



System i
Security
Single sign-on

Version 6 Release 1





System i
Security
Single sign-on

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in “Notices,” on page 87.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© **Copyright International Business Machines Corporation 2004, 2008.**

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

Contents

Single sign-on	1
What's new for V6R1	1
PDF file for Single sign-on.	2
Single sign-on concepts	2
Single sign-on overview	2
Authentication.	3
Authorization	4
Domains.	5
Identity mapping.	6
i5/OS enablement	8
ISV enablement	9
Scenarios: Single sign-on	10
Scenario: Creating a single sign-on test environment	10
Completing the planning work sheets	13
Creating a basic single sign-on configuration for System A	16
Adding System A service principal to the Kerberos server	18
Creating home directory for John Day on System A	19
Testing network authentication service configuration on System A	19
Creating an EIM identifier for John Day	20
Testing EIM identity mappings	20
Configuring System i Access for Windows applications to use Kerberos authentication.	21
Verifying network authentication service and EIM configuration	22
(Optional) Postconfiguration considerations.	22
Scenario: Enabling single sign-on for i5/OS.	23
Completing the planning work sheets	28
Creating a basic single sign-on configuration for System A	33
Configuring System B to participate in the EIM domain and configure System B for network authentication service	35
Adding both i5/OS service principals to the Kerberos server	37
Creating user profiles on System A and System B	38
Creating home directories on System A and System B	38
Testing network authentication service on System A and System B	39
Creating EIM identifiers for two administrators, John Day and Sharon Jones.	39
Creating identifier associations for John Day	40
Creating identifier associations for Sharon Jones	41
Creating default registry policy associations	42
Enabling registries to participate in lookup operations and to use policy associations	43

Testing EIM identity mappings	44
Configuring System i Access for Windows applications to use Kerberos authentication.	47
Verifying network authentication service and EIM configuration	47
(Optional) Postconfiguration considerations.	48
Scenario: Propagating network authentication service and EIM across multiple systems	48
Completing the planning work sheets	53
Creating a system group	55
Propagating system settings from the model system (System A) to System B and System C	55
Completing the configurations for network authentication service and EIM on System B and System C	56
Configuring network authentication service and EIM on the V5R2, or later, system System D.	57
Scenario: Configuring the Management Central servers for single sign-on.	58
Verifying that the domain appears in Domain Management	61
Creating EIM identifiers	61
Creating identifier associations	62
Configuring the Management Central servers to use network authentication service.	62
Configuring the Management Central servers to use EIM	63
Scenario: Enabling single sign-on for ISV applications	64
Completing the planning prerequisite worksheet	65
Writing a new application or change an existing application.	66
Creating a single sign-on test environment	67
Testing your application	67
Example: ISV code	68
Planning for single sign-on	76
Requirements for configuring a single sign-on environment	76
Single sign-on planning worksheets	77
Configuring single sign-on	80
Managing single sign-on	82
Troubleshooting single sign-on	82
Related information for Single sign-on	86
Appendix. Notices	87
Programming interface information	88
Trademarks	89
Terms and conditions	89

Single sign-on

If you are looking for a way to eliminate the number of passwords that your users must use and that your administrators must manage, then implementing a single sign-on environment might be the answer you need.

This information presents a single sign-on solution for i5/OS[®], which uses network authentication service (IBM's implementation of the Kerberos V5 standard from MIT) paired with Enterprise Identity Mapping (EIM). The single sign-on solution reduces the number of sign-ons that a user must perform, as well as the number of passwords that a user requires to access multiple applications and servers.

Note: Read the “Code license and disclaimer information” on page 86 for important legal information.

What's new for V6R1

Read about new or significantly changed information for the single sign-on topic collection.

New or enhanced functions for single sign-on



- | • In previous releases of i5/OS single sign-on only supported mapping to one local user identity in Enterprise Identity Mapping (EIM) per system. In i5/OS V6R1 single sign-on supports selecting from multiple local user identity mappings for the same system, using the IP address of the target system to select the correct local user identity mapping on that system.
- | • EIM and network authentication service enhancements
- | Many of the new or enhanced single sign-on functions are a result of new and enhanced function for EIM and network authentication service, the two technologies which make up the i5/OS single sign-on solution. Refer to the following topics for more information about specific enhancements:
 - | – What's new for EIM
 - | – What's new for Network authentication service

New or enhanced information about this topic

Previously, information about the single sign-on function was available in the network authentication service and EIM topics because these are the two technologies that function together to enable the single sign-on environment. This new topic provides centralized information about configuring and using single sign-on. This new topic also provides enhanced and more complete information, including important concepts, detailed planning material, and scenarios that help you determine when and how to use the single sign-on capabilities.

How to see what's new or changed

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

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

In PDF files, you might see revision bars (|) in the left margin of new and changed information.

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

PDF file for Single sign-on

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select Single sign-on (about 600 KB).

You can view or download these related topics:


- Enterprise Identity Mapping (EIM) (about 700 KB). Enterprise Identity Mapping (EIM) is a mechanism for mapping a person or entity (such as a service) to the appropriate user identities in various user registries throughout the enterprise.
- Network authentication service (about 990 KB). Network authentication service allows your system to participate in an existing Kerberos network.

Saving PDF files

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

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe® Reader

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

Single sign-on concepts

Single sign-on uses multiple services and technologies to achieve a solution that offers simplified identity and authorization management.

The following topics explain the benefits of single sign-on and how different services are used to create this solution. Before you begin using single sign-on, you might find it helpful to review these concepts:

Single sign-on overview

A single sign-on solution is designed to alleviate the use of having multiple user names and passwords across your enterprise. Implementing a single sign-on solution benefits user, administrators, and application developers.

In traditional network environments, a user authenticates to a system or application by providing user credentials defined on and by that system or application. Traditionally, both authentication and authorization mechanisms use the same user registry when a user attempts to access a resource managed by the system or application. In a single sign-on environment, authentication and authorization mechanisms do not have to use the same user registry to enable users to resources managed by the system or application. Single sign-on environments use network authentication service (Kerberos authentication) as their authentication mechanism. In a single sign-on environment, the user registry used for authentication does not have to be the registry that the system or application defines. In a traditional network environment, this poses a problem for authorization.

In a single sign-on network environment, applications use Enterprise Identity Mapping (EIM) to solve this problem. EIM is a mechanism for mapping or associating a person or entity to the appropriate user identities in various registries throughout the enterprise. Application developers for i5/OS use EIM to build applications that use one user registry for authentication and another for authorization--without

requiring the user to provide another set of credentials. The benefits of a single sign-on environment are numerous, and not just for users. Administrators and application developers can also benefit from the single sign-on solution.

Benefits for users

The single sign-on solution reduces the number of sign-ons that a user must perform to access multiple applications and servers. With single sign-on, authentication occurs only once when users sign into the network. Using EIM reduces the need for users to keep track of and manage multiple user names and passwords to access other systems in the network. After a user is authenticated to the network, the user can access services and applications across the enterprise without the need for multiple passwords to these different systems.

Benefits for administrators

For an administrator, single sign-on simplifies overall security management of an enterprise. Without single sign-on, users might cache passwords to different systems, which can compromise the security of the entire network. Administrators spend their time and money on solutions to diminish these security risks. Single sign-on reduces the administrative overhead in managing authentication while helping to keep the entire network secure. Additionally, single sign-on reduces the administrative costs of resetting forgotten passwords. Administrators can set up a single sign-on environment where a user for a Microsoft® Windows® operating system can sign-on once and have access to the entire network, thus minimizing authentication and identification management.

Benefits for application developers

For developers of applications that must run in heterogeneous networks, the challenge is to create multi-tiered applications where each tier is likely to be a different type of platform. By exploiting EIM, application developers are free to write applications that use the most appropriate existing user registry for authentication while using a different user registry for authorization. Not having to implement application specific user registries, associated security semantics, and application level security significantly lowers the cost of implementing multi-tiered, cross-platform applications.

Related concepts

“Authentication”

Authentication is part of a single sign-on solution because it identifies who a user is and then proves it, typically based on a user name and password.

“Authorization” on page 4

Authorization is a process in which a user is granted access to a network or system resource.

Related information

Enterprise Identity Mapping

Authentication

Authentication is part of a single sign-on solution because it identifies who a user is and then proves it, typically based on a user name and password.

The process of authentication is different from the process of authorization, in which an entity or a person is granted or denied access to a network or system resource.

A single sign-on environment streamlines the process and management of authentication for users and administrators. Because of the way single sign-on is implemented on your system, not only do users need to supply fewer IDs and passwords but, if you choose to, they do not even need to have a i5/OS passwords. Administrators need to troubleshoot identity and password problems less often because users need to know fewer identities and passwords to access the systems that they use.

Interfaces that are enabled for single sign-on require the use of Kerberos as the authentication method. Network authentication service is the i5/OS implementation of the Kerberos authentication function. Network authentication service provides a distributed authentication mechanism through the use of a Kerberos server, also called a key distribution center (KDC), which creates service tickets that are used to authenticate the user (a **principal** in Kerberos terms) to some service on the network. The ticket provides proof of the principal's identity to other services that the principal requests in the network.

Note: If you are an application developer, it is possible to make use of other types of authentication methods as you enable your applications to work in a single sign-on environment. For example, you can create applications that use an authentication method, such as digital certificates, in conjunction with EIM APIs to enable your application to participate in a single sign-on environment.

Related concepts

"Single sign-on overview" on page 2

A single sign-on solution is designed to alleviate the use of having multiple user names and passwords across your enterprise. Implementing a single sign-on solution benefits user, administrators, and application developers.

"Authorization"

Authorization is a process in which a user is granted access to a network or system resource.

Related information

Network authentication service

Authorization

Authorization is a process in which a user is granted access to a network or system resource.

Most enterprises use a two-stage process to allow users to access network assets. The first stage of this process is authentication. Authentication is a process in which a user identifies themselves to the enterprise. Typically this requires the user to provide an identifier and a password to the security component of the enterprise. The security component verifies the information that it receives. After a successful authentication, the user is issued a process they can use, a credential, or a ticket to use to demonstrate that they have already authenticated to the enterprise. An example of a user authentication is the ID and password challenge on a System i® Navigator connection. After successful authentication, the user is assigned a job that runs under their user ID. The second stage is authorization. It is important to know the distinction between authentication and authorization.

Authorization is the process of determining if an entity or person has the authority to access an asset within an enterprise. Authorization checks are done after a user has authenticated to the enterprise, because authorization requires that the enterprise knows who is trying to gain access. Authorization checking is mandatory and occurs as part of the system. Users are typically unaware that authorization checks occur unless their access is denied. An example of authorization occurs when a user uses the command CRTSRCPF QGPL/MYFILE. The system performs authorization checks on the command CRTSRCPF and the library QGPL. If the user does not have the authority to access the command and the library, the user's request fails.

An enterprise that has implemented the i5/OS single sign-on solution uses Enterprise Identity Mapping (EIM) to manage user access to enterprise assets. While EIM does not perform authorization checks, the identity mapping establishes the local identities for users that have successfully authenticated into the enterprise. The source (or user) receives access and privileges on the target system through the local ID. For example, assume you have the following simple enterprise environment:

Employee Name (EIM Identity)	Source Users (EIM Source)	Target users for System A (EIM Target)	Employee Responsibility	System A User Comments
Susan Doe	SusanD	SecOfficer	IT Security Officer	All special authority. Has access to all files and information.
Fred Ray	FredR	PrimeAcnt	Lead Accountant	No special authority. Has access to all payroll information.
Nancy Me	NancyM	PrimePGM	IT Application Team Leader	No special authority. Has access to all company application source files.
Brian Fa	BrianF	GenAcnt1	Accountant	No special authority. Has access to some payroll information.
Tracy So	TracyS	ITPgm2	IT Programmer	No special authority. Has access to some company application source files.
Daryl La	DarylL	ITPgm3	IT Programmer	No special authority. Has access to some company application source files.
Sherry Te	SherryT	PrimeMKT	Marketing Representative	No special authority. Has access to all marketing data.

It is important that all of the associations between users and resources are set up correctly. If the associations are incorrect, users will have access to data outside the scope of their responsibilities, which is a security concern for most enterprises. System administrators need to be very careful when creating the EIM mappings and ensure that they map users to the correct local registry IDs. For example if you mapped the IT Programmer, Daryl La, to the SecOfficer ID instead of Susan Doe, you could compromise the security of the system. This reinforces the fact that security administrators must still take care in securing the target systems within the enterprise.

Related concepts

“Single sign-on overview” on page 2

A single sign-on solution is designed to alleviate the use of having multiple user names and passwords across your enterprise. Implementing a single sign-on solution benefits user, administrators, and application developers.

“Authentication” on page 3

Authentication is part of a single sign-on solution because it identifies who a user is and then proves it, typically based on a user name and password.

Related information

Enterprise Identity Mapping

Domains

EIM and Windows domains are used to implement a single sign-on environment.

Although both the EIM domain and Windows domain contain the word domain, they have very different definitions. Use the following descriptions to understand the differences between these two types of domains.

EIM domain

An EIM domain is a collection of data, which includes the EIM identifiers, EIM associations, and EIM user registry definitions that are defined in that domain. This data is stored in a Lightweight Directory Access Protocol (LDAP) server, such as the IBM® Tivoli® Directory Server for i5/OS, which can run on any system in the network, defined in that domain. Administrators can

configure systems (EIM clients), such as i5/OS, to participate in the domain so that systems and applications can use domain data for EIM lookup operations and identity mapping.

Windows 2000 domain

In the context of single sign-on, a Windows 2000 domain is a Windows network that contains several systems operating as clients and servers and a variety of services and applications used by the systems. The following are some of the components pertinent to single sign-on that you might find within a Windows 2000 domain:

Realm A realm is a collection of machines and services. The main purpose of a realm is to authenticate clients and services. Each realm uses a single Kerberos server to manage the principals for that particular realm.

Kerberos server

A Kerberos server, also known as a key distribution center (KDC), is a network service that resides on the Windows 2000 server and provides tickets and temporary session keys for network authentication service. The Kerberos server maintains a database of principals (users and services) and their associated secret keys. It is composed of the authentication server and the ticket granting server. A Kerberos server uses Microsoft Windows Active Directory to store and manage the information in a Kerberos user registry.

Microsoft Windows Active Directory

Microsoft Windows Active Directory is an LDAP server that resides on the Windows 2000 server along with the Kerberos server. The Active Directory is used to store and manage the information in a Kerberos user registry. Microsoft Windows Active Directory uses Kerberos authentication as its default security mechanism. Therefore, if you are using Microsoft Active Directory to manage your users, you are already using Kerberos technology.

Related concepts

“Identity mapping”

Identity mapping is the process of using defined relationships between user identities in an enterprise such that applications and operating systems can map from one user identity to another, related user identity.

Related information

Enterprise Identity Mapping

Enterprise Identity Mapping Concepts

Identity mapping

Identity mapping is the process of using defined relationships between user identities in an enterprise such that applications and operating systems can map from one user identity to another, related user identity.

The ability to map between identities is essential to single sign-on enablement, as it allows you to separate the process of authentication from that of authorization. Identity mapping allows a user to log on to a system and be authenticated based on the credentials of one user identity and then be able to access a subsequent system or resource without having to supply new credentials. Instead, the authenticated identity is mapped to the appropriate identity for the requested system or resource. Not only does this make life easier for the user, who need not supply a second credential for logging on to the second system, but the authorizations he has for the second system are handled by the appropriate identity.

To implement single sign-on, you need to create certain EIM data within the EIM domain to define the relationships needed to appropriately map identities within your single sign-on environment. Doing so ensures that EIM can use that data to perform mapping lookup operations for single sign-on. You use

EIM to create associations to define the relationships between user identities in your enterprise. You can create both identifier associations and policy associations to define these relationships depending on how you want identity mapping to work.

Identifier associations

Identifier associations allow you to define a one-to-one relationship between user identities through an EIM identifier defined for an individual. Identifier associations allow you to specifically control identity mapping for user identities and are especially useful when individuals have user identities with special authorities and other privileges. These associations dictate how the user identities are mapped from one to another. In a typical identity mapping situation, you create source associations for authenticating user identities and target associations to map the authenticating user identity to the appropriate user identities for authorized access to other systems and resources. For example, you might typically create the following identifier associations between an EIM identifier and corresponding user identities for a user:

- A source association for the user's Kerberos principal, which is the identity with which the user logs into, and is authenticated to, the network.
- Target associations for each user identity in the various user registries that the user accesses, such as Windows 2000 user profiles.

The following example illustrates how the identity mapping process works for identifier associations. The security administrator at Myco, Inc creates an EIM identifier (John Day) for an employee. This EIM identifier uniquely identifies John Day in the enterprise. The administrator then creates identifier associations between the John Day identifier and two user identities that he routinely uses in the enterprise. These associations define how the user identities are mapped. The administrator creates a source association for the Windows identity, which is a Kerberos principal, and a target association for an Windows 2000 user profile. These associations enable his Windows identity to be mapped to his Windows 2000 user profile.

John Day uses the appropriate user name and password to log on to his Windows 2000 workstation each morning. After he has logged on, he starts System i Access for Windows to use Windows 2000 to access the Windows 2000 system. Because single sign-on is enabled, the identity mapping process uses his authenticated Windows identity to find the associated Windows 2000 user profile and transparently authenticates and authorizes him to Windows 2000.

- | In previous releases of i5/OS single sign-on only supported mapping to one local user identity in Enterprise Identity Mapping (EIM) per system. Currently, single sign-on supports selecting from multiple local user identity mappings for the same system, using the IP address of the target system to select the correct local user identity mapping on that system.

Policy associations

Policy associations allow you to define a many-to-one relationship between a group of user identities in one or more user registries and a specific individual target user identity in another user registry. Typically, you use policy associations to map from a group of users who require the same level of authority for an application to a single user identity with the appropriate authority.

The following example illustrates how identity mapping works when you define policy associations. A number of workers in the Order Receiving Department of Myco, Inc. all need the same type of authorization to access a Web-based application that runs on Windows 2000 on the server. These users currently have user identities for this purpose in a single user registry named Order_app. The administrator creates a default registry policy association to map all the users in the Order_app user registry to a single Windows 2000 user profile. This Windows 2000 user profile, SYSUSER, provides the minimum authority needed for this group of users. Performing this single configuration step allows the administrator to ensure that all users of the Web-based application have the access they need with the proper level of authorization that they need. However, the administrator also benefits because it

eliminates the need to create and maintain individual Windows 2000 user profiles for each user.

Related concepts

“Domains” on page 5

EIM and Windows domains are used to implement a single sign-on environment.

Related information

EIM identifiers

EIM registry definitions

EIM associations

EIM mapping lookup operations

EIM domain

i5/OS enablement

The i5/OS implementation of Enterprise Identity Mapping (EIM) and Kerberos (referred to as network authentication services) provides a true multi-tier single sign-on environment.

The network authentication service is IBM’s implementation of Kerberos and the Generic Security Service (GSS) APIs. You can use EIM to define associations that will provide a mapping between a Kerberos principal and an i5/OS user profile. You can then use this association to determine which EIM identifier corresponds to a local i5/OS user profile or Kerberos principal. This is one of the benefits of enabling single sign-on in i5/OS on the server.

i5/OS enablement of single sign-on

To enable a single sign-on environment, IBM exploits two technologies that work together: EIM and network authentication service, which is IBM’s implementation of Kerberos and the GSS APIs. By configuring these two technologies, an administrator can enable a single sign-on environment. Windows 2000, XP, Vista, AIX®, and z/OS® use Kerberos protocol to authenticate users to the network. Kerberos involves the use of a network-based, secure, key distribution center which authenticates principals (Kerberos users) to the network. The fact that a user has authenticated to the KDC is represented by a Kerberos ticket. A ticket can be passed from a user to a service that accepts tickets. The service accepting a ticket uses it to determine who the user claims to be (within the Kerberos user registry and realm) and that they are in fact who they claim to be.

While network authentication service allows a server to participate in a Kerberos realm, EIM provides a mechanism for associating these Kerberos principals to a single EIM identifier that represents that user within the entire enterprise. Other user identities, such as an i5/OS user name, can also be associated with this EIM identifier. Based on these associations, EIM provides a mechanism for i5/OS and applications to determine which i5/OS user profile represents the person or entity represented by the Kerberos principal. You can think of the information in EIM as a tree with an EIM identifier as the root, and the list of user identities associated with the EIM identifier as the branches.

Enabling single sign-on for your server simplifies the task of managing i5/OS user profiles and reduces the number of sign-ons that a user must perform to access multiple i5/OS applications and servers. Additionally, it reduces the amount of time that is required for password management by each user. Single sign-on allows each user to remember and use fewer passwords to access applications and servers, thereby simplifying their System i experience.

i5/OS client and server applications currently enabled for single sign-on

- i5/OS Host Servers is currently used by System i Access for Windows and System i Navigator.
- Telnet server: currently used by PC5250 and IBM WebSphere® Host On-Demand Version 8: Web Express Logon feature.
- Open DataBase Connectivity (ODBC): allows single sign-on access to i5/OS databases through ODBC.

- Java™ Database Connectivity (JDBC): allows single sign-on access to i5/OS databases through ODBC.
- Distributed Relational Database Architecture™ (DRDA®): allows single sign-on access to i5/OS databases through ODBC.
- QFileSrv.400

ISV enablement

An independent software vendor (ISV) can create applications and programs that can participate in a single sign-on environment.

As an ISV you know that many of your customers are implementing single sign-on environments to take advantage of the cost and time benefits that single sign-on provides. You want to ensure that you design your application products to participate in single sign-on environments so that you can continue to provide the solutions that your customers want and need.

To enable your applications to participate in an i5/OS single sign-on environment, you need to perform the following tasks:

Enable your i5/OS server applications for EIM

One of the foundations of a single sign-on environment is Enterprise Identity Mapping (EIM). EIM is a mechanism for mapping or associating a person or entity to the appropriate user identities in various registries throughout the enterprise. Application developers for i5/OS use EIM to build applications that use one user registry for authentication and another for authorization--without requiring the user to provide another set of credentials. EIM provides APIs for creating and managing these identity mapping relationships, as well as APIs that applications use to query this information. You can write applications that use EIM APIs to perform lookup operations for user identities within an enterprise.

Enable your i5/OS server and client applications to use a common authentication mechanism

While you are free to choose any common authentication mechanism you want for your application's single sign-on environment, the i5/OS single sign-on environment is based on the network authentication service (Kerberos) which provides an integrated single sign-on environment with Windows 2000 and 2003 domains. If you want your applications to participate with the same secure, integrated single sign-on environment as i5/OS, should choose network authentication service as the authentication mechanism for your applications. The following are examples of the different authentication methods you can choose for your applications:

Network authentication service

Use the Scenario: Enable single sign-on for ISV applications to learn how to use EIM application programming interfaces (APIs) in conjunction with network authentication service to create applications that can fully participate in a single sign-on environment. This scenario includes some ISV code examples, including pseudocode, for example pseudocode and snippets that you can use to help complete your program.

Digital certificates

It is possible to develop applications for a single sign-on environment that use digital certificates as the authentication method. To insert the necessary code into your program for authenticating with digital certificates, you must use the Digital Certificate Management APIs.

Lightweight Directory Access Protocol (LDAP)

It is possible to develop applications for a single sign-on environment that use the directory server as the authentication method. To insert the necessary code into your program for authenticating with the directory server, you must use the Lightweight Directory Access Protocol (LDAP) APIs.

Related information

Enterprise Identity Mapping

Scenarios: Single sign-on

These scenarios provide real world examples for planning, configuring, and using single sign-on in an enterprise.

Although all of these scenarios provide models for network administrators, there is also a scenario for application developers that demonstrates the tasks that a developer needs to complete to create applications that can participate in a single sign-on environment.

Scenario: Creating a single sign-on test environment

In this scenario, you want to configure network authentication service and EIM to create a basic single sign-on test environment. Use this scenario to gain a basic understanding of what configuring a single sign-on environment involves on a small scale before implementing single sign-on across an entire enterprise.

Situation

You, John Day, are a network administrator for a large wholesale company. Currently you spend much of your time troubleshooting password and user identity problems, such as forgotten passwords. Your network is comprised of several System i models and a Windows 2000 server, where your users are registered in Microsoft Windows Active Directory. Based on your research, you know that Microsoft Active Directory uses the Kerberos protocol to authenticate Windows users. You also know that the System i platform provides a single sign-on solution based on an implementation of Kerberos authentication, called network authentication service, in conjunction with EIM.

You are excited about the benefits of using single sign-on. However, you want to thoroughly understand single sign-on configuration and usage before you begin using it across your entire enterprise. Consequently, you decide to configure a test environment first.

After considering the various groups in your company, you decide to create the test environment for the Order Receiving department. The employees in the Order Receiving department use multiple applications on one System i model to handle incoming customer orders. Consequently, the Order Receiving department provides an excellent opportunity for you to create a single sign-on test environment that you can use to better understand how single sign-on works and how to plan a single sign-on implementation across your enterprise.

Scenario advantages

- Allows you to see some of the benefits of single sign-on on a small scale to better understand how you can take full advantage of it before you create a large-scale, single sign-on environment.
- Provides you with a better understanding of the planning process you need to use to successfully and to more quickly implement single sign-on across your entire enterprise.
- Minimizes the learning curve of implementing single sign-on across your enterprise.

Objectives

As the network administrator at MyCo, Inc., you want to create a small single sign-on environment for testing that includes a small number of users and a single System i model. You want to perform thorough testing to ensure that user identities are correctly mapped within your test environment. Based on this configuration, you eventually want to expand the test environment to include the other systems and users in your enterprise.

The objectives of this scenario are as follows:

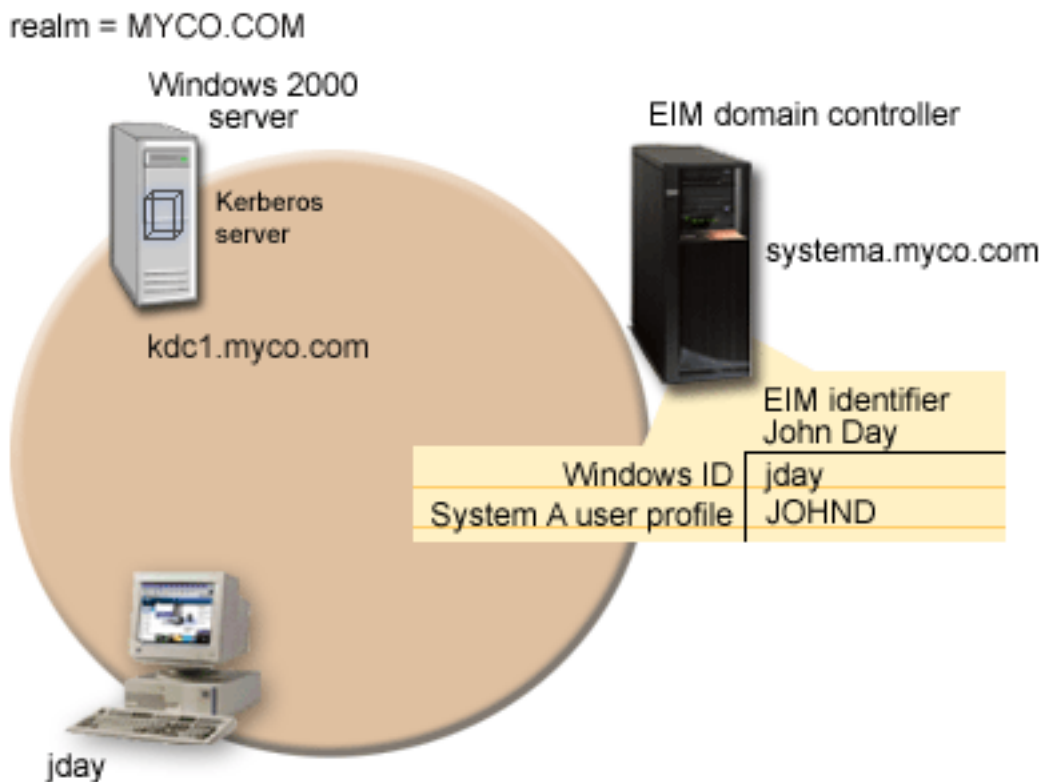
- The System i model, known as System A, must be able to use Kerberos within the MYCO.COM realm to authenticate the users and services that are participating in this single sign-on test environment. To enable the system to use Kerberos, System A must be configured for network authentication service.
- The directory server on System A must function as the domain controller for the new EIM domain.

Note: Refer to “Domains” on page 5 to learn how an EIM domain and a Windows 2000 domain both fit into the single sign-on environment.

- One user profile on System A and one Kerberos principal must each be mapped to a single EIM identifier.
- A Kerberos service principal must be used to authenticate the user to the System i Access for Windows applications.

Details

The following figure illustrates the network environment for this scenario.



The figure illustrates the following points relevant to this scenario.

EIM domain data defined for the enterprise

- An EIM registry definition for System A called SYSTEMA.MYCO.COM.
- An EIM registry definition for the Kerberos registry called MYCO.COM.
- An EIM identifier called John Day. This identifier uniquely identifies John Day, the administrator for MyCo.
- A source association for the jday Kerberos principal on the Windows 2000 server.
- A target association for the JOHND user profile on System A.

Windows 2000 server

- Acts as the Kerberos server (kdc1.myco.com), also known as a key distribution center (KDC), for the network.
- The default realm for the Kerberos server is MYCO.COM.
- A Kerberos principal of jday is registered with the Kerberos server on the Windows 2000 server. This principal will be used to create a source association to the EIM identifier, John Day.

System A

- | • Runs i5/OS Version 5 Release 4 (V5R4), or later, with the following options and licensed programs installed:
 - | – i5/OS Host Servers (5761-SS1 Option 12)
 - | – Qshell Interpreter (5761-SS1 Option 30)
 - | – System i Access for Windows (5761-XE1)
- | **Note:** You can implement this scenario using a server that runs i5/OS V5R3, or later. However, some of the configuration steps will be slightly different due to i5/OS V5R4 enhancements. 5722 is the product code for i5/OS options and products, prior to V6R1.
- The IBM Directory Server for System i (LDAP) on System A will be configured to be the EIM domain controller for the new EIM domain, MyCoEimDomain.
- System A participates in the EIM domain, MyCoEimDomain.
- The principal name for System A is krbsvr400/systema.myco.com@MYCO.COM.
- The user profile of JOHND exists on System A. You will create a target association between this user profile and the EIM identifier, John Day.
- The home directory for the i5/OS user profile, JOHND, (/home/JOHND) is defined on System A.

Client PC used for single sign-on administration

- Runs Microsoft Windows 2000 operating system.
- Runs System i Access for Windows (5761-XE1).
- Runs System i Navigator with the following subcomponents installed:
 - Network
 - Security
- Serves as the primary logon system for administrator John Day.
- Configured to be part of the MYCO.COM realm (Windows domain).

Prerequisites and assumptions

Successful implementation of this scenario requires that the following assumptions and prerequisites are met:

1. All system requirements, including software and operating system installation, have been verified. To verify that the licensed programs have been installed, complete the following:
 - a. In System i Navigator, expand **your system** → **Configuration and Service** → **Software** → **Installed Products**.
 - b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup is complete.
3. TCP/IP and basic system security are configured and tested on each system.
4. The directory server and EIM should not be previously configured on System A.

Note: Instructions in this scenario are based on the assumption that the directory server has not been previously configured on System A. However, if you already configured the directory server,

you can still use these instructions with only slight differences. These differences are noted in the appropriate places within the configuration steps.

5. A single DNS server is used for host name resolution for the network. Host tables are not used for host name resolution.

Note: The use of host tables with Kerberos authentication might result in name resolution errors or other problems.

Configuration steps

Note: You need to thoroughly understand the concepts related to single sign-on which include network authentication service and Enterprise Identity Mapping (EIM) concepts, before you implement this scenario. If you are ready to continue with this scenario complete the following steps:

Related tasks

“Testing your application” on page 67

You have completed the development of both client and server specific updates to your **Calendar** application, enabling it for an i5/OS single sign-on environment. You are now ready to test it.

“Configuring single sign-on” on page 80

To configure a single sign-on environment you must use a compatible authentication method as your authentication method and Enterprise Identity Mapping (EIM) to create and manage your user profiles and identity mappings.

Related information

Host name resolution considerations

Enterprise Identity Mapping (EIM)

Completing the planning work sheets

The following planning work sheets are tailored to fit this scenario based on the general single sign-on planning worksheets.

About this task


These planning work sheets demonstrate the information that you need to gather and the decisions you need to make to prepare the single sign-on implementation described by this scenario. To ensure a successful implementation, you must be able to answer Yes to all prerequisite items in the work sheet and you should gather all the information necessary to complete the work sheets before you perform any configuration tasks.

Note: You need to thoroughly understand the concepts related to single sign-on which include network authentication service and Enterprise Identity Mapping (EIM) concepts, before you implement this scenario.

Table 1. Single sign-on prerequisite work sheet

Prerequisite work sheet	Answers
Is your system running i5/OS V5R4 or later?	Yes
Are the following options and licensed programs installed on System A? <ul style="list-style-type: none"> • i5/OS Host Servers (5761-SS1 Option 12) • Qshell Interpreter (5761-SS1 Option 30) • System i Access for Windows (5761-XE1) Note: 5722 is the product code for i5/OS options and products, prior to V6R1.	Yes

Table 1. Single sign-on prerequisite work sheet (continued)

Prerequisite work sheet	Answers
Have you installed an application that is enabled for single sign-on on each of the PCs that will participate in the single sign-on environment? Note: For this scenario, all of the participating PCs have System i Access for Windows (5761-XE1) installed.	Yes
Is System i Navigator installed on the administrator's PC? • Is the Security subcomponent of System i Navigator installed on the administrator's PC? • Is the Network subcomponent of System i Navigator installed on the administrator's PC?	Yes
Have you installed the latest System i Access for Windows service pack? For the latest service pack see, System i Access  .	Yes
Do you, the administrator, have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes
Do you have one of the following systems acting as the Kerberos server (also known as the KDC)? If yes, specify which system. 1. Windows ^(R) 2000 Server Note: Microsoft Windows 2000 Server uses Kerberos authentication as its default security mechanism. 2. Windows ^(R) Server 2003 3. i5/OS PASE V5R3, or later 4. AIX server 5. z/OS	Yes, Windows 2000 Server
Are all your PCs in your network configured in a Windows 2000 domain?	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is the System i model time within 5 minutes of the system time on the Kerberos server? If not see Synchronizing system times.	Yes
Are you running i5/OS PASE for the Kerberos server?	You must have IBM Network Authentication Enablement for i5/OS(5761-NAE) installed.

You need this information to configure EIM and network authentication service to create a single sign-on test environment.

Table 2. Single sign-on configuration planning work sheet for System A

Configuration planning work sheet for System A	Answers
Use the following information to complete the EIM Configuration wizard. The information in this work sheet correlates with the information you need to supply for each page in the wizard:	
How do you want to configure EIM for your system? • Join an existing domain • Create and join a new domain	Create and join a new domain
Where do you want to configure your EIM domain?	On the local directory server Note: This will configure the directory server on the same system on which you are currently configuring EIM.

Table 2. Single sign-on configuration planning work sheet for System A (continued)

Configuration planning work sheet for System A	Answers
Do you want to configure network authentication service? Note: You must configure network authentication service to configure single sign-on.	Yes
The Network Authentication Service wizard opens from the EIM Configuration wizard. Use the following information to complete the Network Authentication Service wizard: Note: You can launch the Network Authentication Service wizard independently of the EIM Configuration wizard.	
What is the name of the Kerberos default realm to which your System i model will belong? Note: A Windows 2000 domain is similar to a Kerberos realm. Microsoft Windows Active Directory uses Kerberos authentication as its default security mechanism.	MYCO.COM
Are you using Microsoft Active Directory?	Yes
What is the Kerberos server, also known as a key distribution center (KDC), for this Kerberos default realm? What is the port on which the Kerberos server listens?	KDC: kdc1.myco.com Port: 88 Note: This is the default port for the Kerberos server.
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this Kerberos server? What is the port on which the password server listens?	Yes Password server: kdc1.myco.com Port: 464 Note: This is the default port for the password server.
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • IBM HTTP Server for i5/OS • i5/OS NetServer™ • Network File System (NFS) Server	i5/OS Kerberos Authentication
What is the password for your service principal or principals?	systema123 Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
Do you want to create a batch file to automate adding the service principals for System A to the Kerberos registry?	Yes
Do you want to include passwords with the i5/OS service principals in the batch file?	Yes
As you exit the Network Authentication Service wizard, you will return to the EIM Configuration wizard. Use the following information to complete the EIM Configuration wizard:	
Specify user information that the wizard should use when configuring the directory server. This is the connection user. You must specify the port number, administrator distinguished name, and a password for the administrator. Note: Specify the LDAP administrator's distinguished name (DN) and password to ensure the wizard has enough authority to administer the EIM domain and the objects in it.	Port: 389 Distinguished name: cn=administrator Password: mycopwd Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
What is the name of the EIM domain that you want to create?	MyCoEimDomain
Do you want to specify a parent DN for the EIM domain?	No

Table 2. Single sign-on configuration planning work sheet for System A (continued)

Configuration planning work sheet for System A	Answers
Which user registries do you want to add to the EIM domain?	Local i5/OS--SYSTEMA.MYCO.COM Kerberos--MYCO.COM Note: The Kerberos principals stored on the Windows 2000 server are not case sensitive; therefore you should not select Kerberos user identities are case sensitive.
Which EIM user do you want System A to use when performing EIM operations? This is the system user. Note: If you have not configured the directory server before configuring single sign-on, the only distinguished name (DN) you can provide for the system user is the LDAP administrator's DN and password.	User type: Distinguished name and password User: cn=administrator Password: mycopwd Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
After you complete the EIM Configuration wizard, use the following information to complete the remaining steps required for configuring single sign-on:	
What is the i5/OS user profile name for the user?	JOHND
What is the name of the EIM identifier that you want to create?	John Day
What kinds of associations do you want to create?	Source association: Kerberos principal jday Target association: i5/OS user profile JOHND
What is the name of the user registry that contains the Kerberos principal for which you are creating the source association?	MYCO.COM
What is the name of the user registry that contains the i5/OS user profile for which you are creating the target association?	SYSTEMA.MYCO.COM
What information do you need to supply to test EIM identity mapping?	Source registry: MYCO.COM Source user: jday Target registry: SYSTEMA.MYCO.COM

Related information

Enterprise Identity Mapping (EIM)

Creating a basic single sign-on configuration for System A

The EIM Configuration wizard helps you create a basic EIM configuration and also opens the Network Authentication Service wizard to allow you to create a basic network authentication service configuration.

About this task

Note: Instructions in this scenario are based on the assumption that the IBM Tivoli Directory Server for i5/OS has not been previously configured on System A. However, if you already configured the directory server, you can still use these instructions with only slight differences. These differences are noted in the appropriate places within the configuration steps.

When you have finished this step, you will have completed the following tasks:

- Created a new EIM domain
- Configured the directory server on System A to be the EIM domain controller
- Configured network authentication service
- Created EIM registry definitions for the System A i5/OS registry and the Kerberos registry in the newly created EIM domain
- Configured System A to participate in the EIM domain

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping**.

2. Right-click **Configuration** and select **Configure** to start the EIM Configuration wizard.
3. On the **Welcome** page, select **Create and join a new domain**. Click **Next**.
4. On the **Specify EIM Domain Location** page, select **On the local Directory server**. Click **Next** and the Network Authentication Service wizard is displayed.

Note: The Network Authentication Service wizard only displays when the system determines that you need to enter additional information to configure network authentication service for the single sign-on implementation.

5. Complete these tasks to configure network authentication service:

- a. On the **Configure Network Authentication Service** page, select **Yes**.

Note: This launches the Network Authentication Service wizard. With this wizard, you can configure several i5/OS interfaces and services to participate in a Kerberos realm.

- b. On the **Specify Realm Information** page, enter MYCO.COM in the **Default realm** field and select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
- c. On the **Specify KDC Information** page, enter kdc1.myco.com in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
- d. On the **Specify Password Server Information** page, select **Yes**. Enter kdc1.myco.com in the **Password server** field and 464 in the **Port** field. Click **Next**.
- e. On the **Select Keytab Entries** page, select **i5/OS Kerberos Authentication**. Click **Next**.
- f. On the **Create i5/OS Keytab Entry** page, enter and confirm a password, and click **Next**. For example, systema123. This password will be used when System A is added to the Kerberos server.

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

- g. Optional: On the **Create Batch File** page, select **Yes**, specify the following information, and click **Next**:

- **Batch file:** Add the text systema to the end of the default batch file name. For example, C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat.
- Select **Include password**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is recommended that you delete the batch file from the Kerberos server and from your PC immediately after use.

Note: If you do not include the password, you will be prompted for the password when the batch file is run.

- h. On the **Summary** page, review the network authentication service configuration details and click **Finish** to complete the Network Authentication Service wizard and return to the EIM Configuration wizard.

6. On the **Configure Directory Server** page, enter the following information, and click **Next**:

Note: If you configured the directory server before you started this scenario, you will see the **Specify User for Connection** page instead of the **Configure Directory Server** page. In that case, you must specify the distinguished name and password for the LDAP administrator.

- **Port:** 389
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

7. On the **Specify Domain** page, enter the name of the domain in the **Domain** field, and click **Next**. For example, MyCoEimDomain.
8. On the **Specify Parent DN for Domain** page, select **No**, and click **Next**.

Note: If the directory server is active, a message is displayed that indicates you need to end and restart the directory server for the changes to take effect. Click **Yes** to restart the directory server.

9. On the **Registry Information** page, select **Local i5/OS** and **Kerberos**, and click **Next**. Write down the registry names. You will need these registry names when you create associations to EIM identifiers.

Note:

- Registry names must be unique to the domain.
- You can enter a specific registry definition name for the user registry if you want to use a specific registry definition naming plan. However, for this scenario you can accept the default values.

10. On the **Specify EIM System User** page, select the user the operating system uses when performing EIM operations on behalf of operating system functions, and click **Next**.

Note: Because you did not configure the directory server prior to performing the steps in this scenario, the only distinguished name (DN) that you can choose is the LDAP administrator's DN.

- **User type:** Distinguished name and password
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

11. On the **Summary** page, confirm the EIM configuration information. Click **Finish**.

Results

Now that you have completed a basic EIM and network authentication service configuration on System A, you can add the service principal for System A to the Kerberos server.

Adding System A service principal to the Kerberos server

You can use one of two methods to add the necessary i5/OS service principal to the Kerberos server.

About this task

You can manually add the service principal or, as this scenario illustrates, you can use a batch file to add it. You created this batch file in Step 2. To use this file, you can use File Transfer Protocol (FTP) to copy the file to the Kerberos server and run it.

Follow these steps to use the batch file to add principals to the Kerberos server:

FTP batch file created by the wizard

1. On the Windows 2000 workstation that you used to configure network authentication service, open a command prompt and type `ftp kdc1.myco.com` to start an FTP session on your PC. You will be prompted for the administrator's user name and password.

2. At the FTP prompt, enter `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Press Enter. You should receive the message Local directory now C:\Documents and Settings\All Users\Documents\IBM\Client Access.
3. At the FTP prompt, type `cd \mydirectory`, where *mydirectory* is a directory located on kdc1.myco.com.
4. At the FTP prompt, type `put NASConfigsystema.bat`. You should receive this message: 226 Transfer complete.
5. Type `quit` to exit the FTP session.

What to do next

Run the batch file on kdc1.myco.com

1. On your Windows 2000 server, open the directory where you transferred the batch file.
2. Find the `NASConfigsystema.bat` file and double-click the file to run it.
3. After the file runs, verify that the i5/OS principal has been added to the Kerberos server by completing the following:
 - a. On your Windows 2000 server, expand **Administrative Tools** → **Active Directory Users and Computers** → **Users**.
 - b. Verify the System i model has a user account by selecting the appropriate Windows 2000 domain.

Note: This Windows 2000 domain should be the same as the default realm name that you specified in the network authentication service configuration.

- c. In the list of users that is displayed, find `systema_1_krbsvr400`. This is the user account generated for the i5/OS principal name.
- d. (Optional) Access the properties on your Active Directory user. From the **Account** tab, select the **Account is trusted for delegation**.

Note: This optional step enables your system to delegate, or forward, a user's credentials to other systems. As a result, the i5/OS service principal can access services on multiple systems on behalf of the user. This is useful in a multi-tier network.

Now that you have added the System A service principal to the Kerberos server, you can create a home directory for John Day.

Creating home directory for John Day on System A

You need to create a directory in the `/home` directory to store your Kerberos credentials cache.

About this task

To create a home directory, complete the following:

On a command line, enter: `CRTDIR '/home/user profile'` where `user profile` is your i5/OS user profile name. For example: `CRTDIR '/home/JOHND'`.

Now that you have created the home directory, you can verify that network authentication service is configured correctly.

Testing network authentication service configuration on System A

Now that you have completed the network authentication service configuration tasks for System A, you need to test that your configuration works correctly. You can do this by requesting a ticket granting ticket for the System A principal name

About this task

To test the network authentication service configuration, follow these steps:

Note: Ensure that you have created a home directory for your i5/OS user profile before performing this procedure.

1. On a command line, enter QSH to start the Qshell Interpreter.
2. Enter `keytab list` to display a list of principals registered in the keytab file. In this scenario, `krbsvr400/systema.myco.com@MYCO.COM` should display as the principal name for System A.
3. Enter `kinit -k krbsvr400/systema.myco.com@MYCO.COM`. If this is successful, then the `kinit` command is displayed without errors.
4. Enter `klist` to verify that the default principal is `krbsvr400/systema.myco.com@MYCO.COM`.

Results

Now that you have tested the network authentication service configuration, you can create an EIM identifier for John Day.

Creating an EIM identifier for John Day

Now that you have performed the initial steps to create a basic single sign-on configuration, you can begin to add information to this configuration to complete your single sign-on test environment.

About this task

You need to create the EIM identifier that you specified in the planning work sheet. In this scenario, this EIM identifier is a name that uniquely identifies you, John Day, in your enterprise.

To create an EIM identifier, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

- **User type:** Distinguished name
- **Distinguished name:** `cn=administrator`
- **Password:** `mycopwd`

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **Identifiers** and select **New Identifier**.
3. On the **New EIM Identifier** dialog box, enter a name for the new identifier in the **Identifier** field, and click **OK**. For example, John Day.

Results

Now that you have created your identifier, you can add associations to the identifier to define the relationship between the identifier and the corresponding Kerberos principal and i5/OS user profile.

Testing EIM identity mappings

You need to verify that EIM mapping lookup operations return the correct results based on the configured associations.

About this task

To test that EIM mapping operations work correctly, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

- **User type:** Distinguished name
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **MyCoEimDomain** and select **Test a mapping**.
3. In the **Test a mapping** dialog box, specify or **Browse** to select the following information:
 - **Source registry:** MYCO.COM
 - **Source user:** jday
 - **Target registry:** SYSTEMA.MYCO.COM

Note: Click **Help**, if necessary, for more details about what information is needed for each field in the dialog box.

Click **Test**, and click **Close**.

What to do next

If your EIM mappings are correctly configured, the following results are displayed in the **Mapping found** portion of the page:

For these fields	See these results
Target user	JOHND
Origin	EIM Identifier: John Day

If you receive messages or errors that indicate problems with your mappings or with communications, see EIM troubleshooting to help you find solutions to these problems.

Now that you have tested the EIM identify mappings, you can configure System i Access for Windows applications to use Kerberos authentication.

Configuring System i Access for Windows applications to use Kerberos authentication

You must use Kerberos to authenticate before you can use System i Navigator to access your system. Therefore, from your PC, you need to configure System i Access for Windows to use Kerberos authentication.

About this task

To configure System i Access for Windows applications to use Kerberos authentication, complete the following steps:

Note: Each of your users needs to perform all of these steps on their own PC.

1. Log on to the Windows 2000 domain by signing in to your PC.

2. In System i Navigator on your PC, right-click **System A** and select **Properties**.
3. On the **Connection** page, select **Use Kerberos principal name, no prompting**. This will allow System i Access for Windows connections to use the Kerberos principal name and password for authentication.
4. A message is displayed that indicates you need to close and restart all applications that are currently running for the changes to the connection settings to take effect. Click **OK**. Then, end and restart System i Navigator.

Results

Now that you have configured System i Access for Windows applications to use Kerberos authentication, you can verify the single sign-on environment.

Verifying network authentication service and EIM configuration

Now that you have verified the individual pieces of your single sign-on configuration and ensured that all setup is complete, you must verify that you have configured EIM and network authentication service correctly and that single sign-on works as expected.

About this task

To verify that your single sign-on environment works correctly, have John Day follow these steps:

1. In System i Navigator, expand **System A** to open a connection to System A.
2. Press F5 to refresh the screen.
3. In the right pane, find System A in the **Name** column, and verify that John Day's i5/OS user profile, JOHND, is displayed as the corresponding entry in the **Signed On User** column.

Results

System i Navigator successfully used EIM to map the jday Kerberos principal to the JOHND System A user profile because of the associations defined for EIM identifier, John Day. The System i Navigator session for System A is now connected as JOHND.

(Optional) Postconfiguration considerations

Now that you finished this scenario, the only EIM user you have defined that EIM can use is the DN for the LDAP administrator.

About this task

The LDAP administrator DN that you specified for the system user on System A has a high level of authority to all data on the directory server. Therefore, you might consider creating one or more DNs as additional users that have more appropriate and limited access control for EIM data. The number of additional EIM users that you define depends on your security policy's emphasis on the separation of security duties and responsibilities. Typically, you might create at least the two following types of DNs:

- **A user that has EIM administrator access control**

This EIM administrator DN provides the appropriate level of authority for an administrator who is responsible for managing the EIM domain. This EIM administrator DN can be used to connect to the domain controller when managing all aspects of the EIM domain by means of System i Navigator.

- **At least one user that has all of the following access controls:**

- Identifier administrator
- Registry administrator
- EIM mapping operations

This user provides the appropriate level of access control required for the system user that performs EIM operations on behalf of the operating system.

Note: To use this new DN for the system user instead of the LDAP administrator DN, you must change the EIM configuration properties for each system. For this scenario, you need to change the EIM configuration properties for any System i model that you set up.

Related information

Managing EIM configuration properties

Scenario: Enabling single sign-on for i5/OS

View this scenario to learn how to configure network authentication service and EIM to create a single sign-on environment across multiple systems in an enterprise. This scenario expands on the concepts and tasks presented in the previous scenario which demonstrates how to create a simple single sign-on test environment.

Situation

You are a network administrator that manages a network and network security for your company, including the Order Receiving department. You oversee the IT operations for a large number of employees who take customer orders over the telephone. You also supervise two other network administrators who help you maintain the network.

The employees in the Order Receiving department use Windows 2000 and i5/OS and require multiple passwords for the different applications they use every day. Consequently, you spend a lot of time managing and troubleshooting problems related to passwords and user identities, such as resetting forgotten passwords.

As the company's network administrator, you are always looking for ways to improve the business, starting with the Order Receiving department. You know that most of your employees need the same type of authority to access the application that they use to query inventory status. It seems redundant and time consuming for you to maintain individual user profiles and numerous passwords that are required in this situation. In addition, you know that all of your employees can benefit by using fewer user IDs and passwords. You want to do these things:

- Simplify the task of password management for the Order Receiving department. Specifically, you want to efficiently manage user access to the application your employees routinely use for customer orders.
- Decrease the use of multiple user IDs and passwords for the department employees, as well as for the network administrators. However, you do not want to make the Windows 2000 IDs and i5/OS user profiles the same nor do you want to use password caching or syncing.

Based on your research, you know that i5/OS supports single sign-on, a solution that allows your users to log on once to access multiple applications and services that normally require them to log on with multiple user IDs and passwords. Because your users do not need to provide as many user IDs and passwords to do their jobs, you have fewer password problems to solve for them. Single sign-on seems to be an ideal solution because it allows you to simplify password management in the following ways:

- For typical users that require the same authority to an application, you can create policy associations. For example, you want the order clerks in the Order Receiving department to be able to log on once with their Windows user name and password and then be able to access a new inventory query application in the manufacturing department without having to be authenticated again. However, you also want to ensure that the level of authorization that they have when using this application is appropriate. To attain this goal, you decide to create a policy association that maps the Windows 2000 user identities for this group of users to a single i5/OS user profile that has the appropriate level of authority for running the inventory query application. Because this is a query-only application in which users cannot change data, you are not as concerned about detailed auditing for this application. Consequently, you feel confident that using a policy association in this situation conforms to your security policy.

You create a policy association to map the group of order clerks with similar authority requirements to a single i5/OS user profile with the appropriate level of authority for the inventory query application.

Your users benefit by having one less password to remember and one less logon to perform. As the administrator, you benefit by having to maintain only one user profile for user access to the application instead of multiple user profiles for everyone in the group.

- For each of your network administrators who have user profiles with special authorities, such as *ALLOBJ and *SECADM, you can create identifier associations. For example, you want all of the user identities for a single network administrator to be precisely and individually mapped to one another because of the administrator's high level of authority.

Based on your company's security policy, you decide to create identifier associations to map specifically from each network administrator's Windows identity to his i5/OS user profile. You can more easily monitor and trace the activity of the administrator because of the one-to-one mapping that identifier associations provide. For example, you can monitor the jobs and objects that run on the system for a specific user identity. Your network administrator benefits by having one less password to remember and one less logon to perform. As the network administrator, you benefit by tightly controlling the relationships between all of your administrator's user identities.

This scenario has the following advantages:

- Simplifies authentication process for users.
- Simplifies managing access to applications.
- Eases the overhead of managing access to servers in the network.
- Minimizes the threat of password theft.
- Avoids the need for multiple signons.
- Simplifies user identity management across the network.

Objectives

In this scenario, you are the administrator at MyCo, Inc. who wants to enable single sign-on for the users in the Order Receiving department.

The objectives of this scenario are as follows:

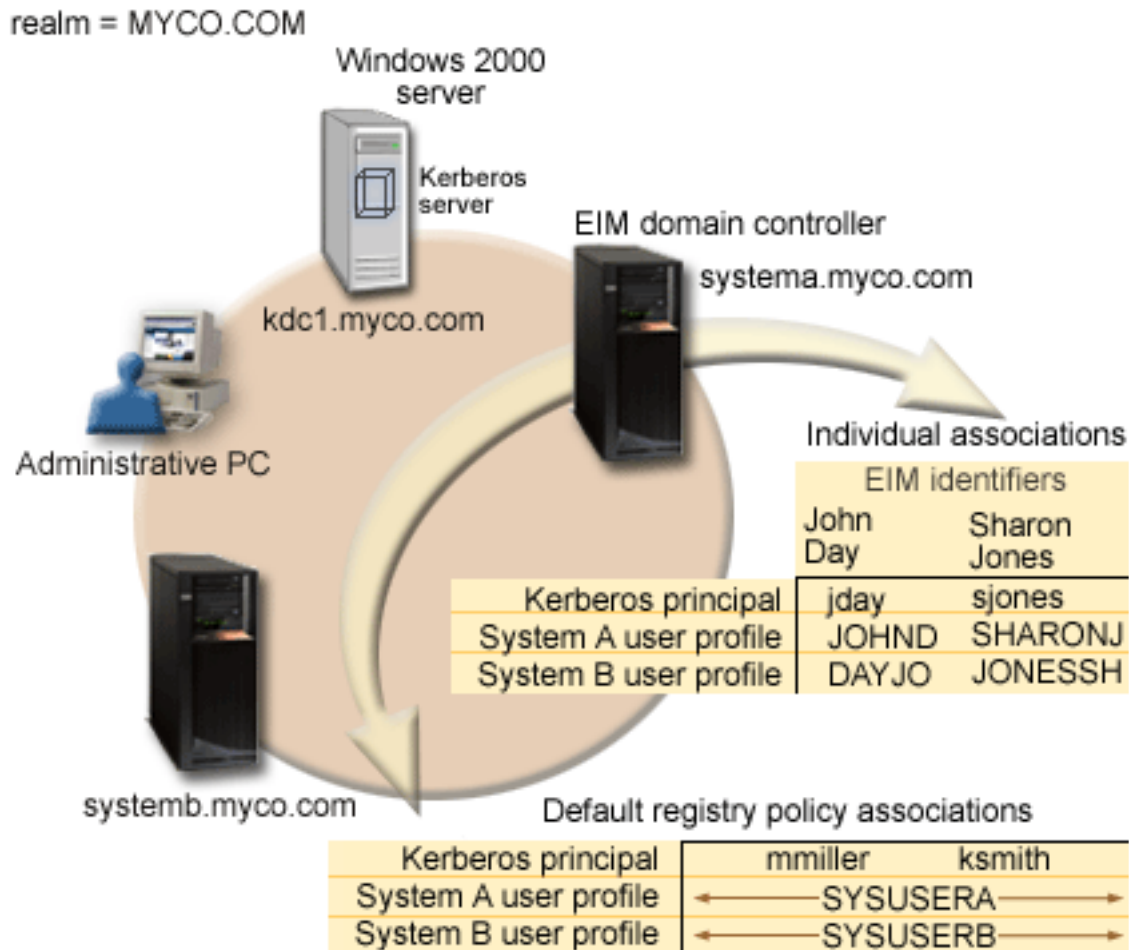
- System A and System B must participate in the MYCO.COM realm to authenticate the users and services that are participating in this single sign-on environment. To enable the systems to use Kerberos, System A and System B must be configured for network authentication service.
- The IBM Directory Server for System i (LDAP) on System A must function as the domain controller for the new EIM domain.

Note: Refer to domains to learn how two different types of domains, an EIM domain and a Windows 2000 domain, fit into the single sign-on environment.

- All user identities in the Kerberos registry must map successfully to a single i5/OS user profile with appropriate authority for user access to the inventory query application.
- Based on your security policy, two administrators, John Day and Sharon Jones, who also have user identities in the Kerberos registry, must have identifier associations to map these identities to their i5/OS user profiles which have *SECADM special authority. These one-to-one mappings enable you to closely monitor the jobs and objects that run on the system for these user identities.
- A Kerberos service principal must be used to authenticate the users to the System i Access for Windows applications, including System i Navigator.

Details

The following figure illustrates the network environment for this scenario.



The figure illustrates the following points relevant to this scenario.

EIM domain data defined for the enterprise

- Three registry definition names:
 - A registry definition name of MYCO.COM for the Windows 2000 server registry. You will define this when you use the EIM configuration wizard on System A.
 - A registry definition name of SYSTEMA.MYCO.COM for the i5/OS registry on System A. You will define this when you use the EIM configuration wizard on System A.
 - A registry definition name of SYSTEMB.MYCO.COM for the i5/OS registry on System B. You will define this when you use the EIM configuration wizard on System B.
- Two default registry policy associations:

Note: EIM lookup operation processing assigns the highest priority to identifier associations. Therefore, when a user identity is defined as a source in both a policy association and an identifier association, only the identifier association maps that user identity. In this scenario, two network administrators, John Day and Sharon Jones, both have user identities in the MYCO.COM registry, which is the source of the default registry policy associations. However, as shown below, these administrators also have identifier associations defined for their user identities in

the MYCO.COM registry. The identifier associations ensure that their MYCO.COM user identities are not mapped by the policy associations. Instead, the identifier associations ensure that their user identities in the MYCO.COM registry are individually mapped to other specific individual user identities.

- One default registry policy association maps all user identities in the Windows 2000 server registry called MYCO.COM, to a single i5/OS user profile called SYSUSERA in the SYSTEMA.MYCO.COM registry on System A. For this scenario, mmiller and ksmith represent two of these user identities.
- One default registry policy association maps all user identities in the Windows 2000 server registry called MYCO.COM, to a single i5/OS user profile called SYSUSERB in the SYSTEMB.MYCO.COM registry on System B. For this scenario, mmiller and ksmith represent two of these user identities.
- Two EIM identifiers named John Day and Sharon Jones to represent the two network administrators in the company who have those names.
- For the John Day EIM identifier, these identifier associations are defined:
 - A source association for the jday user identity, which is a Kerberos principal in the Windows 2000 server registry.
 - A target association for the JOHND user identity, which is a user profile in the i5/OS registry on System A.
 - A target association for the DAYJO user identity, which is a user profile in the i5/OS registry on System B.
- For the Sharon Jones EIM identifier, these identifier associations are defined:
 - A source association for the sjones user identity, which is a Kerberos principal in the Windows 2000 server registry.
 - A target association for the SHARONJ user identity, which is a user profile in the i5/OS registry on System A.
 - A target association for the JONSSH user identity, which is a user profile in the i5/OS registry on System B.

Windows 2000 server

- Acts as the Kerberos server (kdc1.myco.com), also known as a key distribution center (KDC), for the network.
- The default realm for the Kerberos server is MYCO.COM.
- All Microsoft Windows Active Directory users that do not have identifier associations are mapped to a single i5/OS user profile on each of the System i models.

System A

- | • Runs i5/OS Version 5 Release 4 (V5R4), or later, with the following options and licensed programs
- | installed:
- | – i5/OS Host Servers (5761-SS1 Option 12)
- | – Qshell Interpreter (5761-SS1 Option 30)
- | – System i Access for Windows (5761-XE1)
- | **Note:** You can implement this scenario using a server that runs i5/OS V5R3. However, some of the
- | configuration steps will be slightly different due to i5/OS V5R4, or later, enhancements. 5722 is
- | the product code for i5/OS options and products, prior to V6R1.
- The directory server on System A will be configured to be the EIM domain controller for the new EIM domain, MyCoEimDomain.
- Participates in the EIM domain, MyCoEimDomain.
- Has the service principal name of krbsvr400/systema.myco.com@MYCO.COM.
- Has the fully qualified host name of systema.myco.com. This name is registered in a single Domain Name System (DNS) to which all PCs and servers in the network point.

- Home directories on System A store the Kerberos credentials caches for i5/OS user profiles.

System B

- | • Runs i5/OS Version 5 Release 4 (V5R4) or later with the following options and licensed programs installed:
 - | – i5/OS Host Servers (5761-SS1 Option 12)
 - | – Qshell Interpreter (5761-SS1 Option 30)
 - | – System i Access for Windows (5761-XE1)
- Has the fully qualified host name of `systemb.myco.com`. This name is registered in a single Domain Name System (DNS) to which all PCs and servers in the network point.
- The principal name for System B is `krbsvr400/systemb.myco.com@MYCO.COM`.
- Participates in the EIM domain, `MyCoEimDomain`.
- Home directories on System B store the Kerberos credentials caches for i5/OS user profiles.

Administrative PC

- Runs Microsoft Windows 2000 operating system.
- | • Runs i5/OS V5R4 or later System i Access for Windows (5761-XE1).
- Runs System i Navigator with the following subcomponents installed:
 - Network
 - Security
 - Users and Groups
- Serves as the primary logon system for the administrator.
- Configured to be part of the `MYCO.COM` realm (Windows domain).

Prerequisites and assumptions

Successful completion of this scenario requires that the following assumptions and prerequisites are met:

1. All system requirements, including software and operating system installation, have been verified. To verify that these licensed programs have been installed, complete the following:
 - a. In System i Navigator, expand your **system** → **Configuration and Service** → **Software** → **Installed Products**.
 - b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup are complete.
3. TCP/IP and basic system security are configured and tested on each system.
4. The directory server and EIM should not be previously configured on System A.

Note: Instructions in this scenario are based on the assumption that the directory server has not been previously configured on System A. However, if you already configured the directory server, you can still use these instructions with only slight differences. These differences are noted in the appropriate places within the configuration steps.

5. A single DNS server is used for host name resolution for the network. Host tables are not used for host name resolution.

Note: The use of host tables with Kerberos authentication might result in name resolution errors or other problems.

Configuration steps

Note: You need to thoroughly understand the concepts related to single sign-on, which include network authentication service and Enterprise Identity Mapping (EIM) concepts, before you accomplish this scenario. If you are ready to continue with this scenario complete the following steps:

Related tasks

“Configuring single sign-on” on page 80

To configure a single sign-on environment you must use a compatible authentication method as your authentication method and Enterprise Identity Mapping (EIM) to create and manage your user profiles and identity mappings.

Related information

Host name resolution considerations

Enterprise Identity Mapping (EIM)

EIM associations

Host name resolution

Completing the planning work sheets

The following planning work sheets are tailored to fit this scenario based on the general single sign-on planning worksheets.

About this task


These planning work sheets demonstrate the information that you need to gather and the decisions you need to make as you prepare to configure the single sign-on implementation described by this scenario. To ensure a successful implementation, you must be able to answer Yes to all prerequisite items in the work sheet and you should gather all the information necessary to complete the work sheets before you perform any configuration tasks.

Note: You need to thoroughly understand the concepts related to single sign-on, which include network authentication service and Enterprise Identity Mapping (EIM) concepts, before you implement this scenario.

Table 3. Single sign-on prerequisite work sheet

Prerequisite work sheet	Answers
Is your system running i5/OS V5R4, or later?	Yes
Are the following options and licensed programs installed on System A and System B? <ul style="list-style-type: none">i5/OS Host Servers (5761-SS1 Option 12)Qshell Interpreter (5761-SS1 Option 30)System i Access for Windows (5761-XE1) Note: 5722 is the product code for i5/OS options and products, prior to V6R1.	Yes
Have you installed an application that is enabled for single sign-on on each of the PCs that will participate in the single sign-on environment? Note: For this scenario, all of the participating PCs have System i Access for Windows (5761-XE1) installed.	Yes

Table 3. Single sign-on prerequisite work sheet (continued)

Prerequisite work sheet	Answers
<p>Is System i Navigator installed on the administrator's PC?</p> <ul style="list-style-type: none"> Is the Network subcomponent of System i Navigator installed on the PC used to administer single sign-on? Is the Security subcomponent of System i Navigator installed on the PC used to administer single sign-on? Is the Users and Groups subcomponent of System i Navigator installed on the PC used to administer single sign-on? 	Yes
<p>Have you installed the latest IBM System i Access for Windows service pack? For the latest service pack see System i Access web page .</p>	Yes
<p>Does the single sign-on administrator have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?</p>	Yes
<p>Do you have one of the following systems acting as the Kerberos server (also known as the KDC)? If yes, specify which system.</p> <ol style="list-style-type: none"> Microsoft Windows 2000 Server Note: Microsoft Windows 2000 Server uses Kerberos authentication as its default security mechanism. Windows ^(R) Server 2003 i5/OS PASE (V5R3 or later) AIX server z/OS 	Yes, Windows 2000 Server
<p>Are all your PCs in your network configured in a Windows 2000 domain?</p>	Yes
<p>Have you applied the latest program temporary fixes (PTFs)?</p>	Yes
<p>Is the System i model time within 5 minutes of the system time on the Kerberos server? If not see, Synchronize system times.</p>	Yes
<p>Are you running i5/OS PASE for the Kerberos server?</p>	You must have IBM Network Authentication Enablement for i5/OS (5761-NAE) installed.

You need this information to configure EIM and network authentication service on System A

Table 4. Single sign-on configuration planning work sheet for System i A

Configuration planning work sheet for System A	Answers
<p>Use the following information to complete the EIM Configuration wizard. The information in this work sheet correlates with the information you need to supply for each page in the wizard:</p>	
<p>How do you want to configure EIM for your system?</p> <ul style="list-style-type: none"> Join an existing domain Create and join a new domain 	Create and join a new domain
<p>Where do you want to configure the EIM domain?</p>	<p>On the local directory server</p> <p>Note: This will configure the directory server on the same system on which you are currently configuring EIM.</p>
<p>Do you want to configure network authentication service?</p> <p>Note: You must configure network authentication service to configure single sign-on.</p>	Yes
<p>The Network Authentication Service wizard launches from the EIM Configuration wizard. Use the following information to complete the Network Authentication Service wizard.</p>	

Table 4. Single sign-on configuration planning work sheet for System i A (continued)

Configuration planning work sheet for System A	Answers
<p>What is the name of the Kerberos default realm to which your System i model will belong?</p> <p>Note: A Windows 2000 domain is similar to a Kerberos realm. Microsoft Windows Active Directory uses Kerberos authentication as its default security mechanism.</p>	MYCO.COM
Are you using Microsoft Active Directory?	Yes
<p>What is the Kerberos server, also known as a key distribution center (KDC), for this Kerberos default realm? What is the port on which the Kerberos server listens?</p>	<p>KDC: kdc1.myco.com</p> <p>Port: 88</p> <p>Note: This is the default port for the Kerberos server.</p>
<p>Do you want to configure a password server for this default realm? If yes, answer the following questions:</p> <p>What is name of the password server for this Kerberos server?</p> <p>What is the port on which the password server listens?</p>	<p>Yes</p> <p>Password server: kdc1.myco.com</p> <p>Port: 464</p> <p>Note: This is the default port for the password server.</p>
<p>For which services do you want to create keytab entries?</p> <ul style="list-style-type: none"> • i5/OS Kerberos Authentication • LDAP • IBM HTTP Server for i5/OS • i5/OS NetServer • Network File System (NFS) Server 	i5/OS Kerberos Authentication
<p>What is the password for your service principal or principals?</p>	<p>systema123</p> <p>Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.</p>
Do you want to create a batch file to automate adding the service principals for System A to the Kerberos registry?	Yes
Do you want to include passwords with the i5/OS service principals in the batch file?	Yes
<p>As you exit the Network Authentication Service wizard, you will return to the EIM Configuration wizard. Use the following information to complete the EIM Configuration wizard:</p>	
<p>Specify user information that the wizard should use when configuring the directory server. This is the connection user. You must specify the port number, administrator distinguished name, and a password for the administrator.</p> <p>Note: Specify the LDAP administrator's distinguished name (DN) and password to ensure the wizard has enough authority to administer the EIM domain and the objects in it.</p>	<p>Port: 389</p> <p>Distinguished name: cn=administrator</p> <p>Password: mycopwd</p> <p>Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.</p>
What is the name of the EIM domain that you want to create?	MyCoEimDomain
Do you want to specify a parent DN for the EIM domain?	No
Which user registries do you want to add to the EIM domain?	<p>Local i5/OS--SYSTEMA.MYCO.COM</p> <p>Kerberos--KDC1.MYCO.COM</p> <p>Note: You should not select Kerberos user identities are case sensitive when the wizard presents this option.</p>

Table 4. Single sign-on configuration planning work sheet for System i A (continued)

Configuration planning work sheet for System A	Answers
<p>Which EIM user do you want System A to use when performing EIM operations? This is the system user.</p> <p>Note: If you have not configured the directory server prior to configuring single sign-on, the only distinguished name (DN) you can provide for the system user is the LDAP administrator's DN and password.</p>	<p>User type: Distinguished name Distinguished name: cn=administrator Password: mycopwd Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.</p>

You need this information to allow System B to participate in the EIM domain and to configure network authentication service on System B

Table 5. Single sign-on configuration planning work sheet for System B

Configuration planning work sheet for System B	Answers
Use the following information to complete the EIM Configuration wizard for System B:	
How do you want to configure EIM on your system?	Join an existing domain
Do you want to configure network authentication service? Note: You must configure network authentication service to configure single sign-on.	Yes
The Network Authentication Service wizard launches from the EIM Configuration wizard. Use the following information to complete the Network Authentication Service wizard: Note: You can launch the Network Authentication Service wizard independently of the EIM Configuration wizard.	
What is the name of the Kerberos default realm to which your System i model will belong? Note: A Windows 2000 domain is equivalent to a Kerberos realm. Microsoft Active Directory uses Kerberos authentication as its default security mechanism.	MYCO.COM
Are you using Microsoft Active Directory?	Yes
What is the Kerberos server for this Kerberos default realm? What is the port on which the Kerberos server listens?	KDC: kdc1.myco.com Port: 88 Note: This is the default port for the Kerberos server.
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this Kerberos server? What is the port on which the password server listens?	Yes Password server: kdc1.myco.com Port: 464 Note: This is the default port for the password server.
For which services do you want to create keytab entries? <ul style="list-style-type: none"> • i5/OS Kerberos Authentication • LDAP • IBM HTTP Server for i5/OS • i5/OS NetServer 	i5/OS Kerberos Authentication
What is the password for your i5/OS service principals?	systemb123 Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

Table 5. Single sign-on configuration planning work sheet for System B (continued)

Configuration planning work sheet for System B	Answers
Do you want to create a batch file to automate adding the service principals for System B to the Kerberos registry?	Yes
Do you want to include passwords with the i5/OS service principals in the batch file?	Yes
As you exit the Network Authentication Service wizard, you will return to the EIM Configuration wizard. Use the following information to complete the EIM Configuration wizard for System B:	
What is the name of the EIM domain controller for the EIM domain that you want to join?	systema.myco.com
Do you plan on securing the connection with SSL or TLS?	No
What is the port on which the EIM domain controller listens?	389
Which user do you want to use to connect to the domain controller? This is the connection user. Note: Specify the LDAP administrator's distinguished name (DN) and password to ensure the wizard has enough authority to administer the EIM domain and the objects in it.	User type: Distinguished name and password Distinguished name: cn=administrator Password: mycopwd Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
What is the name of the EIM domain that you want to join?	MyCoEimDomain
Do you want to specify a parent DN for the EIM domain?	No
What is the name of the user registry that you want to add to the EIM domain?	Local i5/OS--SYSTEMB.MYCO.COM
Which EIM user do you want System B to use when performing EIM operations? This is the system user. Note: Earlier in this scenario, you used the EIM Configuration wizard to configure the directory server on System A. In doing so, you created a DN and password for the LDAP administrator. This is currently the only DN defined for the directory server. Therefore, this is the DN and password you must supply here.	User type: Distinguished name and password Distinguished name: cn=administrator Password: mycopwd Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

Table 6. Single sign-on configuration planning work sheet - user profiles

i5/OS user profile name	Password is specified	Special authority (Privilege class)	System
SYSUSERA	No	User	System A
SYSUSERB	No	User	System B

Table 7. Single sign-on configuration planning work sheet - EIM domain data

Identifier name	User registry	User identity	Association type	Identifier description
John Day	MYCO.COM	jday	Source	Kerberos (Windows 2000) login user identity
John Day	SYSTEMA.MYCO.COM	JOHND	Target	i5/OS user profile on System A

Table 7. Single sign-on configuration planning work sheet - EIM domain data (continued)

Identifier name	User registry	User identity	Association type	Identifier description
John Day	SYSTEMB.MYCO.COM	DAYJO	Target	i5/OS user profile on System B
Sharon Jones	MYCO.COM	sjones	Source	Kerberos (Windows 2000) login user identity
Sharon Jones	SYSTEMA.MYCO.COM	SHARONJ	Target	i5/OS user profile on System A
Sharon Jones	SYSTEMB.MYCO.COM	JONESSH	Target	i5/OS user profile on System B

Table 8. Single sign-on configuration planning work sheet - EIM domain data - policy associations

Policy association type	Source user registry	Target user registry	User identity	Description
Default registry	MYCO.COM	SYSTEMA.MYCO.COM	SYSUSERA	Maps authenticated Kerberos user to appropriate i5/OS user profile
Default registry	MYCO.COM	SYSTEMB.MYCO.COM	SYSUSERB	Maps authenticated Kerberos user to appropriate i5/OS user profile

Related information

Enterprise Identity Mapping (EIM)

Creating a basic single sign-on configuration for System A

The EIM Configuration wizard helps you create a basic EIM configuration and also opens the Network Authentication Service wizard to allow you to create a basic network authentication service configuration.

About this task

Note: Instructions in this scenario are based on the assumption that the IBM Tivoli Directory Server for i5/OS has not been previously configured on System A. However, if you already configured the directory server, you can still use these instructions with only slight differences. These differences are noted in the appropriate places within the configuration steps.

Use the information from your work sheets to configure EIM and network authentication service on System A. When you complete this step, you accomplish the following:

- Create a new EIM domain.
- Configure the directory server on System A to be the EIM domain controller.
- Configure network authentication service.
- Create EIM registry definitions for the i5/OS registry and the Kerberos registry on System A.
- Configure System A to participate in the EIM domain.

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping**.

2. Right-click **Configuration** and select **Configure** to start the EIM configuration wizard.
3. On the **Welcome** page, select **Create and join a new domain**. Click **Next**.
4. On the **Specify EIM Domain Location** page, select **On the local Directory server**. Click **Next**.
5. Complete these tasks to configure network authentication service:
 - a. On the **Configure Network Authentication Service** page, select **Yes**.

Note: This launches the Network Authentication Service wizard. With this wizard, you can configure several i5/OS interfaces and services to participate in the Kerberos realm.

- b. On the **Specify Realm Information** page, enter MYCO.COM in the **Default realm** field and select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
- c. On the **Specify KDC Information** page, enter kdc1.myco.com for the name of the Kerberos server in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
- d. On the **Specify Password Server Information** page, select **Yes**. Enter kdc1.myco.com in the **Password server** field and 464 in the **Port** field. Click **Next**.
- e. On the **Select Keytab Entries** page, select **i5/OS Kerberos Authentication**. Click **Next**.
- f. On the **Create i5/OS Keytab Entry** page, enter and confirm a password, and click **Next**. For example, systema123. This password is used when the System A service principal is added to the Kerberos server.

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

- g. On the **Create Batch File** page, select **Yes**, specify the following information, and click **Next**:
 - **Batch file:** Add the text systema to the end of the default batch file name. For example, C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat.
 - Select **Include password**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is recommended that you delete the batch file from the Kerberos server and from your PC immediately after use.

Note: If you do not include the password, you will be prompted for the password when the batch file is run.

- h. On the **Summary** page, review the network authentication service configuration details. Click **Finish**.
6. On the **Configure Directory Server** page, enter the following information, and click **Next**.

Note: If you configured the directory server before you started this scenario, you will see the **Specify User for Connection** page instead of the **Configure Directory Server** page. In that case, you must specify the distinguished name and password for the LDAP administrator.

- **Port:** 389
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

7. On the **Specify Domain** page, enter the name of the domain in the **Domain** field. For example, MyCoEimDomain.
8. On the **Specify Parent DN for Domain** page, select **No**. Click **Next**.

Note: If the directory server is active, a message is displayed that indicates you need to end and restart the directory server for the changes to take effect. Click **Yes** to restart the directory server.

9. On the **Registry Information** page, select **Local i5/OS** and **Kerberos**. Click **Next**. Write down the registry names. You will need these registry names when you create associations to EIM identifiers.

Note:

- Registry names must be unique to the domain.
- You can enter a specific registry definition name for the user registry if you want to use a specific registry definition naming plan. However, for this scenario you can accept the default values.

10. On the **Specify EIM System User** page, select the user the operating system uses when performing EIM operations on behalf of operating system functions, and click **Next**.

Note: Because you did not configure the directory server prior to performing the steps in this scenario, the only distinguished name (DN) that you can choose is the LDAP administrator's DN.

- **User type:** Distinguished name and password
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

11. On the **Summary** page, confirm the EIM configuration information. Click **Finish**.

Results

You have completed a basic EIM and network authentication service configuration on System A. The next step is to configure System B to participate in the EIM domain that you just created

Configuring System B to participate in the EIM domain and configure System B for network authentication service

After you have created a new domain and configured network authentication service on System A, you need to configure System B to participate in the EIM domain and configure network authentication service on System B.

About this task

Use the information from your work sheets to complete this step.

1. In System i Navigator, expand **System B** → **Network** → **Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Configure** to start the configuration wizard.
3. On the **Welcome** page, select **Join an existing domain**. Click **Next**.
4. Complete these tasks to configure network authentication service:
 - a. On the **Configure Network Authentication Service** page, select **Yes**.

Note: This launches the Network Authentication Service wizard. This wizard allows you to configure several i5/OS interfaces and services to participate in a Kerberos network.

- b. On the **Specify Realm Information** page, enter MYCO.COM in the **Default realm** field and select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
- c. On the **Specify KDC Information** page, enter kdc1.myco.com for the name of the Kerberos server in the **KDC** field and enter 88 in the **Port** field. Click **Next**.

- d. On the **Specify Password Server Information** page, select **Yes**. Enter `kdc1.myco.com` in the **Password server** field and `464` in the **Port** field. Click **Next**.
- e. On the **Select Keytab Entries** page, select **i5/OS Kerberos Authentication**. Click **Next**.
- f. On the **Create i5/OS Keytab Entry** page, enter and confirm a password, and click **Next**. For example, `systema123`. This password will be used when the System A service principal is added to the Kerberos server.

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

- g. On the **Create Batch File** page, select **Yes**, specify the following information, and click **Next**.
 - **Batch file:** Add the text `systemb` to the end of the default batch file name. For example, `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystemb.bat`.
 - Select **Include password**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is recommended that you delete the batch file from the Kerberos server and from your PC immediately after use.

Note: If you do not include the password, you will be prompted for the password when the batch file is run.

- h. On the **Summary** page, review the network authentication service configuration details. Click **Finish**.
5. On the **Specify Domain Controller** page, specify the following information, and click **Next**.
 - **Domain controller name:** `systema.myco.com`
 - **Port:** `389`
6. On the **Specify User for Connection** page, specify the following information, and click **Next**

Note: Specify the LDAP administrator's DN and password that you created earlier in this scenario on System A.

- **User type:** Distinguished name and password
- **Distinguished name:** `cn=administrator`
- **Password:** `mycopwd`

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

7. On the **Specify Domain** page, select the name of the domain that you want to join. Click **Next**. For example, `MyCoEimDomain`.
8. On the **Registry Information** page, select **Local i5/OS** and deselect **Kerberos registry**. (The Kerberos registry was created when you created the `MyCoEimDomain` domain.) Click **Next**. Write down the registry names. You will need these registry names when you create associations to EIM identifiers.

Note:

- Registry names must be unique to the domain.
 - You can enter a specific registry definition name for the user registry if you want to use a specific registry definition naming plan. However, for this scenario you can accept the default values.
9. On the **Specify EIM System User** page, select the user the operating system uses when performing EIM operations on behalf of operating system functions, and click **Next**.

Note: Specify the LDAP administrator's DN and password that you created earlier in this scenario on System A.

- **User type:** Distinguished name and password
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

10. On the **Summary** page, confirm the EIM configuration. Click **Finish**.

Results

You have now configured System B to participate in the domain and to use network authentication service.

Adding both i5/OS service principals to the Kerberos server

You can use one of two methods to add the necessary i5/OS service principals to the Kerberos server.

About this task

You can manually add the service principals or, as this scenario illustrates, you can use a batch file to add them. You created this batch file in Step 2. To use this file, you can use File Transfer Protocol (FTP) to copy the file to the Kerberos server and run it.

Follow these steps to use the batch file to add principal names to the Kerberos server:

FTP batch files created by the wizard

1. On the Windows 2000 workstation that the administrator used to configure network authentication service, open a command prompt and type `ftp kdc1.myco.com`. This will start an FTP session on your PC. You will be prompted for the administrator's user name and password.
2. At the FTP prompt, type `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Press Enter. You should receive the message `Local directory now C:\Documents and Settings\All Users\Documents\IBM\Client Access`.
3. At the FTP prompt, type `cd \mydirectory`, where *mydirectory* is a directory located on kdc1.myco.com.
4. At the FTP prompt, type `put NASConfigsystema.bat`. You should receive this message: `226 Transfer complete`.
5. Type `quit` to exit the FTP session.

Note: Repeat these steps to transfer `NASConfigsystemb.bat` file to the Windows 2000 server.

What to do next

Run both batch files on kdc1.myco.com

1. On your Windows 2000 server, open the directory where you transferred the batch files.
2. Find the `NASConfigsystema.bat` file and double click the file to run it.
3. Repeat these steps for `NASConfigsystemb.bat`.
4. After each file runs, verify that the i5/OS principal has been added to the Kerberos server by completing the following:
 - a. On your Windows 2000 server, expand **Administrative Tools** → **Active Directory Users and Computers** → **Users**.
 - b. Verify the System i model has a user account by selecting the appropriate Windows 2000 domain.

Note: This Windows 2000 domain should be the same as the default realm name that you specified in the network authentication service configuration.

- c. In the list of users that is displayed, find **systema_1_krbsvr400** and **systemb_1_krbsvr400**. These are the user accounts generated for the i5/OS principal name.
- d. (Optional) Access the properties on your Active Directory users. From the **Account** tab, select the **Account is trusted for delegation**.

Note: This optional step enables your system to delegate, or forward, a user's credentials to other systems. As a result, the i5/OS service principal can access services on multiple systems on behalf of the user. This is useful in a multi-tier network.

Now that you have added the i5/OS service principals to the Kerberos server, you can create user profiles on the System i model.

Creating user profiles on System A and System B

You want all of your users in the MYCO.COM Kerberos registry to map to a single i5/OS user profile on each of your System i model.

About this task

Therefore, you need to create an i5/OS user profile on System A and System B. Use the information from your work sheets to create a user profile for these users:

1. In System i Navigator, expand **System A** → **User and Groups**.
2. Right-click **All Users**, and select **New User**.
3. On the **New User** dialog box, enter SYSUSERA in the **User name** field.
4. In the **Password** field, select **No password (sign-on not allowed)**.
5. Click **Capabilities**.
6. On the **Privileges** page, select **User** in the **Privilege class** field. Click **OK** and click **Add**.

What to do next

Repeat these steps on System B, but enter SYSUSERB in the **User name** field.

Now that you have created the user profiles on System A and System B, you can create the home directories for all of the i5/OS user profiles.

Creating home directories on System A and System B

Each user that connects to a System i model and applications needs a directory in the /home directory. This directory stores the user's Kerberos credentials cache.

About this task

To create a home directory for a user, complete the following:

On the System A command line, enter: CRTDIR '/home/user profile' where user profile is the System i user profile name for the user. For example: CRTDIR '/home/SYSUSERA'. This creates a home directory for the user profile on System A that represents all the Active Directory users.

Repeat this command on System B but specify SYSUSERB to create a home directory for the user profile on System B.

Results

Now that you have created the home directories, you can test the network authentication service configuration on the systems.

Testing network authentication service on System A and System B

After you complete the network authentication service configuration tasks for both of your systems, you need to verify that your configurations work correctly for both System A and System B.

About this task

You can do this testing by completing these steps to request a ticket granting ticket for the System A and System B principals:

Note: Ensure that you have created a home directory for your iSeries® user profile before performing this procedure.

1. On a command line, enter QSH to start the Qshell Interpreter.
2. Enter `keytab list` to display a list of principals registered in the keytab file. In this scenario, `krbsvr400/systema.myco.com@MYCO.COM` should display as the principal name for System A.
3. Enter `kinit -k krbsvr400/systema.myco.com@MYCO.COM` to request a ticket-granting ticket from the Kerberos server. By running this command, you can verify that your System i model has been configured properly and that the password in the keytab file matches the password stored on the Kerberos server. If this is successful then the `kinit` command will display without errors.
4. Enter `klist` to verify that the default principal is `krbsvr400/iseriesa.myco.com@MYCO.COM`. This command displays the contents of a Kerberos credentials cache and verifies that a valid ticket has been created for the System i model service principal and placed within the credentials cache on the system.

```
Ticket cache: FILE:/QIBM/USERDATA/0S400/NETWORKAUTHENTICATION/creds/krbcred
Default principal: krbsvr400/systema.myco.com@MYCO.COM
Server: krbtgt/MYCO.COM@MYCO.COM
Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

Results

Repeat these steps using the service principal name for System B: `krbsvr400/systemb.myco.com@MYCO.COM`

Now that you have tested network authentication service on System A and System B, you can create an EIM identifier for each of the administrators.

Creating EIM identifiers for two administrators, John Day and Sharon Jones

In this scenario, you create two EIM identifiers, one named John Day and the other named Sharon Jones.

About this task

As part of setting up your single sign-on test environment, you need to create EIM identifiers for two of your administrators so they can both log on to System i environments using their Windows user identities.

To create the EIM identifiers, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

- **User type:** Distinguished name
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **Identifiers** and select **New Identifier**.
3. On the **New EIM Identifier** dialog box, enter John Day in the **Identifier** field.
4. Click **OK**.

Results

Repeat steps 2 through 4, but enter Sharon Jones in the **Identifier** field.

Now that you have created an EIM identifier for each of the administrators, you must create identifier associations that map user identities to the identifiers. First, create the identifier associations for John Day.

Creating identifier associations for John Day

You must create the appropriate associations between the EIM identifier, John Day, and the user identities that the person represented by the identifier uses. These identifier associations, when properly configured, enable the user to participate in a single sign-on environment.

About this task

In this scenario, you need to create one source association and two target associations for the John Day identifier:

- A source association for the jday Kerberos principal, which is the user identity that John Day, the person, uses to log in to Windows and the network. The source association allows the Kerberos principal to be mapped to another user identity as defined in a corresponding target association.
- A target association for the JOHND System i user profile, which is the user identity that John Day, the person, uses to log in to System i model and to other System i applications on System A. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.
- A target association for the DAYJO System i user profile, which is the user identity that John Day, the person, uses to log in to System i Navigator and other System i applications on System B. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.

Use the information from your planning work sheets to create the associations.

To create the source association for John Day's Kerberos principal, follow these steps:

1. On System A, expand **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **Identifiers**.
2. Right-click **John Day** and select **Properties**.
3. On the **Associations** page, click **Add**.
4. In the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**.
 - **Registry:** MYCO.COM

- **User:** jday
 - **Association type:** Source
5. Click **OK** to close the **Add Associations** dialog box.

What to do next

To create a target association for John Day's System i user profile on System A, follow these steps:

1. On the **Associations** page, click **Add**.
2. In the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
 - **Registry:** SYSTEMA.MYCO.COM
 - **User:** JOHND
 - **Association type:** Target
3. Click **OK** to close the **Add Associations** dialog box.

To create a target association for John Day's System i user profile on System B, follow these steps:

1. On the **Associations** page, click **Add**.
2. In the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
 - **Registry:** SYSTEMB.MYCO.COM
 - **User:** DAYJO
 - **Association type:** Target
3. Click **OK** to close the **Add Associations** dialog box.
4. Click **OK** to close the **Properties** dialog box.

Now that you have created the identifier associations that map John Day's user identities to his EIM identifier, you can create similar associations for Sharon Jones.

Creating identifier associations for Sharon Jones

You must create the appropriate associations between the EIM identifier, Sharon Jones, and the user identities that the person represented by the identifier uses. These associations, when properly configured, enable the user to participate in a single sign-on environment.

About this task

In this scenario, you need to create one source association and two target associations for the Sharon Jones identifier:

- A source association for the sjones Kerberos principal, which is the user identity that Sharon Jones, the person, uses to log in to Windows and the network. The source association allows the Kerberos principal to be mapped to another user identity as defined in a corresponding target association.
- A target association for the SHARONJ i5/OS user profile, which is the user identity that Sharon Jones, the person, uses to log in to System i Navigator and other i5/OS applications on System A. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.
- A target association for the JONSSH i5/OS user profile, which is the user identity that Sharon Jones, the person, uses to log in to System i Navigator and other i5/OS applications on System B. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.

Use the information from your planning work sheets to create the associations:

To create the source association for Sharon Jones' Kerberos principal, follow these steps:

1. On System A, expand **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **Identifiers**.
2. Right-click **Sharon Jones** and select **Properties**.
3. On the **Associations** page, click **Add**.
4. On the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**.
 - **Registry:** MYCO.COM
 - **User:** sjones
 - **Association type:** Source
5. Click **OK** to close the **Add Associations** dialog box.

What to do next

To create a target association to Sharon Jones' i5/OS user profile on System A, follow these steps:

1. On the **Associations** page, click **Add**.
2. On the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
 - **Registry:** SYSTEMA.MYCO.COM
 - **User:** SHARONJ
 - **Association type:** Target
3. Click **OK** to close the **Add Associations** dialog box.

To create a target association to Sharon Jones' i5/OS user profile on System B, follow these steps:

4. On the **Associations** page, click **Add**.
5. On the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
 - **Registry:** SYSTEMB.MYCO.COM
 - **User:** JONESH
 - **Association type:** Target
6. Click **OK** to close the **Add Associations** dialog box.
7. Click **OK** to close the **Properties** dialog box.

Now that you have created the identifier associations that map Sharon Jones' user identities to her EIM identifier, you can create the default registry policy associations that map all of your Kerberos registry users to a specific user profile in each of the System i model user registries.

Creating default registry policy associations

You want to have all your Microsoft Active Directory users on the Windows 2000 server map to the user profile, SYSUSERA, on System A and to the user profile, SYSUSERB, on System B.

About this task

Fortunately, you can use policy associations to create mappings directly between a group of users and a single target user identity. In this case, you can create a default registry policy association that maps all the user identities (for which no identifier associations exist) in the MYCO.COM Kerberos registry to a single i5/OS user profile on System A.

You need two policy associations to accomplish this goal. Each policy association uses the MYCO.COM user registry definition as the source of the association. However, each policy association maps user identities in this registry to different target user identities, depending on which System i model the Kerberos user accesses:

- One policy association maps the Kerberos principals in the MYCO.COM user registry to a target user of SYSUSERA in the target registry of SYSTEMA.MYCO.COM.
- The other policy association maps the Kerberos principals in the MYCO.COM user registry to a target user of SYSUSERB in the target registry of SYSTEMB.MYCO.COM.

Use the information from your planning works sheets to create two default registry policy associations.

Note: Before you can use policy associations, however, you must first ensure that you enable the domain to use policy associations for mapping lookup operations. You can do this as part of the process for creating your policy associations, as follows:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management**.
2. Right-click **MyCoEimDomain**, and select **Mapping policy**.
3. On the **General** page, select the **Enable mapping lookups using policy associations for domain MyCoEimDomain**.

What to do next

Follow these steps to create the default registry policy association for the users to map to the SYSUSERA user profile on System A:

1. On the **Registry** page, click **Add**.
2. In the **Add Default Registry Policy Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
 - **Source registry:** MYCO.COM
 - **Target registry:** SYSTEMA.MYCO.COM
 - **Target user:** SYSUSERA
3. Click **OK** to close the **Mapping Policy** dialog box.

Follow these steps to create the default registry policy association for the users to map to the SYSUSERB user profile on System B:

4. On the **Registry** page, click **Add**.
5. In the **Add Default Registry Policy Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
 - **Source registry:** MYCO.COM
 - **Target registry:** SYSTEMB.MYCO.COM
 - **Target user:** SYSUSERB
6. Click **OK** to close the **Mapping Policy** dialog box.

Now that you have created the default registry policy associations, you can enable the registries to participate in lookup operations and to use the policy associations.

Enabling registries to participate in lookup operations and to use policy associations

EIM allows you to control how each registry participates in EIM. Because a policy association can have a large scale effect within an enterprise, you can control whether a registry can be affected by policy associations.

About this task

Also, you can control whether a registry can participate in mapping lookup operations at all. To use policy associations for a registry, you must enable their use for that registry as well as enable that registry to participate in lookup operations. To enable registries to use policy associations and participate in lookup operations, complete these steps:

To enable the MYCO.COM registry to participate in mapping lookup operations, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **User registries**.
2. Right-click the MYCO.COM registry and select **Mapping Policy**.
3. On the **General** page, select **Enable mapping lookups for registry MYCO.COM**, and click **OK**.

What to do next

To enable the SYSTEMA.MYCO.COM registry to participate in mapping lookup operations and to use policy associations, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **User registries**.
2. Right-click the SYSTEMA.MYCO.COM registry and select **Mapping Policy**.
3. On the **General** page, select **Enable mapping lookups for registry SYSTEMA.MYCO.COM**, select **Use policy associations**, and click **OK**.

Repeat these steps to enable the SYSTEMB.MYCO.COM registry to participate in mapping lookup operations and to use policy associations, but on the **General** page, select **Enable mapping lookups for registry SYSTEMB.MYCO.COM**, select **Use policy associations**, and click **OK**.

Now that you have completed the EIM configuration for your registries and users, you should test the resulting mappings to ensure that they work as planned.

Testing EIM identity mappings

Now that you have created all the associations that you need, you must verify that EIM mapping lookup operations return the correct results based on the configured associations.

About this task

For this scenario, you must test the mappings used for the identifier associations for each of the administrators and you must test the mappings used for the default registry policy associations. To test the EIM mappings, follow these steps:

Test mappings for John Day

To test that identifier mappings work as expected for John Day, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

- **User type:** Distinguished name
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **MyCoEimDomain** and select **Test a mapping**.
3. On the **Test a mapping** dialog box, specify or **Browse** to select the following information, and click **Test**.

- **Source registry:** MYCO.COM
- **Source user:** jday
- **Target registry:** SYSTEMA.MYCO.COM

4. Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	JOHND
Origin	EIM Identifier: John Day

5. Click **Close**.

Repeat these steps but select SYTEMB.MYCO.COM for the **Target registry** field. Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	DAYJO
Origin	EIM Identifier: John Day

What to do next

Test mappings for Sharon Jones

To test the mappings used for the individual associations for Sharon Jones, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

- **User type:** Distinguished name
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **MyCoEimDomain** and select **Test a mapping**.
3. On the **Test a mapping** dialog box, specify or **Browse** to select the following information, and click **Test**:
 - **Source registry:** MYCO.COM
 - **Source user:** sjones
 - **Target registry:** SYSTEMA.MYCO.COM

4. Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	SHARONJ
Origin	EIM Identifier: Sharon Jones

5. Click **Close**.

Repeat these steps but select SYSTEMB.MYCO.COM for the **Target registry** field. Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	JONESSH
Origin	EIM Identifier: Sharon Jones

Test mappings used for default registry policy associations

To test that mappings work as expected for the users in the Order Receiving Department, as based on the policy associations that you defined, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

- **User type:** Distinguished name
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **MyCoEimDomain** and select **Test a mapping**.
3. On the **Test a mapping** dialog box, specify or **Browse** to select the following information, and click **Test**:
 - **Source registry:** MYCO.COM
 - **Source user:** mmiller
 - **Target registry:** SYSTEMA.MYCO.COM
4. Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	SYSUSERA
Origin	Registry policy association

5. Click **Close**.

To test the mappings used for the default registry policy association that maps your users to the SYSUSERB profile on System B, follow these steps:

1. In System i Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

- **User type:** Distinguished name
- **Distinguished name:** cn=administrator
- **Password:** mycopwd

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **MyCoEimDomain** and select **Test a mapping**.
3. On the **Test a mapping** dialog box, specify or **Browse** to select the following information, and click **Test**:
 - **Source registry:** MYCO.COM
 - **Source user:** ksmith
 - **Target registry:** SYSTEMB.MYCO.COM
4. Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	SYSUSERB
Origin	Registry policy association

5. Click **Close**.

If you receive messages or errors that indicate problems with your mappings or with communications, see **Troubleshoot EIM** to help you find solutions to these problems.

Now that you have tested the EIM identity mappings, you can configure System i Access for Windows applications to use Kerberos authentication.

Configuring System i Access for Windows applications to use Kerberos authentication

You must use Kerberos to authenticate before you can use System i Navigator to access your system. Therefore, from your PC, you need to configure System i Access for Windows to use Kerberos authentication.

About this task

To configure System i Access for Windows applications to use Kerberos authentication, complete the following steps:

Note: Each of your users needs to perform all of these steps on their own PC.

1. Log on to the Windows 2000 domain by signing in to your PC.
2. In System i Navigator on your PC, right-click **System A** and select **Properties**.
3. On the **Connection** page, select **Use Kerberos principal name, no prompting**. This will allow System i Access for Windows connections to use the Kerberos principal name and password for authentication.
4. A message is displayed that indicates you need to close and restart all applications that are currently running for the changes to the connection settings to take effect. Click **OK**. Then, end and restart System i Navigator.

Results

Now that you have configured System i Access for Windows applications to use Kerberos authentication, you can verify the single sign-on environment.

Verifying network authentication service and EIM configuration

Now that you have verified the individual pieces of your single sign-on configuration and ensured that all setup is complete, you must verify that you have configured EIM and network authentication service correctly and that single sign-on works as expected.

About this task

To verify that your single sign-on environment works correctly, have John Day follow these steps:

1. In System i Navigator, expand **System A** to open a connection to System A.
2. Press F5 to refresh the screen.
3. In the right pane, find System A in the **Name** column, and verify that John Day's i5/OS user profile, JOHND, is displayed as the corresponding entry in the **Signed On User** column.

Results

System i Navigator successfully used EIM to map the jday Kerberos principal to the JOHND System A user profile because of the associations defined for EIM identifier, John Day. The System i Navigator session for System A is now connected as JOHND.

Repeat these steps for Sharon Jones and for at least one of the user identities that is mapped to the SYSUSERA or SYSUSERB user profile.

(Optional) Postconfiguration considerations

Now that you finished this scenario, the only EIM user you have defined that EIM can use is the DN for the LDAP administrator.

About this task

The LDAP administrator DN that you specified for the system user on System A has a high level of authority to all data on the directory server. Therefore, you might consider creating one or more DNs as additional users that have more appropriate and limited access control for EIM data. The number of additional EIM users that you define depends on your security policy's emphasis on the separation of security duties and responsibilities. Typically, you might create at least the two following types of DNs:

- **A user that has EIM administrator access control**

This EIM administrator DN provides the appropriate level of authority for an administrator who is responsible for managing the EIM domain. This EIM administrator DN can be used to connect to the domain controller when managing all aspects of the EIM domain by means of System i Navigator.

- **At least one user that has all of the following access controls:**

- Identifier administrator
- Registry administrator
- EIM mapping operations

This user provides the appropriate level of access control required for the system user that performs EIM operations on behalf of the operating system.

Note: To use this new DN for the system user instead of the LDAP administrator DN, you must change the EIM configuration properties for each system. For this scenario, you need to change the EIM configuration properties for any System i model that you set up.

Scenario: Propagating network authentication service and EIM across multiple systems

This scenario demonstrates how to use the Synchronize Functions wizard in System i Navigator to propagate a single sign-on configuration across multiple systems in a mixed i5/OS release environment. Administrators can save time by configuring single sign-on once and propagating that configuration to all of their systems, instead of configuring each system individually.

Situation

You are a network administrator for a large auto parts manufacturer. You manage five systems with System i Navigator. One system operates as the central system, which stores data and manages the endpoint systems. You have read about the benefits of single sign-on and you want to configure a single sign-on environment for your enterprise. You have just completed the process of setting up a test environment on one system and you want to extend your single sign-on environment throughout the enterprise. You have four other servers to configure and you want to find a way to configure them as efficiently as possible.

You know that System i Navigator provides the Synchronize Functions wizard that allows you to copy the single sign-on configuration from one system and apply it to other i5/OS V5R3, or later, systems. This eliminates the need to configure each system separately.

However, one of your systems runs OS/400® Version 5 Release 2 (V5R2). OS/400 V5R2 does not support the Synchronize Functions wizard, which means that you must separately configure this system to match the current network authentication service and EIM configurations on your model system.

This scenario has the following advantages:

- Simplifies the task of configuring network authentication service and EIM on multiple systems to create a single sign-on environment.
- Saves you time and effort as you use a single wizard to copy and apply one manual configuration to a number of other servers.

Objectives

As the network administrator for MyCo, Inc., you want to create a single sign-on environment for your enterprise in which all your servers will participate and you want to configure your servers as quickly and easily as possible.

The objectives of this scenario are as follows:

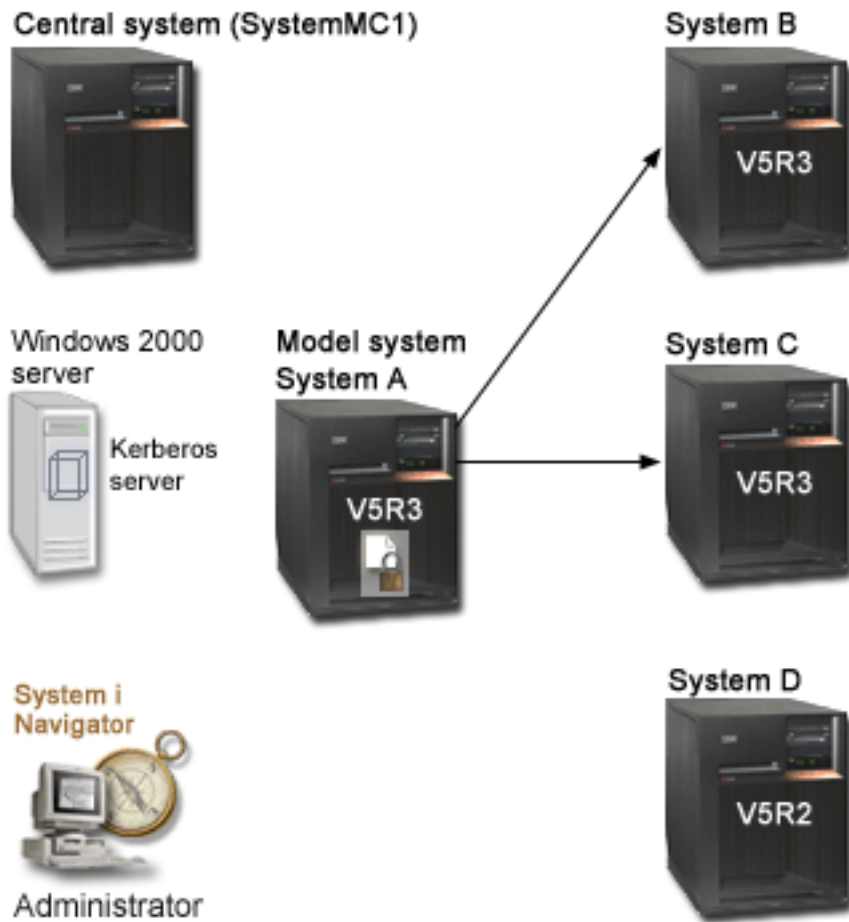
- System A has existing network authentication service and EIM configurations from when it was set up to create a test environment. Consequently, System A must be used as the model system for propagating these configurations to the end point systems of System B and System C.
- All of the systems will be configured to join the same EIM domain and must use the same Kerberos server and the same domain controller.

Note: Refer to Domains to learn how two types of domains, an EIM domain and a Windows 2000 domain, both fit into the single sign-on environment.

- System D, the OS/400 V5R2 system, must be configured manually for network authentication service and EIM.

Details

The following figure illustrates the network environment for this scenario.



The figure illustrates the following points relevant to this scenario.

Windows 2000 server

- Acts as the Kerberos server, also known as the key distribution center (KDC), for the network.
- All users are registered with the Kerberos server on the Windows 2000 server.

System MC1 - Central system

- Runs on i5/OS Version 5 Release 3 (V5R3), or later, with the following options and licensed programs installed:
 - i5/OS Host Servers
 - System i Access for Windows
- Stores, schedules, and runs synchronize functions for each of the endpoint systems.
- Is configured for network authentication service and EIM.

System A - Model system

Note: The model system should be configured similarly to the system identified as System A in the “Scenario: Creating a single sign-on test environment” on page 10 scenario. Refer to this scenario to ensure that all of the single sign-on configuration tasks on the model system are completed and verified.

- | • Runs i5/OS Version 5 Release 3 (V5R3), or later, with the following options and licensed programs installed:
 - | – i5/OS Host Servers
 - | – System i Access for Windows
- | • Is configured for network authentication service and EIM.
- | • Is the model system from which the network authentication service and EIM configurations are propagated to the target systems.

System B

- | • Runs i5/OS Version 5 Release 3 (V5R3), or later, with the following options and licensed programs installed:
 - | – i5/OS Host Servers
 - | – System i Access for Windows
- | • Is one of the target systems for the propagation of network authentication service and EIM configurations.

System C

- | • Runs i5/OS Version 5 Release 3 (V5R3), or later, with the following options and licensed programs installed:
 - | – i5/OS Host Servers
 - | – System i Access for Windows
- | • Is one of the target systems for the propagation of network authentication service and EIM configurations.

System D

- Runs OS/400 Version 5 Release 2 (V5R2) with the following options and licensed programs installed:
 - OS/400 Host Servers
 - System i Access for Windows
 - Cryptographic Access Provider
- Has the following V5R2 PTFs (program temporary fixes) applied:
 - SI08977
 - SI08979
- Requires separate, manual configuration of network authentication service and EIM using the appropriate wizards in System i Navigator.

Administrator’s PC

- | • Runs System i Access for Windows
- | • Runs System i Navigator V5R4, or later, with the following subcomponents:
 - | **Note:** Only required for PC used to administer network authentication service.
 - | – Network
 - | – Security

Prerequisites and assumptions

Successful implementation of this scenario requires that the following assumptions and prerequisites are met:

System MC1 - Central system prerequisites

1. All system requirements, including software and operating system installation, have been verified. To verify that these licensed programs have been installed, complete the following:
 - a. In System i Navigator, expand **your system** → **Configuration and Service** → **Software** → **Installed Products**.
 - b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup is complete.
3. TCP/IP and basic system security are configured and tested.
4. Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these servers.

Note: When you propagate network configuration service configuration among servers, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your Local Area Network (LAN). See Scenario: Secure all connections to your Management Central server with SSL for details.

System A - Model system prerequisites

Note: This scenario assumes that System A is properly configured for single sign-on. Refer to the “Scenario: Creating a single sign-on test environment” on page 10 scenario to ensure that all of the single sign-on configuration tasks on the model system are completed and verified.

1. All system requirements, including software and operating system installation, have been verified. To verify that these licensed programs have been installed, complete the following:
 - a. In System i Navigator, expand **your system** → **Configuration and Service** → **Software** → **Installed Products**.
 - b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup is complete.
3. TCP/IP and basic system security are configured and tested.
4. Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these servers.

Note: When you propagate network configuration service configuration among servers, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your Local Area Network (LAN). See Scenario: Secure all connections to your Management Central server with SSL for details.

System B, System C, and System D - Endpoint systems prerequisites

1. All system requirements, including software and operating system installation, have been verified. To verify that these licensed programs have been installed, complete the following:
 - a. In System i Navigator, expand **your system** → **Configuration and Service** → **Software** → **Installed Products**.
 - b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup is complete.
3. TCP/IP and basic system security are configured and tested.
4. Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these servers.

Note: When you propagate network configuration service configuration among servers, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your Local Area Network (LAN). See Scenario: Secure all connections to your Management Central server with SSL for details.

Windows 2000 server prerequisites

1. All necessary hardware planning and setup have been completed.
2. TCP/IP has been configured and tested on the server.
3. Windows 2000 domain has been configured and tested.
4. All users within your network have been added to the Kerberos server.

Configuration steps

To propagate the network authentication service and EIM configurations from the model system, System A to the endpoint systems, System B and System C, you must complete the following tasks:

Note: You need to understand the concepts related to single sign-on, which include network authentication service and Enterprise Identity Mapping (EIM) concepts, before you implement this scenario. See the following information to learn about the terms and concepts related to single sign-on:

Related information

Enterprise Identity Mapping (EIM)

Completing the planning work sheets

The following planning work sheets are tailored to fit this scenario based on the general single sign-on planning worksheets.

About this task

These planning work sheets demonstrate the information that you need to gather and the decisions you need to make to prepare for this scenario. To ensure a successful implementation, you must be able to answer Yes to all prerequisite items in the work sheet and you should gather all the information necessary to complete the work sheets before you perform any configuration tasks.

Table 9. Propagate network authentication service and EIM - prerequisite work sheet

Prerequisite work sheet	Answers
Is your system running i5/OS V5R3, or later, for the following systems: <ul style="list-style-type: none"> • System MC1 • System A • System B • System C 	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
For System D, are you running OS/400 V5R2, or later?	Yes
For System D, have you applied the latest program temporary fixes (PTFs), including the following: <ul style="list-style-type: none"> • SI08977 • SI08979 	Yes

Table 9. Propagate network authentication service and EIM - prerequisite work sheet (continued)


Prerequisite work sheet	Answers
<p>Are the following options and licensed programs installed on all your System i models?</p> <ul style="list-style-type: none"> • i5/OS Host Servers (5761-SS1 Option 12) • IBM System i Access for Windows (5761-XE1) • Cryptographic Access Provider for OS/400 V5R2 or i5/OS V5R3 systems. This option is not required for systems running i5/OS V5R4, or later. <p>Note: 5722 is the product code for i5/OS options and products, prior to V6R1.</p>	Yes
Is System i Access for Windows (5761-XE1) installed on the administrator's PC?	Yes
<p>Is System i Navigator installed on the administrator's PC with the following subcomponents?</p> <ul style="list-style-type: none"> • Network • Security 	Yes
Have you installed the latest IBM System i Access for Windows service pack? For the latest service pack see, System i Access web page  .	Yes
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes
<p>Do you have one of the following systems acting as the Kerberos server? If yes, specify which system.</p> <ol style="list-style-type: none"> 1. Microsoft Windows 2000 Server Note: Microsoft Windows 2000 Server uses Kerberos authentication as its default security mechanism. 2. Windows^(R) Server 2003 3. i5/OS PASE (V5R3 or later) 4. AIX server 5. z/OS 	Yes, Windows 2000 Server
For Windows 2000 Server and Windows ^(R) Server 2003, do you have Windows Support Tools (which provides the ktpass tool) installed?	Yes
Is the System i model time within 5 minutes of the system time on the Kerberos server? If not see, Synchronize system times.	Yes
Are you running i5/OS PASE for the Kerberos server?	You must have IBM Network Authentication Enablement for i5/OS (5761-NAE) installed.

Table 10. Propagate network authentication service and EIM - planning work sheet

Planning work sheet for propagating the network authentication service and EIM configurations from System A to System B and System C	Answers
What is the name of the system group?	MyCo system group
Which systems will be included in this system group?	System B, System C
Which system is the model system?	System A
Which functions do you plan to propagate to this system group?	Network authentication service and Enterprise Identity Mapping (EIM)
Which type of keytab entries do you want to add to the keytab file for the target systems?	i5/OS Kerberos Authentication

Table 10. Propagate network authentication service and EIM - planning work sheet (continued)

Planning work sheet for propagating the network authentication service and EIM configurations from System A to System B and System C	Answers
<p>What are the passwords that are associated with each of the service principals for the model and target systems? Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.</p>	<p>Password for the principals for System A, B, and C: system123 Password for the principal for System D: systemd123</p>
<p>Which user do you want to use to connect to the domain controller?</p>	<p>User type: Distinguished name and password Distinguished name: cn=administrator Password: mycopwd</p>

Creating a system group

Before you can propagate the network authentication service and EIM configurations to the target systems, you must create a system group for all the endpoint systems.

About this task

A system group is a collection of several systems that you can manage and to which you can apply similar settings and attributes, such as the network authentication service configuration.

1. In System i Navigator, expand **Management Central (System MC1)**.
2. Right-click **System Groups** and select **New System Group** to create a new system group.
3. On the **General** page, enter MyCo system group in the name field.
4. Specify a description for this system group.
5. From the **Available Systems** list, select System B and System C and click **Add**. This will add the systems to the **Selected systems** list.
6. Click **OK**.
7. Expand **System Groups** to verify that your system group was added.

Results

Now that you have created a system group for your endpoint systems, you can propagate the network authentication service and EIM configurations to these systems.

Propagating system settings from the model system (System A) to System B and System C

The Synchronize Functions wizard in, System i Navigator allows you to propagate system settings to multiple endpoint systems within the same system group.

About this task

Complete these tasks to propagate the network authentication service and EIM configurations to target systems:

1. In System i Navigator, expand **Management Central (System MC1)** → **System Groups**.
2. Right-click **MyCo system group** and select **System Values** → **Synchronize Functions**, and click **Next**. This will open the **Synchronize Functions Wizard**.
3. On the **Welcome** page, review the information about the Synchronize Functions wizard. The **Welcome** page lists the functions that you can choose to synchronize later in the wizard.

Note: When you propagate network configuration service and EIM configurations among servers, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your Local Area Network (LAN). See Scenario: Secure all connections to your Management Central server with SSL for details.

4. On the **Model System** page, select **System A** as the model system, and click **Next**. This model system will be used as a base for synchronizing the network authentication service and EIM configurations to other systems.
5. On the **Target Systems and Groups** page, select **MyCo system group**. Click **Next**.
6. On the **What to Update** page, select **Network Authentication Service (Kerberos)** and **Enterprise Identity Mapping**. Click **Verify configuration**. After the configuration has been verified, click **Next**.

Note: If the verification of EIM does not complete successfully, there might be a problem with the EIM configuration on the model system. If the network authentication service configuration fails, there might be a problem with the network authentication service configuration on the model system.

To recover from these errors, you need to check the EIM and network authentication service configurations on the model system, fix the configurations, and then return to the beginning of this scenario. Refer to “Scenario: Creating a single sign-on test environment” on page 10 to ensure that all of the single sign-on configuration tasks on the model system are completed and verified.

7. On the **Network Authentication Service** page, select **i5/OS Kerberos Authentication**, enter `systema123` in the **Password** and **Confirm password** fields, and click **Next**.

Note: This password is used for the keytab entry on each target system. If your security policy requires a different password on each system, then you can skip this step. Instead, after you complete this wizard, you can manually add the keytab entries to individual systems and enter a different password for each system.

8. On the **Enterprise Identity Mapping** page, select the user that the operating system uses when performing EIM operations:
 - **User Type:** Distinguished name and password
 - **Distinguished name:** `cn=administrator`
 - **Password:** `mycopwd`
9. On the **Summary** page, verify that the appropriate settings are listed on this page. Click **Finish**.
10. In System i Navigator, expand **Management Central (System MC1)** → **Task Activity** → **System Values**.
11. Verify that the task has completed successfully.

Related information

Managing keytab files

Completing the configurations for network authentication service and EIM on System B and System C

Although the Synchronize Functions wizard propagates most of the configuration that you need for a single sign-on environment, you still need to perform some additional tasks to complete your single sign-on configuration using System i Navigator for System B and System C.

About this task

These are the tasks you need to perform on System B and System C, depending on how you designed your single sign-on environment:

1. Add i5/OS service principals to the Kerberos server.
2. Create a home directory for each of your users.

3. Test network authentication service.
4. Create EIM identifiers for your users.
5. Create source associations and target associations for the EIM identifiers.
6. Optional: Create policy associations.
7. Optional: Enable the registries to participate in lookup operations and to use the policy associations.
8. Test the EIM mappings.
9. Optional: Configure System i Access for Windows applications to use Kerberos.
10. Verify network authentication service and EIM configuration.

Results

Use the “Scenario: Enabling single sign-on for i5/OS” on page 23 scenario as a guide as you complete the configurations on System B and System C. This scenario provides step-by-step instructions for completing all the tasks required for single sign-on.

You have now completed the tasks required to propagate the EIM and network authentication service configurations from System A to System B and System C.

Configuring network authentication service and EIM on the V5R2, or later, system System D

System D is running OS/400 V5R2, or later, and this release does not support the Synchronize Functions wizard.

About this task

Therefore, the configurations on System A cannot be propagated to System D. Instead, you need to use the EIM Configuration wizard and the Network Authentication Service wizard to manually configure this system, and you need to perform the additional steps required to allow System D to participate in the single sign-on environment.

These are the tasks you need to perform, depending on how you configured single sign-on on System A:

1. Configure System D to participate in the EIM domain and configure System D for network authentication service using the EIM Configuration wizard and Network Authentication Service wizard.
2. Add i5/OS service principals to the Kerberos server.
3. Create a home directory for each of your users.
4. Test network authentication service.
5. Create EIM identifiers for your users.
6. Create source associations and target associations for the EIM identifiers.
7. Optional: Create policy associations.
8. Optional: Enable the registries to participate in lookup operations and to use the policy associations.
9. Test the EIM mappings.
10. Optional: Configure System i Access for Windows applications to use Kerberos.
11. Verify network authentication service and EIM configurations.

Results

You can use the Enable single sign-on for i5/OS scenario as a guide as you configure System D to match the single sign-on configuration on System A. This scenario provides step-by-step instructions for completing all the tasks required for single sign-on. Within the enable single sign-on for i5/OS scenario, you should follow the instructions for the system identified as System B because that system joins an existing EIM domain just as System D should join the existing EIM domain in this scenario.

You have completed the propagation of the network authentication service and EIM configurations to multiple systems. To configure the Management Central server to take advantage of a single sign-on environment, you need to perform some additional tasks. See Scenario: Configure the Management Central server for a single sign-on environment for details.

Scenario: Configuring the Management Central servers for single sign-on

View this scenario to learn how to configure your Management Central servers to participate in a single sign-on environment. After administrators complete the scenario for propagating a single sign-on configuration across multiple systems, they can do the necessary configuration so that their Management Central servers can participate in the single sign-on environment.

Situation

You are a system administrator for a medium-sized parts manufacturer. You have been using the System i Navigator Management Central server to manage a central server and three endpoint servers for the last three years. Your responsibilities include applying PTFs, creating new users on the network and other administrative duties. You have always liked having the ability to send and install PTFs to multiple systems from your central server; this saves you time. Your company has just upgraded to i5/OS V5R4, or later, and your company's security administrator has implemented a new security policy for your company, which requires user passwords to be different on each system in the network. Previously, the Management Central servers required that user profiles and passwords be identical across the network. You have learned that if you enable the Management Central servers for single sign-on in i5/OS V5R4, or later, you no longer need to have matching user profiles and passwords on each endpoint system to use the Management Central server's functions. This limits the need to manage passwords on your i5/OS systems.

You completed the enable single sign-on for i5/OS scenario for one of your new systems, and then you completed the propagate network authentication service and EIM across multiple systems scenario. Now you want to want to configure all of your Management Central servers to participate in this single sign-on environment.

This scenario has the following advantages:

- Reduces administration of user profiles on central and endpoint systems.
- Reduces administrative password management for users on central and endpoint systems.
- Complies with the new company security policy, mandating that user passwords be unique on each system.

Objectives

You are one of three system administrators that work for your company. You and the other two administrators, Amanda and George, want to create a small single sign-on environment that decreases your administrative expense and simplifies your access to centrally managed applications and network assets.

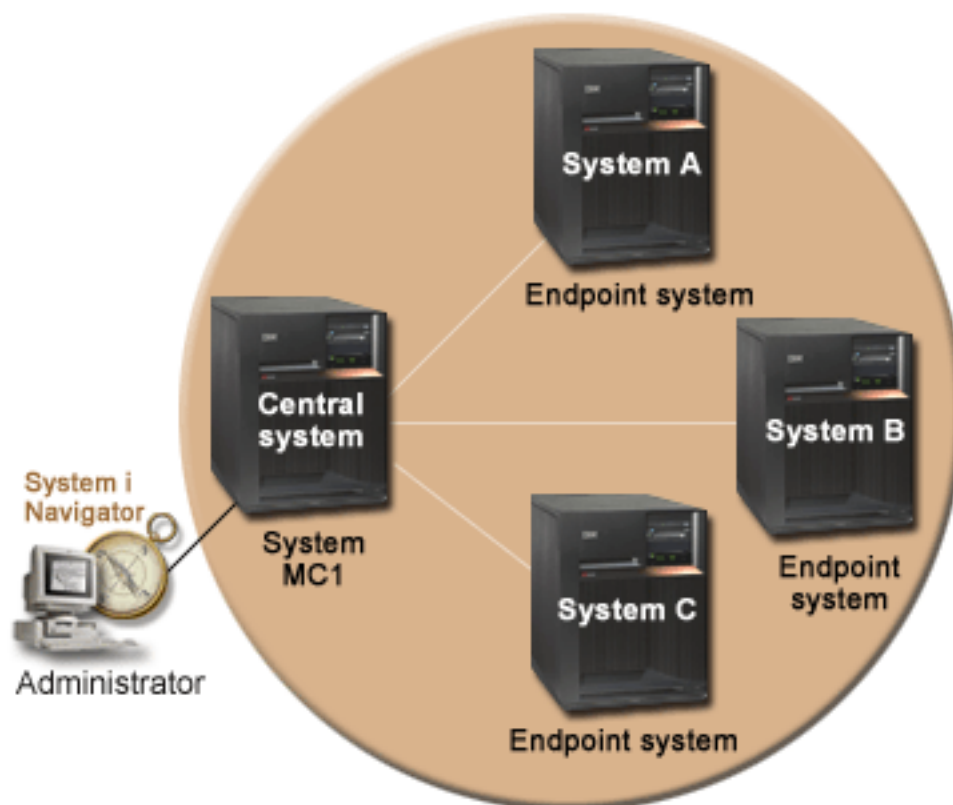
The objectives of this scenario are as follows:

- To comply with your company's new security policy by enabling the i5/OS Management Central servers for single sign-on.
- To simplify password management by eliminating the need to have the same user profile and password on every endpoint system that is managed by the Management Central server.
- To allow all endpoint systems managed by the Management Central server to participate in a single sign-on environment.

- To ensure asset security within the enterprise by mapping users to EIM identifiers instead of using policy associations.

Details

The following figure illustrates the network environment for this scenario:



The figure illustrates the following points relevant to this scenario.

- **Central system System MC1 (also specified as the model system):**
 - Runs i5/OS Version 5 Release 4 (V5R4), or later, with the following options and licensed programs installed:
 - i5/OS Host Servers (5761-SS1 Option 12)
 - IBM System i Access for Windows (5761-XE1)

Note: 5722 is the product code for i5/OS options and products, prior to V6R1.

- Stores, schedules, and runs synchronize settings tasks for each of the endpoint systems.
- Configured for network authentication service and EIM.
- Selected model system from which the network authentication service and EIM configurations are propagated to the target systems.

Note: The model system should be configured similarly to the system identified as System A in the Scenario: Create a single sign-on test environment. Refer to this scenario to ensure that all of the single sign-on configuration tasks on the model system are completed and verified.

- **Endpoint systems System A, System B, and System C:**
 - Runs i5/OS Version 5 Release 4 (V5R4), or later, with the following options and licensed programs installed:

- i5/OS Host Servers (5761-SS1 Option 12)
- System i Access for Windows (5761-XE1)
- Configured for network authentication service and EIM.
- **Administrator's PC:**
 - Runs System i Access for Windows (5761-XE1) V5R4, or later.
 - Runs System i Navigator with the following subcomponents:
 - Network
 - Security

Note: Only required for PC used to administer network authentication service.

Prerequisites and assumptions

Successful implementation of this scenario requires that the following assumptions and prerequisites are met:

- **Central system System MC1 (also specified as the model system):**

Note: This scenario assumes that the central system is properly configured for single sign-on. Refer to the Scenario: Create a single sign-on test environment to ensure that all of the single sign-on configuration tasks on the central system are completed and verified.

- All system requirements, including software and operating system installation, have been verified. To verify that these licensed programs have been installed, complete the following:
 - In System i Navigator, expand **your system** → **Configuration and Service** → **Software** → **Installed Products**.
 - Ensure that all the necessary licensed programs are installed.
- All necessary hardware planning and setup is complete.
- TCP/IP and basic system security are configured and tested.
- Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these servers.

Note: When you propagate network configuration service configuration among servers, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your Local Area Network (LAN). See Scenario: Secure all connections to your Management Central server with SSL for details.

- **Endpoint systems System A, System B, and System C:**

- All system requirements, including software and operating system installation, have been verified. To verify that these licensed programs have been installed, complete the following:
 - In System i Navigator, expand **your system** → **Configuration and Service** → **Software** → **Installed Products**.
 - Ensure that all the necessary licensed programs are installed.
- All necessary hardware planning and setup is complete.
- TCP/IP and basic system security are configured and tested.
- Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these servers.

Note: When you propagate network configuration service configuration among servers, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your Local Area Network (LAN). See Scenario: Secure all connections to your Management Central server with SSL for details.

- You have already configured network authentication service and EIM on your central system and endpoint systems. See Scenario: Enable single sign-on for i5/OS and Scenario: Propagate network authentication service and EIM across multiple systems for details.
- You are using Microsoft Windows Active Directory as a Kerberos server.
- You have already added i5/OS service principal names to the Kerberos server (you perform this task in Scenario: Enable single sign-on for i5/OS).
- You have already tested the network authentication services configuration (you perform this task in Scenario: Propagate network authentication service and EIM across multiple systems).

Configuration steps

To enable single sign-on for users of the Management Central servers, complete the following tasks:

Verifying that the domain appears in Domain Management

Before you can create EIM identifiers, you need to ensure that you have added the EIM domain that you are working with to **Domain Management**.

About this task

If you have already added the EIM domain to **Domain Management**, you can skip the steps required to add the EIM domain to **Domain Management** and continue with the steps required to create a new EIM identifier.

Add the EIM domain to Domain Management:

1. Using the System i Navigator on the PC, expand the central system, **System MC1**, under **My Connections**, and select **Network** → **Enterprise Identity Mapping** → **Domain Management**.
2. Right click **Domain Management** and select **Add Domain**.
3. On the **Add Domain** page, ensure that the **Domain controller** field has the fully qualified name of the domain controller for the domain that you want to add. For this example, the domain controller name is System MC1.myco.com and the EIM domain you want to add is MyCoEimDomain.
4. Click **Ok**.
5. Under **Domain Management**, expand MyCoEimDomain. The **Connect to EIM Domain Controller** is displayed.

Note: Connect to the EIM domain controller before attempting to manage the domain.

6. On the **Connect to EIM Domain Controller** page, enter the distinguished name and password that you created during the configuration of the EIM domain controller and click **OK**. For example, if you completed the enable single sign-on for i5/OS scenario, you would enter the distinguished name, cn=adminstrator, and password, mycopwd.

Creating EIM identifiers

As part of setting up your single sign-on environment, you need to create an EIM identifier to represent a person.

About this task

You need to perform this task for every user that you want to be able to access Management Central server functions. Perform the following steps to create a new EIM identifier:

1. Right click **Identifiers** under MyCoEimDomain and select **New Identifier**.
2. On the **New EIM Identifier** page, specify a name for the new identifier in the **Identifier** field and click **OK**. For this example, you are creating an EIM identifier for one of your peer system administrators, Amanda Jones. The name that you specify in the **Identifier** field is Amanda Jones.

What to do next

Repeat steps 1 through 3 for each person that requires an EIM identifier.

Creating identifier associations

You need to create a source association and a target association between each EIM identifier and the user profiles on each endpoint system and also on the central system, **System MC1**.

About this task

You need to perform this step for each user that you want to be able to access resources through the central system. Although you could use policy associations, you choose not to, thereby avoiding the risk of unintentionally granting asset authority to users inappropriately. After you complete this step, each user has one EIM identifier that is associated with each user's profile on the endpoint systems. These associations allow the user to participate in your single sign-on environment. Perform the following steps to create the associations:

1. Create the **source** association:
 - a. Using System i Navigator on the PC, select the central system, **System MC1**, and expand **Network** → **Enterprise Identity Mapping** → **Domain Management**.
 - b. Expand **MyCoEimDomain** and select **Identifiers**. A list of identifiers is displayed in the right pane.
 - c. Right-click **Amanda Jones** and select **Properties**.
 - d. On the **Associations** tab, click **Add**.
 - e. On the **Add Association** page, click **Browse** next to the **Registry** field, and select the registry definition for the endpoint system registry that contains the user profile that you want to associate with the **Amanda Jones** identifier. For this example, you want to create an association between the EIM identifier, **Amanda Jones**, and the user profile **AMJONES** on endpoint system **System A**.
 - f. In the **User** field, enter the user profile **AMJONES**.
 - g. In the **Association type** field, select **Source** and click **OK**. The association is added to the list of associations on the **Associations** tab.
2. Create the **target** association:
 - a. On the **Associations** tab of the **EIM Identifiers** page, click **Add**.
 - b. On the **Add Association** page, click **Browse** and select the registry name for **System A**.
 - c. In the **User** field, enter the user profile **AMJONES**.

What to do next

Repeat these steps for each endpoint system and each EIM identifier that you want to create associations for. When you are finished, click **OK** on the **EIM Identifiers Properties** dialog box.

Configuring the Management Central servers to use network authentication service

You need to configure the central system and all endpoint systems to use network authentication service (Kerberos).

About this task

Complete the Scenario: Use Kerberos authentication between endpoint systems to configure the central system and all endpoint systems to use Kerberos.

After you have completed this scenario, you need to continue with the next step of this scenario to configure the central system and all endpoint systems to use EIM.

Configuring the Management Central servers to use EIM

To configure the management central server you must use System i Navigator.

About this task

Perform the following steps to configure the central system and all endpoint systems to use EIM:

1. Set the central system to use EIM:
 - a. Using System i Navigator on the PC, right-click the central system, **System MC1**, and select **Properties**.
 - b. Click the **Security** tab and verify that **Use Kerberos authentication** is selected.
 - c. Select the **Use if identity exists (otherwise use profile)** option for identity mapping.

Note: You can select the **Require identity mapping** option. However if you do, System i Navigator functions that are directed to endpoint systems that use the Management Central servers will fail for EIM identifiers for which you have not created EIM associations.
 - d. Click **OK** to set this value on **System MC1**. A message appears, which reminds you of the prerequisites for configuring the Management Central servers to use network authentication service and EIM.
 - e. Click **OK** to indicate that you understand the prerequisites.
2. Create a system group:
 - a. In System i Navigator, expand **System MC1**.
 - b. Right-click **System Groups** and select **New System Group**.
 - c. On the **General** page, specify the system group in the **Name** field. Create a description for this system group. For this example, you specify a system group with a name of **group1** and describe it as the group of endpoint systems managed by **System MC1**.
 - d. From the **Available System** list, select the central system, **System MC1**, and all endpoint systems, **System A**, **System B**, and **System C**, and click **Add**. This will add these systems to the **Selected systems** list.
 - e. Click **OK**.
 - f. Expand **System Groups** to verify that the system group, **group1**, has been added.
3. Collect inventory for the system group:
 - a. In System i Navigator, expand **System MC1** and select **System Group**.
 - b. Right-click **group1** and select **Inventory** → **Collect**.
 - c. On the **Collect Inventory** page for **group1**, select **System values** and click **OK**.

Note: By default, a dialog box is displayed that indicates the **Collect Inventory** task has started. However, if you have changed the default setting, this dialog box is not displayed.
 - d. Click **OK**.
 - e. On the **Collect Inventory Status** page, read all the status values that display and fix any problems that you might encounter. For details on specific status values related to inventory collection that appear on this page, select **Help** → **Task Status Help**.
 - f. From the **Task Status** help page, select **Inventory**. This page displays all the status values that you might encounter with detailed descriptions and recovery information.
 - g. After the inventory collection completes successfully, close the status window.
4. Compare and update EIM settings:
 - a. In System i Navigator, expand the central system **System MC1** and select **System Group**.
 - b. Right-click the system group **group1** and select **System Values** → **Compare and Update**.
 - c. Complete the fields on the **Compare and Update** system group dialog box:
 - 1) Select the central system, **System MC1**, for the **Model system** field.

- 2) Select **Management Central** for the **Category** field.
- 3) From the list of items to compare, select **Use EIM for user mapping** and **Require identity mapping**.
- d. Verify that your target systems are your system group, and click **OK** to start the update. This will update each of the target systems within the system group with the EIM settings that you selected on the model system.

Note: By default, a dialog box is displayed that indicates, the **Compare and Update** task has started. However, if you have changed the default setting, this dialog box is not displayed.
- e. Click **OK**.
- f. On the **Update Values Status** dialog box, verify that the update completes on each system and close the dialog box.
5. Restart the Management Central server on the central system and all endpoint systems:
 - a. In System i Navigator, expand **My Connections**.
 - b. Expand the System i Navigator system that you want to restart.
 - c. Expand **Network** → **Servers** and select **TCP/IP**.
 - d. Right-click **Management Central** and select **Stop**. The server view collapses, and a message is displayed, explaining that you are no longer connected to the server.
 - e. After the Management Central server has stopped, click **Start** to restart it.
6. Repeat these steps on each endpoint system (System A, System B, and System C).

Scenario: Enabling single sign-on for ISV applications

View this information to review scenarios that illustrate typical single sign-on implementation situations to help you plan your own certificate implementation as part of your server security policy.

Situation

You are the lead application developer for an independent software vendor (ISV), and are responsible for overseeing the applications that your company develops and delivers to System i Navigator customers. You know that System i Navigator provides your customers with the capability of creating and participating in a single sign-on environment. You want your applications to leverage these single sign-on capabilities because you feel it will help sell your product. You decide to market an application called **Calendar** to System i Navigator customers that use network authentication service and Enterprise Identity Mapping (EIM) to create their single sign-on environment. The **Calendar** application allows users to view and manage their workday schedule. Enabling the **Calendar** application for single sign-on requires you to include server specific code within your application which enables it to participate within a single sign-on environment. You have previous experience creating applications that call EIM APIs, but this will be your first time working with an application that also calls network authentication service APIs.

Note: It is also possible to develop applications for a single sign-on environment that use a different authentication method. For example, you can insert the necessary code for authenticating with digital certificates, or for binding the directory server, instead of inserting the necessary code for authenticating with network authentication service.

Objectives

You want to be able to market your **Calendar** application to System i Navigator customers who are interested in applications that are capable of participating in a single sign-on environment. You want to enable the server side of the **Calendar** application to participate in a single sign-on environment. You have the following objectives, as you complete this scenario:

- You want to change the server specific part of an existing **Calendar** application or develop a new **Calendar** application which participates in a single sign-on environment that uses EIM and network authentication service.
- You want to create a single sign-on environment in which you can test your application.
- You want to test your **Calendar** application and ensure that it successfully participates in a single sign-on environment.

Prerequisites and assumptions

Implementation of this scenario depends on the following assumptions and prerequisite conditions:

- You want your **Calendar** application to participate in a single sign-on environment that is configured to use Kerberos and EIM.
- You already have experience creating applications for the System i Navigator platform.
- You are using System i Navigator with the following options and licensed programs installed:
 - System i Navigator Host Servers (5761-SS1 Option 12)
 - IBM System i Access for Windows (5761-XE1)

Note: 5722 is the product code for i5/OS options and products, prior to V6R1.

- You have configured your i5/OS system to participate in a Kerberos realm.
- You write applications in one of the following languages:
 - You use an ILE programming language, such as C, to write your applications and you are familiar with the GSS API set.
 - You use Java to write your applications and you are familiar with the JGSS API set.

Note: You might also require the Java toolbox, depending on which set of JGSS APIs you use.

- You have already completed the client-specific portion of your application, enabling it to use Kerberos authentication.

Configuration steps

Related information

Programming

Generic Security Service API


IBM® Java Generic Security Service (JGSS)

Completing the planning prerequisite worksheet

Complete the following planning worksheet to ensure that you have met the prerequisites for a successful single sign-on environment in which you can test your application.

About this task

Prerequisite worksheet	Answers
Is your system running i5/OS V5R4, or later?	Yes
Is System i Access for Windows installed on the PC from which administration is performed?	Yes
Is the Security subcomponent of System i Navigator installed on the PC from which administration is performed?	Yes
Is the Network subcomponent of System i Navigator installed on the PC from which administration is performed?	Yes
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes

Prerequisite worksheet	Answers
Do you have one of the following servers acting as the Kerberos server? If yes, specify which one. 1. Microsoft Windows 2000 Server Note: Microsoft Windows 2000 Server uses Kerberos authentication as its default security mechanism. 2. Windows ^(R) Server 2003 3. i5/OS PASE (V5R3 or later) 4. AIX server 5. z/OS	Yes
For Windows 2000 Server, do you have Windows Support Tools (which provides the ktpass tool) installed?	Yes
Are all of the PCs that you want to be able to participate in a single sign-on environment in your network configured in an i5/OS domain?	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Have you installed the latest System i Access for Windows service packs? For the latest service pack see, System i Access for Windows web page  .	Yes
Is the System i model time within 5 minutes of the system time on the Kerberos server? If not see, Synchronize system times.	Yes

Writing a new application or change an existing application

You are ready to begin including the server specific code that enables your **Calendar** application to participate in an single sign-on environment.

About this task

Using your previous programming experience with EIM APIs, you create a program flow similar to this one:

- Application Initialization
 - EIM Get Handle
 - EIM Connect
- Processing Loop
 - Wait for user request
 - Authenticate user using Kerberos
 - Call EIM to map from network authentication service user to Local user
 - Swap to local user
 - Perform Task
 - Swap back to original user
 - Go to "Wait for user request"

Note: This scenario assumes that you have already created or changed the client specific code to enable your application for an i5/OS single sign-on environment, and therefore only provides the steps required to complete the server specific part of your program.

- Application Termination
 - Destroy EIM Handle

Example

See the ISV code examples for example pseudocode and snippets that you can use to help complete the server specific part of your program. When you have added the necessary client and server specific code to your **Calendar** application, you can create a single sign-on test environment to test it.

Creating a single sign-on test environment

To create a test environment for single sign-on you must complete a different scenario before you can complete this scenario.

About this task

Complete the Scenario: Create a single sign-on test environment. This scenario demonstrates how to configure network authentication service and EIM to create a basic single sign-on test environment. This scenario guides you through the following steps to configure and work with a simple single sign-on environment:

1. Complete necessary planning work sheets.
2. Create a basic single sign-on configuration for the iSeries system.
3. Add the iSeries service principal to the Kerberos server.
4. Create a home directory for a test user, John Day, on the iSeries system.
5. Test the network authentication service configuration on the iSeries system.
6. Create an EIM identifier for John Day.
7. Create a source association and a target association for the new EIM identifier.
8. Test the EIM identity mappings.
9. Configure System i Access for Windows applications to use Kerberos.
10. Verify network authentication service and EIM configuration.

Results

After you have created the single sign-on test environment the scenario describes, you can test your **Calendar** application to ensure that it works correctly.

Testing your application

You have completed the development of both client and server specific updates to your **Calendar** application, enabling it for an i5/OS single sign-on environment. You are now ready to test it.

About this task

Follow these steps to verify that you have created an application that participates successfully in a single signon environment:

1. Log the test user jday (this user was created in the create a single sign-on test environment scenario) into the Windows 2000 domain by signing him into a PC.
2. Have the test user open your **Calendar** application on the PC. If the calendar opens, the application has used EIM to map the jday Kerberos principal to the JOHND i5/OS user profile because of the associations defined for EIM identifier, John Day. The **Calendar** application session for the System i model is now connected as JOHND, and you have successfully enabled your ISV application for an i5/OS single sign-on environment.

Related concepts

“Scenario: Creating a single sign-on test environment” on page 10

In this scenario, you want to configure network authentication service and EIM to create a basic single sign-on test environment. Use this scenario to gain a basic understanding of what configuring a single sign-on environment involves on a small scale before implementing single sign-on across an entire enterprise.

Example: ISV code

This information displays sample code for writing a kerberos server along with calling EIM apis to map from a kerberos principal to an i5/OS user profile.

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

All sample code is provided by IBM for illustrative purposes only. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

All programs contained herein are provided to you "AS IS" without any warranties of any kind. The implied warranties of non-infringement, merchantability and fitness for a particular purpose are expressly disclaimed.

Note: By using the code examples, you agree to the terms of the "Code license and disclaimer information" on page 86.

```
/** START OF SPECIFICATIONS *****/
/* */
/* MODULE NAME: Kerberos/EIM server sample */
/* */
/* DESCRIPTION: Below is sample code for writing a Kerberos server */
/* along with calling EIM APIs to map from a Kerberos */
/* principal to an i5/OS user profile. */
/* */
/* NOTE: Error checking has been removed. */
/*****/

/* #include files removed here */

//-----
// EIM assumptions:
// On the System i model where this program is running the EIM configuration
// information has been set. The information used by this program
// is:
// - ldapURL
// - local registry
// EIM ldap lookup connection
// - The ldap connection information needed for doing the mapping
// lookups in this program can be stored in a validation list
// or other user secure space. Here we will just hard code
// pretend values.
// - This connection will only be used for a lookup operation so
// the ldap user only needs EIM mapping lookup authority.
// All EIM data (Identifiers and associations) has been added.
//-----

#define LDAP_BINDDN "cn=mydummy"
#define LDAP_BINDPW "special"

//-----
//
// Function: l_eimError
// Purpose: EIM error has occurred. This function will print out the
// EIM error message.
//
//-----
void l_eimError(char * function, EimRC * err)
```

```

{
    char * msg = NULL;
    printf("EIM ERROR for function = %s.\n", function);
    msg = eimErr2String(err);
    printf("    %s\n",msg);
    free(msg);
}

//-----
//
// Function:  l_eimConnect
// Purpose:   Get an EIM handle and connect to the ldap server.
//
//-----
int l_eimConnect(EimHandle * handle)
{
    int          rc = 0;
    char eimerr[150];
    EimRC *err = (EimRC *)&eimerr
    EimConnectInfo  con;

    /* This needs to be at least 48. */
    err->memoryProvidedByCaller = 150;

    //-----
    // Create handle.  We will pass NULL for the URL indicating that we
    // will use the information that was configured for the system.
    //-----
    eimCreateHandle(handle,
                    NULL,
                    err);

    //-----
    // Connect
    //-----
    // The ldap user id and password might be stored in a validation
    // list or other user secure space.  Here we will just hard code
    // pretend values.
    // You can also choose to use Kerberos authentication when
    // connecting to ldap.  You will first need to verify your ldap
    // server is set up to accept kerberos authentication.
    //-----
    // This connection will only be used for a lookup operation so the
    // ldap user only needs EIM mapping lookup authority.
    //-----
    con.type = EIM_SIMPLE;
    con.creds.simpleCreds.protect = EIM_PROTECT_NO;
    con.creds.simpleCreds.bindDn = LDAP_BINDDN;
    con.creds.simpleCreds.bindPw = LDAP_BINDPW;
    con.ssl = NULL;
    eimConnect(handle,
               con,
               err);
    return 0;
}

//-----
//-----
//
// Function:  getOS400User
// Purpose:   Get OS400 user associated with the kerberos user and exchange
//           to the user.
//
//-----
int getOS400User(EimHandle * handle,

```

```

        char          * OS400User,
        gss_buffer_desc * client_name)
{
    char * principal;
    char * realm;
    char * atsign;

    //-----
    //
    //  Get principal and realm from the kerberos client_name.
    //
    //-----
    //  client_name.value contains string of principal@realm.  Get
    //  pointer to each piece.
    //-----
    principal = client_name->value;
    atsign = strchr(principal, '@');
    *atsign = 0x00;          // NULL end the principal
    realm = atsign + 1;     // ASdvance pointer to the realm

    //-----
    //
    //  Call EIM to get the target user associated with the kerberos
    //  source user.  This sample application assumes that the
    //  kerberos realm name is also the name of the EIM registry
    //  defining this realm.
    //
    //-----
    listPtr = (EimList *)listBuff;
    for (i = 0; i < 2; i++)
    {
        if (0 != (rc =
            eimGetTargetFromSource(handle,
                realm,
                principal,
                NULL,          // use configured
                             // local
                             // registry.
                NULL,
                listSize,
                listPtr,
                err)))
        {
            l_eimError("eimGetTargetFromSource", err);
            return -1;
        }

        if (listPtr->bytesAvailable == listPtr->bytesReturned)
            break;
        else
        {
            listSize = listPtr->bytesAvailable;
            freeStorage = malloc(listSize);
            listPtr = (EimList *)freeStorage;
        }
    }

    // Check the number of entries found, if 0 no mapping exists
    // otherwise extract user profile from buffer and cleanup
    // storage

    return 0;
}

/*****

```

```

/* Function Name: get_kerberos_credentials_for_server */
/*
/* Descriptive Name: Basically this function finds the keytab entry */
/* for this server. It will use this to validate */
/* the tokens received. */
/*
/* Input: char * service_name - the service name. */
/* gss_buffer_t msg_buf - the input message */
/* Output: gss_cred_id_t *server_creds - The output credential */
/*
/* Exit Normal: return value == 0 */
/* Exit Error: -1, error was encountered, */
/*****
int get_kerberos_credentials_for_server (
    char * service_name, /* name of service principal */
    gss_cred_id_t * server_creds) /* credential acquired */
{
    gss_buffer_desc name_buf; /* buffer for import name */
    gss_name_t server_name; /* gss service name */
    OM_uint32 maj_stat, /* GSS status code */
              min_stat; /* Mechanism kerberos status */

    /* Convert service name to GSS internal format */
    name_buf.value = service_name;
    name_buf.length = strlen((char *)name_buf.value) + 1;
    maj_stat = gss_import_name(
        &min_stat, /* kerberos status */
        &name_buf, /* name to convert */
        (gss_OID) gss_nt_service_name, /* name type */
        &server_name); /* GSS internal name */

    /* Acquire credentials for the service from keytab */
    maj_stat = gss_acquire_cred(
        &min_stat, /* kerberos status */
        server_name, /* gss internal name */
        GSS_C_INDEFINITE, /* max credential life */
        GSS_C_NULL_OID_SET, /* use default mechanism */
        GSS_C_ACCEPT, /* credential usage */
        server_creds, /* output cred handle */
        NULL, /* ignore actual mech */
        NULL); /* ignore time remaining */

    /* Release the gss internal format name */
    gss_release_name(&min_stat, &server_name);

    return 0;
}

/*****
/* Function Name: do_kerberos_authentication() */
/* Purpose: Any valid client request is accepted. If a context */
/* is established, its handle is returned in context and */
/* the client name is returned. */
/*
/* Exit Normal: return value == 0 */
/* Exit Error: -1, error was encountered, */
/*****
int do_kerberos_authentication (
    int s, /* socket connection */
    gss_cred_id_t server_creds, /* credentials for the server */
    gss_ctx_id_t * context, /* GSS context */
    gss_buffer_t client_name) /* kerberos principal */
{
    gss_buffer_desc send_tok, /* token to send to client */
                  rcv_tok; /* token received from client */
    gss_name_t client; /* client principal */

```

```

OM_uint32 maj_stat,      /* GSS status code          */
          min_stat;     /* Mechanism (kerberos) status */
msgDesc_t msgSend,     /* Message buffer to send     */
          msgRecv;     /* Message buffer received    */
gss_OID doid;

*context = GSS_C_NO_CONTEXT; /* initialize the context */

do {
    /* Receive the message from the client */
    memset(&msgRecv, 0x00, sizeof(msgRecv));
    if (0 != recvAmessage(s, &msgRecv))
        return -1;
    rcv_tok.length = msgRecv.dataLength;
    rcv_tok.value = msgRecv.buffer;

    /* Accept the security context */
    maj_stat = gss_accept_sec_context(
        &min_stat, /* kerberos status */
        context, /* context handle */
        server_creds, /* acquired server creds */
        &rcv_tok, /* token received */
        GSS_C_NO_CHANNEL_BINDINGS, /* no CB */
        &client, /* client requestor */
        NULL, /* ignore mech type */
        &send_tok, /* token to be sent */
        NULL, /* ignore ctx flags */
        NULL, /* ignore time_rec */
        NULL); /* ignore delegated cred */

    /* release the received token */
    gss_release_buffer(&min_stat, &rcv_tok);

    /* Check to see if there is a token client wants mutual
       authentication. */
    if (send_tok.length != 0)
    {
        /* Send the token message to the other side */
        /* release the send token buffer */
    }
} while (maj_stat == GSS_S_CONTINUE_NEEDED);

/* client name is returned - extract client from ticket. This
   client name will be used to map to the OS400 user profile */
maj_stat = gss_display_name(&min_stat, client, client_name, &doid);

maj_stat = gss_release_name(&min_stat, &client);

return 0;
}

/*****
/*
/* Function Name: getTestPort()
/*
/* Descriptive Name: get the port on which the server is listening
/*
/* Input: char * service - the service name. If null, looks
/* for kerb-test-server.
/*
/* Output: none
/*
/* Exit Normal: return value == port number
/*
/* Exit Error: N/A
/*
*****/

```

```

/*****
CLINKAGE int getTestPort(char *name)
{
    struct servent service;
    struct servent_data servdata;
    char defaultName[] = "krb-test-server", *servName;
    char tcp[] = "tcp";
    int retPort, rc;
    memset(&servdata, 0x00, sizeof(servdata));
    memset(&service, 0x00, sizeof(service));
    if (name == NULL)
        servName = defaultName;
    else
        servName = name;
    rc = getservbyname_r(servName, tcp, &service,
                        &servdata);
    if (rc != 0)
        retPort = DEFAULT_KERB_SERVER_PORT;
    else
        retPort = service.s_port;

    return ntohs(retPort);
}
/* end getPort */

/*****
/*
/* Function Name: getListeningSocket()
/*
/* Descriptive Name: get a listening socket created and return it.
/*
/* Input:    none.
/*
/* Output:   listening socket created.
/*
/* Exit Normal: return value == listening socket.
/*
/* Exit Error:  -1, error was encountered.
/*
/* NOTE: Error checking removed
/*
/*****
CLINKAGE int getListeningSocket(void)
{
    int          rc, sd, option;
    struct sockaddr_in  sin;

    sd = socket(AF_INET, SOCK_STREAM, 0)

    option = 1;

    setsockopt(sd, SOL_SOCKET, SO_REUSEADDR,
              (char *)&option, sizeof(option));

    memset(&sin, 0x00, sizeof(sin));
    sin.sin_family = AF_INET;
    sin.sin_port = htons(getTestPort(NULL));

    bind(sd, (struct sockaddr *)&sin, sizeof(sin));

    listen(sd, SOMAXCONN);

    return sd;
}
/* end getListeningSocket() */

/*****

```

```

/*                                                                    */
/* Function Name: getServerSocket()                                    */
/*                                                                    */
/* Descriptive Name: get a server socket that is connected to a      */
/*                   client. This routine blocks waiting for         */
/*                   the client.                                     */
/*                                                                    */
/* Input:    int lsd - listening socket.                             */
/*                                                                    */
/* Output:   server socket created.                                  */
/*                                                                    */
/* Exit Normal: return value == server socket.                       */
/*                                                                    */
/* Exit Error:  -1, error was encountered.                           */
/*                                                                    */
/* NOTE: Error checking removed                                     */
/*                                                                    */
/*                                                                    */
/*****
CLINKAGE int getServerSocket(int lsd)
{
    return accept(lsd, NULL, 0);
}
/* end getServerSocket() */

/*****
/*                                                                    */
/* Function Name: main                                              */
/*                                                                    */
/* Descriptive Name: Driver for the server program which performs   */
/*                   kerberos authentication and EIM mapping.       */
/*                                                                    */
/* Input:    char* service_name - name of service requested        */
/*                                                                    */
/* Exit Normal:  0 = success                                         */
/*                                                                    */
/* Exit Error:  -1, error was encountered.                           */
/*                                                                    */
/* NOTE: Error checking removed                                     */
/*                                                                    */
/*                                                                    */
/*****
int main(int argc, char **argv)
{
    int ssd,                /* server socket */
        lsd;               /* listening socket */
    char *service_name;     /* name of service (input) */
    gss_cred_id_t server_creds; /* server credentials to acquire */
    gss_ctx_id_t context;    /* GSS context */
    OM_uint32 maj_stat,     /* GSS status code */
              min_stat;    /* Mechanism (kerberos) status */
    gss_buffer_desc client_name; /* Client principal establishing
                                context. */

    char OS400User[10];
    char save_handle[SY_PH_MAX_PRFHDL_LEN]; // *CURRENT profile handle
    char client_handle[SY_PH_MAX_PRFHDL_LEN]; // Swap to profile handle
    EimHandle eimHandle;

    Qus_EC_t errorcode;
    memset(errorcode, 0x00, 256);
    errorcode->Bytes_Provided = 256;

    service_name = argv[1];

    /*-----
    // Kerberos setup
    // Acquire credentials for the service
    //-----*/

```



```

get_kerberos_credentials_for_server(service_name, &server_creds);

/*-----
// get a listening socket
//-----*/
lzd = getListeningSocket();

/*-----
// EIM setup
// Connect to eim
// -----*/
l_eimConnect(&eimHandle);

/*-----
// Save a copy of the current user so we can swap back to it
// after each request
// -----*/
QsyGetProfileHandleNoPwd(save_handle,
                        "*CURRENT ",
                        "*NOPWD ",
                        &errorcode);

/*-----
// Loop waiting for requests on the socket
//-----*/
do { /* loop until the application or the system is ended */
    /* Save the profile handle of the current user */
    /* Accept a TCP connection */
    ssd = getServerSocket(lzd);

    /* -----
    // Establish context with the client and get the client name.
    //-----
    // The client name contains the kerberos principal and realm. In
    // EIM these equate to the source user and source registry.
    //----- */
    do_kerberos_authentication(ssd,
                              server_creds,
                              &context,
                              &client_name);

/*-----
// Perform eim mapping lookup operation to get the associated
// OS400 user.
//----- */
getOS400User(&eimHandle,
            OS400User,
            &client_name);

/* -----
// Swap to the user returned from EIM lookup
// ----- */
QsyGetProfileHandleNoPwd(client_handle,
                        client_name,
                        "*NOPWDCHK ",
                        &errorcode);
QsySetToProfileHandle(client_handle, &errorcode);

/* -----
// do the real work of the application here as the application is
// now running under an appropriate user profile
// ----- */
// Call or code application specific behavior here.

/* -----
// reset the process to run under the original user profile

```

```

// ----- */
    QsySetToProfileHandle(save_handle, &errorcode);

} while (1)

eimDestroy_handle(&eimHandle);

gss_delete_sec_context(&min_stat, &context, NULL);
close(ssd);
close(lsd);
gss_release_cred(&min_stat, &server_creds);
return 0;
}

```

Planning for single sign-on

The single sign-on planning process identifies the software and hardware prerequisites required to implement single sign-on in your enterprise.

Before you begin

You must plan carefully to create a single sign-on environment that meets the needs of your enterprise. There are several decisions that you must make while planning out an i5/OS single sign-on environment. One such decision is if you want to create policy associations. The security concerns of your enterprise factor heavily on this type of decision.

About this task

Here are some resources that you can use to complete the planning stage for your single sign-on environment:

What to do next

After you have adequately planned for your single sign-on environment, you can configure your single sign-on environment.

Related tasks

“Configuring single sign-on” on page 80

To configure a single sign-on environment you must use a compatible authentication method as your authentication method and Enterprise Identity Mapping (EIM) to create and manage your user profiles and identity mappings.

Related information

Planning Enterprise Identity Mapping for i5/OS

Requirements for configuring a single sign-on environment

Your system must meet the following hardware and software prerequisites before implementing a single sign-on environment.

Requirements for i5/OS V5R4, or later

Note: Single sign-on is also available in OS/400 V5R2 and i5/OS V5R3. However, the detailed configuration information in this topic is based on the new single sign-on function that is only available in i5/OS V5R4, or later, such as policy associations.

To create a successful single sign-on environment, ensure that all these requirements are met:

- i5/OS V5R4, or later, is installed.
- Latest i5/OS program temporary fixes (PTFs) are applied.

- System i Access for Windows V5R4, or later, is installed.
- Latest System i Access for Windows service pack is installed.
For information about acquiring the latest service pack, see System i Access.
- i5/OS Host Servers (5761-SS1 Option 12) is installed.
- Qshell Interpreter (5761-SS1 Option 30) is installed.
- TCP/IP and basic system security are configured.

Note: 5722 is the product code for i5/OS options and products, prior to V6R1. If you intend to use the Synchronize Functions wizard in System i Navigator to propagate an existing single sign-on configuration across multiple systems, you need to configure the systems to use Secure Sockets Layer (SSL) to protect the transmission of sensitive configuration information, such as passwords.

Client PC requirements

To create a successful single sign-on environment, ensure that all these requirements are met:

- Microsoft Windows 2000, Microsoft Windows XP, or Microsoft Windows Vista Ultimate Business operating system is used.
- System i Access for Windows, V5R4, or later, is installed.
 - Network component of System i Navigator is installed on PC that administers single sign-on.
 - Security component of System i Navigator is installed on PC that administers single sign-on.
- Latest System i Access for Windows service pack is installed.
For information about acquiring the latest service pack, see System i Access.
- TCP/IP is configured.

Microsoft Windows server requirements

To create a successful single sign-on environment, ensure that all these requirements are met:

- Hardware planning and setup are completed.
- Windows 2000 Server, Windows Server 2003, or Microsoft Windows Vista Ultimate Business is used.
- Windows Support Tools (which provides the ktpass tool) is installed.
- TCP/IP is configured.
- Windows 2000 domain is configured.
- Users within the network are added to a Windows 2000 domain through Microsoft Windows Active Directory.

You can use the provided planning work sheets to help you gather information and make decisions for your single sign-on implementation. Each work sheet contains a list of tasks that need to be completed.

Single sign-on planning worksheets

Complete these worksheets to ensure that you have met all of the prerequisites for single sign-on and that you have considered all of the aspects of your particular system and its security requirements.


Before you use these configuration planning worksheets, you need to plan your overall single sign-on implementation. Use these configuration planning worksheets to ensure that you have met all of the prerequisites, and that you have taken into consideration all of the aspects of your particular System i environment.

Single sign-on prerequisite worksheet

This detailed work sheet is provided to help you ensure that you meet all hardware and software prerequisites for implementing single sign-on. To ensure a successful implementation, you must be able

to answer **Yes** to all prerequisite items in the work sheet and you should gather all the information necessary to complete the work sheets before you perform any configuration tasks.

Table 11. Single sign-on prerequisite work sheet

Prerequisite work sheet	Answers
Is your system running i5/OS V5R4, or later?	
Are the following options and licensed programs installed on your server? <ul style="list-style-type: none"> • i5/OS Host Servers (5761-SS1 Option 12) • Qshell Interpreter (5761-SS1 Option 30) • System i Access for Windows (5761-XE1) Note: 5722 is the product code for i5/OS options and products, prior to V6R1.	
Have you installed an application that is enabled for single sign-on on each of the PCs that will participate in the single sign-on environment? Note: For the scenarios in this information, all of the PCs have System i Access for Windows (5761-XE1) installed.	
Is System i Navigator installed on the administrator's PC? <ul style="list-style-type: none"> • Is the Security subcomponent of System i Navigator installed on the administrator's PC? • Is the Network subcomponent of System i Navigator installed on the administrator's PC? 	
Have you installed the latest System i Access for Windows service pack? For the latest service pack, see System i Access  .	
Do you, the administrator, have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	
Do you have one of the following systems acting as the Kerberos server (also known as the KDC)? If yes, specify which system. <ol style="list-style-type: none"> 1. Windows 2000 Server Note: Microsoft Windows 2000 uses Kerberos authentication as its default security mechanism. 2. Windows^(R) Server 2003 3. i5/OS PASE (V5R3 or later) 4. AIX server 5. z/OS 	
Are all your PCs in your network configured in a Windows 2000 domain?	
Have you applied the latest program temporary fixes (PTFs)?	
Is the System i model time within 5 minutes of the system time on the Kerberos server? If not, see Synchronize system times.	

Single sign-on configuration planning worksheet

This is a configuration planning worksheets, designed to ensure that you have met all of the hardware and software prerequisites for single sign-on. Additionally, this worksheet ensures that you have completed those Enterprise Identity Mapping (EIM) and network authentication service configuration tasks that are required for a successful single sign-on environment.

Note: The single sign-on configuration planning worksheet is designed to assist you with the implementation of a single sign-on environment based on Enterprise Identity Mapping (EIM) and network authentication services. If you intend to use a different authentication mechanism, such as IBM Tivoli Directory Server for i5/OS or digital certificates, you might need to adapt portions of this work sheet to better suit your needs.

Table 12. Single sign-on configuration planning work sheet

Configuration planning work sheet	Answers
Use the following information to complete the EIM Configuration wizard:	
How do you want to configure EIM for your system? <ul style="list-style-type: none"> • Join an existing domain • Create and join a new domain 	
Where do you want to configure your EIM domain?	
Do you want to configure network authentication service?	
The Network Authentication Service wizard launches from the EIM Configuration wizard. Use the following information to complete the Network Authentication Service wizard: Note: The Network Authentication Service wizard can also be launched independently of the EIM Configuration wizard.	
What is the name of the Kerberos default realm to which your system will belong? Note: A Windows 2000 domain is similar to a Kerberos realm. Microsoft Windows Active Directory uses Kerberos authentication as its default security mechanism.	
Are you using Microsoft Active Directory?	
What is the Kerberos server, also known as a key distribution center (KDC), for this Kerberos default realm? What is the port on which the Kerberos server listens?	
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this Kerberos server? What is the port on which the password server listens?	
For which services do you want to create keytab entries? <ul style="list-style-type: none"> • i5/OS Kerberos Authentication • LDAP • IBM HTTP Server for i5/OS • i5/OS NetServer • Network File System (NFS) Server 	
What is the password for your service principal or principals?	
Do you want to create a batch file to automate adding the service principals for System A to the Kerberos registry?	
Do you want to include passwords with the i5/OS service principals in the batch file?	
As you exit the Network Authentication Service wizard, you will return to the EIM Configuration wizard. Use the following information to complete the EIM Configuration wizard:	
Specify user information that the wizard should use when configuring the directory server. This is the connection user. You must specify the port number, administrator distinguished name, and a password for the administrator.	
What is the name of the EIM domain that you want to create?	

Table 12. Single sign-on configuration planning work sheet (continued)

Do you want to specify a parent DN for the EIM domain?	
Which user registries do you want to add to the EIM domain?	
Which EIM user do you want System A to use when performing EIM operations? This is the system user.	
After you complete the EIM Configuration wizard, use the following information to complete the remaining steps required for configuring single sign-on:	
What is the i5/OS user profile name for the user?	
What is the name of the EIM identifier that you want to create?	
What kinds of associations do you want to create?	
What is the name of the user registry that contains the Kerberos principal for which you are creating the source association?	
What is the name of the user registry that contains the i5/OS user profile for which you are creating the target association?	
What information do you need to supply to test EIM identity mapping?	

Related tasks

“Configuring single sign-on”

To configure a single sign-on environment you must use a compatible authentication method as your authentication method and Enterprise Identity Mapping (EIM) to create and manage your user profiles and identity mappings.

Configuring single sign-on

To configure a single sign-on environment you must use a compatible authentication method as your authentication method and Enterprise Identity Mapping (EIM) to create and manage your user profiles and identity mappings.

Before you begin

In the case of i5/OS single sign-on solutions, the authentication method is network authentication service (Kerberos).

Because a single sign-on environment can be complex to configure, you might find it useful to create a test environment before you implement single sign-on across your enterprise. The create a test single sign-on environment scenario demonstrates how to configure such a test environment so that you can learn more about the planning needs of implementing single sign-on as well as gain a better understanding of how a single sign-on environment can work for you.

After you work with a test environment, you can use what you learn to plan how to implement single sign-on on a larger scale in your enterprise. You might find it useful to work through the enable single sign-on for i5/OS scenario to learn about the more advanced configuration options that you can employ when you implement a single sign-on environment.

After you have reviewed these and the other single sign-on scenarios, you can use the single sign-on planning worksheets to create an informed single sign-on implementation plan that fits the needs of your enterprise. With these planning worksheets in hand, you are ready to continue with the configuration process.

Configuring single sign-on involves a number of detailed configuration steps, this information describes the high-level configuration tasks for single sign-on and provides links to the more detailed configuration

information for both EIM and network authentication service where appropriate.

About this task

Perform these tasks to configure a single sign-on environment:

1. Create your Windows 2000 domain
 - a. Configure the KDC on the Active Directory (AD) Server.

Note: You can choose to create and run your KDC on i5/OS PASE rather than create a Windows domain and run the KDC on a windows server.
 - b. Add i5/OS service principals to the Kerberos server.
 - c. Create a home directory for each Kerberos user who will participate in your single sign-on environment.
 - d. Verify TCP/IP domain information.
2. Create an EIM domain by running the both the network authentication service wizard and the EIM configuration wizard on a server. When you have completed these wizards, you have actually accomplished the following tasks:
 - a. Configured i5/OS interfaces to accept Kerberos tickets.
 - b. Configured the Directory server on System i to be the EIM domain controller.
 - c. Created an EIM domain.
 - d. Configured a user identity for i5/OS and i5/OS applications to use when conducting EIM operations.
 - e. Added a registry definition to EIM for the local i5/OS registry and the local Kerberos registry (if Kerberos is configured).
3. For servers running i5/OS V5R3, or later, see the Scenario: Propagate network authentication service and EIM across multiple systems for a detailed demonstration on how to use the Synchronize Functions wizard in System i Navigator to propagate a single sign-on configuration across multiple servers in a mixed i5/OS release environment. Administrators can save time by configuring single sign-on once and propagating that configuration to all of their systems instead of configuring each system individually.
4. Finish your configuration for the network authentication service. Based on your single sign-on implementation plan, create a home directory for users on your servers.
5. Based on your implementation plan, customize your EIM environment by setting up associations for the user identities in your enterprise.
 - a. Configure other servers to participate in the EIM domain.
 - b. Create EIM identifiers and identifier associations as needed.
 - c. Add additional registry definitions as needed.
 - d. Create policy associations as needed.
6. Test your single sign-on configuration.

To verify that you have configured the network authentication service and EIM correctly, sign on to the system with a user ID, and then open System i Navigator. If no i5/OS sign-on prompt displays, EIM successfully mapped the Kerberos principal to an identifier on the domain.

Note: If you find that your test of your single sign-on configuration fails, there might be a problem with your configuration. You can troubleshoot single sign-on and learn how to recognize and fix common problems with your single sign-on configuration.

Related concepts

“Scenario: Creating a single sign-on test environment” on page 10

In this scenario, you want to configure network authentication service and EIM to create a basic single

sign-on test environment. Use this scenario to gain a basic understanding of what configuring a single sign-on environment involves on a small scale before implementing single sign-on across an entire enterprise.

“Scenario: Enabling single sign-on for i5/OS” on page 23

View this scenario to learn how to configure network authentication service and EIM to create a single sign-on environment across multiple systems in an enterprise. This scenario expands on the concepts and tasks presented in the previous scenario which demonstrates how to create a simple single sign-on test environment.

“Single sign-on planning worksheets” on page 77

Complete these worksheets to ensure that you have met all of the prerequisites for single sign-on and that you have considered all of the aspects of your particular system and its security requirements.

Related tasks

“Planning for single sign-on” on page 76

The single sign-on planning process identifies the software and hardware prerequisites required to implement single sign-on in your enterprise.

“Troubleshooting single sign-on”

Use the following troubleshooting methods to solve some of the basic problems you might experience while configuring and using a single sign-on environment.

Related information

Configuring network authentication service

Configuring Enterprise Identity Mapping

Managing single sign-on

Use network authentication service and Enterprise Identity Mapping (EIM) to manage your single sign-on environment.

After you implement a single sign-on environment, you might need to perform various management tasks to maintain that environment in accordance with your security policy just as you would any other aspect of your network.

To learn more about how to manage these functions to maintain your single sign-on environment, review the following:

- Manage network authentication service
Learn about common network authentication service management tasks such as how to synchronize system times, add and delete realms, add a Kerberos server, and more.
- Manage EIM
Learn about common EIM management tasks, such as how to manage associations, identifiers, registry definitions, and more.

If you experience problems with your single sign-on environment, you can troubleshoot single sign-on.

Related tasks

“Troubleshooting single sign-on”

Use the following troubleshooting methods to solve some of the basic problems you might experience while configuring and using a single sign-on environment.

Troubleshooting single sign-on

Use the following troubleshooting methods to solve some of the basic problems you might experience while configuring and using a single sign-on environment.

About this task

There are several actions that you can take to circumvent problems with your i5/OS single sign-on configuration:

1. You can confirm that your network authentication service configuration is correct by performing the qshell kinit command. To do this, enter the qshell environment and issue the `kinit -k <service name>` command. This command uses the keytab entry that was created in the network authentication service wizard. This command verifies that the encrypted password for the service is the same password that is stored on the KDC. If this command does not complete successfully, revisit your network authentication service configuration.
2. Verify your host name resolution configurations, including your DNS servers.
3. Verify the EIM system configuration information on each i5/OS system that performs mapping lookup operations.
 - a. Open System i Navigator.
 - b. Select the system, and expand **Network** → **Enterprise Identity Mapping** → **Configuration**.
 - c. Right-click the **Configuration** folder and select **Properties**.
 - d. On the **Domain** page, verify the domain connection settings and click **Verify Configuration**. This verifies that the domain controller is active and that the settings for the domain controller are correct.
 - e. On the **System User** page, click **Verify Connection** to verify that the system user is specified correctly.
4. Verify defined EIM associations by using the test EIM mapping function to verify that the associations you have defined provide the mappings you expect.
5. If your single sign-on configuration includes a multiple tier network, verify that ticket delegation is enabled for the server in the middle tier. This is required for the middle tier server to forward user credentials to the next server. You can enable ticket delegation on the Active Directory or Kerberos server. An example of a multiple tier network is a PC which authenticates with one server and then connects to another server.

Results

If you are still experiencing a problem with your single sign-on after reviewing the steps above, use the following table to determine possible solutions to the symptoms of your configuration problems:

Table 13. Troubleshooting table

Symptoms	Possible solutions
Host name resolution problems	
You are unable to connect to i5/OS systems within your single sign-on environment.	<ul style="list-style-type: none"> • This might be due to host resolution problems. Verify that the PC and your System i model resolves to the same host name. Verify your host name resolution configurations, including your DNS server. • This might be due to NAS configuration problems. See the Troubleshoot network authentication service information in the i5/OS Information Center.
The NSLOOKUP utility fails to resolve a host name when given an IP address during an attempt to confirm that the host resolution is consistent between your System i system and a client PC.	The NSLOOKUP utility uses the currently configured DNS to resolve IP addresses from host names, as well as host names from IP addresses. If a host name cannot be resolved from an IP address, the most likely cause is a missing PTR record in DNS. Have your DNS administrator add a PTR record for this IP address.
EIM configuration problems	

Table 13. Troubleshooting table (continued)

Symptoms	Possible solutions
<p>EIM mappings are not working as expected. In some instances, you are unable to sign into your system with System i Navigator when using Kerberos authentication.</p>	<ul style="list-style-type: none"> • The domain controller is inactive. Activate the domain controller. • The EIM configuration is incorrect on the systems that you are trying to use Kerberos authentication with or get mappings for. Verify your EIM configuration. Expand Network → Enterprise Identity Mapping → Configuration on the system that you are trying to authenticate with. Right-click the Configuration folder and select Properties . Network → Enterprise Identity Mapping → Configuration Network → Enterprise Identity Mapping → Configuration. Verify the following: <ul style="list-style-type: none"> – Domain page: <ul style="list-style-type: none"> - The domain controller name and port numbers are correct. - Click Verify Configuration to verify that the domain controller is active. - The local registry name is specified correctly. - The Kerberos registry name is specified correctly. - Verify that Enable EIM operations for this system is selected. – System user page: <ul style="list-style-type: none"> - The specified user has sufficient EIM access control to perform a mapping lookup, and the password is valid for the user. See the online help to learn more about the different types of user credentials. Note: Whenever passwords are updated in the directory server, they must also be updated in the system configuration. - Click Verify Connection to confirm that the user information specified is correct. • The EIM domain configuration is incorrect: <ul style="list-style-type: none"> Note: You can test EIM mapping to help verify that the associations for your EIM domain are properly configured. – A target or source association for an EIM identifier is not set up correctly. For example, there is no source association for the Kerberos principal (or Windows user) or it is incorrect. Or, the target association specifies an incorrect user identity. Display all identifier associations for an EIM identifier to verify associations for a specific identifier. – A policy association is not set up correctly. Display all policy associations for a domain to verify source and target information for all policy associations defined in the domain. – Mapping lookups are returning more than one target identity, indicating that ambiguous mappings are configured. Test EIM mappings to identify which mappings are incorrect. – The registry definition and user identities do not match because of case sensitivity. You can delete and re-create the registry, or delete and re-create the association with the proper case. • EIM support is not enabled. <ul style="list-style-type: none"> – EIM has been disabled for the system. Verify that Enable EIM operations for this system is selected on the Domain page for the system EIM configuration properties by expanding Network → Enterprise Identity Mapping → Configuration → Properties. – Policy association support is not enabled at the domain level. You might need to enable policy associations for a domain. – Mapping lookup support or policy association support is not enabled at the individual registry level. You might need to enable mapping lookup support and the use of policy associations for the target registry.

Table 13. Troubleshooting table (continued)

Symptoms	Possible solutions
Network authentication service configuration problems	
A keytab entry is not found when you perform a keytab list.	<ul style="list-style-type: none"> This can be due to a host resolution problem on the System i model. If you are using a host table, perform the Configure TCP/IP CFGTCP command, option 10 (Work with TCP/IP host table entries) and verify that the primary host name is listed first for the IP address of the server. Verify your host name resolution configurations, including your DNS server.
Users are unable to connect to systems.	<p>Users might be unable to connect to systems if the EIM registry definition for the Kerberos registry was inappropriately defined as case sensitive. Delete and re-create the Kerberos registry.</p> <p>Note: You will lose any associations that have been defined for that registry and will have to re-create them.</p>
User receives a message indicating an incorrect password when verifying the network authentication service configuration.	The password for the service in the KDC does not match the password for the service in the keytab. Update the keytab entry by using the keytab add command, and update the password for the service on the KDC.
User receives the following message: Unable to obtain name of default credentials cache.	Verify that a home directory (/home/<user profile>) exists for the user that is performing the kinit.
User receives the following message: Response too large for datagram.	<p>Update the network authentication service configuration to use TCP as the data communications protocol:</p> <ol style="list-style-type: none"> Using System i Navigator, select the system that issued the message. Select Security → Network Authentication Service properties. On the General page, select Use TCP and click OK.
General problems	
You receive error message CWBSY10XX when attempting single sign-on.	<ul style="list-style-type: none"> Use the help associated with the text to resolve the problem. Use the System Access detail trace feature to determine if the appropriate Kerberos ticket is retrieved. Download the Microsoft kerbtray utility to verify that the user has Kerberos credentials. If single sign-on is failing, check the QZSOSIGN jobs in the QUSRWRK subsystem. Search through the jobs for a CPD3E3F message. If you find the CPD3E3F message, use the recovery information provided within the message. The diagnostic message contains both major and minor status codes to indicate where the problem occurred. The most common errors are documented in the message along with the recovery. If PC5250 is failing, check the following: <ul style="list-style-type: none"> Check the QTVDEVICE jobs for the CPD3E3F message. Check the QRMTSIGN system value and verify that it is set to *VERIFY or *SAMEPRF.

Related information

 RFC 1713: Tools for DNS debugging

Troubleshoot EIM.

Configuring network authentication service

Host name resolution considerations

Testing EIM mappings

Related information for Single sign-on

IBM Redbooks® publications and other information center topic collections contain information that relates to the Single sign-on topic collection. You can view or print any of the PDF files.

IBM Redbooks

The IBM System i Security Guide for IBM i5/OS Version 5 Release 4  IBM Redbooks publication provides a chapter on authentication using Single sign-on.

Other information

- Enterprise Identity Mapping (EIM)
- Network authentication services
- IBM Tivoli Directory Server for i5/OS
- Digital Certificate Manager

Code license and disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1. LOSS OF, OR DAMAGE TO, DATA;
2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR
3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

- | The licensed program described in this document and all licensed material available for it are provided
- | by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement,
- | IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 illustrate 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.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

| **Programming interface information**

- | This Single sign-on publication documents intended Programming Interfaces that allow the customer to
- | write programs to obtain the services of IBM i5/OS.

Trademarks

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

AIX
Distributed Relational Database Architecture
DRDA
i5/OS
IBM
iSeries
NetServer
System i
Tivoli
WebSphere
z/OS

- l Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Printed in USA