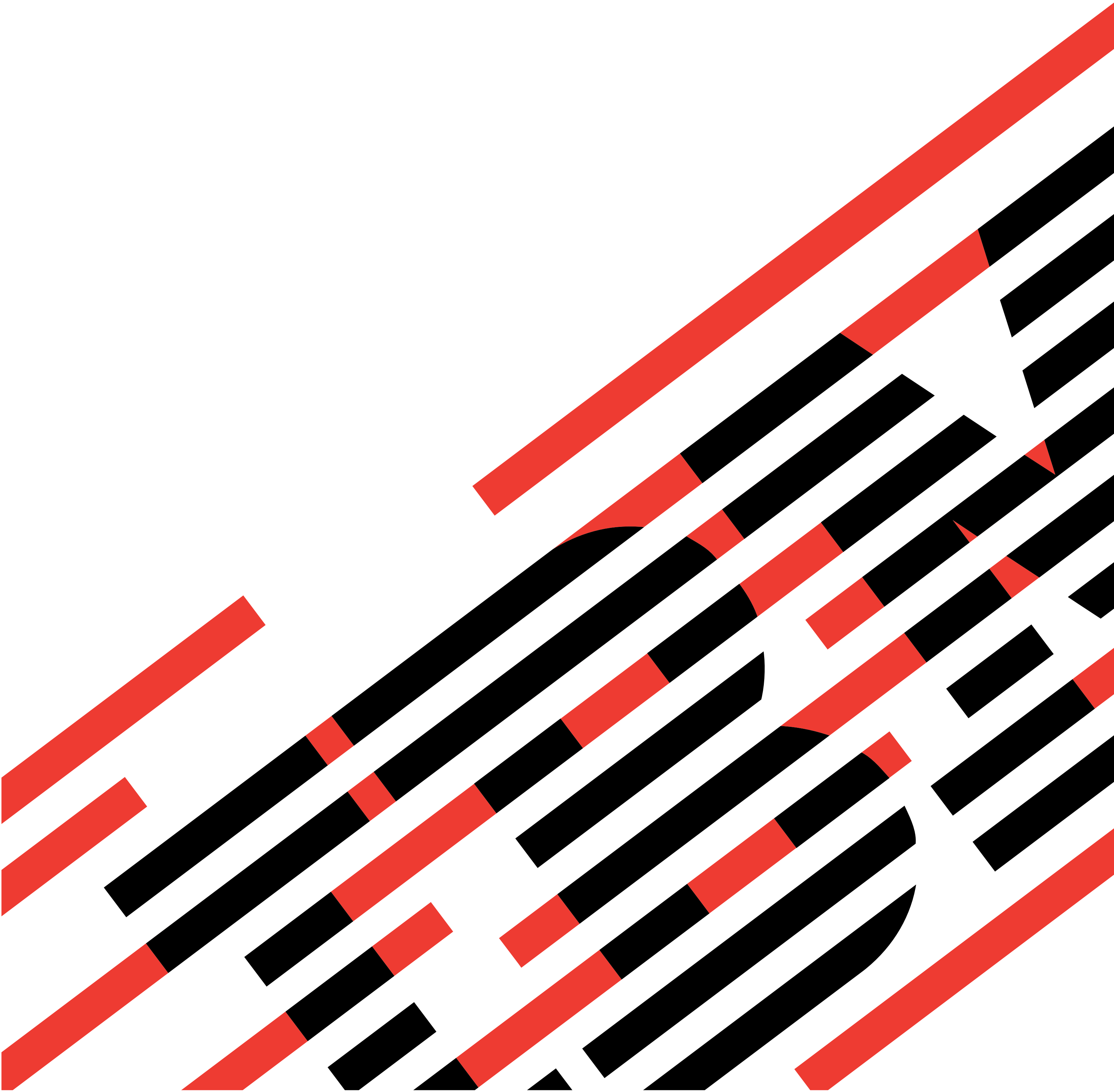
iSeries

Enterprise Identity Mapping



iSeries

Enterprise Identity Mapping

Contents

Enterprise Identity Mapping (EIM)

Most network enterprises face the problem of multiple user registries, which require each person or entity within the enterprise to have a user identity in each registry. The need for multiple user registries quickly grows into a large administrative problem that affects users, administrators, and application developers. Enterprise Identity Mapping (EIM) enables inexpensive solutions for easier management of multiple user registries and user identities in your enterprise.

EIM is a mechanism for mapping (associating) a person or entity to the appropriate user identities in various registries throughout the enterprise. EIM provides APIs for creating and managing these identity mapping relationships, as well as APIs that applications use to query this information. In addition, OS/400$^{(R)}$ uses EIM and Kerberos capabilities to provide a single sign-on environment.

iSeries Navigator, the iSeries graphical user interface, provides wizards to configure and manage EIM. In addition, administrators can manage EIM relationships for user profiles through iSeries Navigator.

The iSeries$^{(TM)}$ server uses EIM to enable OS/400 interfaces to authenticate users by means of network authentication service. Applications, as well as OS/400, can accept Kerberos tickets and use EIM to find the user profile that represents the same person as the Kerberos ticket represents.

The following topics provide specific information about EIM:

“Print this topic” on page 2
Print a PDF of this EIM topic and other related topics.

“Enterprise Identity Mapping overview” on page 2
Learn about the problems that EIM can help you solve, current industry approaches to these problems, and why the EIM approach is a better solution.

“EIM concepts” on page 4
Learn about EIM concepts that you need to understand to implement EIM successfully.

“LDAP concepts for EIM” on page 19
Learn about Lightweight Directory Access Protocol (LDAP) concepts that you need to understand to implement EIM successfully.

“Single sign-on enablement through EIM” on page 21
Read about the benefits that EIM provides in simplifying user sign-on.

“Plan for EIM” on page 23
Ensure that you have all of the required services and applications configured before you configure EIM.

“Configure EIM” on page 24
Use the Enterprise Identity Mapping Configuration Wizard (hereafter referred to as EIM Configuration wizard) to get started with EIM.

“Manage EIM” on page 31
Manage EIM properties, EIM domains, user registries, EIM user authorities, and more.

“APIs for EIM” on page 38
Use the EIM APIs in your applications and network.

“Troubleshoot EIM” on page 39
Find solutions to common problems and errors that may occur when using EIM in your network.

"Related information for EIM" on page 40
Link to related information on EIM.

Print this topic

To view or download the PDF version, select Enterprise Identity Mapping (about 390 KB or 50 pages).

Other information

You can view or download these related topics:

- Network authentication services (about 199 KB or 60 pages) contains information about how to configure network authentication service in conjunction with EIM to create a single sign-on environment.
- Directory Services (LDAP) (about 323 KB or 66 pages) contains information about how to configure the LDAP server, which you can use as an EIM domain controller, along with information about advanced LDAP configuration.

Saving PDF files

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

1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click **File**.
3. Click **Save As...**
4. Navigate to the directory in which you would like to save the PDF.
5. Click **Save**.

Downloading Adobe Acrobat Reader

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

Enterprise Identity Mapping overview

Today's network environments are made up of a complex group of systems and applications, resulting in the need to manage multiple user registries. Dealing with multiple user registries quickly grows into a large administrative problem that affects users, administrators, and application developers. Consequently, many companies are struggling to securely manage authentication and authorization for systems and applications. Enterprise Identity Mapping (EIM) is an IBM eserver infrastructure technology that allows administrators and application developers to address this problem more easily and inexpensively than previously possible.

The following information describes the problems, outlines current industry approaches, and explains why the EIM approach is better.

The problem of managing multiple user registries

Many administrators manage networks that include different systems and servers, each with a unique way of managing users through various user registries. In these complex networks, administrators are responsible for managing each user's identities and passwords across multiple systems. Additionally, administrators often must synchronize these identities and passwords and users are burdened with remembering multiple identities and passwords and with keeping them in sync. The user and administrator overhead in this environment is excessive. Consequently, administrators often spend valuable time troubleshooting failed log-on attempts and resetting forgotten passwords instead of managing the enterprise.

The problem of managing multiple user registries also affects application developers who want to provide multiple-tier or heterogeneous applications. These developers understand that customers have important business data spread across many different types of systems, with each system possessing its own user registries. Consequently, developers must create proprietary user registries and associated security semantics for their applications. Although this solves the problem for the application developer, it increases the overhead for users and administrators.

Current approaches

Several current industry approaches for solving the problem of managing multiple user registries are available, but they all provide incomplete solutions. For example, Lightweight Directory Access Protocol (LDAP) provides a distributed user registry solution. However, using LDAP (or other popular solutions such as Microsoft Passport) means that administrators must manage yet another user registry and security semantics or must replace existing applications that are built to use those registries.

Using this type of solution, administrators must manage multiple security mechanisms for individual resources, thereby increasing administrative overhead and potentially increasing the likelihood of security exposures. When multiple mechanisms support a single resource, the chances of changing the authority through one mechanism and forgetting to change the authority for one or more of the other mechanisms is much higher. For example, a security exposure can result when a user is appropriately denied access through one interface, but allowed access through one or more other interfaces.

After completing this work, administrators find that they have not completely solved the problem. Generally, enterprises have invested too much money in current user registries and in their associated security semantics to make using this type of solution practical. Creating another user registry and associated security semantics solves the problem for the application provider, but not the problems for users or administrators.

One other possible solution is to use a single sign-on approach. Several products are available that allow administrators to manage files that contain all of a user’s identities and passwords. However, this approach has several weaknesses:

- It addresses only one of the problems that users face. Although it allows users to sign on to multiple systems by supplying one identity and password, it does not eliminate the need for the user to have passwords on other systems, or the need to manage these passwords.
- It introduces a new problem by creating a security exposure because clear-text or decryptable passwords are stored in these files. Passwords should never be stored in clear-text files or be easily accessible by anyone, including administrators.
- It does not solve the problems of third-party application developers that provide heterogeneous, multiple-tier applications. They must still provide proprietary user registries for their applications.

Despite these weaknesses, some enterprises have chosen to adopt these approaches because they provide some relief for the multiple user registry problems.

The EIM approach

EIM offers a new approach to enable inexpensive solutions to easily manage multiple user registries and user identities in an enterprise. EIM is an architecture for describing the relationships between individuals or entities (like file servers and print servers) in the enterprise and the many identities that represent them within an enterprise. In addition, EIM provides a set of APIs that allow applications to ask questions about these relationships.

For example, given a person’s user identity in one user registry, you can determine which user identity in another user registry represents that same person. If the user has authenticated with one user identity and you can map that user identity to the appropriate identity in another user registry, the user does not need to provide credentials for authentication again. You know who the user is and only need to know which user identity represents that user in another user registry. Therefore, EIM provides a generalized identity mapping function for the enterprise.

The ability to map between a user’s identities in different user registries provides many benefits. Primarily, it means that applications may have the flexibility of using one user registry for authentication while using an entirely different user registry for authorization. For example, an administrator could map an SAP identity (or better yet, SAP could do the mapping itself) to access SAP resources.

The use of identity mapping requires that administrators do the following:

1. Create EIM identifiers that represent people or entities in their enterprise.
2. Create EIM registry definitions that describe the existing user registries in their enterprise.
3. Define the relationship between the user identities in those registries to the EIM identifiers that they created.

No code changes are required to existing user registries. The administrator does not need to have mappings for all identities in a user registry. EIM allows one-to-many mappings (in other words, a single user with more than one user identity in a single user registry). EIM also allows many-to-one mappings (in other words, multiple users sharing a single user identity in a single user registry, which although supported is not advised). An administrator can represent any user registry of any type in EIM.

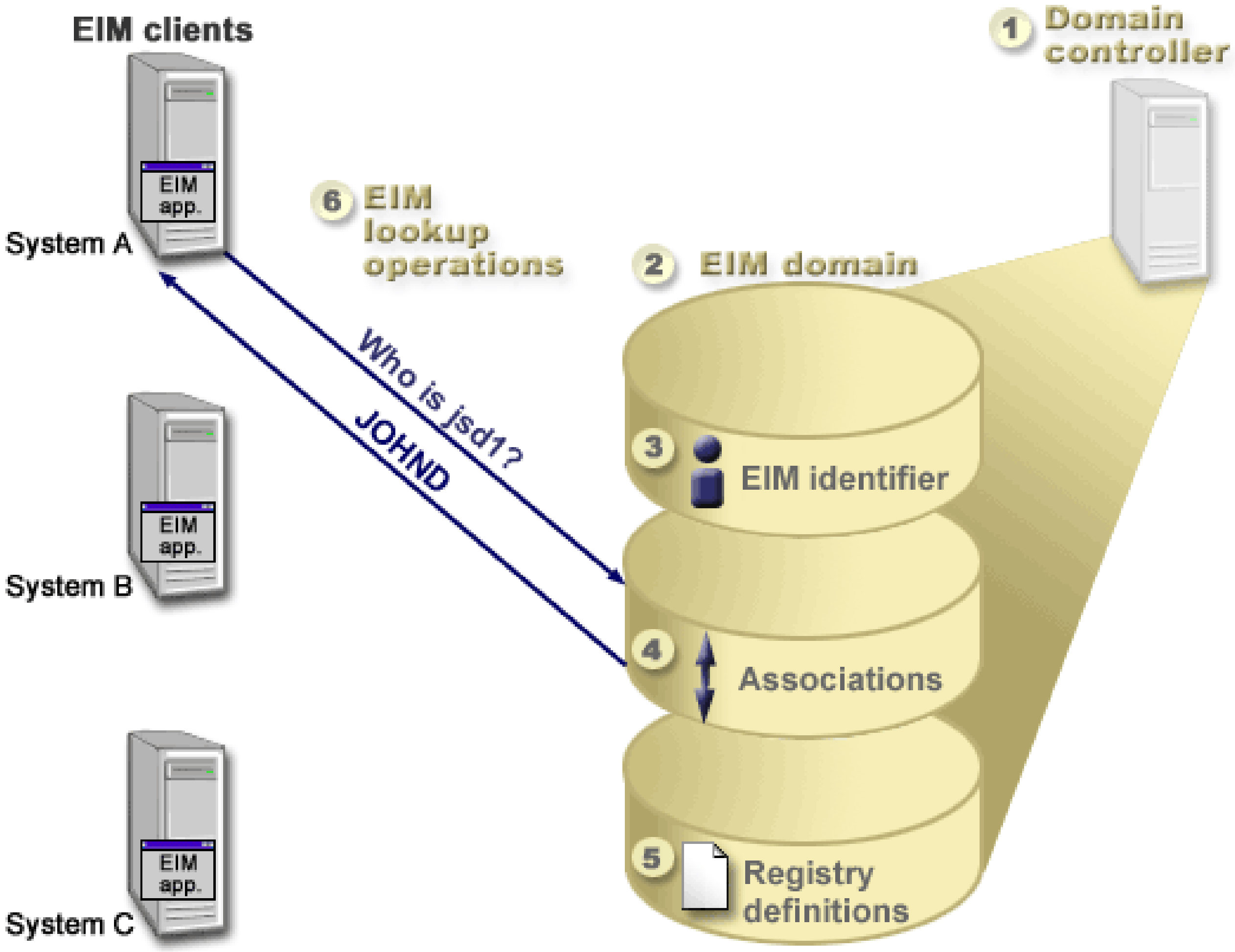
EIM is an open architecture that administrators may use to represent identity mapping relationships for any registry. It does not require copying existing data to a new repository and trying to keep both copies synchronized. The only new data that EIM introduces is the relationship information. Administrators manage this data in an LDAP directory, which provides the flexibility of managing the data in one place and having replicas wherever the information is used. Ultimately, EIM gives enterprises and application developers the flexibility to easily work in a wider range of environments with less cost than would be possible without this support.

EIM concepts

A conceptual understanding of how Enterprise Identity Mapping (EIM) works is necessary to fully understand how you can use EIM in your enterprise. Although the configuration and implementation of EIM APIs can differ among server platforms, EIM concepts are common across IBM @server platforms.

Figure 1 provides an EIM implementation example in an enterprise. Three servers act as EIM clients and contain EIM-enabled applications that request EIM data using EIM lookup operations ⑥. The domain controller ① stores information about the EIM domain ②, which includes an EIM identifier ③, associations ④ between these EIM identifiers and user identities, and EIM registry definitions ⑤.

Figure 1: An EIM implementation example



Review the following information to learn more about these EIM concepts:

- “EIM domain controller”
- “EIM domain” on page 6
- “EIM identifier” on page 7
- “EIM registry definitions” on page 9
- “EIM associations” on page 12
- “EIM lookup operations” on page 15
- “EIM authorities” on page 16

EIM domain controller

The *EIM domain controller* is a Lightweight Directory Access Protocol (LDAP) server that is configured to manage at least one EIM domain. An *EIM domain* is an LDAP directory that consists of all the EIM identifiers, EIM associations, and user registries that are defined in that domain. Systems (EIM clients) participate in the EIM domain by using the domain data for EIM lookup operations. A minimum of one EIM domain controller must exist in the enterprise.

Currently, you can configure some IBM eserver platforms to act as an EIM domain controller. Any system that supports the EIM APIs can participate as a client in the domain. These client systems use EIM APIs to contact an EIM domain controller to perform “EIM lookup operations” on page 15.

The location of the EIM client determines whether the EIM domain controller is a local or remote system. The domain controller is *local* if the EIM client is running on the same system as the domain controller. The domain controller is *remote* if the EIM client is running on a separate system from the domain controller.

EIM domain

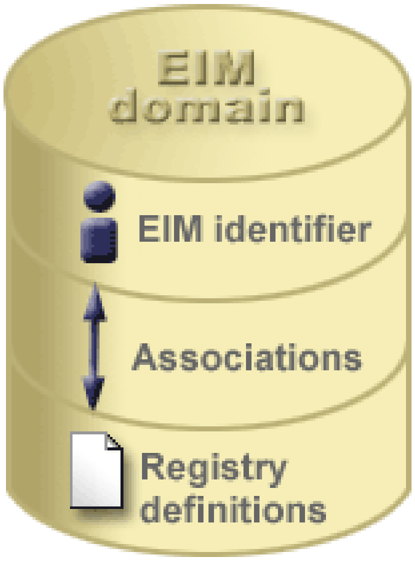
An *EIM domain* is a directory within a Lightweight Directory Access Protocol (LDAP) server that contains EIM data for an enterprise. An EIM domain is the collection of all the EIM identifiers, EIM associations, and user registries that are defined in that domain. Systems (EIM clients) participate in the domain by using the domain data for EIM lookup operations.

An EIM domain is different from a user registry. A user registry defines a set of user identities known to and trusted by a particular instance of an operating system or application. A user registry also contains the information needed to authenticate the user of the identity. Additionally, a user registry often contains other attributes such as user preferences, system privileges, or personal information for that identity.

In contrast, an EIM domain *refers* to user identities that are defined in user registries. An EIM domain contains information about the *relationship* between identities in various user registries (user name, registry type, and registry instance) and the actual people or entities that these identities represent. Because EIM tracks relationship information only, there is nothing to synchronize between user registries and EIM.

Figure 2 shows the data that is stored within an EIM domain. This data includes EIM identifiers, EIM registry definitions, and EIM associations. EIM data defines the relationship between user identities and the people or entities that these identities represent in an enterprise.

Figure 2: EIM domain and the data that is stored within the domain



EIM data includes:

- **EIM identifiers.** Each EIM identifier that you create represents a person or entity (such as a print server or a file server) within an enterprise. See “EIM identifier” on page 7 for more information.
- **EIM registry definitions.** Each EIM registry definition that you create represents an actual user registry (and the user identity information it contains) that exists on a system within the enterprise. Once you

define a specific user registry in EIM, that user registry can participate in the EIM domain. See “EIM registry definitions” on page 9 for more information.

- **EIM associations.** Each EIM association that you create represents the relationship between an EIM identifier and an associated identity within an enterprise. You create associations for identities in user registries that are participating in the EIM domain. Associations provide the information that ties an EIM identifier to a specific user identity in a specific user registry. Consequently, associations must be defined so that EIM clients can use EIM APIs to perform successful EIM lookup operations. These EIM lookup operations search an EIM domain for defined associations between EIM identifiers and user identities in recognized user registries. See “EIM lookup operations” on page 15 for more information.

Once you create your EIM identifiers, registry definitions, and associations, you can begin using EIM to more easily organize and work with user identities within your enterprise.

EIM identifier

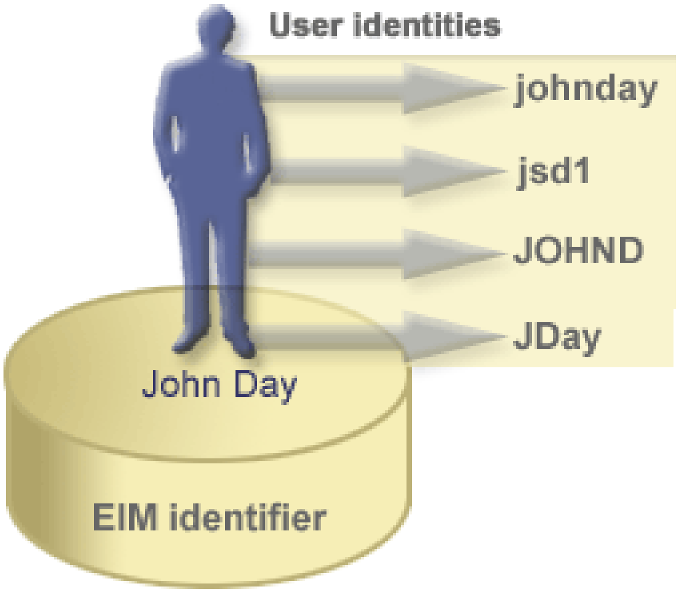
An *EIM identifier* represents a person or entity in an enterprise. A typical network consists of various hardware platforms and applications and their associated user registries. Most platforms and many applications use platform-specific or application-specific user registries. These user registries contain all of the user identification information for users who work with those servers or applications.

When you create an EIM identifier and associate it with the various user identities for a person or entity, it becomes easier to build heterogeneous, multiple-tier applications, for example, a single sign-on environment. When you create an EIM identifier and associations, it also becomes easier to build and use tools that simplify the administration involved with managing every user identity that a person or entity has within the enterprise.

EIM identifier representing a person

Figure 3 shows an example of an EIM identifier that represents a person named *John Day* and his various user identities in an enterprise. In this example, the person *John Day* has four user identities in four different user registries: `johnday`, `jsd1`, `JOHND`, and `JDay`.

Figure 3: The relationship between the EIM identifier for *John Day* and his various user identities

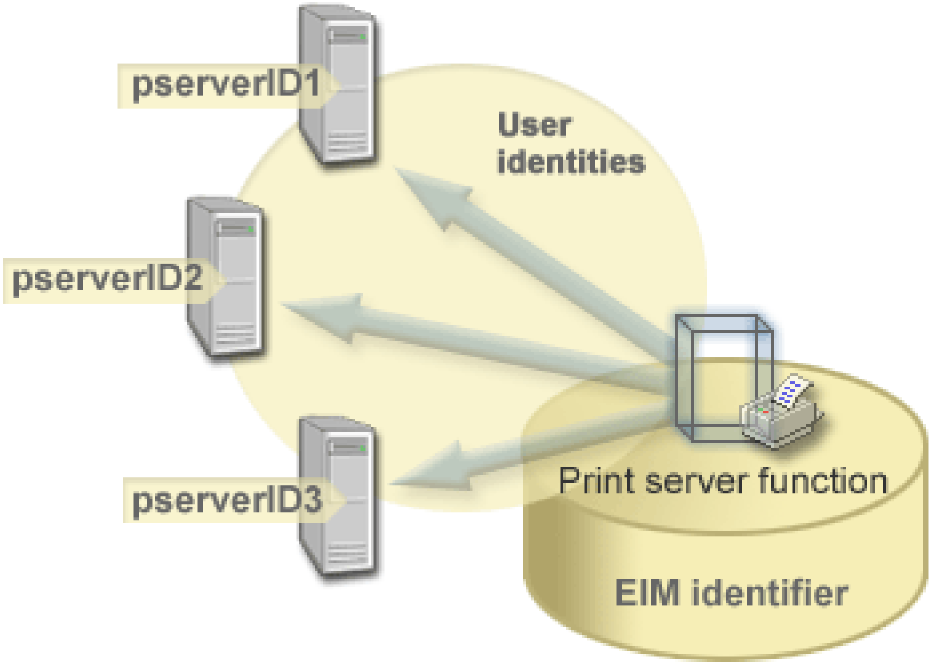


In EIM, you can create associations that define the relationships between the John Day identifier and each of the different user identities for *John Day*. By creating these associations to define these relationships, you and others can write applications that use the EIM APIs to look up a needed, but unknown, user identity based on a known user identity.

EIM identifier representing an entity

In addition to representing users, EIM identifiers can represent entities within your enterprise as Figure 4 illustrates. For example, often the print server function in an enterprise runs on multiple systems. In Figure 4, the print server function in the enterprise runs on three different systems under three different user identities of pserverID1, pserverID2, and pserverID3.

Figure 4: The relationship between the EIM identifier that represents the print server function and the various user identities for that function



With EIM, you can create a single identifier that represents the print server function within the entire enterprise. In this example, the EIM identifier print server function represents the actual print server function entity in the enterprise. Associations are created to define the relationships between the EIM identifier (print server function) and each of the user identities for this function (pserverID1, pserverID2, and pserverID3). These associations allow application developers to use EIM lookup operations to find a specific print server function. Application providers can then write distributed applications that manage the print server function more easily across the enterprise.

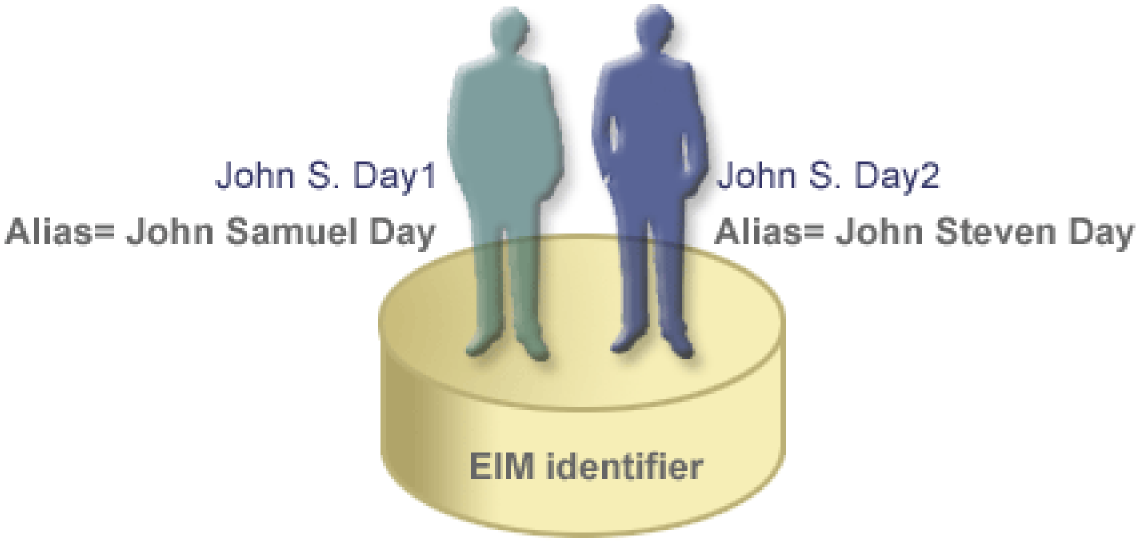
EIM identifiers and aliasing

You can also create aliases for EIM identifiers. Aliases can aid in locating a specific EIM identifier when performing an EIM lookup operation. For example, aliases can be useful in situations where someone's legal name is different from the name that that person is known as.

EIM identifier names must be unique within an EIM domain. Aliases can help address situations where using unique identifier names can be difficult. For example, different individuals within an enterprise can share the same name, which can be confusing if you are using proper names as EIM identifiers.

Figure 5 illustrates an example in which an enterprise has two users named *John S. Day*. The EIM administrator creates two different EIM identifiers to distinguish between them: `John S. Day1` and `John S. Day2`. However, which *John S. Day* is represented by each of these identifiers is not readily apparent.

Figure 5: Aliases for two EIM identifiers based on the shared proper name *John S. Day*



By using aliases, the EIM administrator can provide additional information about the individual for each EIM identifier. This information can also be used in an EIM lookup operation to distinguish between the users that the identifier represents. For example, the alias for `John S. Day1` might be `John Samuel Day` and the alias for `John S. Day2` might be `John Steven Day`.

Each EIM identifier can have multiple aliases to identify which *John S. Day* the EIM identifier represents. The EIM administrator might add another alias to each of the EIM identifiers for the two individuals to further distinguish between them. For example, the additional aliases might contain each user's employee number, department number, job title, or other distinguishing attribute.

EIM registry definitions

An *EIM registry definition* represents an actual user registry that exists on a system within the enterprise. A user registry operates like a directory and contains a list of valid user identities for a particular system or application. A basic user registry contains user identities and their passwords. One example of a user registry is the z/OS Security Server Resource Access Control Facility (RACF$^{(R)}$) registry. User registries can contain other information as well. For example, a Lightweight Directory Access Protocol (LDAP) directory contains bind distinguished names, passwords, and access controls to data that is stored in LDAP. Other examples of common user registries are a Kerberos key distribution center (KDC) and the OS/400 user profiles registry.

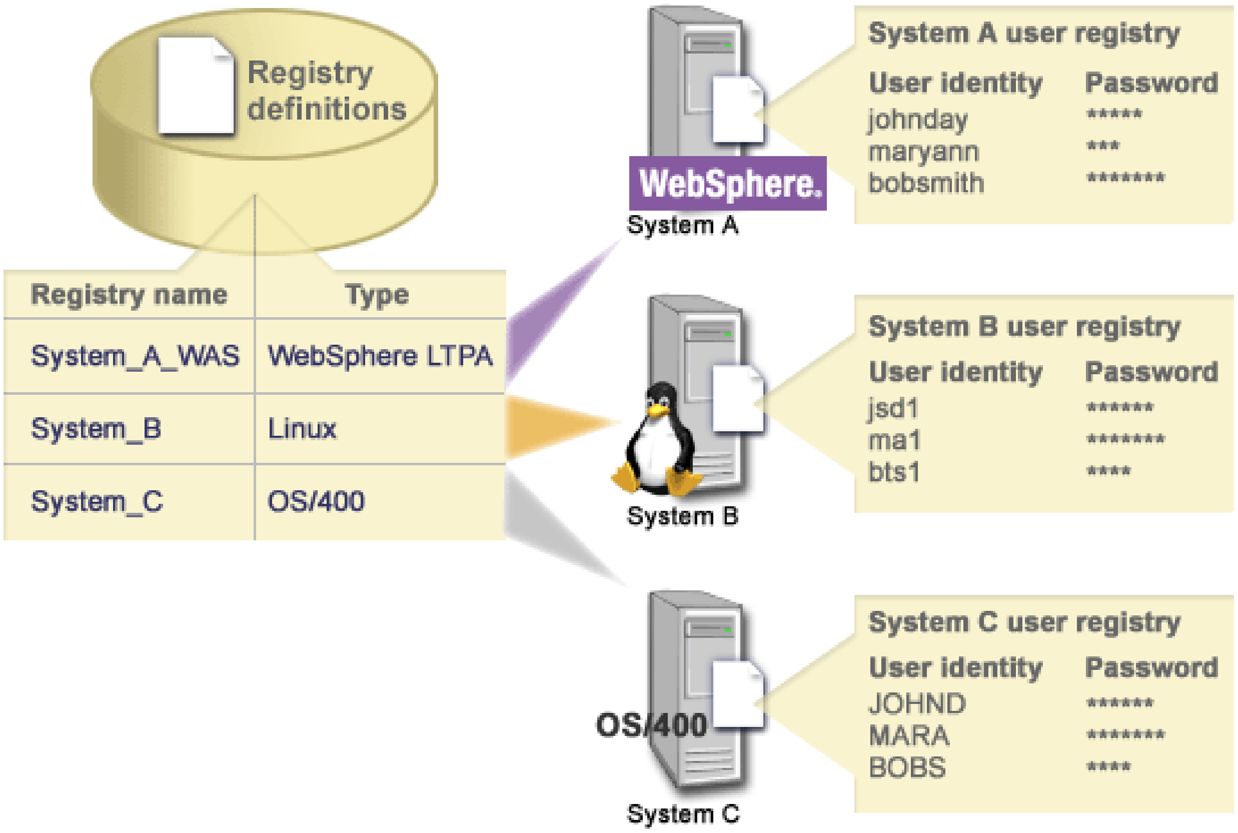
EIM registry definitions provide information regarding those user registries in an enterprise. The administrator defines these registries to EIM by providing the following information:

- A unique, arbitrary EIM registry name
- The type of user registry

Each registry definition represents a specific instance of a user registry. Consequently, you should choose an EIM registry definition name that helps you to identify the particular instance of the user registry. For example, you could choose the TCP/IP host name for a system user registry, or the host name combined with the name of the application for an application user registry. You can use any combination of alphanumeric characters, mixed case, and spaces to create unique EIM registry definition names.

In Figure 6, the administrator created EIM registry definitions for user registries representing System A, System B, and System C. For example, System A contains a user registry for WebSphere Lightweight Third-Party Authentication (LTPA). The registry definition name that the administrator uses helps to identify the specific occurrence of the type of user registry. For example, an IP address or host name is often sufficient for many types of user registries. In this example, the administrator identifies the specific user registry instance by using `System_A_WAS` as the registry definition name. In addition to the name, the administrator also provides the type of registry as `WebSphere LTPA`.

Figure 6: EIM registry definitions for three user registries in an enterprise



Registry name	Type
System_A_WAS	WebSphere LTPA
System_B	Linux
System_C	OS/400

System A user registry

User identity	Password
johnday	*****
maryann	***
bobsmith	*******

System B user registry

User identity	Password
jsd1	******
ma1	*******
bts1	****

System C user registry

User identity	Password
JOHND	******
MARA	*******
BOBS	****

You can also define user registries that exist within other user registries. For example, the z/OS Security Server (RACF) registry can contain specific user registries that are a subset of users within the overall RACF user registry. For a more detailed example of how this works, see “System and application registry definitions” on page 11.

EIM registry definitions and aliasing

You can also create aliases for EIM registry definitions. You can use predefined alias types or you can define your own alias types to use. The predefined alias types include:

- Domain Name System (DNS) host name
- Kerberos realm
- Issuer distinguish name (DN)
- Root distinguished name (DN)

- TCP/IP address
- LDAP DNS host name

This alias support allows programmers to write applications without having to know in advance the arbitrary EIM registry name chosen by the administrator who deploys the application. Application documentation can provide the EIM administrator with the alias name that the application uses. Using this information, the EIM administrator can assign this alias name to the EIM registry definition that represents the actual user registry that the administrator wants the application to use.

When the administrator adds the alias to the EIM registry definition, the application can perform an alias lookup to find the EIM registry name at initialization. The alias lookup allows the application to determine the EIM registry name or names to use as input to the APIs that perform “EIM lookup operations” on page 15.

System and application registry definitions

Some applications use a subset of user identities within a single instance of a user registry. EIM allows administrators to model this scenario by providing two kinds of EIM registry definitions: system and application.

A **system registry definition** represents a distinct registry within a workstation or server. You can create a system registry definition when the registry in the enterprise has one of the following traits:

- The registry is provided by an operating system, such as AIX$^{(R)}$, OS/400$^{(R)}$, or a security management product such as z/OS Security Server Resource Access Control Facility (RACF$^{(R)}$).
- The registry contains user identities that are unique to a specific application, such as Lotus Notes$^{(R)}$.
- The registry contains distributed user identities, such as Kerberos principals or Lightweight Directory Access Protocol (LDAP) distinguished names.

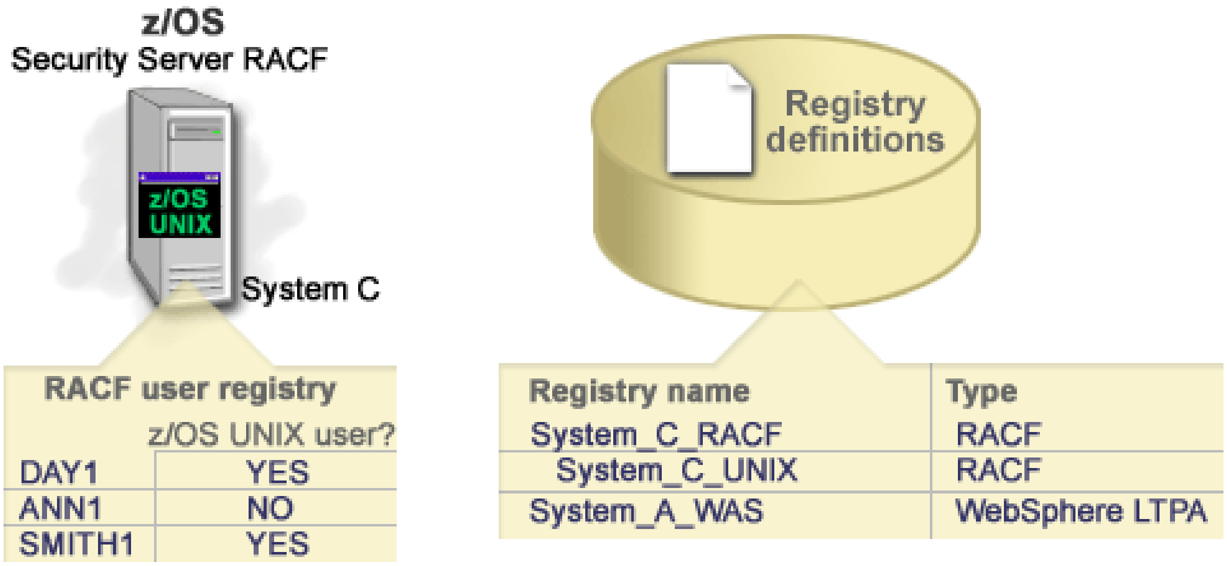
An **application registry definition** represents a subset of user identities that are defined in a system registry. These user identities share a common set of attributes or characteristics that allow them to use a particular application or set of applications. You can create an application registry definition when the user identities have the following traits:

- The user identities for the application or set of applications are not stored in a user registry specific to the application or set of applications.
- The user identities for the application or set of applications are stored in a system registry that contains user identities for other applications.

EIM lookup operations perform correctly regardless of whether an EIM administrator defines a registry either as system or application. However, separate registry definitions allow mapping data to be managed on an application basis. The responsibility of managing application-specific mappings can be assigned to an administrator for a specific registry.

For example, Figure 7 shows how an EIM administrator created a system registry definition to represent a z/OS Security Server RACF registry. The administrator also created an application registry definition to represent the user identities within the RACF registry that use z/OS UNIX System Services (z/OS UNIX). System C contains a RACF user registry that contains information for three user identities, `DAY1`, `ANN1`, and `SMITH1`. Two of these user identities (`DAY1` and `SMITH1`) access z/OS UNIX on System C. These user identities are actually RACF users with unique attributes that identify them as z/OS UNIX users. Within the EIM registry definitions, the EIM administrator defined `System_C_RACF` to represent the overall RACF user registry. The administrator also defined `System_C_UNIX` to represent the user identities that have z/OS UNIX attributes.

Figure 7: EIM registry definitions for the RACF user registry and for users of z/OS UNIX



RACF user registry	z/OS UNIX user?
DAY1	YES
ANN1	NO
SMITH1	YES

Registry name	Type
System_C_RACF	RACF
System_C_UNIX	RACF
System_A_WAS	WebSphere LTPA

EIM associations

An *EIM association* is a relationship between an EIM identifier that represents a specific person and a single user identity in a user registry that also represents that person. When you create associations between an EIM identifier and all of a person's or entity's user identities, you provide a single, complete understanding of how that person or entity uses the resources in an enterprise. EIM provides APIs that allow applications to find an unknown user identity in a specific (target) user registry by providing a known user identity in some other (source) user registry. This process is called *identity mapping*.

Before you can create an association, you first must create the appropriate EIM identifier and the appropriate EIM registry definition for the user registry that contains the associated user identity. An association defines a relationship between an EIM identifier and a user identity by using the following information:

- EIM identifier name
- User identity name
- EIM registry definition name
- Association type

An administrator can create different types of associations between an EIM identifier and a user identity based on how the user identity is used. User identities can be used for authentication, authorization, or both.

Authentication is the process of verifying that an entity or person who provides a user identity has the right to assume that identity. Verification is often accomplished by forcing the person who submits the user identity to provide secret or private information associated with the user identity, such as a password.

Authorization is the process of ensuring that a properly authenticated user identity can only perform functions or access resources for which the identity has been given privileges. In the past, nearly all applications were forced to use the user identities in a single user registry for both authentication and authorization. By using "EIM lookup operations" on page 15, applications now can use user identities in one user registry for authentication while using associated user identities in a different user registry for authorization.

In EIM, there are three types of associations that an administrator can define between an EIM identifier and a user identity. These types are source, target, and administrative associations.

Source association

When a user identity is used for *authentication*, that user identity should have a source association with an EIM identifier. A source association allows the user identity to be used as the source in an EIM lookup operation to find a different user identity that is associated with the same EIM identifier. If a user identity with only a source association is used as the target identity in an EIM lookup operation, no associated user identities are returned.

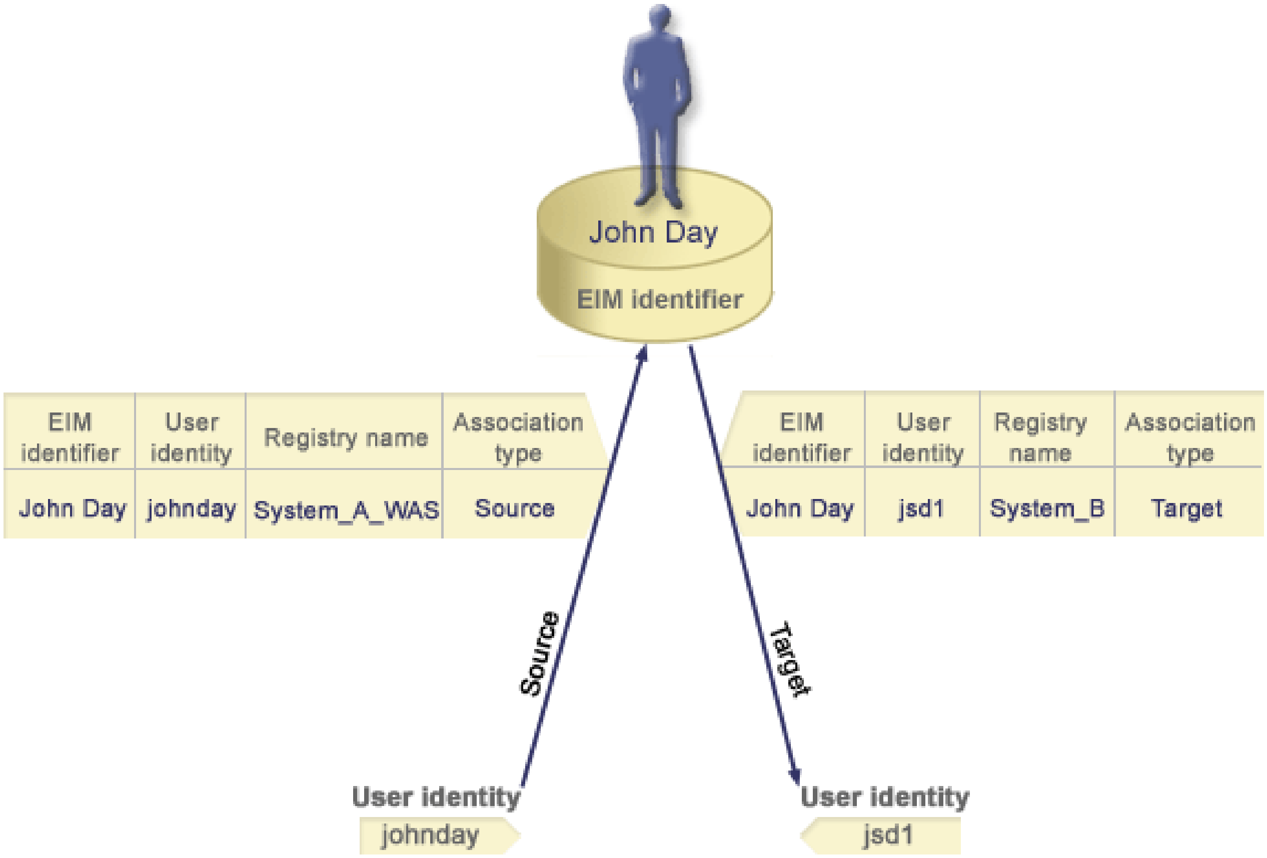
Target association

When a user identity is used for *authorization* rather than for authentication, that user identity should have a target association with an EIM identifier. A target association allows the user identity to be returned as the result of an EIM lookup operation. If a user identity with only a target association is used as the source identity in an EIM lookup operation, no associated user identities are returned.

It may be necessary to create both a target and a source association for a single user identity. This is required when an individual uses a single system as both a client and a server or for individuals who act as administrators. For example, a user normally authenticates to a Windows platform and runs applications that access an AIX server. Because of the user's job responsibilities, the user must occasionally also log directly into an AIX server. In this situation you would create both source and target associations between the AIX user identity and the person's EIM identifier. User identities that represent end users normally need a target association only.

Figure 6 shows an example of a source and a target association. In this example, the administrator created two associations for the EIM identifier `John Day` to define the relationship between this identifier and two associated user identities. The administrator created a source association for `johnday`, the WebSphere Lightweight Third-Party Authentication (LTPA) user identity in the `System_A_WAS` user registry. The administrator also created a target association for `jsd1`, the OS/400 user profile in the System B user registry. These associations provide a means for applications to obtain an unknown user identity (the target, `jsd1`) based on a known user identity (the source, `johnday`) as part of an EIM lookup operation.

Figure 6: EIM target and source associations for the EIM identifier `John Day`



EIM identifier	User identity	Registry name	Association type
John Day	johnday	System_A_WAS	Source

EIM identifier	User identity	Registry name	Association type
John Day	jsd1	System_B	Target

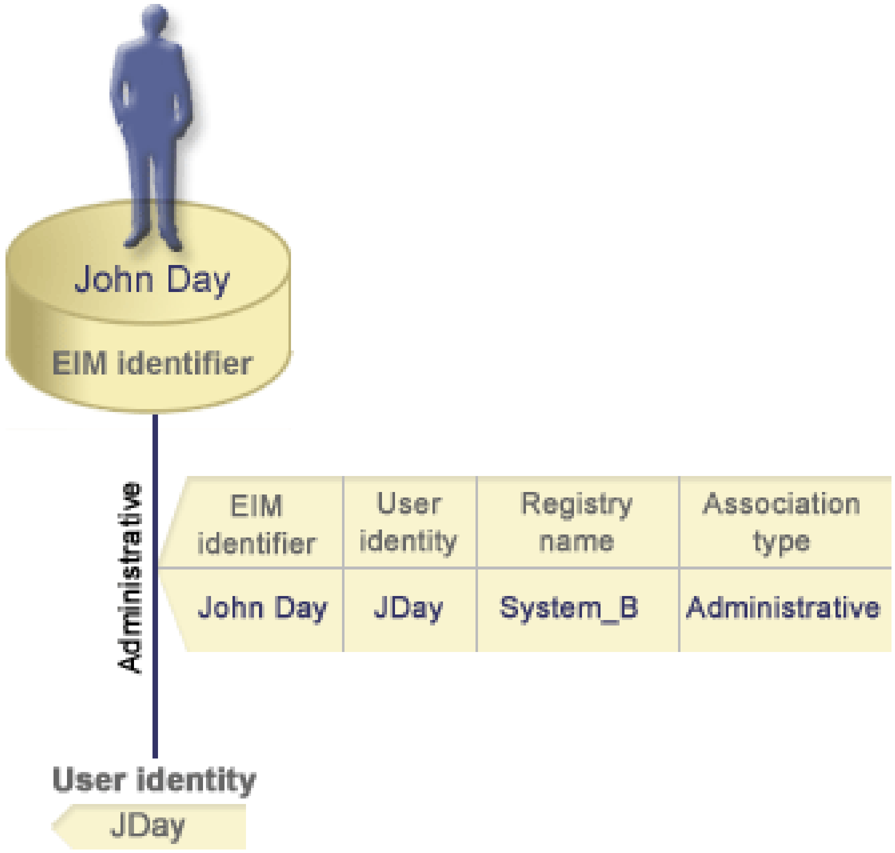
Administrative association

An administrative association for an EIM identifier is typically used to show that the person or entity represented by the EIM identifier owns a user identity that requires special considerations for a specified system. This type of association can be used, for example, with highly sensitive user registries.

Due to the nature of what an administrative association represents, an EIM lookup operation that supplies a source user identity with an administrative association returns no results. Similarly, a user identity with an administrative association is never returned as the result of an EIM lookup operation.

Figure 7 shows an example of an administrative association. In this example, `John Day` has one user identity on System A and another user identity on System B, which is a highly secure system. The system administrator wants to ensure that users authenticate to System B by using only the local user registry of this system. The administrator does not want to allow an application to authenticate `John Day` to the system by using some foreign authentication mechanism. By using an administrative association for the `JDay` user identity on System B, the EIM administrator can see that John Day owns an account on System B, but EIM does not return information about the `JDay` identity in EIM lookup operations. Even if applications exist on this system that use EIM lookup operations, they cannot find user identities that have administrative associations.

Figure 7: EIM administrative association for the EIM identifier `John Day`



EIM identifier	User identity	Registry name	Association type
John Day	JDay	System_B	Administrative

EIM lookup operations

An *EIM lookup operation* is a process through which an application or operating system finds an unknown associated user identity in a specific target registry by supplying some known and trusted information. Applications that use EIM APIs can perform these EIM lookup operations on information only if that information is stored in the EIM domain. An application can perform one of two types of EIM lookup operations based on the type of information the application supplies as the source of the EIM lookup operation: a user identity or an EIM identifier.

When an application supplies a *user identity as the source*, the application also must supply the EIM registry definition name for the source user identity and the EIM registry definition name that is the target of the EIM lookup operation. To be used as the source in a EIM lookup operation, a user identity must have a source "EIM associations" on page 12 defined for it.

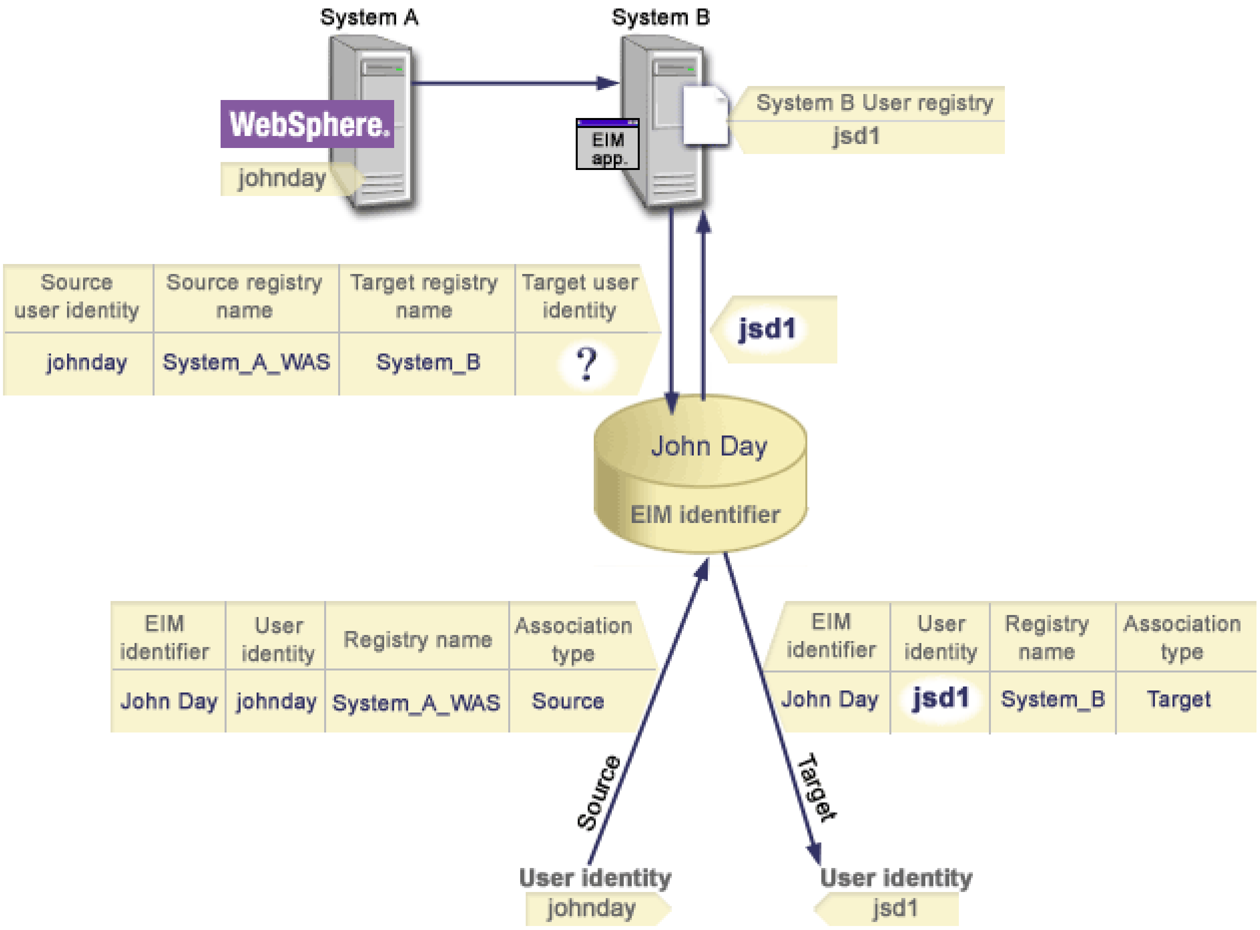
When an application supplies an *EIM identifier as the source* of the EIM lookup operation, the application must also supply the EIM registry definition name that is the target of the EIM lookup operation. For a user identity to be returned as the target of either type of EIM lookup operation, the user identity must have a target association defined for it.

The supplied information is passed to the EIM domain controller where all EIM information is stored and the EIM lookup operation searches for the source association that matches the supplied information. Based on the EIM identifier (supplied to the API or determined from the source association information), the EIM lookup operation then searches for a target association for that identifier that matches the target EIM registry definition name.

In Figure 10, the user identity `johnday` authenticates to the Websphere Application Server by using Lightweight Third-Party Authentication (LPTA) on System A. The Websphere Application Server on System

A calls a native program on System B to access data on System B. The native program uses an EIM API to perform an EIM lookup operation based on the user identity on System A as the source of the operation. The application supplies the following information to perform the operation: `johnday` as the source user identity, `System_A_WAS` as the source EIM registry definition name, and `System_B` as the target EIM registry definition name. This source information is passed to the EIM domain controller and the EIM lookup operation finds a source association that matches the information. Using the EIM identifier name, the EIM lookup operation searches for a target association for the `John Day` identifier that matches the target EIM registry definition name for `System_B`. When the matching target association is found, the EIM lookup operation returns the `jsd1` user identity to the application.

Figure 10: EIM lookup operation based on the known user identity `johnday`



Source user identity	Source registry name	Target registry name	Target user identity
johnday	System_A_WAS	System_B	?

EIM identifier	User identity	Registry name	Association type
John Day	johnday	System_A_WAS	Source

EIM identifier	User identity	Registry name	Association type
John Day	jsd1	System_B	Target

EIM authorities

EIM authorities allow a user to perform specific administrative tasks or EIM lookup operations. Only users with EIM administrator authority are allowed to grant or revoke authorities for other users. EIM authorities are granted only to user identities that are known to the EIM domain controller.

The following are brief descriptions of the functions that each EIM authority group can perform:

- **Lightweight Directory Access Protocol (LDAP) administrator.** This authority allows the user to configure a new EIM domain. A user with this authority can perform the following functions:
  - Create a domain
  - Delete a domain

- Create and remove EIM identifiers
  - Create and remove an EIM registry definition
  - Create and remove source, target, and administrative associations
  - Perform EIM lookup operations
  - Retrieve associations, EIM identifiers, and EIM registry definitions
  - Add, remove, and list EIM authority information
- **EIM administrator.** This authority allows the user to manage all of the EIM data within this EIM domain. A user with this authority can perform the following functions:
  - Delete a domain
  - Create and remove EIM identifiers
  - Create and remove an EIM registry definition
  - Create and remove source, target, and administrative associations
  - Perform EIM lookup operations
  - Retrieve associations, EIM identifiers, and EIM registry definitions
  - Add, remove, and list EIM authority information
- **EIM identifiers administrator.** This authority allows the user to add and change EIM identifiers and manage source and administrative associations. A user with this authority can perform the following functions:
  - Create an EIM identifier
  - Add and remove source associations
  - Add and remove administrative associations
  - Perform EIM lookup operations
  - Retrieve associations, EIM identifiers, and EIM registry definitions
- **EIM mapping lookup.** This authority allows the user to conduct EIM lookup operations. A user with this authority can perform the following functions:
  - Perform EIM lookup operations
  - Retrieve associations, EIM identifiers, and EIM registry definitions
- **EIM registries administrator.** This authority allows the user to manage all EIM registry definitions. A user with this authority can perform the following functions:
  - Add and remove target associations
  - Perform EIM lookup operations
  - Retrieve associations, EIM identifiers, and EIM registry definitions
- **EIM registry X administrator.** This authority allows the user to manage a specific EIM registry definition. This authority allows a user to:
  - Add and remove target associations for the EIM registry definition
  - Perform EIM lookup operations
  - Retrieve associations, EIM identifiers, and EIM registry definitions

Each of the following tables are organized by the EIM task that the API performs. Each table displays each EIM API, the different EIM authorities, and the access each of these authorities has to certain EIM functions.

Table 1: Working with domains

EIM API	LDAP administrator	EIM administrator	EIM identifiers administrator	EIM mapping lookup	EIM registries administrator	EIM registry X administrator
eimChangeDomain	X	X	-	-	-	-

EIM API	LDAP administrator	EIM administrator	EIM identifiers administrator	EIM mapping lookup	EIM registries administrator	EIM registry X administrator
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Table 2: Working with identifiers

EIM API	LDAP administrator	EIM administrator	EIM identifiers administrator	EIM mapping lookup	EIM registries administrator	EIM registry X administrator
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-

Table 3: Working with registries

EIM API	LDAP administrator	EIM administrator	EIM identifiers administrator	EIM mapping lookup	EIM registries administrator	EIM registry X administrator
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Table 4: Working with associations

For eimAddAssociation() and eimRemoveAssociation() APIs there are four parameters that determine the type of association that is either being added or removed. The authority to these APIs differs based on the type of association specified in these parameters. In the following table, the type of association is included for each of these APIs.

EIM API	LDAP administrator	EIM administrator	EIM identifiers administrator	EIM mapping lookup	EIM registries administrator	EIM registry X administrator
eimAddAssociation (administrative)	X	X	X	-	-	-
eimAddAssociation (source)	X	X	X	-	-	-
eimAddAssociation (source and target)	X	X	X	-	X	X
eimAddAssociation (target)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administrative)	X	X	X	-	-	-
eimRemoveAssociation (source)	X	X	X	-	-	-
eimRemoveAssociation (source and target)	X	X	X	-	X	X
eimRemoveAssociation (target)	X	X	-	-	X	X

Table 5: Working with mappings

EIM API	LDAP administrator	EIM administrator	EIM identifiers administrator	EIM mapping lookup	EIM registries administrator	EIM registry X administrator
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Table 6: Working with access

EIM API	LDAP administrator	EIM administrator	EIM identifiers administrator	EIM mapping lookup	EIM registries administrator	EIM registry X administrator
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

LDAP concepts for EIM

Enterprise Identity Mapping (EIM) uses a Lightweight Directory Access Protocol (LDAP) server as a “EIM domain controller” on page 5 to store EIM data. You can use LDAP distinguished names when configuring EIM for your iSeries server and as a means of authenticating to the EIM domain controller.

To use LDAP distinguished names when configuring and administering EIM, you should understand the following LDAP concepts:

- “LDAP distinguished name”
- “LDAP parent distinguished name”

LDAP distinguished name

An LDAP distinguished name (DN) is a Lightweight Directory Access Protocol (LDAP) entry that identifies and describes an authorized user for an LDAP server. You use the EIM Configuration wizard to configure the LDAP server to store the EIM domain information. You can use LDAP distinguished names as a means of accessing and retrieving this EIM data so that your iSeries server can participate in a “Single sign-on enablement through EIM” on page 21.

Distinguished names consist of the name of the entry itself as well as the names, in order from bottom to top, of the objects above it in the LDAP directory. An example of a complete LDAP distinguished name could be `cn=Tim Jones, o=IBM, c=US`. Each entry has at least one attribute that is used to name the entry. This naming attribute is called the relative distinguished name (RDN) of the entry. The entry above a given RDN is called its LDAP parent distinguished name. In this example, `cn=Tim Jones` names the entry, so it is the RDN. `o=IBM, c=US` is the parent DN for `cn=Tim Jones`. See “LDAP parent distinguished name” to learn more about how EIM uses these.

Because EIM uses the LDAP server to store EIM data, you can use LDAP distinguished names as a means of authenticating to the “EIM domain controller” on page 5. You also can use LDAP distinguished names when configuring EIM for your iSeries server. For example, you can use LDAP distinguished names when you:

- Configure the LDAP server to act as the EIM domain controller. You do this by creating and using the LDAP distinguished name that identifies the LDAP administrator for the LDAP server. If the LDAP server has not been configured previously, you can configure the LDAP server when you use the EIM Configuration wizard to create and join a new domain.
- Use the EIM Configuration wizard to select the type of user identity the wizard should use to connect to the EIM domain controller. Distinguished name is one of the user types that you can select. The LDAP distinguished name must represent a user who is authorized to create objects in the local namespace of the LDAP server.
- Use the EIM Configuration wizard to select the type of user to perform EIM operations on behalf of operating system functions. These operations include mapping lookups and deleting associations when deleting a local OS/400 user profile. Distinguished name is one of the user types that you can select.
- Connect to the domain controller to do EIM administration, for example, to manage registries and identifiers and to perform mapping lookup operations.

To learn more about distinguished names and how LDAP uses them, see LDAP basics.

LDAP parent distinguished name

An LDAP parent distinguished name (DN) is an entry in a Lightweight Directory Access Protocol (LDAP) directory server namespace. LDAP server entries are arranged in a hierarchical structure that could reflect political, geographic, organizational, or domain boundaries. A distinguished name is considered a parent DN when the DN is at the highest level of the LDAP server namespace.

An example of a complete LDAP distinguished name could be `cn=Tim Jones, o=IBM, c=US`. Each entry has at least one attribute that is used to name the entry. This naming attribute is called the relative distinguished name (RDN) of the entry. The entry above a given RDN is called its parent distinguished name. In this example, `cn=Tim Jones` names the entry, so it is the RDN. `o=IBM, c=US` is the parent DN for `cn=Tim Jones`.

Because EIM uses the LDAP server to store EIM data, you can use LDAP distinguished names as a means of authenticating to the “EIM domain controller” on page 5. You also can use “LDAP distinguished name” and parent distinguished names when configuring EIM for your iSeries server. For example, when you use the EIM Configuration wizard to create and join a new domain, you can choose to specify a parent DN for the domain that you are creating. By using a parent DN, you can specify where in the local LDAP namespace that EIM data should reside for the domain. When you do not specify a parent DN, EIM data resides in its own suffix in the namespace.

To learn more about distinguished names and how they are used, see LDAP basics.

Single sign-on enablement through EIM

EIM provides an inexpensive mechanism for single sign-on enablement across an enterprise. OS/400 implementation of EIM and Kerberos provides a true multi-tier, heterogeneous single sign-on environment. The benefits for users, administrators, and application developers when a single sign-on environment is available in an enterprise follows:

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

Benefits for administrators
For an administrator, single sign-on simplifies overall security management of an enterprise. Without single sign-on, users and applications may cache passwords to different systems, which can compromise the security of the entire network. Administrators spend time and money on solutions to diminish these security risks. Single sign-on reduces the administrative overhead in managing authentication while keeping the entire network secure. Additionally, single sign-on reduces the administrative costs of resetting forgotten passwords.

Benefits for application developers
For developers of applications that must run in heterogeneous networks, EIM provides the infrastructure to develop applications that work across platforms. By using EIM APIs, programmers can write applications that use the most appropriate existing user registry for authentication while using a different user registry for authorization. Application developers do not need to support platform-specific user registries within the applications they create because EIM provides the infrastructure to create applications that map user identities within those user registries to a single EIM identifier. In addition, EIM allows programmers to maintain these applications without changing associated security semantics, and application-level security significantly lowers the cost of implementing multi-tiered, cross-platform applications.

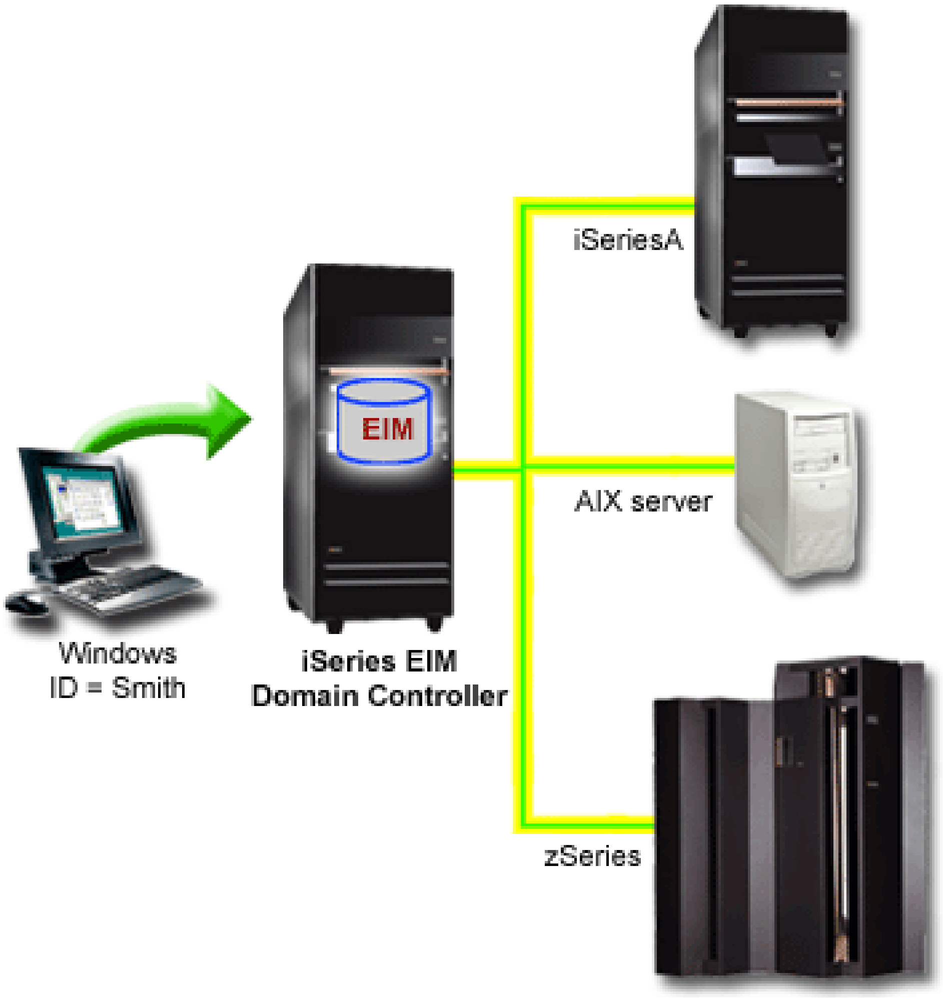
iSeries enablement of single sign-on

To enable a single sign-on environment, IBM uses two technologies that work together: EIM and network authentication service, which is the IBM implementation of Kerberos and the GSS APIs. By configuring these two technologies, an administrator can enable a single sign-on environment. Windows 2000, XP, AIX, and zSeries use Kerberos protocol to authenticate users to the network. Kerberos involves the use of a network-based, secure, key distribution center that authenticates principals (Kerberos users) to the network. A user receives a Kerberos ticket from a centralized, key distribution center. This ticket authenticates the user to other service in an enterprise. 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 an iSeries 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 OS/400 user name, can also be associated with this EIM identifier. Based on these associations, EIM provides a mechanism for OS/400 and applications to determine which OS/400 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.

Using the figure below as an example, imagine that a user, such as John Smith, signs onto the network through his Windows PC and accesses an instance of OS/400 to access Kerberos-enabled applications. John is not prompted for his OS/400 user name. These applications can look up the association to John’s EIM identifier to find the OS/400 user name. John Smith no longer needs a password in his OS/400 user profile because the user profile is not used for authentication; it is only used for authorization.

Figure 1. Single sign-on environment



The topic, Scenario: Enable single sign-on, provides an example of how an administrator configures network authentication service and EIM to enable a single sign-on environment.

The following applications can be accessed through single sign-on:

- iSeries Navigator
- PC5250 Emulator
- Distributed Relational Database Architecture $^{(TM)}$(DRDA)$^{(R)}$
- NetServer
- QFileSvr.400

Plan for EIM

There are multiple technologies and services that EIM encompasses on the iSeries server. Prior to configuring EIM on your server, you should decide the functionality that you want to implement using EIM and single sign-on capabilities.

Before implementing EIM, you should have decided basic security requirements for your network and have implemented those security measures. EIM provides administrators and users easier identity management throughout the enterprise. When used with network authentication service, EIM provides single sign-on capabilities for your enterprise.

The following planning worksheet identifies the services that you should install prior to configuring EIM.

Planning worksheet	Answers
Is your OS/400 V5R2 (5722-SS1) or later?	
Is Cryptographic Access Provider (5722-AC3) installed on your iSeries servers?	
Is iSeries Access for Windows (5722-XE1) installed on the appropriate PCs in your network (the PCs used to work with iSeries servers) and on your iSeries servers?	
Is the Network subcomponent of iSeries Navigator installed on all of the PCs in your network and on your iSeries systems?	
If an LDAP server is currently configured and you want to use it as the EIM domain controller, do you know the LDAP administrator distinguished name (DN) and password?	
If an LDAP server is currently configured, can it be stopped temporarily? (This will be required to complete the EIM configuration process.)	
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	
Have you applied the latest program temporary fixes (PTFs)?	

If you plan on using Kerberos to authenticate users, you should also configure network authentication service. See Plan network authentication service for a complete worksheet for planning network authentication service.

If you are configuring network authentication service and EIM to enable single sign-on, see the Scenario: Enable single sign-on that shows how a company configured both of these products.

Install required iSeries Navigator options

To enable a single sign-on environment with EIM and network authentication service, you must install both the Network option and the Security option of iSeries Navigator. EIM is located within the Network option and network authentication service is within the Security option. If you do not plan to use network authentication service in your network, you do not need to install the Security option of iSeries Navigator.

To install the Network option of iSeries Navigator or to verify that you have this option currently installed, ensure that iSeries Access for Windows is installed on the PC that you are using to work with the iSeries server.

To install the Network option:

1. Click **Start —> Programs —> IBM iSeries Access for Windows —> Selective Setup**.
2. Follow the instructions on the dialog. On the **Component Selection** dialog, expand **iSeries Navigator**, and then select the **Network** option.
   If you plan to use network authentication service, you should also select the **Security** option.
3. Continue through the rest of Selective Setup.

Configure network authentication service

Network authentication service enables you to use Kerberos authentication on your iSeries server. This service is not a prerequisite for using EIM on your server; however, there are many benefits to using Kerberos authentication for security in your network.

Network authentication service, when used in conjunction with EIM, provides you with the means to enable a “Single sign-on enablement through EIM” on page 21. A single sign-on environment is beneficial for users and administrators. Users have fewer user names and passwords to manage and administrators have less information to track for each user. Because single sign-on enablement also helps bridge the gap between multiple platforms and different systems that may be within your network, application development and general administrative costs can be reduced.

If you do not currently have network authentication service configured on your iSeries server or on all servers in your network, see Plan network authentication service for planning information to help you get started. If you are familiar with network authentication service, see Configure network authentication service to get started with the configuration process.

Configure EIM

To enable a single sign-on environment across multiple platforms without the need to change underlying security policies, you must configure EIM as well as network authentication service. However, configuring and using network authentication service is not a prerequisite or requirement for configuring and using EIM.

To begin the process of configuring EIM for iSeries server to take part in a single sign-on environment, you use the EIM Configuration wizard. Depending on your configuration needs, you can use the wizard either to join an existing domain or to create and join a new domain.

The EIM Configuration wizard allows you to easily complete a basic EIM configuration. For example, if you do not already have an LDAP server configured or if you have not configured network authentication service, the EIM Configuration wizard helps you perform these tasks.

After you use the wizard to perform basic EIM configuration, you must perform some additional configuration steps before you can use a single sign-on environment. See Scenario: Enable single sign-on for an example that shows how a fictitious company configured a single sign-on environment using network authentication service and EIM.

Before you use the EIM Configuration wizard, you should have completed all “Plan for EIM” on page 23 steps to determine exactly how you will use both EIM and network authentication service to enable a single sign-on environment. Once your planning is complete, you can use the wizard to configure EIM for your iSeries server in one of two ways: create new domains or join existing domains. The following topics provide instructions for configuring EIM:

“Create and join a new domain” on page 25
Choose this task to create an EIM domain for your network and to configure the iSeries server to participate in it. The wizard creates the new domain and configures the local LDAP server to be the EIM domain controller for the new domain. Also, if Kerberos is not currently configured on the iSeries server, the wizard prompts you to launch the Network Authentication Service Configuration Wizard. After you complete this task, you can configure other iSeries servers to participate in the domain. To configure other servers to participate in the domain, connect to each of them and use the EIM Configuration wizard to configure a server to join an existing EIM domain.

“Join an existing domain” on page 28
Once you use the EIM Configuration wizard to configure a domain controller and an EIM domain, choose this task to configure other iSeries servers to participate in the domain. You need to complete

this task for each iSeries server in the network that will use EIM. After you complete the wizard, you must supply information about the domain being joined, including connection information (such as port number and whether to use Transport Layer Security (TLS)/Secure Sockets Layer (SSL) to the EIM domain controller. If Kerberos is not currently configured on the iSeries server, the wizard prompts you to launch the Network Authentication Service Configuration Wizard.

How to access the EIM Configuration wizard

To access the EIM Configuration wizard, follow these steps:

1. Start iSeries Navigator.
2. Sign on to the iSeries server for which you want to configure EIM.
   If you are configuring EIM for more than one iSeries server, begin with the one on which you want to configure the domain controller for EIM.
3. Expand **Network —> Enterprise Identity Mapping**.
4. Right-click **Configuration** and select **Configure...** to launch the EIM Configuration wizard.
5. Select either the **Join an existing domain** or the **Create and join a new domain** path.

After you finish using the EIM Configuration wizard to create the domain controller and to configure your iSeries servers to participate in the domain, you must complete these tasks to finalize your EIM configuration:

1. “Add a user registry” on page 35 to the EIM domain for non-iSeries servers and applications that you want to participate in the EIM domain.
2. “Create an EIM identifier” on page 34 in the domain for each unique user or entity for systems participating in the EIM domain.
3. “Create an association” on page 32 between the various user identities of a person or entity to these EIM identifiers.

Create and join a new domain

You can use the EIM Configuration wizard to configure the LDAP server on the iSeries server to be the “EIM domain controller” on page 5 for a new domain. If necessary, the EIM Configuration wizard ensures that you provide basic configuration information for the LDAP server.

Also, if Kerberos is not currently configured on the iSeries server, the wizard prompts you to launch the Network Authentication Service Configuration Wizard. When you complete this wizard, a new EIM domain is configured, your iSeries system is configured to join the new domain, and the user registries that you specified are added to the domain.

To use the wizard to complete this task, you must have Security Administrator (*SECADM), All Object (*ALLOBJ), and System Configuration (*IOSYSCFG) special authorities.

To start and use the EIM Configuration wizard to create and join a new EIM domain, complete these steps from within iSeries Navigator:

Note: This wizard also configures the local LDAP server as the new EIM domain controller.

1. Expand **Network** —> **Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Configure...** to launch the EIM Configuration wizard.
3. On the **Welcome** page of the wizard, select **Create and join a new domain**, and click **Next**.
4. If network authentication service is not currently configured on the iSeries server, the **Network Authentication Services Configuration** dialog displays. This dialog prompts you to select whether to configure network authentication service. If you select **Yes**, the Network Authentication Service Configuration Wizard launches. When you complete network authentication service configuration, the EIM Configuration wizard continues.

5. If the local LDAP server is not currently configured, the **Configure Directory Server** dialog displays. Provide the following information on the dialog to configure the local LDAP server:
   - In the **Port** field, accept the default port number **389**, or enter a different port number to use for nonsecure EIM communications with the directory server.
   - In the **Distinguished name** field, enter the LDAP distinguished name (DN) that identifies the LDAP administrator for the LDAP server. The EIM Configuration wizard creates this LDAP administrator DN and uses it to configure the LDAP server as the domain controller for the domain that you are creating.
   - In the **Password** field, enter the password for the LDAP administrator.
   - In the **Confirm password** field, re-enter the password.
   - Click **Next**.
6. On the **Specify Domain Controller** dialog, provide the following information:
   - In the **Domain** field, specify the name of the EIM domain that you want to create. Accept the default name of **EIM**, or use any string of characters that makes sense to you. However, you cannot use special characters such as = + < > , # ; \ and *.
   - In the **Description** field, enter text to describe the domain.
   - Click **Next**.
7. On the **Specify Domain Parent DN** dialog, select whether to specify a parent DN for the domain that you are creating. By specifying a parent DN, you can specify where in the local LDAP namespace EIM data should reside for the domain. When you do not specify a parent DN, EIM data resides in its own suffix in the namespace. If you select **Yes**, use the list box to select the local LDAP suffix to use as the parent DN, or enter text to create and name a new parent DN. It is not necessary to specify a parent DN for the new domain.
8. On the **Specify User For Connection** dialog, select a **user type** for the connection. You can select one of the following types of users: Distinguished name and password, Kerberos keytab file and principal, or Kerberos principal and password. The two Kerberos user types are available only if network authentication service is configured for the local iSeries system. The user type that you select determines the other information that you must provide to complete the dialog as follows:
   - If you select **Distinguished name and password**, provide the following information:
     - In the **Distinguished name** field, enter the LDAP distinguished name (DN) that identifies the user who is authorized to create objects in the local namespace of the LDAP server. If you used this wizard to configure the LDAP server in an earlier step, you should enter the Distinguished name of the LDAP administrator that you created in that step.
     - In the **Password** field, enter the password for the user.
     - In the **Confirm password** field, re-enter the password.
   - If you select **Kerberos keytab file and principal**, provide the following information:
     - In the **Keytab file** field, enter the name of the keytab file name on the iSeries server that identifies the user who is authorized to create objects in the local namespace of LDAP server. Or, you can click **Browse** to select the keytab file.
     - In the **Principal** field, enter the name of the Kerberos principal to be used to identify the user.
     - In the **Realm** field, enter the name of the Kerberos realm for the principal. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com, is represented in the keytab file as jsmith@ordept.myco.com.
   - If you select **Kerberos principal and password**, provide the following information:
     - In the **Principal** field, enter the name of the Kerberos principal that identifies the user who is authorized to create objects in the local namespace of LDAP server.
     - In the **Realm** field, enter the name of the Kerberos realm for the principal.
     - In the **Password** field, enter the password for the user.

  - In the **Confirm password** field, re-enter the password. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
- Click **Verify Connection** to test your user configuration information for connecting to the domain controller.
- Click **Next**.

9. On the **Registry Information** dialog, select the type of user registries that you want to add to the EIM domain. Select one or both of these user registry types:
   - Select **OS400** to add a user registry that represents the local registry to the EIM domain. In the field provided, enter the name of the registry to be created in the domain. The EIM registry name is an arbitrary string that represents the registry type and specific instance of that registry.
   - Select **Kerberos** to add a Kerberos user registry to the EIM domain. In the field provided, enter the name of the registry to be created in the domain and select **Kerberos user identities are case sensitive**, if necessary.
   - Click **Next**.
10. On the **Specify EIM System User** dialog, select the type of user that you want the system to use when performing EIM operations on behalf of operating system functions. These operations include mapping lookups and deleting associations when deleting a local OS/400 user profile. You can select one of the following types of users: Distinguished name and password, Kerberos keytab file and principal, or Kerberos principal and password. The user type that you select determines the other information that you must provide to complete the dialog as follows:

Note: The user that you specify must have privileges to perform mapping lookup and registry administration for the local user registry at a minimum. If the user that you specify does not have these privileges, then certain operating system functions related to single sign-on and deleting user profiles may fail.

11. If you select **Distinguished name and password**, provide the following information:
    - In the **Distinguished name** field, enter the LDAP distinguished name that identifies the user for OS/400 to use when contacting the EIM domain controller.
    - In the **Password** field, enter the password for the user.
    - In the **Confirm password** field, re-enter the password.
12. If you select **Kerberos principal and password**, provide the following information:
    - In the **Principal** field, enter the name of the Kerberos principal that identifies the user for OS/400 to use when contacting the EIM domain controller.
    - In the **Realm** field, enter the name of the Kerberos realm for the principal.
    - In the **Password** field, enter the password for the user.
    - In the **Confirm password** field, re-enter the password. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
13. If you select **Kerberos keytab file and principal**, provide the following information:
    - In the **Keytab file** field, enter the name of the keytab file name on the iSeries server that identifies the user for OS/400 to use when contacting the EIM domain controller. Or, you can click **Browse** to select the keytab file.
    - In the **Principal** field, enter the name of the Kerberos principal to be used to identify the user.
    - In the **Realm** field, enter the name of the Kerberos realm for the principal. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
14. Click **Verify Connection** to test the connection to the domain controller for system user that you just created.

15. Click **Next**.
16. In the **Summary** panel, review the configuration information that you have provided. If all information is correct, click **Finish**.

When the wizard finishes, you have finished your basic EIM configuration. However, you must complete these tasks to finalize your EIM configuration for this server:

1. “Add a domain to domain management” on page 31 that you created to the EIM Domain Management folder.
2. “Add a user registry” on page 35 to the EIM domain for other servers and applications that you want to participate in the EIM domain.
3. “Create an EIM identifier” on page 34 in the domain for each unique user or entity for systems participating in the EIM domain.
4. “Create an association” on page 32 between the various user identities of a person or entity to these EIM identifiers.

Additionally, you may want to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to “Configure a secure connection to the EIM domain controller”.

Configure a secure connection to the EIM domain controller

After you use the wizard to “Create and join a new domain” on page 25, you may want to use Secure Sockets Layer (SSL) or Transport Layer Security Protocol (TLS) to establish a secure connection to the EIM domain controller. To configure SSL or TLS for EIM, you must complete these tasks:

1. Enable SSL for the LDAP server domain controller.
2. Use Digital Certificate Manager (DCM) to a create the certificate that the LDAP server needs to use for SSL.
3. Use DCM to assign the certificate to the LDAP server.
4. Update EIM Configuration properties to specify that the iSeries server uses a secure SSL connection.
5. Update EIM Domain properties for each EIM domain to specify that EIM uses an SSL connection when managing the domain through iSeries Navigator.

Join an existing domain

You can use the EIM Configuration wizard to join an existing EIM domain. Use this option in the EIM Configuration wizard when an EIM domain and domain controller have already been configured in the network. As you work through the wizard you must supply information about the domain, including connection information to the EIM domain controller. The wizard stores this information on the iSeries server and then uses it to connect to the EIM domain controller. The wizard also creates an EIM user registry representing the OS/400 user profile registry on this iSeries server.

To use the wizard to complete this task, you must have Security Administrator (*SECADM) and All Object (*ALLOBJ) special authorities.

To start and use the EIM Configuration wizard to join an existing EIM domain, complete these steps using iSeries Navigator:

1. Expand **Network —> Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Configure...** to launch the EIM Configuration wizard. When the wizard starts, provide the following information as you work through the dialogs.
3. In the **Welcome** dialog of the wizard, select **Join an existing domain** and click **Next**.
4. If network authentication service is not currently configured on the iSeries server, the **Network Authentication Services Configuration** dialog displays. This dialog prompts you to select whether to configure network authentication service. If you select **Yes**, the Network Authentication Service Configuration Wizard launches. When you complete network authentication service configuration, the EIM Configuration wizard continues.

5. When the **Specify Domain Controller** dialog displays provide the following information:
   - In the **Domain controller name** field, specify the name of the system that serves as the domain controller for the EIM domain that you want the iSeries server to join.
   - Click **Use Secure Sockets Layer (SSL)** if you want EIM information retrieval from the domain controller to use SSL to protect the transmission of EIM data.
   - Click **Verify Connection** to test your domain controller configuration information.

Note: If you specified SSL to be used and you receive an error message, the message may indicate that the LDAP server has not been configured to use SSL.

   - Click **Next**.
6. On the **Specify User For Connection** dialog, select a **user type** for the connection. You can select one of the following types of users: Distinguished name and password, Kerberos keytab file and principal, or Kerberos principal and password. The two Kerberos user types are available only if network authentication service is configured for the local iSeries system. The user type that you select determines the other information that you must provide to complete the dialog, as follows:
   - If you select **Distinguished name and password**, provide the following information:
     - In the **Distinguished name** field, enter the LDAP distinguished name (DN) that identifies the user who is authorized to create objects in the local namespace of the LDAP server.
     - In the **Password** field, enter the password for the user.
     - In the **Confirm password** field, re-enter the password.
   - If you select **Kerberos keytab file and principal**, provide the following information:
     - In the **Keytab file** field, enter the name of the keytab file name on the iSeries server that identifies the user who is authorized to create objects in the local namespace of LDAP server. Or, you can click **Browse** to select the keytab file.
     - In the **Principal** field, enter the name of the Kerberos principal to be used to identify the user.
     - In the **Realm** field, enter the name of the Kerberos realm for the principal. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
   - If you select **Kerberos principal and password**, provide the following information:
     - In the **Principal** field, enter the name of the Kerberos principal that identifies the user who is authorized to create objects in the local namespace of the LDAP server.
     - In the **Realm** field, enter the name of the Kerberos realm for the principal.
     - In the **Password** field, enter the password for the user.
     - In the **Confirm password** field, re-enter the password. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
   - Click **Verify Connection** to test your user configuration information for connecting to the domain controller.
   - Click **Next**.
7. On the **Specify Domain** page, select the name of the domain that you want to join and click **Next**.
8. On the **Registry Information** page, select the type of user registries that you want to add to the EIM domain. Select one or both of these user registry types:
   - Select **OS400** to add a user registry that represents the local registry to the EIM domain. In the field provided, enter the name of the registry to be created in the domain. The EIM registry name is an arbitrary string that represents the registry type and specific instance of that registry.
   - Select **Kerberos** to add a Kerberos user registry to the EIM domain. In the field provided, enter the name of the registry to be created in the domain and select **Kerberos user identities are case sensitive** if necessary. You can accept the default value; the Kerberos registry name is the same

as the realm name. By using the same Kerberos registry name as the realm name, you can increase performance in retrieving information from the registry. For more information on how user registries can be defined within EIM, see “EIM registry definitions” on page 9.

- Click **Next**.

9. On the **Specify EIM System User** dialog, select the type of user that you want the system to use when performing EIM operations on behalf of operating system functions. These operations include mapping lookups and deleting associations when deleting a local OS/400 user profile. You can select one of the following types of users: Distinguished name and password, Kerberos keytab file and principal, or Kerberos principal and password. The user type that you select determines the other information that you must provide to complete the dialog as follows:
   - If you select **Distinguished name and password**, provide the following information:
     - In the **Distinguished name** field, enter the LDAP distinguished name that identifies the user for OS/400 to use when contacting the EIM domain controller.
     - In the **Password** field, enter the password for the user.
     - In the **Confirm password** field, re-enter the password.
   - If you select **Kerberos principal and password**, provide the following information:
     - In the **Principal** field, enter the name of the Kerberos principal that identifies the user for OS/400 to use when contacting the EIM domain controller.
     - In the **Realm** field, enter the name of the Kerberos realm for the principal.
     - In the **Password** field, enter the password for the user.
     - In the **Confirm password** field, re-enter the password. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
   - If you select **Kerberos keytab file and principal**, provide the following information:
     - In the **Keytab file** field, enter the name of the keytab file name on the iSeries server that identifies the user for OS/400 to use when contacting the EIM domain controller. Or, you can click **Browse** to select the keytab file.
     - In the **Principal** field, enter the name of the Kerberos principal to be used to identify the user.
     - In the **Realm** field, enter the name of the Kerberos realm for the principal.
   - Click **Verify Connection** to test the connection for system user that you just created.
   - Click **Next**.
10. In the **Summary** panel, review the configuration information that you have provided. If all information is correct, click **Finish**.

When the wizard finishes, you have finished your basic EIM configuration. However, you must complete these tasks to finalize your EIM configuration for this server:

1. “Add a domain to domain management” on page 31 that you joined to the EIM Domain Management folder.
2. “Add a user registry” on page 35 to the EIM domain for non-iSeries servers and applications that you want to participate in the EIM domain.
3. “Create an EIM identifier” on page 34 in the domain for each unique user or entity for systems participating in the EIM domain.
4. “Create an association” on page 32 between the various user identities of a person or entity to these EIM identifiers.

Also, to enable a single sign-on environment, you must configure network authentication service for the iSeries server.

Manage EIM

After you have configured EIM on your iSeries server, there are many tasks that you can perform to manage your EIM domain and information. The following topics discuss specific tasks used to manage EIM on your iSeries server and within your network enterprise.

“Manage EIM domains”
Work with the EIM information contained in your EIM domain and your EIM domain properties.

“Manage associations” on page 32
Maintain the associations of user identities to EIM identifiers for all users within the enterprise.

“Manage EIM identifiers” on page 33
Maintain the EIM identifiers associated with users in the enterprise.

“Manage EIM user authorities” on page 35
Maintain the security of your EIM information by working with the EIM authorities to control the EIM functions and operations that users can perform.

“Manage user registries” on page 35
Work with user registries that you have added to your EIM domain.

Manage EIM domains

You can use iSeries Navigator to manage all of your EIM domains. To manage any EIM domain, the domain must be listed in, or you must add it to, the Domain Management folder under the Network folder in iSeries Navigator. After you “Create and join a new domain” on page 25, you must add it to the Domain Management folder to manage the information in the domain.

You can use any iSeries connection to manage an EIM domain that resides anywhere in the same network. The iSeries that is connected to iSeries Navigator does not need to be participating in a domain to manage that domain.

You can complete the following tasks to manage your EIM domains:

- “Add a domain to domain management”
- “Connect to a domain”
- “Delete a domain” on page 32
- “Remove a domain from domain management” on page 32

Add a domain to domain management

To add a domain, you must have *SECADM special authority. To add an existing EIM domain to domain management, complete the following steps.

1. Expand **Network —> Enterprise Identity Mapping**.
2. Right-click **Domain Management** and select **Add Domain...**.
3. Specify the required domain and connection information.
4. Click **OK** to add the domain.

Connect to a domain

If you are not currently connected to the EIM domain in which you want to work, you must first connect to the domain. You may connect to an EIM domain even if your iSeries server is not currently configured to participate in this domain.

To connect to an EIM domain, complete the following steps:

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.

2. Select the domain to which you want to connect. If the domain with which you want to work is not listed, you need to "Add a domain to domain management" on page 31.
3. Right-click the EIM domain to which you want to connect and select **Connect...**.
4. Specify the user type and the required user information that should be used to connect to the EIM domain controller.
5. Click **OK**.

Delete a domain

To complete this task, you must have either LDAP administrator or EIM administrator authority. Before deleting an EIM domain, you must first remove all registries and EIM identifier information from the domain.

To delete an EIM domain, complete the following steps.

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Remove all user registries from the EIM domain.
3. Delete all EIM identifiers from the EIM domain.
4. Right-click the domain that you want to delete and select **Delete...**.
5. Click **Yes** on the **Delete Confirmation** dialog.

Remove a domain from domain management

While not required, you may remove an EIM domain from the Domain Management folder when you have finished making changes.

To remove a domain, complete the following steps:

1. Expand **Network —> Enterprise Identity Mapping**.
2. Right-click **Domain Management** and select **Remove Domain...**.
3. Select the EIM domain that you want to remove from domain management.
4. Click **OK** to remove the domain.

Manage associations

An "EIM associations" on page 12 defines a relationship between an "EIM identifier" on page 7 and a user identity within a registry. For example, you can create an association between an OS/400 user profile or a Kerberos principal and an EIM identifier. This association can then be used to determine which EIM identifier corresponds to a local iSeries user profile or Kerberos principal.

Maintaining the associations of user identities with the appropriate EIM identifiers is key to simplifying the administrative tasks required to keep track of which users have accounts on the various systems in the network.

Managing these associations also allows you to take advantage of "Single sign-on enablement through EIM" on page 21 in your network. You need to keep associations current when you implement a secure single sign-on network.

There are three types of associations that you can create: source, target, and administrative. To create or maintain associations between user identities to the appropriate EIM identifiers, you can perform one of the following tasks:

- "Create an association"
- "Delete an association" on page 33

Create an association

To enable a single sign-on environment you must create "EIM associations" on page 12 between the various user identities of a person or entity to a single "EIM identifier" on page 7 for that person or entity. You can create three types of association: target, source, and administrative.

To create a source or administrative association, you must have either identifier administrator authority or EIM administrator authority. To create a target association, you must have registry administrator for all registries, registry administrator for the specific registry, or EIM administrator authority.

To create an association for an EIM identifier, complete these steps:

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work.
   - If the EIM domain you want to work with is not listed under the Domain Management folder, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are now connected.
4. Click **Identifiers** to display the list of EIM identifiers.
5. Right-click the appropriate EIM identifier and select **Properties...**.
6. Click the **Associations** tab.
7. Click **Add...** to display the **Add association** dialog.
8. Click **Help** if you need more information to complete the fields.
9. When you have specified the required information, click **OK**.

Delete an association

To delete an administrative or source association, you must have identifier administrator authority or EIM administrator authority. To delete a target association, you must have administrator authority for selected registries (including the registry you want to work with), registry administrator authority, or EIM administrator authority.

To delete an association, complete the following steps.

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work:
   - If the EIM domain you want to work with is not listed under Domain Management, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are now connected.
4. Click **Identifiers**.
5. Right-click the EIM identifier that you want and select **Properties...** .
6. Click the **Associations** tab to display the current associations for the EIM identifier.
7. Select the association that you want to remove.
8. Click **Remove** to remove the associations.
9. Click **OK**.

Manage EIM identifiers

Maintaining the "EIM identifier" on page 7 that represent the users in your network is crucial for security purposes. Users within the enterprise are nearly always changing, with some coming, some going, and others moving between areas. Along with these changes comes the necessity to track the users' accounts and their access to systems within the network. Creating EIM identifiers and associating them with the user identities for each user makes this tracking task easier.

"Single sign-on enablement through EIM" on page 21 makes the task for users much easier as well when they move to another department or area within the enterprise. Their security clearance and system access needs may also have changed. Single sign-on enablement eliminates the need for these users to remember new user names and passwords for new systems.

Managing the EIM identifiers for your users within the enterprise involves many tasks that may be routine. You can use the following tasks to manage the EIM identifiers in your network and domains:

- "Create an EIM identifier"
- "Add an alias to an EIM identifier"
- "Delete an EIM identifier" on page 35

For information on managing associations, see the "Manage associations" on page 32 topic.

Create an EIM identifier

To create an EIM identifier, you must have either identifier administrator authority or EIM administrator authority.

To create an EIM identifier for a person or entity, complete these steps:

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work:
   - If the EIM domain you want to work with is not listed under **Domain Management**, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are now connected.
4. Right-click **Identifiers**, and select **New identifier...**.
5. Click **Help** if you need more information on any of the fields.
6. When you have specified the required information, click **OK**.

Add an alias to an EIM identifier

You may want to create an alias to provide additional distinguishing information for an "EIM identifier" on page 7. You, or others, can then use the alias to distinguish one EIM identifier from another. For example, if you have two users named John J. Johnson, you could create an alias of John Joseph Johnson for one and an alias of John Jeffrey Johnson to make it easier to distinguish the identity of each user.

To add an alias to an identifier, you must have either identifier administrator authority or EIM administrator authority.

To add an alias to an EIM identifier, complete these steps.

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work:
   - If the EIM domain you want to work with is not listed under Domain Management, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are connected.
4. Right-click the EIM identifier that you want and select **Properties**. If no EIM identifiers exist, see "Create an EIM identifier".
5. Specify the name of the alias you want to add to this EIM identifier and click **Add**.
6. Click **OK** to save the changes.

Delete an EIM identifier

To delete an EIM identifier, you must have EIM administrator authority.

WTo delete an EIM identifier, complete these steps:

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work:
   - If the EIM domain you want to work with is not listed under Domain Management, see “Add a domain to domain management” on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 31.
3. Expand the EIM domain to which you are now connected.
4. Click **Identifiers**.
5. Select one or more EIM identifiers to delete.
6. Right-click the selected EIM identifiers and select **Delete**.
7. Click **Yes** on the **Delete Confirmation** dialog to remove the selected EIM identifiers.

Manage EIM user authorities

EIM defines various EIM authorities that are needed to perform various operations within the domain. This includes domain management functions like creating identifiers, listing registries, and performing “EIM lookup operations” on page 15. Only users with EIM administrator authority are allowed to grant or revoke authorities for other users.

See “EIM authorities” on page 16 for brief definitions of each authority group and details on specific access each of these authorities have to certain EIM functions.

To change the EIM authorities for a user, follow these steps:

1. In iSeries Navigator, expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Expand the EIM domain in which you want to work. If you are not currently connected to this domain, you are prompted to connect. Ensure that you connect to the domain with a user authority that has EIM administrator authority.
3. Right-click the EIM domain and select **Authority...**.
4. On the **Edit EIM Authority** dialog, specify the user for which you are changing EIM authorities.
5. Click **OK**.
6. On the **Edit EIM Authority** dialog, make the necessary changes to the authorities for the user.
7. When you are finished, click **OK** to save the changes to the authorities.

Manage user registries

Before you can “Create an association” on page 32 between identities contained in user registries and the appropriate “EIM identifier” on page 7, you must first define the user registry to the EIM domain:

The following tasks are part of managing the user registries within the EIM domain.

- “Add a user registry”
- “Add an alias to a user registry” on page 36
- “Define a private user registry type in EIM” on page 36
- “Remove a user registry” on page 37
- “Remove an alias from a user registry” on page 38

Add a user registry

To add a user registry, you must have EIM administrator authority. For details on this authority and what a user with this authority can access, see “EIM authorities” on page 16.

To add a user registry to an EIM domain, complete these steps.

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Connect to the EIM domain with a user that has EIM administrator authority.
   - If the EIM domain you want to work with is not listed under the Domain Management folder, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are now connected.
4. Right-click **User Registries** and select **Add Registry...**.
5. Specify the required user registry information. You can also specify alias information for the user registry.
6. Click **OK** to save the information and add the user registry to the EIM domain.

Add an alias to a user registry

You, or an application developer, may want to create an alias to provide additional distinguishing information for a user registry. You, or others, can then use the alias to distinguish one user registry from another. For example, application developers and administrators use an alias on a user registry to communicate which EIM registries an application should use. For information on using aliasing with user registries, see "EIM registry definitions" on page 9.

To add an alias to a user registry, you must use one of the following authorities: EIM administrator, registry administrator for all registries, or registry administrator for the specific registry for which you are performing this task.

To add an alias to a user registry within an EIM domain, complete these steps:

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work:
   - If the EIM domain you want to work with is not listed under the Domain Management folder, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are now connected.
4. Click **User Registries** to display the list of registries within the domain.
5. Right-click the user registry to which you are adding an alias and select **Properties...**.
6. Click the **Alias** tab on the **Properties** dialog.
7. Specify the name and type of alias that you want to add. You may specify an alias type that is not included in the list of types.
8. Click **Add**.
9. Click **OK** to save the changes.

Define a private user registry type in EIM

To define a user registry type that EIM is not predefined to recognize, you must specify the registry type in the form of **ObjectIdentifier-normalization**, where **ObjectIdentifier** is a dotted-decimal object identifier, such as 1.2.3.4.5.6.7, and **normalization** is either the value **caseExact** or the value **caseIgnore**. For example, the object identifier (OID) for OS/400 is `1.3.18.0.2.33.2-caseIgnore`.

You should obtain any OIDs that you need from legitimate OID registration authorities to ensure that you create and use unique OIDs. Unique OIDs help you avoid potential conflicts with OIDs created by other organizations or applications.

There are two ways of obtaining OIDs:

- **Register the objects with an authority**.
  This method is a good choice when you need a small number of fixed OIDs to represent information. For example, these OIDs might represent certificate policies for users in your enterprise.
- **Obtain an arc assignment from a registration authority and assign your own OIDs as needed**. This method, which is a dotted-decimal object-identifier range assignment, is a good choice if you need a large number of OIDs, or if your OID assignments are subject to change. The arc assignment consists of the beginning dotted-decimal numbers from which you must base your **ObjectIdentifier**. For example, the arc assignment could be `1.2.3.4.5.`. You could then create OIDs by adding to this basic arc. For example, you could create OIDs in the form `1.2.3.4.5.x.x.x`).

You can learn more about registering your OIDs with a registration authority by reviewing these Internet resources:

- American National Standards Institute (ANSI) is the registration authority for the United States for organization names under the global registration process established by International Standards Organization (ISO) and International Telecommunication Union (ITU). A fact sheet with links to an application form is located at the ANSI Web site http://web.ansi.org/public/services/reg_org.html . The ANSI OID arc for organizations is 2.16.840.1. ANSI charges a fee for OID arc assignments. It takes approximately two weeks to receive the assigned OID arc from ANSI. ANSI will assign a number (NEWNUM), creating a new OID arc: 2.16.840.1.NEWNUM.
- In most countries or regions, the national standards association maintains an OID registry. As with the ANSI arc, these are generally arcs assigned under the OID 2.16. It may take some investigation to find the OID authority for a particular country or region. The addresses for ISO national member bodies may be found at http://www.iso.ch/addresse/membodies.html . The information includes postal address and electronic mail. In many cases, a Web site is specified as well.
- Another possible starting point is the International Register of ISO DCC NSAP schemes. NSAP stands for Network Service Access Point, and is used in various international standards. The registry for schemes may be obtained at http://www.fei.org.uk under the heading ISO DCC NSAP . The Web site currently lists contact information for 13 naming authorities, some of which will also assign OIDs.
- The Internet Assigned Numbers Authority (IANA) assigns private enterprise numbers, which are OIDs, in the arc 1.3.6.1.4.1. IANA has assigned arcs to over 7500 companies to date. The application page is located at http://www.iana.org/cgi-bin/enterprise.pl , under Private Enterprise Numbers. The IANA usually takes about one week. An OID from IANA is free. IANA will assign a number (NEWNUM) so that the new OID arc will be 1.3.6.1.4.1.NEWNUM.
- The U.S. Federal Government maintains the Computer Security Objects Registry (CSOR). The CSOR is the naming authority for the arc 2.16.840.1.101.3, and is currently registering objects for security labels, cryptographic algorithms, and certificate policies. The certificate policy OIDs are defined in the arc 2.16.840.1.101.3.2.1. The CSOR provides policy OIDs to agencies of the U.S. Federal Government. For more information about the CSOR, see http://csrc.nist.gov/csor/ .

For more information on OIDs for certificate policies, see http://csrc.nist.gov/csor/pkireg.htm .

Remove a user registry

Removal of a user registry from an EIM domain causes any associations with EIM identifiers for the user identities within the user registry to be lost. Adding the user registry back into the EIM domain after removing it does not reset the association relationships.

To remove a user registry, you must have EIM administrator authority.

To remove a user registry, complete the following steps:

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work.
   - If the EIM domain you want to work with is not listed under the Domain Management folder, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are now connected.
4. Click **User Registries** to display the list of user registries in the domain.
5. Right-click the user registry that you want to remove and select **Delete...**.
6. Click **Yes** on the **Confirmation** dialog to delete the user registry.

Remove an alias from a user registry

To remove an alias from a user registry, you must have registry administrator authority and administrator authority for selected registries (including the registry you want to work with), or EIM administrator authority.

To remove an alias from a user registry within an EIM domain, complete the following steps:

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. You must be connected to the EIM domain in which you want to work:
   - If the EIM domain you want to work with is not listed under the Domain Management folder, see "Add a domain to domain management" on page 31.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 31.
3. Expand the EIM domain to which you are now connected.
4. Click **User Registries** to display the list of registries within the domain.
5. Right-click the user registry for which you are removing an alias and select **Properties**.
6. Click the **Alias** tab on the **Properties** dialog.
7. Select the alias you want to remove and click **Remove**.
8. Click **OK** to save the changes.

APIs for EIM

EIM has multiple application programming interfaces (APIs) that applications can use to conduct EIM operations on behalf of the application or an application user. You can use these APIs to conduct identity mapping lookup operations, various EIM management and configuration functions, as well as information changes and query capabilities.

EIM APIs fall into multiple categories, as follows:

- EIM handle and connection operations
- EIM domain administration
- Registry operations
- EIM identifier operations
- EIM association management
- EIM mapping lookup operations
- EIM authorization management

Applications that use these APIs to manage or use the EIM information in an EIM domain typically adhere to the following programming model:

1. Get an EIM handle

2. Connect to an EIM domain
3. Normal application processing
4. Use an EIM administration or EIM identity mapping lookup operation API
5. Normal application processing
6. Before ending, destroy the EIM handle

For detailed information and a complete list of the EIM APIs available for the iSeries server, see the Enterprise Identity Mapping (EIM) APIs topic.

Troubleshoot EIM

EIM is composed of multiple technologies and many applications and functions. Because there are many paths that can be taken to troubleshoot problems, the following topics contain detailed information and instructions about how to troubleshoot or fix some of the common errors that you may encounter, such as:

- "Unable to connect to domain controller"
- "List of EIM identifiers takes a long time"
- "EIM Configuration wizard hangs during finish processing" on page 40
- "EIM handle is no longer valid" on page 40
- "Kerberos authentication and diagnostic messages" on page 40

Unable to connect to domain controller

A number of factors can contribute to connection problems when trying to connect to the domain controller. Check the following items to help find the cause of the problem:

- Verify that the information specified for the following items are correct:
  - Domain controller name
  - Specified port
  - User ID and password
- Verify that the domain controller is active. If the domain controller is an iSeries server, you can use iSeries Navigator and follow these steps:
  1. Expand **Network —> Servers —> TCP/IP**.
  2. Verify that the Directory Server has a status of **Started**. If the server is stopped, right-click **Directory Server** and select **Start...**

Once the domain controller is active, try reconnecting to the domain.

1. Expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Select the domain to which you want to connect. If no EIM domains are listed or the EIM domain you want to work with is not listed under the Domain Management folder, you need to "Add a domain to domain management" on page 31.
3. Right-click the EIM domain to which you want to connect and select **Connect...**.
4. Specify the user type and the required user information that should be used to connect to the EIM domain controller.
5. Click **OK**.

List of EIM identifiers takes a long time

When opening the Identifiers folder in iSeries Navigator, it may take a long time for the list of identifiers to be generated. You may want to narrow the search criteria for displaying the list of EIM identifiers if you have a large number of EIM identifiers in your domain.

To customize the view for EIM identifiers, follow these steps:

1. In iSeries Navigator, expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Expand the domain in which you want to display the EIM identifiers.
3. Right-click **Identifiers** and select **Customize this view —> Include...**.
4. Specify the display criteria that you want. The asterisk (*) character may be used as a wildcard character.
5. Click OK.

The next time you click **Identifiers**, the EIM identifiers displayed are only those that match the criteria that you specified. If you want to view all EIM identifiers, use the steps above and select **All Identifiers** as your customized view option.

EIM Configuration wizard hangs during finish processing

If the wizard appears to hang during finish processing, the wizard may be waiting for the domain controller to start. Verify that no errors occurred during the startup of the LDAP server. For iSeries servers, check the job log for the QDIRSRV job in the QSYSWRK subsystem.

To check the job log, follow these steps:

1. In iSeries Navigator, expand **Work Management —> Subsystems —> Qsyswrk**.
2. Right-click **Qdirsrv** and select **Job Log**.

EIM handle is no longer valid

While managing EIM through iSeries Navigator, if the user receives an error indicating that the EIM handle is no longer valid, the connection to the domain controller has been lost.

To reconnect to the domain controller, follow these steps:

1. In iSeries Navigator, expand **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Right-click the domain that you want to work with and select **Reconnect...**.
3. Specify the connection information.
4. Click **OK**.

Kerberos authentication and diagnostic messages

When using the Kerberos protocol for authentication with EIM, diagnostic message CPD3E3F is written to the job log whenever the authentication or identity mapping operations fail. 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.

Refer to the help information associated with the diagnostic message to begin troubleshooting the problem.

Related information for EIM

You may want to learn about other technologies that are related to EIM. The following Information Center topics can help you understand these related technologies:

- **Network authentication service**
  This topic provides information on configuring network authentication service on the iSeries. Network authentication service allows an iSeries to participate in an existing Kerberos network. When used with EIM, network authentication service provides single sign-on for a network.
- **Directory Services (LDAP)**
  This topic provides configuration and conceptual information for Directory Services (LDAP). EIM uses the LDAP server to store EIM data and mapping associations.

Printed in U.S.A.