows to use the client's default OEM code page.
 - EBCDIC code page: Specifies the extended binary-coded decimal interchange code (EBCDIC) coded character set identifier (CCSID) number from 0 to 65535 that should be used to override the current client EBCDIC CCSID. Type in a code page number or select Default from the list to instruct iSeries Access for Windows to use the client's default EBCDIC code page.
- ▶ Enable bidirectional script transformations: Some languages, such as Hebrew and Arabic, require bidirectional scripts. On the iSeries server, bidirectional scripts are typically stored in the visual form. On Windows platforms, bidirectional scripts are stored in the logical form. This option enables the transformation between the logical and visual forms.

Administrators can use the Service tab (not shown) to specify whether or not to start background service jobs automatically for specific profiles. A background service job can start in the background after high priority jobs complete. If you select this option, a background service job begins as soon as it reaches the top of the queue list and enough system resources are available. But, if there is a higher priority job in the queue, that job will start first.

An administrator can use the Environments tab to define one or more iSeries environments, each with a specified list of one or more server connections, that will be automatically downloaded to iSeries Access for Windows clients. Environments and server connections can only be defined as mandated, which means that the client cannot modify them after they've been downloaded to the client's PC. The administrator can also indicate whether clients are allowed to add connections to each environment or define additional environments.

In Figure 3-17 on page 49, we provide additional details about the Environments settings.

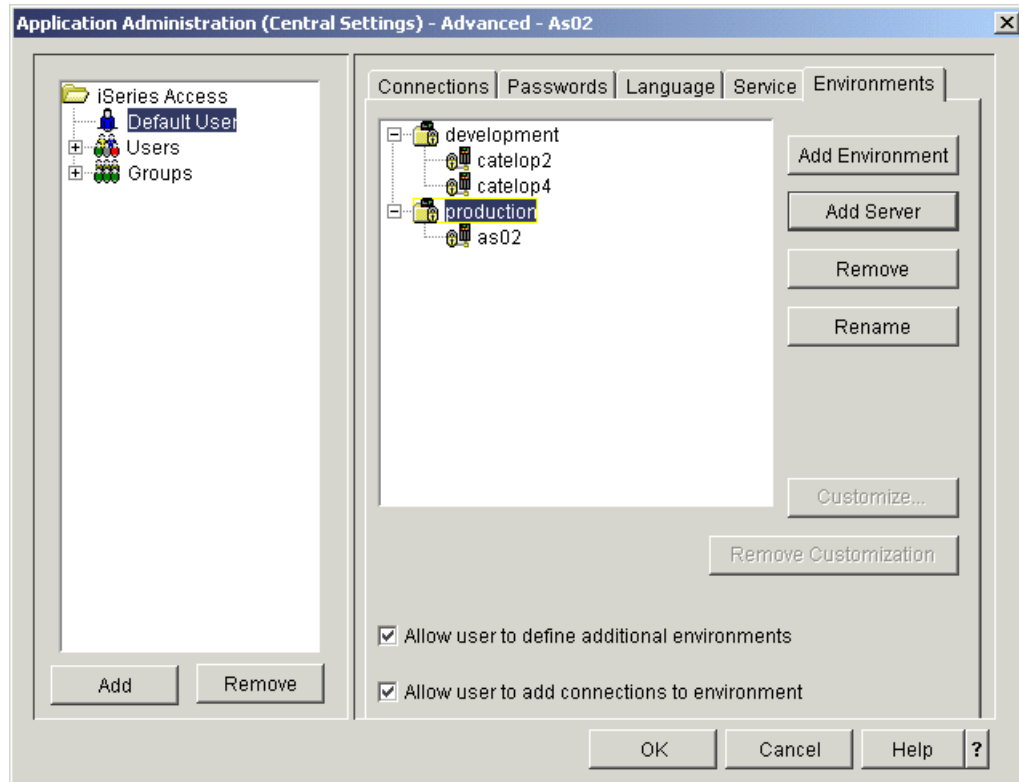


Figure 3-17 Environments tab

The Environments tab contains the following settings:

- ▶ **Add Environment:** Adds an environment to the list of environments. An administrator can use this button to define an environment that is downloaded automatically to clients.
- ▶ **Add Server:** Adds a system to the current environment (either the selected environment or the environment of the selected server). This button is available only when a server or an environment is selected.
- ▶ **Remove:** Deletes an environment or server. This button is available only when a server or an environment is selected.
- ▶ **Rename:** Changes the name of an environment or server. This button is available only when a server or an environment is selected.
- ▶ **Allow user to define additional environments:** Specifies whether or not users can add environments to their list of connections. An environment is a network of servers. If this is not selected, users must use the environments that the system administrator provides for their user name or the group to which they belong. If this is selected, users can add environments to their list of connections.
- ▶ **Allow user to add connections to environment:** Specifies whether or not users can add a specific OS/400 connection to an environment they have access to. An environment is a network of servers. If this option is selected, users are able to add servers to an environment. When a user adds a connection, it is added to the environment only on their own PC. The additional connection does not affect other users that use the same environment. If this option is not selected, users are not able to add servers to their environment. They must use the servers that are predefined for that environment.

When an administrator adds a server connection (with the Add Server button) on the Environments tab, it is initially set up as a non-customized connection. This means that the connection will use the connection properties as defined on the Connections tab.

To provide different connection properties for a specific server, use the Customize button. To perform this customization, select a server (As02 in our example). This enables the Customize button, as shown in Figure 3-18. Click **Customize**, which opens the Environments - Customize panel also shown in Figure 3-18.

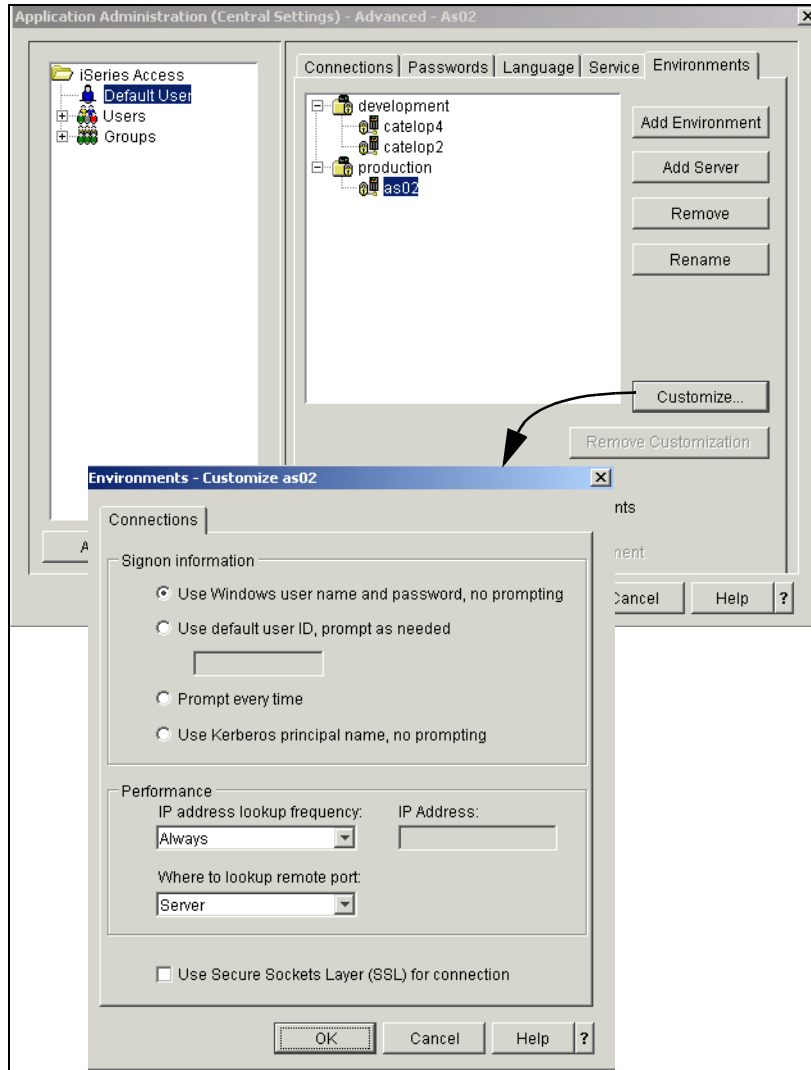


Figure 3-18 Advanced Settings: User system customization

On this panel, you can modify the connection properties for the server. The values on the Environments - Customize panel are always mandated (that is, a user cannot modify them after they've been downloaded to their PC from the administration system).

3.6 Client discovery of the administration system

After an administrator has configured an iSeries to be an administration system, and then registered and set up the Central Settings, the client PC (any PC with V5R2 or later iSeries Access for Windows installed) must still “discover” the administration system and use it to download its settings. The administration system that a client PC user uses as the source of its Central Settings is called the *current administration system* of the PC user.

This client “discovery” of its current administration system can be done in any of the following ways:

- ▶ Manual selection of the current administration system by the client PC user.
- ▶ By signing on with iSeries Navigator to an administration system that can administer the current user (as long as the current PC user does not already have a current administration system defined).
- ▶ By installing from an iSeries Access for Windows image that has an initial current administration system defined.

Restriction: If you do not have Service Pack SI09809 or later installed, the *only* supported way for the client to discover the administration system and the Central Settings is the manual selection method, as described in 3.6.1, “Administration system discovery: Manual” on page 52. Install the service pack to remove this restriction.

From the client PC user's perspective, the Central Settings are downloaded from the user's current administration system using the current administration user. These values can be viewed from the Administration System tab in iSeries Access for Windows Properties window, as shown in Figure 3-19 on page 52. To get to this tab:

1. Select **Start** from the Windows task bar.
2. Select **Programs** → **IBM iSeries Access for Windows** → **iSeries Access for Windows Properties** to launch iSeries Access properties panels.
3. Select the Administration System tab.

The Administration System tab, shown in Figure 3-19 on page 52, displays information about the current client workstation user's administration system:

- ▶ **Current administration system:** Indicates the administration system, if any, from which the current PC user is obtaining its Central Settings.
- ▶ **Current administration user:** Indicates the user profile used, if any, to obtain the Central Settings from the current administration system.
- ▶ **Scan frequency:** Indicates how frequently the client PC downloads the Central Settings from the current administration system.
- ▶ **Scan Settings Now:** This button causes the client PC to download the Central Settings from the current administration system for the current administration user.
- ▶ **Available administration systems and users:** This list will contain the administration systems and users that the client has signed on to that are configured as administration systems that will administer the user. Each time a user signs on from iSeries Navigator to an administration system that administers the user, that system and user pair will be added to this list (if it doesn't already exist). A user can manually add or remove a system/user pair from this list by using the Add and Remove buttons. In order to add a system/user pair to this list, the system must be configured as an administration system, and the system must be configured to administer the user profile; otherwise, an error will occur and the Add request will fail.

Note: A signed-on user cannot remove the currently active administration system/ user pair.

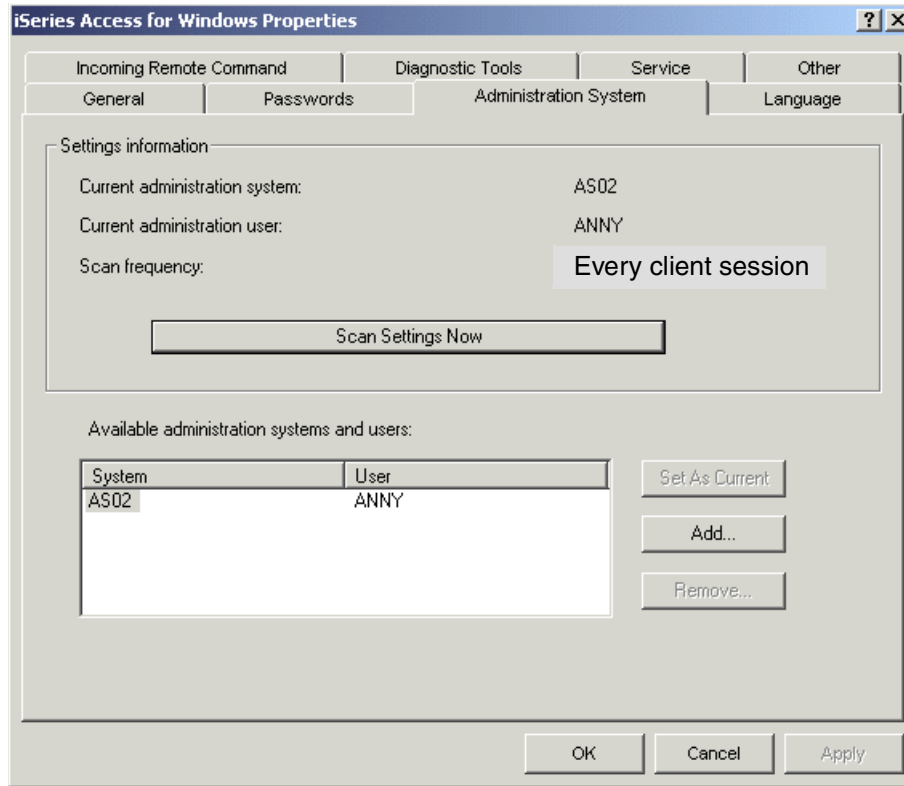


Figure 3-19 Administration System tab

3.6.1 Administration system discovery: Manual

The manual mechanism was designed to allow a client user to set their own current administration system/user, as long as an administrator had already defined the system as an administration system that administers the given user.

This can be done by selecting an administration system/user pair in the Available administration systems and users list on the Administration System page of the iSeries Access properties sheet and clicking the **Set as Current** button.

3.6.2 Administration system discovery: Signon

Another way of having a client discover its administration system is through signon. This mechanism was designed to allow an administrator to set up an administration system and then have clients “automatically” start using it as their current administration system the first time they connect to it (assuming that the client does not already have a current administration system/user defined).

When a user signs on to an iSeries in iSeries Navigator, the system is checked to determine if it is an administration system that is administering the currently signed-on user. If so, the administration system and user pair will be added to the “Available administration systems and users” list on Administration System properties tab displayed in Figure 3-19. If no current administration system/user pair are currently set, this system/user pair will also be set as the Current administration system/user on the Administration System properties tab displayed in Figure 3-19.

3.6.3 Administration system discovery: Install

The install mechanism allows an administrator to define the administration system (but not user) in an iSeries Access for Windows install image.

If a client PC installs using this image, the client PC will begin to use the administration system as its current administration system. The first time the client PC attempts to download the Central Settings from this system, the client PC user will have to specify a user, which will then be used as the current administration user.

The install image can be modified from iSeries Navigator by displaying the Administration System properties tab for an iSeries properties:

1. From iSeries Navigator, select an iSeries and right-click. Select **Properties**.
2. Select the Administration System tab after the Properties window opens. This opens the panel shown in Figure 3-20.

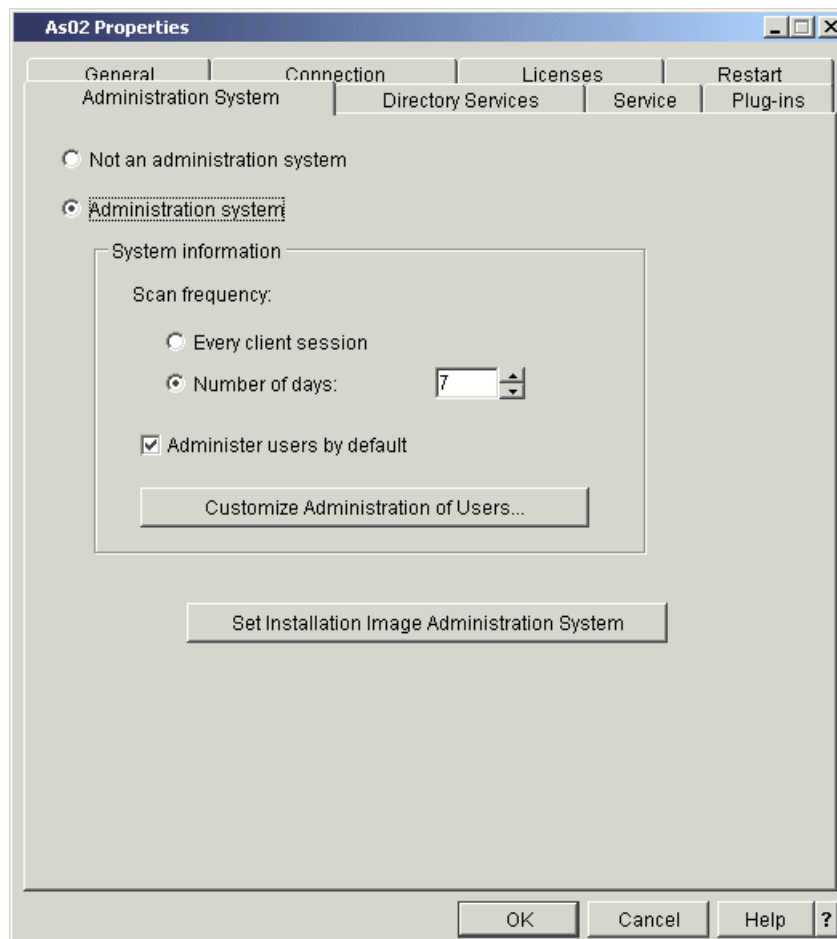


Figure 3-20 Administration System tab

3. To alter the install image, click the **Set Installation Image Administration System** button.

Tip: The Set Installation Image Administration System button can be used to alter install images on iSeries that are *not* configured as administration systems.

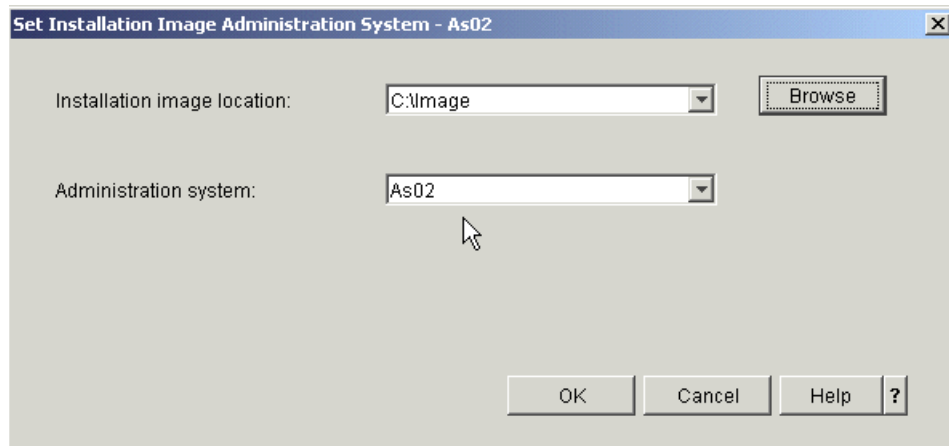


Figure 3-21 Installation image: Non-iSeries

4. In the Set Installation Image Administration System panel displayed in Figure 3-21, you can modify an install image so that it contains an administration system that is used by all clients that install using that image:
 - Installation image location: This is the location of the install image to be modified. If the current iSeries system is selected, the iSeries Access for Windows install image on that iSeries will be modified. Otherwise, click **Browse** to select any other install image.
 - Administration system: This is the name of the administration system that is to be stored in the install image.

This completes the setting up and using V5R2 Application Administration Central Settings.



Secure Sockets Layer (SSL)

This chapter describes the following topics:

- ▶ Securing OS/400 servers with SSL server authentication
- ▶ Client authentication
- ▶ Configuring iSeries Access for Windows to use SSL

4.1 Introduction

Secure Sockets Layer (SSL) is a popular security method that allows the PC client to authenticate the server and encrypt all data and requests. Use it when transferring sensitive data between systems. The transfers of credit card and bank statement information are examples of client/server transactions that typically take advantage of SSL. There is an increased cost in performance with SSL because of the added encryption and decryption processing.

iSeries Access for Windows includes optionally-installable support for Secure Sockets Layer (SSL) and a way to manage key databases with IBM Key Management. All functions of iSeries Access for Windows can communicate over SSL except Incoming Remote Command and Ultimedia. However, on a PC using an Intel® 64-bit processor, such as Itanium, only 32-bit applications and connections can use SSL. iSeries Access for Windows allows SSL communications with the iSeries server at the 128-bit level of encryption.

Beginning with Client Access Express for Windows (V5R1M0), SSL client authentication is also available for PC5250.

There are two ways that Secure Sockets Layer (SSL) verifies identification: client authentication and server authentication. Server authentication occurs when the client verifies the identity of the server application based on the server certificate passed down to the client application. Client authentication occurs when the server verifies the identity of the client based upon the client certificate passed up to the server application. If client authentication is performed, server authentication is always done first.

Important: Certificates, key databases, and key database passwords

Certificates are used by SSL to implement much of the encryption/decryption and validation work. These certificates used by SSL are stored in *key databases* (sometimes called *key stores*). There can be several different key databases on each platform (PC, iSeries, and so on). These databases are usually protected by a password.

It is very important to have SSL certificates under key database password control on iSeries, because data inside each certificate makes it possible for SSL to establish trust and validation for each connection. It is also very important to track and understand when the certificates you are using will expire, so you can renew them ahead of time. Failures can occur if you use an expired certificate.

To view and renew your configured certificates, use Digital Certificate Manager interfaces. We place a short example of how to view the expiration of a certificate authority (CA) certificate at the end of this chapter in 4.6, “Viewing a certificate authority certificate” on page 91. If you are using digital certificates for the first time, you need to review this entire chapter first before using the instructions in 4.6, “Viewing a certificate authority certificate” on page 91.

Throughout this chapter, certificate types and names, the name of the key database containing the certificates, and key database passwords are important parameters that must be known to create and manage certificates.

4.1.1 iSeries Access for Windows SSL utility program

Throughout this chapter, we use normal iSeries components, such as the OS/400 Digital Certificate Manager (DCM) browser interface and iSeries Access for Windows component interfaces, to set up and manage the SSL with iSeries Access for Windows functions.

However, you should be aware of an advanced SSL setup and management tool that is included with iSeries Access for Windows V5R2 and Client Access for Windows V5R1 for use in more advanced scenarios. You can discuss using this tool with your IBM @server iSeries Support Personnel after you become proficient with the interfaces described in this chapter.

Although complete coverage of this tool is beyond the scope of this book, we provide a short summary of its capabilities here.

The SSL utility program, `cwbcossl.exe`, is shipped with iSeries Access for Windows in the main installation directory. This program is an advanced SSL configuration tool that provides the following functions:

- ▶ Download iSeries CA certificates
- ▶ Import external CA certificates
- ▶ Start and launch iSeries Digital Certificate Manager
- ▶ Launch IBM Key Management for both Java™ and PC SSL key databases
- ▶ Verify SSL connections
- ▶ Verify iSeries SSL software requirements
- ▶ Rebuild the Java key database for iSeries Navigator
- ▶ Launch the iSeries Access for Windows SSL properties

You can find this program in the directory path shown in Figure 4-1.

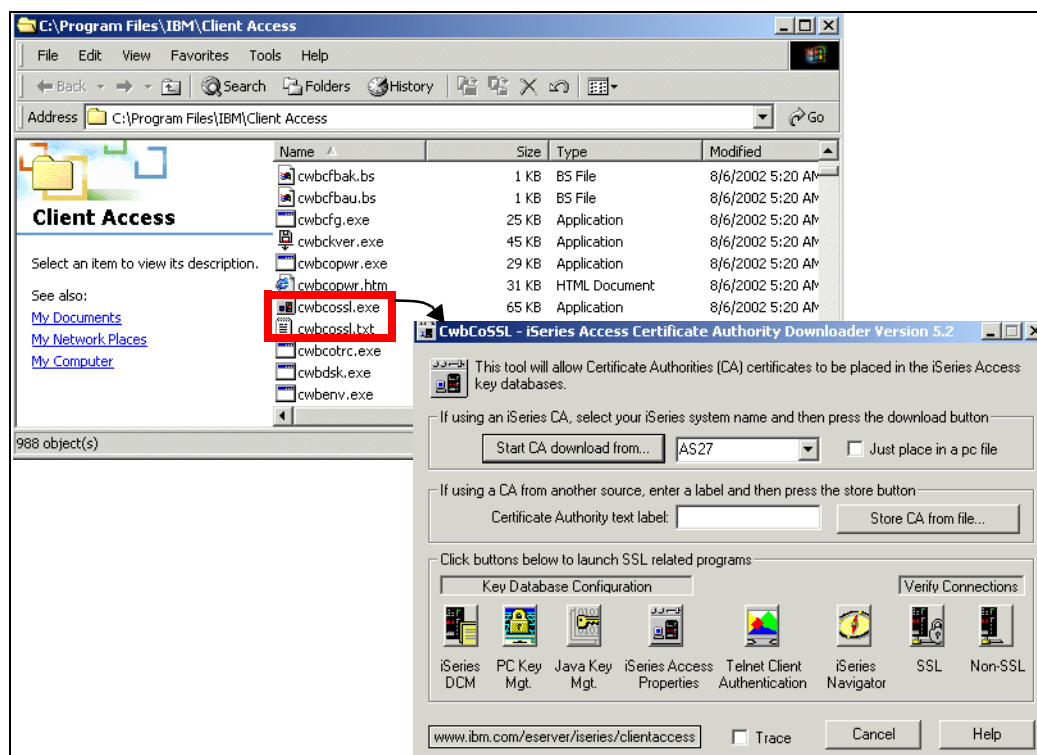


Figure 4-1 iSeries Access for Windows SSL utility program

Double-click `cwbcossl.exe` to get the first panel shown in Figure 4-1. For more help and features available with the `cwbcossl` program, click its **Help** button.

We do not use this program in this redbook.

4.2 SSL prerequisites

The following are the SSL software prerequisites on the iSeries:

- ▶ IBM Digital Certificate Manager (DCM), option 34 of OS/400 (5722-SS1).
- ▶ TCP/IP Connectivity Utilities for iSeries (5722-TC1).
- ▶ IBM HTTP Server for iSeries (5722-DG1). If you are trying to use the HTTP server to use the DCM, be sure you have the IBM Developer Kit for Java (5722-JV1) installed. By default on the iSeries, this product provides the iSeries HTTP Administration Server, which has a link to the Digital Certificate Manager from the administration server's initial page.

If you need to start this administration server, enter the following Start TCP Server command from a 5250 session:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

- ▶ The IBM Cryptographic Access Provider product, 5722-AC3 (128-bit). The bit size for this product indicates the maximum size of the secret material within the symmetric keys that can be used in cryptographic operations. The size allowed for a symmetric key is controlled by the export and import laws of each country. A higher bit size results in a more secure connection.
- ▶ Client Encryption product, 5722-CE3 (128-bit). iSeries Access for Windows needs this product in order to establish the secure connection.

4.3 Server authentication

This section describes how to create a system certificate and assign the system certificate to the Telnet and host server applications.

4.3.1 Creating the system certificate

The Digital Certificate Manager (DCM) is used to create the system certificate that will be used for SSL authentication.

To create a system certificate:

1. Access the DCM through the HTTP administration instance, enter the following URL in a Web browser:

```
http://systemname:2001
```

This should prompt you to sign on to your iSeries system as shown in Figure 4-2 on page 59. If the DCM server has not been started on the iSeries, use a 5250 session to issue the Start TCP Servers command to start it:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

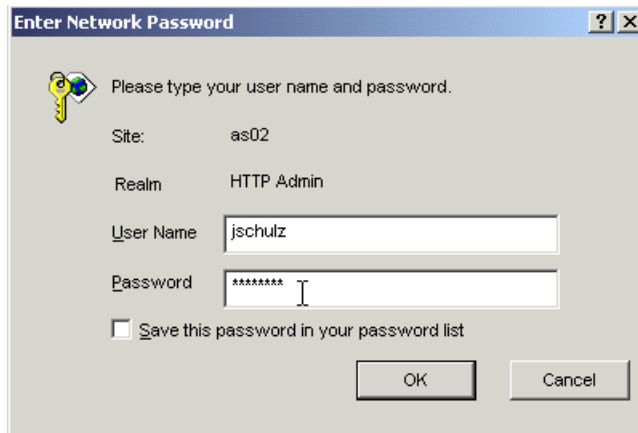



Figure 4-2 User name and password prompt accessing the HTTP administration instance

2. Enter a valid OS/400 user name and password and click **OK**. This should result in a connection to the HTTP administration server instance, which brings up the page shown in Figure 4-3.

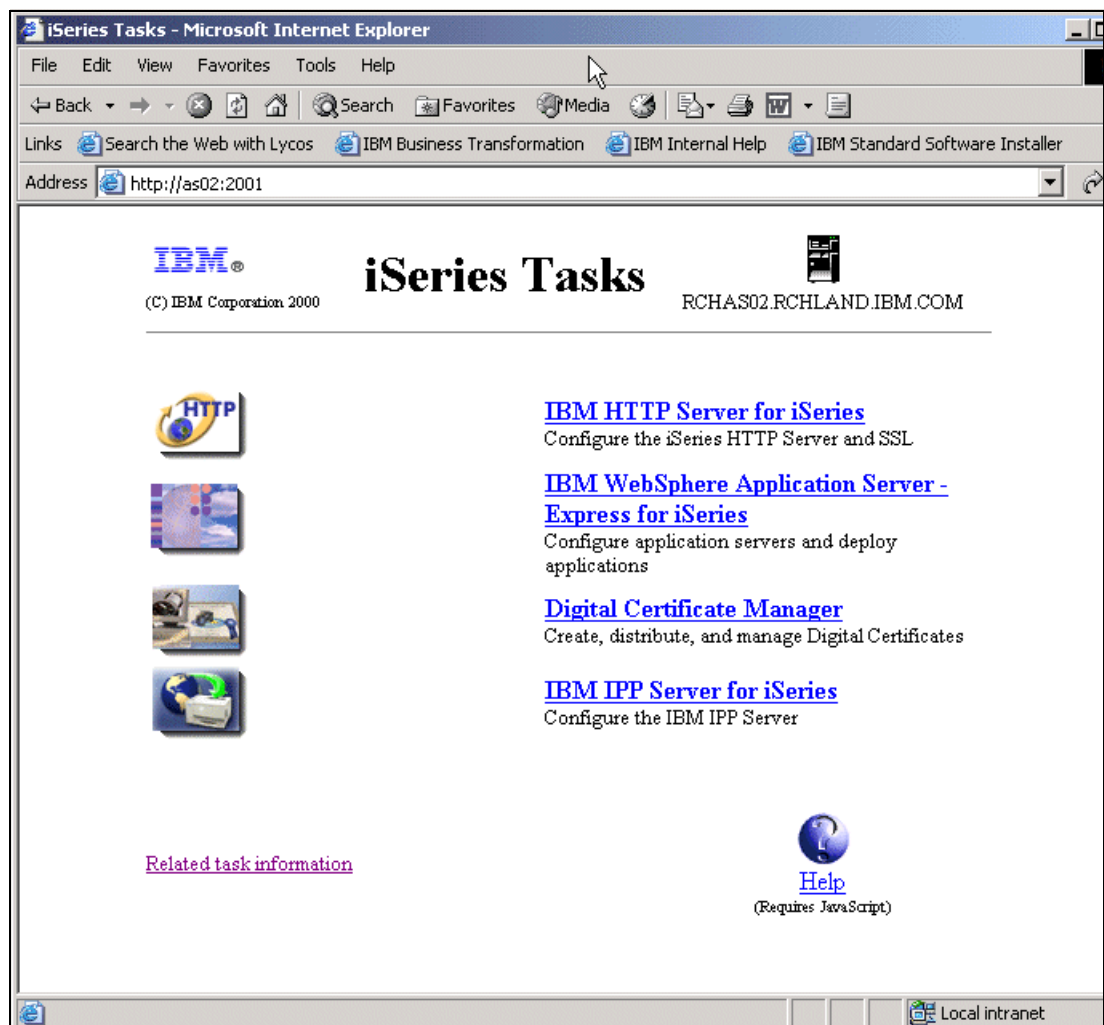


Figure 4-3 HTTP administration server instance

3. Select the **Digital Certificate Manager** link, which will result in access to the Digital Certificate Manager, as shown in Figure 4-4.



Figure 4-4 Digital Certificate Manager

4.3.2 Certificate authority (CA)

A certificate authority (CA) is a trusted central administrative entity that can issue digital certificates to users (to be used for client authentication) and servers. The trust in the CA is the foundation of trust in the certificate as a valid credential. A CA uses its private key to create a digital signature on the certificate that it issues to validate the certificate's origin. Others can use the CA certificate's public key to verify the authenticity of the certificates that the CA issues and signs.

A CA can be either a public commercial entity, such as VeriSign, or it can be a private entity that an organization operates for internal purposes. Several businesses provide commercial certificate authority services for Internet users. With OS/400 Digital Certificate Manager (DCM), you can manage certificates from both public and private CAs.

You can also use DCM to operate your own private CA to issue private certificates to systems and users. When the CA issues a user certificate, DCM automatically associates the certificate with the user's iSeries system user profile. This ensures that the access and authorization privileges for the certificate are the same as those for the owner's user profile.

Trusted root status

The term trusted root refers to a special designation that is given to a certificate authority certificate. This trusted root designation allows a browser or other application to authenticate and accept certificates that the certificate authority (CA) issues.

When you download a certificate authority's certificate into your browser, the browser allows you to designate it as a trusted root. Other applications that support using certificates must also be configured to trust a CA before the application can authenticate and trust certificates that a specific CA issues.

You can use DCM to enable or disable the trust status for a certificate authority (CA) certificate in the certificate store. When you enable a CA certificate, you can specify that applications can use it to authenticate and accept certificates that the CA issues. When you disable a CA certificate, you cannot specify that applications can use it to authenticate and accept certificates that the CA issues.

To enable the trust status:

1. Select **Create a Certificate Authority (CA)** from the Digital Certificate Manager.

Note: You will not see Create a Certificate Authority (CA) link within Digital Certificate Manager if you have already created a certificate authority.

Figure 4-5 Create a CA

2. Fill out the required data fields, and click **Continue**. This opens the page shown in Figure 4-6 on page 62, which can also be accessed directly if you already have a CA by clicking the **Install Local CA Certificate** link.



Figure 4-6 Install Local CA Certificate

3. Click **Continue**.



Figure 4-7 CA Policy Data

4. Set the value for Allow creation of user certificates to Yes or No. If you are only going to implement server authentication, you will want this set to No. Click **Continue**.

Important: User certificates are used for client authentication. If you are going to implement client authentication, set Allow creation of user certificates to **Yes**. See also 4.4, “Client authentication” on page 66.



Figure 4-8 Policy Data Accepted

5. Select **Continue**. This creates a system store and then creates a system certificate, signed by the local CA.

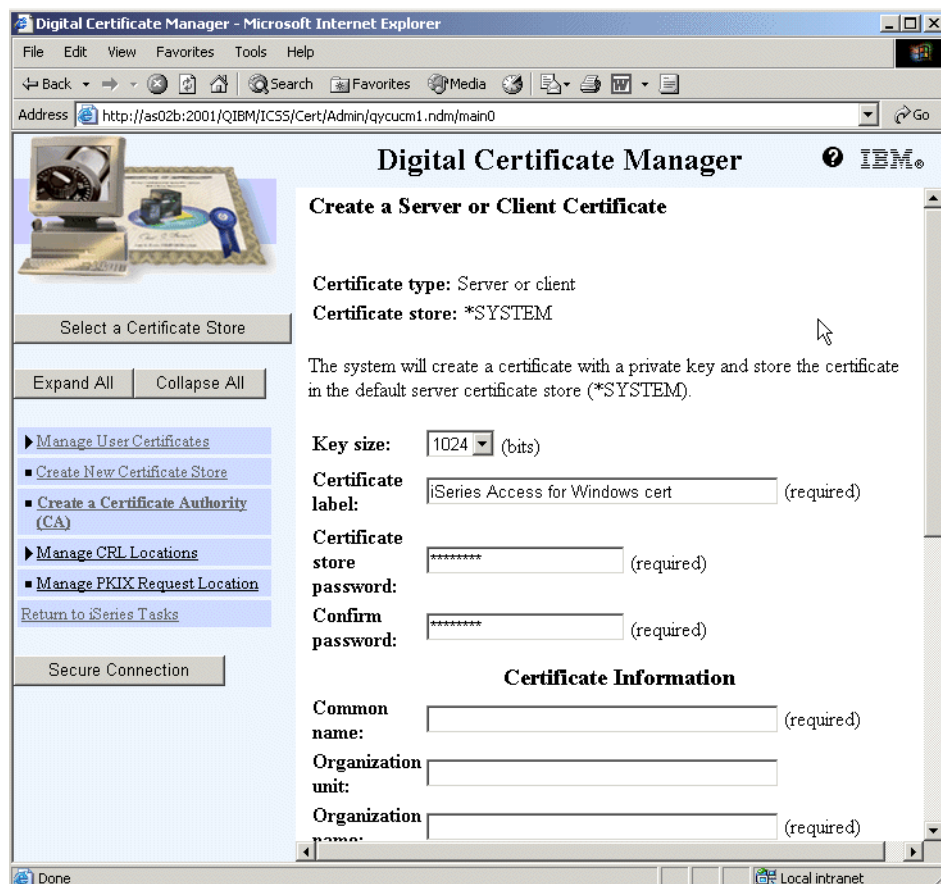


Figure 4-9 Creating a certificate

6. Fill in the required fields: Certificate label, Certificate store password values, and Common name. Placing a character string representing the local system name somewhere in the common name helps identify this certificate later when looking at multiple certificates.

7. Click **Continue** (not shown in our figure). In the next page, you can assign your certificate to the iSeries applications of your choice.

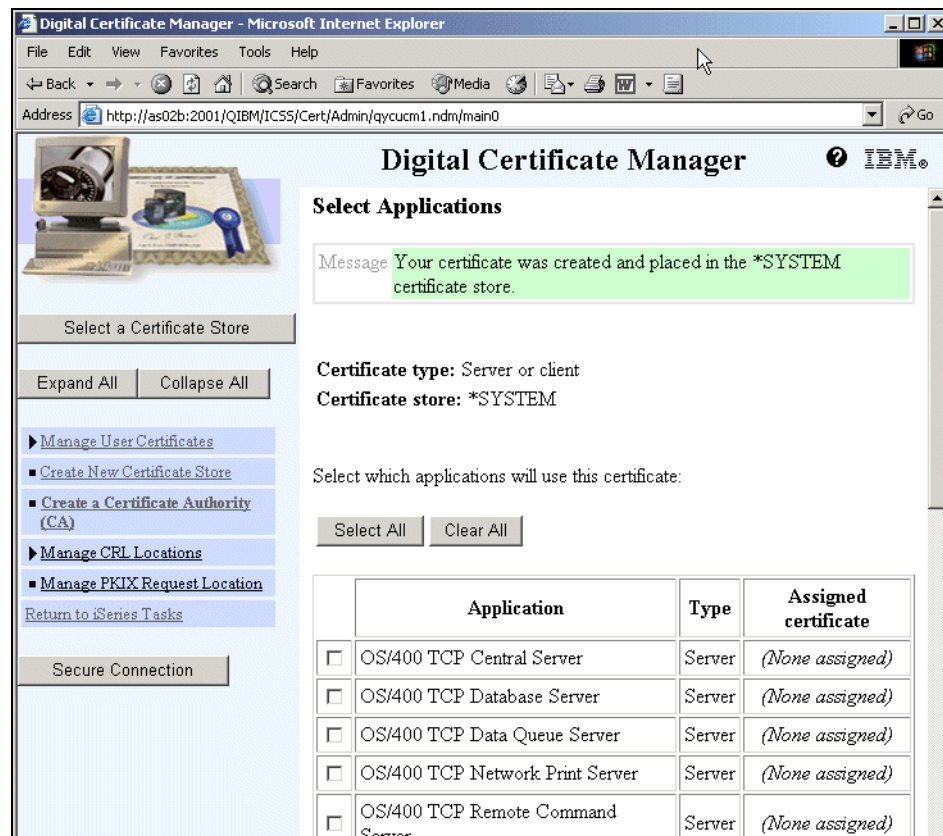


Figure 4-10 Selecting applications to use a certificate: 1 of 2

8. Select the applications to which you want to assign the certificate and then click **Continue**. If you are securing PC5250 emulation, you assign the certificate to the Telnet Server, Central Server, and Signon Server. In Figure 4-11, all of the servers used by iSeries Access for Windows and iSeries Navigator have been secured with the exception of the Management Central Server.

<input checked="" type="checkbox"/>	OS/400 TCP Central Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Database Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Data Queue Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Network Print Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Remote Command Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Signon Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP/IP Telnet Server	Server	(None assigned)
<input type="checkbox"/>	OS/400 DDM/DRDA Server - TCP/IP	Server	(None assigned)
<input type="checkbox"/>	OS/400 Cluster Security	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 - Host Servers	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP File Server	Server	(None assigned)
<input type="checkbox"/>	AS/400 Management Central Server	Server	(None assigned)

Figure 4-11 iSeries Access for Windows applications

Note: In this example, we are not securing the Management Central Server. Setting up Management Central to use SSL between its central system and target endpoint systems requires steps in addition to those covered in this redbook. For detailed information regarding SSL and Management Central, refer to the Information Center:

<http://publib.boulder.ibm.com/series/v5r2/ic2924/index.htm>

Select **Security** → **Secure Sockets Layer (SSL)** → **SSL Scenarios** → **Scenario: Secure Management Central with SSL**.

9. Scroll down the window shown in Figure 4-10 on page 64 and select the **OS/400 TCP/IP Telnet Server** (as shown in Figure 4-12) to include this CA in its CA trust list. This is done only for client authentication.

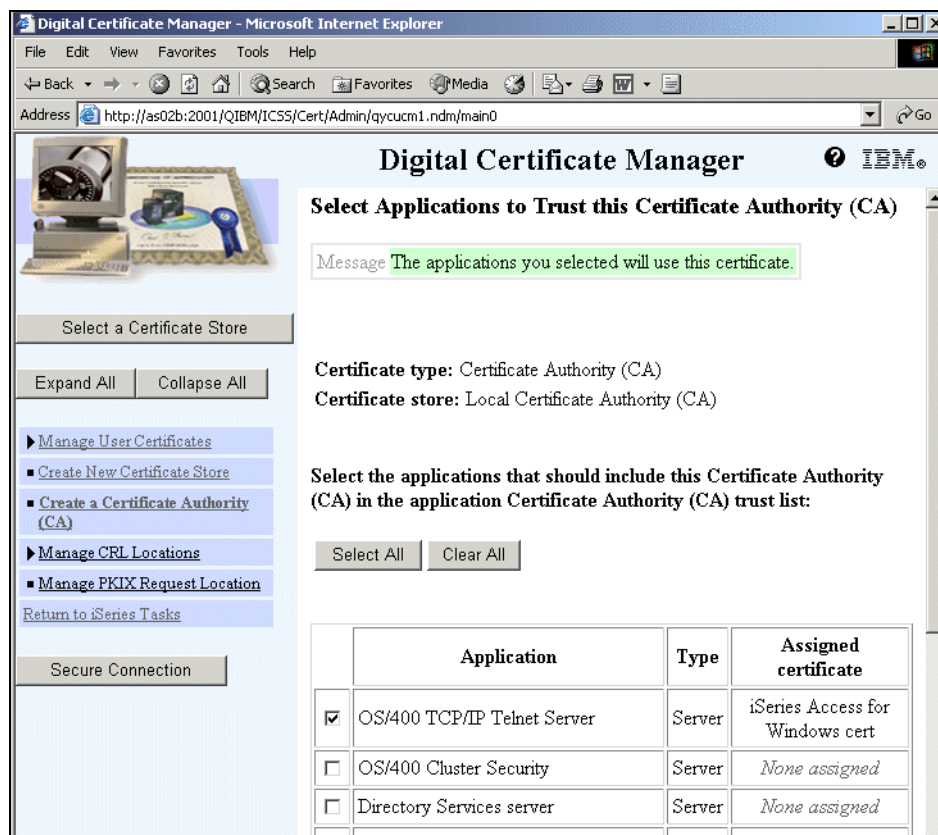


Figure 4-12 Selecting applications to use a certificate: 2 of 2

10. Click **Continue** (not shown) to get a summary (Application Status) page, as shown in Figure 4-13 on page 66.

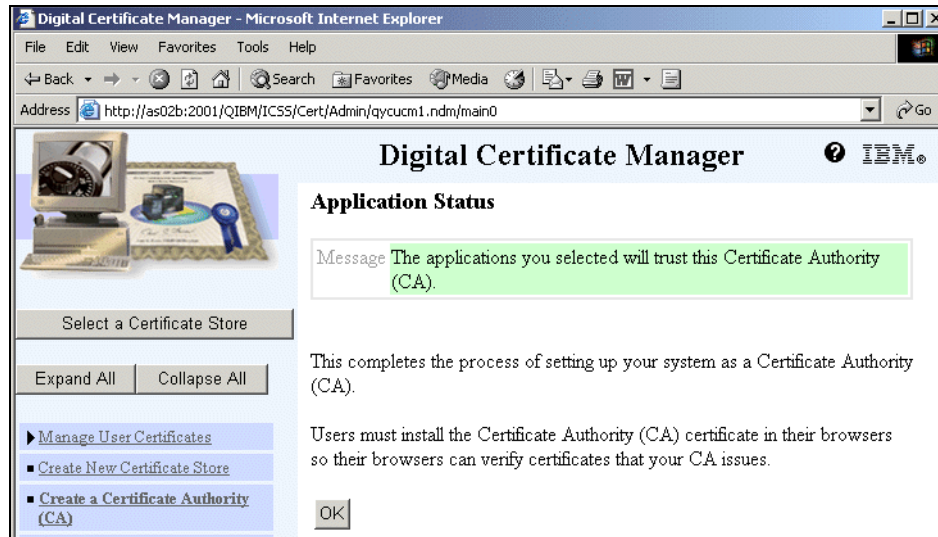


Figure 4-13 Application Status

11. Select **OK**.

You have configured your selected applications to use SSL. You will need to end and restart the Telnet server and host servers on the iSeries system. You need to schedule this end and start, because ending these servers will abnormally end any jobs active that are using these servers.

For the Telnet server, enter the following in a 5250 session or in a schedule submitted job:

```
ENDTCPSVR SERVER(*TELNET), STRTCPSVR SERVER(*TELNET)
```

For host servers, enter the following in a 5250 session or in a schedule submitted job:

```
ENDSTRHOSTSVR SERVER(*ALL), STRHOSTSVR SERVER(*ALL)
```

After restarting the servers, you can verify that they are listening on their assigned SSL ports by issuing the following command from a 5250 session:

```
netstat *cnn
```

On the Work with TCP/IP Connection Status screen (not shown), use PF14 to display the port numbers. Page down. You should see port 992 for Telnet and ports 9470-9476 all listening, depending on which applications you secured.

If you are planning to use server authentication only, the server configuration is complete.

You can continue with the client configuration, as described in 4.5, "Configuring iSeries Access for Windows to use SSL" on page 84.

4.4 Client authentication

There are two ways that Secure Sockets Layer (SSL) verifies identification: client authentication and server authentication. Server authentication occurs when the client verifies the identity of the server application by the server certificate passed down to the client application. Client authentication occurs when the server verifies the identity of the client by the client certificate passed up to the server application. If client authentication is performed, server authentication is always done first.

Important: If the iSeries is used to create client certificates, a browser capable of importing/exporting secure PKCS12 files is required. (Currently Microsoft Internet Explorer 5.x and Netscape 4.x or later have this capability.) After the client certificate is created, you need to export it from the browser and import it into the PC SSL key database using IBM Key Management.

You can select IBM Key Management on your client workstation on the panel that appears after double-clicking the IBM iSeries Access for Windows shortcut on your desktop.

When exporting client certificates from the browser, always include the private key, as described in , “Internet Explorer: Exporting the user certificate” on page 74 and , “Netscape Communicator: Exporting the user certificate” on page 78.

The certificate authority that signed/created the client certificate needs to be imported into the PC SSL key database before the actual client certificate, or else the PC SSL key database will not be able to trust the client certificate and fail to import it. If more than one valid client certificate is in the PC SSL key database, you can either use IBM Key Management to change the default client certificate, or use the PC5250 configuration properties to allow selecting which one to use during a connection attempt.

Note: Any valid client certificate will work. There is no need to choose one.

4.4.1 Creating a user certificate for client authentication

Section 4.3, “Server authentication” on page 58 describes the configuration of server authentication that needs to be completed prior to the creation of user certificates.

To create a user certificate for client authentication:

1. The first step in creating a user certificate is to ensure that your certificate authority (CA) allows the creation of user certificates. This can be checked in the Digital Certificate Manager within the administrative HTTP server instance running on your iSeries system. Access the HTTP administration instance by typing the following in a Web browser:
`http:systemname:2001`
If the DCM is not started, using a 5250 session, try to start it by entering:
`STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`
2. Sign on with a valid OS/400 user ID and password and select **OK**. Select the **Digital Certificate Manager** link, which opens the Digital Certificate Manager page, as shown in Figure 4-4 on page 60.
3. Select the **Select a Certificate Store** button, which opens the page shown in Figure 4-14 on page 68.

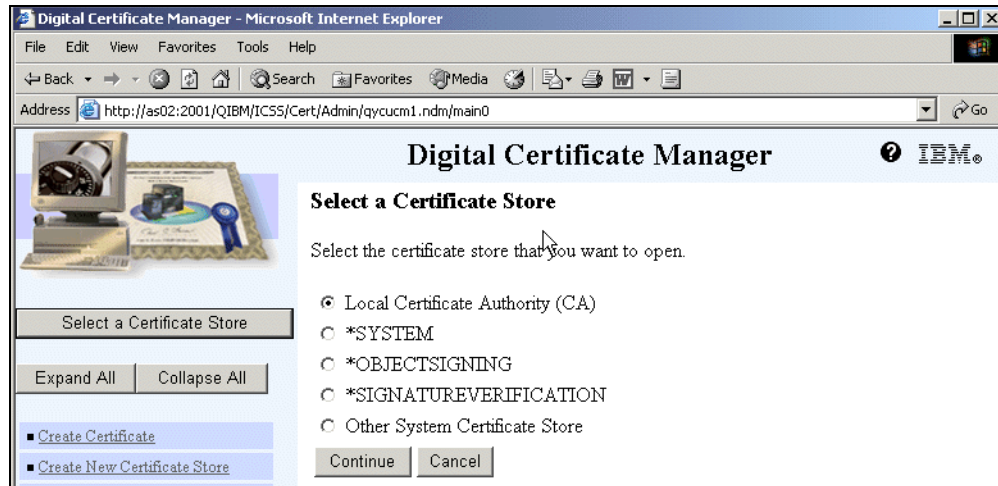


Figure 4-14 Select a Certificate Store

4. Select the **Local Certificate Authority (CA)** radio button, and click **Continue**.

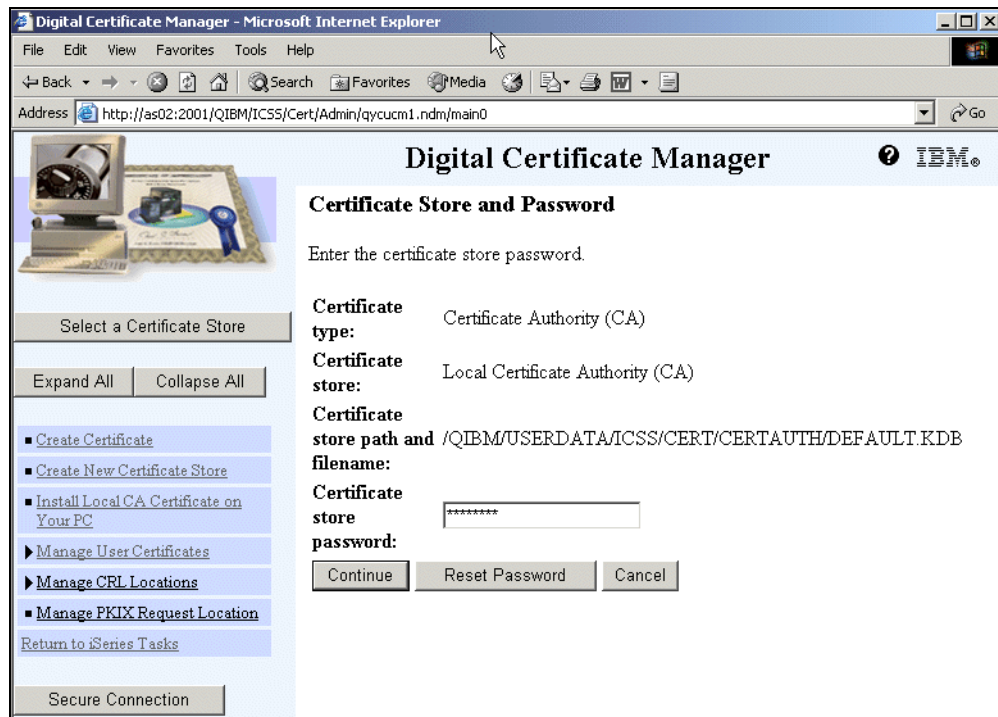


Figure 4-15 Certificate Store and Password

5. Enter the Certificate store password, and click **Continue**.

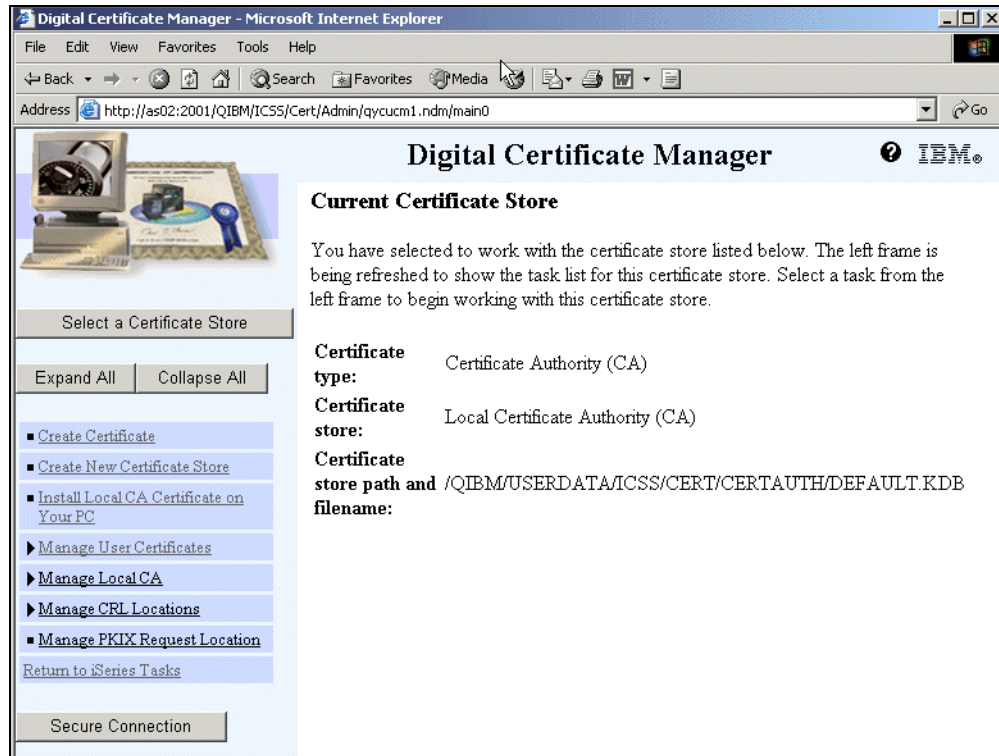


Figure 4-16 Current Certificate Store

6. Select the **Manage Local CA** link on the left.



Figure 4-17 Manage Local Certificate Authority (CA)

7. Select the **Change policy data** radio button, and click **Continue**.

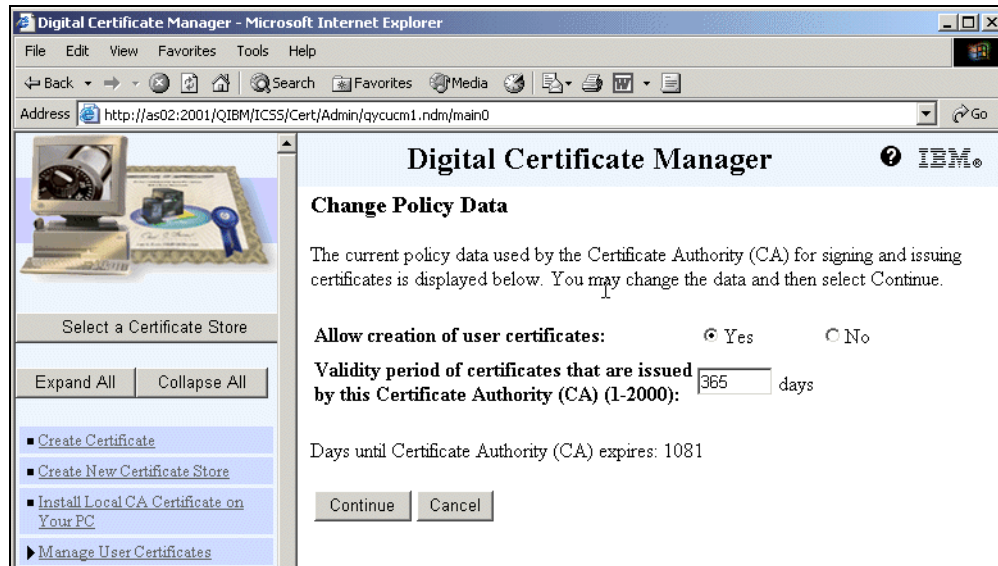


Figure 4-18 Change Policy Data

8. The Allow creation of user certificates must be set to **Yes**. Any changes to this parameter take effect immediately. Click **Continue**.

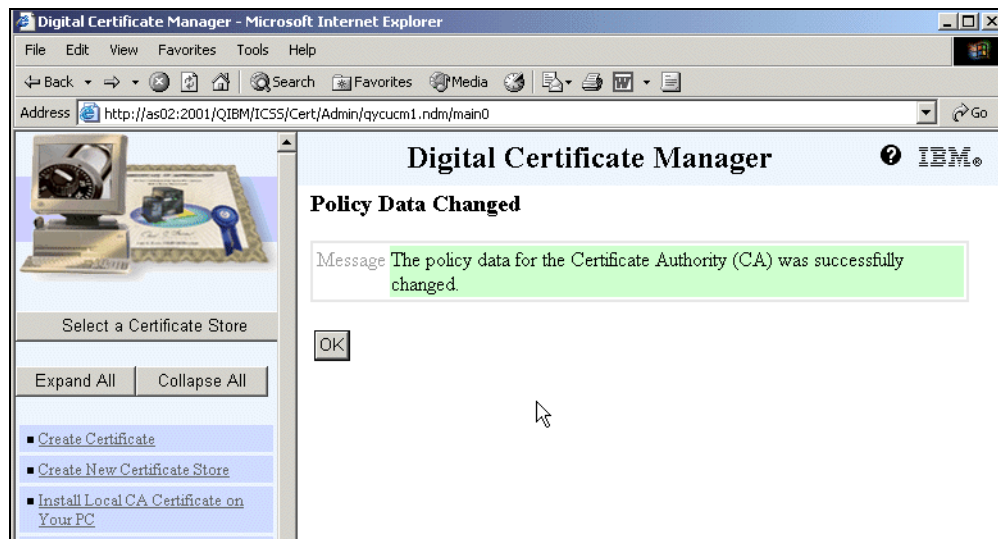


Figure 4-19 Policy Data Changed

9. Select the **Create Certificate** link.

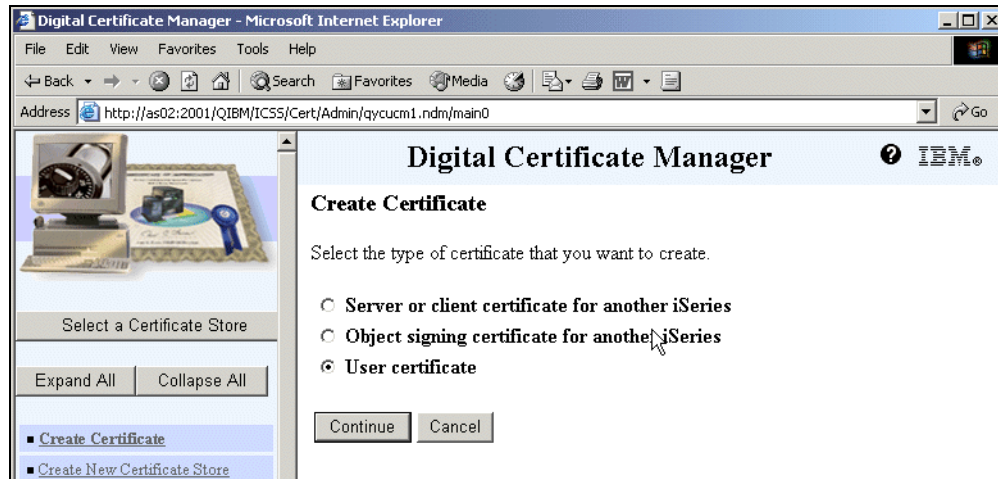


Figure 4-20 Create Certificate

10. Select the **User certificate** radio button, and click **Continue**.

Figure 4-21 Create User Certificate

11. Fill out the required fields, and click **Continue**. At this point, there are some subtle differences in how different browsers handle the installation of the user certificate. The differences are discussed in the following topics.

Internet Explorer: User certificate installation

To install a user certificate using Internet Explorer:

1. When installing the user certificate using Internet Explorer, you will see the page shown in Figure 4-22.

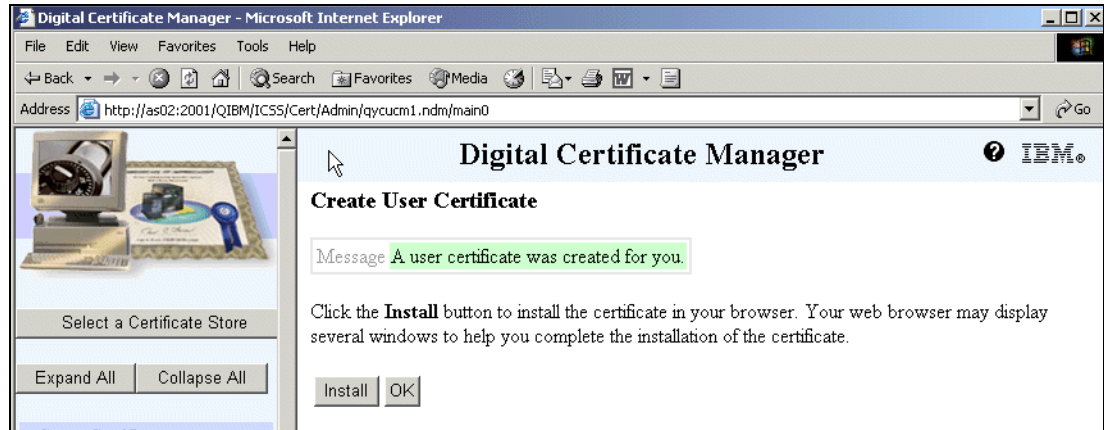


Figure 4-22 User certificate successfully created

2. For the warning message shown in Figure 4-23, click **Yes**; this is a normal warning message.

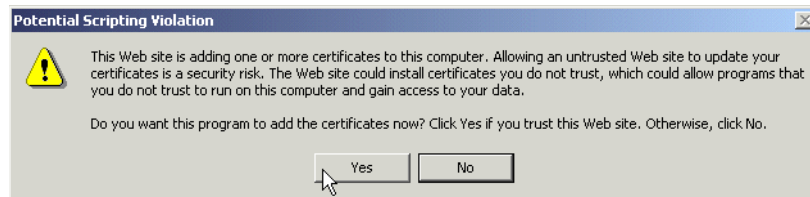


Figure 4-23 Expected Scripting error with Internet Explorer

The certificate is then installed in the browser, as indicated in Figure 4-24.

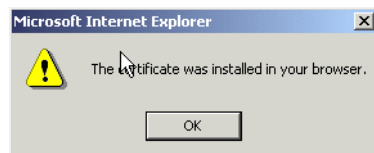


Figure 4-24 Successful install with Internet Explorer

Netscape Communicator: User certificate installation

To install a user certificate using Netscape Communicator:

1. When installing the user certificate using Netscape Communicator, you will see the page shown in Figure 4-25 on page 73.



Figure 4-25 Netscape private key message

2. Click **OK**. The page shown in Figure 4-26 opens.



Figure 4-26 Netscape password prompt to protect private keys

3. It is your choice if you want to protect you private key within your browser with a password. Click **OK**.

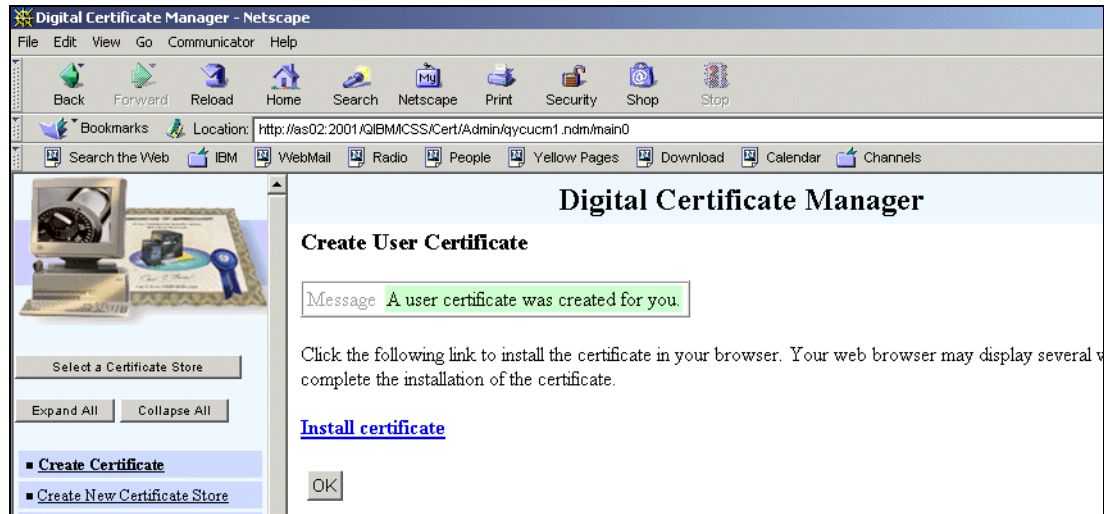


Figure 4-27 Netscape user certificate created message

4. Select the **Install certificate** link. The certificate is automatically installed to your browser without any additional messages being displayed.

Internet Explorer: Exporting the user certificate

To export a user certificate using Internet Explorer:

1. The Web browser that you use determines how you export the user certificate. If you are using Internet Explorer 6.0 or later, select **Tools** → **Internet Options**.

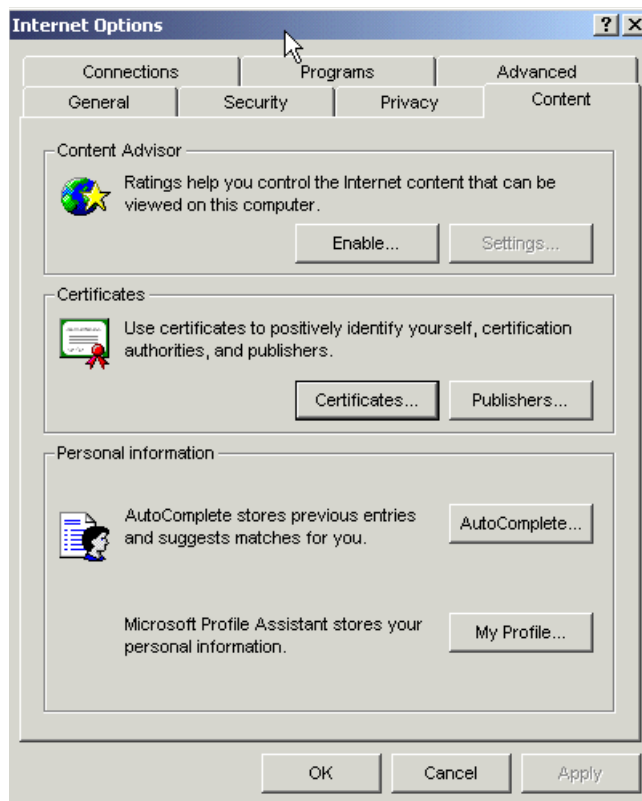


Figure 4-28 Internet Explorer Internet Options

2. Click the **Certificates** button.

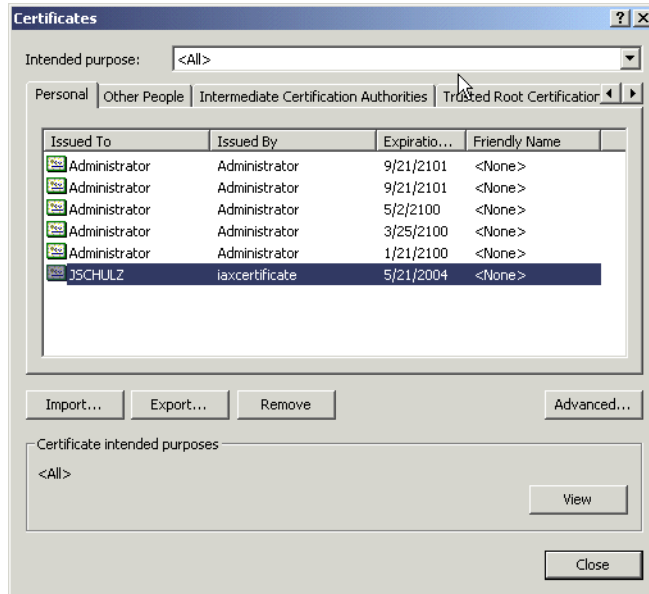


Figure 4-29 Certificates

3. Highlight the certificate, and click **Export**.



Figure 4-30 Certificate Export Wizard

4. Click **Next**.

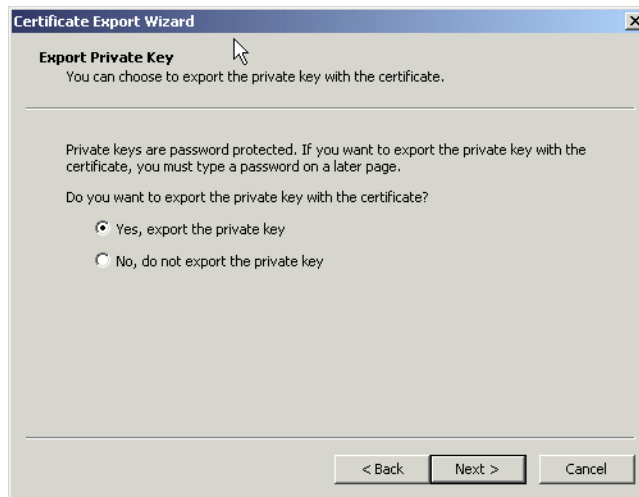


Figure 4-31 Export Private Key

5. Select **Yes, export the private key**, and click **Next**.

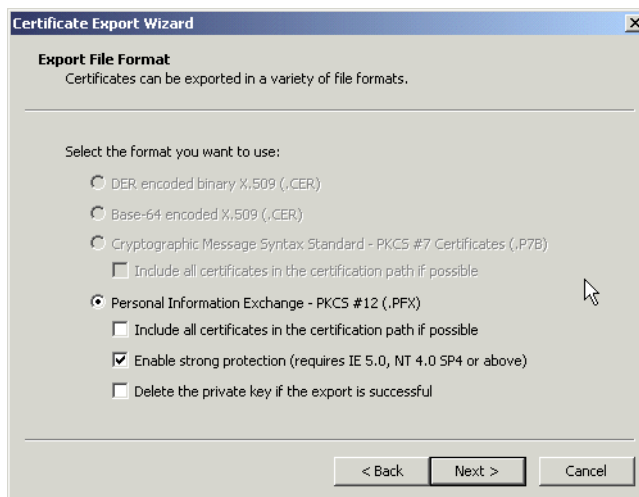


Figure 4-32 Export File Format

6. Select **Personal Information Exchange**, and click **Next**.



Figure 4-33 Password

7. Enter a password, confirm the password, and then click **Next**.

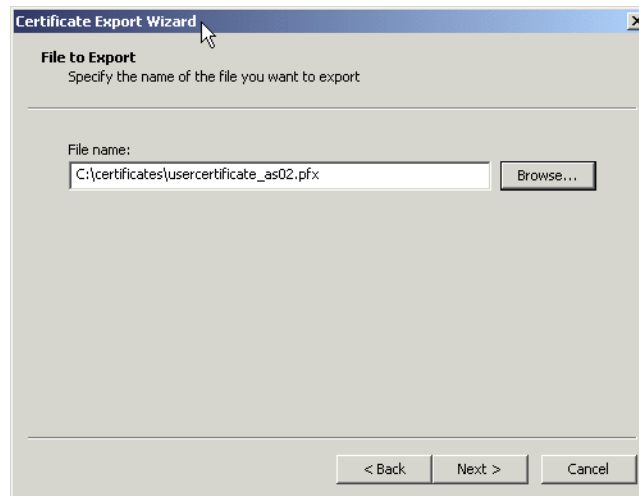


Figure 4-34 File to Export

8. Use the **Browse** button to indicate where you want to export (store) the certificate. Enter a file name and save as type Personal Information Exchange (.pfx), and select **Next**.



Figure 4-35 Completing the Wizard

9. Click **Finish**.

Netscape Communicator: Exporting the user certificate

To export a user certificate using Netscape Communicator:

1. Access the Netscape Communicator export function by selecting **Communicator** → **Tools** → **Security Info**, as shown in Figure 4-36. This opens the Netscape Your Certificates panel shown in Figure 4-37 on page 79.

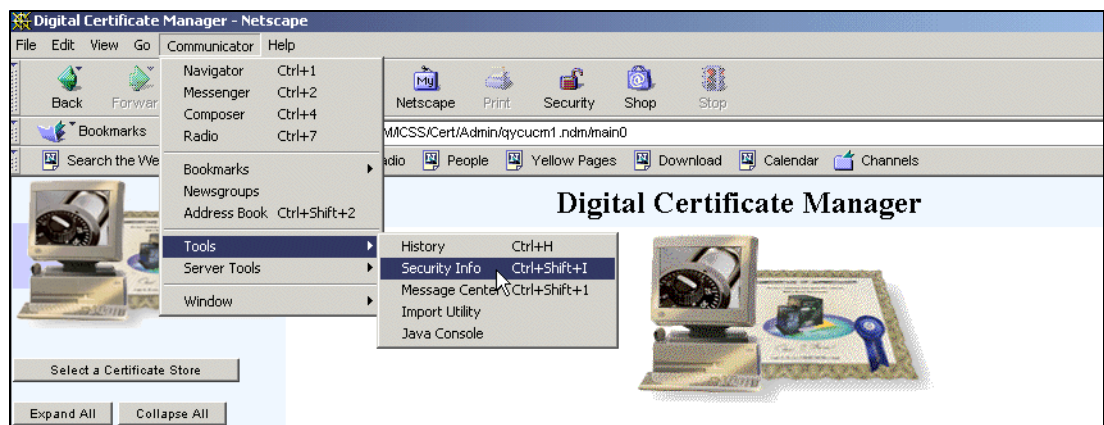


Figure 4-36 Netscape Communicator

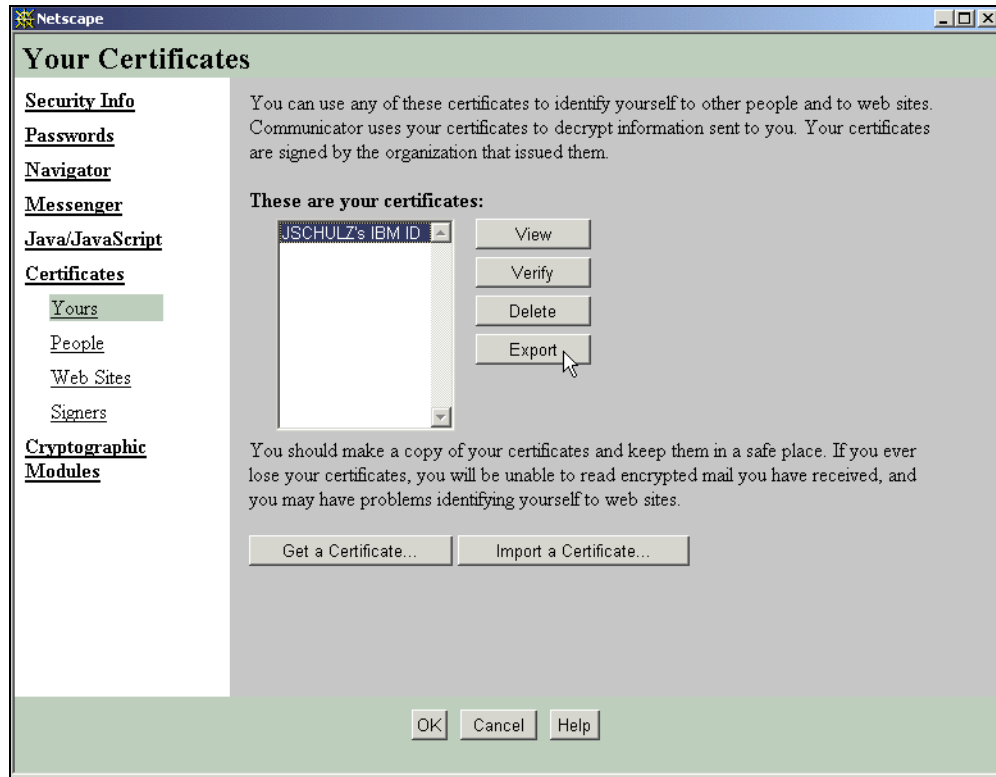


Figure 4-37 Your Certificates

2. Select the **Yours** link under the Certificates heading, highlight the certificate, and click **Export**.
3. Enter a password. Save the file as a PKCS12 File (.p12).

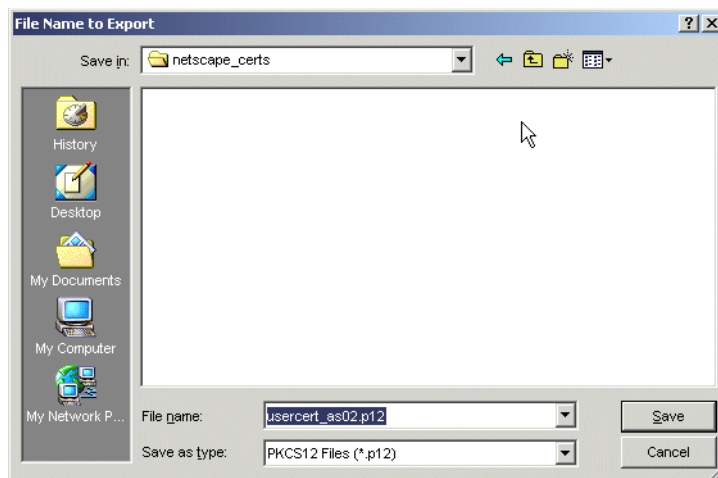


Figure 4-38 Specifying the File Name to Export

You will receive a message indicating that your certificate has been successfully exported.

4. After you export the certificate, import the certificate to the IBM Key Management database. The SSL component of iSeries Access for Windows must be installed on the PC in order to have the IBM Key Management database. See 4.5, “Configuring iSeries Access for Windows to use SSL” on page 84.

4.4.2 Importing the user certificate

Prior to importing the certificate, ensure that you have downloaded the parent certificate authority. See 4.5.2, “Downloading the certificate authority” on page 86.

To import the user certificate:

1. Open IBM Key Management by selecting **Start** → **Programs** → **IBM iSeries Access** → **IBM Key Management**.

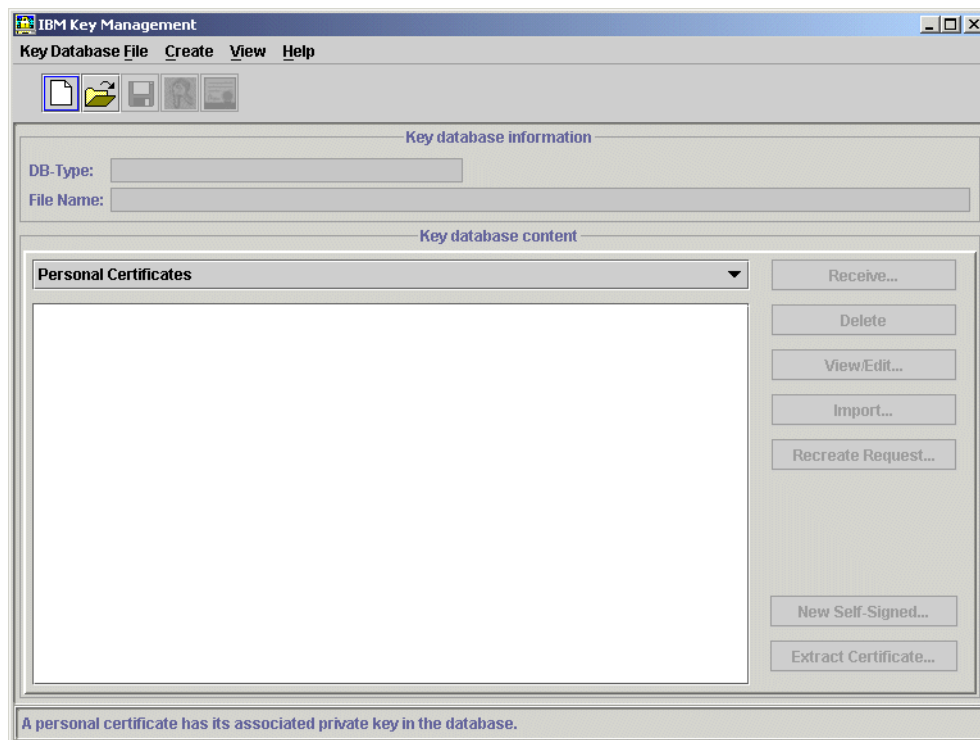


Figure 4-39 IBM Key Management

2. Select **File** → **Open** and open the cwbsldf.kdb file. The PC operating system determines the location of the cwbsldf.kdb file. On Windows 2000 and XP, it is located in C:/Documents and Settings/All Users/Documents/IBM/Client Access. A search for the cwbsldf.kdb of your PC's hard drive can also reveal its location.
3. You will be prompted for a password, which by default is ca400. Click **OK**.

Notes:

- ▶ Consider changing this password (record the new password) when using client authentication where private client certificates are being used.
- ▶ You can automatically access the currently configured SSL key database by performing the following steps:
 - a. Double-click the iSeries Access for Windows shortcut icon on your desktop
 - b. On the resulting window (upper-left window in Figure 4-40), double-click **iSeries Access for Windows Properties**.
 - c. On the main Properties panel, select the Secure Sockets tab to view the SSL properties shown in the lower-right panel in Figure 4-40.
 - d. Click the **IBM Key Management** button.

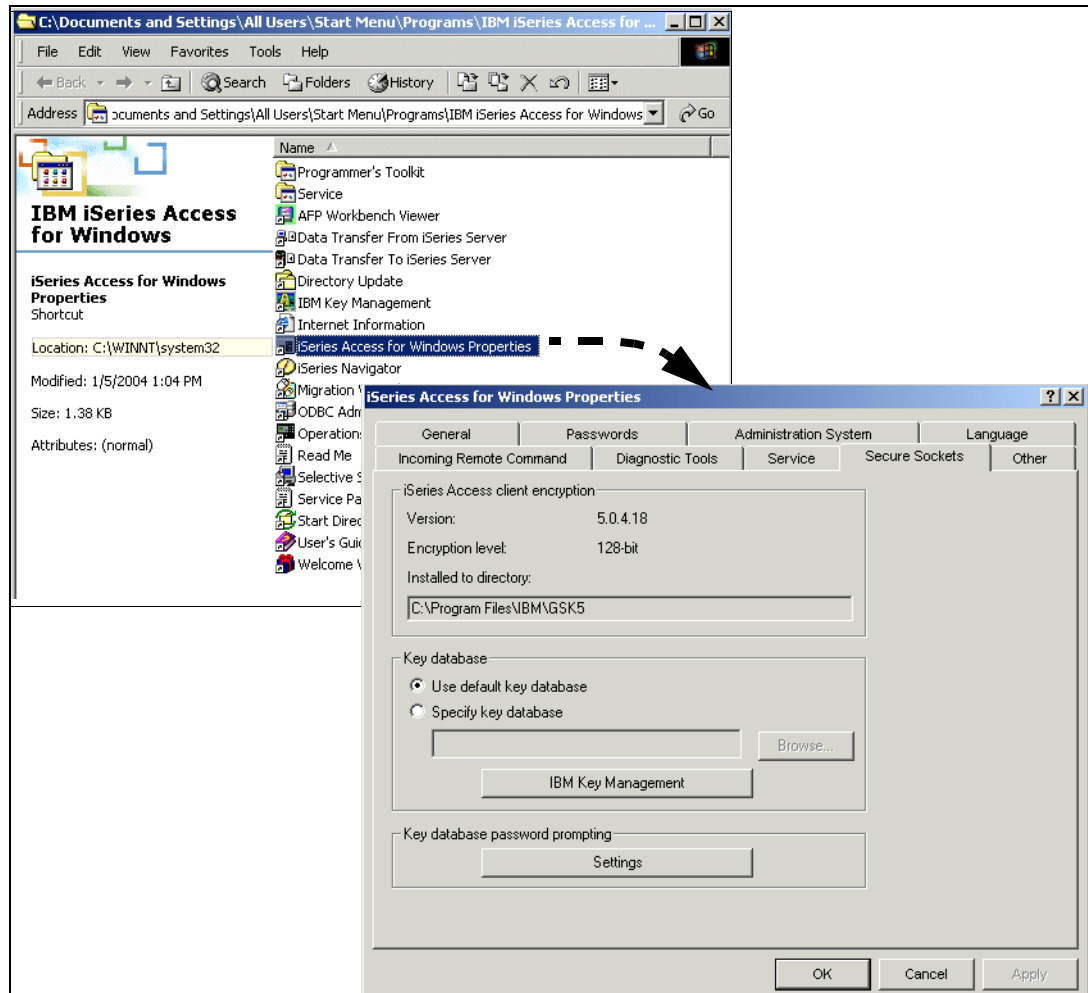


Figure 4-40 iSeries Access for Windows Properties: Secure Sockets IBM Key Management

Figure 4-41 on page 82 shows the currently available certificates in the current key database and provides additional certificate management capabilities.

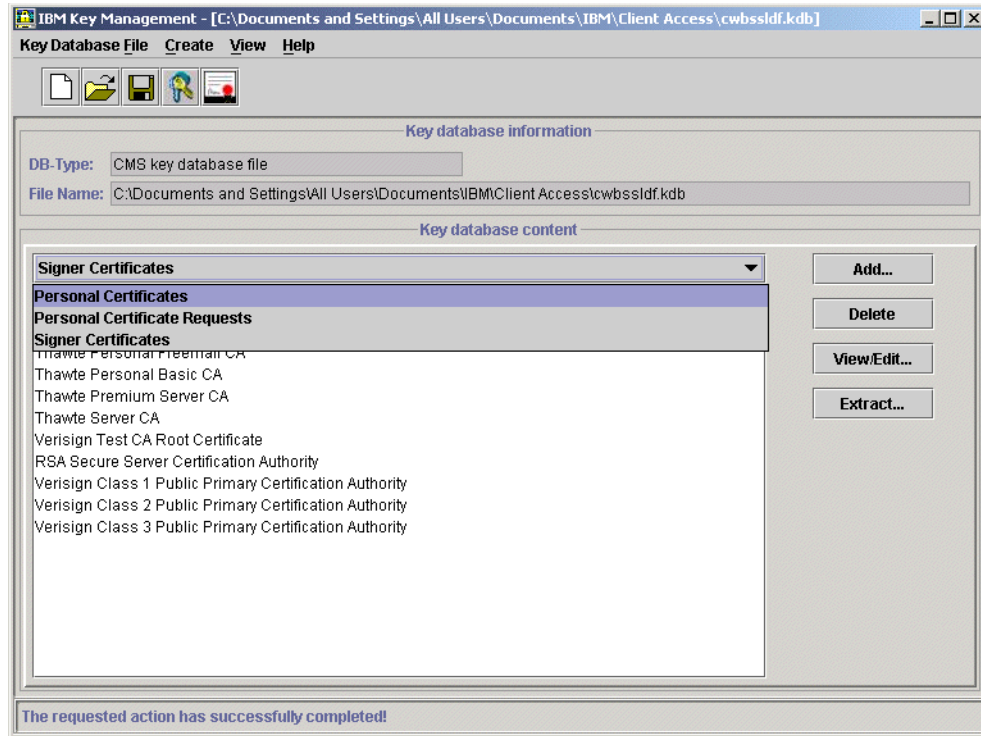


Figure 4-41 Current certificates in the key database example

4. Click the down arrow just under the “Key database content” heading and select **Personal Certificates**, as shown in Figure 4-41. Then click **Import**. This opens the Import Key window.

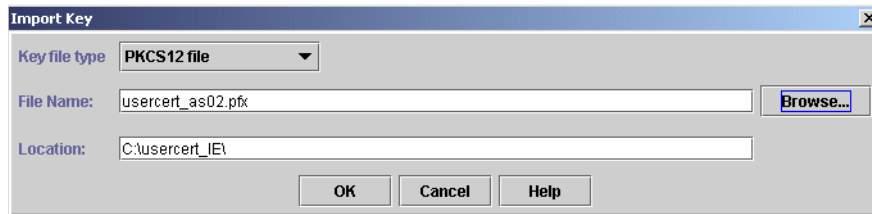


Figure 4-42 Import Key file selection

5. Click **Browse** and browse to the location where you exported the certificate. Select that location, and click **OK**.

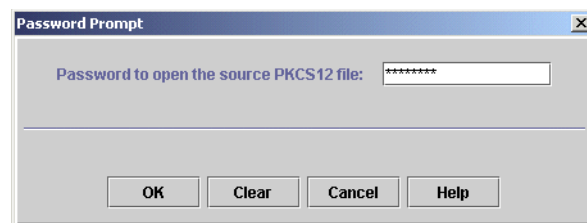


Figure 4-43 Import Key file Password Prompt

6. Enter the same password used when exporting the certificate. Click **OK**.

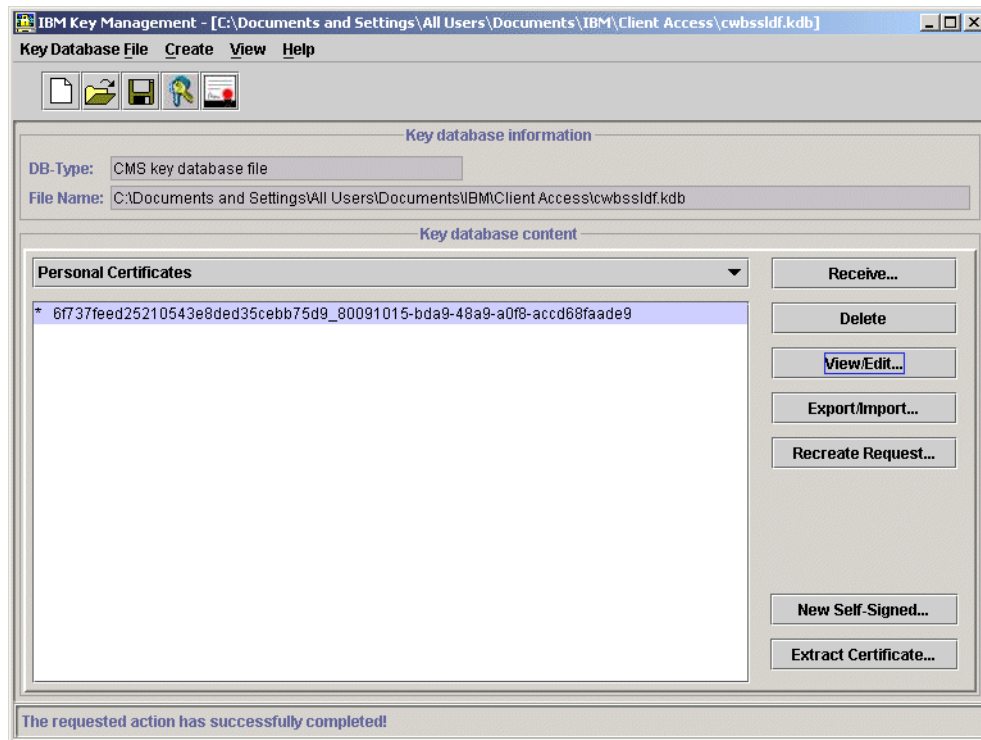


Figure 4-44 Imported certificate example

7. If you have more than one certificate installed, select the appropriate certificate, and click **View/Edit**.

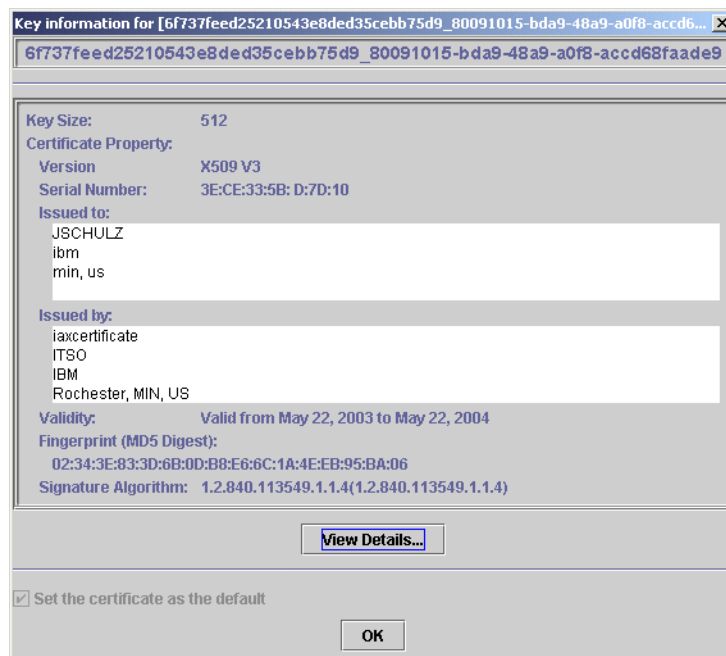


Figure 4-45 Editing view of the certificate

8. Ensure that **Set the certificate as the default** (unavailable text in the lower-left of the panel) is selected, and click **OK**. If it is the only certificate, it will be selected by default as shown here and cannot be cleared.

The client is now set to use client authentication. You simply need to configure or reconfigure your PC5250 session to use SSL.

Important: Ensure that the Telnet server on the iSeries is set to require client authentication. See the next topic.

4.5 Configuring iSeries Access for Windows to use SSL

Prior to configuring the client to use SSL, ensure that the Telnet server and host servers on the iSeries server are configured to use Secure Sockets Layer as described in the text for Figure 4-11 on page 64.

4.5.1 Installing the Secure Sockets Layer

The Secure Sockets Layer (SSL) component of iSeries Access for Windows can be installed in a number of ways. Ensure that the no charge Client Encryption 128-bit licensed program 5722-CE3 has been installed on the iSeries server.

The Secure Sockets Layer component can be installed using one of the following methods:

- ▶ The easiest way to install the SSL component is to install it as part of your base initial installation. This can be done either by using the iSeries server that has both 5722-XE1 and 5722-CE3 installed as your installation source, or by creating a tailored installation image that contains SSL, as described in Chapter 2, “Installing iSeries Access for Windows” on page 5, in the following sections:
 - 2.1, “Introduction” on page 6
 - 2.2, “Tailored installation image” on page 7
 - 2.4, “Distributing and installing the merged installation image” on page 20
- ▶ If you have already installed iSeries Access for Windows on your workstation, but did not initially install SSL, you should use Selective Setup to install SSL. You will need to supply the source directory for the installation. The easiest way is to map a drive to the iSeries QIBM share point (`\\NetServerName\QIBM`) so that the various directory paths are available to the path discovery function and use this mapped drive as the source directory. Alternatively, you can specify `\\netservername\qibm` (Figure 4-46) or `\\ipaddress\qibm` (Figure 4-47 on page 85) as the source directory.

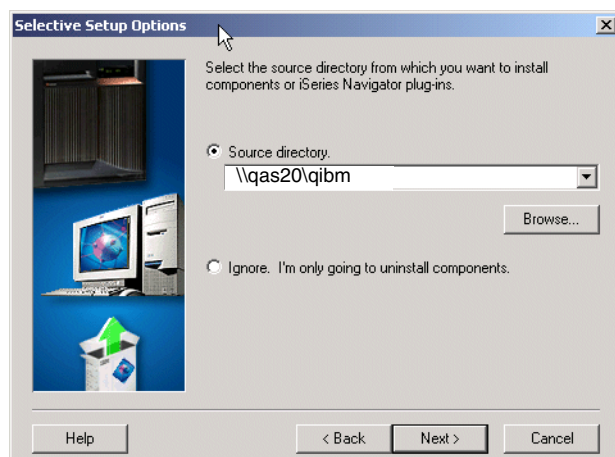


Figure 4-46 NetServer name specified

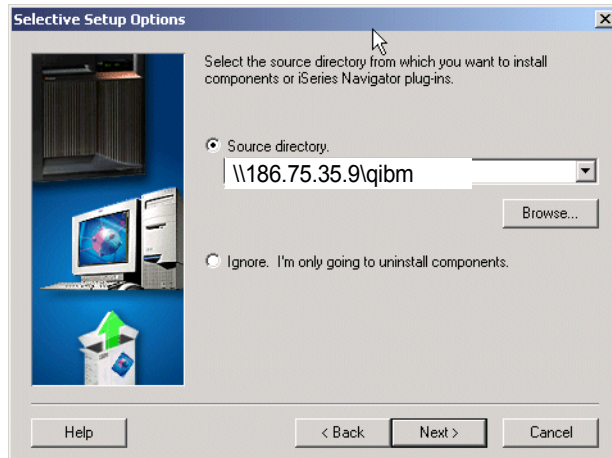


Figure 4-47 IP address of iSeries is specified

See Chapter 2, “Installing iSeries Access for Windows” on page 5 for general installation information.

To use Selective Setup to install SSL:

1. If you have a slower network environment, you might want to copy the installation image to a Windows drive. Copy the \\QIBM\ProdData\Access\Windows directory and its subdirectories to the desired location. You can now run either an initial install or Selective Setup to install SSL from this copy of the installation image. Note that this technique would not normally be used.
2. Run Selective Setup, specifying your mapped drive to this network share and \\Express, as shown in Figure 4-48.

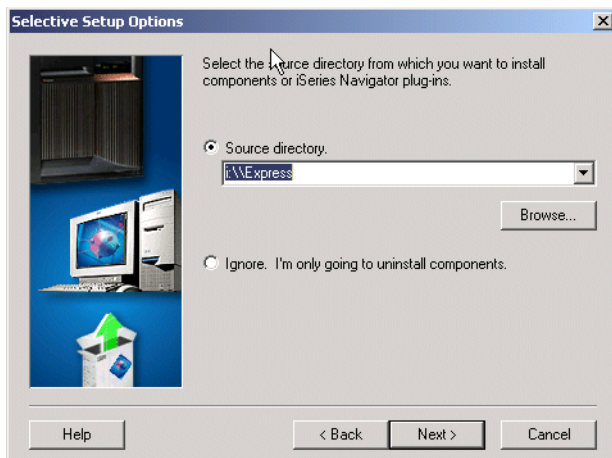


Figure 4-48 Mapped drive is specified

3. Click **Next**. You should see Secure Sockets Layer as one of the available components to install.

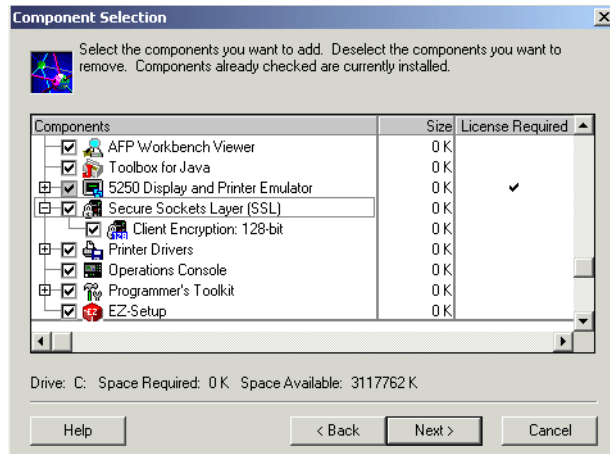


Figure 4-49 Component Selection

4. Follow the normal selective install wizard steps.

4.5.2 Downloading the certificate authority

After the Secure Sockets component of iSeries Access for Windows is installed, the certificate authority (CA) must be downloaded.

To download the certificate authority:

1. Open iSeries Navigator, right-click the iSeries system name or IP address, and select **Properties**.
2. On the Properties window, select the Secure Sockets tab, as shown in Figure 4-50.

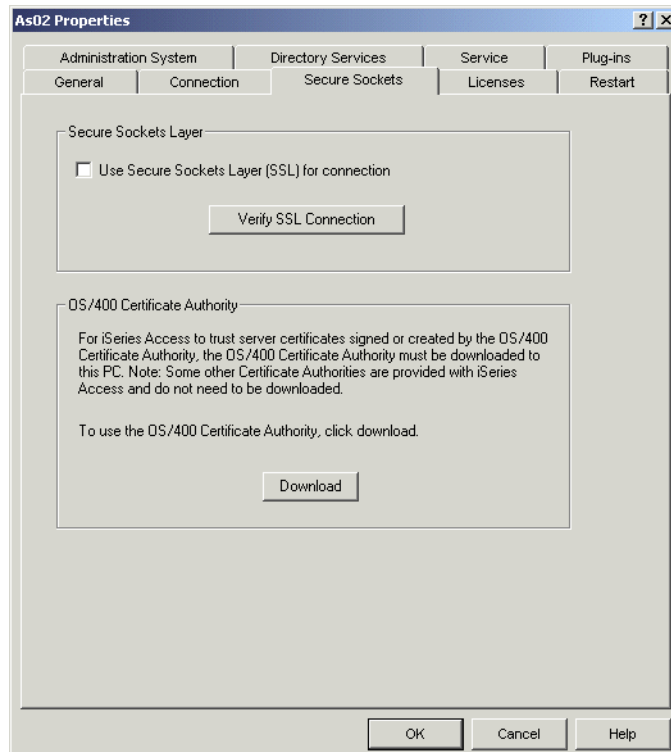


Figure 4-50 Secure Sockets tab

3. Click **Download** to download the OS/400 certificate authority.

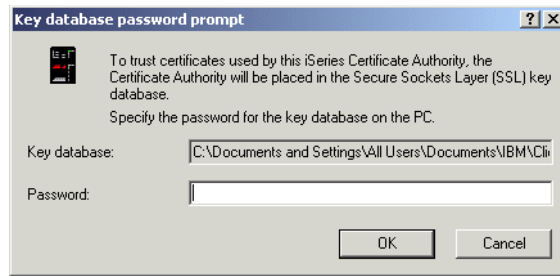


Figure 4-51 Key database password prompt

4. Enter the key database password, and click **OK**.

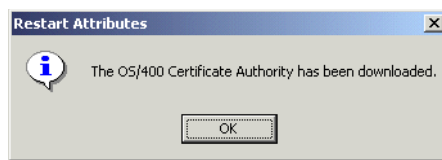


Figure 4-52 Download complete message

4.5.3 Verifying the SSL connection

To verify the SSL connection:

1. Select **Use Secure Sockets Layer (SSL) for connection**.

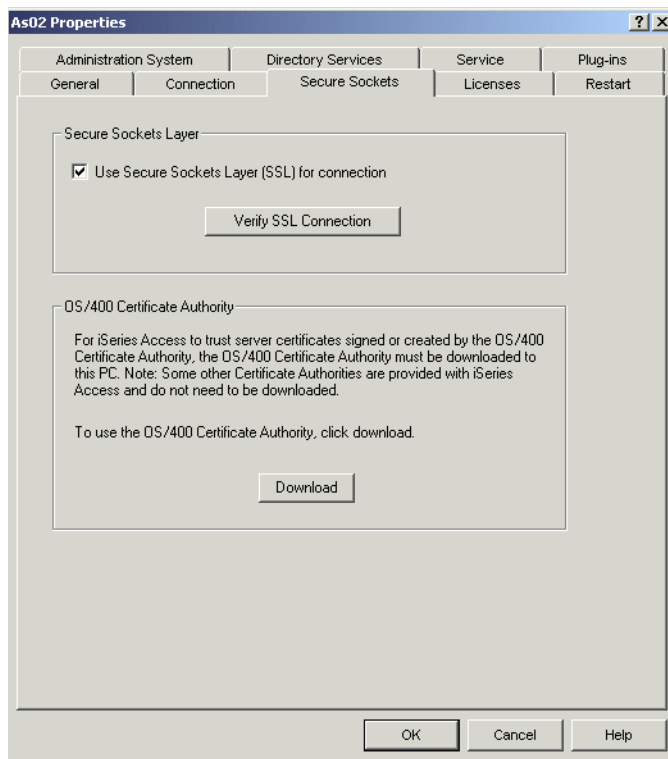


Figure 4-53 System properties panel to verify SSL connection

2. Click **Verify SSL Connection**. After some seconds of processing, a window similar to the one shown in Figure 4-54 opens.

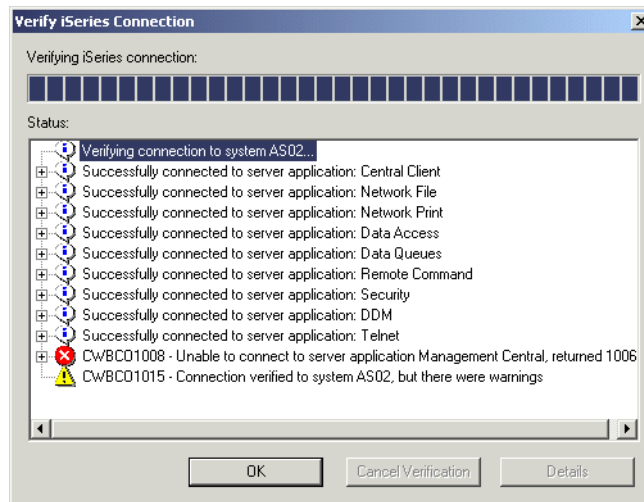


Figure 4-54 Verifying SSL results

Notice in Figure 4-54 that all of the host servers and Telnet servers are verified. Management Central was not configured for SSL, and therefore, verification failed as we expected.

A message appears that indicates a close and restart of the currently running iSeries Access for Windows applications must be performed to use the new SSL connection settings.

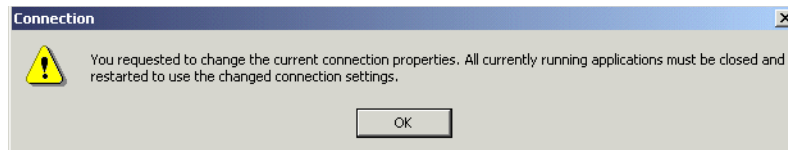


Figure 4-55 Close iSeries Navigator and restart

When SSL has been successfully enabled for iSeries Navigator to a specific iSeries system, a lock symbol appears next to that iSeries system, as shown in Figure 4-56 on page 89. This indicates connections to this server will use SSL.

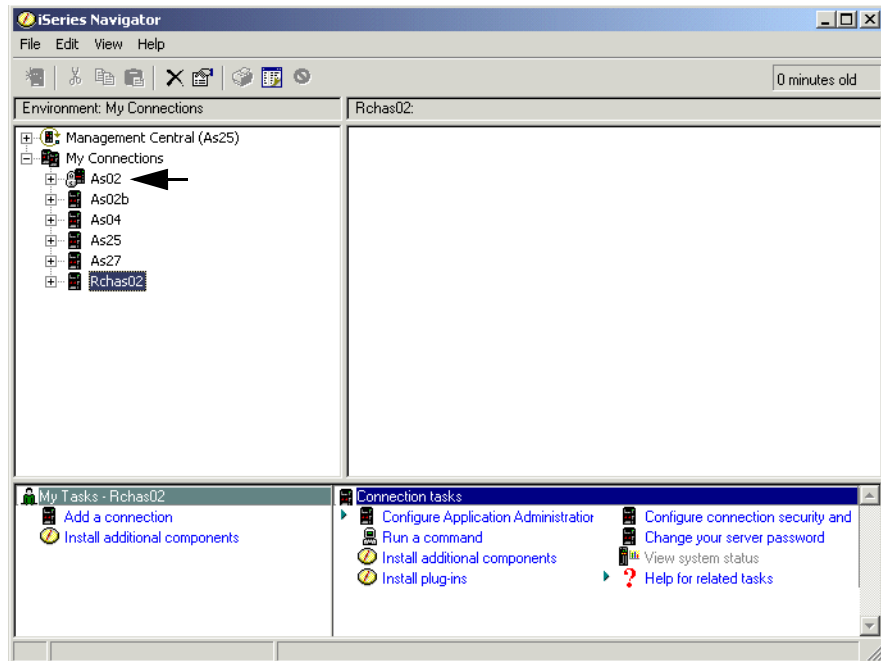


Figure 4-56 Secured connection: Lock symbol indication

4.5.4 Configuring PC5250 emulation to use SSL

To configure PC5250 emulation to use SSL:

1. The configuration options of a current PC5250 emulation session can be accessed by selecting the Communication drop down list and selecting **Configure**.
2. In the Configure panel, click **Properties**.

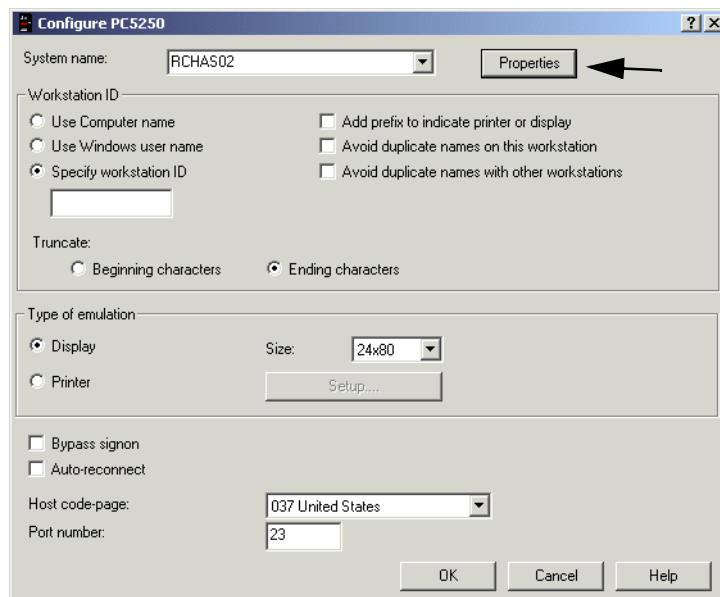


Figure 4-57 Configure PC5250 to use SSL: Starting with Properties

3. In the Connection panel shown in Figure 4-58 on page 90, select **Use Secured Sockets Layer (SSL)**.

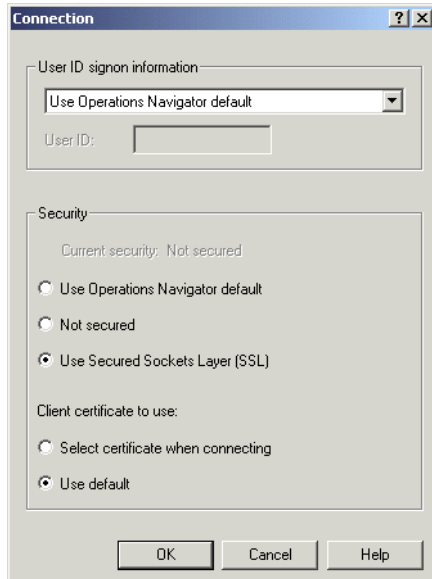


Figure 4-58 Selecting to use SSL and the default client certificate

Note: If you are using client authentication and have multiple user certificates and want the user to select which certificate to use, select the option **Select certificate when connecting**. In all other cases, select the **Use default** option. If you know what was specified for iSeries Navigator, you can select **Use Operations Navigator default**.

4. In our example, we select **Use default** client certificate for PC5250. Click **OK**.

This returns you to the Configure PC5250 panel, as shown in Figure 4-59.

Now, this panel shows a Port number value of 992, which is the Telnet server's default port for SSL connections.

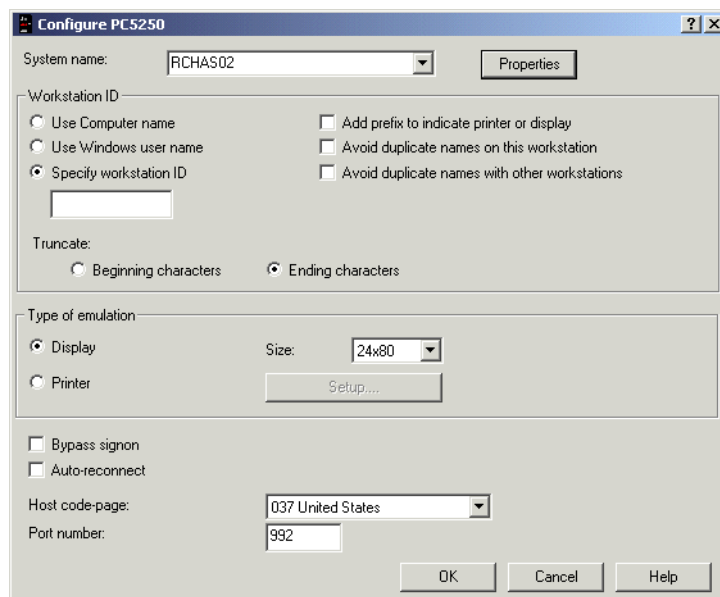


Figure 4-59 Configured to use secure Telnet

5. Click **OK**. Assuming everything is set up correctly, in a few seconds, you see the iSeries 5250 Sign on screen, as shown in Figure 4-60.

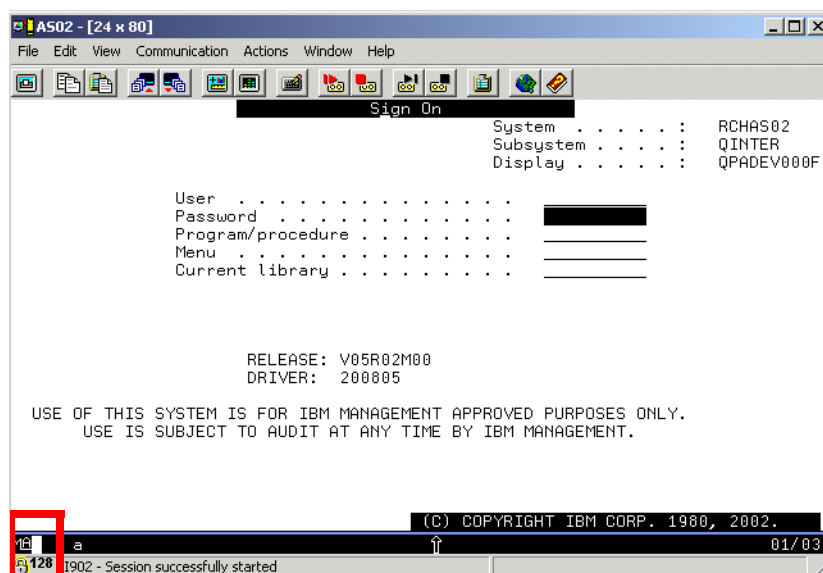


Figure 4-60 PC5250 emulation using SSL

Notice the lock symbol in the lower-left corner of Figure 4-60, which indicates the session is using SSL and is secure.

This concludes how to set up to use SSL with iSeries Navigator and PC5250 sessions. The next topic gives a summary for viewing CA certificates for their expiration dates.

4.6 Viewing a certificate authority certificate

At the start of this chapter, in 4.1, “Introduction” on page 56, we discuss the importance of certificates, protecting them with passwords, and renewing a certificate before it expires.

In this topic, we show the primary steps to view the expiration date of a CA certificate shipped with OS/400. Similar steps would be followed for other certificates.

If you need to renew a certificate, follow the Renew link you see in some of our figures. If necessary, contact your IBM Support Line representative for assistance in certificate renewal.

Follow these steps to view a certificate:

1. From a browser enter:
<http://system name:2001>
 (This is the Administration HTTP server.) In our example, we use system as27.
2. Click the **Digital Certificate** link to get the upper window in Figure 4-61 on page 92.
3. Click the **Select a Certificate Store** button to get the middle window in Figure 4-61 on page 92.
4. For a CA certificate that shipped with OS/400, select ***SYSTEM**. Click **Continue** to get the Certificate Store and Password window shown as the lowest window of Figure 4-61 on page 92.

5. Enter the store's password and click **Continue**. This opens to the Current Certificate Store window, as shown in Figure 4-61 on page 92.

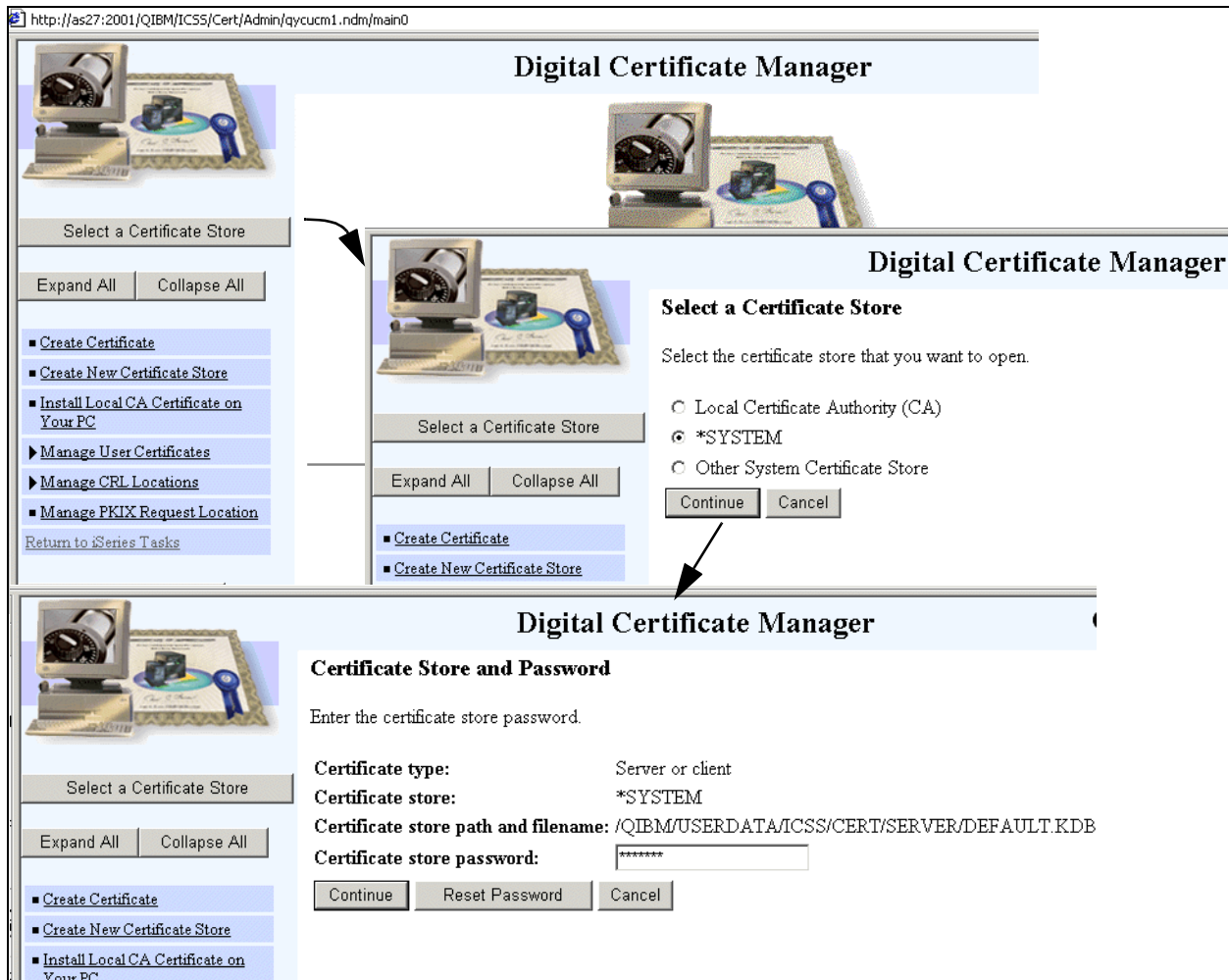


Figure 4-61 Finding a certificate's expiration date: 1 of 3

6. Using Figure 4-62 on page 93 as our example, click the left navigation bar **View certificate** link.
7. In the View Certificate window, select **Certificate Authority (CA)**, which opens the list of Certificate Authority (CA) certificates shown in Figure 4-63 on page 94. Select, for example, **Verisign Class 3 Public Primary Certification Authority**. Click **View**.

This opens to the lower View Certificate Authority (CA) certificate window for Verisign Class 3 Public CA.

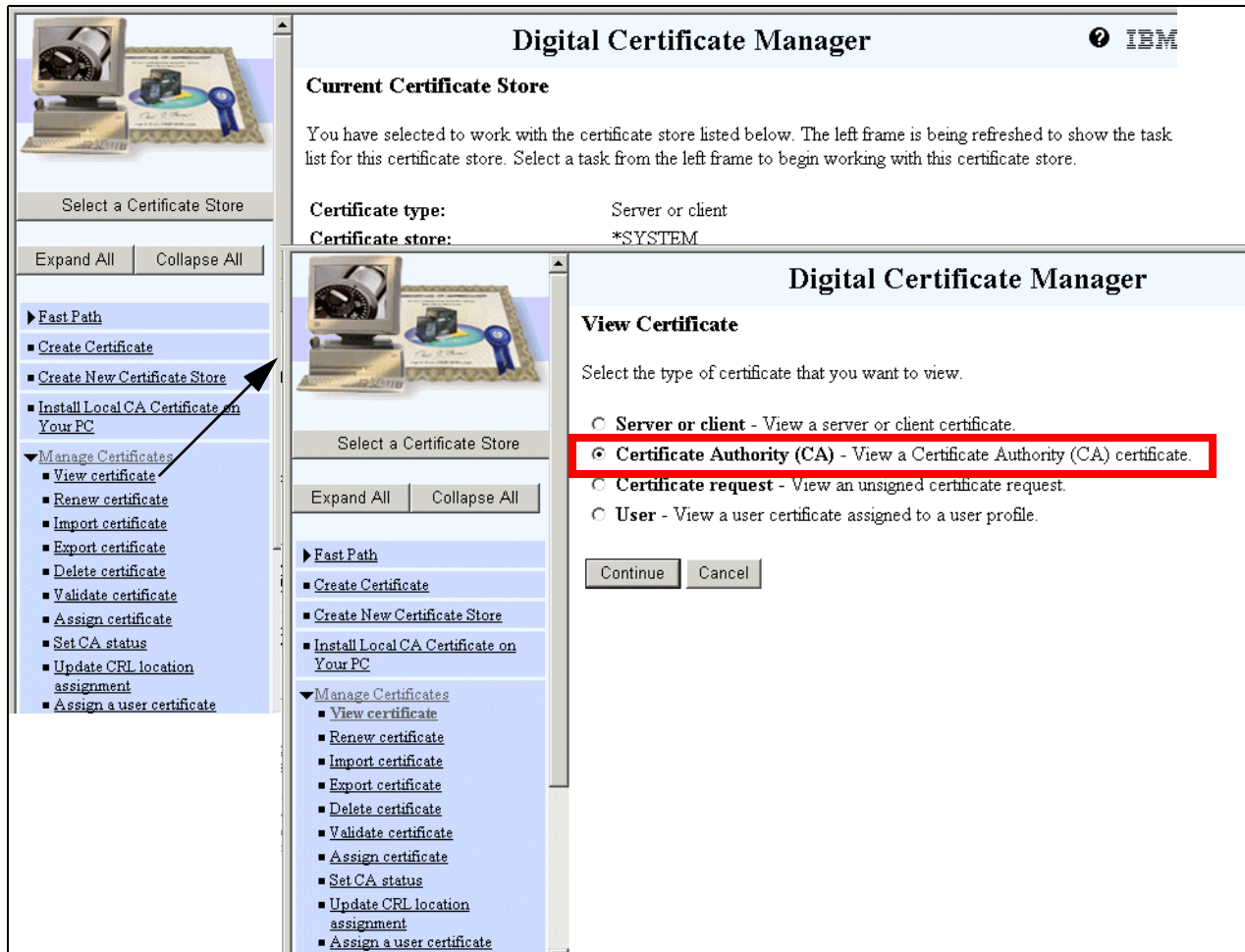


Figure 4-62 Finding a certificate's expiration date: 2 of 3

Note that the Additional information area in Figure 4-63 on page 94. We annotated the Validity period field, which shows this certificate expires on August 01, 2028.

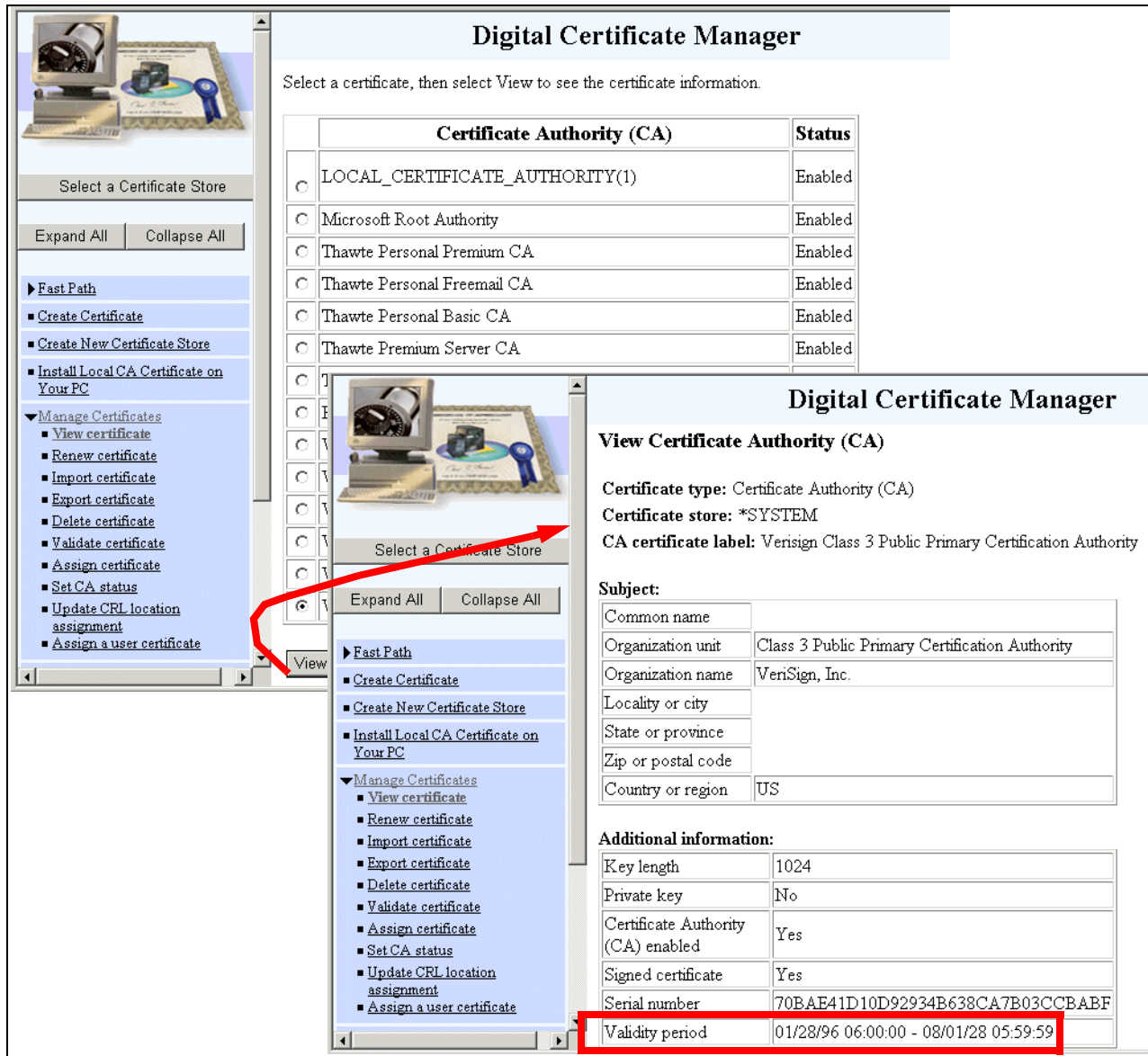


Figure 4-63 Finding a certificate's expiration date: 3 of 3 (CA certificate for Verisign Class 3 Public CA)

You can scroll down this window to see additional information. By clicking the **View Applications** button (not shown), you can see applications using the certificate. In our example shown in Figure 4-64 on page 95, you can see that the Telnet server uses this certificate.

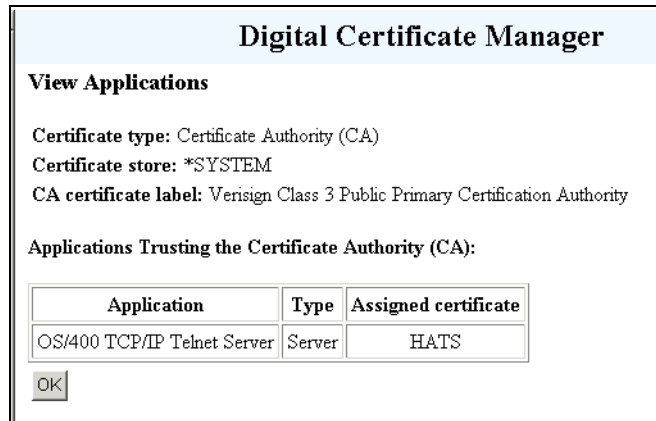


Figure 4-64 Viewing applications using the certificate

8. Click **OK** to finish viewing the certificate information.



iSeries Access for Windows in a Kerberos environment

This chapter describes the following topics:

- ▶ An example of using Kerberos authentication with iSeries Access for Windows functions.
- ▶ Kerberos support overview, including a setup example.
- ▶ Basic Enterprise Identity Mapping (EIM) support on iSeries. EIM provides user mapping functions across a network with the extended capabilities that include the same user ("identity") having different IDs on various servers in the network.

In the context of this book, we use iSeries EIM support to map a Kerberos principal ("user") to an OS/400 user.

It is important to note that configuration of both the Network Authentication Service and Enterprise Identify Mapping on the iSeries server is required to map a Kerberos authenticated principal to an OS/400 user even when the user ID on the client and the server are identical.

Note: This chapter provides sufficient details to enable a Windows client workstation user to perform iSeries Access for Windows PC5250 emulation and iSeries Navigator functions using Kerberos authentication and EIM mapping for an OS/400 user profile.

Full coverage of iSeries Kerberos and Enterprise Identity Mapping functions and parameter options is beyond the scope of this book. For detailed information about iSeries support of these two capabilities, we suggest that you review the IBM Redbook *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975. Much of the Kerberos and Enterprise Identity Mapping information in this chapter is based on this Redbook.

Other good sources of iSeries Kerberos and EIM information are iSeries Information Center articles and the iSeries Navigator online help information (select **system** → **Security** → **Network Authentication Service** or **system** → **Network** → **Enterprise Identity Mapping**).

A good source for industry-wide details about Kerberos is the book *Kerberos: The Definitive Guide*, by Jason Garman, ISBN 0596004036.

5.1 Using Kerberos authentication with iSeries Access for Windows functions

Kerberos can be considered as a set of protocols intended to enable network security, primarily focused on the process of being authenticated to use various servers and services within the network. Kerberos does not provide the process to validate authorization to use a function. That is, authentication is concerned with the identity of the user; and authorization is the ability to actually do something as that user, such as perform a function, read, write, or update data, or run a program on a specific server system.

Although full details are not covered in this chapter, we do provide information about the Kerberos set up requirements. Before going further, from an iSeries viewpoint, it is important to note:

- ▶ Kerberos is used for authentication of a user, system, device, or service (all referred to as Kerberos *principals*), instead of the typical user ID and password components for authentication. Kerberos does provide a level of “single signon to a network.” It does not, by itself, provide authorization to specific functions within the network.
- ▶ Enterprise Identity Mapping is the IBM architecture and implementation for taking that single signon authentication to another level, which includes mapping that authenticated user to a corresponding operating system specific user ID and password, all of which could be unique on each system within the network.

In a simple iSeries Access for Windows scenario, when initiating an iSeries Navigator session that has been set up to use Kerberos, Kerberos processing authenticates that the PC client workstation user, KUSER1, for example, can sign on to a Windows domain. On iSeries, EIM must be used to map the received Kerberos principal (“user”) represented by KUSER1 to an OS/400 user. That OS/400 user could be spelled KUSER1 or any other valid OS/400 user set up through OS/400 security commands or the iSeries Navigator Security interface.

Note that OS/400 security and iSeries Access for Windows installation options and Application Administration control what iSeries Access functions can actually be performed by that user (KUSER1 in our example) once signed on to the iSeries server.

When attempting to connect to an iSeries server (or any other server product in the Kerberos domain, called a realm), the process of obtaining a “ticket granting ticket,” and in turn, a “service ticket” to perform iSeries Access for Windows functions is performed through a dialog with a Kerberos Key Distribution Center (KDC), without any visible indication to the workstation user. Assuming successful authentication, then without any interruption, the next thing the workstation user sees is:

- ▶ For a PC 5250 emulation session: Either the main OS/400 command entry screen or an associated initial program screen as specified for the OS/400 user profile
- ▶ For an iSeries Navigator session: The main iSeries Navigator window with the left pane hierarchy tree expanded for that system

There is no sign-on prompt to the workstation user.

In this topic, we assume (so do not show the setup) the Kerberos principals for the Windows client workstation and its user are set up correctly on your Kerberos Key Distribution Center (KDC) server.

The capability to initiate connections using Kerberos is available on your PC client workstation with Microsoft Windows 2000, XP, or later installed.

In the remainder of this chapter, we explain how to set up iSeries Access for Windows PC5250 emulation and iSeries Navigator functions to run under Kerberos and EIM in the following order:

1. Kerberos overview and setting up a Kerberos authentication network.

Note, this includes coordinating the “system times” on the Kerberos Key Distribution Center (KDC) server and all the servers in the Kerberos domain (*realm*) have been synchronized within a Kerberos “time skew” limit. Five minutes is the default skew value.
2. EIM overview and setting up a simple EIM domain with an iSeries system.
3. Setting up iSeries Navigator and PC5250 emulation on the PC workstations to use Kerberos (EIM is not apparent).
4. Verifying that iSeries Navigator and PC5250 emulation connect to an iSeries server using Kerberos and EIM.

5.2 Kerberos overview

This major section provides an overview of Kerberos concepts and terminology, as well as listing software requirements for Kerberos support on the iSeries server and other servers that provide Kerberos functions.

Later topics provide more details and an example setup using a Windows 2000 Server to provide the Key Distribution Center functions and an iSeries server to which an iSeries Navigator session is initiated.

See the Note box on page 98 for documentation that provides details beyond what is covered in the remainder of this chapter.

The Kerberos architecture was originally designed and developed in the 1980s by the Massachusetts Institute of Technology (MIT) as part of the Athena project. Its name derives from Cerberus, the legendary three-headed dog of Greek mythology, which guarded the gates of the underworld. This guardian made sure only the souls of the dead could enter Hades and that no souls could escape.

Kerberos Version 4 has been available for some time and has been superseded by the current Kerberos Version 5, which is standardized in RFC 1510. This book presumes that you are using Kerberos Version 5 in your network. For more details, see

<http://www.ietf.org/rfc/rfc1510.txt>

There are two main open source implementations of Kerberos, which you should at least be aware of:

- MIT's Kerberos: The Massachusetts Institute of Technology (MIT) implementation of Kerberos is currently at Version 5 with a Release Version of 1.3.1. In January 2000 and again in October 2000, the U.S. export laws for open source cryptography were relaxed. This means that open source code and objects relating to this open source code can now be freely exported from the U.S. The MIT download page, however, still asks questions pertaining to the laws before they were relaxed. MIT is doing this until they can consult legal council over the widespread download of their binaries. In the meantime, a version of the MIT Kerberos implementation can be downloaded from the MIT distribution Web site, available at:

<http://web.mit.edu/kerberos/dist/index.html>

For more information about the MIT version, see:

<http://web.mit.edu/Kerberos/>

When flaws are found in their Kerberos implementation, MIT produces a Security Advisory that lists a summary of the problems, the impact that this has on the protocol, where to get fixes, and what the fixes actually change in the Kerberos implementation in order to remove the weakness. The advisories can be found at:

<http://web.mit.edu/kerberos/www/advisories>

- Heimdal: This version of Kerberos is also at V5 and the release of this Version is 0.6. The goal of Heimdal is to produce a free version of Kerberos that can be used by anyone. It aims to be compatible with the MIT Kerberos V5 API and also the Generic Security Services API (GSS). Information about the GSS-API can be found in several places, one of which is the book *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.

The Heimdal version of Kerberos is a cleanroom implementation of Kerberos, meaning that it has been built from the ground up, and although it has the same functionality as the MIT version of Kerberos, the underlying code in each implementation is unique. Both Heimdal and MIT resolve the same bugs in their implementations within very similar time frames.

For more information about the Heimdal version, see:

<http://www.pdc.kth.se/heimdal/>

Since the original implementation of the Version 5 Kerberos protocol, more weaknesses with the Version 4 protocol have been detected. Many of the differences between the versions are because parts of the Kerberos implementation have been rewritten using more standardized protocol formats (such as Abstract Syntax Notation One (ASN.1), which defines a methodology for defining a byte stream that conveys, for example, "realm information" versus "principal information"). This is done in order to make the implementation more easily extendible in the future.

The only true way to avoid compatibility problems between Versions 4 and 5 is to use only the Version 5 support in your Key Distribution Center (KDC), which is discussed later in this chapter. We recommend only using the version 5 Kerberos protocol if implementing Kerberos. If you are working with Kerberos Version 4, we suggest migrating to Version 5.

Kerberos can be part of handling your network security issues. It provides the tools of authentication and also strong cryptography over the network to help you secure your information systems across your entire enterprise. Kerberos authentication itself does not automatically imply that an entire session is encrypted. However, Kerberos enables a secure exchange of encryption keys that could be used by a client program for session encryption.

Note that iSeries Access for Windows, for example, does not implement encryption based on Kerberos, but instead uses iSeries-based SSL encryption.

5.2.1 Kerberos concepts

Kerberos defines a *realm*, often also referred to as an administration domain. A realm contains members. A member can be a user, a server (system), a service (such as Telnet or iSeries Navigator), or a network resource.

Each member is registered within a Key Distribution Center (KDC) server's database. Each member has a unique identifier that is referred to as a *principal*. A Key Distribution Center has the primary responsibility of holding the authentication security information and granting *tickets* to connect to the network so that a principal can perform some service function on a system (server) within the Kerberos realm.

Therefore, a Kerberos realm is made up of the KDC and all of its enrolled principals.

A principal name is made up of several parts, including a primary part, an optional instance part, and the realm name itself. We provide more information about realms and principals later in this chapter.

After a principal has been defined to the realm, the principal information is used when, for example, an iSeries Access for Windows user wants to connect to an iSeries system and do some iSeries Access for Windows function, such as using iSeries Navigator.

When a principal initiates a connection, there are two main "Kerberos server" functions performed to complete the authentication process. Each of these involve a protocol for obtaining the appropriate ticket to identify the principal and the service function the principal wants to perform. Assuming these two Kerberos server functions are successful, the principal's workstation Kerberos software sends a service ticket to the system on which the principal wants to perform the intended function.

The following summarizes the two major Kerberos server authentication functions:

- ▶ Authentication server (AS) process: As part of connecting to a network and initiating a request to perform a function, the client sends a clear text request for a ticket for the desired server (the system on which this user wants to perform a function) to the *authentication server* (AS). Both the user and the target server are defined as Kerberos principals. The authentication server's reply is sent encrypted in the client's *secret key*. Usually this request is for a *ticket granting ticket* (TGT) that can later be used with the ticket granting server (TGS).
- ▶ Ticket granting server (TGS) process: After the client has a valid TGT, it sends a request to the TGS. The client sends the TGT to the TGS in the same manner as though it were contacting any other application server that requires Kerberos credentials. Included in this information is the identification of the service to be authenticated.

The reply is encrypted with the session key from the TGT. The reply includes a ticket for using "service xxx".

On behalf of the workstation's Kerberos principal, the originating workstation then sends the service ticket information to the intended target server system on which the function is to be

performed. This target server, configured to accept Kerberos tickets, accepts the user principal as having been already authenticated.

The following topic provides additional details about the components that implement the Kerberos protocol just described.

5.3 Kerberos protocol components

In this topic, we provide more details about the following primary Kerberos authentication protocol components:

- ▶ Tickets
- ▶ Principals and realms
- ▶ Key Distribution Center (KDC)
- ▶ Services

Figure 5-1 on page 102 shows how all the different Kerberos components fit together and the “ticket protocol” to perform a Kerberos realm authentication process. As an example, we use the principal represented by John to connect to principal Server1 to start an iSeries Navigator session as “Service A.”

Review the text in each of the numbered protocol steps within the figure. Steps 1 and 2 complete the authentication server processing and Steps 3 and 4 complete the ticket granting server processing. Steps 5 and 6 complete the use of the service ticket as authentication to the system on which the intended function (for example, an iSeries Navigator connection) is to be performed.

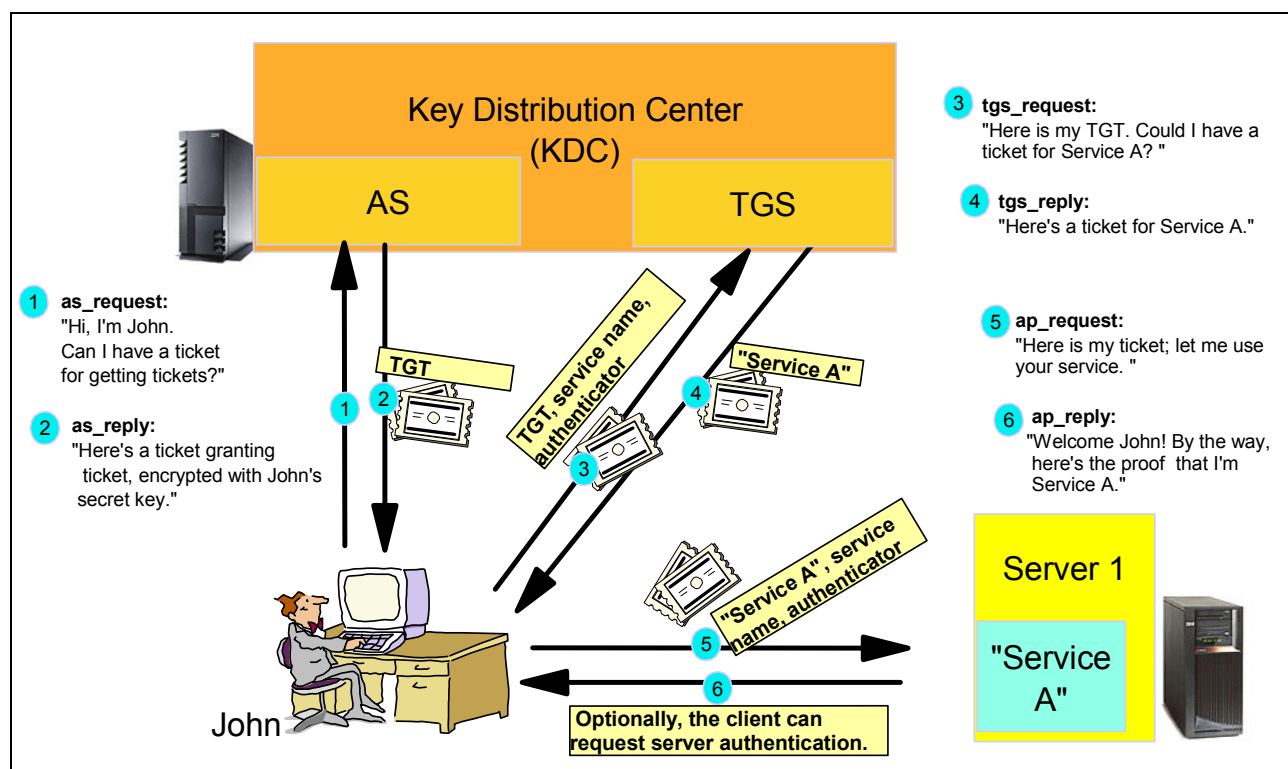


Figure 5-1 Kerberos components: Processing a principal's request and using tickets

5.3.1 Kerberos tickets

Kerberos uses the word ticket to describe how authentication data is transmitted in the Kerberos environment. Tickets are essentially encrypted data structures that use shared keys issued by the KDC to communicate in a secure fashion. Where the ticket has been created from within the KDC defines the purpose of the ticket. When a principal requests the initial authentication the ticket comes from the authentication server (AS), as shown within the Key Distribution Center in Figure 5-1.

This is the ticket granting ticket (TGT), which is used to request other tickets for services in the network. When the principal wants to use a service in the network, the TGT, along with a service request, is sent to the ticket granting server (TGS), as shown in step 3. The TGS responds by issuing a service ticket (ST). The details of creating and issuing tickets is not covered in this book.

In step 5, the server Server1 recognizes the principal as user profile John (with an already validated password indication) and that John wants to use, in our example, an iSeries Navigator session. Assuming there is no OS/400 security or iSeries Access for Windows Application Administration specification to prohibit John from running iSeries Navigator functions, Server1 responds in step 6, indicating “this is Server1,” “John has signed on,” and performs the requested iSeries Navigator function.

Note that Kerberos supports ticket options that give you more control over the use of the tickets. Options in Kerberos Version 5 include:

- Can the ticket be forwarded? For example, this enables passing the ticket on to other back-end services to retrieve information.
- Is the ticket renewable? This forces a ticket with a long lifetime to be renewed periodically from the KDC.

5.3.2 Principals and realms

In order to understand how principal names are generated in Kerberos, you need to understand more about Kerberos realms first. As previously stated, the realm (also called an administrative domain) consists of members, which can be users, servers, services, or network resources and a Key Distribution Center as an authenticating authority. The members are registered within a KDC database. Each of these members has a unique identifier that is called a principal.

Important: The normal conventions of naming Kerberos realms is to create them using uppercase characters.

The three part principal name helps make the principal name a unique identifier within the realm to which the KDC can assign tickets. The three parts of a principal name are described as follows:

- The *primary part* of the principal name can be either the user’s name, the word *host*, or the name of the service. An example of a user principal in the ITSO.IBM.COM realm would be johnprin@ITSO.IBM.COM.

- The *instance component* is optional and normally not used for an individual principal. The instance is used to qualify the primary, for example, if johnprin was the administrator of the KDC database, he would have an additional principal that looks something like johnprin/admin@ITSO.IBM.COM. Note that the principals johnprin and johnprin/admin are two completely separate principals with different passwords and possibly a different set of authorities.

The instance component is also used when specifying a host or a service principal. It is the fully qualified domain name of the host, for example:

```
krbsvr400/as20.itso.ibm.com@ITSO.IBM.COM
```

- The *realm portion* of the principal's name is the name of the Kerberos realm that, as stated previously, is usually the domain name in uppercase.

5.3.3 Key Distribution Center

The Key Distribution Center (KDC) is the heart and brains of the Kerberos realm. Within the KDC there are three primary functional components: the authentication server (AS), a ticket granting server (TGS), and the KDC database, which holds shared secret information about each principal in the Kerberos realm. Because these functions are incorporated into the KDC, and are also linked by the services provided to the principals, they usually reside on the same physical machine.

In most cases, the system providing KDC functions also provides a Kerberos password server, whose functions are included in a later topic in this chapter.

Read the following shaded boxes before continuing in this topic.

Important: An administrator needs to successfully complete the following tasks in order to use Kerberos authentication to iSeries functions (services):

- Configure the Key Distribution Center.
- Enroll Kerberos principals with the KDC.
- Define service principals on the KDC for each iSeries that will use Kerberos authentication.
- Configure each iSeries (using the iSeries Navigator interface to Network Authentication Service) to know the location of the KDC.

Note: OS/400 V5R2 provides participation in a Kerberos realm with authentication support. Through OS/400 V5R2, an iSeries system cannot act as a Kerberos KDC. KDC functions are provided on some Windows and UNIX®-based operating systems, including Linux and IBM operating systems such as AIX® and z/OS®.

KDC functionality is included in Windows 2000 Server and Windows Server 2003.

Some KDC functions might require additional install options on these operating systems.

Because a Microsoft KDC is the most common provider within a Kerberos realm, all information in this book about Kerberos setup is based on Windows 2000 Server and iSeries V5R2 support.

KDC support on an iSeries system is being considered in a future release. Note that IBM plans are subject to change without notice.

The Key Distribution Center database

When a principal is created, a shared secret is generated that only the KDC and the created principal know about. This shared secret is used to encrypt communications between the principal and the KDC. This shared secret is never transmitted in plain text. The KDC database contains all of the principals in the realm and their associated secret keys. There is no requirement that this database reside on the same physical machine that the KDC is on, but it is considered good practice to store the information on the same system.

Functions of the Key Distribution Center

The two primary functions of the KDC are:

- ▶ Grant a ticket granting ticket
- ▶ Grant a service ticket

Receiving a ticket granting ticket

When a principal logs on to either their computer or a *Kerberized* application (such as iSeries Access for Windows) for the first time either that day or since a previous ticket the principal has received has expired, an interaction takes place between the client and the authentication server.

Note: *Kerberized* is the term given to services that use Kerberos for authentication.

In this interaction, the principal sends a request to the AS based on their identity and who they want to talk to; in this case, it is a principal and the TGS. This information is transmitted in plain text. The AS, based on the identity of the principal, builds a ticket granting ticket (TGT), and replies to the principal encrypting the ticket using the shared secret of the principal who requested it. The encrypted ticket can be decrypted by the authentic principal and used to obtain services in the network, such as Telnet or iSeries Navigator, which are Kerberized applications.

There are additional levels of encryption below this level, but they are beyond the scope of this redbook. See *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975, for more information.

Kerberos and network security considerations

Although very secure, the Kerberos protocol is by no means infallible. The protocol might work as it is intended, but there are many outside factors that can greatly impact the Kerberos implementation on a network. Some of these include:

- ▶ Unauthorized access to a client machine. This could lead to users' tickets being copied, and a malicious user could impersonate this user until the tickets expire.
- ▶ Unauthorized access to servers. This could lead to the compromise of all the services that a server would offer. It could also lead to the compromise of Kerberos principals as a higher level of authority could be achieved for users through potential services offered by other machines.
- ▶ Compromise of the KDC. If the KDC is compromised, a malicious user would have full control over the entire KDC. The database of all users' shared secrets would be compromised also, because by default, Kerberos implementations allow root users and Kerberos administrators unencrypted access to the database.
- ▶ Compromise of users' passwords. If a password is divulged to another user by legitimate means or by unauthorized means, that user is compromised. This could be especially severe if it is the Kerberos administrator's password that is divulged.

5.4 Kerberos and Microsoft: Implicit support by Microsoft

As previously discussed, there are Kerberos implementations under Windows and other operating systems. This topic focuses on Microsoft implementations, because, in existing Kerberos realms, this is the most common component providing Kerberos support.

Unknown to many users and administrators, Kerberos is actually implemented in Microsoft Windows 2000 Servers, Windows Server 2003, and Windows 2000 and XP clients. The Kerberos implementation in Windows conforms to the protocol specification as generally described in this book and in internet RFCs.

There are two parts to Kerberos implementation on a Windows *server*. These are the Kerberos full function service and the Active Directory, which is the Microsoft implementation of the Lightweight Directory Access Protocol (LDAP) protocol.

The Windows client workstation must first be enrolled in the Windows domain.

When a user logs on to the enrolled Windows client workstation, the information entered by the user is captured by the Windows logon program and is passed to the computer's Local Security Authority (LSA). The LSA is a Windows component that authenticates users to the local system. The LSA also controls all aspects of local security on a system. This LSA then communicates with the network's KDC in order to receive ticket granting tickets and service tickets so that this user can access Kerberized services on the Windows domain.

Kerberos on a Windows server platform uses the Active Directory for all information about principals on the Kerberos realm. The encryption key used in communicating with principals is stored in the Active Directory database in the user's profile. This password is highly secured, and the password object is only an encryption key derived from the password. In addition, only the person who the account represents can change the password, not even administrators have permission to do this.

Password changes are managed through trusted security programs running in the security context of the LSA. From this, we can see that the Active Directory not only plays the role of an LDAP server on a Windows server, but it is also used as the KDC database. This can be a great benefit to an organization in terms of one central store, but can be equally devastating in the event of a system failure!

5.5 Kerberos commands

Internally, there is a set of commands used to implement Kerberos requests and responses. It is helpful to understand some of the more common commands Kerberos principals can use within a realm. When a command is run, it runs using the principal name of the logged in user.

Here is a list of these common commands:

- ▶ **kinit**: This command authenticates the principal with the KDC and retrieves a ticket granting ticket for that user.
- ▶ **klist**: This command shows a list of all the tickets relating to this principal. The **klist** command is not installed by default in windows; for information about installing this "support tools" command, see "Installing Windows Kerberos support tools" on page 117.
- ▶ **kdestroy**: This command destroys the list of tickets that are available to the local principal.

- **kpasswd**: This command is used to change the Kerberos password for this principal user. This command requires that the kpasswd (kpasswd daemon) service is running on the server. This service is included in Windows 2000 Server and Windows 2003 Server.
- **kadmin**: This command can be used to administer principals on the KDC. It does require the kadmind (kadmin daemon) service to be running on the computer containing the KDC. This service is included in Windows 2000 Server and Windows 2003 Server.

It is worth noting that under the Windows implementation of Kerberos, the **kinit** and **kdestroy** commands are performed for principals “under the covers” of the operating system. In 5.4, “Kerberos and Microsoft: Implicit support by Microsoft” on page 106, we indicate that after the principal logged into Windows, a TGT was obtained. This is done through the **kinit** command that requests TGTs for principals. Similarly, under the covers of the operating system the **kdestroy** command runs when the user logs out of Windows and removes the cache of tickets relating to that user.

The commands listed above are the standard Kerberos commands.

There are additional Kerberos “support tool commands” available under Windows 2000 Server and Windows Server 2003, which run on the Windows command line to support certain Kerberos functions for interoperability between operating systems and Kerberos implementations. Two of the most important of these “additional tools” are:

- **ktpass**: This command is used to allow interoperability between a Windows KDC and non-Windows clients such as UNIX, Linux, or iSeries (iSeries QShell is required to run this command). The command links the name of a principal in the network to the entry in the Active Directory and assigns a password to it. This command would be used more than once when there is some security requirement for a user password to be changed periodically.

You can run the **ktpass** command on the Windows KDC server using either the command prompt window or by selecting the Windows **Start** → **Accessories** → **Command Prompt** interface.

As well as linking principals to accounts, a UNIX-style keytab is also created. This can be transferred to Linux and UNIX machines and is used by the client to communicate with the Windows server.

Important: The **ktpass** command is required to register an iSeries server service as a principal in the KDC, because iSeries Network Authentication Service support uses a UNIX-like implementation of Kerberos processing. This is essentially an authentication to use any iSeries Kerberized application, such as the OS/400 host servers used by iSeries Access for Windows.

There is no requirement to register an iSeries user profile as a principal in the KDC. This is because there is a requirement, for example, to enroll the iSeries Access for Windows PC workstation user as a Kerberos principal. On iSeries systems, EIM is used to map the Kerberos principal to the OS/400 user ID. See 5.6.4, “Setting up an iSeries server to perform Kerberos functions” on page 123 for more information.

From the viewpoint of an iSeries server, the only requirement is the PC workstation’s user ID has to be defined on the iSeries server performing the iSeries Access for Windows function as a normal OS/400 user. This is essentially the same requirement for an iSeries Access for Windows PC workstation user to access the same iSeries server without using Kerberos authentication. The only real difference is that when not using Kerberos to authenticate a user, that user must have a matching password on the iSeries and the PC workstation as well. When using Kerberos from the PC workstation, the KDC provides the user authentication and accepts the service request for user xxxx, who is defined on the iSeries server, as well as on the Windows PC client workstation, and the Windows server Active Directory, KDC system.

In either sign-on process, after the user is considered valid on the iSeries server, normal OS/400 security (and any iSeries Access for Windows Application Administration function) determine exactly which functions under OS/400 this user is authorized to perform.

- **ksetup:** This command can be used to modify the windows registry so that another Kerberos KDC can run on a Windows server. Similar to the **ktpass** command, the **ksetup** command can be run from the command line in either Windows or Linux Kerberos implementations. The command can also be run in a QShell session on the iSeries.

The support tools are not included in the standard Windows installation, but are available from the Windows Server CD.

For information about how to install Kerberos support tools, refer to “Installing Windows Kerberos support tools” on page 117.

Note: V5R2 OS/400 contains a subset of the Kerberos commands discussed here. These commands can be run using the QShell interface. Although running these commands on a iSeries system is not required to make Kerberos work, they can often be used to verify what has been configured and test that the basic Kerberos setup on iSeries is correct.

In this redbook, we use the **keytab list** and **kinit** commands on the iSeries server in 5.6.5, “Verifying Network Authentication Service setup” on page 130.

See the next section for a complete overview of what it takes to set up an operational Kerberos realm with an iSeries Access for Windows client workstation using Kerberos authentication to an iSeries system.

5.6 Setting up an operational Kerberos realm example

The necessary Kerberos realm set up for iSeries Access for Windows requires you to:

- ▶ Enroll the Windows client workstation in the Windows domain. We do not show this in this book, but it is required for Kerberos support to be invoked.
- ▶ Set up the TCP/IP network host name, TCP/IP address resolution, and synchronize the “system time value” on the Kerberos KDC server and all the servers in the Kerberos domain (*realm*) within a Kerberos “time skew” limit.
- ▶ Configure the Key Distribution Center on the Microsoft Windows 2000 or Windows Server 2003 that provides KDC support. We use Windows 2000 Server in examples shown in this book. Note there are other operating systems or products that provide KDC support. For example, a pSeries running AIX can provide KDC support.
- ▶ Enroll Kerberos user principals within the KDC.
- ▶ Define service principals on the KDC for each iSeries that will use Kerberos authentication.
- ▶ Configure the Network Authentication Service (Kerberos support) on each iSeries system participating in the Kerberos realm. This includes identifying the KDC server to the iSeries system.
- ▶ Configure iSeries EIM support on each iSeries system to map between the Kerberos principal name and the OS/400 user ID.
- ▶ Configure iSeries Access for Windows on your PC client workstation to use a Kerberos principal name that represents the Windows user ID.

This section includes a list of software requirements and setup parameters for the KDC server and an iSeries server to support Kerberos requested services. We configured the iSeries Access for Windows PC client workstation to use Kerberos according to Table 5-1 on page 109.

We use the parameters and example values shown in Table 5-1 in our Kerberos realm configuration example in the topics that follow.

This table is based on the table used in the “Configure Network Authentication Service” chapter in the redbook *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975. The Item column characters (A,B, ..., S) are referenced in the topics and steps that follow later in this chapter.

Table 5-1 Example Kerberos and Enterprise Identity Mapping setup worksheet

Item	Information to collect	Result
A	What is the name of the Kerberos default realm to which the iSeries will belong?	ITSO.IBM.COM
B	What is the KDC for this Kerberos default realm?	KrbSvr2000
C	What is your KDC fully qualified host name?	KrbSvr2000.itso.ibm.com
D	What is the port on which the KDC listens?	88
E	What is name of the password server for this KDC?	KrbSvr2000
F	What is the port of your password server?	464
G	What is the password for your iSeries service principal or principals?	win4IBM

Item	Information to collect	Result
<i>The following items will be used to create the iSeries principal on the KDC:</i>		
H	What is the name of the Kerberos principal?	krbsvr400 (When creating the iSeries principal this name must be used; this name has been defined by iSeries development to uniquely represent an iSeries principal.)
I	What is your iSeries host name?	as20
J	What is the fully qualified host name of the iSeries?	as20.itso.ibm.com
K	What is the name of the Kerberos default realm to which the iSeries server belongs? (Default: domain name converted to uppercase)	ITSO.IBM.COM
L	What is the full name of the Kerberos principal? (krbsvr400/fully.qualified.host.name@YOUR.KERBEROS.REALM) Note: For iSeries, the service principal/host name is always forced to lowercase. Therefore, the fully qualified host name must always be entered in lowercase.	krbsvr400/as20.itso.ibm.com@ITSO.IBM.COM
M	What is the password/shared secret for this principal? (Must be the same as item G.)	win4IBM
<i>The following items will be used to configure Enterprise Identity Mapping (EIM):</i>		
N	Which type of basic EIM configuration do you want to create on your iSeries system? ► Join an existing domain ► Create and join new domain	Create and join new domain
O	Where do you want to configure your EIM domain, or what EIM domain you want to join?	as20.itso.ibm.com
P	What is the name of the EIM domain you want to create or join?	ITSO EIM
Q	Do you want to specify a parent DN for the EIM domain? If yes, specify the parent DN.	NO
R	What is the administrator distinguished name (DN) on the LDAP server that will be used as the EIM domain controller?	CN=administrator
S	What is the administrator password on the LDAP server that will be used as the EIM domain controller?	ldappw

5.6.1 General TCP/IP network host name resolution considerations

For Kerberos (and EIM) to properly work on your network, you must ensure a reliable IP address/host name resolution process. One of the reasons that this is important is that Kerberos is case sensitive, and the Domain Name System (DNS) process is not.

The simplest method to minimize problems in this area is use a DNS server on your network. A DNS server can be implemented on a variety of platforms, including an iSeries server. For

detailed information about implementing a DNS on iSeries, see Chapter 8 in the redbook *iSeries IP Networks: Dynamic!*, SG24-6718.

In order to determine how your iSeries host name should be resolved, you need to check your iSeries system's Host Domain properties as seen in Figure 5-2 on page 111, using an iSeries Navigator session. Select your **system** → **Network** → **TCP/IP Configuration** → **Properties**.

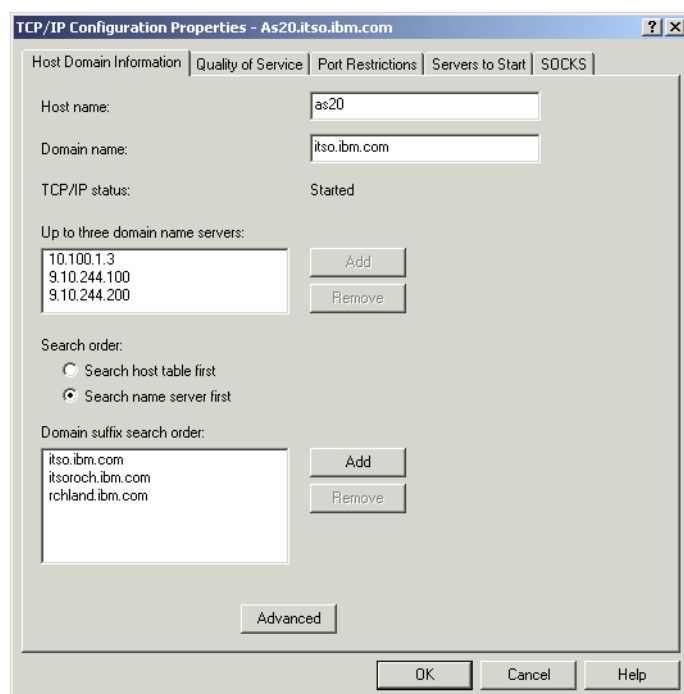


Figure 5-2 iSeries host domain information

Note the host and domain name shown in Figure 5-2. Also notice that the iSeries server has an ordered list of IP addresses for DNS servers. In our network, we used one of these IP addresses as the DNS server for the PC workstations that want to use Kerberos to get to this iSeries server.

You now need to verify how this system's iSeries name is being resolved in the network so that Kerberos-based transmissions can be successful. Here are two ways to do this:

1. The iSeries host name can be resolved on the client PC workstation itself. This is done using a host entry for the iSeries server in the PC *hosts* file. In Windows 2000, this file is located at C:\WINNT\system32\drivers\etc\hosts. On a Windows XP workstation, the file can be found at C:\WINDOWS\system32\drivers\etc\hosts.

Open the file using the appropriate path for your PC operating system and verify whether the iSeries host name and correct IP address is listed. If so, make note of the name (including uppercase and lowercase characters) and the IP address associated with it. If the file does not exist, or there is no entry for the iSeries, we suggest that you go to the next way to verify the correct iSeries host name: using a DNS server.

You can enter the iSeries host name and associated IP address on the PC workstation in a hosts file. However, as we discuss in this book, we recommend that you use a Domain Name System (DNS) server as described in the second verification technique that follows.

2. The iSeries name can be resolved by a DNS server in your network. To determine how the DNS server is resolving the host name, we have to do an NSLOOKUP (Name Server Lookup). On your PC workstation, open a Windows command prompt window by clicking **Start** → **Run**, and then typing command when prompted. This opens the command window. Enter NSLOOKUP, followed by the IP address of the iSeries.

Note the host name that is returned, including the case of each of the characters (uppercase or lowercase). To verify that the DNS record is complete, run the NSLOOKUP command again. This time substitute the returned host name from the preceding NSLOOKUP.

If the IP address returned is different than the one you used in the first NSLOOKUP, you will need to contact the administrator of the DNS to correct the record.

Tip: Either verification technique will work, but the DNS server method provides a more reliable, easier to manage solution to your name resolution. Using DNS gives you a single point to manage your name resolution, rather than having to make host entries in the hosts file on each of the workstations or systems in your network.

If the host name that has been used is an exact match with what you saw in Figure 5-2 on page 111, your resolution will satisfy the Network Authentication Service and Kerberos requirements. If not, you can change either your iSeries host name and domain name to the value returned by the NSLOOKUP function, change the value found in the PC workstation's hosts file, or change your DNS server to resolve to the name listed in the Host Domain Information window.

We offer the following if you decide to make the change on the iSeries server. You need OS/400 *IOSYSCFG and *ALLOBJ special authorities to make the changes we describe here.

In a 5250 session to your iSeries server, enter the Configure TCP (CFGTCP) command and then select option 12 (Change TCP/IP domain information). Press PF11 to show the keywords for each parameter. Enter the correct uppercase and lowercase text for your host name and domain information. Use the single quote (') character around each of your entries. This enables the uppercase and lowercase characters to be saved exactly as you entered them, as shown Figure 5-3 on page 113.

```

Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . HOSTNAME      'as20'

Domain name . . . . . DMNNAME      'itso.ibm.com'

Domain search list . . . . . DMNSCHLIST      'itso.ibm.com itsoroch.ibm.com
rchland.ibm.com'

Host name search priority . . . HOSTSCHPTY      *LOCAL
Domain name server:          INTNETADR
Internet address . . . . .      '10.100.1.3'
                                '9.yy.244.100'
                                '9.yy.244.200'

Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display   F24=More keys

```

Figure 5-3 Configure the host and domain name to match the DNS resolution

Remember, when changing the host or domain name on this screen, that DNS is case *insensitive* (uppercase and lowercase characters are equivalent), but Kerberos is case sensitive.

Note also that the iSeries Access for Windows client Kerberos code will automatically (with Service Pack SI09808 or later) lowercase the internal Kerberos fully qualified host name command before asking for the service ticket.

Later in 5.6.5, “Verifying Network Authentication Service setup” on page 130, we perform a test using our example as20.itso.ibm.com in a Kerberos **kinit** command to attempt to get a ticket from the KDC, as shown in Figure 5-22 on page 134.

Tip: One way to identify a possible name resolution problem when attempting to use Kerberos is getting the message “CWBSY1017 - rc=608 Kerberos credentials not valid on server...” This means that host names are not being resolved correctly (server side). Another error message, “CWBSY1012 - Kerberos principal not found on server...”, usually means that you have a name resolution problem on your client. For detailed iSeries-related Kerberos problem determination assistance, see *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.

5.6.2 Coordinating the time used on all network servers

When using Kerberos for network authentication in your network, setting the time and time zone values on all your servers is an absolute requirement. Kerberos protocol uses time stamps and time skew (difference in time values) as part of its security implementation. The maximum time skew allowed by default in Kerberos is 300 seconds (five minutes). If your server is outside this maximum skew, Kerberos authentication will fail.

On all servers, the time value, time zone, and time skew values are configurable. The time skew can be raised to a maximum of 900 seconds in the iSeries Network Authentication Service configuration, which we describe later in this chapter.

The following iSeries time and time zone system values need to be checked and synchronized with the rest of your network:

- ▶ QTIME
- ▶ QUTCOFFSET: The Coordinated Universal Time Offset from Greenwich mean time

Before synchronizing service times in the network (corresponds to OS/400 QTIME system value), set the iSeries QUTCOFFSET system value according to your time zone.

You can synchronize the system times on servers within the Kerberos realm by changing the KDC time using the Windows operating system date and time interface and the QTIME system value to change the iSeries system time.

However, to keep system times in a network synchronized more easily, we recommend that you set up a Simple Network Time Protocol (SNTP) server in your network (not an iSeries system).

SNTP allows multiple systems to base their time on a single time server.

On a Windows system, you can use NET HELP TIME from a DOS command window to access SNTP set up.

To set up the iSeries to get its time from an SNTP server, use one of the following interfaces to the iSeries server's SNTP client support:

- ▶ Enter the Change Network Time Protocol Attributes (CHGNTPA) command in a 5250 session.
- ▶ Using an iSeries Navigator session, click **system** → **Network** → **Servers** → **TCP**. All the TCP servers are displayed in the right pane. Right-click the SNTP client server and select **Properties**.

SNTP client support on an iSeries is included in no charge OS/400 5722-TC1 (must be installed) as a client service. We show an iSeries Navigator example, starting with the SNTP client server Properties panel shown in Figure 5-4 on page 115.

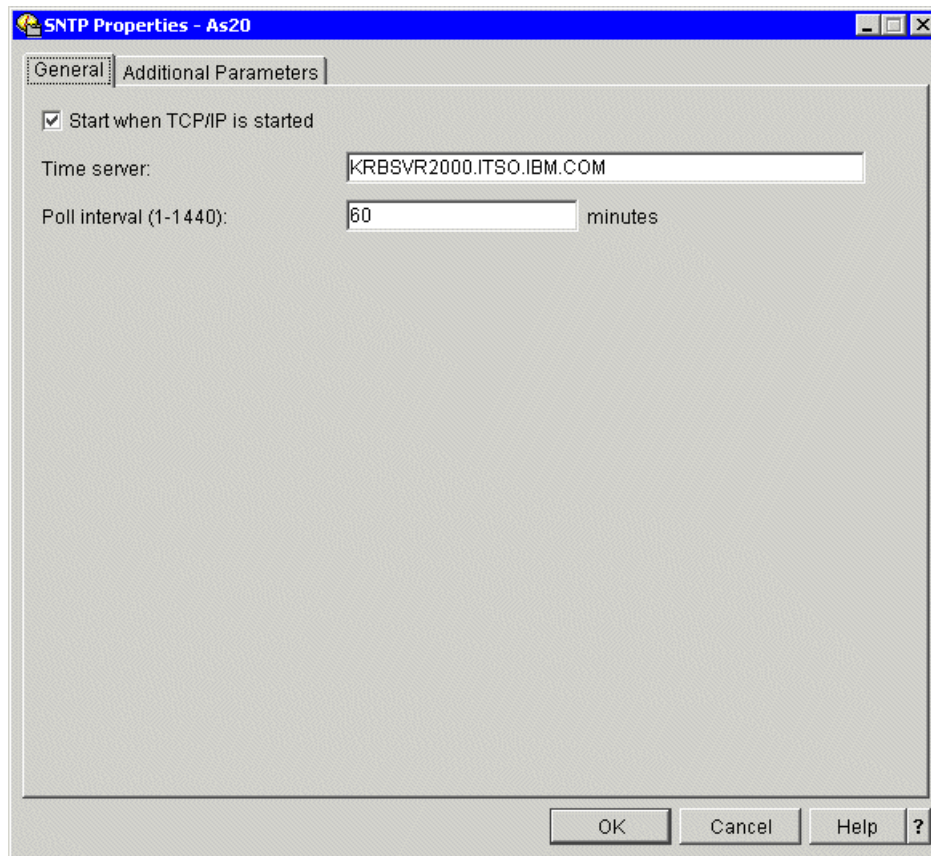


Figure 5-4 SNTP configuration on an iSeries system

Enter the fully qualified name of a SNTP server in your network into the Time server field. This could either be an external (Internet) SNTP server, your Windows server's Active Directory support, or any other SNTP server. In our example network, we used the same Windows system on which the KDC resides. The default Poll interval is 60 minutes, which is satisfactory for most implementations. The other Additional Parameters properties are not shown in this book

Click **OK** to continue.

Whenever you are changing the SNTP properties using either the CHGNTPA command or the iSeries Navigator interface, we recommend that you stop (if active) and start the iSeries SNTP server job. This can be done using either of the following methods:

- ▶ From a 5250 session, use:
`ENDTCPSVR SERVER(*NTP)`
 Followed by:
`STRTCPSVR SERVER(*NTP)`
- ▶ From an iSeries Navigator session, click **system** → **Network** → **Servers** → **TCP**. Right-click the SNTP client server and select **Stop** and then **Start**.

Using our iSeries Navigator properties example, the iSeries SNTP client server will now poll the SNTP server every 60 minutes and adjust its software clock.

For a network of iSeries systems, consider an initial step to synchronize their system time (QTIME) and QUTCOFFSET values by using an iSeries Navigator session Management Central interface described as follows.

Define a Management Central system group of the iSeries systems whose time values you want to synchronize. Right-click this system group name and select **System Values** → **Synchronize Date and Time**. A model iSeries system, specified by you, is used as the source for the system time value, the system Universal Time Coordinated Offset value, and the system date value that are sent to the target systems in the defined system group.

This Management Central support includes scheduling the time synchronization and has options that include specifying what to do if each target system in the system group also has the Simple Network Time Protocol (SNTP) server active.

5.6.3 KDC server setup

On this server, you create, manage, and delete realms and principals. We assume that the KDC server is running a Windows operating system with the following requirements:

- ▶ Windows 2000 Server or Windows Server 2003 and the “necessary Kerberos support tools” are installed on this machine.
- ▶ An administrator needs to have successfully completed the following tasks in order to use Kerberos authentication to iSeries functions (services):
 - Configure the Key Distribution Center.
 - Enroll Kerberos user principals (such as a Windows 2000 client workstation user) with the KDC.
 - Define service principals on the KDC for each iSeries that will use Kerberos authentication. We show this later in this book.
- ▶ The Kerberos KDC service is running. You can manage this on your Windows 2000 Server by selecting **Programs** → **Administrative Tools** → **Component Services**. Check that the Kerberos KDC service (part of Services (Local)) is Started, as shown in Figure 5-5.

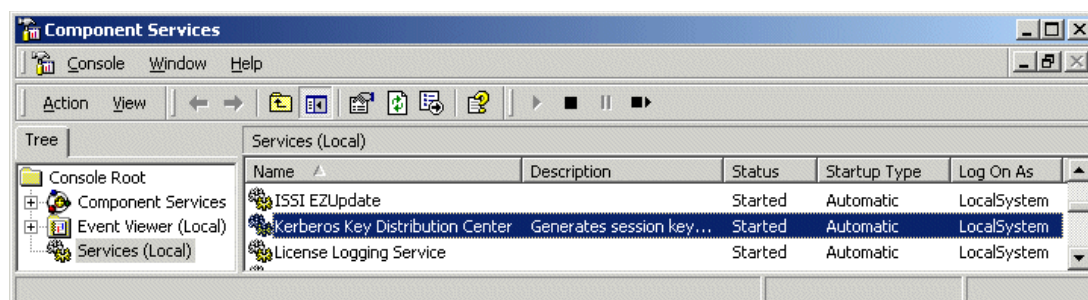


Figure 5-5 Checking the Windows Kerberos KDC service

- ▶ You have Windows Active Directory active. We assume that you have already defined users that will be used as Kerberos principals.

You can manage users by selecting **Programs** → **Administrative Tools** → **Active Directory Users and Computers** and then select **Users**. In Figure 5-6 on page 117, we show a number of users within the Active Directory. In this book, we use the user Description column text “Kerberos User” to illustrate user principals already created.

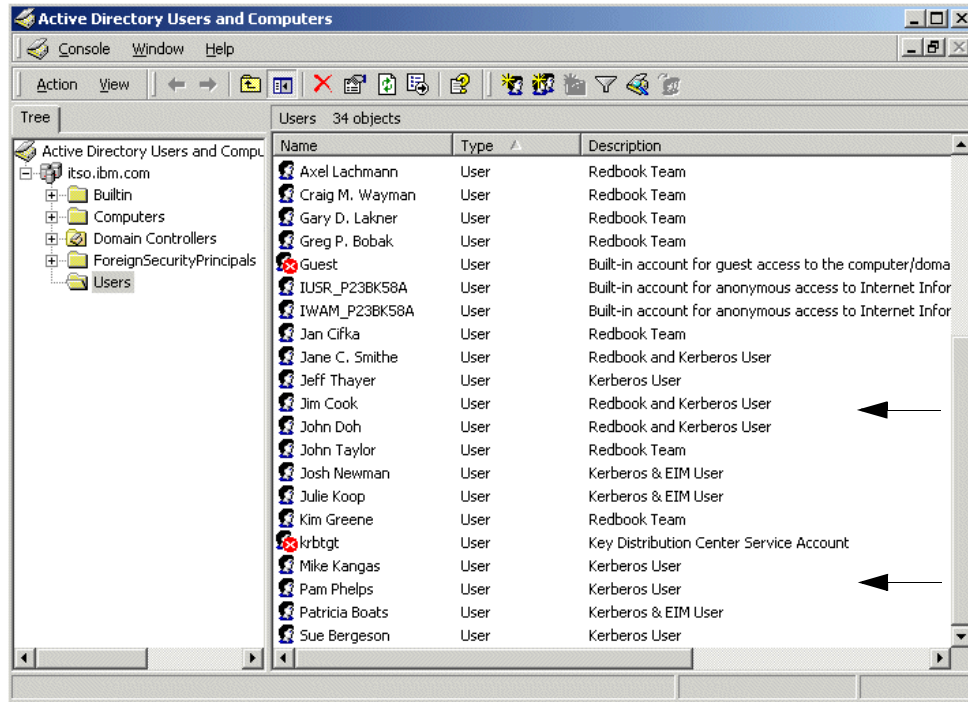


Figure 5-6 Windows Active Directory: Showing users

If the Kerberos KDC is not started or the Active Directory is not populated by your users, you are not using Active Directory. Go to the Microsoft Active Directory home page for more information about configuration, available at:

<http://www.microsoft.com/windows2000/technologies/directory/AD/default.asp>

Important: If you are unfamiliar with Active Directory, do not attempt to set it up in a production environment without first reading about the implications at this Web site.

Each user that will connect to the iSeries and iSeries applications needs a user ID defined in the Windows server's Active Directory and enrolled in the server's Kerberos KDC as a user principal.

We previously discussed Windows Kerberos support tools that might not have been installed by default when installing the Windows server code. Some of these tools are necessary for acceptable management of a Kerberos realm using a non-Windows operating system. In the next topic, we explain how to install them on a Windows operating system.

Installing Windows Kerberos support tools

The Windows Kerberos support tools typically need to be explicitly installed. Follow these steps to install the necessary Windows 2000 Server Kerberos support tools. The steps for installing these Kerberos support tools on other Windows operating systems would be similar.

1. Place the Windows 2000 Server CD into the CD-ROM drive on the server.
2. Navigate to the CDROM\Support\Tools directory.

The window you see should look similar to the one shown in Figure 5-7.

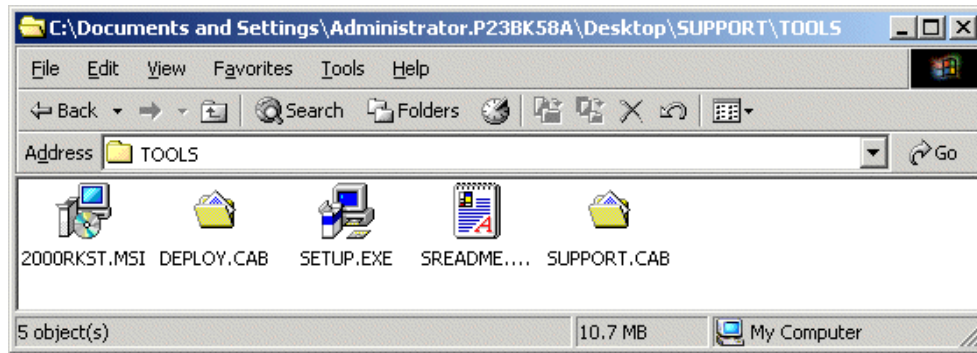


Figure 5-7 Windows 2000 Server support tools directory

3. Double-click **setup.exe**, and follow the default installation instructions until the support tools are installed.

Verifying successful support tools and support tools path installation

We recommend that you verify that the specific support tools have been installed. Because the function **ktpass**, as described in “Associating the iSeries account with the Kerberos principal” on page 121, is an important tool, we show using the Windows file search function to verify that the **ktpass** command has been installed in the following steps:

1. Click the **Start** button in the lower-left corner of the window.
2. Select **Search** and then **Files and Folders**.
3. In the Search for files or folders named field, enter **ktpass**.
4. Make sure that the **Look in** field holds the value of the drive where the operating system is installed.
5. Click **Search Now**.

The search results should return a reference to the **ktpass** command stored in C:\Program Files\Support Tools, as shown in Figure 5-8.

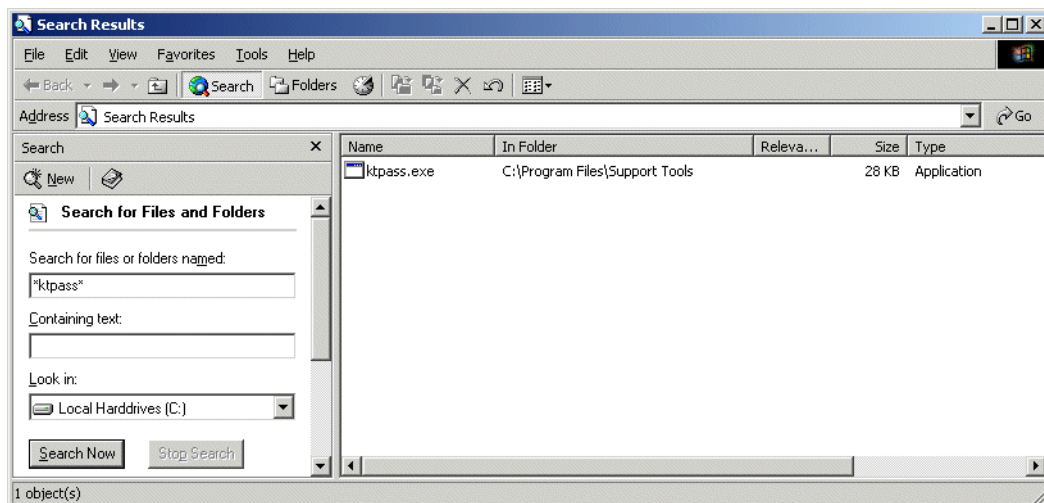


Figure 5-8 Search results for the **ktpass** command on your Windows KDC server

It is also important to verify the Support Tools directory is in the Windows operating system's Path Environment Variable. Follow these steps:

1. Right-click **My Computer** and then click **Properties**.
2. Click the Advanced tab at the top of the window.
3. Then, click **Environmental Variables**.
4. In the System Variables, scroll to the **Path** variable and click **Edit**.

The value should be C:\Program Files\Support Tools\, as shown in Figure 5-9.

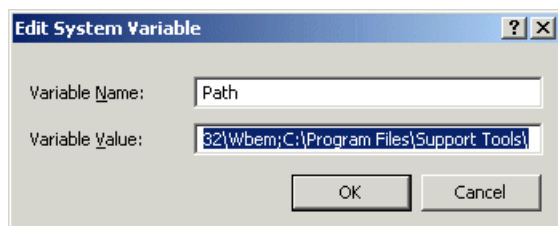


Figure 5-9 Path environment variable showing Support Tools

Setting up the iSeries principal name on the KDC

Your next task is to create a Kerberos principal for your iSeries system. This allows the iSeries to take part in the Kerberos realm for the authentication of the users.

You perform these steps:

1. Create an Active Directory account for your iSeries system.
2. Associate the account with the Kerberos principal using the **ktpass** command.
3. Check and complete the Active Directory account.

Creating an Active Directory account for your iSeries server

We do not show the entering of the user principals, such as johnprin, discussed in 5.3.2, "Principals and realms" on page 103. This has to be done, but it is basic and not covered here.

In this topic, we do describe the required creation of a user account for your iSeries system itself in the Active Directory.

To create an Active Directory account:

1. At the console of your Windows 2000 Server, click **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**. This opens the Active Directory Users and Computers window.
2. Right-click the **Users** folder in the left pane, and select **New** → **User**. This opens the New Object - User window.
3. In the New Object - User window (Table 5-1 on page 109), enter the name of the Active Directory account you are creating (item J in Table 5-1). Although this name might be arbitrary, we recommend that you use the name of your iSeries system.
 - Enter this name in the Full name field.
 - Enter host name (item I in Table 5-1 on page 109) in the User logon name field; it is automatically copied in the pre-Windows 2000 name field.

The name of the account (we use as20 in our example) can be entered in lowercase, uppercase, or mixed case as desired. This holds true for the left part of the User logon

name also, because we use the **ktpass** command later, which will change it. You don't need to fill in the First name, Last name, and Initials.

4. For the second part of the User logon name field, leave the default (here @ITS0.IBM.COM) in the combo box on the right of the User logon name. It is the default Kerberos realm name for the Active Directory, prefixed with the @ sign. By default, it is the domain name of the server *converted to uppercase*.

Important: The Windows 2000 KDC is case sensitive, and the name of the Kerberos realm is always in uppercase.

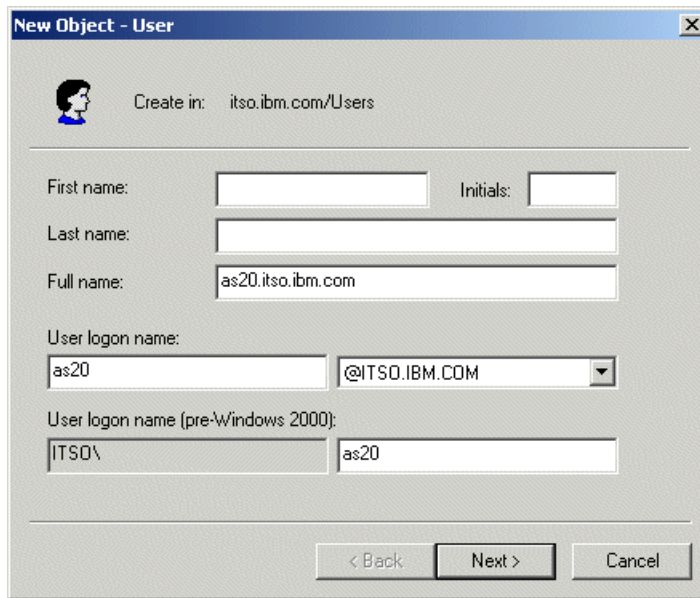


Figure 5-10 Enter the name of the Active Directory account

5. Click **Next** to proceed to a second New Object - User window, as shown Figure 5-11. In this window, you are prompted to enter the password and make several password policy decisions. The password is the *Kerberos shared secret* that you will also enter in the iSeries Network Authentication Service configuration wizard, discussed later in this chapter. The value entered must correspond to item M in Table 5-1 on page 109. You have to enter it twice for verification, because it is not displayed.

Suggestion: Depending on your internal policies for passwords, you might want to select the **User cannot change password** and **Password never expires** attributes to prevent the account getting locked either by human error or by a password change policy being applied to it.

We do not expand on these considerations in this redbook.

Figure 5-11 Fill in the Kerberos shared secret

6. Click **Next**, and then **Finish** in the next window.

Associating the iSeries account with the Kerberos principal

Unlike the Windows clients, the Network Authentication Service on an iSeries system uses UNIX-type services of the Kerberos implementation in Active Directory. Therefore, you need to use the **ktpass** command to modify the Active Directory account that creates an associated Kerberos principal.

Note: The **ktpass** command is a part of the Support Tools included on the Windows 2000 Server installation CD. If the **ktpass** command is missing from your Windows 2000 Server, you must install it as described in “Installing Windows Kerberos support tools” on page 117.

To associate the iSeries account with the Kerberos principal:

1. Open the Windows 2000 Server command window and enter the **ktpass** command, as shown in Figure 5-12 on page 122.
2. You substitute your own values, using as our example, entries L, I, and M from Table 5-1 on page 109:
 - princ = item L (full name of Kerberos principal)
 - mapuser = item I (iSeries host name)
 - pass = item M (password/shared secret for this principal)

Note: The **-mapOp** set parameter used in Figure 5-12 is optional. This option overwrites the existing principal mapping with the new one and is particularly useful when you think you made a mistake. The **Op** portion of the command is an uppercase O, not a zero.

```
C:\>ktpass -princ krbsvr400/as20.itso.ibm.com@ITS0.IBM.COM -mapuser as20 -pass win4IBM
-mapOp set

Successfully mapped krbsvr400/as20.itso.ibm.com to as20.
Key created.
Account has been set for DES-only encryption.
C:\>
```

Figure 5-12 Entering the ktpass command

Checking and completing the Active Directory account

To check and complete the Active Directory account:

1. On the Windows server window in the right pane of the Active Directory Users and Computers window, right-click your account and select **Properties**. In the Properties window, click the Account tab to see the changes made by the **ktpass** command you just issued. Figure 5-13 on page 122 shows an example of the iSeries Account properties.
2. In the Account options area in this Account properties panel, scroll down until you see the option **Account is trusted for delegation** item, as shown in Figure 5-13. You need to explicitly select this check box.

Trusting the account for delegation allows the iSeries system to forward its service tickets to other services internal to the iSeries, such as QFileSrv.400, DRDA, PC5250, and the host servers used by iSeries Navigator.

Note also, that Service principals must be trusted for delegation for single signon (when using EIM support).

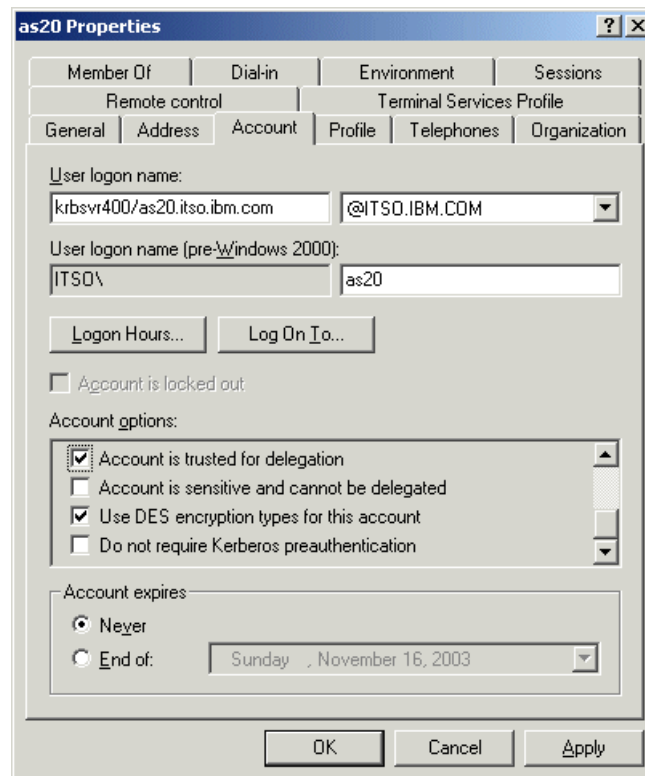


Figure 5-13 iSeries Kerberos Account Properties

3. Click **OK**. You have now completed the Windows 2000 Server portion of the setup.

5.6.4 Setting up an iSeries server to perform Kerberos functions

Setting up an iSeries server to accept Kerberos authenticated tickets requires some base OS/400 software options to be installed, the target user ID defined as an OS/400 user, and appropriate configuration of iSeries Network Authentication Service, which is done through an iSeries Navigator interface.

iSeries V5R2 Kerberos support is based on:

- ▶ Kerberos Version 5 protocol Request for Comment (RFC) 1510
- ▶ Many of the de facto standard Kerberos protocol APIs prevalent in the industry today
- ▶ Generic Security Service (GSS) APIs as defined by RFCs 1509, 1964, and 2743

Network Authentication Service, which is part of OS/400, interoperates with authentication, delegation, and data confidentiality services and is compliant with these RFCs and other products, such as Microsoft Windows 2000 Security Service Provider Interface (SSPI) APIs.

The following iSeries V5R2 “services” or “applications” are enabled for Kerberos:

- ▶ OS/400 host servers
- ▶ iSeries NetServer
- ▶ 5250 Telnet
- ▶ Structured Query Language (SQL)/Distributed Relational Database Architecture™ (DRDA®)
- ▶ JDBC/ODBC
- ▶ Distributed Data Management (DDM)
- ▶ QFileSvr.400
- ▶ HTTP (Powered by Apache)

Note: Enabling an iSeries HTTP server Powered by Apache to accept Kerberos authentication is supported by some V5R2 PTFs that became available during late 2003. Refer to the iSeries Internet Support Web site for more details.

- ▶ LDAP

Important: Note that OS/400 V5R2 supporting Kerberos authentication does not mean every “client” connecting to the iSeries server to use one of the listed functions (services) supports Kerberos authentication. For example, iSeries Access for Windows PC5250 supports initiating a session using Kerberos and Version 8 of Host on Demand supports initiating a session using Kerberos. PC5250 uses the OS/400 Telnet server.

However, at the time of writing this redbook, neither the IBM Personal Communications product supporting 5250 emulation nor earlier releases of Host on Demand support initiating a session using Kerberos authentication.

iSeries system software required

This redbook is based on V5R2 OS/400 and iSeries Access for Windows, 5722-XE1, installed on your iSeries system, which come with built-in Kerberos capability. The following V5R2 OS/400 options must be installed:

- ▶ 5722-SS1 Option 12 OS/400 - Host Servers
- ▶ 5722-SS1 Option 30 OS/400 - QShell Interpreter
- ▶ 5722-AC3 Cryptographic Access Provider 128-bit for AS/400
- ▶ 5722-CE3 Client Encryption 128-bit (optional for client-side encryption)

- ▶ 5722-DG1 IBM HTTP Server for iSeries (optional, not for iSeries Access for Windows functions covered in this book)
- ▶ 5722-XE1 iSeries Access for Windows
- ▶ 5722-TC1 - TCP/IP Connectivity Utilities for iSeries

Setting up iSeries system user IDs and home directories

Each PC client workstation user using Kerberos authentication must be defined as a Kerberos principal. We discuss this in 5.6.3, “KDC server setup” on page 116.

On the target iSeries system or partition, an OS/400 user profile must be defined that corresponds to the incoming Kerberos principal. EIM on the iSeries maps the incoming Kerberos principal to an associated OS/400 user.

When an iSeries system is functioning only as a target for a Kerberos authenticated principal, there is no requirement for the mapped to OS/400 user to be defined as a Kerberos principal. However, if an OS/400 user initiates a connection to another system using Kerberos, then that OS/400 user has to be defined as a Kerberos principal to the KDC.

Note also that any iSeries “user” requesting a Kerberos ticket requires an associated home directory on that iSeries server. That directory is used to contain the user’s Kerberos credentials’ cache.

To create a home directory for an OS/400 user that would initiate a request for a Kerberos ticket, enter the following using a 5250 session:

```
CRTDIR '/home/username'
```

Where *username* is the iSeries user ID (and the Windows client workstation user ID).

For example, John N Smith has user ID Johns:

```
CRTDIR '/home/Johns'
```

Repeat the Create Directory command for each OS/400 user that is to be a Kerberos principal who requests a Kerberos ticket from this iSeries system.

If no OS/400 users on your target iSeries system will be acting as a Kerberos principal and requesting a ticket, you still need a minimum of one home directory, the one representing the iSeries system itself. For this directory, you must specify:

```
CRTDIR '/home/krbsvr400/'
```

This directory is required to store the Kerberos credentials for the iSeries server.

Now, you need to set up iSeries Network Authentication Service on the iSeries.

Setting up iSeries Network Authentication Service

To start the iSeries Navigator Network Authentication Service wizard on your client workstation, you must have the iSeries Navigator Security component installed on the client workstation. The iSeries Navigator Security component is not required on a workstation that initiates an iSeries Navigator session using Kerberos authentication.

On the workstation you use to set up Network Authentication Service, perform the following steps:

1. In the left pane of the iSeries Navigator, expand your **iSeries system** → **Security**. Right-click **Network Authentication Service** and select **Configure**.

Note: If you see the **Reconfigure** option instead of **Configure**, it indicates that the Network Authentication Service has already been configured. You can either reconfigure it (the reconfiguration proceeds in a similar way to configuration), or you can right-click Network Authentication Service and select **Properties** to verify that the current configuration is appropriate for your network.

2. The Network Authentication Service configuration wizard welcome window opens. Read the information, and click **Next**.
3. In the Specify Realm Information window (Figure 5-14), enter the name of the realm that serves as your default Kerberos realm. This is item A in Table 5-1 on page 109. Click **Next**.

Note: The Windows 2000 KDC is case sensitive, and the name of the realm is always in uppercase. Under standard conventions, the name of the realm is the domain name, converted to uppercase.



Figure 5-14 Network Authentication Service Configuration - Specify Realm Information

4. In the Specify KDC Information window, Figure 5-15, enter the following:
 - The fully qualified host and domain name of your Kerberos Key Distribution Center (KDC). This is item C in Table 5-1 on page 109.
 - The default port for Kerberos is 88. Unless your KDC has been configured to listen on a port other than the default, this parameter does not need to be changed. Item D in Table 5-1 is the value that should be entered.

Click **Next**.

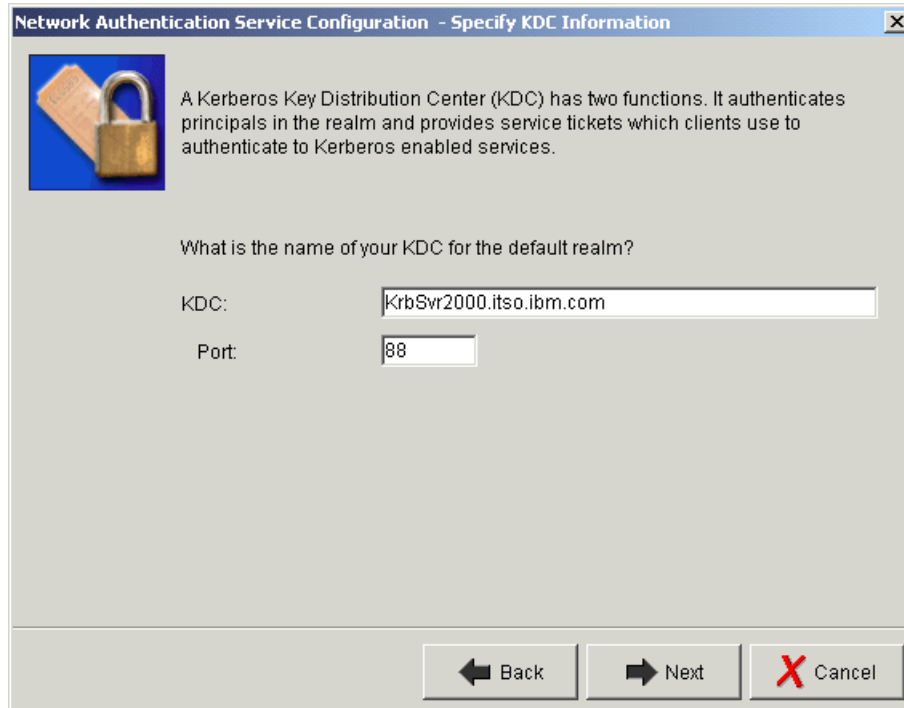


Figure 5-15 Network Authentication Service Configuration - Specify KDC Information

5. The next window (Figure 5-16 on page 127) gives you the option to allow principals to change the Kerberos passwords remotely. If you want to allow clients to change passwords, select **Yes** in the Specify Password Server Information window. After selecting **Yes**, fill in the required fields:
 - Specify the fully qualified name of your Windows 2000 Server as the name of the password server, item E in Table 5-1 on page 109.
 - Leave the default port number 464 unchanged, unless you know that your Windows 2000 Server has been configured differently. This is item F in Table 5-1 on page 109.Click **Next**.



Figure 5-16 Network Authentication Service Configuration - Specify Password Server Information

6. The Create Keytab Entry (for a keytab file) window (Figure 5-17 on page 128) lets you select which services on your iSeries the wizard should enable for Kerberos authentication. In our scenario, we only enable the iSeries Kerberos Authentication, as shown in Figure 5-17. By default, nearly all OS/400 services, except LDAP and NetServer, are enabled for Kerberos by going through this wizard.

Read this wizard window text of a keytab file definition.

Important: Both LDAP and iSeries NetServer can use Kerberos tickets to authenticate, while only NetServer can take advantage of EIM. If your current plans are to enable NetServer and LDAP for Kerberos authentication, it might save you some time to check the boxes in this step.

We do not follow that path for these two “additional services” in this chapter. However, if you checked LDAP and NetServer, you would see two additional windows that would prompt you for the passwords for the LDAP principal and the NetServer principal.

If you choose these options, be sure you document those passwords, because you will need to supply them in the KDC configurations. See the redbook *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975, for how to enable NetServer for Kerberos authentication (and EIM usage).

In our example, select only the **iSeries Kerberos Authentication** check box, and then click **Next**.



Figure 5-17 Network Authentication Service Configuration - Create Keytab Entry

7. In the Create iSeries Keytab Entry window (Figure 5-18 on page 129), specify the password for the Kerberos principal, that is, its *shared secret*. This is item G in Table 5-1 on page 109. Enter it twice for verification because it is not displayed.

Note: In Figure 5-18, the Create iSeries Keytab Entry window shows two important items:

- ▶ The path to the keytab file which the wizard is to generate (next to the Keytab label).
- ▶ The name of the corresponding Kerberos principal in the KDC (next to the Principal label).



Network Authentication Service Configuration - Create iSeries Keytab Entry

Multiple iSeries services, including iSeries Access for Windows, will utilize the following Kerberos service principal to do client authentication.

What password will be used for the service principal? This password must be the same password entered for this principal on the KDC.

Keytab: /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab

Principal: krbsvr400/as20.itso.ibm.com

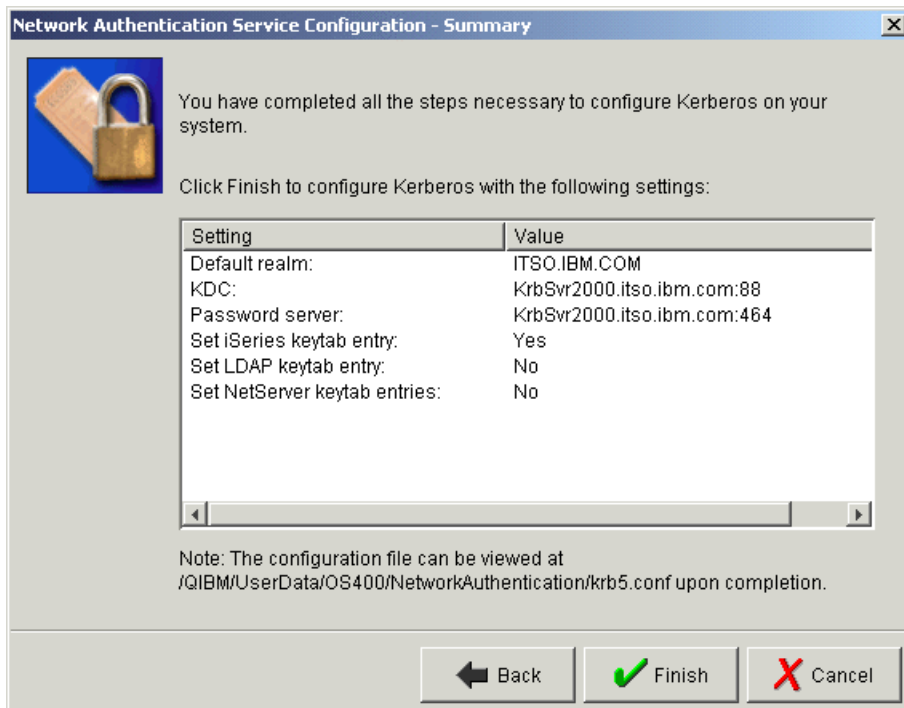
Password:

Confirm password:

Back Next Cancel

Figure 5-18 Network Authentication Service Configuration - Create iSeries Keytab Entry

8. Click **Next**. The final step is to verify the entries in the Configuration Summary window (Figure 5-19). Review the setting values and the note text on the bottom of the window. Use the Back button if you need to go back and make any changes. When satisfied with all the setting values, click **Finish**.



Network Authentication Service Configuration - Summary

You have completed all the steps necessary to configure Kerberos on your system.

Click Finish to configure Kerberos with the following settings:

Setting	Value
Default realm:	ITSO.IBM.COM
KDC:	KrbSvr2000.itso.ibm.com:88
Password server:	KrbSvr2000.itso.ibm.com:464
Set iSeries keytab entry:	Yes
Set LDAP keytab entry:	No
Set NetServer keytab entries:	No

Note: The configuration file can be viewed at /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf upon completion.

Back Finish Cancel

Figure 5-19 Network Authentication Service Configuration - Summary

Your new realm should now be in the right pane of iSeries Navigator. You might need to refresh the contents of the window using the F5 key.

5.6.5 Verifying Network Authentication Service setup

You have completed two steps needed to implement Network Authentication Service authentication of users on your iSeries system:

- ▶ Network Authentication Service is now set up on the iSeries system.
- ▶ The KDC of your Windows 2000 Server contains a Kerberos service principal for your iSeries system.

Remember that you must have previously assured a Windows client workstation's user ID is contained in the Windows server's Active Directory, as discussed in the beginning of 5.6.3, "KDC server setup" on page 116. This becomes associated with an Kerberos user principal in the KDC that will be used when connecting to iSeries server (without user ID and password prompting).

You should now check that these two components cooperate. The steps described in this topic are not required for the Network Authentication Service to work. However, by performing these steps, you confirm that the Kerberos environment for use with your iSeries system is working correctly.

Note: In order to verify Network Authentication setup, you need to have created a directory on the target iSeries server representing the principal for the iSeries server itself. This is discussed in "Setting up iSeries system user IDs and home directories" on page 124.

We verify this setup by running the `kinit` command in an OS/400 Qshell session within a 5250 workstation session.

OS/400 V5R2 comes with the necessary Kerberos commands to verify this setup.

To verify the Network Authentication Service setup:

1. Start the QShell Interpreter in a 5250 session to your iSeries system by entering the OS/400 Start QShell command in either of the following two formats:
 - `qsh`
 - `strqsh`
2. Use the following QShell command to list the current keys in the Kerberos key tab file (key table):

```
keytab list
```

An example of the output is shown in Figure 5-20 on page 131.

If the wizard completed correctly and made contact with the KDC, the key table should contain three entries for the `krbsvr400` principal (at different encryption levels). If you don't see the entries, or they appear to be incorrect, you should go to the "Troubleshooting" appendix in *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.

QSH Command Entry

```
$
> keytab list
Key table: /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab

Principal: krbsvr400/as20.itso.ibm.com@ITS0.IBM.COM
  Key version: 1
  Key type: 56-bit DES
  Entry timestamp: 2003/11/10-17:23:35

Principal: krbsvr400/as20.itso.ibm.com@ITS0.IBM.COM
  Key version: 1
  Key type: 56-bit DES using key derivation
  Entry timestamp: 2003/11/10-17:23:35

Principal: krbsvr400/as20.itso.ibm.com@ITS0.IBM.COM
  Key version: 1
  Key type: 168-bit DES using key derivation

==> _____
_____
_____
_____

F3=Exit F6=Print F9=Retrieve F12=Disconnect
F13=Clear F17=Top F18=Bottom F21=CL command entry
```

Figure 5-20 List the Kerberos keytab entries

3. After the key table has been verified, the next verification step is to request a ticket granting ticket (TGT) from the KDC. Use the **kinit** command from a QShell command line as shown in Figure 5-21 on page 132.

Note that in normal production mode when a PC workstation is set up for iSeries Access for Windows to connect to this iSeries server using a Kerberos ticket, the Kerberos support on the PC workstation initiates the **kinit** command “under the covers” when the workstation user tries to connect to this iSeries server.

Important: All components of the principal name have to be entered in the correct case.

- ▶ The service name `krbsvr400` has to be entered in lowercase.
- ▶ The iSeries host name has to agree in case with the DNS entry or with the entry in the local host table on the client, if used.
- ▶ The name of the realm has to be entered in uppercase.

The **kinit** command should complete without any messages and return to the QShell command prompt (as indicated by the second \$ character in Figure 5-21).

4. List the ticket granting ticket (TGT) using the **klist** command from QShell, as shown in the middle part of Figure 5-21.
5. If any of the QShell commands ended with an error message, you should use the “Troubleshooting” appendix in *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.

```
QSH Command Entry

$
> kinit -k krbsvr400/as20.itso.ibm.com@ITSO.IBM.COM
$
> klist
Ticketcache: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred_fe8869c0
Default principal: krbsvr400/as20.itso.ibm.com@ITSO.IBM.COM

Server: krbtgt/ITSO.IBM.COM@ITSO.IBM.COM
Valid 2003/12/23-12:17:00 to 2003/12/23-22:17:00
$

===>

F3=Exit F6=Print F9=Retrieve F12=Disconnect
F13=Clear F17=Top F18=Bottom F21=CL command entry
```

Figure 5-21 Request TGT

This completes the verification of the Network Authentication Service setup.

On iSeries, you next need to set up EIM.

5.7 Enterprise Identity Mapping

As we discussed previously in this chapter, user authentication, such as is provided through Kerberos, is an important network security consideration and offers a form of single signon (SSO) to a network of servers with varying operating systems, functions, and applications, or in Kerberos terms, services. At this time, Kerberos requires the user principal to be spelled the same on every workstation or server in the network to which that user wants to “do business with.”

The IBM Enterprise Identify Mapping (EIM) architecture and implementation offers an extension to that single signon, which includes the capability for that same user to have different user IDs, multiple aliases for the same user, and more extensions on the various servers in the network.

For example, while iSeries Network Authentication Service allows an iSeries server to participate in a Kerberos realm, EIM provides a mechanism for associating valid Kerberos principals to a single EIM identifier that represents that user within the entire enterprise. Other user identities, such as an OS/400 user name, can be associated with this EIM identifier. Based on this association and from an OS/400 viewpoint, *EIM provides a mechanism for OS/400 and specific applications to determine which OS/400 user profile represents the person or entity represented by the Kerberos principal.*

Later in this topic, we provide an example showing Kerberos and EIM working together.

In this book, we provide a broad overview of EIM capabilities and basic setup details and an example. We do not provide additional details such as administering the EIM identifiers (“users”) and defining multiple systems within an EIM *domain*.

Complete EIM coverage is beyond the scope of this redbook. For more complete iSeries EIM support information, refer to:

- ▶ The IBM Redbook *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.
- ▶ iSeries Information Center articles.
- ▶ iSeries Navigator online help information by selecting **system name** → **Network** → **Enterprise Identity Mapping**. This is the iSeries interface for setting up and managing iSeries EIM support.

EIM addresses a single signon (SSO) for the same user and provides other advantages regarding user management across a network.

The following are V5R2 iSeries IBM-supplied “applications” enabled to use EIM. iSeries also has EIM APIs that can be used to enable your application to use EIM.

- ▶ iSeries Navigator
- ▶ DRDA
- ▶ PC5250 and Telnet
- ▶ NetServer
- ▶ QFileSvr.400

In the following topics, we show an example of setting up EIM, based upon our previous Kerberos example setup.

5.7.1 EIM overview and components

Using the SSO example, consider that user John Smith has user ID JSmith in one registry, JohnS in another registry, and JS50852 in another registry. A registry is the EIM generic term for the repository of authorized user information on various operating systems’ “directory of users.”

Figure 5-22 on page 134 shows an example of Kerberos and EIM working together for user authentication of John N. Smith. In Kerberos, this user is known as principal John Smith. Using the EIM identifier John N. Smith, John N. Smith is mapped to John in a Windows client workstation, JohnS in an AIX registry, and JS50852 in an iSeries “registry” on iSeries server SysA.

In this figure, user John at the workstation is initiating an iSeries Navigator session to SysA.

In our pictured scenario, JSmith has already used Kerberos Authentication Service to obtain a ticket granting ticket (TGT). Our protocol flow starts with the iSeries Access for Windows connection attempt triggering the communication protocol to obtain a service ticket from the KDC ticket granting service for John. As with normal Kerberos flow, the service ticket and associated Kerberos principal authentication information are sent to the iSeries system SysA in step 3.

In our figure example, EIM identifier John N. Smith has been defined in the EIM Domain Controller as JS50852 for registry SysA (registry type OS/400).

When server SysA, set up to use EIM, receives the service ticket information, it communicates with its EIM domain controller. Because it is properly configured for SysA, the EIM Domain Controller responds to SysA, indicating that Kerberos principal JSmith is defined

as JS50852 on your system. In our example, JS50852 has been defined on SysA as a valid OS/400 user, with various levels of OS/400 authorization. The main iSeries Navigator window opens on JSmith's client workstation in step 6.

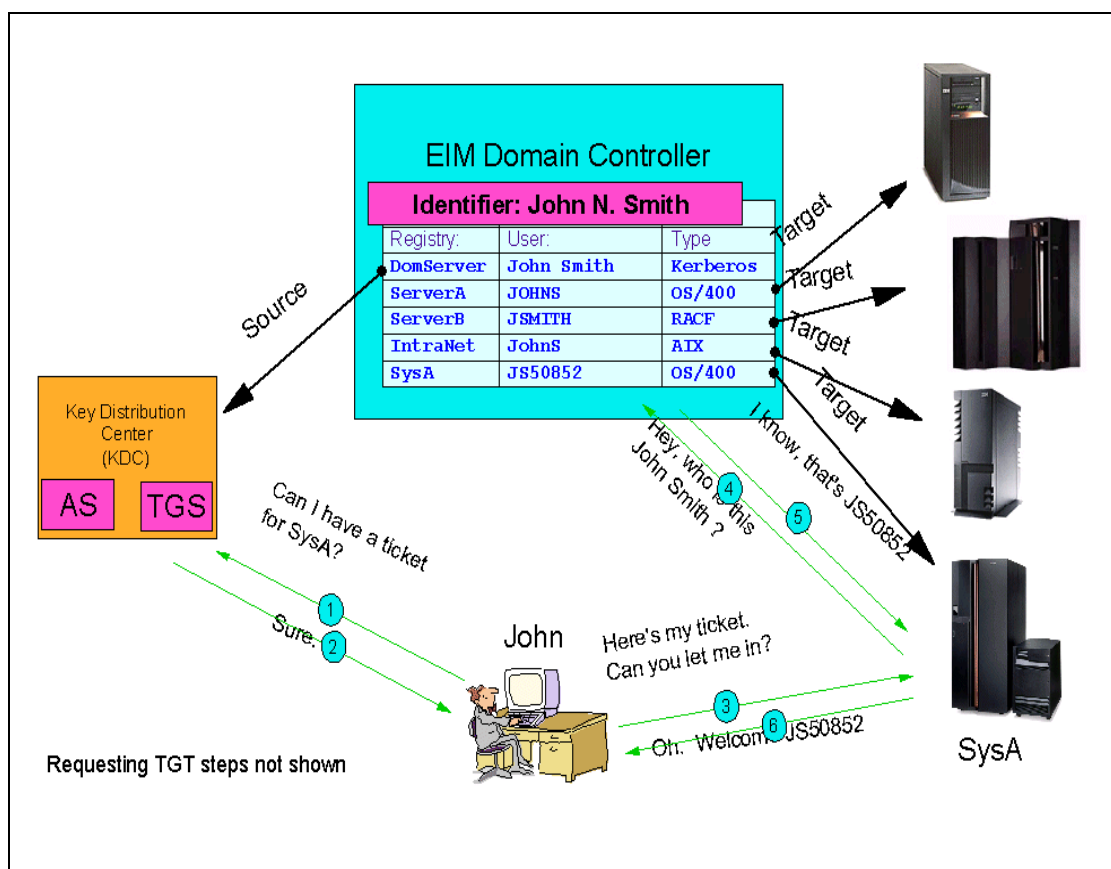


Figure 5-22 Example showing Kerberos and EIM working together

Because EIM is essentially a mechanism for mapping (associating) a person or entity to the appropriate user identities in various registries throughout the enterprise, it is ideal for a staged implementation within a network.

For example, assume a user currently signs on to five servers. Three of these servers could each have this user defined with a different user ID. If these three user IDs were mapped in the EIM Domain Controller for the same EIM identifier, these three servers can offer transparent access, while the remaining two servers require either a user ID and password or have Kerberos authentication enabled.

As the IDs on these two remaining servers are added to EIM and EIM is enabled, the non-prompted authentication will occur and different user IDs could then be used on the client workstation and iSeries server.

This means that a small or pilot group of identities can be implemented in EIM based on groups of users or by server and can then later be extended to a more comprehensive solution. It is not necessary for all users, servers, and applications to participate from the start.

EIM itself is included at no extra charge in major IBM @server operating systems such as OS/400, AIX, and z/OS. It is downloadable free of charge for the Windows and Linux operating systems. EIM is implemented in IBM Directory Server, which is an LDAP-enabled

directory component typically included in the base operating system available on all IBM @server platforms. IBM Directory Server is integrated into the OS/400 and z/OS operating systems.

You do need to understand some Lightweight Directory Access Protocol (LDAP) concepts to implement EIM successfully.

Before showing a simplified example of setting up EIM on iSeries to be used with iSeries Access for Windows PC5250 and iSeries Navigator functions, we must first give an overview of the main configuration and run time components of EIM.

Figure 5-23 depicts a simple network with just the major EIM components shown.

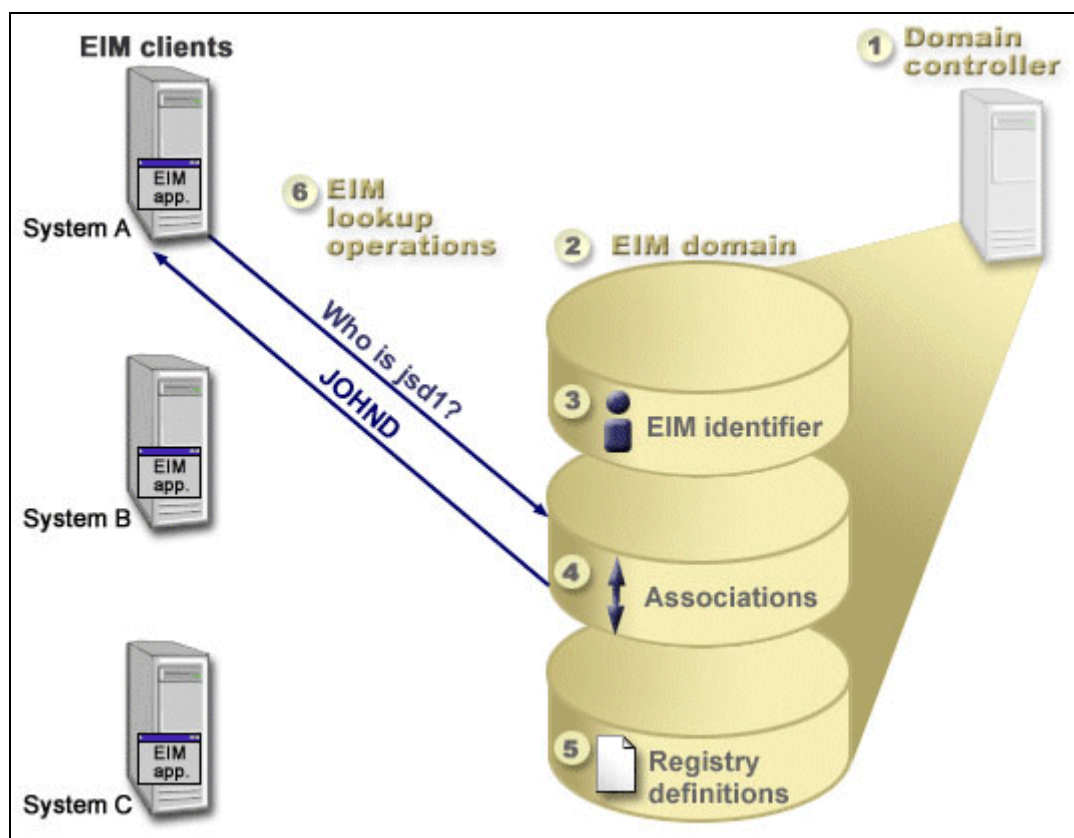


Figure 5-23 EIM components overview

The following topics provide an overview of the primary EIM components:

- ▶ EIM domain controller
- ▶ EIM domain
- ▶ EIM identifier
- ▶ EIM associations
- ▶ EIM registry definitions
- ▶ EIM lookup operations

EIM domain controller

At the top level of the EIM architecture is the domain controller (item 1 in Figure 5-23). The EIM domain controller is a Lightweight Directory Access Protocol (LDAP) server that is configured to manage at least one EIM domain. The domain controller is implemented as a

tree structure in the LDAP server. You can only have one domain controller per physical server or logical partition (LPAR) on a system supporting LPAR.

To enable EIM in your enterprise, a minimum of one domain controller must exist. If you have multiple EIM domains in your enterprise, you can use one domain controller to link all of the EIM domains created on different servers.

Any IBM @server platforms can act as a domain controller, provided they are running the IBM Directory Server. Critical to the server being able to act as a domain controller is that the system must have proper LDAP support. Without this support, a server cannot be used as a domain controller. Below are some examples of servers that can provide the EIM domain controller function because of their LDAP support:

- ▶ iSeries, formerly known as the AS/400
- ▶ zSeries, formerly known as the S/390
- ▶ pSeries, formerly known as RS/6000
- ▶ xSeries, also known as Windows
- ▶ Linux
- ▶ Open LDAP

EIM domain

The domain, as shown as item 2 in Figure 5-23, is the collection of EIM identifiers, registries for each of the different user registries in an organization, and mapped associations between specific user IDs in the user registries (for example, OS/400 within a system/partition) and the EIM identifier with which they are associated.

Because EIM is implemented in a tree structure, there is a node or branch in this tree that represents an individual EIM domain. The EIM domain can either be connected to a parent node or it can be connected directly to the root of the LDAP tree. Most companies will only require one EIM domain to host their EIM implementation. On iSeries servers, the EIM domain is created through the iSeries Navigator interface. Section 5.7.3, “Simple EIM setup example for iSeries Access for Windows users” on page 142 provides details about configuring an EIM domain.

An EIM domain is different from a user registry. A user registry defines a set of user identities known to and trusted by a particular instance of an operating system or application. A user registry also contains the information needed to authenticate the user of the identity. In addition, a user registry (again illustrated by OS/400 on a system or partition) often contains other attributes such as user preferences, system privileges, or personal information for that identity.

In contrast, an EIM domain *refers* to user identities that are defined in user registries. An EIM domain contains information about the *relationship* between identities in various user registries (user name, registry type, and registry instance) and the actual people or entities that these identities represent. Because EIM tracks relationship information only, there is nothing to synchronize between user registries and EIM. This segregation of passwords and information is one of the major benefits of EIM. Passwords can be changed in specific user registries on a system and nothing needs to be changed within EIM.

EIM identifier

Each unique entity that is added to an EIM domain is represented as an EIM identifier (item 3 in Figure 5-23 on page 135). An EIM identifier can represent a person, a server, a printer, or a number of other resources. An EIM identifier and associations are required before that entry can use the EIM infrastructure.

Figure 5-24 provides an example of a person in the organization named Kim Greene. Kim has to be added to the EIM domain as an EIM identifier. After this identifier is added, associations can then be created mapping which user IDs Kim Greene has on the various servers throughout the organization.

Figure 5-24 shows an example EIM identifier for Kim Greene that has user identities in different registries:

- ▶ kimgreene
- ▶ kkg1
- ▶ KIMG
- ▶ KGreene

Associations need to be made to map these various user identifies to the Kim Greene EIM identifier. By creating these associations, EIM lookup operations can be performed to retrieve the correct user identity for Kim Greene based on which system is being accessed.

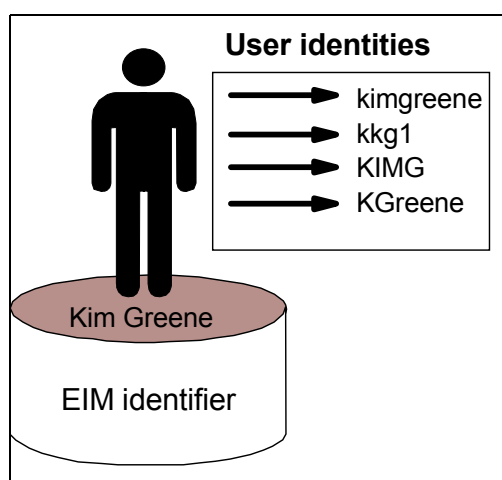


Figure 5-24 EIM identifier example

An EIM identifier needs to be unique within a domain. We strongly recommend that each EIM identifier is called something unique to the specific entry type, such as an employee number, fully qualified domain name, or TCP/IP address.

As previously stated, in addition to a “user,” an EIM identifier can represent a server, a print device or service, or some other network resource. This is similar to the Kerberos *principal* concept. One example of an EIM identifier for a service could be the print server function, which in an enterprise, runs on multiple systems. Assuming three such systems, the print server function could run under three different user identities, such as pserverID1, pserverID2, and pserverID3, on each of the three systems.

Associations need to be created to define the relationships between the EIM identifier (print server function in our example) and each of the user identities for this function (pserverID1, pserverID2, and pserverID3). These associations enable application developers to use EIM lookup operations to find a specific print server function. Application providers can then write distributed applications that manage the print server function more easily across the enterprise.

Before discussing EIM associations and EIM registries, we discuss alias support with EIM identifiers.

EIM identifiers and aliasing

You can also create aliases for EIM identifiers. Aliases can aid in locating a specific EIM identifier when performing an EIM lookup operation. One use of an alias might be a situation where an individual's legal name is different from the name that person is known as. An alias can be created to allow that individual to be referred to by their more commonly known name.

EIM identifier names must be unique within an EIM domain. Aliases can help address situations where using unique identifier names can be difficult. For example, different individuals within an enterprise can share the same name, which can be confusing if you are using proper names as EIM identifiers.

As an example, the alias for John S. Day1 might be John Samuel Day, and the alias for John S. Day2 might be John Steven Day. The EIM administrator could create two different EIM identifiers to distinguish between John S. Day: One is John S. Day1 and the other is John S. Day2. Each EIM identifier can have multiple aliases to identify which John S. Day the EIM identifier represents.

The EIM administrator might add another alias to each of the EIM identifiers for the two individuals to further distinguish between them. For example, the additional aliases might contain each user's employee number, department number, job title, or some other distinguishing attribute.

EIM registry definitions

An EIM registry definition (item 5 in Figure 5-23 on page 135) represents an actual user registry that exists on a system within the enterprise. A user registry operates like a directory and contains a list of valid user identities for a particular system or application. A basic user registry contains user identities and their passwords. One example of a user registry is the z/OS Security Server Resource Access Control Facility (RACF) registry. User registries can contain other information as well. For example, a Lightweight Directory Access Protocol (LDAP) directory contains bind distinguished names, passwords, and access controls to data that is stored in LDAP. Other examples of common user registries are a Kerberos Key Distribution Center (KDC) and the OS/400 user profiles registry for a specific system or partition.

EIM registry definitions provide information regarding those user registries in an enterprise. The administrator defines these registries to EIM by providing the following information:

- ▶ A unique, arbitrary EIM registry name
- ▶ The type of user registry

Each registry definition represents a specific instance of a user registry. Consequently, you should choose an EIM registry definition name that helps you to identify the particular instance of the user registry. For example, you could choose the TCP/IP host name for a system user registry, or the host name combined with the name of the application for an application user registry. You can use any combination of alphanumeric characters, mixed case, and spaces to create unique EIM registry definition names.

In Figure 5-25, an EIM administrator created EIM registry definitions for user registries representing System A, System B, and System C. System A contains a user registry for WebSphere Lightweight Third-Party Authentication (LTPA). The registry definition name that the administrator uses helps to identify the specific occurrence of the type of user registry. An IP address or host name is often sufficient for many types of user registries. In this example, the administrator identifies the specific user registry instance by using System_A_WAS as the registry definition name. In addition to the name, the administrator also provides the type of registry as WebSphere LTPA. In this example figure, we see the registry entry for System_C is registry type OS/400.

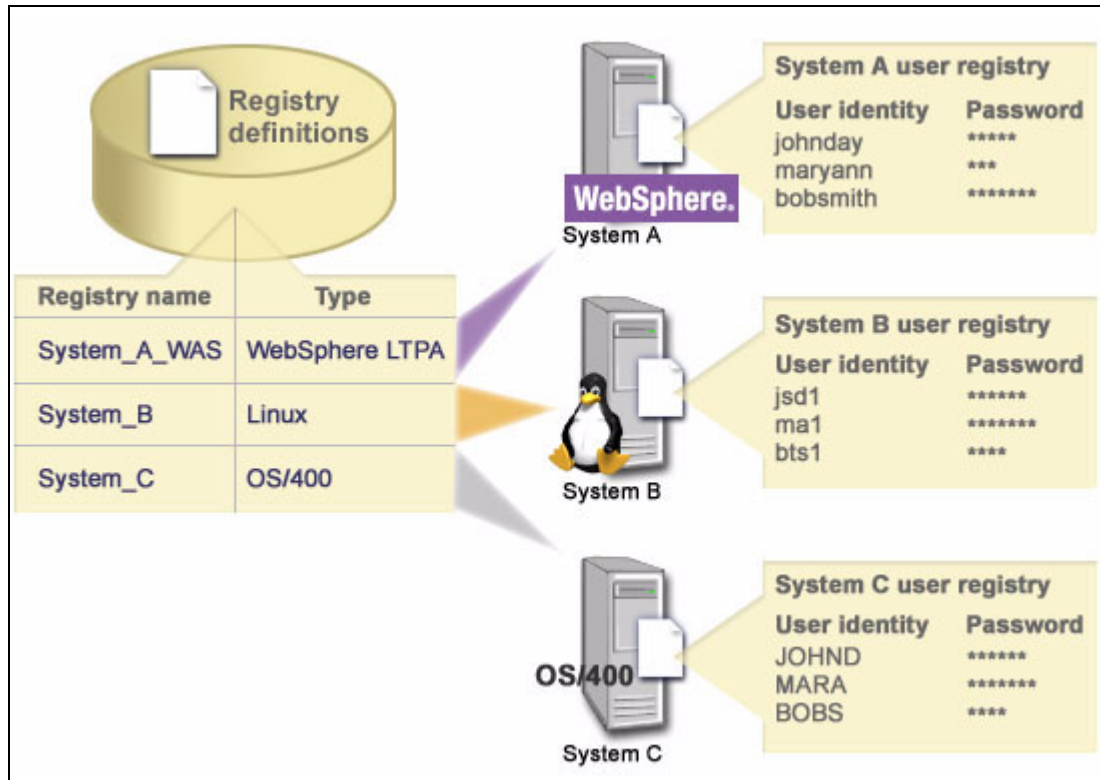


Figure 5-25 Example: EIM registry definitions using three user registries

EIM support has other registry definition capabilities, including defining user registries within other user registries. This is beyond the scope of this book.

System and application registry definitions

Some applications use a subset of user identities within a single instance of a user registry. EIM allows administrators to model this scenario by providing two kinds of EIM registry definitions: system and application.

A system registry definition represents a distinct registry within a workstation or server. You can create a system registry definition when the registry in the enterprise has at least one of the following traits:

- ▶ The registry is provided by an operating system, such as AIX, OS/400, or a security management product, such as z/OS Security Server Resource Access Control Facility (RACF).
- ▶ The registry contains user identities that are unique to a specific application, such as Lotus Notes®.
- ▶ The registry contains distributed user identities, such as Kerberos principals or Lightweight Directory Access Protocol (LDAP) distinguished names.

An application registry definition represents a subset of user identities that are defined in a system registry. These user identities share a common set of attributes or characteristics that allow them to use a particular application or set of applications. You can create an application registry definition when the user identities have the following traits:

- ▶ The user identities for the application or set of applications are not stored in a user registry specific to the application or set of applications.
- ▶ The user identities for the application or set of applications are stored in a system registry that contains user identities for other applications.

EIM lookup operations (item 6 in Figure 5-23 on page 135) perform correctly regardless of whether an EIM administrator defines a registry either as system or application. However, separate registry definitions allow mapping data to be managed on an application basis. The responsibility of managing application-specific mappings can be assigned to an administrator for a specific registry.

See *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975, for more details about this capability.

EIM registry definitions and aliasing

You can also create aliases for EIM registry definitions. You can use predefined alias types or you can define your own alias types to use. The predefined alias types include:

- ▶ Domain Name System (DNS) host name
- ▶ Kerberos realm
- ▶ Issuer distinguished name (DN)
- ▶ Root distinguished name (DN)
- ▶ TCP/IP address
- ▶ LDAP DNS host name

This alias support allows programmers to write applications without having to know in advance the arbitrary EIM registry name chosen by the administrator who deploys the application. Application documentation can provide the EIM administrator with the alias name that the application uses. Using this information, the EIM administrator can assign this alias name to the EIM registry definition that represents the actual user registry that the administrator wants the application to use.

When the administrator adds the alias to the EIM registry definition, the application can perform an alias lookup to find the EIM registry name at initialization. The alias lookup allows the application to determine the EIM registry name or names to use as input to the APIs that perform EIM lookup operations.

EIM associations

An EIM association is a relationship between an EIM identifier that represents a specific person and a single user identity in a user registry that also represents that person. When you create associations between an EIM identifier and all of a person's or entity's user identities, you provide a single, complete understanding of how that person or entity uses the resources in an enterprise. EIM provides APIs that allow applications to find an unknown user identity in a specific (target) user registry by providing a known user identity in some other (source) user registry.

Using associations like this is called identity mapping.

Before you can create an association, you first must create the appropriate EIM identifier and the appropriate EIM registry definition for the user registry that contains the associated user identity. "Using iSeries Navigator to add identifiers and associations" on page 150 demonstrates how to create identifiers and associations. An association defines a relationship between an EIM identifier and a user identity by using the following information:

- ▶ EIM identifier name
- ▶ User identity name
- ▶ EIM registry definition name
- ▶ Association type

An administrator can create different types of associations between an EIM identifier and a user identity based on how the user identity is used. User identities can be used for authentication, authorization, or both.

Authentication is the process of verifying that an entity or person who provides a user identity has the right to assume that identity. Verification is often accomplished by forcing the person who submits the user identity to provide secret or private information associated with the user identity, such as a password.

Authorization is the process of ensuring that a properly authenticated user identity can only perform functions or access resources for which the identity has been given privileges. In the past, nearly all applications were forced to use the user identities in a single user registry for both authentication and authorization. By using EIM lookup operations, applications now can use user identities in one user registry for authentication while using associated user identities in a different user registry for authorization.

In EIM, there are three types of associations that an EIM administrator can define between an EIM identifier and a user identity. These types are source, target, and administrative associations.

Source association

When a user identity is used for authentication, such as your Windows login, that user identity should have an EIM identifier that uses that authenticated identity as a source association. A source association allows the user identity to be used as the source in an EIM lookup operation to find a different user identity (target) that is associated with the same EIM identifier.

Important: In order for an EIM identifier to have any benefit, there must be at least one source association and one target association.

Target association

When a user identity is used for authorization rather than for authentication, that user identity should have an EIM identifier that uses that ID as a target association. A target association allows the user identity to be returned as the result of an EIM lookup operation. If a user identity with only a target association is used as the source identity in an EIM lookup operation, no associated user identities are returned.

It might be necessary to create both a target and a source association for a single user identity. This is required when an individual uses a single system as both a client and a server or for individuals who act as administrators. For example, a user normally authenticates to a Windows platform and runs applications that access an AIX server. Because of the user's job responsibilities, the user must occasionally also log in directly to an AIX server. To run programs that access other systems in the Kerberos-EIM network, you need to create both source and target associations between the AIX user identity and the person's EIM identifier. User identities that represent end users normally need a target association only.

Administrative association

An administrative association for an EIM identifier is typically used to show that the person or entity represented by the EIM identifier owns a user identity that requires special considerations for a specified system. This type of association can be used, for example, with highly sensitive user registries.

Due to the nature of what an administrative association represents, an EIM lookup operation that supplies a source user identity with an administrative association returns no results. Similarly, a user identity with an administrative association is never returned as the result of an EIM lookup operation. It could be a serious issue if an administrative association is returned in the case of root on Linux or the QSECOFR user profile on OS400.

EIM lookup operations

An EIM lookup operation (item 6 in Figure 5-23 on page 135) is a process through which an application or operating system finds an unknown associated user identity in a specific target registry by supplying some known and trusted information. Applications that use EIM APIs can perform these EIM lookup operations on information only if that information is stored in the EIM domain. An application can perform one of two types of EIM lookup operations based on the type of information the application supplies as the source of the EIM lookup operation: a user identity or an EIM identifier.

When an application supplies a user identity as the source, the application also must supply the EIM registry definition name for the source user identity and the EIM registry definition name that is the target of the EIM lookup operation. To be used as the source in a EIM lookup operation, a user identity must have a source association defined for it.

When an application supplies an EIM identifier as the source of the EIM lookup operation, the application must also supply the EIM registry definition name that is the target of the EIM lookup operation. For a user identity to be returned as the target of either type of EIM lookup operation, the user identity must have a target association defined for it.

The supplied information is passed to the EIM domain controller where all EIM information is stored and the EIM lookup operation searches for the source association that matches the supplied information. Based on the EIM identifier (supplied to the API or determined from the source association information), the EIM lookup operation then searches for a target association for that identifier that matches the target EIM registry definition name.

5.7.2 EIM authorities

There are different authority groups within EIM that allow you to perform different functions, depending on which group is being used to access and work with the EIM environment. The EIM administrator groups include:

- ▶ Lightweight Directory Access Protocol (LDAP) administrator
- ▶ EIM administrator
- ▶ EIM identifiers administrator
- ▶ EIM mapping lookup
- ▶ EIM registries administrator

To set up these authorities on an iSeries system, select iSeries Navigator **system** → **Networks** → **Enterprise Identity Mapping** → **Domain Management**. Select your EIM domain and right-click it. Select **Authority** from the context menu.

In this book, we do not provide additional details about each of these EIM administrator groups and setting up their authority levels. For those details, refer to *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.

SG24-6975 also provides guidance about planning and managing your EIM environment.

5.7.3 Simple EIM setup example for iSeries Access for Windows users

In this topic we show how to set up EIM on an iSeries server so that a Kerberos authenticated user can successfully perform iSeries Access for Windows functions.

The client workstation used to set up EIM on an iSeries server must have the iSeries Navigator Network component installed.

The use of identity mapping requires that appropriate EIM administrators do the following:

- ▶ Configure the EIM domain and EIM domain controller using the EIM configuration wizard.
- ▶ Add the EIM domain to the list of domains to be managed from your client.
- ▶ Create EIM identifiers that represent people or entities in their enterprise.
- ▶ Create EIM registry definitions that describe the existing user registries in their enterprise.
- ▶ Use iSeries Navigator to add a user to the domain and associate that user with their identities in user registries.

The following topics provide an example of using iSeries Navigator interfaces to set up a base configuration of a single EIM domain. This is based upon the example Kerberos setup performed earlier in this chapter for iSeries Access for Windows 5250 Emulation (Telnet application) and the iSeries Navigator “application.” We use example EIM Domain entries located in Table 5-1 on page 109.

Creating and joining a new EIM domain

Use the following steps to begin setting up the EIM domain:

1. In the iSeries Navigator window, expand the iSeries system on which you want to configure the EIM domain controller. As shown for system As20 in Figure 5-26, expand **Network** → **Enterprise Identity Mapping**, right-click **Configuration**, and then select **Configure**. This opens the EIM Wizard Welcome window. (Our window in Figure 5-26 shows Reconfigure, because we had already configured the EIM domain before capturing this window.)

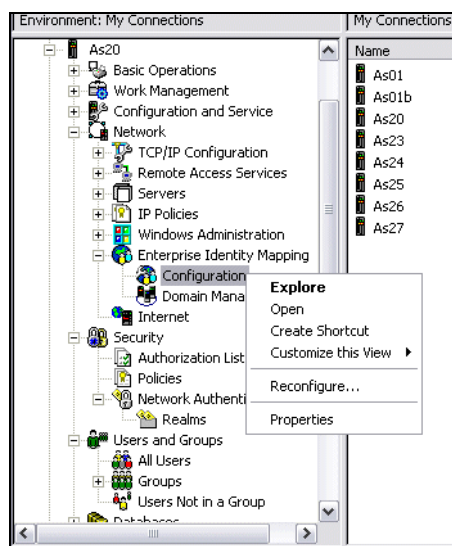


Figure 5-26 Getting started with EIM: Configuring an EIM domain

2. In the EIM Wizard Welcome window (Figure 5-27), select the option **Create and join new domain** and click **Next**.

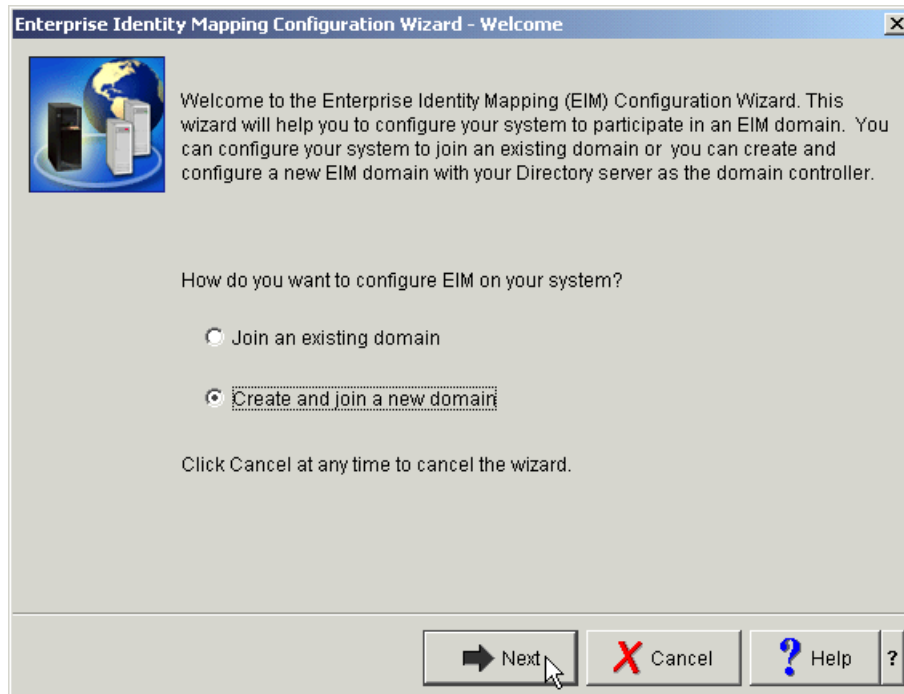


Figure 5-27 EIM Configuration Wizard - Welcome

3. If your LDAP server is running while you are using the wizard, a warning window appears to inform you that the wizard will need to stop and restart the LDAP server after your EIM setup process is complete in order for the EIM setup to take effect. Click **Yes**.
4. In the Specify Domain window (Figure 5-28), enter the EIM domain name (item P from our example worksheet in Table 5-1 on page 109) and a meaningful description. Click **Next**.

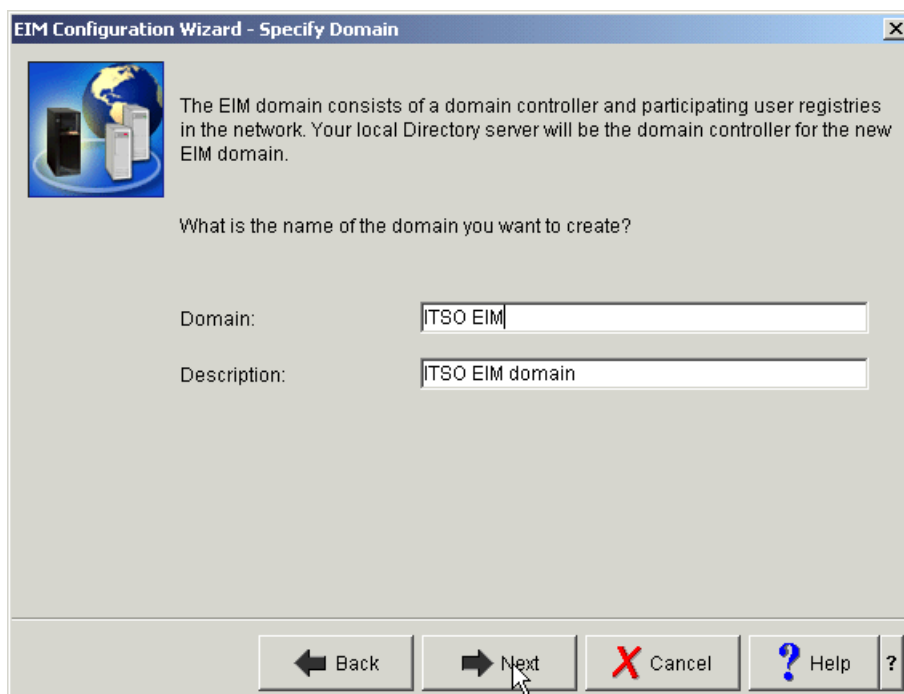


Figure 5-28 EIM Configuration Wizard - Specify Domain

5. In the Specify Parent DN window (Figure 5-29), you can designate specific placement of the EIM domain sub-tree in the LDAP directory structure (item Q in example worksheet in Table 5-1 on page 109). We are creating the EIM domain controller as a separate tree in the LDAP structure. Therefore, select the **No** option. Click **Next**.

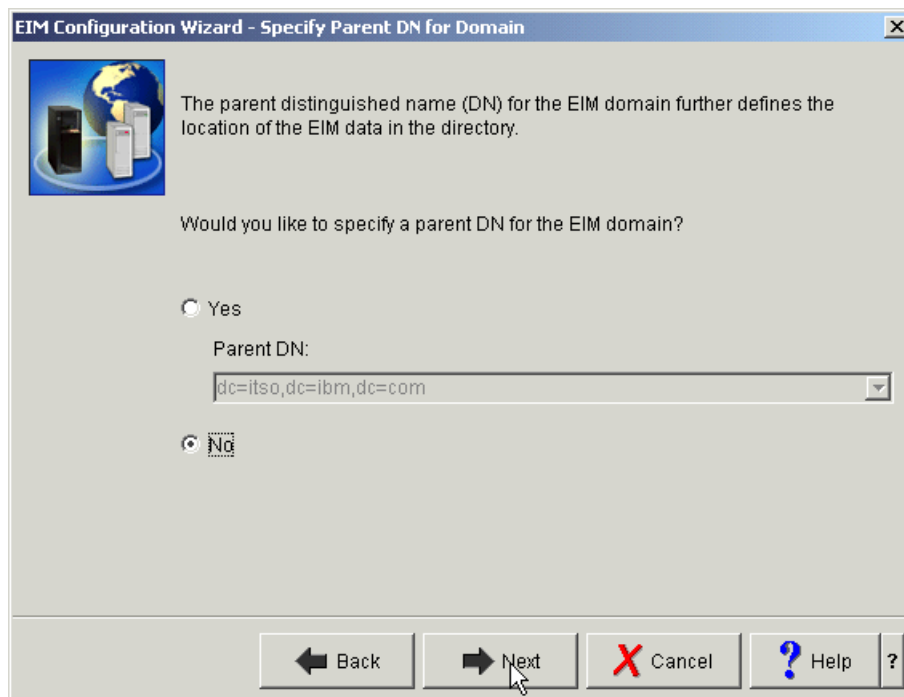


Figure 5-29 EIM Configuration Wizard - Specify Parent DN for Domain

6. In the Specify User For Connection window (Figure 5-30 on page 146), specify which user the wizard uses when it connects to the LDAP server to perform the configuration task for you (this is just a one-time connection while the wizard is running).

Use the distinguished name (DN) and password from items R and S in the Table 5-1 on page 109. We use the value `cn=adminstrator`, as shown in Figure 5-30. `cn=adminstrator` is the primary distinguished name for administering an LDAP server. You need to enter a password value twice. Remember this password for later use.

7. Click **Verify Connection** to verify the connection to the LDAP server. If the connection is successfully verified, click **OK** in the confirmation window and then **Next** in the Specify User For Connection window.

If you have trouble getting the connection to the LDAP server, refer to the online help information. You can also refer to the "Troubleshooting" appendix in *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.



Figure 5-30 EIM Configuration Wizard - Specify User For Connection

8. Assuming successful connection verification, you are now at the Registry Information window (Figure 5-31). You can request two user registries to be automatically added to your domain; you should select both of them:
 - Local OS/400 registry for your iSeries system, hosting the EIM domain controller
 - Kerberos registry, in our case, located on the Windows 2000 server

Tip: We recommend that you simplify your configuration and consequently any debugging that might need to be done by clearing (uncheck) the Kerberos user identities are case sensitive check box shown in Figure 5-31.

Click **Next** to proceed to the Specify EIM System User window.

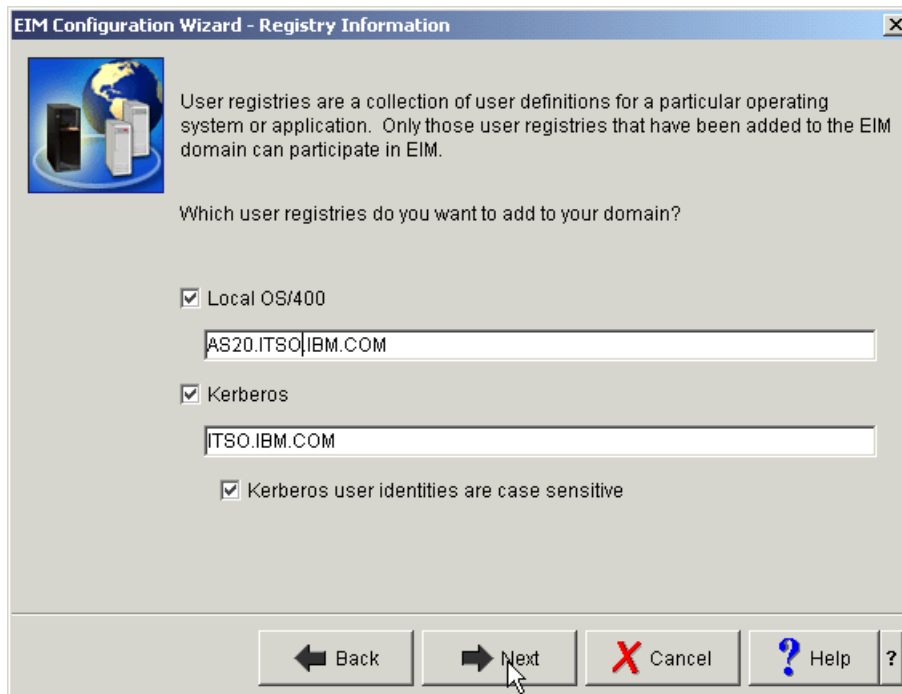


Figure 5-31 EIM Configuration Wizard - Registry Information

9. The Specify EIM System User window (Figure 5-32) is very similar to the Specify User For Connection window (step 7 on page 145 and Figure 5-30 on page 146). But now, you specify an EIM system user, whose account is used to connect to the EIM domain controller by various operating system functions. This contrasts with the Specify User For Connection window, where you specified the user that is to be used currently by the EIM set-up wizard (only once).

Again, we recommend that you create a new LDAP user and add it to the EIM Admin group. Use this new user ID and password for the system. Further details and considerations for creating LDAP users is outside the scope of this book, so here we use the LDAP administrator's ID and password.

Verify the connection, as you did in step 7 on page 145. Assuming successful verification, click **Next** on the Specify EIM System User window. This opens the Summary window.



Figure 5-32 EIM Configuration Wizard - Specify EIM System User

10. The Summary window (Figure 5-33) recaps the settings you have specified. Verify that they are accurate and then click **Finish**.

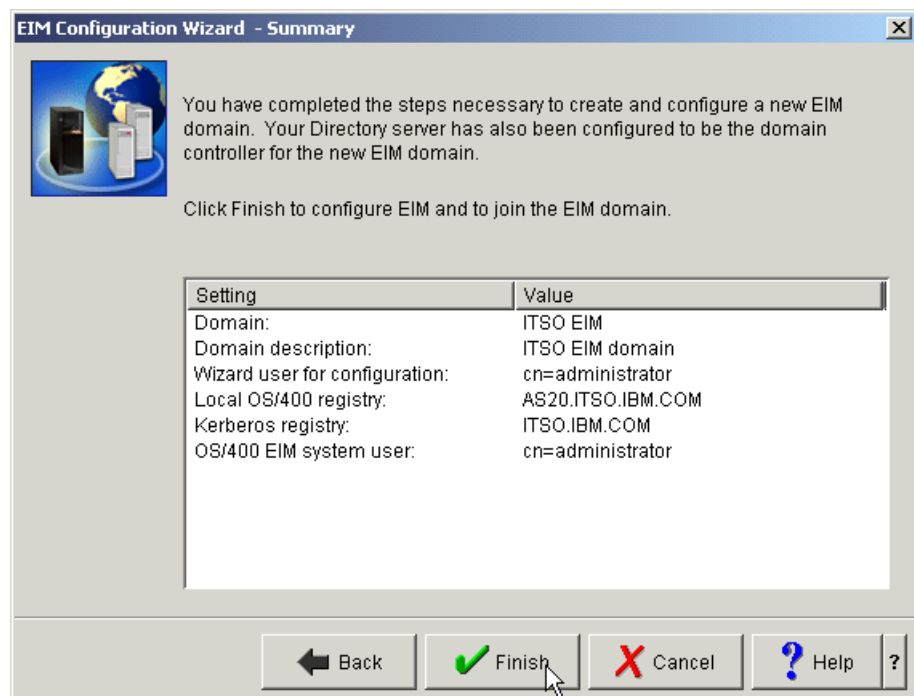


Figure 5-33 EIM Configuration Wizard - Summary

After clicking Finish, the configuration processing takes place, and you will see progress window information displayed. The LDAP server is started. If already started, it is stopped and started as part of this processing.

Adding the EIM domain to be managed

Now you need to add the EIM domain just configured to the list of EIM domains to be managed from your client (iSeries Navigator on your client workstation).

Note: The domain management information is stored locally on the client workstation. That is, if you use iSeries Navigator on another PC after performing the Add domain function (described later) on this workstation, you will have to use the Add domain function on that workstation to view domain details and perform any domain management functions. After the domain is added at the particular client, it should appear in its Domain Management folder information.

To add the EIM domain to be managed:

1. In the iSeries Navigator session, expand **Network** → **Enterprise Identity Mapping**. Right-click **Domain Management**, and click **Add Domain** in the context menu. In the Add Domain window (Figure 5-34), all the fields might already be filled in. If not, click browse and a list of configured domains will be presented. Select your EIM domain and click **OK**.

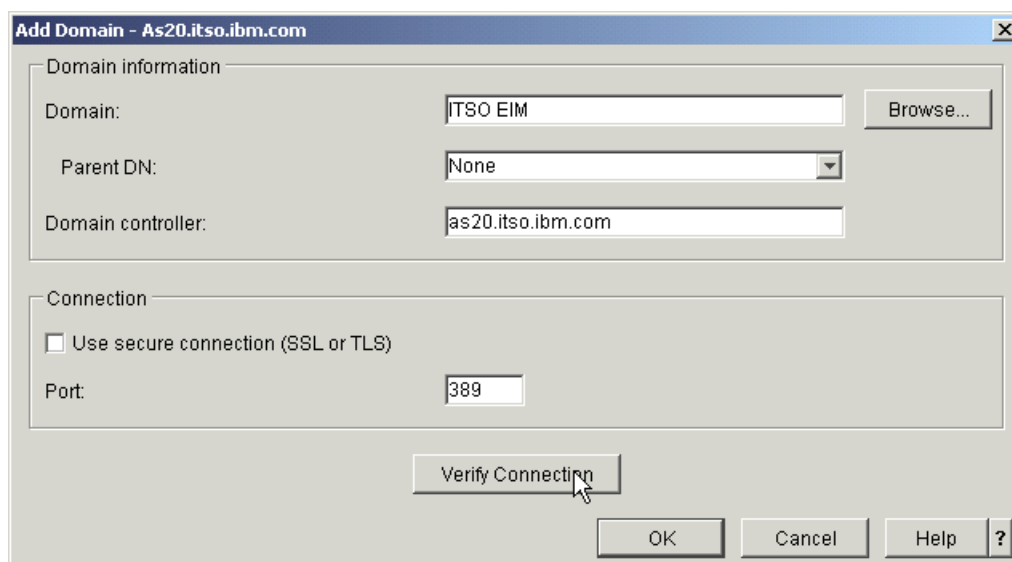


Figure 5-34 Adding your new domain to the navigation pane

Important: The options “Add domain” and “Remove domain,” available from the Domain Management context menu, act only locally on the client workstation. They can be run at any time without having any effect on the operation of the EIM domain or domain controller. In contrast, the Delete option, available from the local menu of the particular domain, deletes the domain from the domain controller.

2. The added domain now appears in the iSeries Navigator left pane folder tree structure. Click the + character next to the domain name to expand the information shown. At this point, you might be prompted to specify a DN and password for LDAP access. Assuming a successful sign-on, you will see two new subcategories, User Registries and Identifiers, added to the list, as shown in Figure 5-35.

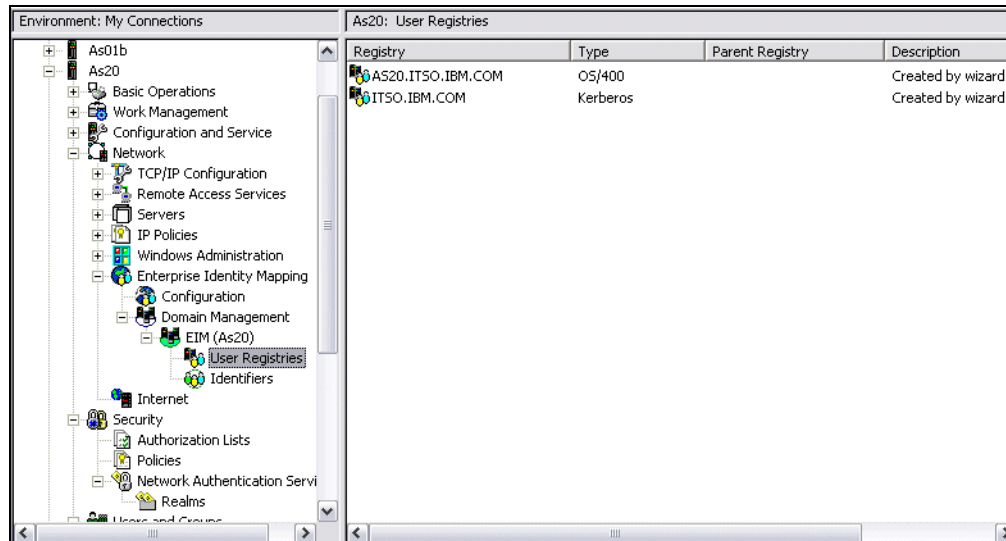


Figure 5-35 EIM domain subcategories: User Registries and Identifiers

When you click **User Registries**, there should be two user registries that the wizard has added; these were specified in step 8 on page 146. You can optionally right-click one of the registries in the panel on the right and select **Properties** in the local menu. In the Properties window, you can change the description set by the wizard to something more meaningful for you.

We cover identifiers in the next section. They are used to define the mapping of users from one system to another.

This completes adding the domain to the domain management of this client workstation.

Using iSeries Navigator to add identifiers and associations

Prior to testing your EIM configuration, you need to create at least one user in your EIM domain. You can use iSeries Navigator to manage a small number of users in EIM. However, in iSeries Navigator, you cannot browse the user profiles or accounts in the user registries; you have to key in all the user ID's.

Adding users to the EIM domain

Perform the following steps to add a user (or rather an EIM identifier) to the EIM domain:

1. In iSeries Navigator, expand your **iSeries system** → **Network** → **Enterprise Identity Mapping**. If you haven't connected to the EIM domain controller previously, you will be prompted to enter the distinguished name (item R from the worksheet in Table 5-1 on page 109) and its password.
2. Right-click **Identifiers** in the left panel of the iSeries navigator, and then select **New Identifier** in the local menu.
3. The New EIM Identifier window (showing your EIM domain) opens, as shown in Figure 5-36. Enter the EIM identifier of the new user you are adding. Remember, the EIM identifier has to be unique within the EIM domain. iSeries Navigator will issue an error message that indicates an identifier by this name already exists when you try to create a duplicate ID. You can choose to select the Generate unique identifier box. If you happen to add a duplicate EIM ID, the system will append a number to the end of the ID.

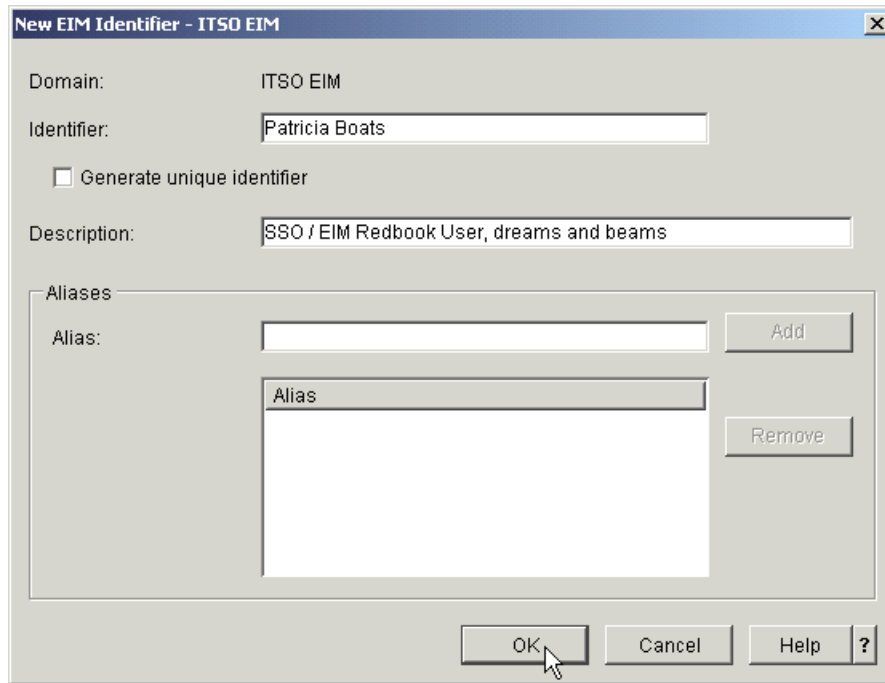


Figure 5-36 Create new EIM ID

Adding associations

You have added the EIM identifier of the user in the EIM domain. Now you have to associate this identifier with the user it represents in the various registries. The following steps demonstrate how to associate the users with their identities in the user registries:

1. In the iSeries Navigator main window left pane under your EIM domain click **Identifiers**. A list of identifiers (if any already exist) is shown in the right pane. Right-click the user you just added and select **Properties** from the menu.
2. The Properties window of the selected EIM ID opens. Select the **Associations** tab and click the **Add** button. The Add Association window opens.
3. We first add the association to the Kerberos registry. In the Add Association window (Figure 5-37), click the **Browse** button for a list of the available registries.

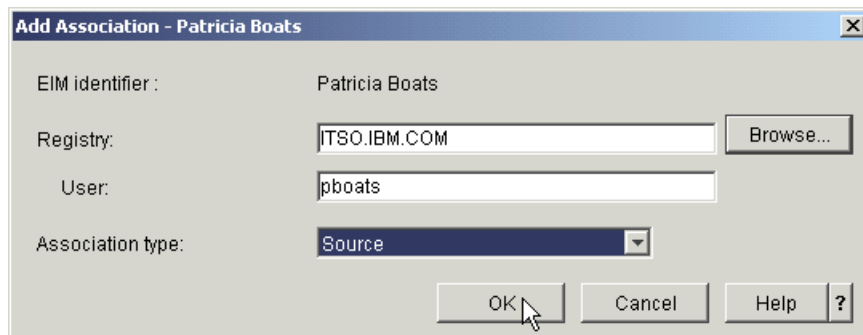


Figure 5-37 Add Kerberos association

4. The Browse EIM registries window (Figure 5-38) shows the two user registry definitions, added to the EIM domain by the EIM wizard (as you saw in Figure 5-31 on page 147):
 - The local OS/400 registry for your iSeries system, hosting the EIM domain controller, represented here by its fully qualified host name, AS20.ITSO.IBM.COM in our example.
 - The Kerberos registry on the Windows 2000 server, represented here by bare domain name (that is, not representing any host name), ITSO.IBM.COM in our example.

Select our Kerberos registry and click **OK**.

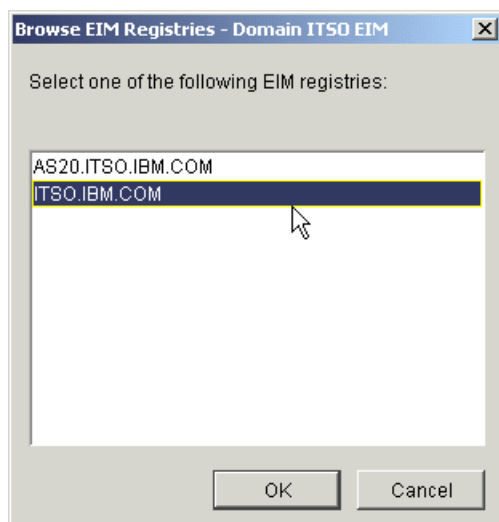


Figure 5-38 Select Kerberos registry

5. Clicking OK takes us back to the Add Association window. Complete it as shown in Figure 5-37 on page 151:
 - a. Fill in the User field with the user ID which the user uses to sign on to the Windows domain; we use pboats (Kerberos principal name) in our example.
 - b. Make sure that you select **Source** in the Association type box.
 - c. Click **OK**.
6. Next, you need to add the OS/400 registry to this EIM identifier:
 - a. As previously done in the left iSeries Navigator pane, right-click your EIM identifier. Select **Properties** and then the **Associations** tab. Click the **Add** button again
 - b. In the Add Association window (as shown in Figure 5-37 on page 151), click the **Browse** button.
 - c. In the Browse EIM registries window, as shown in Figure 5-38, we select the OS/400 registry, AS20.ITSO.IBM.COM in our case.
 - d. In the Add Association window (Figure 5-39), fill in the User field with the name of the user profile (PATRICIAB in our example) of the user in OS/400.
 - e. This time, select **Target** in the Association type box.
 - f. Click **OK** in the Add Association window.

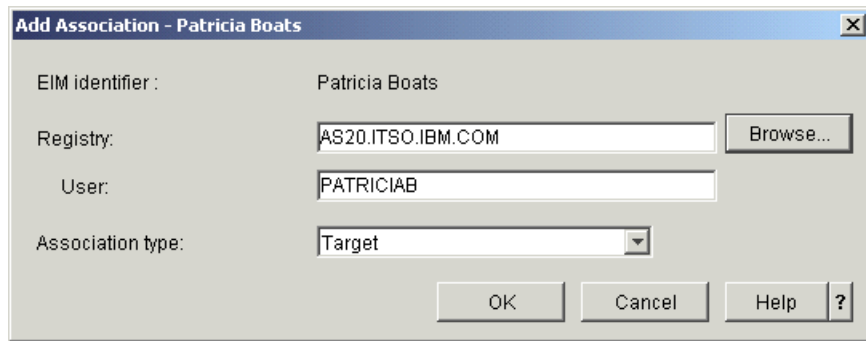


Figure 5-39 Add OS/400 association

7. Back in the Properties window for the selected EIM ID (Figure 5-40), we can see both associations:
 - The OS/400 registry with the Target association, AS20.ITSO.IBM.COM in our example
 - The Windows 2000 Kerberos registry with the Source association, ITSO.IBM.COM in our example

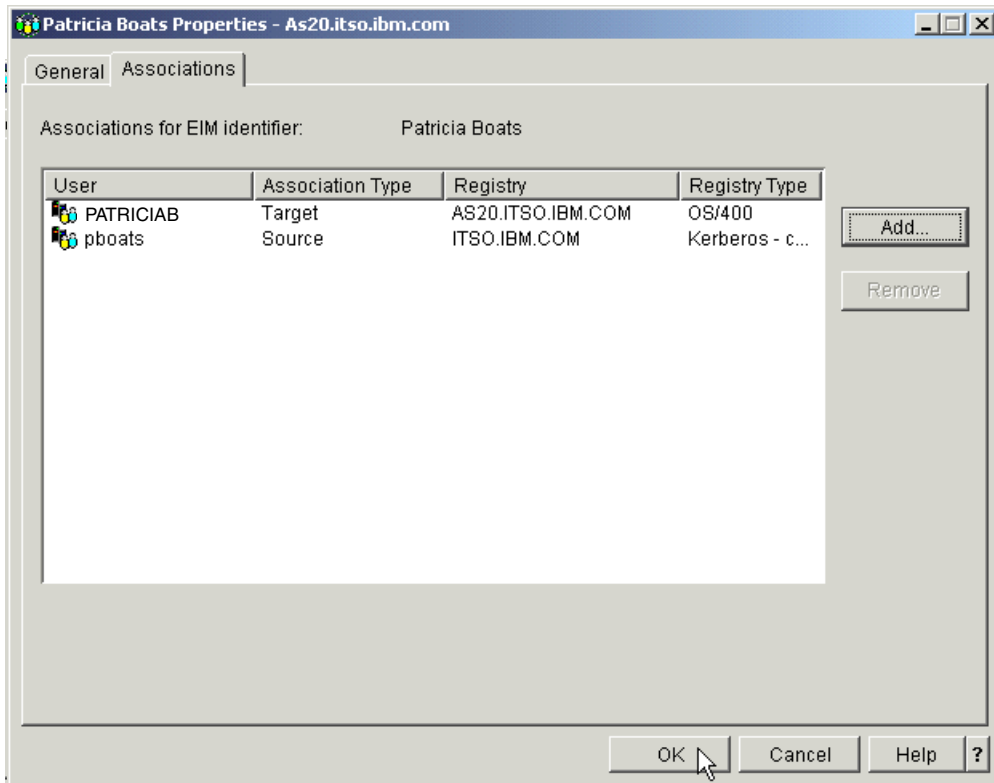


Figure 5-40 Both associations added

Verify the associations are correct and click **OK**.

This completes adding the user and the user's associations in the EIM domain. Repeat the steps for additional users.

In our simple example (a client workstation and a single iSeries server, As20), we are ready to set up and verify that we can use Kerberos and EIM for our iSeries Access for Windows PC5250 emulation and iSeries Navigator functions to iSeries server As20.

5.7.4 Setting up Kerberos authentication for an iSeries Navigator session

With V5R2 iSeries Navigator components installed on your Windows PC client workstation, you enable use of Kerberos authentication for use with iSeries Navigator sessions using the following steps:

1. In an iSeries Navigator main window on your PC, right-click the iSeries system name you want to connect to using Kerberos. Select **Properties**, as shown in Figure 5-41.

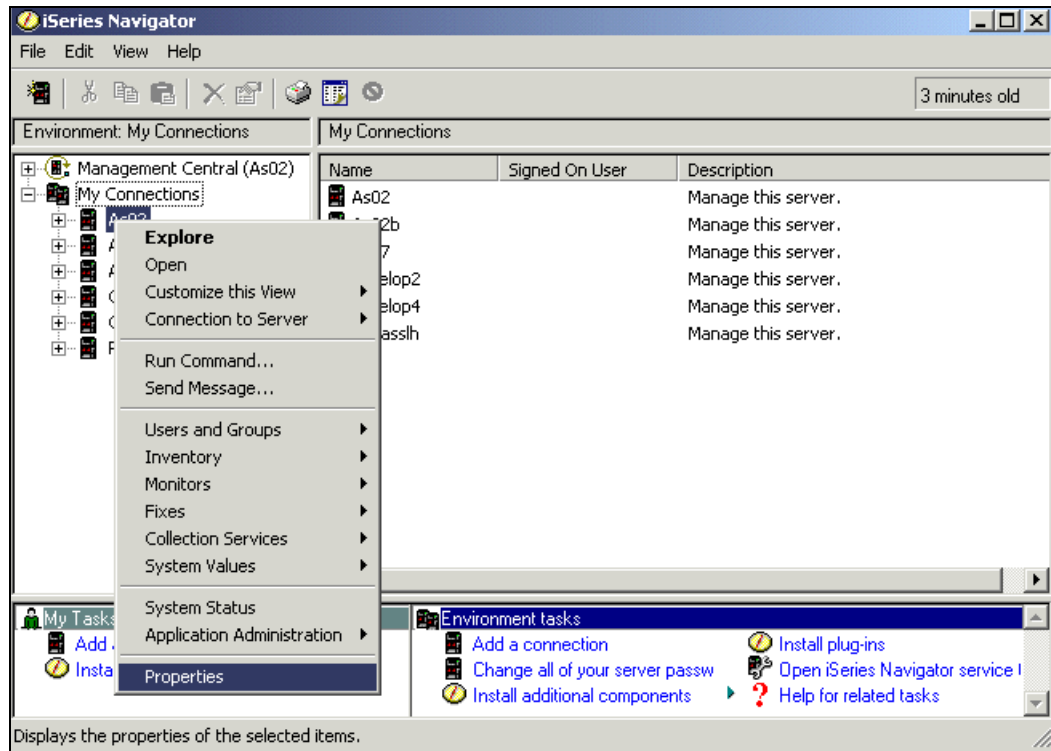


Figure 5-41 iSeries Navigator: Selecting system Properties to use Kerberos

2. In the Properties window, select the **Connection** tab to open the panel shown in Figure 5-42 on page 155.

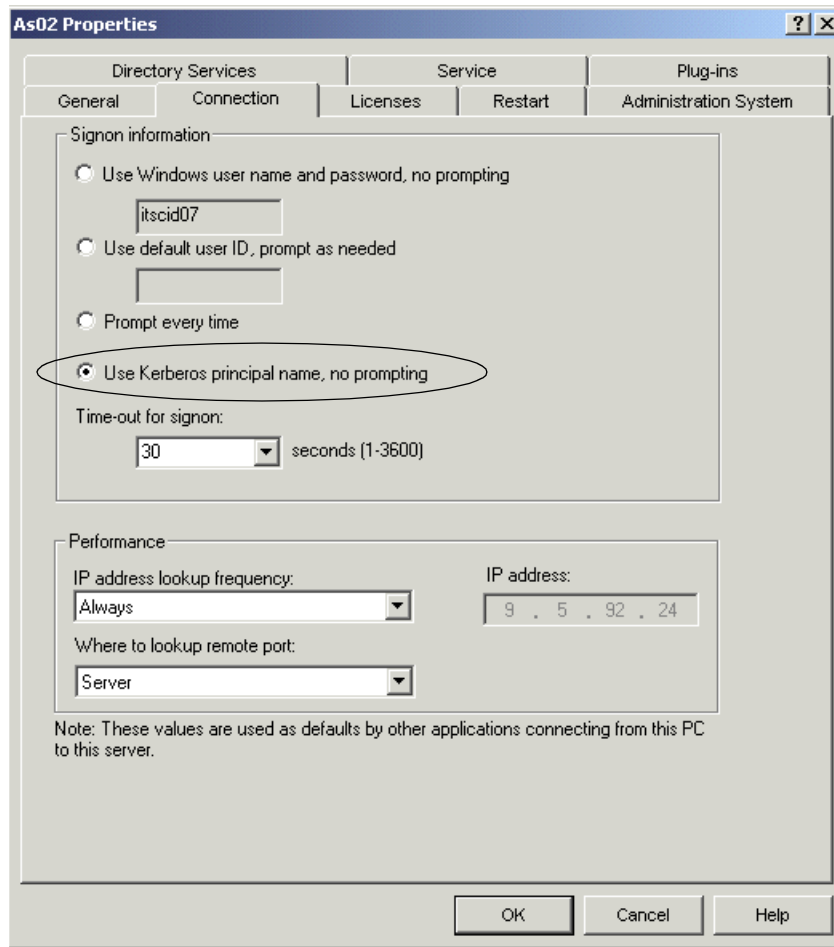


Figure 5-42 Use Kerberos principal name, no prompting

3. Select the **Use Kerberos principal name, no prompting** option under Signon information to enable Kerberos authentication. Click **OK**.
4. You are presented with a window, as shown in Figure 5-43, that enables this change to become effective. Click **OK**.

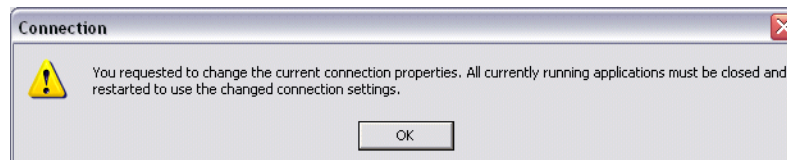


Figure 5-43 Enabling the change to use a Kerberos principal name

The next time this PC workstation user performs an iSeries Navigator action requiring authentication to the iSeries server, the sufficient Kerberos ticket processing will be performed without prompting for user ID and password.

We show an example of verifying this connection later in this book in “Testing iSeries Navigator single signon” on page 158.

5.7.5 Setting up Kerberos authentication for an iSeries Access PC5250 session

Perform the following steps to enable iSeries Access 5250 emulation from the client PC workstation to use Kerberos authentication:

1. On your client workstation, open the iSeries Access 5250 emulation session to your iSeries server. If the session is connected to the server, disconnect it by selecting **Communication** → **Disconnect** in the menu.
2. Then, select **Communication** → **Configure** in the session menu.
3. In the Configure PC5250 window (Figure 5-44 on page 156), click **Properties**.

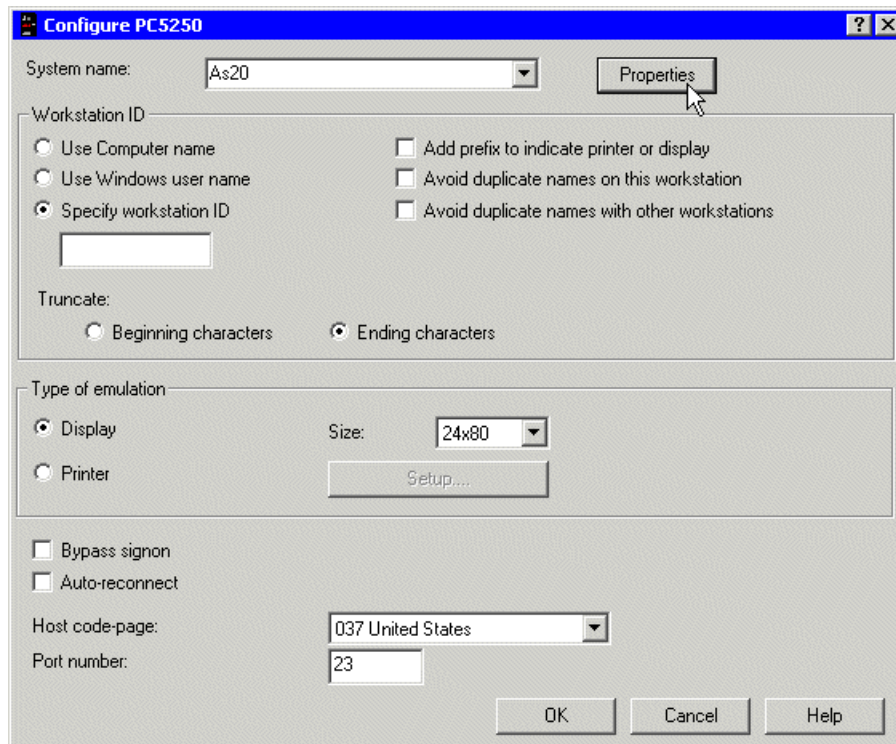


Figure 5-44 Setting up PC5250 to use Kerberos: Select Properties

4. When the Connection window (Figure 5-45 on page 157) opens, use the combo box in the section labeled User ID signon information. Scroll down and select the option **Use Kerberos principal name, no prompting**, as shown in the Figure 5-45.

Alternatively, you can select the option **Use Operation navigator default**. With this option, you can control all connections to a particular iSeries server from one place. You previously selected the Kerberos-type connection for this iSeries server in the iSeries Navigator connection properties in 5.7.4, "Setting up Kerberos authentication for an iSeries Navigator session" on page 154.

5. Click **OK**.

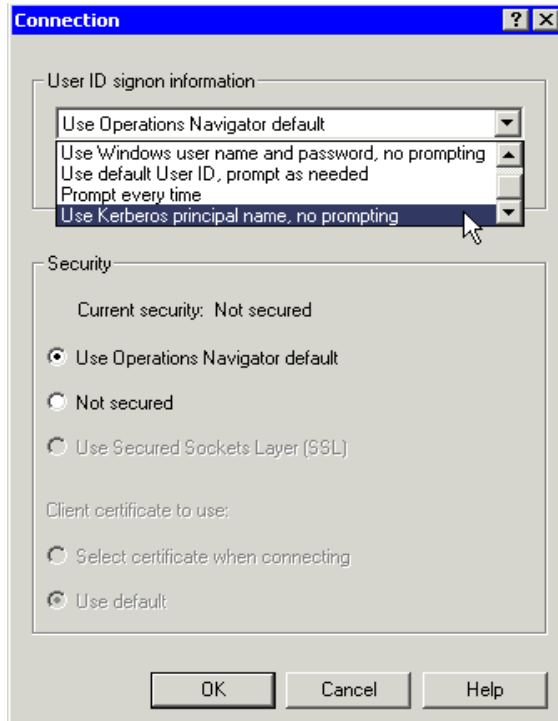


Figure 5-45 Setting up PC5250 to use Kerberos: Select Use Kerberos principal name

Using Kerberos authentication with iSeries Access 5250 emulation is now enabled the next time you connect to this iSeries using PC5250 emulation. In this book, we show an example of this connection later in “Testing iSeries Access for Windows 5250 emulation single signon” on page 159.

Important: It is important that you save this newly specified “User Kerberos principal name, no prompting” selection, or you will use the Kerberos function only once during the current PC 5250 emulation window when performing a new connection. To ensure that the Kerberos principal is used in later 5250 emulation connections, you can perform the save of the changed properties when exiting the PC 5250 emulation window in response to a message window that appears indicating you have made changes or within an active PC 5250 emulation session window by selecting **File** → **Save** from the menu bar.

When you connect to the iSeries server, you get the window displayed as defined for the associated OS/400 user profile. This initial window could be one of the following:

- ▶ OS/400 command or menu window
- ▶ OS/400 window showing past sign-on or message information (DSPSGNINF user profile parameter)
- ▶ A window displayed by an initial program optionally specified in the INLPGM user profile parameter

5.7.6 Verifying iSeries Access for Windows with single signon

Now that we have completed the setup of the Kerberos network and OS/400 Network Authentication Service and Enterprise Identity Mapping components and set up iSeries Navigator and PC5250 emulation connections to use a Kerberos principal, we verify this setup with the following example.

Remember, when connecting through Kerberos and EIM, you should not be prompted for a user ID or password by the server application. Instead, the Kerberos principal is exchanged, and because the authentication is trusted and the mapping is defined properly, there is no need for a password to be exchanged.

If Kerberos and EIM are being used for all access to the system by the mapped to OS/400 user ID, you can even have that user profile's password (PASSWORD) parameter value set to *NONE.

This user ID needs a password if other access to the system by this user does not go through a Kerberos/EIM network. One example requiring a password would be a user signing on to the system from a twinax attached 5250 workstation or using iSeries Access for Windows PC5250 emulation or iSeries Navigator from a workstation not set up to use Kerberos.

In the following topics, we show examples of connecting to the iSeries server in the Kerberos realm and EIM domain using iSeries Navigator and iSeries Access PC5250 emulation.

Before verifying the two applications, we completed the following prerequisites:

1. In order to fully test the configuration, we suggest using at least one user that has a user ID on the iSeries that is different from their Windows logon ID or the same user ID but with the password parameter value set to *NONE.
2. For an example of the associations for such a test user, we use Patricia Boats as explained in "Adding associations" on page 151. Recall that Patricia Boats logs on to her Windows PC using *pboats* (source association), while her OS/400 user profile is *PATRICIAB* (target association).
3. Change the target system or partition's OS/400 user profile of the test user to PASSWORD(*NONE) to demonstrate the full strength of this single signon solution. To do this:
 - a. Using a 5250 workstation, sign on to OS/400 as a user with *ALLOBJ and *SECADM authorities.
 - b. Enter the Change User Profile (CHGUSRPRF) OS/400 command, for example:
`CHGUSRPRF USRPRF(PATRICIAB) PASSWORD(*NONE)`
4. To enable the 5250 emulation for single signon, the system value QRMTSIGN needs to be set to *VERIFY (recommended) or alternatively to *SAMEPRF (less secure environment). Do the following to check, change, or both the QRMTSIGN system value:
 - a. Again, using an OS/400 user with *ALLOBJ and *SECADM authorities, enter the Display System Value (DSPSYSVAL) OS/400 command:
`DSPSYSVAL SYSVAL(QRMTSIGN)`
 - b. If the value shown is *FRCSIGNON or *REJECT, use the Change System Value (CHGSYSVAL) OS/400 command to change the setting:
`CHGSYSVAL SYSVAL(QRMTSIGN) VALUE(*VERIFY)`

Testing iSeries Navigator single signon

We presume your iSeries Navigator client workstation session to the system has been set up to use Kerberos using the "Use the Kerberos principal name, no prompting" parameter as described in 5.7.4, "Setting up Kerberos authentication for an iSeries Navigator session" on page 154.

To verify this, in your iSeries Navigator window, perform the following:

1. In the left panel of the iSeries Navigator window, expand your target iSeries server by clicking the + button to the left of the iSeries server name. This causes the iSeries Navigator code to make a connection to the iSeries system.

When the connection to the iSeries server is started, the hierarchy tree in the left pane for this server is expanded. Note that no sign-on prompt window appeared.

2. To find which user ID this connection is using, click (select) the environment in the left panel (its default name is My Connections, but we use “SSO/EIM environment” in our example) and press the F5 key to refresh the window contents. The user ID now appears next to the iSeries server name in the Signed On User column, as shown in Figure 5-46.

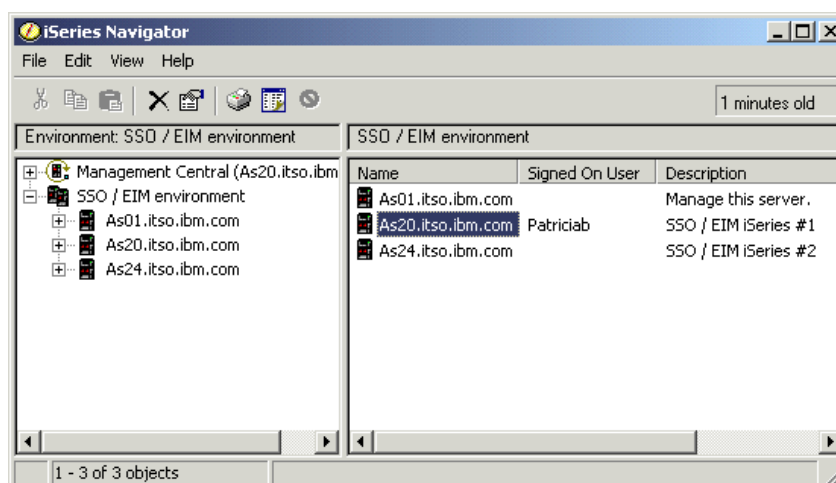


Figure 5-46 iSeries Navigator: Check signed on user

You have completed the verification of the iSeries Navigator single signon.

Testing iSeries Access for Windows 5250 emulation single signon

In this section, we presume your PC5250 emulation session has been set up to use Kerberos authentication using the “Use the Kerberos principal name, no prompting” parameter, as described 5.7.5, “Setting up Kerberos authentication for an iSeries Access PC5250 session” on page 156.

Perform the following to verify that single signon works for the iSeries Access 5250 emulation:

1. Select **Communication** → **Connect** from the menu of the 5250 session window.
2. The session connects to the iSeries server and you are signed on and a window opens, as defined for your mapped to OS/400 user profile: an OS/400 command or menu window, signon information window, or one displayed by an “initial program.” Note that no sign-on prompt window appears.
3. One of the ways to find out which user profile the session is using is to use a 5250 session and enter the OS/400 Display Workstation User (DSPWSUSR) command. No parameters are required. The screen will look similar to the one shown in Figure 5-47.

```

Display Work Station User          AS20
                                     12/02/03  15:30:55
User . . . . . : PATRICIAB
Text . . . . . : Patricia Boats, EIM Residency
862644897
Work station . . . . . : P782XNXKA
Text . . . . . : Device created for AS20.

Number of interactive jobs in session . . : 1
Interactive job currently active . . . . : A
Interactive job A . . . . . : 073320/PATRICIAB/P782XNXKA
Interactive job B . . . . . : *NONE

```

Figure 5-47 Display Workstation User (DSPWSUSR) command results

You have completed the verification of the iSeries Access 5250 emulation single signon.

Note, during the same PC5250 emulation session, you can issue the OS/400 Sign Off (SIGNOFF) command, which does not perform a PC5250 emulation disconnect. If you do this, you are then prompted with the default OS/400 sign-on screen expecting a user ID and password. If the user during this emulation session knows a valid OS/400 user ID and password other than the EIM mapped to OS/400 user profile, that user can sign on to the iSeries system with this different user ID.

Normal confidentiality of other OS/400 user profiles and passwords and using the OS/400 user profile PASSWORD parameter set to *NONE, as described in step 3 on page 158, can assist in restricting this capability.

The Kerberos principal name and “no signon prompt window” processing occurs only when performing the PC5250 emulation **Communication** → **Connect** function or double-clicking a PC5250 emulation icon.

For more details, such as having multiple iSeries systems in the Kerberos realm and EIM domain, refer to:

- ▶ V5R2 Information Center articles. Use EIM as a search argument, or use the left navigation bar and click **Security** → **Enterprise Identity Mapping**.
- ▶ The IBM Redbook *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975.



A

Coming attractions for iSeries Access for Windows

This appendix provides an overview of planned enhancements for iSeries Access for Windows following Version 5 Release 2.

iSeries Access for Windows: Beyond V5R2 overview

iSeries Access for Windows has many new enhancements available at the time this book was being published as a beta level code that can be downloaded from the following location:

<http://www.ibm.com/eserver/iseries/access/>

The following are the primary planned enhancement areas that are included in the beta level code:

- ▶ A new database provider
- ▶ Database enhancements in data transfer, Open Database Connectivity (ODBC), and Object Linking and Embedding (OLE) DB
- ▶ Added function in Incoming Remote Command
- ▶ Integration of the latest Personal Communications 5250 (PC5250)
- ▶ Use of Unicode in configuration utilities

The following topics provide additional summary-level information in these areas.

New database provider

The new IBM.Data.DB2.iSeries Data Provider will allow your applications that use the .NET framework to access DB2 UDB for iSeries databases using a full set of .NET classes and data types. It complements the existing OLE DB providers and allows you to take advantage of the newer .NET technologies to read and retrieve data, make changes, and execute SQL server commands against data objects in the secure environment of your iSeries server.

Data transfer

You will be able to use data compression for faster transfers, and your applications can take advantage of Unicode enablement and a new Unicode text file type. You will be able to manage a larger decimal precision for your numeric data and use the new BINARY and VARBINARY SQL data types. Your DB2 database tables will support UTF-8 and UTF-16 data for additional flexibility.

With Microsoft Excel, new support for standard date and time cells and numeric-to-character conversions will make it easier to manage transfer of data to and from your servers in your desired format. In addition, the Excel Add-in most recently used request list and last directory support will be added for more administrative ease.

ODBC

ODBC support will include BINARY and VARBINARY data types, UTF-8 and UTF-16 data for globalization of your applications, increased precision of decimal numbers, and offers enhanced Microsoft Transaction Server (MTS) support.

OLE DB

Much work has been done in the OLE DB component to keep current with industry advancements. iSeries Access for Windows integrates the following:

- ▶ New SQL-only provider (IBMDASQL)
- ▶ New Record-Level Access-only provider (IBMDARLA)
- ▶ SQL commitment control using IBMDASQL
- ▶ MTS support using IBMDASQL
- ▶ Custom blocking in SQL
- ▶ SQL data compression
- ▶ SQL package support
- ▶ Record-level access support for forward-only cursors and blocked reads using IBMDARLA
- ▶ Database BINARY and VARBINARY data types
- ▶ Database larger decimal precision support
- ▶ UTF-8 and UTF-16 support

Incoming Remote Command (IRC)

You will be able to load the user profile information for a remote command that runs in the security context of a known user ID. Some commands will then succeed that formerly failed due to lack of needed authorization to the user registry and environment variables. You can set and conveniently save this option so that it does not have to be reset each time the command is run.

PC5250

Accessibility enhancements to the operator information area (OIA), will include:

- ▶ Pop-up keypad
- ▶ Color mapping, as well as visual indication of sounds
- ▶ Enhanced mouse marking
- ▶ Bidirectional (LamAlef) enhancements
- ▶ USB Japanese 106 keyboard support
- ▶ basic_ascii print PDF and PDT

Configuration

Configuration utilities available to back up configuration information and to import or export server environments will default to save information using a Unicode encoding but retain the capability to save the information using the ANSI code page for compatibility.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 166. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *Windows-based Single Sign on and the EIM Infrastructure on the IBM @server iSeries Server*, SG24-6975
- ▶ *iSeries IP Networks: Dynamic!*, SG24-6718
- ▶ *IBM @server iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements*, SG24-6168
- ▶ *Managing OS/400 with Operations Navigator V5R1, Volume 1: Overview and More*, SG24-6226
- ▶ *Managing OS/400 with Operations Navigator V5R1, Volume 2: Security*, SG24-6227
- ▶ *Managing OS/400 with Operations Navigator V5R1, Volume 3: Configuration and Service*, SG24-5951
- ▶ *Managing OS/400 with Operations Navigator V5R1, Volume 4: Packages and Products*, SG24-6564
- ▶ *Managing OS/400 with Operations Navigator V5R1, Volume 5: Performance Management*, SG24-6565
- ▶ *Managing OS/400 with Operations Navigator V5R1, Volume 6: Networking*, SG24-6566

Other publications

This publication is also relevant as a further information source:

- ▶ Garman, J., *Kerberos: The Definitive Guide*, O'Reilly & Associates, 2003, ISBN 0596004036

Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ iSeries Information Center

<http://www.ibm.com/eserver/iseries/infocenter>

Select your geographical region, your V5R2 language, and the **Connecting to iSeries** link. You can also search with the keywords Kerberos or EIM.

- ▶ iSeries Access Web site

<http://www.ibm.com/eserver/iseries/access>

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

You can use the Domain field in the left navigation bar to select only iSeries documents.

Index

Symbols

- *ALLOBJ authority 31
- *SECADM authority 31, 40

Numerics

- 5250 emulation 159
- 5250 emulation (PC525) 2
- 5250 Telnet 123
- 5722-AC3 123
- 5722-CE3 8, 12, 84, 123
- 5722-SS1 Option 12 123
- 5722-SS1 Option 30 123
- 5722-XE1 vii, 7, 84, 123

A

- Abstract Syntax Notation One (ASN.1) 100
- Access denied 42
- account for delegation 122
- Account is trusted for delegation 122
- Active Directory 106, 117, 119
 - Windows Web site 117
- Active Directory home page 117
- Active Directory Users and Computers window 122
- Add domain 149
- Add Environment 49
- Add Server 49
- adding EIM identifiers 150
- Administer Users by Default 35
- Administer users by default 36
- administrable function 30
- Administration system 54
- administration system 31–33
 - client discovery 50
 - tip 35
- Administration system and Central Settings overview 30
- Administration system discovery
 - install 53
 - Signon 52
- Administration System tab 33
- administration system tip 35
- administrative HTTP server
 - *ADMIN 67
- advanced Central Settings
 - mandated 45
 - suggested 45
- Advanced Settings
 - Add Profile 45
 - Remove 46
- Advanced Settings - Add Profile 45
- Advanced Settings tip 44
- AIX 104, 134
- All Object Access 40
- all object authority 31

- All Users 42
- Allow all incoming remote commands when password caching is disabled 47
- Allow caching of server passwords 47
- Allow creation of user certificates 62, 70
- Allow user to add connections to environment 49
- Allow user to define additional environments 49
- alternate response file
 - f1d parameter 24
 - file.iss 24
- ANSI code page 48
- Application Administration
 - administration system 31
- Application Administration component 30
- Application Administration concepts
 - administration system 31
 - Local Settings 32
- Application Administration note 14
- application registry definition 139
- Applications available to be administered list 38
- Applications to be administered list 38
- APYPTF 16
- Arabic 48
- association
 - administrative 141
 - source 141
 - target 141
- Association type 140
- authentication server 105
- authentication server (Kerberos) 101
- authority groups 142
- Available administration systems and users 51

B

- background service job 48
- Basic Customization 41
- BM Developer Kit for Java (5722-JV1) 58
- BootOption 24
- BootOption=3 27

C

- CA certificate 60
- CA Policy 62
- caecfg.adm policy 30
- caerestr.adm template 30
- case insensitive 113
- case sensitive 113, 125
- CCSID 48
- CD 20
- central administration of users or groups 36
- Central Server 64
- Central Settings 30, 32, 35, 37
 - advanced 43
 - Advanced Settings for iSeries Access for Windows

- 37
- Application Administration example 40
- basic 41
- basic customization 41
- choosing an administration system 32
- configuration 37
- connections 43, 46
- discover 43
- Environments 43
- groups 36
- implementation 32
- iSeries Access for Windows 37
- Language 43
- languages 48
- managing 39
- mandated values 37
- Passwords 43
- registration 37
- Service 43
- Central Settings - Advanced 43
- certificate 60
 - assigning to an application 64
 - common name 63
 - editing 83
 - expiration 56
 - validity period 93
 - view applications assigned 94
 - viewing expiration date 91
- certificate authority 67
- certificate authority (CA) 60
- certificate authority (CA) certificate 61
- certificate authority (CA) download 86
- certificate importance 56
- certificate store password 63
- Change Network Time Protocol Attributes 114
- Change policy data 69
- Character conversion overrides 48
- Check Service Level shortcut 22
- CHGNTPA 114
- Choosing an administration system 32
- client authentication
 - using multiple user certificates 90
- client certificates
 - browser considerations 67
 - important tip 67
- client discovery of administration system 50
- Client Encryption 128-bit 123
- Client Encryption 128-bit, 5722-CE3 6
- Client Encryption product (5722-CE3) 58
- coded character set identifier 48
- completion percentage 23
- component
 - deletion 14
- Component Selection window 11
- Compromise of the KDC 105
- Compromise of users passwords 105
- config.adm property 30
- Configuration and Service vii, 2
- Configuration Policies 30
- Configuring PC5250 Emulation to use SSL 89

- connections 46
- connections list
 - automatically downloaded 48
- Create a Certificate Authority (CA) tip 61
- Create and join a new EIM domain 143
- Create Directory 124
- Create Keytab Entry 127
- Creating Active Directory account for iSeries 119
- Creating user certificate for client authentication 67
- Crypto Access Provider 123
- Cryptographic Access Provider 128-bit for AS/400, 5722-AC3 6
- Custom installation 6
- Customize Administration of Users 35–36
- Customized Access 40
- cwbcssl.exe 57
- cwbinimg 7
- cwbinimg.bat 9
- cwbinimg.bat file 8
- cwbssldf.kd 80
- CWBSY1012 message 113
- CWBSY1017 - rc=608 message 113

D

- data transfer 2
- Database access 2
- Default Access 40
- Default User 44
- Delete domain 149
- Deselect 12
- destination directory 10
- destination folder 10
- Digital Certificate Manager (DCM) 58
- Digital Certificate Manager link 60
- digital signature 60
- Distributed Data Management (DDM) 123
- Distributing and installing the merged installation image 20
- DNS 111, 131
- domain 136
- domain controller 135
- domain name 125
- Domain Name Service (DNS) 111
- Domain Name System 110
- DRDA 122–123
- DSPSGNINF (display sign-on information) 157
- DSPWSUSR 159

E

- EBCDIC code page 48
- EIM
 - Domain Controller 134
 - registry 133
 - registry type 133
- EIM administrator 141
- EIM and registry passwords 136
- EIM association
 - Add associations 151
 - Source association 141

- Target association 141
- EIM Associations 140
- EIM authorities 142
- EIM domain 136
 - adding the EIM domain 149
- EIM Domain Controller 133
- EIM domain controller 135
- EIM example 134
- EIM identifier 132–134, 136–137
 - aliasing 138
 - Source association 141
 - Target association 141
- EIM identifier name 140
- EIM identifiers
 - adding a new Identifier 150
- EIM installation 134
- EIM lookup operation 141
- EIM lookup operations 140, 142
 - EIM domain controller 142
 - EIM registry definition 142
 - identifier 142
 - source 142
 - target 142
 - user identity 142
- EIM predefined registries
 - Domain Name Service (DNS) 140
 - Issuer distinguished name (DN) 140
 - Kerberos 140
 - LDAP DNS host name 140
 - Root distinguished name (DN) 140
 - TCP/IP address 140
- EIM registry
 - AIX 139
 - aliases 140
 - Kerberos Key Distribution Center 138
 - OS/400 139
 - OS/400 user profiles 138
 - z/OS RACF 138–139
- EIM registry definition name 140
- EIM registry definitions and aliasing 140
- EIM requirement 108
- Enable bidirectional script transformations 48
- encrypted ticket 105
- encryption key 106
- enrolling the Windows client workstation 106
- Enrolling the Windows client workstation in the Windows Domain 109
- Enterprise Identity Mapping 4, 132
- Enterprise Identity Mapping (EIM) 97
- Environmental Variables 119
- environments 37
- Environments window 48
- exclude users 14
- expiration of a certificate 56

F

- File Permissions 14
- fix level 7, 14
- Full installation 6

G

- Generic Security Services API (GSS) 100
- Groups 42, 44
- GUI download 41

H

- Hebrew 48
- Heimdal 100
- home directory 124
- Host Domain Information 112
- Host on Demand 123
- Host Servers 123
 - ending and starting 66
- hosts file 111
- http 58
- HTTP (Powered by Apache) 123
- HTTP Administration Server 58
- HTTP administration server 59

I

- IBM Cryptographic Access Provider (5722-AC3) 58
- IBM Digital Certificate Manager (DCM), option 34 58
- IBM Directory Server 135–136
- IBM HTTP Server for iSeries (5722-DG1) 58
- IBM Key Management 67
- IBM Key Management and key database file 80
- IBM Key Management database 79
- identifier 136
 - aliases 138
- identity mapping 140
- Import certificate 82
- Importing the User Certificate 80
- Information Center 32
- INLPGM (initial program) 157
- install
 - Custom 21
 - destination folder 19
 - Full 21
 - Typical 21
- install image 35
- install image and service packs 15
- installation
 - silent 5
- Installation Image Administration System 35
- Installation image location 54
- installation install program - cwbimimg 7
- installation of user certificate
 - Netscape Communicator 72
- installation upgrade 14
- installation wizard 14
 - not copied 14
- Installing Secure Sockets on your Windows PC client 84
- Integrated File System (IFS) management 2
- Internet Explorer 67
- iSeries Access for Windows
 - multiple languages 10
- iSeries Access for Windows Application Administration 108
- iSeries Access for Windows overview 2

- iSeries Access for Windows Properties 22, 27
- iSeries Access for Windows service pack 15
- iSeries Access for Windows setup 6
- iSeries Access for Windows shortcut 67
- iSeries Access for Windows SSL utility program 56
- iSeries Access Install Image 11, 19
- iSeries Kerberos Authentication 127
- iSeries Navigator vii, 150
 - 158
 - adding EIM associations 151
- iSeries Navigator File Permissions 14
- iSeries Navigator Network component 142
- iSeries Navigator Security component 124
- iSeries Network Authentication Service 123
- iSeries server 7, 15
- iSeries Setup and Operations CD 7
- iSeries system defined in KDC 119
- iSeries system software required 123
- iSeries' name network resolution 111

J

- JDBC/ODBC 123

K

- KDC Information (iSeries Navigator Network Authentication interface) 125
- KDC server setup 116
- KDC setup on iSeries Network Authentication Service 130
- kdestroy 107
- Kerberized application 105
- Kerberized applications 105
- Kerberos 4, 97, 112
 - authentication requirement 98
 - case sensitive 113
 - complete the Active Directory account 122
 - creating Active Directory account for your iSeries 119
 - default port (88) 125
 - EIM requirement 4
 - iSeries Access for Windows 97
 - iSeries functions supporting Kerberos authentication 123
 - iSeries Navigator enablement 99
 - iSeries Navigator interface 124
 - password never expires 120
 - passwords, password change 126
 - protocol components 102
 - realms 103
 - Services 102
 - setting up an iSeries server 123
 - Setting up the iSeries principal name on the KDC 119
 - supported iSeries services 123
 - time value considerations 113
- Kerberos - DNS host name tip 113
- Kerberos and network security considerations 105
- Kerberos and SNTP 115
- Kerberos and uppercase 120
- Kerberos commands
 - kadmin 107

- kdestroy 106
- kinit 106
- klist 106
- kpasswd 107
- ksetup 108
- ktpass 107
- Kerberos concepts 101
- Kerberos credentials and home directory 124
- Kerberos KDC and iSeries 104
- Kerberos KDC service status 116
- Kerberos overview 99
- Kerberos password server 104
- Kerberos principal 101
- Kerberos principal name 155
- Kerberos services
 - iSeries 122
 - iSeries Navigator 122
 - OS/400 host servers 122
- Kerberos support tools 117
- Kerberos tickets 103
- key database 67
- key database file
 - password 80, 82
 - Personal Certificates 82
- key database importance 56
- key database passwords 56
- Key Distribution Center 116
 - KDC 102
- Key Distribution Center (KDC) 100
- Key Distribution Center database 105
- Key Distribution Center server database 101
- key table 131
- keytab file definition 127
- keytab list 108, 130
- kinit 107
- kinit command 113, 131
- klist command 131
- ksetup 108
- ktpass 107, 118–119, 121
- ktpass and iSeries 108
- ktpass command parameters 121

L

- Language option 10
- languages 48
- LDAP 123, 127, 135
- Lightweight Directory Access Protocol (LDAP) 106
- Lightweight Third-Party Authentication (LTPA) 138
- Linux 134
- local CA 63
- Local Certificate Authority (CA) 68
- Local Security Authority (LSA) 106
- Local Settings 30–32, 37
- locked padlock icon 46
- LODPTF 16
- log file for silent install 24
- log file return codes 23
- logical partition (LPAR) 136
- lookup operation 142

M

- Machine Readable Image 8
- Manage Local CA 69
- Management Central 2
 - Synchronize Date and Time 116
- Management Central using SSL 65
- mandated 48
- mandated and suggested settings example 46
- Mandated Connection Properties 30
- mandated setting 46
- mapOp on ktpass 121
- mapped drive 9
- mapuser on ktpass 121
- Massachusetts Institute of Technology (MIT) 100
- Merging service pack in the install image on a network drive 16
- Merging service pack with install image on iSeries server 15
- Microsoft Transaction Server (MTS) 162
- MIT version of Kerberos 100
- MRI 8
- Multiple profiles 45
- My Connections 32

N

- Name Server Lookup (NSLOOKUP) 112
- NET HELP TIME 114
- Netscape 67
- Netscape Communicator - exporting the User Certificate 78
- NetServer 127
- netstat *cnn 66
- Network Authentication Service 4, 109, 112, 124
 - Configuration Summary 129
- Network Authentication Service (iSeries Navigator interface) 124
- Network Authentication Service Configuration
 - create keytab entry 128
- Network Authentication Service configuration wizard 120
- Network Authentication Service verification 132
- network drive 7, 15
- Network management 2
- node 136
- Notes and tips 14
- NSLOOKUP (Name Server Lookup) 112

O

- OEM 48
- OEM code page 48
- original equipment manufacturer 48
- OS/400 Certificate Authority download 87
- OS/400 Host Servers 123
- OS/400 V5R2 Kerberos authentication important tip 123
- overriding the central setting 46

P

- Padlock icons 45
- parent Certificate Authority 80

- pass on ktpass 121
- Password 120
- password
 - Kerberos shared secret 120
- password and Kerberos 106
- password changes and Kerberos 106
- Password expire warning 47
- passwords
 - Kerberos suggestion 120
- PC5250 2, 56, 122
- PC5250 installation 6
- PCOMM 5250 emulation 123
- Perform silent installation 27
- Performance setting 47
- Personal Information Exchange 76
- Personal Information Exchange (.pfx) file type 77
- PKCS12 File (.p12) file type 79
- plug-ins 2
- port numbers 66
- princ on ktpass 121
- principal 133
- principal (OS/400 user) 124
- principal name - case sensitivity 131
- principals 98
- Principals and Realms 102
- Printer Output 30
- private CA (Certificate Authority) 60
- private key 60, 67
- Properties 32
- protect you private key 73
- PTFFORM.EXE 16–17
- public key 60

Q

- QFileSrv.400 122
- QFileSrv.400 123
- QIBM/ProdData/Access/Windows/Install/Image directory 9
- QIBMProdDataAccess 7
- QRMTSIGN and EIM 158
- QRMTSIGN system value 158
- qsh 130
- QShell command 130
- QShell Interpreter 123, 130
- QTIME 116
- QUTCFFSET 116

R

- realm 101, 125
 - Microsoft network 106
- Receiving a ticket granting ticket 105
- Redbooks Web site 166
 - Contact us ix
- registry 133
- registry definition 138
 - aliases 140
 - application 139
 - system 139

- Remove domain 149
- Remove server 49
- Rename server 49
- renewing a certificate 91
- response file 23, 27
 - alternate 24
 - example 24
 - silent service pack install 27
- response file creation 23
- response file example 24
- restricting users
 - tip 14
- Runtime Restrictions 30

S

- scan frequency 34–35
- secondary language 10
- secret key 101
- Secure Sockets Layer
 - IBM Key Management 56
- Secure Sockets Layer (SSL) 6
- Secure Sockets tab 86
- Security 2, 160
- security administrator 31
- Send PTF Order (SNDPTFORD) 15
- server connections 37
- server passwords 47
- service 27
- service pack 15
- service pack and install image 14
- service pack download tip 17
- service pack merge
 - on the iSeries server 15
- service pack merge caution 16
- service pack shortcut 22
- Service Pack SI09808 51
- service pack tip - temporary folder 17
- Service Packs 16
- service principals 109
- service ticket 99
- Set as default 36
- Set Installation Image Administration System 34, 54
- Set Installation Image Administration System button 53
- Setting up an operational Kerberos realm example 109
- Setting up iSeries system user IDs 124
- Setting up iSeries system user IDs and home directories 124
- Setting up Kerberos authentication for an iSeries Navigator session 154
- Setting up Network Authentication Service 124
- Setting up the iSeries principal name on the KDC 119
- setup -r (create response file for silent install) 23
- setup restrictions 30
- setup -s (start silent install) 24
- Setup.exe 20
- setup.exe 27
- setup.iss 24
- setup.iss file 24
- setupsp.bat 22
- shared secret 105, 120, 128

- SI09808 113
- Signon information 46
- Signon Server 64
- silent install
 - file.log 24
 - response file 24
 - response file national language version 24
- silent install - SCHEDCHECK 27
- silent install debug 23
- Silent Install Indicator 23
- silent install of service packs 27
- silent install of upgrades 27
- silent install tip 23
- silent installation
 - f1 24
 - f2 24
 - start 24
- silent service pack install
 - automatic reboot 27
- single sign on 133
- single signon
 - enabling iSeries Navigator 157
- single signon (SSO) 132–133
- SLTSP.ISS - for service packs 27
- SLTSP.ISS - for upgrades 27
- SLTSP.ISS file 27
- SNDPTFORD 15
- Specify Password Server Information (iSeries Navigator Network Authentication Service interface) 126
- SQL 123
- SSL 46
 - 128-bit level encryption 56
 - 5250 client authentication 56
 - client authentication 56
 - key database 67
 - Management Central consideration 65
 - Remote Command 56
 - server authentication 56
 - Ultimedia 56
 - using Selective Setup to install 84
 - verifying the connection 87
- SSL prerequisites 58
- SSL setting 47
- Start Copying Files window 12
- strqsh 130
- STRTCPSVR 67
- STRTCPSVR SERVER(*NTP) 115
- suggested setting 46
- support tools
 - Kerberos commands on iSeries 108
 - successful installation 118
- support tools (Kerberos on Windows server) 108
- system administrator 31
- System and application registry definitions 139
- System Certificate 58
 - assigning to Telnet, host servers 58
- system certificate 63
- system registry definition 139
- system store 63
- system time value (Kerberos) 109

System Variables 119

T

- tailored directory 17
- tailored image completion 13
- tailored image directory name 11
- tailored installation image
 - create 5
- tailored installation image distribution 20
- Tailored installation image wizard 7
- tailored installation image wizard - from iSeries 8
- tailored installation images 14
- tailored installation tips 14
- TCP/IP Connectivity Utilities for iSeries (5722-TC1) 58
- TCP/IP network host name - TCP/IP address resolution 109
- TCP/IP network host name resolution considerations 110
- Telnet Server 64
- Telnet server
 - ending and starting 66
- Testing iSeries Navigator single signon 158
- ticket 102
- ticket encrypting 105
- ticket granting server (Kerberos) 101
- ticket granting service 133
- ticket granting ticket 99
- ticket granting ticket (TGT) 101, 103, 105
- tickets 101
- time skew 113
- time skew (Kerberos) 109
- time synchronization 116
- trusted root 60
- Typical installation 6

U

- Unauthorized access to a client machine. 105
- Unauthorized access to servers 105
- UNC share 9
- Universal Naming Convention share 9
- unlocked padlock icon 46
- US Export regulations 6
- User and group profile management 2
- user certificate installation
 - Internet Explorer 72
- user exit programs 30
- User identity authentication 140
- user identity authorization 140
- User identity name 140
- user principal 117
- user principals 109
- user profile 30
- user profile PASSWORD(*NONE) consideration 160
- user registry 136
- Users 36, 44
- Users administered 36
- Users and Groups folders 44
- Users not administered 36
- Users Not in a Group 42
- users or groups 36

using 122

V

- Verifying successful support tools installation 118
- VeriSign 60
- Viewing a Certificate Authority Certificate 91

W

- Windows 2000 KDC 120, 125
- Windows 2000 Server 104
- Windows Active Directory 116
- Windows administration 2
- Windows Kerberos support tools 117
- Windows Server 2003 104
- Windows user 30
- Windows Install Image directory 8
- Work Management vii, 2, 30
- Work with TCP/IP Connection Status 66
- WRKLNK 14

X

- XP 99

Z

- z/OS 104, 134



iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos



**Speeding up your
multiple workstation
install using a tailored
image**

**Centralizing your
Application
Administration tasks**

**Securing your
connections with SSL
and Kerberos single
sign on**

This IBM Redbook covers the “hot topic tasks” (according to client feedback) related to running the following iSeries Access for Windows, 5722-XE1, capabilities:

- ▶ iSeries Access for Windows installation, focusing on tailored and silent installation
- ▶ iSeries Access for Windows Application Administration, focusing on the new starting in V5R2, Central Settings support
- ▶ Setting up iSeries Access for Windows functions to use Secure Sockets Layer (SSL) support
- ▶ iSeries Access for Windows functions using Kerberos and IBM Enterprise Identity Mapping (EIM) network authentication capabilities

This information should get you up and running quickly using these capabilities.

This book also includes a summary of what is coming in the next release of iSeries Access for Windows by describing what is available as Beta code from the iSeries Access Web site at:

<http://www.ibm.com/eserver/iseries/access/windows>

The information in this book is generally available through sets of information located at the various iSeries Web sites, but is documented here all in one place and with actual examples.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:
ibm.com/redbooks**