IBM

eserver

iSeries

Enterprise Identity Mapping

IBM

eserver

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 more easily managing and working with 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 used by applications to query this information. In addition, OS/400^{R} exploits EIM and Kerberos capabilitiesto provide a single sign-on environment.

GUI interfaces and wizards are provided through iSeries Navigator for configuring and managing EIM. You can also manage Enterprise Identity Mapping 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 Enterprise Identity Mapping:

“Print this topic”
Print this topic and other related topics.

“What is EIM?” on page 2
Find out what EIM is and how it works.

“Single sign-on enablement through EIM” on page 11
Read about the benefits EIM provides in simplifying user sign-on.

“Prepare for EIM” on page 13
Ensure that you have all of the required services and applications configured before you configure EIM.

“Configure EIM” on page 15
Use the EIM configuration wizard to get started with EIM.

“Manage EIM” on page 22
Manage EIM properties along with EIM domains, user registries, EIM user authorities, and more.

“APIs for EIM” on page 31
Utilize the EIM APIs in your applications and network.

“Troubleshoot EIM” on page 32
Find solutions to common problems and errors that may occur when using EIM in your network.

Print this topic

To view or download the PDF version, select Enterprise Identity Mapping (about 280 KB or 42 pages).

You can view or download these related topics:

- Network authentication services (about 199 KB or 50 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 directory server, which you can use as an EIM domain controller, along with information on 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) .

What is EIM?

In today's heterogeneous networks with partitioned servers and multiple platforms, administrators, users, and application developers all have to cope with the complexities that multiple user identities for individual users create within an enterprise. Users have to remember each user ID and password for each system they use. Administrators must perform password resets, attempt to synchronize user IDs and passwords, and track every system in the network to which each individual has access. Application developers are often forced to use non-secure techniques to solve the problem of diverse platforms or to invest large amounts of money in writing applications that implement their own user registries and associated security semantics.

These problems quickly become a large administrative problem for all of those involved. Enterprise Identity Mapping (EIM) provides an infrastructure that lowers the expense for application developers because they can easily and inexpensively build applications that participate in a single sign-on environment, regardless of platform. OS/400's exploitation of EIM and Kerberos, along with exploitation by other e(logo)Server and IBM software, provides "Single sign-on enablement through EIM" on page 11 capabilities at the operating system layer in addition to the application layer. Single sign-on capabilities provide users, administrators, and application developers with the benefits of easier password and user identity management across multiple platforms — without forcing administrators to use multiple sets of security controls for a single resource.

How does EIM work?

EIM is comprised of multiple technologies that work together to further the security of your network in many ways. The problem of having large numbers of users, each with multiple user names and passwords to remember for multiple systems that they use regularly, is very common for most network administrators and users. In many cases, most users will attempt to set all of their passwords the same for the ease of remembering them all. This further compromises the security of the network, even though it may reduce the number of user account password resets done by the administrator!

EIM and single sign-on enablement provide a solution to both of these issues. This solution works on multiple system platforms and eliminates the need for the user to sign-on or authenticate to each and every system they need to access.

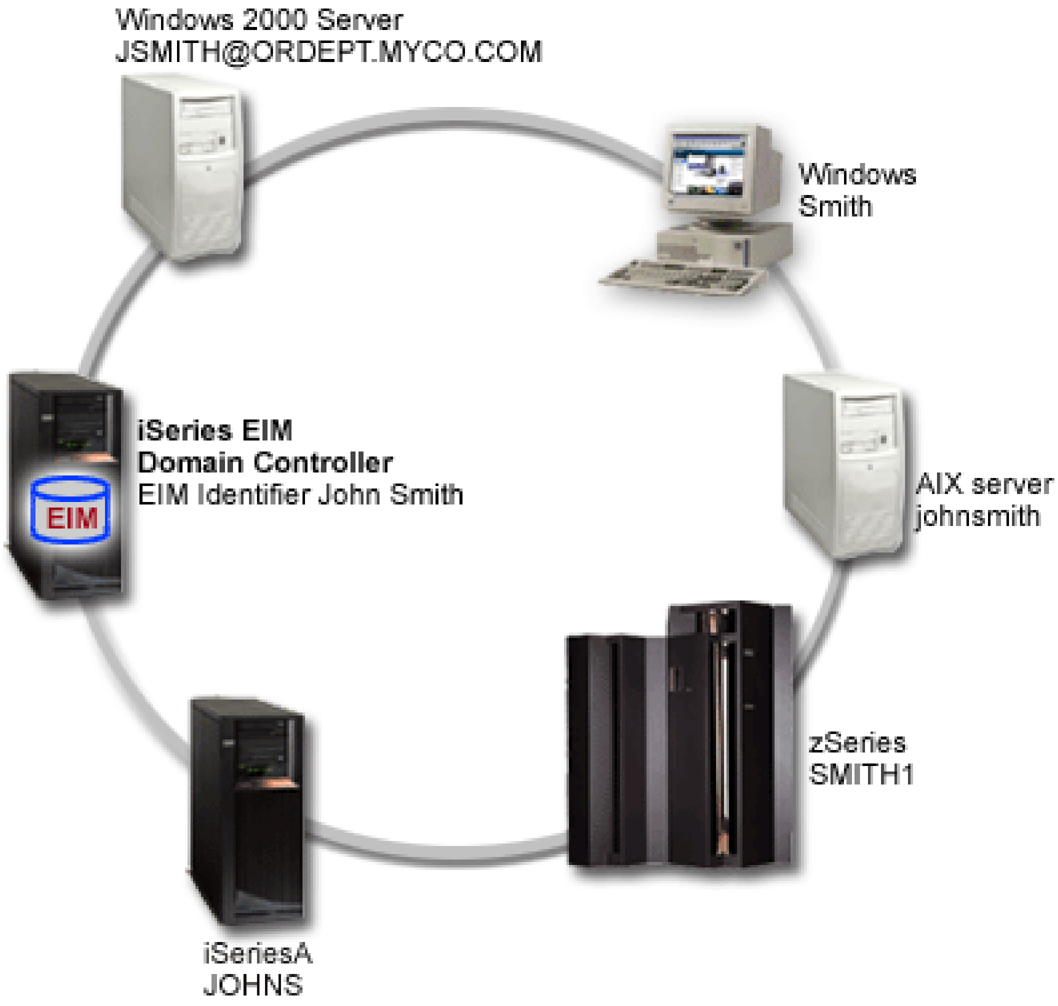
EIM domain

An EIM domain is much like a typical network domain except that the domain controller not only controls the access to the domain, but also stores all of the EIM data for that domain. By participating in an EIM domain, these systems can also participate in the single sign-on environment.

The following diagram shows that these systems are participating in the EIM domain:

- Windows^R 2000 server (configured as the Kerberos KDC)
- Windows^R PC
- AIX server
- zSeries^{TM} server
- iSeries server
- LDAP Directory Server (configured as the "EIM domain controller" on page 7)

Figure 1. Example EIM domain



To be able to participate in the EIM domain, you configure EIM on each system. To participate in the single sign-on environment, you must also configure network authentication service on each system. You then add the appropriate system or application user registries to the EIM domain and create EIM identifiers to represent each user in EIM.

User registries and EIM identifiers

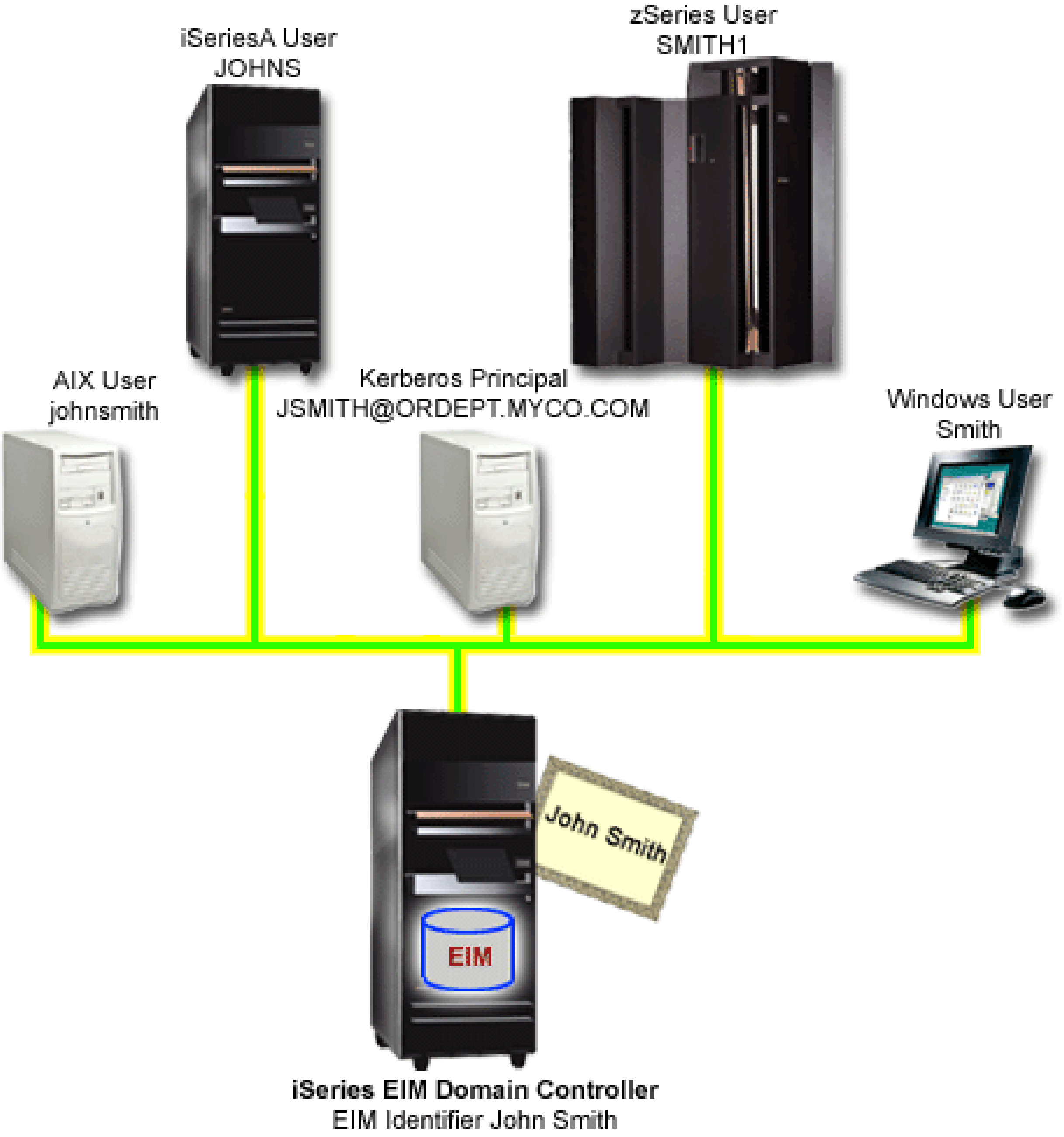
You use EIM to tie together the “User registry” on page 11 of the various systems and applications within your network. By creating an “EIM identifier” on page 7 for each user and associating the various “User identity” on page 10 for each user to his or her respective EIM identifier, the single sign-on solution is made possible.

The following diagram describes an example user, John Smith, who has user identities on the these systems in the EIM domain:

- **AIX server:** johnsmith
- **iSeriesA server:** JOHNS
- **zSeries server:** SMITH1
- **Windows NT/2000 PC:** Smith
- **Windows 2000 server (Kerberos KDC):** JSMITH

John’s EIM identifier, John Smith, represents him as a person in EIM and the various user identities he has on these five systems can then be mapped to, or “EIM identity mapping association” on page 8 with, his EIM identifier to establish the relationship between them.

Figure 2. EIM identifier and associated user identities



You associate John's user identities with the EIM identifier by using different "EIM identity mapping association" on page 8. The types of associations that you create affect the way in which the associated user identity can be used in EIM. For example, the iSeriesA server is highly secure and you want to restrict John's access to the system so that he must authenticate directly to the server. To do this, you create an administrative association between the John Smith EIM identifier and the JOHNS user identity on iSeriesA. With this type of association, you can see that John Smith owns an account on iSeriesA, but EIM cannot return information about this identity in a "Identity mapping lookup operation" on page 9.

Having created the needed EIM identifiers and associations, your systems and users are ready to participate in a single sign-on environment. To learn more about how single sign-on enablement works and how it can benefit you, see "Single sign-on enablement through EIM" on page 11

See “EIM terminology” to familiarize yourself with the various terms used in this document.

EIM terminology

Multiple technologies are incorporated into Enterprise Identity Mapping functions. Although some EIM terminology may be familiar to you, some of the EIM terminology and other terms common to the various technologies may be new to you.

The following terms have been defined in detail and examples are included where appropriate. Understanding these terms will help you plan and implement EIM capabilities and single sign-on enablement.

Alias

You can create one or more aliases for an “EIM identifier” on page 7 or a “User registry” on page 11 to provide additional information by which the identifier or registry is known. Aliases can be used to help find a specific EIM identifier or user registry during a search or “Identity mapping lookup operation” on page 9. An alias does not have to be unique within the EIM domain because it is additional information, not an actual object name.

You can “Add an alias to a user registry” on page 29 either for an EIM identifier or for a user registry.

An EIM identifier alias supplies more information about the person or entity that the EIM Identifier name represents.

A user registry alias is used to separate and distinguish the user registry names that an administrator creates from user registry names that applications use. When an administrator creates a user registry, the administrator should specify an alias for it. The type of alias the administrator specifies varies based on how the alias is meant to identify the registry. For example, the alias could be the TCP/IP address of the system. Applications can then use the TCP/IP address and the eimGetRegistryFromAlias() API to determine from which registry to obtain the correct user ID for the application to run under.

Application developers and administrators use an alias on a user registry to communicate which EIM registries an application should use. Typically, the application provider defines application specific aliases; for example, APP1_SOURCE_REGISTRY or some other distinguishing information. The application provider documents which aliases the application searches for to find the EIM registry name that the application developer needs to use for source and target registries. The application then uses the appropriate EIM API to search for a registry with the specified alias. Alternatively, the application developer could tell the administrator to choose the alias names (or the EIM registry name) and to add that information to an application configuration file.

EIM authorities

EIM authorities describe and provide authorization for an EIM user to perform specific administrative tasks or “Identity mapping lookup operation” on page 9. Only users with EIM administrator authority are allowed to grant or revoke authorities for other users. EIM authorities are granted to users identities that are known to EIM. These user identities can be LDAP distinguished names or Kerberos principals.

How you “Manage EIM user authorities” on page 26 determines which users can perform the actions needed to use EIM functions.

EIM domain controller

The EIM domain controller is an LDAP directory server that is configured to manage, and control access to, all EIM data for an EIM domain.

The EIM domain controller can be either local or remote. A domain controller is considered to be local when it is configured on the same system that you are using to conduct EIM operations. A domain controller is considered to be remote when it is configured on a different server, separate from the server you are using to conduct EIM operations.

You perform all “Manage EIM domains” on page 22 through the EIM domain controller.

EIM identifier

An EIM identifier represents an actual person or entity in EIM. When you create an EIM identifier, you associate it with the “User identity” on page 10 for that person or entity. Using these “EIM identity mapping association” on page 8, or identity mappings, helps you simplify the administrative task of keeping track of all of the user IDs that a person or entity has in the enterprise.

For example, your company has a security policy that requires that users on certain systems have a unique user ID that is not used on other systems. Consequently, Mary A. Jones has two different user IDs for accessing various systems. One of these is MAJONES and the other is JONESMA. Using EIM, you can create a single identifier that represents a single user or entity, such as Mary A. Jones, in the enterprise. You can then associate user identities on different platforms or in different user registries (for example, OS/400 or Kerberos registries) to this single EIM identifier. These associations, or identity mappings, can then be used to enable a “Single sign-on enablement through EIM” on page 11.

EIM identifiers can have a description, which can further define the person or entity it represents. You can also create “Alias” on page 6 for the EIM identifiers, which can aid in locating a specific EIM identifier when performing a “Identity mapping lookup operation” on page 9.

Quite often different individuals within an enterprise share the same name, which can be confusing if you are using proper names as EIM identifiers. EIM identifier names must be unique within the EIM domain. Using aliases, the EIM administrator can ensure that EIM identifier names are unique and can provide additional information about the individual to which the EIM identifier belongs. This information can also be used in a mapping lookup operation.

For example, the EIM identifiers for two people named John S. Smith might be **John S. Smith1** and **John S. Smith2**. The alias for **John S. Smith1** could be **John Samuel Smith** and the alias for **John S. Smith2** could be **John Steven Smith**.

Each EIM identifier can have multiple aliases that can be used to identify which John S. Smith the EIM identifier is representing. 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 department number, job title, or another distinguishing attribute.

EIM identity mapping association

A single sign-on enabled environment is made possible by associating the various user identities of a person or entity to a single “EIM identifier” on page 7 for that person or entity. By associating all of a person’s user identities with that person’s corresponding EIM identifier, applications and operating system functions can then use EIM APIs to map from an authenticated ID in one user registry to a different ID in another user registry that represents the same person.

You can create three different types of associations between a user identifier and an EIM identifier: source, target, and administrative.

Source association

This type of association indicates that this “User identity” on page 10 (ID) can be used as the source in a “Identity mapping lookup operation” on page 9 to find the EIM identifier it is associated with, or to find another user ID that has a target association with the EIM identifier. A user ID with only a source association will not be returned as the target of a mapping lookup operation. Identities that are used only for authentication, such as Kerberos principals, should have source associations. Therefore, Kerberos principals will normally have source associations only.

Target association

This type of association indicates that the user ID can be returned as the result of a mapping lookup operation. This type of association cannot be used as the source ID in a “APIs for EIM” on page 31 mapping lookup operation. If a target association is used as the source ID, no associated identities will be returned. Identities that are not used for authentication purposes should have target associations. OS/400 user profiles very often have target associations with EIM identifiers.

A single user ID may have both a target and a source associations with an EIM identifier. Having both types of associations for a user ID can be very useful. For example, sometimes a single user identity is used for both authentication and authorization. This may be because the user sometimes logs into a Windows platform, but also is required to sometimes log into OS/400 directly. In this case, the OS/400 user profile is sometimes used as a source identity (when logging into OS/400 directly) and sometimes as a target identity (when logging into, for example, a Windows platform). This is most likely to be the case for individuals that act as administrators. User profiles that represent typical end users will normally only need a target association.

Administrative association

An administrative association with an EIM identifier is typically used to show that the person or entity represented by the EIM identifier owns a user ID within a specified system or application user registry which requires special treatment. This type of association may be used, for example, in conjunction with highly sensitive user registries that the administrator does not want to be used in a single sign-on environment. For example, the user registry is part of a classified computer system that is not allowed to participate in a single sign-on environment. However, when viewing a person’s associated identities, the administrator wants to be able to see all of the user’s identities in the enterprise; not just those that are used in mapping lookup operations.

Due to the nature of what an administrative association represents, a mapping lookup operation that uses a user ID with an administrative association returns no results. Similarly, a user ID with an administrative association will never be returned as the result of mapping lookup operations.

For example, John Smith has one user ID on System A and another user ID on System B. Because System B is highly secure, the system administrator wants to force users to authenticate to the system by using the system’s local user registry only. He does not want to allow EIM or an application to indirectly authenticate John Smith to the system. By using an administrative association for Mr. Smith’s user ID on System B, the EIM administrator can see that John Smith owns an account on System B, but EIM will not return information about this identity in the mapping lookup operations. Even if applications exist on this system that exploit EIM mapping lookup operations, they will find no user identities that have administrative associations.

How you “Manage associations” on page 23 between user identities and the appropriate EIM identifiers is the key to simplifying the tasks that you perform to administer users within your enterprise.

Identity mapping lookup operation

An identity mapping lookup operation is conducted by an application that uses the appropriate “APIs for EIM” on page 31 (eimGetTargetFromSource() or eimGetTargetFromIdentifier() APIs). By allowing the operating system and applications to perform a mapping lookup operation to access this information at run-time, the operating system and applications can easily use one “User registry” on page 11 for authentication while using an entirely different user registry for authorization.

For example, John Smith has an “EIM identifier” on page 7 of **John Smith** and four user identities in the enterprise that are associated with the EIM identifier:

- **johnsmith** in Kerberos realmZ - has a source association
- **jsmith** in iSeries 1 - has a target association
- **jsmith** in iSeries 2 - has a target association
- **jss** in system A (which is highly secure) - has an administrative association

John typically logs into a Windows 2000 platform. By default, Windows 2000 uses Kerberos for authentication. Therefore, an application can be written that runs on Windows 2000 and accesses data from both the iSeries servers, in addition to any windows platform in the domain, without ever prompting John to specify his user profile or password.

The application passes a Kerberos ticket to the iSeries 1 server which accepts the Kerberos ticket and conducts an EIM mapping lookup operation. This operation allows the operating system to map from the **johnsmith** Kerberos identity to the EIM identifier, **John Smith**, and then from the EIM identifier to his **jsmith** identity on iSeries 1. The mapping lookup operation is conducted using one EIM API.

GSS APIs are used at the server for accepting and authenticating the Kerberos ticket. The application or operating system interface that is running on the iSeries server maps to the local user identity by using an EIM API. The application or operating system then performs the request on behalf of that identity by using the swap APIs provided by the operating system; thus utilizing the security semantics of iSeries server.

By using the different types of EIM “EIM identity mapping association” on page 8, the administrator can also control if applications can use mapping lookup operations to find the associated user identities. A source association can be used as the source in an EIM mapping lookup operation. A target association can be returned as the result of a mapping lookup operation. And an administrative association indicates that a user identity is associated with an EIM identifier, but cannot be used in EIM mapping lookup operations.

For example, the system administrator for highly secure System A wants to force applications on System A to use that system’s user registry for authentication and authorization. The EIM administrator, therefore, creates an administrative association between the **jss** user identity and the **John Smith** EIM identifier, rather than a target association. Applications that attempt to perform a mapping lookup operation from an external user identity to a local user identity will not find the local **jss** user identity.

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. The EIM wizard configures the iSeries Directory Server (LDAP server) to store the EIM Domain information. You can use LDAP distinguish 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 11.

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 the example above, `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 Directory server to store EIM data, you can use LDAP distinguished names as a means of authenticating to the "EIM domain controller" on page 7. 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 Directory server. If the Directory server has not been configured previously, you can configure the directory 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 Directory server's local namespace.
- Use the EIM configuration wizard to select the type of user the system should 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. 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, and so forth.

To learn more about distinguished names and how LDAP uses them, see LDAP basics in the Information Center.

LDAP parent distinguished name

An LDAP parent distinguished name (DN) is an entry in a Lightweight Directory Access Protocol (LDAP) directory server's namespace. LDAP directory entries are arranged in a hierarchical structure that reflects political, geographic, organizational, or domain boundaries. A distinguished name is considered a parent DN when the DN is at the highest level of the directory server's 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 the example above, `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 Directory server to store EIM data, you use LDAP distinguished names as a means of authenticating to the "EIM domain controller" on page 7. You also use LDAP "LDAP distinguished name" on page 9 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 distinguished name (DN) for the domain that you are creating. Specifying a parent DN allows you to 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 LDAP uses them, see LDAP basics in the Information Center.

User identity

A user identity (ID) is an entry in a "User registry" on page 11. This entry is typically a string of alphanumeric characters, unique within the registry, that is used to represent a specific person or entity to a system or application.

User IDs are associated with an “EIM identifier” on page 7, which represents a person or entity within the enterprise.

When you add a user registry to an EIM domain, you can “Create association” on page 24 between the user identities in the user registry and the appropriate “EIM identifier” on page 7 that represent the users or entities within the network.

User registry

A user registry contains a set of entries that represents a set of “User identity” on page 10 an operating system or an application either knows or trusts, or both. The set of user identities can be a complete system user registry or a subset of a system user registry that is used with a particular application. A list of users defined for CICS^R in a particular RACF user registry is an example of such an application registry.

When a user registry is created for an operating system to use; for example, the list of OS/400 user profiles on a particular iSeries server, this type of user registry is referred to as a *system user registry* within EIM. When a user registry is created for a particular application to use, this type of user registry is referred to as an *application user registry* within EIM. The majority of user registries that you work with in EIM are system user registries.

These user registry types are predefined in EIM:

- OS/400
- AIX^R
- Kerberos
- Kerberos - case sensitive
- LDAP
- RACF^R
- Windows^R 2000
- Novell Directory Services
- Policy Director

Among other “Manage user registries” on page 28, administrators can define other user registry types that they want to use with EIM. When EIM recognizes the definition of a user registry type, you can add specific instances of user registries to the EIM domain.

Single sign-on enablement through EIM

Enterprise Identity Mapping (EIM) provides the mechanics for inexpensive cross-platform single sign-on enablement. OS/400 exploitation of EIM and Kerberos provides a true multi-tier, heterogeneous single sign-on environment. There are multiple benefits for users, administrators, and application developers alike when a single sign-on environment is available in an enterprise.

Benefits for users
With single sign-on, authentication occurs only once when users sign into the network. Using EIM reduces the need for users to keep track of and manage multiple user names and passwords to access other systems in the network. 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 may cache passwords to different systems, which can compromise the security of the entire network. Adminstrators spend their time and money on solutions to diminish these security risks. Single sign-on reduces the administrative overhead in managing authentication while helping to keeping the entire network secure. Additionally, single sign-on reduces the administrative

costs of resetting forgotten passwords. Administrators can set up a single sign-on environment where a Windows (R) (for Windows 2000 and later releases) sign-on that allows access to the entire network, thus minimizing authentication and identification management.

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

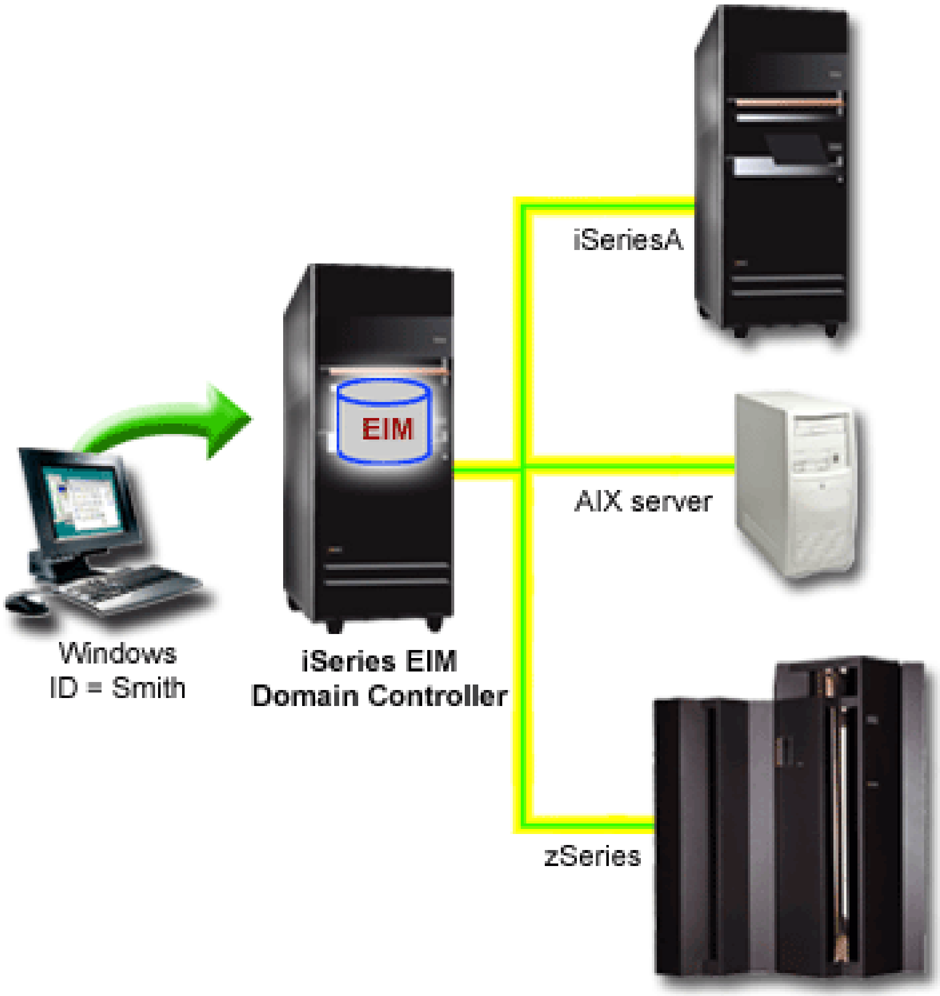
iSeries enablement of single sign-on

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

While network authentication service allows 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 username, 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 diagram 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 username. These applications can look up the association to John's EIM identifier to find the OS/400 username. 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 these technologies to allow users in his company's Order Receiving Department to use iSeries Access for Windows (R) to connect to OS/400 and other systems without the user ever being prompted to re-enter any user ID and password and without the use of cached user IDs and passwords.

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

- iSeries Navigator
- PC5250 Emulator
- DRDA(R)
- NetServer
- QFileSvr.400

Prepare 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 Enterprise Identity Mapping and single sign-on capabilities.

Making the initial decisions on the type of environment that you currently have in your network and the security measures that you need helps you to better understand the way in which EIM and single sign-on capabilities can enhance your network and systems security. Additional benefits of carefully planning your EIM configuration are ease of use for your users and a thorough understanding how EIM can help minimize the administrative and application programming costs of maintaining systems and network security.

The services that are required to be installed on the iSeries server prior to installing EIM are listed in the following planning worksheet. Use this worksheet to aid in configuring Enterprise Identity Mapping.

Prerequisite checklist	**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 (used to work with iSeries servers) and on your iSeries servers?	
Is the Network subcomponent of iSeries Navigator installed on all the PCs in your network and your iSeries systems?	
If Directory Services (LDAP) is currently configured and you want to use this LDAP server as the EIM domain controller, do you know the LDAP administrator distinguished name (DN) and password?`	
If Directory Services (LDAP) is currently configured, can the directory server be stopped temporarily? (This will be required in order to complete the EIM configuration process.)	
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	
Have you applied the latest program temporary fixes (PTFs)?	

Optional checklist	**Answers**
Do you want to use or are you currently using Kerberos authentication in your network?	
If you are using or want to use Kerberos authentication in your network, do you have network authentication service configured on all of your iSeries servers?	

If you are configuring Network authentication service and Enterprise Identity Mapping for the first time, see the example scenario Enable single sign-on for a detailed example of planning and configuration information that is used in a fictitious company setting.

Install required iSeries Navigator options

To configure and use Enterprise Identity Mapping (EIM) and network authentication service (Kerberos) successfully to enable a single sign-on environment, you must install both the Network option and the Security option of iSeries Navigator. If you do not plan to use network authentication service (Kerberos authentication) 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 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 screen. On the **Component Selection** dialog, expand **iSeries Navigator**, 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 Enterprise Identity Mapping (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 11. A single sign-on environment is beneficial for users and administrators in multiple ways. Users have fewer user names and passwords to try to remember 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 enablement through EIM" on page 11 across multiple platforms without the need to change underlying security policies, you must configure Enterprise Identity Mapping (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 a Directory server configured or 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 begin to enjoy the benefits of a single sign-on environment. For example, you must have configured Network authentication service for the iSeries server and you must also create identifiers and associations in EIM.

Before you use the EIM configuration wizard, you should have completed all "Prepare for EIM" on page 13 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 16
Choose this task to create an EIM domain for your network and configure the iSeries server to participate in it. The wizard creates the new domain and configures the local directory server to be the EIM "EIM domain controller" on page 7 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 (Kerberos) configuration wizard. After you complete this task, you can configure other iSeries

servers to participate in the domain. You do so by connecting to the server that you want to configure and using the EIM configuration wizard to join an existing domain.

"Join an existing domain" on page 19
Once you use the EIM wizard to configure a domain controller and an EIM domain in your network, 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. As you work through the wizard you must supply information about the domain being joined, including connection information (such as port # and whether to use TLS/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 (Kerberos) 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 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 29 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 25 in the domain for each unique user or entity for systems participating in the EIM domain.
3. "Create association" on page 24 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 Directory server on the iSeries server to be the EIM "EIM domain controller" on page 7 for a new domain. If necessary, the EIM configuration wizard ensures that you provide basic configuration information for the Directory server.

Also, if Kerberos is not currently configured on the iSeries server, the wizard prompts you to launch the Network authentication service (Kerberos) 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 task also configures the local directory 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. When the wizard starts, provide the following information as you work through the dialogs:
3. In the **Welcome** dialog of the wizard, select **Create and join a new domain** and click **Next**.
4. If Kerberos 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 (Kerberos). If you select **Yes**, the Kerberos configuration wizard launches. When you complete Kerberos configuration, the EIM configuration wizard continues.
5. If the local Directory server is not currently configured, the **Configure Directory Server** dialog displays. Provide the following information on the dialog to configure the local Directory server:
   - In the **Port** field, accept the default port number *389*, or enter a different port number to use for non-secure EIM communications with the directory server.
   - In the **Distinguished name** field, enter the LDAP distinguished name (DN) that identifies the LDAP administrator for the directory server. The EIM configuration wizard creates this LDAP administrator DN for the Directory server and uses it to configure the Directory 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 distinguished name (DN) for the domain that you are creating. Specifying a parent DN allows you to 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. 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 what 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 Directory server's local namespace. If you used this wizard to configure the Directory 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 Directory server's local namespace. 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 value principal@realm is used in conjunction with the keytab file to uniquely identify the Kerberos user.

- 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 Directory server's local namespace.
  – 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 value principal@realm is used in conjunction with the password to uniquely identify the Kerberos user.
- 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" on page 11 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 what 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 OS functions related to single sign-on and deleting user profiles may fail.

- 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 value principal@realm is used in conjunction with the password to uniquely identify the Kerberos user.
- 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 value principal@realm is used in conjunction with the keytab file to uniquely identify the Kerberos user.
- Click **Verify Connection** to test your EIM system user configuration information for connecting to the domain controller.
- Click **Next**.

11. 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 23 that you created to the EIM Domain Management folder.
2. "Add a user registry" on page 29 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 25 in the domain for each unique user or entity for systems participating in the EIM domain.
4. "Create association" on page 24 between the various user identities of a person or entity to these EIM identifiers.

Also, to begin enjoying the benefits of a single sign-on environment, you must you must configure Network authentication service for the iSeries server.

Additionally, you may want to use Secure Sockets Layer (SSL) or Transport Layer Security Protocol (TLS) to **"Use a secure connection to the EIM domain controller"**.

Use a secure connection to the EIM domain controller

After you use the wizard to "Create and join a new domain" on page 16, 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 Directory server domain controller.
2. Use Digital Certificate Manager (DCM) to create the certificate that the Directory server needs to use for SSL.
3. Use DCM to assign the certificate that you create to the Directory services application.
4. Update EIM Configuration folder properties to specify that the iSeries system use an SSL connection when doing operating system functions.
5. Update EIM Domain folder properties for each EIM domain to specify that EIM use 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. Choosing this wizard task is the best choice 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 and create an EIM user registry representing the OS/400 user profile registry on this iSeries system.

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 from within iSeries Navigator:

Note: This wizard task also configures the local Directory 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. 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 Kerberos 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 (Kerberos). If you select **Yes**, the Kerberos configuration wizard launches. When you complete Kerberos 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 Directory 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 what 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 Directory server's local namespace.
     - 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 Directory server's local namespace. 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 value principal@realm is used in conjunction with the keytab file to uniquely identify the Kerberos user.
   - 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 Directory server's local namespace.
     - 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 value principal@realm is used in conjunction with the password to uniquely identify the Kerberos user.
   - Click **Verify Connection** to test your user configuration information for connecting to the domain controller.

- Click **Next**.

7. On the **Specify Domain** panel, select the name of the domain that you want to join and click **Next**.
8. 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” on page 11 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. Having the Kerberos registry name match the realm name can increase performance in retrieving information from the registry.
   - 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 what other information that you must provide to complete the dialog, as follows:

Note: The user the you specify must, at a minimum, be a member of the mapping lookup operation group in EIM in order for this system to participate in single sign-on. Also, the user should be a member of the EIM group that allows management of EIM associations for identities in the local user registry. This ensures that the user can manage associations for local user profiles through iSeries Navigator. If the user that you specify does not have these privileges, then certain OS functions related to single sign-on and deleting user profiles may fail until you add the user to these EIM groups.

   - 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 value principal@realm is used in conjunction with the password to uniquely identify the Kerberos user.
   - 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 value principal@realm is used in conjunction with the keytab file to uniquely identify the Kerberos user.

- Click **Verify Connection** to test your EIM system user configuration information for connecting to the domain controller.
- 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 23 that you joined to the EIM Domain Management folder.
2. "Add a user registry" on page 29 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 25 in the domain for each unique user or entity for systems participating in the EIM domain.
4. "Create association" on page 24 between the various user identities of a person or entity to these EIM identifiers.

Also, to begin enjoying the benefits of a single sign-on environment, you must 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 23
Maintain the associations of user identities to EIM identifiers for all users within the enterprise.

"Manage EIM identifiers" on page 25
Maintain the EIM identifiers associated with users in the enterprise.

"Manage EIM user authorities" on page 26
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 28
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 Enterprise Identity Mapping (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 16, you must add it to the Domain management folder in order 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 to which iSeries Navigator is connected need not be participating in a domain in order to manage that domain.

The following are routine tasks that you may need to conduct in managing your EIM domains.

- "Add a domain to Domain Management" on page 23

- “Connect to a domain”
- “Delete a domain”
- “Remove a domain from Domain Management”

Add a domain to Domain Management

In order to complete this task, 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 no EIM domains are listed or the EIM domain you want work with is not listed under Domain Management, you need to “Add a domain to Domain Management”.
3. Right-click the EIM domain to which you want to connect and select **Connect...**
4. Specify the user type and required user information to be used to connect to the EIM domain controller.
5. Click **OK**.

Delete a domain

In order to complete this task, you must have either LDAP administrator or EIM administrator authority. Deleting an EIM domain requires that you first remove all registry 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 are done making changes. To do this, 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 identity mapping association” on page 8 defines a relationship between an “EIM identifier” on page 7 and a user identity (ID) 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 11 in your network. Keeping associations current is important when you want to implement a secure single sign-on network.

There are three types of "EIM identity mapping association" on page 8 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.

See the following informtion to manage associations.

- "Create association"
- "Delete an association"

Create association

To enable a single sign-on environment you must create "EIM identity mapping association" on page 8 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 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 Domain Management, see "Add a domain to Domain Management" on page 23.
   - If you are not currently connected to the EIM domain in which you want to work, see "Connect to a domain" on page 23.
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 in order to complete the fields.
9. When you have specified the required information, click **OK**.

Delete an association

Delete an association

In order to delete an administrative or source association, you must have Identifier administrator or EIM administrator authority. To delete a target association, you must have Administrator for selected registries (including the registry you want to work with), Registry administrator, 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 23
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
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 user’s accounts and access to systems within the network. Creating EIM identifiers and associating them with the “User identity” on page 10 for each user make this tracking task much more simple.

“Single sign-on enablement through EIM” on page 11 makes the task for the user much easier as well if they are moving 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 them to have to try and remember new usernames and passwords for new systems.

Managing the EIM identifiers for your users within the enterprise involves many tasks that may be routine. The following are tasks that you can use 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 26

For information on managing associations, see the “Manage associations” on page 23 topic.

Create an EIM identifier

In order to complete this task, you must have either Identifier administrator or EIM administrator authority. To create an EIM identifier for a person or entity, 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 23.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
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” on page 6 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 clarify the identity of each user.

In order to complete this task, you must have either Identifier administrator or EIM administrator authority. To add an alias to an EIM identifier, 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 23.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
3. Expand the EIM domain to which you have connected.
4. Right-click the EIM identifier that you want and select **Properties**. If no EIM identifiers exist, see “Create an EIM identifier” on page 25.
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

In complete this task, you must have EIM administrator authority. To 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 23.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
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” on page 7 that are needed in order to perform various operations within the domain. This includes domain management functions like creating identifers, listing registries, and perfoming “Identity mapping lookup operation” on page 9. Only users with EIM administrator authority are allowed to grant or revoke authorities for other users. The following table displays the relationships between the different EIM user authorities and the EIM operations allowed for each authority group.

To modify 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 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 modifying 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.

For brief overviews of each authority group, see “EIM user authority descriptions” on page 28.

The following table displays each EIM operation, the different EIM authorities, and defines which authorities can perform certain EIM operations.

Note: The LDAP administrator authority is not listed in the following table. However, this authority is required to “Create and join a new domain” on page 16. LDAP administrators have EIM administrator authorities, but EIM administrators do not automatically have LDAP administrator authorities.

EIM Operation	EIM Administrator	Identifier administrator	EIM Mapping Operations	Registry administrator	Administrator for selected registries
Create Domain**	-	-	-	-	-
Delete Domain	X	-	-	-	-
Modify Domain	X	-	-	-	-
Search for Domains	X	-	-	-	-
Add System Registry	X	-	-	-	-
Add Application Registry	X	-	-	-	-
Remove Registry	X	-	-	-	-
Modify Registry	X	-	-	X	X
Search for Registries	X	X	X	X	X
Add Identifier	X	X	-	-	-
Remove Identifier	X	-	-	-	-
Modify Identifier	X	X	-	-	-
Search for Identifiers	X	X	X	X	X
Retrieve Associated Identifiers	X	X	X	X	X
Add/Remove Administrative Association	X	X	-	-	-
Add/Remove Source Association	X	X	-	-	-
Add/Remove Target Association	X	-	-	X	X
Search for Associations	X	X	X	X	X
Retrieve Target Association from Source Association	X	X	X	X	X
Retrieve Target Association from Identifier	X	X	X	X	X
Modify Registry Users	X	-	-	X	X
Search for Registry Users	X	X	X	X	X
Modify Registry Alias	X	-	-	X	X
Search for Registry Aliases	X	X	X	X	X

EIM Operation	EIM Administrator	Identifier administrator	EIM Mapping Operations	Registry administrator	Administrator for selected registries
Retrieve Registry from Alias	X	X	X	X	X
Add/Remove EIM authority	X	-	-	-	-
Display authority group members	X	-	-	-	-
Display EIM authorities for a specified user	X	-	-	-	-
Query EIM authority	X	-	-	-	-
****** Only users with LDAP administrator authority can create a new EIM domain.					

EIM user authority descriptions

The following are brief overviews of the functions that each EIM authority group can perform.

EIM administrator
Allows the user to manage all of the EIM data within this EIM domain. This authority is required in order to delete user registries from the EIM domain. The EIM administrator authority does not have the ability to create EIM domains. LDAP administrator authority is required to create or delete a user registry.

Registry administrator
Allows the user to add and modify user registries, add and remove target associations, and to search for and retrieve association information, including EIM identifiers in all registries. This authority does not encompass the ability to remove user registries.

Identifier administrator
Allows the user to add and modify EIM identifiers, manage source and administrative associations, and to search for and retrieve association information, including EIM identifiers in all registries.

EIM mapping operations
Allows the user to conduct mapping lookup operations and to search for and retrieve user registry information.

Administrator for selected registries
Allows the user to manage registry users and target associations in the specified registries only, add and remove target associations, and to search for and retrieve associations and EIM identifiers.

Manage user registries

Before you can “Create association” on page 24 between identities contained in “User registry” on page 11 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” on page 29
- “Add an alias to a user registry” on page 29
- “Define a private user registry type in EIM” on page 29
- “Remove a user registry” on page 30
- “Remove an alias from a user registry” on page 31

Add a user registry

To complete this task, you must have EIM administrator “Manage EIM user authorities” on page 26. 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 Domain Management, see “Add a domain to Domain Management” on page 23.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
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” on page 6 to provide additional distinguishing information for a “User registry” on page 11. 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.

In order to complete this task, you must 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 Domain Management, see “Add a domain to Domain Management” on page 23.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
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 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” on page 11 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 (OID), such as 1.2.3.4.5.6.7, and **normalization** is either the value **caseExact** or the value **caseIgnore**. For example, the 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. Doing so ensures that you create and use unique OIDs which helps you avoid potential OID conflicts with OIDs created by other organizations or applications.

There are two ways of obtaining OIDs:

- **Register the objects with an authority**.
  Registering your OIDs with an authority is a good choice, for example, 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**.
  Obtaining an arc assignment, 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:

- ANSI is the registration authority for the United States for organization names under the global registration process established by ISO and 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 thirteen 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 7,500 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

Removing a user registry from an EIM domain will cause 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 will not reset the association relationships.

In order to complete this task, 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 Domain Management, see “Add a domain to Domain Management” on page 23.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
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

In order to complete this task, you must have Registry administrator, Administrator 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 Domain Management, see “Add a domain to Domain Management” on page 23.
   - If you are not currently connected to the EIM domain in which you want to work, see “Connect to a domain” on page 23.
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

Enterprise Identity Mapping (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 modification 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 utilize 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 mapping lookup operation API

5. Normal application processing
6. Before ending, destroy the EIM handle

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

Troubleshoot EIM

Enterprise Identity Mapping is composed of multiple technologies and many applications and functions. Because there are many avenues that can be taken to troubleshoot problems, the following topics contain detailed information and instructions on how to further troubleshoot or fix some of the common errors that you may encounter.

“Unable to connect to domain controller”

“List EIM identifiers takes a long time”

“EIM configuration wizard hangs during finish processing” on page 33

“EIM handle is no longer valid” on page 33

“Kerberos authentication and diagnostic messages” on page 33

Unable to connect to domain controller

There are a number of factors that 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 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 work with is not listed under Domain Management, you need to “Add a domain to Domain Management” on page 23.
3. Right-click the EIM domain to which you want to connect and select **Connect...**
4. Specify the user type and required user information to be used to connect to the EIM domain controller.
5. Click **OK**.

List 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 * 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 EIM 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 directory 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 thru 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 in conjunction with EIM, a diagnostic message, CPD3E3F, is written to the joblog 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 text associated with the diagnostic message to begin troubleshooting the problem.

Printed in U.S.A.