



System i
Security
Enterprise Identity Mapping

Version 6 Release 1





System i
Security
Enterprise Identity Mapping

Version 6 Release 1

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 123.

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

© Copyright International Business Machines Corporation 2002, 2008. All rights reserved.

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

Contents

Enterprise Identity Mapping 1

| | |
|---|----|
| What's new for V6R1 | 1 |
| PDF file for Enterprise Identity Mapping | 2 |
| Enterprise Identity Mapping overview | 2 |
| Enterprise Identity Mapping concepts | 5 |
| EIM domain controller | 5 |
| EIM domain | 6 |
| EIM identifier | 8 |
| EIM registry definitions | 11 |
| System registry definitions | 13 |
| Application registry definitions | 13 |
| Group registry definitions | 14 |
| EIM associations | 15 |
| Lookup information | 15 |
| Identifier associations | 16 |
| Policy associations | 20 |
| Default domain policy associations | 20 |
| Default registry policy associations | 22 |
| Certificate filter policy associations | 23 |
| EIM lookup operations | 26 |
| Lookup operation examples: Example 1 | 28 |
| Lookup operation examples: Example 2 | 29 |
| Lookup operation examples: Example 3 | 31 |
| Lookup operation examples: Example 4 | 32 |
| Lookup operation examples: Example 5 | 33 |
| EIM mapping policy support and enablement | 35 |
| EIM access control | 36 |
| EIM access control group: API authority | 39 |
| EIM access control group: EIM task authority | 41 |
| LDAP concepts for EIM | 44 |
| Distinguished name | 44 |
| Parent distinguished name | 45 |
| LDAP schema and other considerations for EIM | 46 |
| Enterprise Identity Mapping concepts for i5/OS | 47 |
| i5/OS user profile considerations for EIM | 47 |
| i5/OS auditing for EIM | 48 |
| EIM enabled applications for i5/OS | 48 |
| Scenarios: Enterprise Identity Mapping | 49 |
| Planning for Enterprise Identity Mapping | 49 |
| Planning Enterprise Identity Mapping for eServer | 49 |
| Enterprise Identity Mapping setup requirements for eServer | 49 |
| Identifying needed skills and roles | 51 |
| Planning an Enterprise Identity Mapping domain | 53 |
| Planning an Enterprise Identity Mapping domain controller | 54 |
| Developing an Enterprise Identity Mapping registry definition naming plan | 57 |
| Developing an identity mapping plan | 58 |
| Planning Enterprise Identity Mapping associations | 59 |
| Developing an EIM identifier naming plan | 61 |
| Enterprise Identity Mapping implementation planning worksheets | 62 |

| | |
|--|----|
| Planning for Enterprise Identity mapping application development | 64 |
| Planning Enterprise Identity Mapping for i5/OS | 65 |
| EIM installation prerequisites for i5/OS | 65 |
| Installing required System i Navigator options | 66 |
| Backup and recovery considerations for EIM | 66 |
| Backup and recovery of EIM domain data | 66 |
| Backup and recovery of EIM configuration information | 67 |
| Configuring Enterprise Identity Mapping | 67 |
| Creating and joining a new local domain | 68 |
| Finalize your EIM configuration for the domain | 72 |
| Creating and joining a new remote domain | 73 |
| Finalize your EIM configuration for the domain | 77 |
| Joining an existing domain | 78 |
| Finalize your EIM configuration for the domain | 82 |
| Configuring a secure connection to the EIM domain controller | 83 |
| Managing Enterprise Identity Mapping | 84 |
| Managing Enterprise Identity Mapping domains | 84 |
| Adding an EIM domain to the Domain Management folder | 84 |
| Connecting to an EIM domain | 85 |
| Enabling policy associations for a domain | 85 |
| Testing EIM mappings | 86 |
| Working with test results and resolving problems | 87 |
| Removing an EIM domain from the Domain Management folder | 88 |
| Deleting an EIM domain and all configuration objects | 88 |
| Managing Enterprise Identity Mapping registry definitions | 89 |
| Adding a system registry definition | 89 |
| Adding an application registry definition | 90 |
| Adding a group registry definition | 90 |
| Adding an alias to a registry definition | 91 |
| Defining a private user registry type in EIM | 91 |
| Enabling mapping lookup support and the use of policy associations for a target registry | 93 |
| Deleting a registry definition | 94 |
| Removing an alias from a registry definition | 94 |
| Adding a member to a group registry definition | 95 |
| Managing Enterprise Identity Mapping identifiers | 95 |
| Creating an EIM identifier | 96 |
| Adding an alias to an EIM identifier | 96 |
| Removing an alias from an EIM identifier | 97 |
| Deleting an EIM identifier | 97 |
| Customizing the EIM identifiers view | 98 |
| Managing EIM associations | 98 |
| Creating EIM associations | 99 |

| | |
|---|-----|
| Creating EIM identifier association | 99 |
| Creating a policy association | 100 |
| Adding lookup information to a target user identity | 106 |
| Add lookup information to a target user identity in an identifier association | 106 |
| Add lookup information to a target user identity in a policy association | 107 |
| Removing lookup information from a target user identity. | 108 |
| Remove lookup information for a target user identity in an identifier association | 108 |
| Displaying all identifier associations for an EIM identifier | 109 |
| Displaying all policy associations for a domain | 110 |
| Displaying all policy associations for a registry definition | 110 |

| | |
|---|-----|
| Deleting an identifier association | 111 |
| Deleting a policy association | 112 |
| Managing EIM user access control | 113 |
| Managing EIM configuration properties | 113 |
| Troubleshooting Enterprise Identity Mapping. | 114 |
| Troubleshooting domain controller connection problems | 115 |
| Troubleshooting general EIM configuration and domain problems | 116 |
| Troubleshooting EIM mapping problems | 117 |
| Enterprise Identity Mapping APIs | 120 |
| Related information for Enterprise Identity Mapping | 121 |

Appendix. Notices 123

| | |
|-------------------------------|-----|
| Trademarks | 125 |
| Terms and conditions. | 125 |

Enterprise Identity Mapping

Enterprise Identity Mapping (EIM) for the System i[™] platform is the i5/OS[®] implementation of an IBM[®] infrastructure that allows administrators and application developers to solve the problem of managing multiple user registries across their enterprise.

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. EIM enables inexpensive solutions for easier management of multiple user registries and user identities in your enterprise.

EIM allows you to create a system of identity mappings, called associations, between the various user identities in various user registries for a person in your enterprise. EIM also provides a common set of APIs that can be used across platforms to develop applications that can use the identity mappings that you create to look up the relationships between user identities. In addition, you can use EIM in conjunction with network authentication service, the i5/OS implementation of Kerberos, to provide a single sign-on environment.

You can configure and manage EIM through System i Navigator, the System i graphical user interface. The System i platform uses EIM to enable i5/OS interfaces to authenticate users by means of network authentication service. Applications, as well as i5/OS, can accept Kerberos tickets and use EIM to find the user profile that represents the same person as the Kerberos ticket represents.

To learn more about how EIM works, about EIM concepts, and about how you can use EIM in your enterprise review the following:

What's new for V6R1

Read about new or significantly changed information for the Enterprise Identity Mapping (EIM) topic collection.



New or enhanced functions for EIM

- In previous releases of i5/OS EIM only supported mapping to one local user identity per system. In i5/OS V6R1 EIM supports selecting from multiple local user identity mappings for the same system, using the IP address of the target system to select the correct local user identity mapping on that system.

Additionally, the topic Single sign-on was updated and provides documentation about implementing EIM as part of a single sign-on environment to decrease password management. This topic provides a number of detailed scenarios of common single sign-on situations with detailed configuration instructions for implementing them.

How to see what's new or changed

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

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

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

PDF file for Enterprise Identity Mapping

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

To view or download the PDF version of this document, select Enterprise Identity Mapping (about 1820 KB).

You can view or download these related topic PDFs:


- Network authentication services (about 1398 KB) contains information about how to configure network authentication service in conjunction with EIM to create a single sign-on environment.
- IBM Tivoli® Directory Server for i5/OS (LDAP) (about 1700 KB) contains information about how to configure the LDAP server, which you can use as an EIM domain controller, along with information about advanced LDAP configuration.

Saving PDF files

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

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

Downloading Adobe® Reader

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

Enterprise Identity Mapping overview

Enterprise Identity Mapping (EIM) can help you solve problems that occur when you try to manage more than one user registry.

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

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

The problem of managing multiple user registries

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

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

Current approaches

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

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

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

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

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

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

The EIM approach

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

For example, given a person's user identity in one user registry, you can determine which user identity in another user registry represents that same person. If the user has authenticated with one user identity and you can map that user identity to the appropriate identity in another user registry, the user does not

need to provide credentials for authentication again. You know who the user is and only need to know which user identity represents that user in another user registry. Therefore, EIM provides a generalized identity mapping function for the enterprise.

EIM allows one-to-many mappings (in other words, a single user with more than one user identity in a single user registry). However, the administrator does not need to have specific individual mappings for all user identities in a user registry. EIM also allows many-to-one mappings (in other words, multiple users mapped to a single user identity in a single user registry).

The ability to map between a user's identities in different user registries provides many benefits. Primarily, it means that applications may have the flexibility of using one user registry for authentication while using an entirely different user registry for authorization. For example, an administrator could map a Windows® user identity in a Kerberos registry to an i5/OS user profile in a different user registry to access i5/OS resources to which the i5/OS user profile is authorized.

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

EIM, used in conjunction with network authentication service, the i5/OS implementation of Kerberos, provides a single sign-on solution. Applications can be written that use GSS APIs and EIM to accept Kerberos tickets and map to another, associated user identity in a different user registry. The association between user identities that provides this identity mapping can be accomplished by creating identifier associations that indirectly associate one user identity with another through an EIM identifier or by creating policy associations that directly associate one user identity in a group with a single specific user identity.

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

1. Configure an EIM domain in the network. You can use the EIM Configuration wizard to create a domain controller for the domain and configure access to the domain. When you use the wizard you can choose to create a new EIM domain and create a domain controller on the local system or a remote system. Or, if an EIM domain already exists, you can choose to participate in an existing EIM domain.
2. Determine which users defined to the directory server that hosts the EIM domain controller are allowed to manage or access specific information in the EIM domain and assign them to appropriate EIM access control groups.
3. Create EIM registry definitions for those user registries that will participate in the EIM domain. Although you can define any user registry to an EIM domain, you must define user registries for those applications and operating systems that are EIM-enabled.
4. Based on your EIM implementation needs, determine which of the following tasks to perform to complete your EIM configuration:
 - Create EIM identifiers for each unique user in the domain and create identifier associations for them.
 - Create policy associations.
 - Create a combination of these.

Related information

Single sign-on overview

Enterprise Identity Mapping concepts

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

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

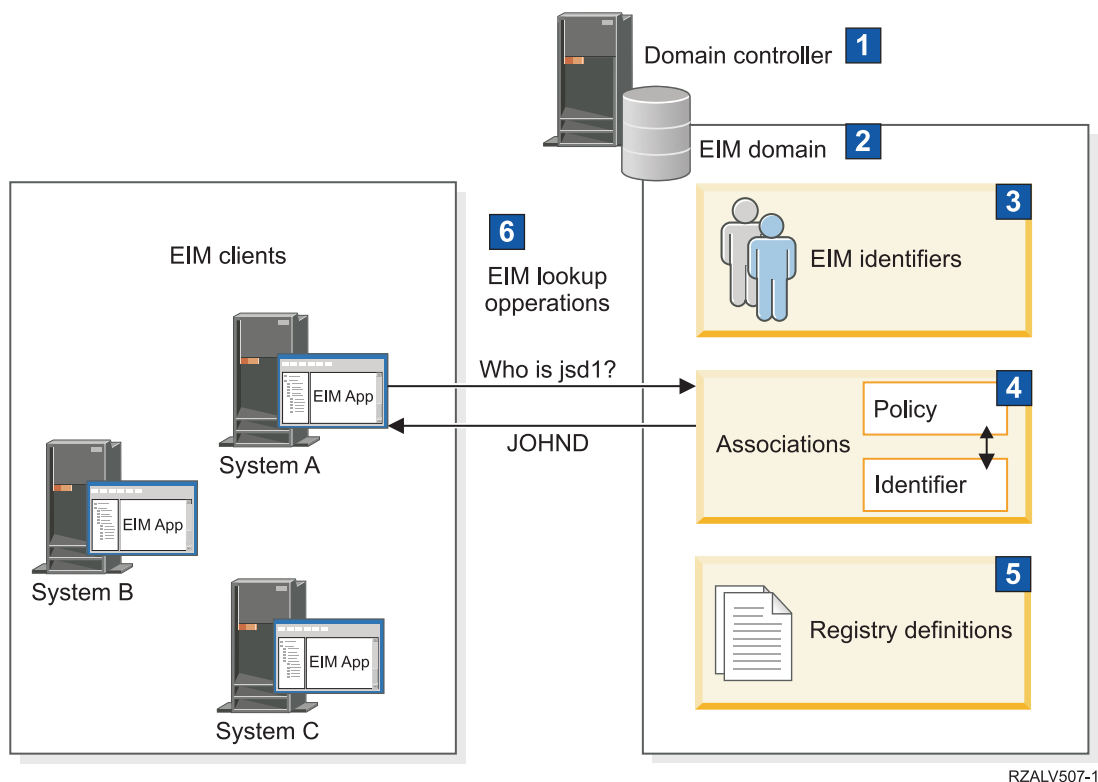


Figure 1. An EIM implementation example

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

EIM domain controller

An EIM domain controller is a Lightweight Directory Access Protocol (LDAP) server that is configured to manage one or more EIM domains. An EIM domain consists of all the EIM identifiers, EIM associations, and user registries that are defined in that domain. Systems (EIM clients) participate in the EIM domain by using the domain data for EIM lookup operations.

Currently, you can configure the IBM Tivoli Directory Server for i5/OS on some IBM eServer platforms to act as an EIM domain controller. Any system that supports the EIM APIs can participate as a client in the domain. These client systems use EIM APIs to contact an EIM domain controller to perform. The location of the EIM client determines whether the EIM domain controller is a local or remote system. The domain controller is *local* if the EIM client is running on the same system as the domain controller. The domain controller is *remote* if the EIM client is running on a separate system from the domain controller.

Note: If you plan to configure a directory server on a remote system, the directory server must provide EIM support. EIM requires that the domain controller be hosted by a directory server that supports Lightweight Directory Access Protocol (LDAP) Version 3. Additionally, the directory server product must be configured to accept the EIM schema. The IBM Tivoli Directory Server for i5/OS provides this support.

Related concepts

“EIM lookup operations” on page 26

An application or an operating system uses an EIM API to perform a lookup operation so that the application or operating system can map from one user identity in one registry to another user identity in another registry. An EIM lookup operation is a process through which an application or operating system finds an unknown associated user identity in a specific target registry by supplying some known and trusted information.

“LDAP schema and other considerations for EIM” on page 46

Use this information to learn what is required for the directory server to function with Enterprise Identity Mapping (EIM).

EIM domain

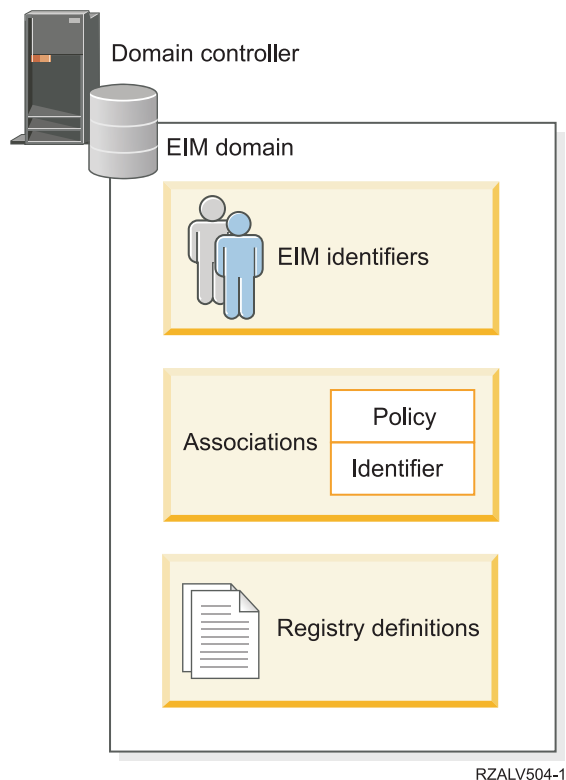
An Enterprise Identity Mapping (EIM) domain is a directory within a Lightweight Directory Access Protocol (LDAP) server that contains EIM data for an enterprise.

An EIM domain is the collection of all the EIM identifiers, EIM associations, and user registries that are defined in that domain, as well as access control for the data. Systems (EIM clients) participate in the domain by using the domain data for EIM lookup operations.

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

In contrast, an EIM domain *refers* to user identities that are defined in user registries. An EIM domain contains information about the *relationship* between identities in various user registries (user name, registry type, and registry instance) and the actual people or entities that these identities represent.

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



RZALV504-1

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

EIM data includes:

EIM registry definitions

Each EIM registry definition that you create represents an actual user registry (and the user identity information it contains) that exists on a system within the enterprise. Once you define a specific user registry in EIM, that user registry can participate in the EIM domain. You can create two types of registry definitions, one type refers to system user registries and the other type refers to application user registries.

EIM identifiers

Each EIM identifier that you create uniquely represents a person or entity (such as a print server or a file server) within an enterprise. You can create an EIM identifier when you want to have one-to-one mappings between the user identities that belong to a person or entity to whom the EIM identifier corresponds.

EIM associations

The EIM associations that you create represent relationships between user identities. You must define associations so that EIM clients can use EIM APIs to perform successful EIM lookup operations. These EIM lookup operations search an EIM domain for defined associations. There are two different types of associations that you can create:

Identifier associations

Identifier associations allow you to define a one-to-one relationship between user identities through an EIM identifier defined for an individual. Each EIM identifier association that you create represents a single, specific relationship between an EIM identifier and an associated user identity within an enterprise. Identifier associations provide the information that ties an EIM identifier to a specific user identity in a specific user registry and allow you to create one-to-one identity mapping for a user. Identity associations are especially useful when individuals have user identities with special authorities and other privileges that you want to specifically control by creating one-to-one mappings between their user identities.

Policy associations

Policy associations allow you to define a relationship between a group of user identities in one or more user registries and an individual user identity in another user registry. Each EIM policy association that you create results in a many-to-one mapping between the source group of user identities in one user registry and a single target user identity. Typically, you create policy associations to map a group of users who all require the same level of authorization to a single user identity with that level of authorization.

Related concepts

“EIM registry definitions” on page 11

An Enterprise Identity Mapping (EIM) registry definition is an entry within EIM that you create to represent an actual user registry that exists on a system within the enterprise. A user registry operates like a directory and contains a list of valid user identities for a particular system or application.

“EIM identifier”

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

“EIM lookup operations” on page 26

An application or an operating system uses an EIM API to perform a lookup operation so that the application or operating system can map from one user identity in one registry to another user identity in another registry. An EIM lookup operation is a process through which an application or operating system finds an unknown associated user identity in a specific target registry by supplying some known and trusted information.

EIM identifier

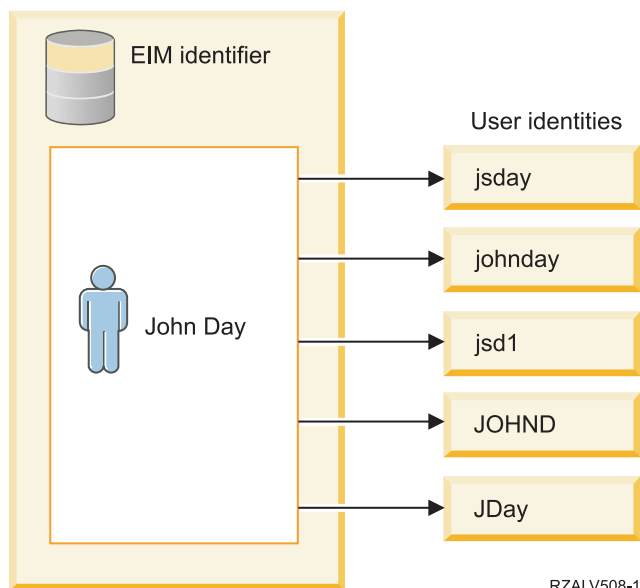
An Enterprise Identity Mapping (EIM) identifier represents a person or entity in an enterprise. A typical network consists of various hardware platforms and applications and their associated user registries. Most platforms and many applications use platform-specific or application-specific user registries.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

You can use EIM to create unique EIM identifiers for people or entities in your enterprise. You can then create identifier associations, or one-to-one identity mappings, between the EIM identifier and the various user identities for the person or entity that the EIM identifier represents. This process makes it easier to build heterogeneous, multiple-tier applications. It also becomes easier to build and use tools that simplify the administration involved with managing every user identity that a person or entity has within the enterprise.

EIM identifier representing a person

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

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

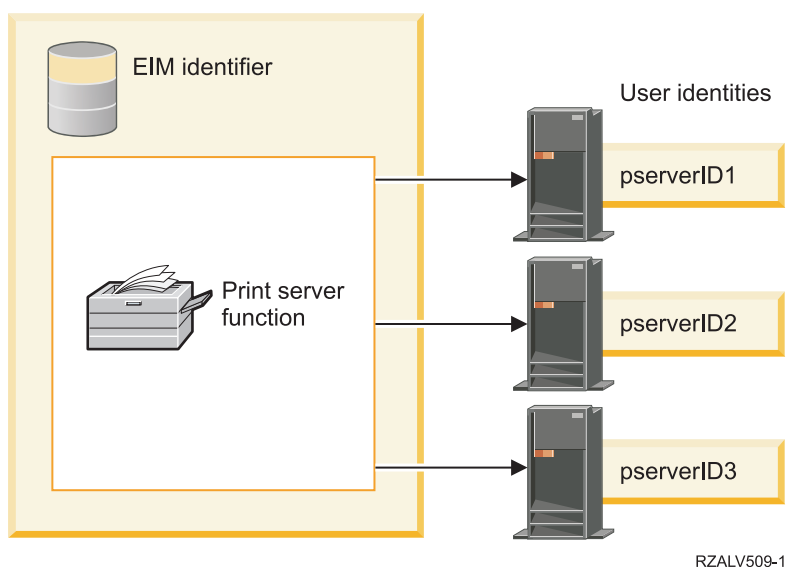


In EIM, you can create associations that define the relationships between the John Day identifier and each of the different user identities for *John Day*. By creating these associations to define these relationships, you and others can write applications that use the EIM APIs to look up a needed, but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

EIM identifier representing an entity

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

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



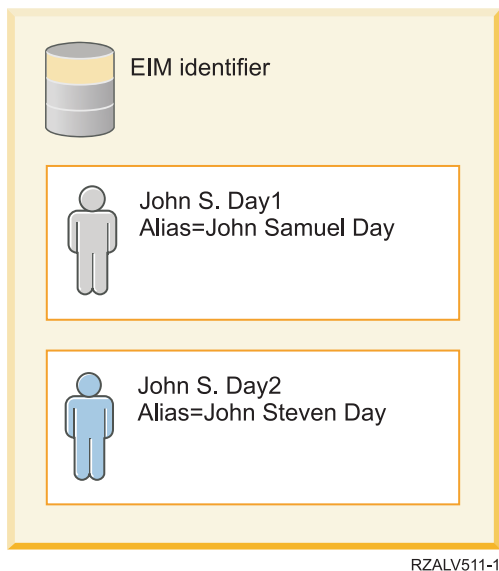
With EIM, you can create a single identifier that represents the print server function within the entire enterprise. As the example shows, the EIM identifier Print server function represents the actual print server function entity in the enterprise. Associations are created to define the relationships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

EIM identifiers and aliasing

EIM identifier names must be unique within an EIM domain. Aliases can help address situations where using unique identifier names can be difficult. An example of the usefulness of EIM identifier aliases is in situations where someone's legal name is different from the name that person is known as. For example, different individuals within an enterprise can share the same name, which can be confusing if you are using proper names as EIM identifiers.

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

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



By using aliases, the EIM administrator can provide additional information about the individual for each EIM identifier. Each EIM identifier can have multiple aliases to identify which *John S. Day* the EIM identifier represents. For example, the additional aliases might contain each user's employee number, department number, job title, or other distinguishing attribute. In this example, an alias for John S. Day1 might be John Samuel Day and an alias for John S. Day2 might be John Steven Day.

You can use the alias information to aid in locating a specific EIM identifier. For example, an application that uses EIM may specify an alias that it uses to find the appropriate EIM identifier for the application. An administrator can add this alias to an EIM identifier so that the application can use the alias rather than the unique identifier name for EIM operations. An application can specify this information when using the Get EIM Target Identities from the Identifier (`eimGetTargetFromIdentifier()`) API to perform an EIM lookup operation to find the appropriate user identity it needs.

Related concepts

“EIM domain” on page 6

An Enterprise Identity Mapping (EIM) domain is a directory within a Lightweight Directory Access Protocol (LDAP) server that contains EIM data for an enterprise.

EIM registry definitions

An Enterprise Identity Mapping (EIM) registry definition is an entry within EIM that you create to represent an actual user registry that exists on a system within the enterprise. A user registry operates like a directory and contains a list of valid user identities for a particular system or application.

A basic user registry contains user identities and their passwords. One example of a user registry is the z/OS® Security Server Resource Access Control Facility (RACF®) registry. User registries can contain other information as well. For example, a Lightweight Directory Access Protocol (LDAP) directory contains bind distinguished names, passwords, and access controls to data that is stored in LDAP. Other examples of common user registries are the principals in a Kerberos realm or user identities in an Windows Active Directory domain, and the i5/OS user profiles registry.

You can also define user registries that exist within other user registries. Some applications use a subset of user identities within a single instance of a user registry. For example, the z/OS Security Server (RACF) registry can contain specific user registries that are a subset of users within the overall RACF user registry.

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

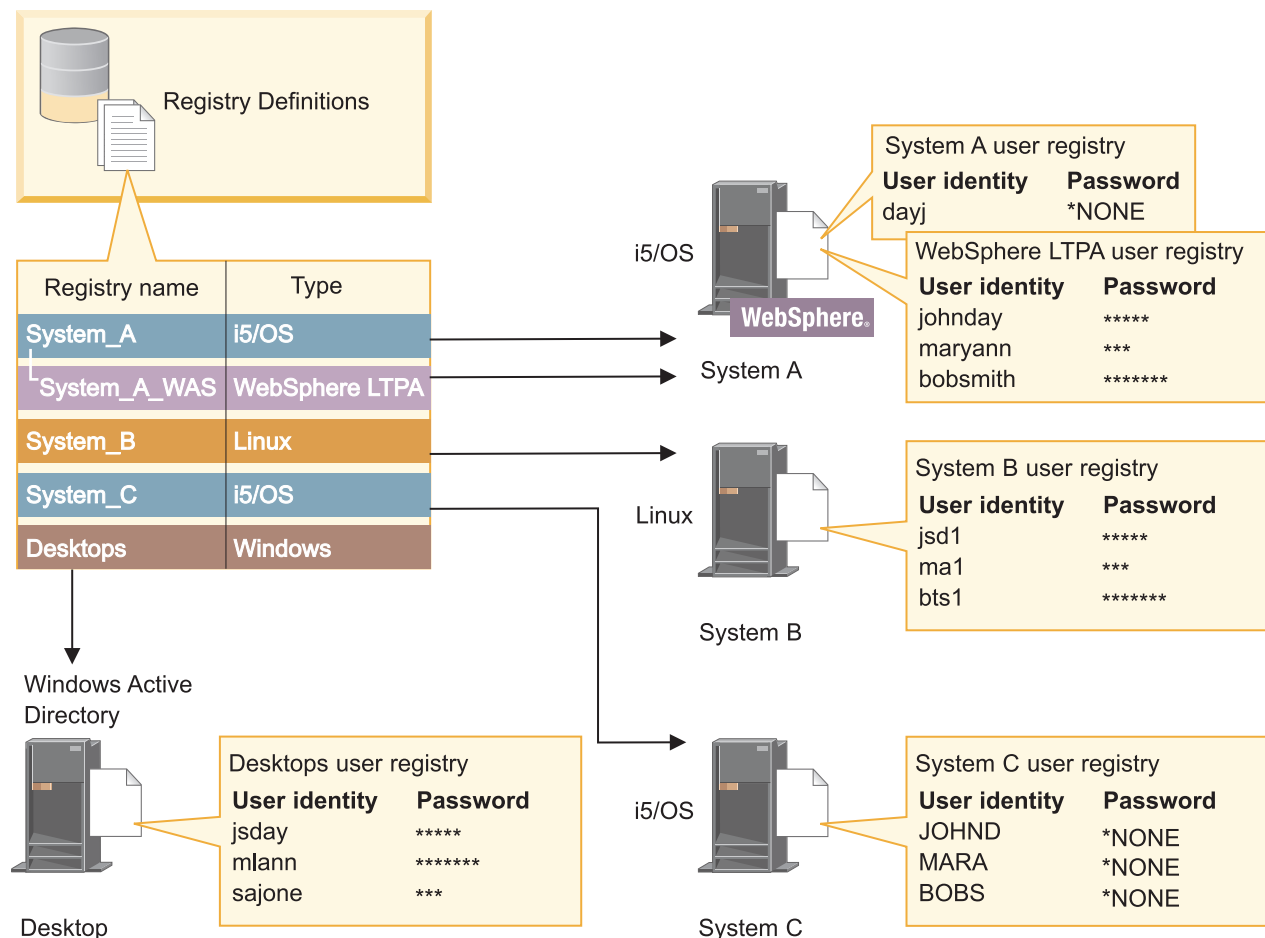
- A unique, arbitrary EIM registry name. Each registry definition represents a specific instance of a user registry. Consequently, you should choose an EIM registry definition name that helps you to identify the particular instance of the user registry. For example, you could choose the TCP/IP host name for a system user registry, or the host name combined with the name of the application for an application user registry. You can use any combination of alphanumeric characters, mixed case, and spaces to create unique EIM registry definition names.
- The type of user registry. There are a number of predefined user registry types that EIM provides to cover most operating system user registries. These include:
 - AIX®
 - Domino® - long name
 - Domino - short name
 - Kerberos
 - Kerberos - case sensitive
 - LDAP
 - - LDAP - short name
 - Linux®
 - Novell Directory Server
 - - Other
 - - Other - case sensitive
 - i5/OS (or OS/400®)
 - Tivoli Access Manager
 - RACF
 - Windows - local
 - Windows domain (Kerberos) (This type is case sensitive.)
 - X.509

Although the predefined registry definition types cover most operating system user registries, you may need to create a registry definition for which EIM does not include a predefined registry type. You

have two options in this situation. You can either use an existing registry definition which matches the characteristics of your user registry or you can define a private user registry type. For example in Figure 6, the administrator followed the process required and defined the type of registry as WebSphere LTPA for the System_A_WAS application registry definition.

In Figure 6, the administrator created EIM system registry definitions for user registries representing System A, System B, System C, and a Windows Active Directory that contains users' Kerberos principals with which users log into their desk top workstations. In addition, the administrator created an application registry definition for WebSphere® (R) Lightweight Third-Party Authentication (LTPA), which runs on System A. The registry definition name that the administrator uses helps to identify the specific occurrence of the type of user registry. For example, an IP address or host name is often sufficient for many types of user registries. In this example, the administrator uses System_A_WAS as the application registry definition name to identify this specific instance of the WebSphere LTPA application. He also specifies that the parent system registry for the application registry definition is the System_A registry.

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



RZALV510-2

Note: To further reduce the need to manage user passwords, the administrator in Figure 6 sets the i5/OS user profile passwords on System A and on System C to *NONE. The administrator in this case is configuring a single sign-on environment and the only application that his users work with are EIM-enabled applications such as System i Navigator. Consequently, the administrator wants to remove the passwords from their i5/OS user profiles so that both the users and he have fewer passwords to manage.

Related concepts

“EIM domain” on page 6

An Enterprise Identity Mapping (EIM) domain is a directory within a Lightweight Directory Access Protocol (LDAP) server that contains EIM data for an enterprise.

“Defining a private user registry type in EIM” on page 91

When you create an Enterprise Identity Mapping (EIM) registry definition you can specify one of a number of predefined user registry types to represent an actual user registry that exists on a system within the enterprise.

System registry definitions

A system registry definition is an entry that you create in Enterprise Identity Mapping (EIM) to represent and describe a distinct user registry within a workstation or server.

You can create an EIM system registry definition for a user registry when the registry in the enterprise has one of the following traits:

- The registry is provided by an operating system, such as AIX, i5/OS, or a security management product such as z/OS Security Server Resource Access Control Facility (RACF).
- The registry contains user identities that are unique to a specific application, such as Lotus Notes®.
- The registry contains distributed user identities, such as Kerberos principals or Lightweight Directory Access Protocol (LDAP) distinguished names.

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

Related tasks

“Adding an application registry definition” on page 90

To create an application registry definition, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM administrator access control.

Application registry definitions

An application registry definition is an entry in Enterprise Identity Mapping (EIM) that you create to describe and represent a subset of user identities that are defined in a system registry. These user identities share a common set of attributes or characteristics that allow them to use a particular application or set of applications.

Application registry definitions represent user registries that exist within other user registries. For example, the z/OS Security Server (RACF) registry can contain specific user registries that are a subset of users within the overall RACF user registry. Because of this relationship, you must specify the name of the parent system registry for any application registry definition that you create.

You can create an EIM application registry definition for a user registry when the user identities in the registry have the following traits:

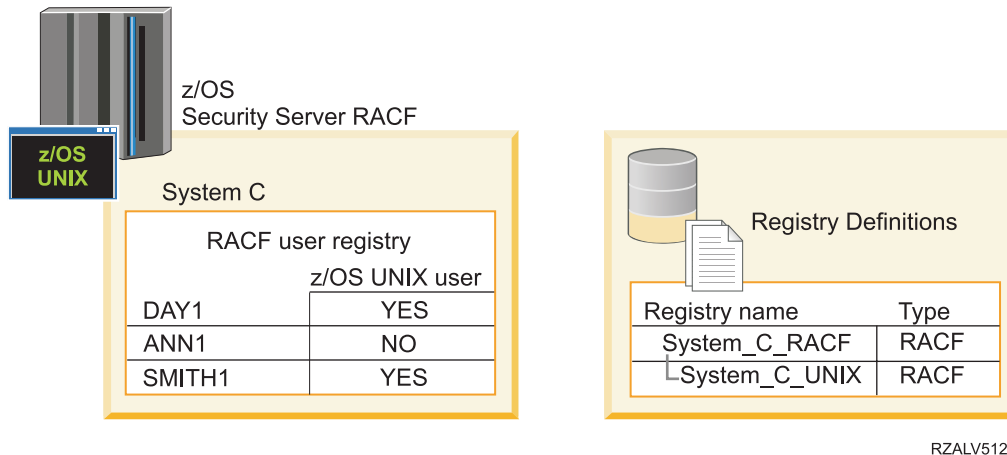
- The user identities for an application is not stored in a user registry specific to the application.
- The user identities for an application is stored in a system registry that contains user identities for other applications.

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

For example, Figure 7 shows how an EIM administrator created a system registry definition to represent a z/OS Security Server RACF registry. The administrator also created an application registry definition to represent the user identities within the RACF registry that use z/OSTM UNIX[®] System Services (z/OS

UNIX). System C contains a RACF user registry that contains information for three user identities, DAY1, ANN1, and SMITH1. Two of these user identities (DAY1 and SMITH1) access z/OS UNIX on System C. These user identities are actually RACF users with unique attributes that identify them as z/OS UNIX users. Within the EIM registry definitions, the EIM administrator defined System_C_RACF to represent the overall RACF user registry. The administrator also defined System_C_UNIX to represent the user identities that have z/OS UNIX attributes.

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



Group registry definitions

Logically grouping the registry definitions allows you to reduce the amount of work that you must perform to configure EIM mapping. You can manage a group registry definition similarly to the way that you manage an individual registry definition.

All members of the group registry definition typically contain at least one common user identity to which you want to create a target or source association. By grouping members together you are able to create only one association, rather than multiple associations, to the group registry definition and user identity.

For example, John Day logs on to his primary system with a user identity of jday and uses the same user identity, JOHND, on multiple systems. Therefore, the user registry for each system contains the JOHND user identity. Typically, John Day creates a separate target association from the John Day EIM identifier to each of the individual user registries that contain the JOHND user identity. To reduce the amount of work that he must perform to configure EIM mapping, he can create one group registry definition with all the user registries that hold the JOHND user identity as members of the group. He is then able to create a single target association from the John Day EIM identifier to the group registry definition rather than multiple target associations from the John Day EIM identifier to each of the individual registry definitions. This single target association to the group registry definition allows John Day's user identity of jday to map to the JOHND user identity.

Read the following information about group registry definitions:

- All of the members (individual registry definitions) of the group registry definition must have the same case sensitivity.
- All of the members (individual registry definitions) of the group registry definition must be defined in the EIM domain before you can add them to a group registry definition.
- A registry definition can be a member of more than one group, but you should avoid specifying an individual user registry as a member of multiple group registry definitions because lookup operation might return ambiguous results. The group registry definition cannot be a member of another group registry definition.

Related concepts

“Lookup operation examples: Example 5” on page 33

Use this example to learn about lookup operations returning ambiguous results that involve group registry definitions.

EIM associations

An Enterprise Identity Mapping (EIM) association is an entry that you create in an EIM domain to define a relationship between user identities in different user registries. The type of association that you create determines whether the defined relationship is direct or indirect.

You can create one of two types of associations in EIM: identifier associations and policy associations. You can use policy associations instead of, or in combination with, identifier associations. How you use associations depends on your overall EIM implementation plan.

To learn more about working with associations, review the following information:

Lookup information

With Enterprise Identity Mapping (EIM) you can provide optional data called lookup information to further identify a target user identity. This target user identity can be specified either in an identifier association or in a policy association.

Lookup information is a unique character string that either the `eimGetTargetFromSource` EIM API or the `eimGetTargetFromIdentifier` EIM API can use during a mapping lookup operation to further refine the search for the target user identity that is the object of the operation. Data that you specify for lookup information corresponds to the registry users additional information parameter for these EIM APIs.

Lookup information is necessary only when a mapping lookup operation can return more than one target user identity. A mapping lookup operation can return multiple target user identities when one or more of the following situations exist:

- An EIM identifier has multiple individual target associations to the same target registry.
- More than one EIM identifier has the same user identity specified in a source association and each of these EIM identifiers has a target association to the same target registry, although the user identity specified for each target association may be different.
- More than one default domain policy association specifies the same target registry.
- More than one default registry policy association specifies the same source registry and the same target registry.
- More than one certificate filter policy association specifies the same source X.509 registry, certificate filter, and target registry.

Note: A mapping lookup operation that returns more than one target user identity can create problems for EIM-enabled applications, including i5/OS applications and products, that are not designed to handle these ambiguous results. However, base i5/OS applications such as System i Access for Windows can not use lookup information to distinguish among multiple target user identities returned by a lookup operation. Consequently, you might consider redefining associations for the domain to ensure that a mapping lookup operation can return a single target user identity to ensure that base i5/OS applications can successfully perform lookup operations and map identities.

You can use lookup information to avoid situations where it is possible for mapping lookup operations to return more than one target user identity. To prevent mapping lookup operations from returning multiple target user identities, you must define unique lookup information for each target user identity in each association. This lookup information must be provided to the mapping lookup operation to ensure that the operation can return a unique target user identity. Otherwise, applications that rely on EIM may not be able to determine the exact target identity to use.

For example, you have an EIM identifier named John Day who has two user profiles on System A. One of these user profiles is JDUSER on System A and another is JDSECADM, which has security administrator special authority. There are two target association for the John Day identifier. One of these target associations is for the JDUSER user identity in the target registry of System_A and has lookup information of user authority specified for JDUSER. The other target association is for the JDSECADM user identity in the target registry of System_A and has lookup information of security officer specified for JDSECADM.

If a mapping lookup operation does not specify any lookup information, the lookup operation returns both the JDUSER and the JDSECADM user identities. If a mapping lookup operation specifies lookup information of user authority, the lookup operation returns the JDUSER user identity only. If a mapping lookup operation specifies lookup information of security officer, the lookup operation returns the JDSECADM user identity only.

Note: If you delete the last target association for a user identity (whether it is an identifier association or a policy association), the target user identity and all lookup information is deleted from the domain as well.

Because you can use certificate policy associations and other associations in a variety of overlapping ways, you should have a thorough understanding of both EIM mapping policy support and how lookup operations work before you create and use certificate policy associations.

Related concepts

“EIM mapping policy support and enablement” on page 35

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain. You can use policy associations instead of, or in combination with, identifier associations.

“EIM lookup operations” on page 26

An application or an operating system uses an EIM API to perform a lookup operation so that the application or operating system can map from one user identity in one registry to another user identity in another registry. An EIM lookup operation is a process through which an application or operating system finds an unknown associated user identity in a specific target registry by supplying some known and trusted information.

“Default domain policy associations” on page 20

A default domain policy association is one type of policy association that you can use to create many-to-one mappings between user identities.

“Default registry policy associations” on page 22

A default registry policy association is one type of policy association that you can use to create many-to-one mappings between user identities.

Identifier associations

An EIM identifier represents a specific person or entity in the enterprise. An EIM identifier association describes a relationship between an EIM identifier and a single user identity in a user registry that also represents that person. When you create associations between an EIM identifier and all of a person's or entity's user identities, you provide a single, complete understanding of how that person or entity uses the resources in an enterprise.

User identities can be used for authentication, authorization, or both. *Authentication* is the process of verifying that an entity or person who provides a user identity has the right to assume that identity. Verification is often accomplished by forcing the person who submits the user identity to provide secret or private information associated with the user identity, such as a password. *Authorization* is the process of ensuring that a properly authenticated user identity can only perform functions or access resources for which the identity has been given privileges. In the past, nearly all applications were forced to use the identities in a single user registry for both authentication and authorization. By using EIM lookup operations, applications now can use the identities in one user registry for authentication while they use associated user identities in a different user registry for authorization.

The EIM identifier provides an indirect association between those user identities, which allows applications to find a different user identity for an EIM identifier based on a known user identity. EIM provides APIs that allow applications to find an unknown user identity in a specific (target) user registry by providing a known user identity in some other (source) user registry. This process is called identity mapping.

In EIM, an administrator can define three different types of associations to describe the relationship between an EIM identifier and a user identity. Identifier associations can be any of the following types: source, target, or administrative. The type of association that you create is based on how the user identity is used. For example, you create source and target associations for those user identities that you want to participate in mapping lookup operations. Typically, if a user identity is used for authentication, you create a source association for it. You then create target associations for those user identities that are used for authorization.

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

- EIM identifier name
- User identity name
- EIM registry definition name
- Association type
- Optional: lookup information to further identify the target user identity in a target association.

Source association

A source association allows the user identity to be used as the source in an EIM lookup operation to find a different user identity that is associated with the same EIM identifier.

When a user identity is used for *authentication*, that user identity should have a source association with an EIM identifier. For example, you might create a source association for a Kerberos principal because this form of user identity is used for authentication. To ensure successful mapping lookup operations for EIM identifiers, source and target associations must be used together for a single EIM identifier.

Target association

A target association allows the user identity to be returned as the result of an EIM lookup operation. User identities that represent end users normally need a target association only.

When a user identity is used for *authorization* rather than for authentication, that user identity should have a target association with an EIM identifier. For example, you might create a target association for an i5/OS user profile because this form of user identity determines what resources and privileges the user has on a specific System i platform. To ensure successful mapping lookup operations for EIM identifiers, source and target associations must be used together for a single EIM identifier.

Source and target association relationship

To ensure successful mapping lookup operations, you need to create at least one source and one or more target associations for a single EIM identifier. Typically, you create a target association for each user identity in a user registry that the person can use for authorization to the system or application to which the user registry corresponds.

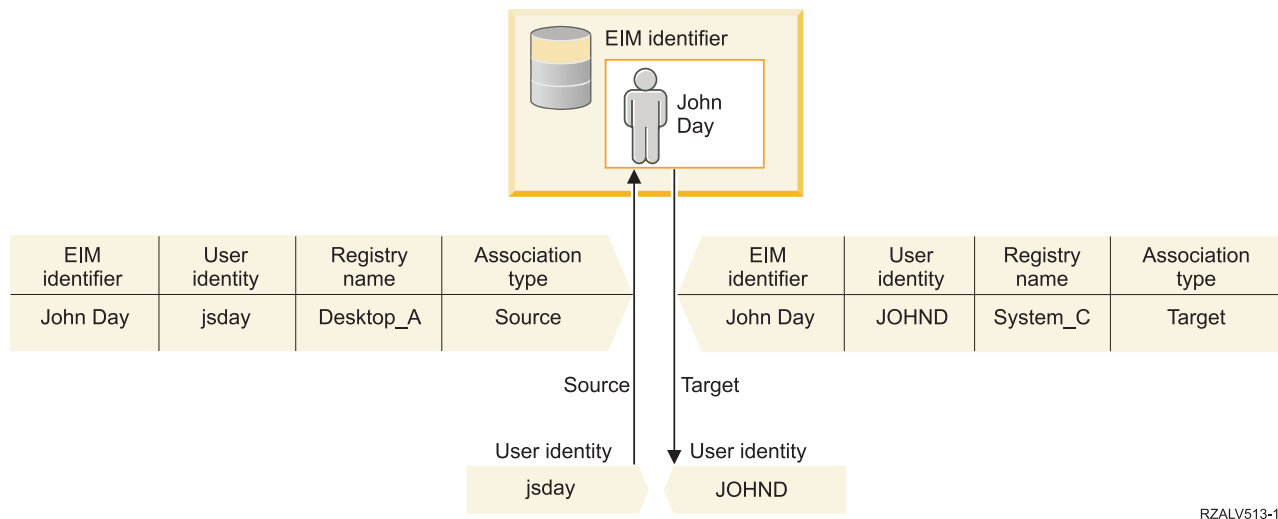
For example, users in your enterprise normally logon and authenticate to Windows desktops and access a System i platform to perform a number of tasks. Users logon to their desktops by using a Kerberos principal and logon to the System i platform by using an i5/OS user profile. You want to create a single

sign-on environment in which users authenticate to their desktops by using their Kerberos principal and no longer have to manually authenticate to the System i platform.

To accomplish this goal, you create a source association for the Kerberos principal for each user and that user's EIM identifier. You then create a target association for the i5/OS user profile for each user and that user's EIM identifier. This configuration ensures that i5/OS can perform a mapping lookup operation to determine the correct user profile needed for a user that accesses the System i platform after he has authenticated to his desktop. i5/OS then allows the user access to resources on the server based on the appropriate user profile without requiring the user to manually authenticate to the server.

Figure 6 illustrates another example in which an EIM administrator creates two associations, a source association and a target association, for the EIM identifier John Day to define the relationship between this identifier and two associated user identities. The administrator creates a source association for jsday, a Kerberos principal in the Desktops user registry. The administrator also creates a target association for JOHND, the i5/OS user profile in the System_C user registry. These associations provide a means for applications to obtain an unknown user identity (the target, JOHND) based on a known user identity (the source, jsday) as part of an EIM lookup operation.

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



To extend the example, suppose the EIM administrator realizes that John Day uses the same i5/OS user profile, jsd1, on five different systems. In this situation, the administrator must create six associations for the EIM identifier John Day to define the relationship between this identifier and an associated user identity in five user registries: a source association for johnday, a Kerberos principal in Desktop_A user registry and five target associations for jsd1, the i5/OS user profile in the five user registries: System_B, System_C, System_D, System_E, and System_F. To reduce the amount of work that he must perform to configure EIM mapping, the EIM administrator creates a group registry definition. Members of the group registry definition include the registry definition names of System_B, System_C, System_D, System_E, and System_F. Grouping members together enables the administrator to create a single target association to the group registry definition and user identity, rather than multiple associations to individual registry definition names. The source and target associations provide a means for applications to obtain an unknown user identity (the target, jsd1) in the five user registries represented as members of the group registry definition based on a known user identity (the source, johnday) as part of an EIM lookup operation.

For some users, it may be necessary to create both a target and a source association for the same user identity. This is required when an individual uses a single system as both a client and a server or for individuals who act as administrators.

Note: User identities that represent typical users normally need a target association only.

For some users, it may be necessary to create both a target and a source association for the same user identity. This is required when an individual uses a single system as both a client and a server or for individuals who act as administrators.

For example, an administrator uses the Management Central function in System i Navigator to manage a central system and several endpoint systems. The administrator performs various functions and these functions can originate on the central system or on an endpoint system. In this situation you would create both a source association and a target association for each of the administrator's user identities on each of the systems. This ensures that, whichever system the administrator uses to originate access to one of the other systems, the user identity used to originate access to the other system can be mapped to the appropriate user identity for the subsequent system the administrator accesses.

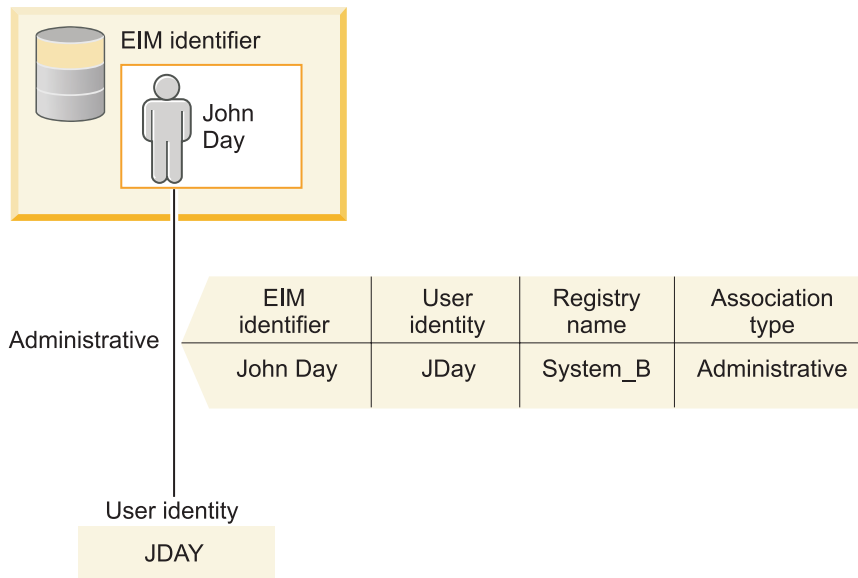
Administrative association

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

Due to the special nature of administrative associations, this type of association can not participate in EIM mapping lookup operations. Consequently, an EIM lookup operation that supplies a source user identity with an administrative association returns no results. Similarly, a user identity with an administrative association is never returned as the result of an EIM lookup operation.

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

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



RZALV514-1

Policy associations

Enterprise Identity Mapping (EIM) mapping policy allows an EIM administrator to create and use policy associations to define a relationship between multiple user identities in one or more user registries and a single user identity in another user registry.

Policy associations use EIM mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier. You can use policy associations instead of, or in combination with, identifier associations that provide one-to-one mappings between an EIM identifier and a single user identity.

A policy association affects only those user identities for which specific individual EIM associations do not exist. When specific identifier associations exist between an EIM identifier and user identities, then the target user identity from the identifier association is returned to the application performing the lookup operation, even when a policy association exists and the use of policy associations is enabled.

You can create three different types of policy associations:

Related concepts

“EIM lookup operations” on page 26

An application or an operating system uses an EIM API to perform a lookup operation so that the application or operating system can map from one user identity in one registry to another user identity in another registry. An EIM lookup operation is a process through which an application or operating system finds an unknown associated user identity in a specific target registry by supplying some known and trusted information.

Default domain policy associations:

A default domain policy association is one type of policy association that you can use to create many-to-one mappings between user identities.

You can use a default domain policy association to map a source set of multiple user identities (in this case, all users in the domain) to a single target user identity in a specified target user registry. In a default domain policy association, all users in the domain are the source of the policy association and are mapped to a single target registry and target user identity.

To use a default domain policy association, you must enable mapping lookups using policy associations for the domain. You must also enable mapping lookups for the target user registry of the policy association. When you configure this enablement, the user registries in the policy association can participate in mapping lookup operations.

The default domain policy association takes effect when a mapping lookup operation is not satisfied by identifier associations, certificate filter policy associations, or default registry policy associations for the target registry. The result is that all user identities in the domain are mapped to the single target user identity as specified by the default domain policy association.

For example, you create a default domain policy association with a target user identity of John_Day in target registry Registry_xyz and you have not created any identifier associations or other policy associations that map to this user identity. Therefore, when Registry_xyz is specified as the target registry in lookup operations, the default domain policy ensures that the target user identity of John_Day is returned for all user identities in the domain that do not have any other associations defined for them.

You specify these two things to define a default domain policy association:

- **Target registry.** The target registry that you specify is the name of an Enterprise Identity Mapping (EIM) registry definition which contains the user identity to which all user identities in the domain are to be mapped.
- **Target user.** The target user is the name of user identity that is returned as the target of an EIM mapping lookup operation based on this policy association.

You can define a default domain policy association for each registry in the domain. If two or more domain policy associations refer to the same target registry, you must define unique lookup information for each of these policy associations to ensure that mapping lookup operations can distinguish among them. Otherwise, mapping lookup operations may return multiple target user identities. As a result of these ambiguous results, applications that rely on EIM may not be able to determine the exact target user identity to use.

Because you can use policy associations in a variety of overlapping ways, you should have a thorough understanding of EIM mapping policy support and how lookup operations work before you create and use policy associations.

Note: You might want to create a default domain policy association with a target user identity that exists within a group registry definition. All users in the domain are the source of the policy association and are mapped to a target user identity in a target group registry definition. The user identity that you define in the default domain policy association exists within the members of the group registry definition.

For example, John Day uses the same i5/OS user profile, John_Day, on five different systems: System B, System C, System D, System E, and System F. To reduce the amount of work that he must perform to configure EIM mapping, the EIM administrator creates a group registry definition called Group_1. Members of the group registry definition include the registry definition names of System_B, System_C, System_D, System_E, and System_F. Grouping members together enables the administrator to create a single target association to the group registry definition and user identity, rather than multiple associations to the individual registry definitions.

The EIM administrator creates a default domain policy association with a target user identity of John_Day in target registry Group_1. In this case, no other specific identifier associations or policy associations apply. Therefore, when Group_1 is specified as the target registry in lookup operations, the default domain policy ensures that the target user identity of John_Day is returned for all user identities in the domain that do not have any specific identifier associations defined for them.

Related concepts

“Lookup information” on page 15

With Enterprise Identity Mapping (EIM) you can provide optional data called lookup information to further identify a target user identity. This target user identity can be specified either in an identifier association or in a policy association.

“EIM mapping policy support and enablement” on page 35

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain. You can use policy associations instead of, or in combination with, identifier associations.

Default registry policy associations:

A default registry policy association is one type of policy association that you can use to create many-to-one mappings between user identities.

You can use a default registry policy association to map a source set of multiple user identities (in this case those in a single registry) to a single target user identity in a specified target user registry. In a default registry policy association, all users in a single registry are the source of the policy association and are mapped to a single target registry and target user.

To use default registry policy associations, you must enable mapping lookups using policy associations for the domain. You must also enable mapping lookups for the source registry and enable mapping lookups and the use of policy associations for the target user registry of the policy association. When you configure this enablement, the user registries in the policy association can participate in mapping lookup operations.

The default registry policy association takes effect when a mapping lookup operation is not satisfied by identifier associations, certificate filter policy associations, or other default registry policy associations for the target registry. The result is that all user identities in the source registry are mapped to the single target user identity as specified by the default registry policy association.

For example, you create a default registry policy association that has a source registry of `my_realm.com`, which are principals in a specific Kerberos realm. For this policy association, you also specify a target user identity of `general_user1` in target registry `i5/OS_system_reg`, which is a specific user profile in an `i5/OS` user registry. In this case, you have not created any identifier associations or policy associations that apply to any of the user identities in the source registry. Therefore, when `i5/OS_system_reg` is specified as the target registry and `my_realm.com` is specified as the source registry in lookup operations, the default registry policy association ensures that the target user identity of `general_user1` is returned for all user identities in `my_realm.com` that do not have any specific identifier associations or certificate filter policy associations defined for them.

You specify these three things to define a default registry policy association:

- **Source registry.** This is the registry definition that you want the policy association to use as the source of the mapping. All the user identities in this source user registry are to be mapped to the specified target user of the policy association.
- **Target registry.** The target registry that you specify is the name of an Enterprise Identity Mapping (EIM) registry definition. The target registry must contain the target user identity to which all user identities in the source registry are to be mapped.
- **Target user.** The target user is the name of user identity that is returned as the target of an EIM mapping lookup operation based on this policy association.

You can define more than one default registry policy association. If two or more policy associations with the same source registry refer to the same target registry, you must define unique lookup information for each of these policy associations to ensure that mapping lookup operations can distinguish among them.

Otherwise, mapping lookup operations may return multiple target user identities. As a result of these ambiguous results, applications that rely on EIM may not be able to determine the exact target identity to use.

Because you can use policy associations in a variety of overlapping ways, you should have a thorough understanding of EIM mapping policy support and how lookup operations work before you create and use policy associations.

Note: You might want to create a default registry policy association with a target user identity that exists within a group registry definition. All users in the source user registry are the source of the policy association and are mapped to a target user identity in a target group registry definition. The user identity that you define in the default registry policy association exists within the members of the group registry definition.

For example, John Day uses the same i5/OS user profile, John_Day, on five different systems: System_B, System_C, System_D, System_E, and System_F. To reduce the amount of work that he must perform to configure EIM mapping, the EIM administrator creates a group registry definition called Group_1. Members of the group registry definition include the registry definition names of System_B, System_C, System_D, System_E, and System_F. Grouping members together enables the administrator to create a single target association to the group registry definition and user identity, rather than multiple associations to the individual registry definitions.

The EIM administrator creates a default registry policy association that has a source registry of my_realm.com, which are principals in a specific Kerberos realm. For this policy association, he also specifies a target user identity of John_Day in target registry Group_1. In this case, no other identifier associations or policy associations apply. Therefore, when Group_1 is specified as the target registry and my_realm.com is specified as the source registry in lookup operations, the default registry policy association ensures that the target user identity of John_Day is returned for all user identities in my_realm.com that do not have any specific identifier associations defined for them.

Related concepts

“Lookup information” on page 15

With Enterprise Identity Mapping (EIM) you can provide optional data called lookup information to further identify a target user identity. This target user identity can be specified either in an identifier association or in a policy association.

“EIM mapping policy support and enablement” on page 35

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain. You can use policy associations instead of, or in combination with, identifier associations.

Certificate filter policy associations:

A certificate filter policy association is one type of policy association that you can use to create many-to-one mappings between user identities. You can use a certificate filter policy association to map a source set of certificates to a single target user identity in a specified target user registry.

In a certificate filter policy association, you specify a set of certificates in a single X.509 registry as the source of the policy association. These certificates are mapped to a single target registry and target user that you specify. Unlike a default registry policy association in which all users in a single registry are the source of the policy association, the scope of a certificate filter policy association is more flexible. You can specify a subset of certificates in the registry as the source. The certificate filter that you specify for the policy association is what determines its scope.

Note: When you want to map all the certificates in an X.509 user registry to a single target user identity, create and use a default registry policy association.

To use certificate filter policy associations, you must enable mapping lookups using policy associations for the domain. You must also enable mapping lookups for the source registry and enable mapping lookups and the use of policy associations for the target user registry of the policy association. When you configure this enablement, the user registries in the policy association can participate in mapping lookup operations.

When a digital certificate is the source user identity in an Enterprise Identity Mapping (EIM) mapping lookup operation (after the requesting application uses the `eimFormatUserIdentity()` EIM API to format the user identity name), EIM first checks to see if there is an identifier association between an EIM identifier and the specified user identity. If none exist, EIM then compares the DN information in the certificate against the DN or partial DN information specified in the filter for the policy association. If the DN information in the certificate satisfies the criteria of the filter, EIM returns the target user identity that the policy association specified. The result is that certificates in the source X.509 registry that satisfy the certificate filter criteria are mapped to the single target user identity as specified by the certificate filter policy association.

For example, you create a certificate filter policy association that has a source registry of `certificates.x509`. This registry contains the certificates for all company employees, including those that all managers in the human resources department use to access certain private internal Web pages and other resources that they access through an System i model. For this policy association, you also specify a target user identity of `hr_managers` in target registry `system_abc` which is a specific user profile in an i5/OS user registry. To ensure that only the certificates that belong to the human resource managers are covered by this policy association, you specify a certificate filter with a subject distinguished name (SDN) of `ou=hrmgr,o=myco.com,c=us`.

In this case, you have not created any identifier associations or other certificate filter policy associations that apply to any of the user identities in the source registry. Therefore, when `system_abc` is specified as the target registry and `certificates.x509` is specified as the source registry in lookup operations, the certificate filter policy association ensures that the target user identity of `hr_managers` is returned for all certificates in `certificates.x509` registry that match the specified certificate filter and which do not have any specific identifier associations defined for them.

You specify the following information to define a certificate filter policy association:

- **Source registry.** The source registry definition that you specify must be an X.509 type user registry. The certificate filter policy creates an association between user identities in this X.509 user registry and a single, specific target user identity. The association is applied to only those user identities in the registry that meet the criteria of the certificate filter that you specify for this policy.
- **Certificate filter.** A certificate filter defines a set of similar user certificate attributes. The certificate filter policy association maps any certificates with these defined attributes in the X.509 user registry to a specific target user identity. You specify the filter based on a combination of the Subject distinguished name (SDN) and the Issuer distinguished name (IDN) that matches the certificates that you want to use as the source of the mapping. The certificate filter that you specify for the policy must already exist in the EIM domain.
- **Target registry.** The target registry definition that you specify is the user registry that contains the user identity to which you want to map the certificates that match the certificate filter.
- **Target user.** The target user is the name of the user identity that is returned as the target of an EIM mapping lookup operation based on this policy association.

Because you can use certificate policy associations and other associations in a variety of overlapping ways, you should have a thorough understanding of both EIM mapping policy support and how lookup operations work before you create and use certificate policy associations.

Note: You might want to create a certificate filter policy association with a target user identity that exists within a group registry definition. Users in the source registry that meet the criteria specified by the certificate filter are the source of the policy association and are mapped to a target user identity

in a target group registry definition. The user identity that you define in the certificate filter policy association exists within the members of the group registry definition.

For example, John Day uses the same i5/OS user profile, John_Day, on five different systems: System B, System C, System D, System E, and System F. To reduce the amount of work that he must perform to configure EIM mapping, the EIM administrator creates a group registry definition. Members of the group registry definition include the registry definition names of System_B, System_C, System_D, System_E, and System_F. Grouping members together enables the administrator to create a single target association to the group registry definition and user identity, rather than multiple associations to the individual registry definitions.

The EIM administrator creates a certificate filter policy association where he defines a subset of certificates within a single X.509 registry as the source of the policy association. He specifies a target user identity of John_Day in target registry Group_1. In this case, no other specific identifier associations or other certificate filter policy associations apply. Therefore, when Group_1 is specified as the target registry in lookup operations, all certificates in the source X.509 registry that match the certificate filter criteria are mapped to the specified target user identity.

Certificate filters:

A certificate filter defines a set of similar distinguished name certificate attributes for a group of user certificates in an X.509 source user registry. You can use the certificate filter as the basis of a certificate filter policy association.

The certificate filter in a policy association determines which certificates in the specified source X.509 registry to map to the specified target user. Those certificates that have Subject DN and Issuer DN information that satisfy the criteria of the filter are mapped to the specified target user during Enterprise Identity Mapping (EIM) mapping lookup operations.

For example, you create a certificate filter with a subject distinguished name (SDN) of o=ibm,c=us. All certificates with these DNs as part of their SDN information meet the criteria of the filter, such as a certificate with an SDN of cn=JohnDay,ou=LegalDept,o=ibm,c=us. If there is more than one certificate filter for which the certificate meets the criteria, the more specific certificate filter value that a certificate matches most closely takes precedence. For example, you have a certificate filter with an SDN of o=ibm,c=us and you have another certificate filter with an SDN of ou=LegalDept,o=ibm,c=us. If you have a certificate in the source X.509 registry with an SDN of cn=JohnDay,ou=LegalDept,o=ibm,c=us, then the second, or more specific certificate filter is used. If you have a certificate in the source X.509 registry with an SDN of cn=SharonJones,o=ibm,c=us, then the less specific certificate filter is used because the certificate matches its criteria more closely.

You can specify one or both of the following to define a certificate filter:

- Subject distinguished name (SDN). The full or partial DN that you specify for the filter must correspond to the subject DN portion of the digital certificate, which designates the owner of the certificate. You can provide the full subject DN string, or you can provide one or more partial DNs that might comprise the complete SDN.
- Issuer distinguished name (IDN). The full or partial DN that you specify for the filter must correspond to the issuer DN portion of the digital certificate, which designates the Certificate Authority who issued the certificate. You can provide the full issuer DN string, or you can provide one or more of partial DNs that might comprise the complete IDN.

There are several methods that you can use to create a certificate filter, including the use of the Format EIM Policy Filter (eimFormatPolicyFilter) API to generate certificate filters by using a certificate as a template to create the necessary DNs in the correct order and format for the SDN and IDN.

Related concepts

“Distinguished name” on page 44

A distinguished name (DN) is a LDAP entry that uniquely identifies and describes an entry in a directory (LDAP) server. You use the Enterprise Identity Mapping (EIM) Configuration wizard to configure the directory server to store EIM domain information. Because EIM uses the directory server to store EIM data, you can use distinguished names as a means of authenticating to the EIM domain controller.

Related information

Format EIM Policy Filter (eimFormatPolicyFilter) API

EIM lookup operations

An application or an operating system uses an EIM API to perform a lookup operation so that the application or operating system can map from one user identity in one registry to another user identity in another registry. An EIM lookup operation is a process through which an application or operating system finds an unknown associated user identity in a specific target registry by supplying some known and trusted information.

Applications that use EIM APIs can perform these EIM lookup operations on information only if that information is stored in the EIM domain. An application can perform one of two types of EIM lookup operations based on the type of information the application supplies as the source of the EIM lookup operation: a user identity or an EIM identifier.

When applications or operating systems use the `eimGetTargetFromSource()` API to obtain a target user identity for a given target registry, they must supply a *user identity as the source* of the lookup operation. To be used as the source in a EIM lookup operation, a user identity must have either an identifier source association defined for it or be covered by a policy association. When an application or operating system uses this API, the application or operating system must supply three pieces of information:

- A user identity as the source, or starting point of the operation.
- The EIM registry definition name for the source user identity.
- The EIM registry definition name that is the target of the EIM lookup operation. This registry definition describes the user registry that contains the user identity that the application is seeking.

When applications or operating systems use the `eimGetTargetFromIdentifier()` API to obtain a user identity for a given target registry, they must supply an *EIM identifier as the source* of the EIM lookup operation. When an application uses this API, the application must supply two pieces of information:

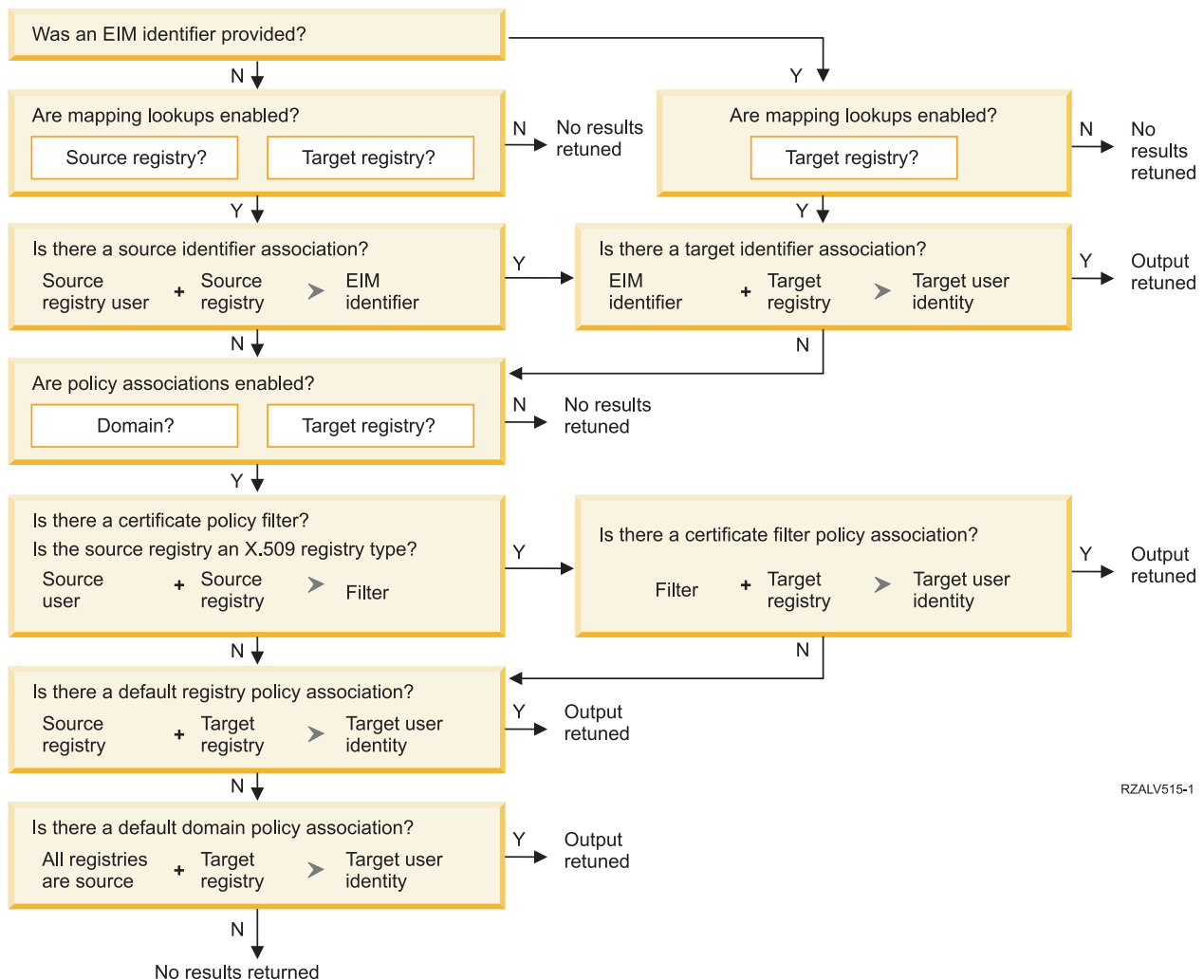
- An EIM identifier as the source, or starting point of the operation.
- The EIM registry definition name that is the target of the EIM lookup operation. This registry definition describes the user registry that contains the user identity that the application is seeking.

For a user identity to be returned as the target of either type of EIM lookup operation, the user identity must have a target association defined for it. This target association can be in the form of an identifier association or a policy association.

The supplied information is passed to EIM and the EIM lookup operation searches for and returns any target user identities, by searching EIM data in the following order, as Figure 10 illustrates:

1. Identifier target association for an EIM identifier. The EIM identifier is identified in one of two ways: It is supplied by the `eimGetTargetFromIdentifier()` API. Or, the EIM identifier is determined from information supplied by the `eimGetTargetFromSource()` API.
2. Certificate filter policy association.
3. Default registry policy association.
4. Default domain policy association.

Figure 10: EIM lookup operation general processing flow chart



Note: In the following flow, lookup operations first checks the individual registry definition, such as the specified source registry or target registry. If lookup operations fail to find a mapping using the individual registry definition, it determines whether the individual registry definition is a member of a group registry definition. If it is a member of a group registry definition, the lookup operation checks the group registry definition to satisfy the mapping lookup request.

The lookup operation search flows in this manner:

1. The lookup operation checks whether mapping lookups are enabled. The lookup operation determines whether mapping lookups are enabled for the specified source registry, the specified target registry, or both specified registries. If mapping lookups are not enabled for one or both of the registries, then the lookup operation ends without returning a target user identity.
2. The lookup operation checks whether there are identifier associations that match the lookup criteria. If an EIM identifier was provided, the lookup operation uses the specified EIM identifier name. Otherwise, the lookup operation checks whether there is a specific identifier source association that matches the supplied source user identity and source registry. If there is one, the lookup operation uses it to determine the appropriate EIM identifier name. The lookup operation then uses the EIM identifier name to search for an identifier target association for the EIM identifier that matches the specified target EIM registry definition name. If there is an identifier target association that matches, the lookup operation returns the target user identity defined in the target association.
3. The lookup operation checks whether the use of policy associations are enabled. The lookup operation checks whether the domain is enabled to allow mapping lookups using policy associations. The

lookup operation also checks whether the target registry is enabled to use policy associations. If the domain is not enabled for policy associations or the registry is not enabled for policy associations, then the lookup operation ends without returning a target user identity.

4. The lookup operation checks for certificate filter policy associations. The lookup operation checks whether the source registry is an X.509 registry type. If it is an X.509 registry type, the lookup operation checks whether there is a certificate filter policy association that matches the source and target registry definition names. The lookup operation checks whether there are certificates in the source X.509 registry that satisfy the criteria specified in the certificate filter policy association. If there is a matching policy association and there are certificates that satisfy the certificate filter criteria, the lookup operation returns the appropriate target user identity for that policy association.
5. The lookup operation checks for default registry policy associations. The lookup operation checks whether there is a default registry policy association that matches the source and target registry definition names. If there is a matching policy association, the lookup operation returns the appropriate target user identity for that policy association.
6. The lookup operation checks for default domain policy associations. The lookup operation checks whether there is a default domain policy association defined for the target registry definition. If there is a matching policy association, the lookup operation returns the associated target user identity for that policy association.
7. The lookup operation is unable to return any results.

To learn more about Enterprise Identity Mapping lookup operations view the following examples:

Related concepts

“EIM domain” on page 6

An Enterprise Identity Mapping (EIM) domain is a directory within a Lightweight Directory Access Protocol (LDAP) server that contains EIM data for an enterprise.

“Policy associations” on page 20

Enterprise Identity Mapping (EIM) mapping policy allows an EIM administrator to create and use policy associations to define a relationship between multiple user identities in one or more user registries and a single user identity in another user registry.

“EIM domain controller” on page 5

An EIM domain controller is a Lightweight Directory Access Protocol (LDAP) server that is configured to manage one or more EIM domains. An EIM domain consists of all the EIM identifiers, EIM associations, and user registries that are defined in that domain. Systems (EIM clients) participate in the EIM domain by using the domain data for EIM lookup operations.

“Lookup information” on page 15

With Enterprise Identity Mapping (EIM) you can provide optional data called lookup information to further identify a target user identity. This target user identity can be specified either in an identifier association or in a policy association.

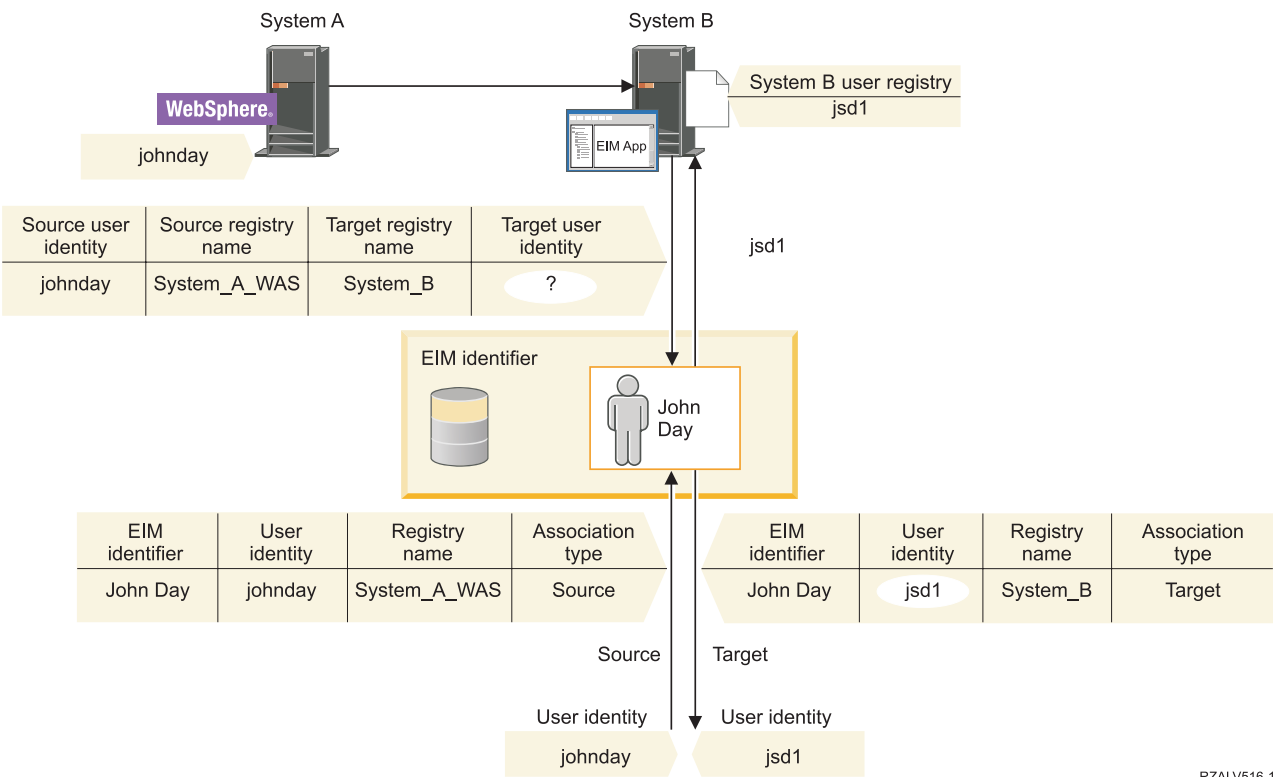
Lookup operation examples: Example 1

Use this example to learn how the search flow works for a lookup operation that returns a target user identity from specific identifier associations based on the known user identity.

In Figure 11, the user identity johnday authenticates to the WebSphere Application Server by using Lightweight Third-Party Authentication (LPTA) on System A. The WebSphere Application Server on System A calls an integrated program on System B to access data on System B. The integrated program uses an Enterprise Identity Mapping (EIM) API to perform an EIM lookup operation based on the user identity on System A as the source of the operation. The application supplies the following information to perform the operation: johnday as the source user identity, System_A_WAS as the source EIM registry definition name, and System_B as the target EIM registry definition name. This source information is passed to EIM and the EIM lookup operation finds an identifier source association that matches the information. Using the EIM identifier name John Day, the EIM lookup operation searches for an identifier

target association for this identifier that matches the target EIM registry definition name for System_B. When the matching target association is found, the EIM lookup operation returns the jsd1 user identity to the application.

Figure 11: EIM lookup operation returns a target user identity from specific identifier associations based on the known user identity johnday



RZALV516-1

Lookup operation examples: Example 2

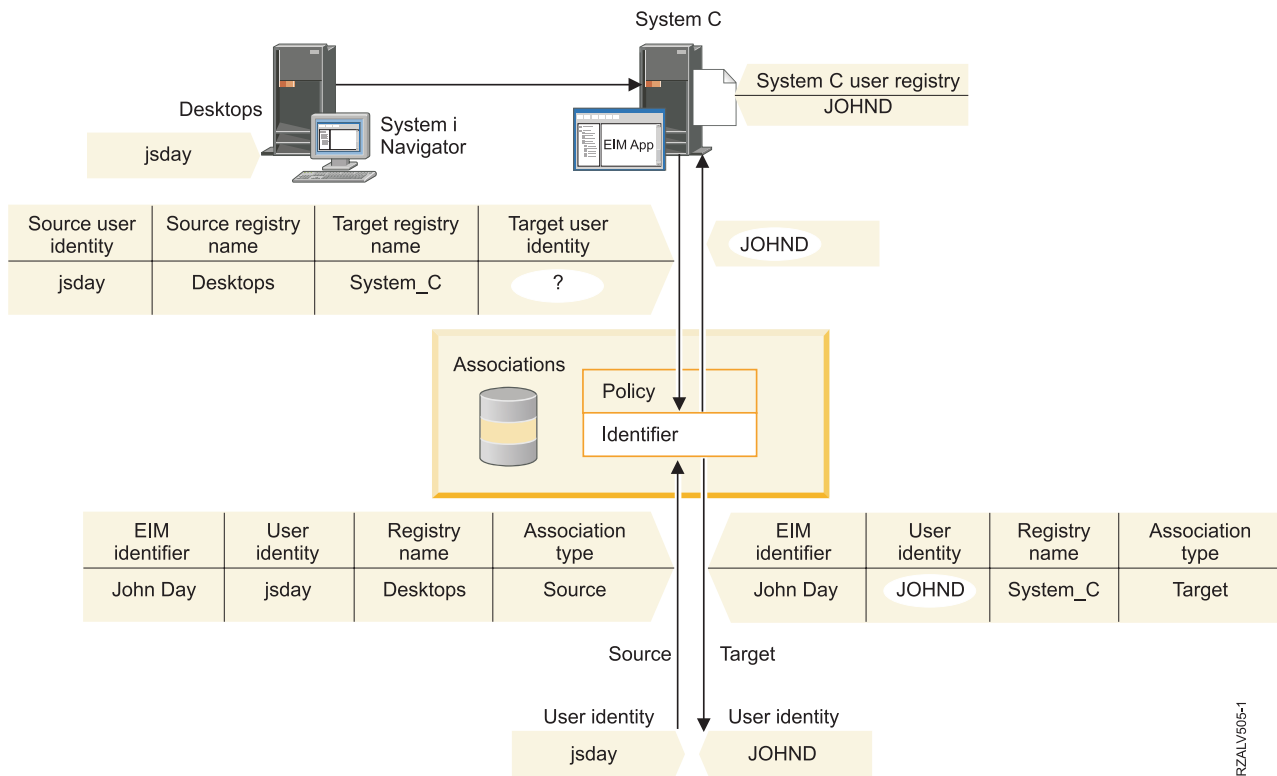
Use this example to learn how the search flow works for a lookup operation that returns a target user identity from specific identifier associations based on the known Kerberos principal.

In Figure 12, an administrator wants to map a Windows user in a Windows Active Directory registry to an i5/OS user profile. Kerberos is the authentication method that Windows uses and the name of the Windows Active Directory registry as the administrator defined it in EIM is Desktops. The user identity that the administrator wants to map from is a Kerberos principal named jsday. The name of the i5/OS registry as the administrator defined it in EIM is System_C and the user identity that the administrator wants to map to is a user profile named JOHND.

The administrator creates an EIM identifier named John Day. He then adds two associations to this EIM identifier:

- A source association for the Kerberos principal named jsday in the Desktops registry.
- A target association for the i5/OS user profile named JOHND in the System_C registry.

Figure 12: EIM lookup operation returns a target user identity from specific identifier associations based on the known Kerberos principal jsday



This configuration allows a mapping lookup operation to map from the Kerberos principal to the i5/OS user profile as follows:

| Source user identity and registry | --- | EIM identifier | --- | Target user identity |
|-----------------------------------|-----|----------------|-----|------------------------------|
| jsday in Desktops registry | --- | John Day | --- | JOHND (in System_C registry) |

The lookup operation search flows in this manner:

1. The user jsday logs on and authenticates to Windows by means of his Kerberos principal in the Windows Active Directory registry Desktops.
2. The user opens System i Navigator to access data on System_C.
3. i5/OS uses an EIM API to perform an EIM lookup operation with a source user identity of jsday, a source registry of Desktops, and a target registry of System_C.
4. The EIM lookup operation checks whether mapping lookups are enabled for the source registry Desktops and target registry System_C. They are.
5. The lookup operation checks for a specific identifier source association that matches the supplied source user identity of jsday in a source registry of Desktops.
6. The lookup operation uses the matching identifier source association to determine the appropriate EIM identifier name, which is John Day.
7. The lookup operation uses this EIM identifier name to search for an identifier target association for the EIM identifier that matches the specified target EIM registry definition name of System_C.
8. There is a such an identifier target association and the lookup operation returns the target user identity of JOHND as defined in the target association.

- With the mapping lookup operation complete, System i Navigator begins to run under the JOHND user profile. The user's authority to access resources and perform actions within System i Navigator is determined by the authority defined for the JOHND user profile rather than the authority defined for the jsday user identity.

Lookup operation examples: Example 3

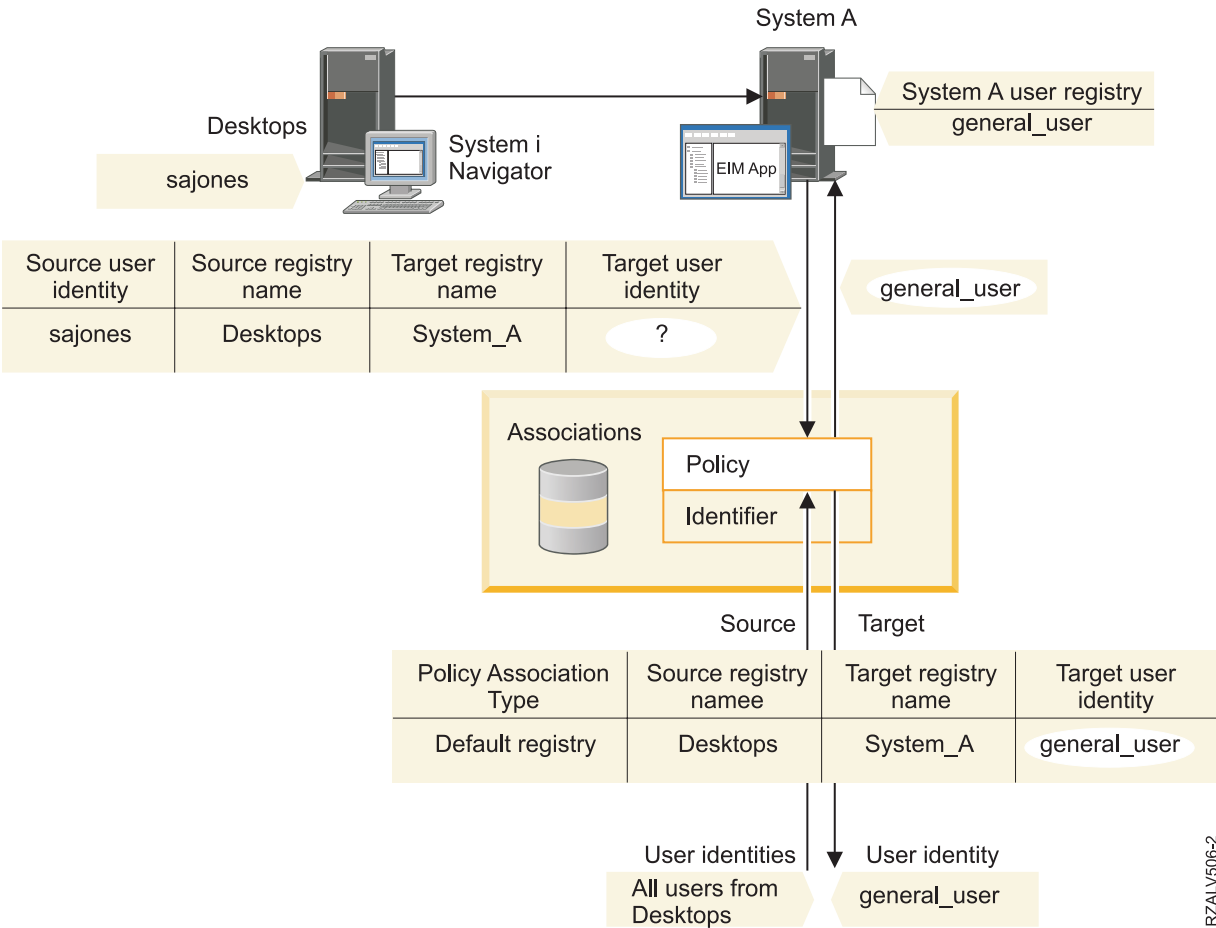
Use this example to learn how the search flow works for a lookup operation that returns a target user identity from a default registry policy association.

In Figure 13, an administrator wants to map all desktop workstation users in a Windows Active Directory registry to a single i5/OS user profile named `general_user` in an i5/OS registry that he named `System_A` in Enterprise Identity Mapping (EIM). Kerberos is the authentication method that Windows uses and the name of the Windows Active Directory registry as the administrator defined it in EIM is `Desktops`. One of the user identities that the administrator wants to map from is a Kerberos principal named `sajones`.

The administrator creates a default registry policy association with the following information:

- A source registry of `Desktops`.
- A target registry of `System_A`.
- A target user identity of `general_user`.

Figure 13: A lookup operation returns a target user identity from a default registry policy association.



This configuration allows a mapping lookup operation to map all the Kerberos principals in the Desktops registry, including the `sajones` principal, to the i5/OS user profile named `general_user` as follows:

| Source user identity and registry | ---> | Default registry policy association | ---> | Target user identity |
|-----------------------------------|------|-------------------------------------|------|-------------------------------------|
| sajones in Desktops registry | ---> | Default registry policy association | ---> | general_user (in System_A registry) |

The lookup operation search flows in this manner:

1. The user sajones logs on and authenticates to her Windows desktop by means of her Kerberos principal in the Desktops registry.
2. The user opens System i Navigator to access data on System A.
3. i5/OS uses an EIM API to perform an EIM lookup operation with a source user identity of sajones, a source registry of Desktops, and a target registry of System_A.
4. The EIM lookup operation checks whether mapping lookups are enabled for the source registry Desktops and target registry System_A. They are.
5. The lookup operation checks for a specific identifier source association that matches the supplied source user identity of sajones in a source registry of Desktops. It does not find a matching identifier association.
6. The lookup operation checks whether the domain is enabled to use policy associations. It is.
7. The lookup operation checks whether the target registry (System_A) is enabled to use policy associations. It is.
8. The lookup operation checks whether the source registry (Desktops) is an X.509 registry. It is not.
9. The lookup operation checks whether there is a default registry policy association that matches the source registry definition name (Desktops) and the target registry definition name (System_A).
10. The lookup operation determines that there is one and returns general_user as the target user identity.

Sometimes an EIM lookup operation returns ambiguous results. This can happen, for example, when more than one target user identity matches the specified lookup operation criteria. Some EIM-enabled applications, including i5/OS applications and products are not designed to handle these ambiguous results and may fail or give unexpected results. You may need to take action to resolve this situation. For example, you may need to either change your EIM configuration or define lookup information for each target user identity to prevent multiple matching target user identities. Also, you can test a mapping to determine whether the changes you make work as expected.

Lookup operation examples: Example 4

Use this example to learn how the search flow works for a lookup operation that returns a target user identity in a user registry that is a member of a group registry definition.

An administrator wants to map a Windows user to an i5/OS user profile. Kerberos is the authentication method that Windows uses and the name of the Kerberos registry as the administrator defined it in Enterprise Identity Mapping (EIM) is Desktop_A. The user identity that the administrator wants to map from is a Kerberos principal named jday. The name of the i5/OS registry definition as the administrator defined it in EIM is Group_1 and the user identity that the administrator wants to map to is a user profile named JOHND which exists in three individual registries: System_B, System_C, and System_D. Each of the individual registries is a member of the Group_1 group registry definition.

The administrator creates an EIM identifier named John Day. He then adds two associations to this EIM identifier:

- A source association for the Kerberos principal named jday in the Desktop_A registry.
- A target association for the i5/OS user profile named JOHND in the Group_1 registry.

This configuration allows a mapping lookup operation to map from the Kerberos principal to the i5/OS user profile as follows:

| Source user identity and registry | ---> | EIM Identifier | ---> | Target user identity |
|-----------------------------------|------|----------------|------|--|
| jday in Desktop_A registry | ---> | John Day | ---> | JOHND (in Group_1 group registry definition) |

The lookup operation search flows in this manner:

1. The user (jday) logs on and authenticates to Windows on Desktop_A.
2. The user opens System i Navigator to access data on System_B.
3. i5/OS uses an EIM API to perform an EIM lookup operation with a source user identity of jday, a source registry of Desktop_A, and a target registry of System_B.
4. The EIM lookup operation checks whether mapping lookups are enabled for the source registry (Desktop_A) and target registry (System_B).
5. The lookup operation checks for a specific individual source association that matches the supplied source user identity of jday in a source registry of Desktop_A.
6. The lookup operation uses the matching source association to determine the appropriate EIM identifier name, which is John Day.
7. The lookup operation uses this EIM identifier name to search for an individual target association for the EIM identifier that matches the specified target EIM registry definition name of System_B. (There is none.)
8. The lookup operation checks to see if the source registry (Desktop_A) is a member of any group registry definitions. (It is not.)
9. The lookup operation checks to see if the target registry (System_B) is a member of any group registry definitions. It is a member of the Group_1 group registry definition.
10. The lookup operation uses the EIM identifier name to search for an individual target association for the EIM identifier that matches the specified target EIM registry definition name of Group_1.
11. There is such an individual target association and the lookup operation returns the target user identity of JOHND as defined in the target association.

Note: In some cases, the EIM lookup operation returns ambiguous results when more than one target user identity matches the specified lookup operation criteria. Because EIM cannot return a single target user identity, EIM-enabled applications, including i5/OS applications and products, that are not designed to handle these ambiguous results may fail or give unexpected results. You may need to take action to resolve this situation. For example, you may need to either change your EIM configuration or define lookup information for each target user identity to prevent multiple matching target user identities. You can test a mapping to determine whether the changes you make work as expected.

Lookup operation examples: Example 5

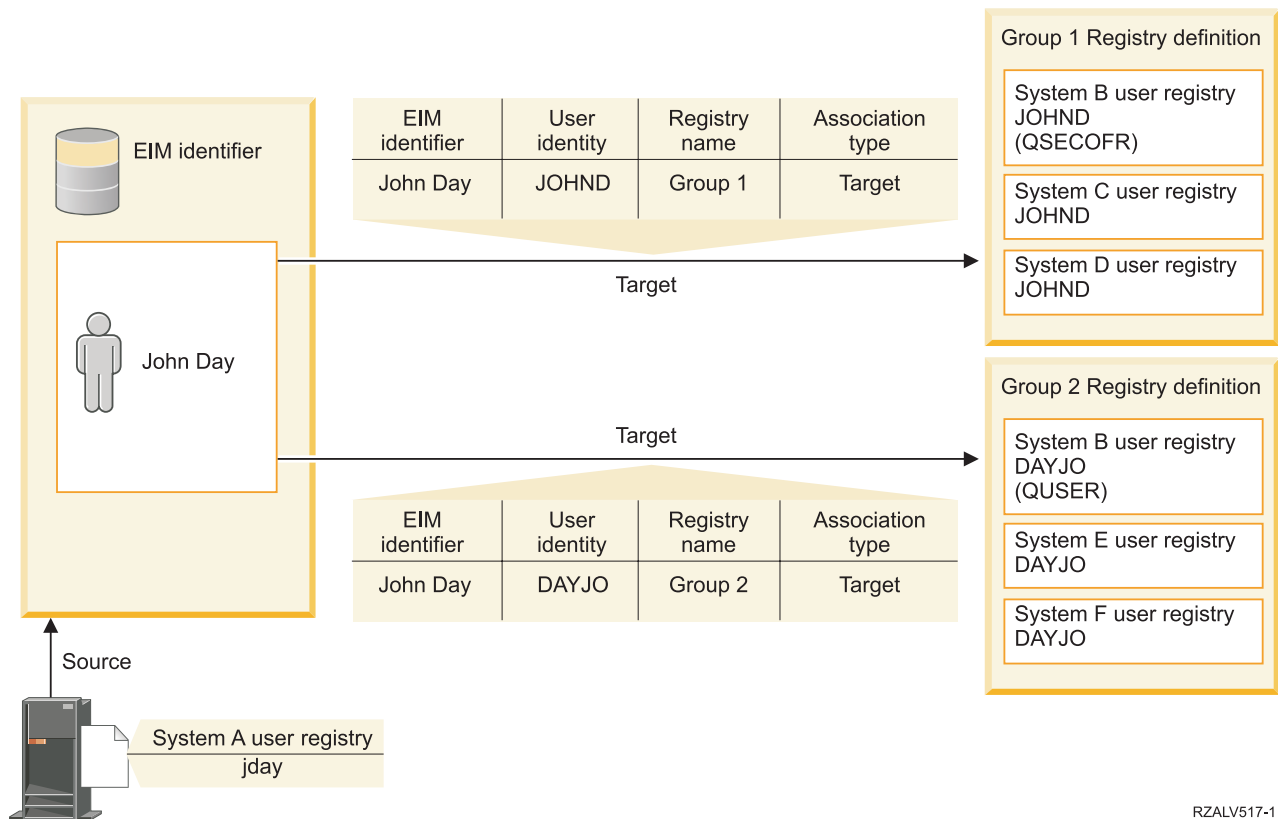
Use this example to learn about lookup operations returning ambiguous results that involve group registry definitions.

In some cases a mapping lookup operation returns ambiguous results when more than one target user identity matches the specified lookup criteria. Because an ambiguous results situation could cause applications that use EIM to fail or give unexpected results, you must take action to prevent or resolve the situation.

In particular, be aware that lookup operations can return ambiguous results when you specify an individual user registry definition as a member of more than one group registry definition. If an individual user registry definition is a member of multiple group registry definitions and you create individual EIM identifier associations or policy associations that use a group registry definition as either the source registry or target registry, lookup operations might return ambiguous results. For example, you

might use two different user identities for two different types of system tasks that you perform: you perform tasks as a security administrator that require a user identity with QSECOFR authority, and you perform typical user tasks that require a user identity with QUSER authority. If both of your user identities reside within the individual user registry that is a member of two different group registry definitions and you create target identifier associations to both of the target user identities, lookup operations finds both of the target user identities and consequently returns ambiguous results.

The following example describes how this problem can occur when you specify an individual user registry as a member of two group registry definitions and you specify one of the group registry definitions as the target registry in two individual EIM identifier associations.



RZALV517-1

Example:

John Day has the following user identities within a system registry definition called System B user registry:

- JOHND
- DAYJO

System B user registry is a member of the following group registry definitions:

- Group 1
- Group 2

EIM identifier John Day has two target associations with the following specifications:

- Target association: Target registry is Group 1 which contains user identity JOHND in System B user registry.
- Target association: Target registry is Group 2 which contains user identity DAYJO in System B user registry.

In this situation, the mapping lookup operation returns ambiguous results because more than one target user identity matches the specified lookup criteria; both user identities (JOHND and DAYOJO) match the specified lookup criteria.

Similarly, mapping lookup operations might return ambiguous results if you create two policy associations (rather than individual EIM identifier associations) that use group registry definitions as target registries.

To prevent lookup operations from returning ambiguous results that involve group registry definitions, consider the following guidelines:

- Specify an individual user registry as a member of no more than one group registry definition.
- Use caution when creating individual EIM identifier associations or policy associations that use group registry definitions as either the source registry or target registry. Verify that the group registry definition is a member of no more than one group registry definition. Be aware that if a member of the target group registry definition is also a member of another group registry definition, lookup operations can return ambiguous results.
- If you have an ambiguous results situation where you specify an individual registry definition as a member of multiple group registry definitions, and you create an individual identifier association or policy association that uses one of those group registry definitions as either the source registry or target registry, you can define unique lookup information for each target user identity in each association to further refine the search.

You might define the following lookup information for each target user identity in the example about John Day:

- For JOHND: Define Administrator as the lookup information
- For DAYJO: Define User as the lookup information

However, base i5/OS applications such as System i Access for Windows can not use lookup information to distinguish among multiple target user identities returned by a lookup operation. Consequently, you might consider redefining associations for the domain to ensure that a mapping lookup operation can return a single target user identity to ensure that base i5/OS applications can successfully perform lookup operations and map identities.

Related concepts

“Group registry definitions” on page 14

Logically grouping the registry definitions allows you to reduce the amount of work that you must perform to configure EIM mapping. You can manage a group registry definition similarly to the way that you manage an individual registry definition.

EIM mapping policy support and enablement

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain. You can use policy associations instead of, or in combination with, identifier associations.

EIM mapping policy support provides a means of enabling and disabling the use of policy associations for the entire domain, as well as for each specific target user registry. EIM also allows you to set whether a specific registry can participate in mapping lookup operations in general. Consequently, you can use mapping policy support to more precisely control how mapping lookup operations return results.

The default setting for an EIM domain is that mapping lookups that use policy associations are disabled for the domain. When the use of policy associations is disabled for the domain, all mapping lookup operations for the domain return results only by using specific, identifier associations between user identities and EIM identifiers.

The default settings for each individual registry are that mapping lookup participation is enabled and the use of policy associations is disabled. When you enable the use of policy associations for an individual target registry, you must also ensure that this setting is enabled for the domain.

You can configure mapping lookup participation and the use of policy associations for each registry in one of three ways:

- Mapping lookup operations can not be used for the specified registry at all. In other words, an application that performs a mapping lookup operation involving that registry will fail to return results.
- Mapping lookup operations can use specific identifier associations between user identities and EIM identifiers only. Mapping lookups are enabled for the registry, but the use of policy associations is disabled for the registry.
- Mapping lookup operations can use specific identifier associations when they exist and policy associations when specific identifier associations do not exist (all settings are enabled).

Related concepts

“Lookup information” on page 15

With Enterprise Identity Mapping (EIM) you can provide optional data called lookup information to further identify a target user identity. This target user identity can be specified either in an identifier association or in a policy association.

“Default domain policy associations” on page 20

A default domain policy association is one type of policy association that you can use to create many-to-one mappings between user identities.

“Default registry policy associations” on page 22

A default registry policy association is one type of policy association that you can use to create many-to-one mappings between user identities.

“Creating a policy association” on page 100

A policy association provides a means to directly define a relationship between multiple user identities in one or more registries and an individual target user identity in another registry.

Related tasks

“Enabling policy associations for a domain” on page 85

A policy association provides a means of creating many-to-one mappings in situations where associations between user identities and an Enterprise Identity Mapping (EIM) identifier do not exist.

“Enabling mapping lookup support and the use of policy associations for a target registry” on page 93

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as a means of creating many-to-one mappings in situations where associations between user identities and an EIM identifier do not exist. You can use a policy association to map a source set of multiple user identities (rather than a single user identity) to a single target user identity in a specified target user registry.

EIM access control

An Enterprise Identity Mapping (EIM) user is a user who possesses EIM access control based on their membership in a predefined Lightweight Directory Access Protocol (LDAP) user group for a specific domain.

Specifying EIM access control for a user adds that user to a specific LDAP user group for a particular domain. Each LDAP group has authority to perform specific EIM administrative tasks for that domain. Which and what type of administrative tasks, including lookup operations, an EIM user can perform is determined by the access control group to which the EIM user belongs.

Note: To configure EIM, you need to prove that you are trusted within the context of the network, not by one specific system. Authorization to configure EIM is not based on your i5/OS user profile authority, but rather on your EIM access control authority. EIM is a network resource, not a resource for any one particular system; consequently, EIM doesn't recognize i5/OS-specific special authorities such as *ALLOBJ and *SECADM for configuration. Once EIM is configured, however,

authorization to perform tasks can be based on a number of different user types, including i5/OS user profiles. For example, the IBM Tivoli Directory Server for i5/OS treats i5/OS profiles with *ALLOBJ and *IOSYSCFG special authority as directory administrators.

Only users with EIM administrator access control can add other users to an EIM access control group or change other users access control settings. Before a user can become a member of an EIM access control group, that user must have an entry in the directory server that acts as the EIM domain controller. Also, only specific types of users can be made a member of an EIM access control group. The user identity can be in the form of a Kerberos principal, an LDAP distinguished name, or an i5/OS user profile so long as the user identity is defined to the directory server.

Note: To have the Kerberos principal user type available in EIM, network authentication service must be configured on the system. To have the i5/OS user profile type available in EIM, you must configure a system object suffix on the directory server. This allows the directory server to reference i5/OS system objects, such as i5/OS user profiles.

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

Lightweight Directory Access Protocol (LDAP) administrator

The LDAP administrator is a special distinguished name (DN) in the directory that is an administrator for the entire directory. Thus, the LDAP administrator has access to all EIM administrative functions, as well as access to the entire directory. A user with this access control can perform the following functions:

- Create a domain.
- Delete a domain.
- Create and remove EIM identifiers.
- Create and remove EIM registry definitions.
- Create and remove source, target, and administrative associations.
- Create and remove policy associations.
- Create and remove certificate filters.
- Enable and disable the use of policy associations for a domain.
- Enable and disable mapping lookups for a registry.
- Enable and disable the use of policy associations for a registry.
- Perform EIM lookup operations.
- Retrieve identifier associations, policy associations, certificate filters, EIM identifiers, and EIM registry definitions.
- Add, remove, and list EIM access control information.
- Change and remove credential information for a registry user.

EIM administrator

Membership in this access control group allows the user to manage all of the EIM data within this EIM domain. A user with this access control can perform the following functions:

- Delete a domain.
- Create and remove EIM identifiers.
- Create and remove EIM registry definitions.
- Create and remove source, target, and administrative associations.
- Create and remove policy associations.
- Create and remove certificate filters.
- Enable and disable the use of policy associations for a domain.

- Enable and disable mapping lookups for a registry.
- Enable and disable the use of policy associations for a registry.
- Perform EIM lookup operations.
- Retrieve identifier associations, policy associations, certificate filters, EIM identifiers, and EIM registry definitions.
- Add, remove, and list EIM access control information.
- Change and remove credential information for a registry user.

Identifier administrator

Membership in this access control group allows the user to add and change EIM identifiers and manage source and administrative associations. A user with this access control can perform the following functions:

- Create EIM identifiers.
- Add and remove source associations.
- Add and remove administrative associations.
- Perform EIM lookup operations.
- Retrieve identifier associations, policy associations, certificate filters, EIM identifiers, and EIM registry definitions.

EIM mapping operations

Membership in this access control group allows the user to conduct EIM mapping lookup operations. A user with this access control can perform the following functions:

- Perform EIM lookup operations.
- Retrieve identifier associations, policy associations, certificate filters, EIM identifiers, and EIM registry definitions.

Registry administrator

Membership in this access control group allows the user to manage all EIM registry definitions. A user with this access control can perform the following functions:

- Add and remove target associations.
- Create and remove policy associations.
- Create and remove certificate filters.
- Enable and disable mapping lookups for a registry.
- Enable and disable the use of policy associations for a registry.
- Perform EIM lookup operations.
- Retrieve identifier associations, policy associations, certificate filters, EIM identifiers, and EIM registry definitions.

Administrator for selected registries

Membership in this access control group allows the user to manage EIM information only for a specified user registry definition (such as Registry_X). Membership in this access control group also allows the user to add and remove target associations only for a specified user registry definition. To take full advantage of mapping lookup operations and policy associations, a user with this access control should also have **EIM mapping operations** access control. This access control allows a user to perform the following functions for specific authorized registry definitions:

- Create, remove, and list target associations for the specified EIM registry definitions only.
- Add and remove default domain policy associations.

- Add and remove policy associations for the specified registry definitions only.
- Add certificate filters for the specified registry definitions only.
- Enable and disable mapping lookups for the specified registry definitions only.
- Enable and disable the use of policy associations for the specified registry definitions only.
- Retrieve EIM identifiers.
- Retrieve identifier associations and certificate filters for the specified registry definitions only.
- Retrieve EIM registry definition information for the specified registry definitions only.

Note: If the specified registry definition is a group registry definition, a user with Administrator for selected registries access control has administrator access to the group only, not to the members of the group.

A user with both **Administrator for selected registries** access control and **EIM mapping lookup operations** access control gains the ability to perform the following functions:

- Add and remove policy associations only for the specified registries.
- Perform EIM lookup operations.
- Retrieve all identifier associations, policy associations, certificate filters, EIM identifiers, and EIM registry definitions.

Credential lookup

This access control group allows the user to retrieve credential information, such as passwords.

If a user with this access control wants to perform an additional EIM operation, the user needs to be a member of the access control group that provides authority for the desired EIM operation. For example, if a user with this access control wants to retrieve the target association from a source association, the user needs to be a member of one of the following access control groups:

- EIM administrator
- Identifier administrator
- EIM mapping lookup operations
- Registry administrator

Related concepts

“i5/OS user profile considerations for EIM” on page 47

Being able to perform tasks in Enterprise Identity Mapping (EIM) is not based on your i5/OS user profile authority, but rather on your EIM access control authority.

“Identifying needed skills and roles” on page 51

Enterprise Identity Mapping (EIM) is designed so that a single person can easily be responsible for configuration and administration in a small organization. Or, in a larger organization, you may prefer to have a number of different individuals handle these responsibilities.

Related tasks

“Managing EIM user access control” on page 113

An Enterprise Identity Mapping (EIM) user is a user who possesses EIM access control based on their membership in predefined Lightweight Directory Access Protocol (LDAP) user groups. Specifying EIM access control for a user adds that user to a specific LDAP user group.

EIM access control group: API authority

This information displays tables that are organized by the Enterprise Identity Mapping (EIM) operation that the API performs.

Each of the following tables displays each EIM API, the different EIM access control groups, and the whether the access control group has authority to perform a specific EIM function.

Table 1. Working with domains

| EIM API | LDAP administrator | EIM administrator | Identifiers administrator | EIM mapping lookup | Registry administrator | Aministrator for selected registry |
|-----------------|--------------------|-------------------|---------------------------|--------------------|------------------------|------------------------------------|
| eimChangeDomain | X | X | - | - | - | - |
| eimCreateDomain | X | - | - | - | - | - |
| eimDeleteDomain | X | X | - | - | - | - |
| eimListDomains | X | X | - | - | - | - |

Table 2. Working with identifiers

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

Table 3. Working with registries

| EIM API | LDAP administrator | EIM administrator | EIM identifiers administrator | EIM mapping lookup | EIM registries administrator | EIM registry X administrator |
|------------------------------|--------------------|-------------------|-------------------------------|--------------------|------------------------------|------------------------------|
| eimAddApplication Registry | X | X | - | - | - | - |
| eimAddSystemRegistry | X | X | - | - | - | - |
| eimChangeRegistry | X | X | - | - | X | X |
| eimChange RegistryUser | X | X | - | - | X | X |
| eimChangeRegistryAlias | X | X | - | - | X | X |
| eimGetRegistry NameFromAlias | X | X | X | X | X | X |
| eimListRegistries | X | X | X | X | X | X |
| eimListRegistry Associations | X | X | X | X | X | X |
| eimListRegistryAliases | X | X | X | X | X | X |
| eimListRegistry Users | X | X | X | X | X | X |
| eimRemoveRegistry | X | X | - | - | - | - |

Table 4. Working with identifier associations. For `eimAddAssociation()` and `eimRemoveAssociation()` APIs there are four parameters that determine the type of association that is either being added or removed. The authority to these APIs differs based on the type of association specified in these parameters. In the following table, the type of association is included for each of these APIs.

| EIM API | LDAP administrator | EIM administrator | EIM identifiers administrator | EIM mapping lookup | EIM registries administrator | EIM registry X administrator |
|------------------------------------|--------------------|-------------------|-------------------------------|--------------------|------------------------------|------------------------------|
| eimAddAssociation (administrative) | X | X | X | - | - | - |
| eimAddAssociation (source) | X | X | X | - | - | - |

Table 4. Working with identifier associations (continued). For `eimAddAssociation()` and `eimRemoveAssociation()` APIs there are four parameters that determine the type of association that is either being added or removed. The authority to these APIs differs based on the type of association specified in these parameters. In the following table, the type of association is included for each of these APIs.

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

Table 5. Working with policy associations

| EIM API | LDAP administrator | EIM administrator | EIM identifiers administrator | EIM mapping lookup | EIM registries administrator | EIM registry X administrator |
|---|--------------------|-------------------|-------------------------------|--------------------|------------------------------|------------------------------|
| <code>eimAddPolicyAssociation</code> | X | X | - | - | X | X |
| <code>eimAddPolicyFilter</code> | X | X | - | - | X | X |
| <code>eimListPolicyFilters</code> | X | X | X | X | X | X |
| <code>eimRemovePolicyAssociation</code> | X | X | | | X | X |
| <code>eimRemovePolicyFilter</code> | - | - | - | - | - | |

Table 6. Working with mappings

| EIM API | LDAP administrator | EIM administrator | EIM identifiers administrator | EIM mapping lookup | EIM registries administrator | EIM registry X administrator |
|---|--------------------|-------------------|-------------------------------|--------------------|------------------------------|------------------------------|
| <code>eimGetAssociatedIdentifier</code> | X | X | X | X | X | X |
| <code>eimGetTargetFromIdentifier</code> | X | X | X | X | X | X |
| <code>eimGetTargetFromSource</code> | X | X | X | X | X | X |

Table 7. Working with access

| EIM API | LDAP administrator | EIM administrator | EIM identifiers administrator | EIM mapping lookup | EIM registries administrator | EIM registry X administrator |
|--------------------------------|--------------------|-------------------|-------------------------------|--------------------|------------------------------|------------------------------|
| <code>eimAddAccess</code> | X | X | - | - | - | - |
| <code>eimListAccess</code> | X | X | - | - | - | - |
| <code>eimListUserAccess</code> | X | X | - | - | - | - |
| <code>eimQueryAccess</code> | X | X | - | - | - | - |
| <code>eimRemoveAccess</code> | X | X | - | - | - | - |

EIM access control group: EIM task authority

This information displays a table that explains the relationships between the different Enterprise Identity Mapping (EIM) access control groups and the EIM tasks that they can perform.

Although the LDAP administrator is not listed in the table, this level of access control is required to create a new EIM domain. Also, the LDAP administrator has the same access control as the EIM administrator, but the EIM administrator does not automatically have LDAP administrator access control.

Table 8. Table 1: EIM access control groups

| EIM task | EIM administrator | Identifier administrator | EIM mapping lookup operations | Registry administrator | Administrator for selected registry | Credential lookup |
|---|-------------------|--------------------------|-------------------------------|------------------------|-------------------------------------|-------------------|
| Create domain | - | - | - | - | - | |
| Delete domain | X | - | - | - | - | |
| Modify domain | X | - | - | - | - | |
| Enable/Disable Policy Associations for Domain | X | - | - | - | - | |
| Search for Domains | X | - | - | - | - | |
| | | | | | | |
| Add System Registry | X | - | - | - | - | |
| Add Application Registry | X | - | - | - | - | |
| Remove Registry | X | - | - | - | - | |
| Modify Registry | X | - | - | X | X | |
| Enable/Disable Mapping Lookups for Registry | X | - | - | X | X | |
| Enable/Disable Policy Associations for 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 | |
| | | | | | | |

Table 8. Table 1: EIM access control groups (continued)

| EIM task | EIM administrator | Identifier administrator | EIM mapping lookup operations | Registry administrator | Administrator for selected registry | Credential lookup |
|---|-------------------|--------------------------|-------------------------------|------------------------|-------------------------------------|-------------------|
| Add/Remove Administrative Association | X | X | - | - | - | |
| Add/Remove Source Association | X | X | - | - | - | |
| Add/Remove Target Association | X | - | - | X | X | |
| Add/Remove Policy Association | X | - | - | X | X | |
| Add/Remove certificate filter | X | - | - | X | X | |
| Search for Certificate Filter | X | X | X | X | X | |
| Search for Associations | X | X | X | X | X | |
| Search for Policy Associations | X | X | X | X | X | |
| Retrieve Target Association from Source Association | 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 | |
| Retrieve Registry from Alias | X | X | X | X | X | |
| | | | | | | |
| Add/Remove EIM Access Control | X | - | - | - | - | |

Table 8. Table 1: EIM access control groups (continued)

| EIM task | EIM administrator | Identifier administrator | EIM mapping lookup operations | Registry administrator | Administrator for selected registry | Credential lookup |
|--|-------------------|--------------------------|-------------------------------|------------------------|-------------------------------------|-------------------|
| Display Access Control Group Members | X | - | - | - | - | |
| Display EIM Access Control for a Specified User | X | - | - | - | - | |
| Query EIM Access Control | X | - | - | - | - | |
| | | | | | | |
| Modify Credential | X | - | - | - | - | - |
| Retrieve Credential | X | - | - | - | - | X |
| 1 - If the specified registry definition is a group registry definition, a user with Administrator for selected registries access control has administrator access to the group only, not to the members of the group. | | | | | | |

LDAP concepts for EIM

EIM uses a LDAP server as a domain controller to store EIM data. Consequently, you should understand some LDAP concepts that relate to configuring and using EIM in your enterprise. For example, you can use an LDAP distinguished name as the user identity to configure EIM and to authenticate to the EIM domain controller.

To have a better understanding of configuring and using EIM, you should understand the following LDAP concepts:

Distinguished name

A distinguished name (DN) is a LDAP entry that uniquely identifies and describes an entry in a directory (LDAP) server. You use the Enterprise Identity Mapping (EIM) Configuration wizard to configure the directory server to store EIM domain information. Because EIM uses the directory server to store EIM data, you can use distinguished names as a means of authenticating to the EIM domain controller.

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

Because EIM uses the directory server to store EIM data, you can use a distinguished name for the user identity that authenticates to the domain controller. You also can use a distinguished name for the user identity that configures EIM for your System i platform. For example, you can use a distinguished name when you do the following:

- Configure the directory server to act as the EIM domain controller. You do this by creating and using the 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 distinguished name must represent a user who is authorized to create objects in the local namespace of the Directory server.
- Use the EIM Configuration wizard to select the type of user to perform EIM operations on behalf of operating system functions. These operations include mapping lookup operations and deleting associations when deleting a local i5/OS 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.
- Create certificate filters to determine the scope of a certificate filter policy association. When you create a certificate filter, you must supply distinguished name information for either the Subject DN or the Issuer DN or the certificate to specify the criteria that the filter uses to determine which certificates are affected by the policy association.

Related concepts

“Parent distinguished name”

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

“Certificate filters” on page 25

A certificate filter defines a set of similar distinguished name certificate attributes for a group of user certificates in an X.509 source user registry. You can use the certificate filter as the basis of a certificate filter policy association.

Related information

Directory server concepts

Parent distinguished name

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

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

Enterprise Identity Mapping (EIM) uses a directory server as a domain controller for storing EIM domain data. The parent DN combined with the EIM domain name determines the location of EIM domain data in the directory server namespace. When you use the EIM Configuration wizard to create and join a new domain, you can choose to specify a parent DN for the domain that you are creating. By using a parent DN, you can specify where in the 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 and the default location of the EIM domain data is `ibm-eimDomainName=EIM`.

Related concepts

“Distinguished name” on page 44

A distinguished name (DN) is a LDAP entry that uniquely identifies and describes an entry in a directory (LDAP) server. You use the Enterprise Identity Mapping (EIM) Configuration wizard to configure the directory server to store EIM domain information. Because EIM uses the directory server to store EIM data, you can use distinguished names as a means of authenticating to the EIM domain controller.

Related information

Directory server concepts

LDAP schema and other considerations for EIM

Use this information to learn what is required for the directory server to function with Enterprise Identity Mapping (EIM).

EIM requires that the domain controller be hosted by a directory server that supports Lightweight Directory Access Protocol (LDAP) Version 3. Additionally, the directory server product must be able to accept the EIM schema and understand the following attributes and object classes:

- The `ibm-entryUUID` attribute.
- The `ibmattributetypes`:
 - `acIEntry`
 - `acIPropagate`
 - `acISource`
 - `entryOwner`
 - `ownerPropagate`
 - `ownerSource`
- EIM attributes, including three new attributes for policy association support:
 - `ibm-eimAdditionalInformation`
 - `ibm-eimAdminUserAssoc`
 - `ibm-eimDomainName`, `ibm-eimDomainVersion`,
 - `ibm-eimRegistryAliases`
 - `ibm-eimRegistryEntryName`
 - `ibm-eimRegistryName`
 - `ibm-eimRegistryType`
 - `ibm-eimSourceUserAssoc`
 - `ibm-eimTargetIdAssoc`
 - `ibm-eimTargetUserName`
 - `ibm-eimUserAssoc`
 - `ibm-eimFilterType`
 - `ibm-eimFilterValue`
 - `ibm-eimPolicyStatus`
- EIM object classes, including three new classes for policy association support:
 - `ibm-eimApplicationRegistry`
 - `ibm-eimDomain`
 - `ibm-eimIdentifier`
 - `ibm-eimRegistry`
 - `ibm-eimRegistryUser`
 - `ibm-eimSourceRelationship`
 - `ibm-eimSystemRegistry`
 - `ibm-eimTargetRelationship`
 - `ibm-eimFilterPolicy`
 - `ibm-eimDefaultPolicy`
 - `ibm-eimPolicyListAux`

Related concepts

“EIM domain controller” on page 5

An EIM domain controller is a Lightweight Directory Access Protocol (LDAP) server that is configured to manage one or more EIM domains. An EIM domain consists of all the EIM identifiers, EIM associations, and user registries that are defined in that domain. Systems (EIM clients) participate in the EIM domain by using the domain data for EIM lookup operations.

Enterprise Identity Mapping concepts for i5/OS

- | You can implement EIM on any IBM eServer platform. However, when you implement EIM on a System i model, you should be aware of some information that is specific to the System i implementation.

Review the following information to learn about i5/OS applications that are enabled for EIM, user profile considerations, and other topics that can help you use EIM on a System i platform effectively:

i5/OS user profile considerations for EIM

Being able to perform tasks in Enterprise Identity Mapping (EIM) is not based on your i5/OS user profile authority, but rather on your EIM access control authority.

There are some additional tasks that need to be performed to set up i5/OS to use EIM. These additional tasks require you to have an i5/OS user profile with the appropriate special authorities.

To set up i5/OS to use EIM using System i Navigator, your user profile must have the following special authorities:

- Security administrator (*SECADM).
- All object (*ALLOBJ).
- System configuration (*IOSYSCFG).

i5/OS user profile command enhancement for EIM identifiers

Once you configure EIM for your system, you can take advantage of a new parameter for both the Create user profile (CRTUSRPRF) command and the Change user profile (CHGUSRPRF) command, called EIMASSOC. You can use this parameter to define EIM identifier associations for the specified user profile for the local registry.

When you use this parameter, you can specify the following information:

- EIM identifier name, which can be a new name or an existing identifier name.
- An action option for the association, which can be to add (*ADD), to replace (*REPLACE), or to remove (*REMOVE), the association that you specify.

Note: Use the *ADD to set up new associations. Use the *REPLACE option, for example, if you previously defined associations to the wrong identifier. The *REPLACE option removes any existing associations of the specified type for the local registry to any other identifiers, and then adds the one that is specified for the parameter. Use the *REMOVE option to remove any specified associations from the specified identifier.

- The type of identifier association, which can be target, source, both a target and a source, or an administrative association.
- Whether to create the specified EIM identifier if it does not already exist.

You typically create a target association for an i5/OS profile, especially in a single sign-on environment. After you use the command to create the needed target association for the user profile (and the EIM identifier, if necessary), you may need to create a corresponding source association. You can use System i Navigator to create a source association for another user identity, such as the Kerberos principal with which the user signs on to the network.

When you configured EIM for the system, you specified a user identity and password for the system to use when performing EIM operations on behalf of the operating system. This user identity must have EIM access control authority sufficient for creating identifiers and adding associations.

i5/OS user profile passwords and EIM

As an administrator, your primary goal for configuring EIM as part of a single sign-on environment is to reduce the amount of user password management that you must perform for the typical end users in your enterprise. By using the identity mapping that EIM provides in combination with Kerberos authentication, you know that your users will have to perform fewer logons and remember and manage fewer passwords. You benefit because you have fewer calls to manage problems for the mapped user identities, such as calls to reset these passwords when users forget them. However, your security policy password rules are still in effect and you must still manage these user profiles for users whenever the password expires.

To further benefit from your single sign-on environment, you may want to consider changing the password setting for those user profiles that are the target of identity mappings. As the target of an identity mapping, the user no longer needs to provide the password for the user profile when the user accesses a System i platform or EIM-enabled i5/OS resource. For typical users, you can change the password setting to *NONE so that no password can be used with the user profile. The owner of the user profile no longer needs a password because of identity mapping and single sign-on. By setting the password to *NONE, you benefit further because you and your users no longer have to manage password expiration; additionally, no one can use the profile to directly signon to a System i platform or access EIM-enabled i5/OS resources. However, you may prefer that administrators continue to have a password value for their user profiles in case they ever need to signon directly to a System i platform. For example, if your EIM domain controller is down and identity mapping can not occur, an administrator may need to be able to signon directly to an System i platform until the problem with the domain controller is resolved.

Related concepts

“EIM access control” on page 36

An Enterprise Identity Mapping (EIM) user is a user who possesses EIM access control based on their membership in a predefined Lightweight Directory Access Protocol (LDAP) user group for a specific domain.

Related information

Create user profile (CRTUSRPRF) command

i5/OS auditing for EIM

What auditing you perform is an important consideration for your overall security plan.

When you configure and use Enterprise Identity Mapping (EIM), you may want to configure auditing support for the directory server to ensure you provide the appropriate level of accountability that your security policy requires. For example, auditing support can be helpful in determining which of the users mapped by a policy association performed an action on your system or changed an object.

Related information

Directory Server Auditing

EIM enabled applications for i5/OS

EIM can use a variety of i5/OS applications.

The following i5/OS applications can be configured to use Enterprise Identity Mapping (EIM):

- i5/OS host servers (currently used by System i Access for Windows
- and System i Navigator)
- Telnet Server (currently used by PC5250 and IBM Websphere host on demand)
- QFileSrv.400 ODBC (allows the use of single sign-on through SQL)

- JDBC (allows the use of EIM through SQL)
- Distributed Relational Database Architecture™ (DRDA®) (allows the use of EIM through SQL)
- IBM WebSphere Host On-Demand Version 8, (Web Express Logon feature)
- i5/OS NetServer™
- QFileSvr.400

Scenarios: Enterprise Identity Mapping

Use this information to learn how to manage user identities across different systems within a single sign-on environment.

Enterprise Identity Mapping (EIM) is an IBM infrastructure technology that allows you to track and manage user identities across an enterprise. Typically, you use EIM with an authenticating technology, such as network authentication service to implement a single sign-on environment.

Related information

Single signon scenarios

Planning for Enterprise Identity Mapping

Before you setup EIM you should develop an Enterprise Identity Mapping (EIM) implementation plan to ensure that you successfully configure EIM for a System i environment or in a mixed platform environment.

An implementation plan is essential to successfully configuring and using Enterprise Identity Mapping (EIM) in your enterprise. To develop your plan, you need to collect data about the systems, applications, and users that will use EIM. You will use the information you gather to make decisions about how to best configure EIM for your enterprise.

Because EIM is an IBM eServer infrastructure technology available for all IBM platforms, how you plan your implementation depends on what platforms are in your enterprise. Although there are a number of planning activities that are specific to each platform, many EIM planning activities apply to all IBM platforms. You should work through the common EIM planning activities to create your overall implementation plan. To learn more about how to plan your EIM implementation, review these pages:

Planning Enterprise Identity Mapping for eServer

An implementation plan is essential to successfully configuring and using Enterprise Identity Mapping (EIM) in a mixed platform enterprise. To develop your implementation plan, you need to collect data about the systems, applications, and users that will use EIM. You will use the information you gather to make decisions about how best to configure EIM for a mixed platform environment.

The following list provides a roadmap of the planning tasks that you should complete before configuring and using EIM in a mixed platform environment. Read through the information in these pages to learn how to successfully plan your EIM configuration needs, including what skills your implementation team needs, what information you need to gather, and configuration decisions you need to make. You may find it helpful to print the EIM planning work sheets (number 8 in the list below) so you can complete them as you work through the planning process.

Enterprise Identity Mapping setup requirements for eServer

To implement Enterprise Identity Mapping (EIM) successfully, you must meet three requirements: enterprise or network level, system, and application.

Enterprise or network level requirements

You must configure one system in your enterprise or network to act as an EIM domain controller, which is a specially configured Lightweight Directory Access Protocol (LDAP) server that stores and provides EIM domain data. There are a number of considerations for choosing which directory services product to use as a domain controller, including the fact that not all LDAP server products provide EIM domain controller support.

Another consideration is the availability of administration tools. One option is that you can use the EIM APIs in your own applications to perform administrative functions. If you plan to use the IBM Tivoli Directory Server for i5/OS as the EIM domain controller, you can use System i Navigator to manage EIM. If you plan to use the IBM Directory product, you can use the `eimadmin` utility that is part of the V1R4 LDAP SPE.

The following information provides basic information about which IBM platforms provide a directory server product that supports EIM. You can find more detailed information about choosing a directory server to provide EIM domain controller support in [Plan an EIM domain controller](#).

System and application requirements

Each system that participates in an EIM domain must meet the following requirements:

- Have LDAP client software installed.
- Have an implementation of the EIM APIs.

Each application that will participate in an EIM domain must be able to use the EIM APIs to perform mapping lookup and other operations.

Note: In the case of a distributed application, it may not be necessary that both the server side and the client side be able to use the EIM APIs. Typically, only the server side of the application may need to use the EIM APIs.

The following table provides information about the EIM support that the eServer platforms provide. Information is organized by platform with columns that indicate the following:

- The EIM client needed for the platform to support the EIM APIs.
- The type of EIM configuration and administration tools are available for the platform.
- The directory server product that can be installed for the platform to serve as an EIM domain controller.

A platform does not have to be able to serve as an EIM domain controller to participate in an EIM domain.

Table 9. eServer EIM support


| Platform | EIM client (API support) | Domain controller | EIM administration tools |
|--|---|---------------------------------------|--------------------------|
| AIX on System p™ | AIX R5.2 | IBM Directory V5.1 | Not available |
| Linux <ul style="list-style-type: none">• SLES8 on PPC64• Red Hat 7.3 on i386• SLES7 on System z | Download one of these: <ul style="list-style-type: none">• IBM Directory V4.1 client• IBM Directory V5.1 client• Open LDAP v2.0.23 client  | IBM Directory V5.1 | Not available |
| i5/OS on System i | i5/OS V5R3, or later | IBM Tivoli Directory Server for i5/OS | System i Navigator |

Table 9. eServer EIM support (continued)

| Platform | EIM client (API support) | Domain controller | EIM administration tools |
|---------------------------------------|---|---------------------------|--------------------------|
| Windows 2000 on System X [™] | Download one of these: <ul style="list-style-type: none"> • IBM Directory V4.1 client • IBM Directory V5.1 client | IBM Directory V5.1 client | Not available |
| z/OS on System z [™] | z/OS V1R4 LDAP SPE OW57137 | z/OS V1R4 LDAP | V1R4 LDAP SPE OW57137 |

As long as a platform provides EIM client (API) support that system can participate in an EIM domain. It is not necessary that a platform provide EIM domain controller support unless you want to use that particular platform as the EIM domain controller for your enterprise.

Related information

 IBM Tivoli Directory Server

Identifying needed skills and roles

Enterprise Identity Mapping (EIM) is designed so that a single person can easily be responsible for configuration and administration in a small organization. Or, in a larger organization, you may prefer to have a number of different individuals handle these responsibilities.

The number of people that you need on your team varies depending on the number of required skills that each team member possesses, the types of platforms involved in your EIM implementation, and how your organization prefers to divide its security roles and responsibilities.

A successful EIM implementation requires the configuration and interaction of several software products. Because each of these products requires specific skills and roles, you may choose to create an EIM implementation team that consists of people from several different disciplines, particularly if you work in a large organization.

The following information describes the skills and EIM access control authority required to implement EIM successfully. These skills are presented in terms of job titles for people who specialize in those skills. For example, a task requiring Lightweight Directory Access Protocol (LDAP) skills is referred to as a task for a Directory Server administrator.

Team members and their roles

The following information describes the responsibilities and required authority of the roles that are needed for managing EIM. You can use this list of roles to determine the team members that are needed to install and configure prerequisite products and to configure EIM and one or more EIM domains.

One of the first sets of roles that you need to define is the number and type of administrators for your EIM domain. All personnel that are given EIM administrative duties and authority need to be involved in the EIM planning process as members of the EIM implementation team.

Note: EIM administrators play an important role in your organization and have as much power as individuals that are allowed to create user identities on your systems. When they create EIM associations for user identities, they determine who can access your computer systems and what privileges they have when doing so. IBM recommends that you give this authority to those individuals in whom you have a high level of trust based on your company's security policy.

The following table lists potential team member roles and the tasks and skills needed for configuring and managing EIM.

Note: If a single person in your organization will be responsible for all EIM configuration and administration tasks, that person should be given the role and authority of EIM administrator.

Table 10. Roles, tasks, and skills for configuring EIM

| Role | Authorized tasks | Required skills |
|---------------------------------------|--|--|
| EIM administrator | <ul style="list-style-type: none"> Coordinating domain operations Adding, removing, and changing registry definitions, EIM identifiers, and associations for user identities Controller authority to the data within an EIM domain | Knowledge of the EIM administration tools |
| EIM identifiers administrator | <ul style="list-style-type: none"> Creating and changing EIM identifiers Adding and removing administrative and source associations (cannot add or remove target associations) | Knowledge of the EIM administration tools |
| EIM registries administrator | Managing all EIM registry definitions: <ul style="list-style-type: none"> Adding and removing target associations (cannot add or remove source and administrative associations) Updating EIM registry definitions | Knowledge of: <ul style="list-style-type: none"> All the user registries defined to the EIM domain (such as information about user identities) The EIM administration tools |
| EIM registry X administrator | Managing a specific EIM registry definition: <ul style="list-style-type: none"> Adding and removing target associations for a specific user registry (for example, registry X) Updating a specific EIM registry definition | Knowledge of: <ul style="list-style-type: none"> The particular user registry defined to the EIM domain (such as information about user identities) The EIM administration tools |
| Directory server (LDAP) administrator | <ul style="list-style-type: none"> Installing and configuring a directory server (if necessary) Customizing directory server configuration for EIM Creating an EIM domain (see note) Defining users that are authorized to access the EIM domain controller Optional: Defining the first EIM administrator <p>Note: The directory server administrator can do everything that an EIM administrator can do.</p> | Knowledge of: <ul style="list-style-type: none"> Directory server installation, configuration, and customization EIM administration tools |
| User registry administrator | <ul style="list-style-type: none"> Setting up user profiles or user identities for a specific user registry Optional: Serving as an EIM registry administrator for specified user registry | Knowledge of: <ul style="list-style-type: none"> Tools for administering the user registry EIM administration tools |

Table 10. Roles, tasks, and skills for configuring EIM (continued)

| Role | Authorized tasks | Required skills |
|---|--|---|
| System programmer or System administrator | Installing needed software products (may include installing EIM) | Knowledge of: <ul style="list-style-type: none"> • System programming or administration skills • Installation procedures for the platform |
| Application programmer | Writing applications that use EIM APIs | Knowledge of: <ul style="list-style-type: none"> • Platform • Programming skills • Compiling programs |

Related concepts

“EIM access control” on page 36

An Enterprise Identity Mapping (EIM) user is a user who possesses EIM access control based on their membership in a predefined Lightweight Directory Access Protocol (LDAP) user group for a specific domain.

Planning an Enterprise Identity Mapping domain

Part of the initial Enterprise Identity Mapping (EIM) implementation planning process requires that you define an EIM domain. To gain the maximum benefit from having a centralized repository of mapping information, you need to plan for the domain to be shared between many applications and systems.

As you work through the EIM planning topic, you will gather the information that you need to define the domain and to record it on the planning work sheets. The example sections from the work sheets may help guide you to gather and record this information at each planning stage in this topic.

The following table lists the information you need to gather when planning your domain and suggests the EIM implementation team role or roles that could be responsible for each information item needed.

Note: Although the table lists a particular role as a suggestion for assigning the responsibility of gathering the described information, you should assign roles based on the needs and security policy for your organization. For example, in a smaller organization you may prefer to designate a single person as the EIM administrator to be responsible for all aspects of planning, configuration, and managing EIM.

Table 11. Information needed for EIM domain planning

| Information needed | Role |
|---|---|
| 1. Whether there is an existing domain to use that suits your needs, or if you should create one. | EIM administrator |
| 2. Which directory server will act as the EIM domain controller. (Review “Planning an Enterprise Identity Mapping domain controller” on page 54 for detailed information about choosing a domain controller.) | Directory server (LDAP) administrator or EIM administrator |
| 3. A name for the domain. (You can also provide an optional description.) | EIM administrator |
| 4. Where in the directory to store EIM domain data. Note: Depending on your choice of system for hosting the directory server and your choice of a directory for storing EIM domain data, you may need to perform some directory services configuration tasks before the domain can be created. | Both the directory server (LDAP) administrator or EIM administrator |

Table 11. Information needed for EIM domain planning (continued)

| Information needed | Role |
|--|----------|
| 5. The applications and operating systems that will participate in the domain. If you are configuring your first domain, this initial set may consist of as few as one system. (Review “Developing an Enterprise Identity Mapping registry definition naming plan” on page 57 for more information.) | EIM team |
| 6. The people and entities that will participate in the domain. Note: To make initial testing easier, you may want to limit the number of participants to one or two. | EIM team |

Planning an Enterprise Identity Mapping domain controller

As you gather information to define your Enterprise Identity Mapping (EIM) domain, you need to determine which directory server product will act as the EIM domain controller.

EIM requires that the domain controller be hosted by a directory server that supports Lightweight Directory Access Protocol (LDAP) Version 3. Additionally, the directory server product must be able to accept the LDAP schema and other considerations for EIM and understand certain attributes and object classes.

If your enterprise possesses more than one directory server that can host an EIM domain controller, you should also consider whether to use secondary replicated domain controllers. For example, if you expect to have a large number of EIM mapping lookup operations occurring, replicas can improve the performance of the lookup operations.

Also, you should consider whether to make your domain controller *local* or *remote* in relationship to the system you expect to be running the largest number of mapping lookup operations. By having the domain controller be local to the high-volume system, you may improve the performance of the lookup operations for the local system. Use the planning work sheets to record these planning decisions, as well as those you make about your domain and other directory information.

After you determine which directory server in your enterprise will host your EIM domain controller, you need to make some decisions about domain controller access.

Plan domain controller access

You need to plan how you and EIM-enable applications and operating systems will access the directory server that hosts the EIM domain controller. To access an EIM domain you must:

1. Be able to bind to the EIM domain controller
2. Make sure that the bind subject is a member of an EIM access control group, or is the LDAP administrator. Refer to Manage EIM access control for more information.

Select type of EIM binding

EIM APIs support several different mechanisms for establishing a connection, also known as binding, with the EIM domain controller. Each type of binding mechanism provides a different level of authentication and encryption for the connection. The possible choices are:

Simple Binds

A simple bind is an LDAP connection where an LDAP client provides a bind distinguished name and a bind password to the LDAP server for authentication. The bind distinguished name and password are defined by the LDAP administrator in the LDAP directory. This is the weakest form of authentication and the least secure as the bind distinguished name and password are sent

unencrypted and are vulnerable to eavesdropping. You use CRAM-MD5 (challenge-response authentication mechanism) to add an additional level of protection for the bind password. With the CRAM-MD5 protocol, the client sends a hashed value instead of the clear text password to the server for authentication.

Server authentication with Secure Sockets Layer (SSL) - server side authentication

An LDAP server can be configured for SSL or Transport Layer Security (TLS) connections. The LDAP server uses a digital certificate to authenticate itself to the LDAP client and establishes an encrypted communications session between them. Only the LDAP server is authenticated by means of a certificate. The end user is authenticated by means of a bind distinguished name and password. The strength of the authentication is the same as for a simple bind, but all data (including the bind distinguished name and password) is encrypted for privacy.

Client authentication with SSL

An LDAP server can be configured to require that the end user be authenticated by means of a digital certificate rather than a bind distinguished name and password for SSL or TLS secure connections to the LDAP server. Both client and server are authenticated and the session is encrypted. This option provides a stronger level of user authentication and protects the privacy of all data transmitted.

Kerberos authentication

An LDAP client can be authenticated to the server by using a Kerberos ticket as an optional replacement for a bind distinguished name and password. (Kerberos), which is a trusted third-party network authentication system, allows a principal (a user or service) to prove its identity to another service within an unsecured network. Authentication of principals is completed through a centralized server called a key distribution center (KDC). The KDC authenticates a user with a Kerberos ticket. These tickets prove the principal's identity to other services in a network. After a principal is authenticated by these tickets, the principal and service can exchange encrypted data with a target service. This option provides a stronger level of user authentication and protects the privacy of authentication information.

The choice of a bind mechanism is based on the level of security required by the EIM-enabled application and the authentication mechanisms supported by the LDAP server that hosts the EIM domain.

Also, you might have to perform additional configuration tasks for the LDAP server to enable the authentication mechanism that you choose to use. Check the documentation for the LDAP server that hosts your domain controller to determine what other configuration tasks you may need to perform.

Example planning work sheet: domain controller information

After making your decisions about your EIM domain controller, use the planning worksheets to record the EIM domain controller information that your EIM-enabled operating systems and applications need. The information that you gather as part of this process can be used by the LDAP administrator to define the bind identity of the application or operating system to the LDAP directory server that hosts the EIM domain controller.

The following sample portion of the planning work sheets shows the type of information that you need to gather. It also includes sample values that you could use when you configure the EIM domain controller.

Table 12. Domain and domain controller information for EIM planning worksheet

| Information needed to configure EIM domain and domain controller | Example answers |
|--|-----------------|
| A meaningful name for the domain. This could be the name of a company, a department, or an application that uses the domain. | MyDomain |

Table 12. Domain and domain controller information for EIM planning worksheet (continued)

| Information needed to configure EIM domain and domain controller | Example answers |
|---|--|
| Optional: If configuring an EIM domain in an already existing LDAP directory, specify a parent distinguished name for the domain. This is the distinguished name that represents the entry immediately above your domain name entry in the directory information tree hierarchy, for example, o=ibm,c=us. | o=ibm,c=us |
| Resulting fully qualified EIM domain distinguished name. This is the fully defined name of the EIM domain that describes the directory location for EIM domain data. The fully qualified domain distinguished name consists of, at a minimum, the DN for the domain (ibm-eimDomainName=), plus the domain name that you specified. If you choose to specify a parent DN for the domain, then the fully qualified domain DN consists of the relative domain DN (ibm-eimDomainName=), the domain name (MyDomain), and the parent DN (o=ibm,c=us). Note: | Either of these, depending on whether you choose a parent DN: <ul style="list-style-type: none"> ibm-eimDomainName=MyDomain ibm-eimDomainName=MyDomain,o=ibm,c=us |
| Connection address for the domain controller. This consists of the type of connection (basic ldap or secure ldap, for example, ldap:// or ldaps://) plus the following information: | ldap:// |
| <ul style="list-style-type: none"> Optional: The host name or IP address Optional: The port number | <ul style="list-style-type: none"> some.ldap.host 389 |
| Resulting complete connection address for the domain controller. | ldap://some.ldap.host:389 |
| Bind mechanism required by applications or systems. Choices include: <ul style="list-style-type: none"> Simple bind CRAM MD5 Server authentication Client authentication Kerberos | Kerberos |

If your EIM configuration and administration team consists of multiple team members, you will need to determine the bind identity and mechanism that each team member should use for accessing the EIM domain based on their role. Also, you need to determine the bind identity and mechanism for EIM application end users. You may find the following work sheet helpful as an example for gathering this information.

Table 13. Example bind identities planning work sheet

| EIM authority or role | Bind identity | Bind mechanism | Reason needed |
|------------------------------|------------------------|----------------|---|
| EIM administrator | eimadmin@krbrealm1.com | kerberos | configure and manage EIM |
| LDAP administrator | cn=administrator | simple bind | configure EIM domain controller |
| EIM registry X administrator | cn=admin2 | CRAM MD5 | manage specific registry definition |
| EIM mapping lookup | cn=MyApp,c=US | simple bind | perform application mapping lookup operations |

Developing an Enterprise Identity Mapping registry definition naming plan

To use Enterprise Identity Mapping (EIM) to map the user identity in one user registry to an equivalent user identity in another user registry, both user registries must be defined to EIM.

You must create an EIM registry definition for each application or operating system user registry that will participate in the EIM domain. User registries can represent operating system registries such as Resource Access Control Facility (RACF) or i5/OS, a distributed registry such as Kerberos, or a subset of a system registry that is used exclusively by an application.

An EIM domain can contain registry definitions for user registries that exist on any platform. For example, a domain managed by a domain controller on i5/OS might contain registry definitions for non-i5/OS platforms (such as an AIX registry). Although you can define any user registry to an EIM domain, you must define user registries for those applications and operating systems that are EIM-enabled.

You can name an EIM registry definition anything that you like as long as the name is unique in the EIM domain. For example, you could name the EIM registry definition based on the name of the system that hosts the user registry. If this is not sufficient to distinguish the registry definition from similar definitions, you could use a period (.) or an underscore (_) to add the type of user registry that you are defining. Regardless of the criteria you choose to use, you should consider developing a naming convention for your EIM registry definitions. Doing so ensures that the definition names are consistent throughout the domain and are adequately descriptive of the type and instance of the user registry defined and how it is used. For example, you could choose the name of each registry definition by using a combination of the application or operating system name that uses the registry and the user registry's physical location in your enterprise.

An application that is written to use EIM may specify either a source registry alias or a target registry alias, or aliases for both. When you create EIM registry definitions you need to check the documentation for your applications to determine whether you need to specify one or more aliases for registry definitions. When you assign these aliases to the appropriate registry definitions, the application can perform an alias lookup to find the EIM registry definition or definitions that match the aliases in the application.

You may find the following sample portion of the planning work sheet helpful as a guide to use for recording information about participating user registries. You can use the actual work sheet to specify a registry definition name for each user registry, to specify whether it uses an alias, and to describe the user registry location and use. The installation and configuration documentation for the application will provide some of the information that you need for the worksheet.

Table 14. Sample EIM registry definition information planning work sheet

| Registry definition name | User registry type | Registry definition alias | Registry description |
|--------------------------|----------------------------|--|---|
| System_C | i5/OS system user registry | Review application documentation | Main system user registry for i5/OS on System C |
| System_A_WAS | WebSphere LTPA | app_23_alias_source | WebSphere LTPA user registry on System A |
| System_B | Linux | Review application documentation | Linux user registry on System B |
| System_A | i5/OS system user registry | app_23_alias_target app_xx_alias_target | Main system user registry for i5/OS on System A |
| System_D | Kerberos user registry | app_xx_alias_source | legal.mydomain.com Kerberos realm |

Table 14. Sample EIM registry definition information planning work sheet (continued)

| Registry definition name | User registry type | Registry definition alias | Registry description |
|--------------------------|----------------------------|----------------------------------|---|
| System_4 | Windows 2000 user registry | Review application documentation | Human resources application user registry on System 4 |

Note: Association types for each registry will be determined later in the planning process.

After you complete this section of the planning worksheet, you should develop your identity mapping plan to determine whether to use identifier associations, policy associations, or both types of associations to create the mappings that you need for the user identities in each defined user registry.

Developing an identity mapping plan

A critical part of the initial Enterprise Identity Mapping (EIM) implementation planning process requires that you determine how you want to use identity mapping in your enterprise.

There are two methods that you can use to map identities in EIM:

- **Identifier associations** describe relationships between an EIM identifier and the user identities in user registries that represent that person. An identifier association creates a direct one-to-one mapping between an EIM identifier and a specific user identity. You can use identifier associations to indirectly define a relationship between user identities through the EIM identifier.

If your security policy requires a high degree of detailed accountability, you may need to use identifier associations almost exclusively for your identity mapping implementation. Because you use identity associations to create one-to-one mappings for the user identities that users own, you can always determine exactly who performed an action on an object or on the system.

- **Policy associations** describe a relationship between multiple user identities and a single user identity in a user registry. Policy associations use EIM mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier.

Policy associations can be useful when you have one or more large groups of users who need access to systems or applications in your enterprise where you do not want them to have specific user identities for gaining this access. For example, you maintain a Web application that access a specific internal application. You may not want to set up hundreds or thousands of user identities to authenticate users to this internal application. In this situation, you may want to configure identity mapping such that all the users of this Web application are mapped to a single user identity with the minimum level of authorization required to run the application. You can do this type of identity mapping by using policy associations.

You may decide to use identifier associations to provide the best control of the user identities in your enterprise while gaining the largest degree of streamlined password management. Or, you may decide to use a mixture of policy associations and identifier associations to streamline single sign-on, where appropriate, while you maintain specific control over user identities for administrators. Regardless of what type of identity mapping you decide best meets your business needs and properly fits your security policy, you need to create an identity mapping plan to ensure that you implement identity mapping appropriately.

To create an identity mapping plan, you need to do the following:

Related concepts

“Creating EIM associations” on page 99

There are two different types of EIM associations you can create. You can create either an identifier association or a policy association.

“Creating a policy association” on page 100

A policy association provides a means to directly define a relationship between multiple user identities in one or more registries and an individual target user identity in another registry.

Planning Enterprise Identity Mapping associations:

Associations are entries that you create in an Enterprise Identity Mapping (EIM) domain to define a relationship between user identities in different user registries.

You can create one of two types of associations in EIM: identifier associations to define one-to-one mappings and policy associations to define many-to-one mappings. You can use policy associations instead of, or in conjunction with, identifier associations.

The specific types of associations that you choose to create depends on how a user uses a particular user identity, as well as your overall identity mapping plan.

You can create any of the following types of identifier associations:

- **Target associations**

You define target associations for users that normally only access this system as a server from some other client system. This type of association is used when an application performs mapping lookup operations.

- **Source associations**

You define source associations when the user identity is the first one that a user provides to sign on to the system or network. This type of association is used when an application performs mapping lookup operations.

- **Administrative associations**

You define administrative associations when you want to be able to track the fact that the user identity belongs to a specific user, but do not want the user identity to be available to mapping lookup operations. You can use this type of association to track all the user identities that a person uses in the enterprise.

A **policy association** always defines a target association.

It is possible for a single registry definition to have more than one type of association depending on how the user registry that it refers to is used. Although there are no limits to the numbers of, or the combinations of, associations that you can define, keep the number to a minimum to simplify the administration of your EIM domain.

Typically, an application will provide guidance on which registry definitions it expects for source and target registries, but not the association types. Each end user of the application needs to be mapped to the application by at least one association. This association can be a one-to-one mapping between their unique EIM identifier and a user identity in the required target registry or a many-to-one mapping between a source registry of which the user identity is a member and the required target registry. Which type of association you use depends on your identity mapping requirements and the criteria the application provides.

Previously as part of the planning process, you completed two planning work sheets for the user identities in your organization with information about the EIM identifiers and EIM registry definitions that you need. Now you need to bring this information together by specifying the types of associations you want to use to map the users identities in your enterprise. You need to determine whether to define a policy association for a particular application and its registry of users, or to define specific identifier associations (source, target, or administrative) for each user identity in the system or application registry. You can do this by recording information about the required association types in both the registry definition planning work sheet and in the corresponding rows of each associations work sheet.

To complete your identity mapping plan, you can use the following example work sheets as a guide to help you record the association information that you need to describe a complete picture of how you plan to implement identity mapping.

Table 15. Example EIM registry definition information planning work sheet

| Registry definition name | User registry type | Registry definition alias | Registry description | Association types |
|--------------------------|------------------------------|--|---|---|
| System_C | i5/OS system user registry | Review application documentation | Main system user registry for i5/OS on System C | Target |
| System_A_WAS | WebSphere LTPA | app_23_alias_source | WebSphere LTPA user registry on System A | Primarily source |
| System_B | Linux | Review application documentation | Linux user registry on System B | Source and target |
| System_A | i5/OS system user registry | app_23_alias_target app_xx_alias_target | Main system user registry for i5/OS on System A | Target |
| System_D | Kerberos user registry | app_xx_alias_source | legal.mydomain.com Kerberos realm | Source |
| System_4 | Windows 2000 user registry | Review application documentation | Human resources application user registry on System 4 | Administrative |
| order.mydomain.com | Windows 2000 user registry | | Main logon registry for order department employees | Default registry policy (source registry) |
| System_A_order_app | Order department application | | Application specific registry for order updates | Default registry policy (target registry) |
| System_C_order_app | Order department application | | Application specific registry for order updates | Default registry policy (target registry) |

Table 16. Example EIM identifier planning work sheet

| Unique identifier name | Identifier or user identity description | Identifier alias |
|------------------------|---|------------------|
| John S Day | Human resources manager | app_23_admin |
| John J Day | Legal Department | app_xx_admin |
| Sharon A. Jones | Order Department Administrator | |

Table 17. Example identifier association planning work sheet

| Identifier unique name: ____John S Day____ | | |
|---|---------------|-------------------|
| User registry | User identity | Association types |
| System A WAS on System A | johnday | Source |
| Linux on System B | jsd1 | Source and target |
| i5/OS on System C | JOHND | Target |
| Registry 4 on Windows 2000 human resources system | JDAY | Administrative |

Table 18. Example planning work sheet for policy associations

| Policy association type | Source user registry | Target user registry | User identity | Description |
|-------------------------|----------------------|----------------------|---------------|---|
| Default registry | order.mydomain.com | System_A_order_app | SYSUSERA | Maps authenticated Windows order department user to appropriate application user identity |
| Default registry | order.mydomain.com | System_C_order_app | SYSUSERB | Maps authenticated Windows order department user to appropriate application user identity |

Developing an EIM identifier naming plan:

When planning your Enterprise Identity Mapping (EIM) identity mapping needs, you can create unique EIM identifiers for users of EIM-enabled applications and operating systems in your enterprise when you want to create one-to-one mappings between user identities for a user. By using identifier associations to create one-to-one mappings you can maximize the password management benefits that EIM provides.

The naming plan that you develop depends on your business needs and preferences; the only requirement for EIM identifier names is that they be unique. Some companies may prefer to use each person's full, legal name; other companies may prefer to use a different type of data, such as each person's employee number. If you want to create EIM identifier names based on each person's full name, you may anticipate possible name duplication. How you handle potential duplicate identifier names is a matter of personal preference. You may want to handle each case manually by adding a predetermined character string to each identifier name to ensure uniqueness; for example, you might decide to add each person's department number.

As part of developing an EIM identifier naming plan, you need to decide on your overall identity mapping plan. Doing so can help you to decide when you need to be using identifiers and identifier associations versus using policy associations for mapping identities within your enterprise. To develop your EIM identifier naming plan, you can use the work sheet below to help you gather information about the user identities in your organization and to plan EIM identifiers for the user identities. The work sheet represents the kind of information the EIM administrator needs to know when he creates EIM identifiers or policy associations for the users of an application.

Table 19. Example EIM identifier planning work sheet

| Unique identifier name | Identifier or user identity description | Identifier alias |
|------------------------|---|------------------|
| John S Day | Human resources manager | app_23_admin |
| John J Day | Legal Department | app_xx_admin |
| Sharon A. Jones | Order Department Administrator | |

An application that is written to use EIM may specify an alias that it uses to find the appropriate EIM identifier for the application, which the application may use in turn to determine a specific user identity to use. You need to check the documentation for your applications to determine whether you need to specify one or more aliases for the identifier. The EIM identifier or user identity description fields are free form and can be used to provide descriptive information about the user.

You do not need to create EIM identifiers for all members of your enterprise at one time. After creating an initial EIM identifier and using it to test your EIM configuration, you can create additional EIM identifiers based on your organization's goals for using EIM. For example, you can add EIM identifiers on a departmental or area basis. Or, you can add EIM identifiers as you deploy additional EIM applications.

After you gather the information that you need to develop an EIM identifier naming plan, you can plan associations for your user identities.

Enterprise Identity Mapping implementation planning worksheets

As you work through the Enterprise Identity Mapping (EIM) planning process, you might find it helpful to use these worksheets to gather information that you will need to configure and use EIM in your enterprise. Examples of completed sections of the worksheets are provided in the planning pages as appropriate.

These work sheets are provided as an example of the types of work sheets that you need for creating your EIM implementation plan. The number of entries provided are fewer than the number that you will probably need for your EIM information. You can edit these work sheets to make them more useful for your situation.

Table 20. Domain and domain controller information work sheet

| Information needed to configure EIM domain and domain controller | Answers |
|---|---------|
| A meaningful name for the domain. This might be the name of a company, a department, or an application that uses the domain. | |
| Optional: A parent distinguished name for the domain. This is the distinguished name that represents the entry immediately above your domain name entry in the directory information tree hierarchy, for example, o=ibm,c=us. | |
| Resulting fully qualified EIM domain distinguished name. This is the fully defined name of the EIM domain that describes the directory location for EIM domain data. The fully qualified domain distinguished name consists of, at a minimum, the DN for the domain (ibm-eimDomainName=), plus the domain name that you specified. If you choose to specify a parent DN for the domain, then the fully qualified domain DN consists of the relative domain DN (ibm-eimDomainName=), the domain name (MyDomain), and the parent DN (o=ibm,c=us). | |
| Connection address for the domain controller. This consists of the type of connection (basic ldap or secure ldap, for example, ldap:// or ldaps://) plus the following information: | |
| <ul style="list-style-type: none"> Optional: The host name or IP address Optional: The port number | |
| Resulting complete connection address for the domain controller. | |

Table 20. Domain and domain controller information work sheet (continued)

| | |
|---|--|
| Bind mechanism required by applications or systems. Choices include: <ul style="list-style-type: none"> • Simple bind • CRAM MD5 • Server authentication • Client authentication • Kerberos | |
|---|--|

Review Plan an EIM domain controller for an example of how to use this work sheet.

Table 21. Bind identities planning work sheet

| EIM authority or role | Bind identity | Bind mechanism | Reason needed |
|-----------------------|---------------|----------------|---------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Review Plan an EIM domain controller for an example of how to use this work sheet.

Table 22. EIM registry definition information planning work sheet

| Registry definition name | User registry type | Registry definition alias | Registry description | Association types |
|--------------------------|--------------------|---------------------------|----------------------|-------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Review Develop an EIM registry definition naming plan for an example of how to use this work sheet.

Table 23. EIM identifier planning work sheet

| Unique identifier name | Identifier or user identity description | Identifier alias |
|------------------------|---|------------------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Review Develop an EIM identifier naming plan for an example of how to use this work sheet.

Table 24. Identifier association planning work sheet

| Identifier unique name: ____John S Day____ | | |
|--|---------------|-------------------|
| User registry | User identity | Association types |
| | | |
| | | |
| | | |
| | | |

Review Plan EIM associations for an example of how to use this work sheet.

Table 25. Policy association planning work sheet

| Policy association type | Source user registry | Target user registry | User identity | Description |
|-------------------------|----------------------|----------------------|---------------|-------------|
| | | | | |
| | | | | |

Review Plan EIM associations for an example of how to use this work sheet.

Planning for Enterprise Identity mapping application development

For an application to use Enterprise Identity Mapping (EIM) and participate in a domain, that application must be able to use the EIM APIs.

You should review the EIM API documentation and platform specific EIM documentation to determine if there are any special planning considerations you should understand when you write or adapt

applications to use the EIM APIs. For example, there may be compile and other considerations for C or C++ applications that make calls to the EIM APIs. Depending on the application's platform, there may be link-edit or other considerations as well.

Related tasks

"Enterprise Identity Mapping APIs" on page 120

Enterprise Identity Mapping (EIM) provides the mechanics for cross-platform user identity management. EIM has multiple application programming interfaces (APIs) that applications can use to conduct EIM operations on behalf of the application or an application user.

Planning Enterprise Identity Mapping for i5/OS

There are multiple technologies and services that Enterprise Identity Mapping (EIM) encompasses on the System i platform. Prior to configuring EIM on your server, you should decide what functionality you want to implement by using EIM and single sign-on capabilities.

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

If you plan on using Kerberos to authenticate users as part of a single signon implementation, you should also configure network authentication service.

To learn more about how to plan your systems EIM configuration, review the following information:

Related information

Planning network authentication service

EIM installation prerequisites for i5/OS

The planning work sheet identifies the services that you should install prior to configuring EIM.

Table 26. EIM installation planning work sheet


| EIM prerequisite planning work sheet | Answers |
|---|---------|
| Is your system running i5/OS V5R4, or later? | |
| Are the following options and licensed products installed on your system? <ul style="list-style-type: none"> i5/OS Host Servers (5761-SS1 Option 12) System i Access for Windows (5761-XE1) Qshell Interpreter (5761-SS1 Option 30) Necessary if you intend to configure network authentication service as well as EIM. Note: 5722 is the product code for i5/OS options and products, prior to V6R1. | |
| Is System i Navigator installed on the administrator PC, including the following subcomponents? <ul style="list-style-type: none"> Network Security (necessary if you intend to configure network authentication service as well as EIM) | |
| Have you installed the latest System i Access for Windows service pack? For the latest service pack see System i Access  | |
| If a directory server, for example, the IBM Tivoli Directory Server for i5/OS is currently configured and you want to use it as the EIM domain controller, do you know the LDAP administrator distinguished name (DN) and password? | |
| If a directoryserver is currently configured, can it be stopped temporarily? (This will be required to complete the EIM configuration process.) | |
| Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities? | |

Table 26. EIM installation planning work sheet (continued)

| | |
|---|--|
| Have you applied the latest program temporary fixes (PTFs)? | |
|---|--|

Installing required System i Navigator options

To enable a single sign-on environment with Enterprise Identity Mapping (EIM) and network authentication service, you must install both the **Network** option and the **Security** option of System i Navigator.

EIM is located within the **Network** option and network authentication service is within the **Security** option. If you do not plan to use network authentication service in your network, you do not need to install the **Security** option of System i Navigator.

To install the Network option of System i Navigator or to verify that you have this option currently installed, ensure that System i Access for Windows is installed on the PC that you are using to administer the System i model.

To install the **Network** option:

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

Related information

Network authentication service

Backup and recovery considerations for EIM

You need to develop a backup and recovery plan for your Enterprise Identity Mapping (EIM) data to ensure that your EIM data is protected and can be recovered should there ever be a problem with the directory server that hosts the EIM domain controller. There is also important EIM configuration information that you need to understand how to recover.

Related information

Directory Server Replication

Replication tasks

Directory Server save and restore considerations

Backup and recovery of EIM domain data:

How you save your EIM data depends on how you decide to manage this aspect of the directory server that acts as the domain controller for your EIM data.

One way to back up the data, especially for disaster recovery purposes is to save the database library. By default, this is QUSRDIRDB. If changelog is enabled, then you should also save the library QUSRDIRCL. The directory server on the system where you want to restore the library must have the same LDAP schema and configuration as the original directory server. The files that store this information are in /QIBM/UserData/OS400/DirSrv. Additional configuration data is stored in QUSRSYS/QGLDCFG (*USRSPC object) and QUSRSYS/QGLDVLDL (*VLDL object). In order to have a complete backup of everything for your directory server, you must save both libraries, the integrated file system files, and the QUSRSYS objects.

For example, you could use an LDIF file to save all or part of the directory server contents. To back up the domain information for a IBM Tivoli Directory Server for i5/OS domain controller complete these steps:

1. In System i Navigator, expand **Network > Servers > TCP/IP**.

2. Right-click the **Directory Server**, select **Tools**, then select **Export file** to display a page that allows you to specify what parts of the directory server contents to export to a file.
3. Transfer the export file to the System i platform that you want to use as your backup directory server.
4. In System i Navigator on the backup server, expand **Network > Servers > TCP/IP**.
5. Right-click the **Directory Server**, select **Tools**, then select **Import** to load the contents of the transferred file to the new directory server.

Another method you may consider for saving your EIM domain data, is to configure and use a replica directory server. All changes to EIM domain data are automatically forwarded to the replica directory server so that if the directory server that hosts the domain controller fails or loses EIM data, you can retrieve the data from the replica server.

How you configure and use a replica directory server varies depending on the type of replication model that you choose to use.

Backup and recovery of EIM configuration information:

Should your system go down, you may need to restore EIM configuration information for that system. This information cannot be saved and restored easily across systems.

These options are available to you to save and restore EIM configuration:

- Use the Save Security Data (SAVSECDTA) command on each system to save EIM and other important configuration information. Then restore the QSYS user profile object on each system.

Note: You must use the SAVSECDTA command and restore the QSYS user profile object on each system with an EIM configuration individually. You may experience problems if you try to recover the QSYS user profile object on one system when it was saved on a different system.

- Either rerun the EIM Configuration wizard or you manually update the EIM Configuration folder properties. To make this process easier, you should save your EIM implementation planning work sheets or make a record of the EIM configuration information for each system.

Additionally, you need to consider and plan how to back up and recover you network authentication service data if you configured network authentication service as part of implementing a single sign-on environment.

Configuring Enterprise Identity Mapping

The EIM Configuration wizard allows you to complete a basic EIM configuration for your system quickly and easily. The wizard provides you with three EIM system configuration options.

How you use the wizard to configure EIM on a specific system depends on your overall plan for using EIM in your enterprise and your EIM configuration needs. For example, many administrators want to use EIM in conjunction with network authentication service to create a single sign-on environment across multiple systems and platforms without a need to change underlying security policies. Consequently, the EIM Configuration wizard allows you to configure network authentication service as part of your EIM configuration. However, configuring and using network authentication service is not a prerequisite or requirement for configuring and using EIM.

Before you begin the process of configuring EIM for one or more systems, plan your EIM implementation to gather the information you need. For example, you need to make decisions about the following:

- Which System i platform do you want to configure as the EIM domain controller for the EIM domain? Use the EIM Configuration wizard to create a new domain on this system first, then use the wizard to configure all additional systems to join this domain.

- Do you want to configure network authentication service on each system that you configure for EIM? If so, you can use the EIM Configuration wizard to create a basic network authentication service configuration on each System i model. However, you must perform other tasks to complete your network authentication service configuration.

After you use the EIM Configuration wizard to create a basic configuration for each System i platform, there are still a number of EIM configuration tasks that you must perform before you have a complete EIM configuration. Review Scenario: Enable single sign-on for an example that shows how a fictitious company configured a single sign-on environment using network authentication service and EIM.

To configure EIM, you must have all of the following special authorities:

- Security administrator (*SECADM).
- All object (*ALLOBJ).
- System configuration (*IOSYSCFG).

Before you use the EIM Configuration wizard, you should have completed all “Planning for Enterprise Identity Mapping” on page 49 steps to determine exactly how you will use EIM. If you are configuring EIM as part of creating a single signon environment, then you should complete all single sign-on planning steps as well.

To access the EIM Configuration wizard, follow these steps:

1. Start System i Navigator.
2. Sign on to the system you want to configure for EIM. If you are configuring EIM for more than one system, 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 an EIM configuration option and follow the instructions that the wizard provides to complete the wizard.
6. Click **Help**, if necessary, to determine what information to specify as you proceed through the wizard.

Once your planning is complete, you can use the EIM Configuration wizard to create one of three basic EIM configurations. You can use the wizard to join an existing domain or to create and join a new domain. When you use the EIM Configuration wizard to create and join a new domain, you can choose whether to configure an EIM domain controller on a local or a remote system. The following information provides instructions for configuring EIM based on which type of basic EIM configuration you need:

Related information

Network authentication service

Single sign-on

Creating and joining a new local domain

When you use the EIM Configuration wizard to create and join a new domain, you can choose to configure the EIM domain controller on the local system as part of creating your EIM configuration.

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 System i platform, the wizard prompts you to launch the Network Authentication Service Configuration wizard.

When you complete the EIM Configuration wizard, you can accomplish these tasks:

- Create a new EIM domain.
- Configure the local directory server to act as the EIM domain controller.
- Configure network authentication service for the system.

- Create EIM registry definitions for the local i5/OS registry and the Kerberos registry.
- Configure the system to participate in the new EIM domain.

To configure your system to create and join a new EIM domain, you must have all the following special authorities:

- Security administrator (*SECADM).
- All object (*ALLOBJ).
- System configuration (*IOSYSCFG).

To use the EIM Configuration wizard to create and join a new local domain, complete these steps:

1. In System i Navigator, select the system for which you want to configure EIM and expand **Network > Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Configure** to start the EIM Configuration wizard.

Note: This option is labeled **Reconfigure** if EIM has been previously configured on the system.

3. On the **Welcome** page of the wizard, select **Create and join a new domain**, and click **Next**.
4. On the **Specify EIM Domain Location** page, select **On the local Directory server** and click **Next**.

Note: This option configures the local directory server to act as the EIM domain controller. Because this directory server stores all EIM data for the domain, it must be active and remain active to support EIM mapping lookups and other operations.

If network authentication service is not currently configured on the System i platform, or additional network authentication configuration information is needed to configure a single sign-on environment, the **Network Authentication Services Configuration** page displays. This page allows you start the Network Authentication Service Configuration wizard so that you can configure network authentication service. Or, you can configure Network Authentication Service at a later time by using the configuration wizard for this service through System i Navigator. When you complete network authentication service configuration, the EIM Configuration wizard continues.

5. To configure network authentication service, complete these steps:
 - a. On the **Configure Network Authentication Service** page, select **Yes** to start the Network Authentication Service Configuration wizard. With this wizard, you can configure several i5/OS interfaces and services to participate in a Kerberos realm as well as configure a single signon environment that uses both EIM and network authentication service.
 - b. On the **Specify Realm Information** page, specify the name of the default realm in the **Default realm** field. If you are using Microsoft Active Directory for Kerberos authentication, select **Microsoft Active Directory is used for Kerberos authentication**, and click **Next**.
 - c. On the **Specify KDC Information** page, specify the fully qualified name of the Kerberos server for this realm in the **KDC** field, specify 88 in the **Port** field, and click **Next**.
 - d. On the **Specify Password Server Information** page, select either **Yes** or **No** for setting up a password server. The password server allows principals to change passwords on the Kerberos server. If you select **Yes**, enter the password server name in the **Password server** field. In the **Port** field, accept the default value of 464, and click **Next**.
 - e. On the **Select Keytab Entries** page, select **i5/OS Kerberos Authentication**, and click **Next**.

Note: In addition you can also create keytab entries for the IBM Tivoli Directory Server for i5/OS, i5/OS NetServer, and IBM HTTP Server for i5/OS if you want these services to use Kerberos authentication. You may need to perform additional configuration for these services before they can use Kerberos authentication.

- f. On the **Create i5/OS Keytab Entry** page, enter and confirm a password, and click **Next**. This is the same password you will use when you add the i5/OS principals to the Kerberos server.
- g. Optional: On the **Create Batch File** page, select **Yes**, specify the following information, and click **Next**:

- In the **Batch file** field, update the directory path. Click **Browse** to locate the appropriate directory path, or edit the path in the **Batch file** field.
- In the **Include password** field, select **Yes**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is essential that you delete the batch file from the Kerberos server and from the PC immediately after you use it. If you do not include the password, you will be prompted for the password when you run the batch file.

Note: You can also manually add the service principals that are generated by the wizard to Microsoft Active Directory. To learn how to do this, review *Add i5/OS principals to the Kerberos server*

- On the **Summary** page, review the network authentication service configuration details, and click **Finish** to return to the EIM Configuration wizard.
6. If the local directory server is not currently configured, the **Configure Directory Server** page displays when the EIM Configuration wizard resumes. Provide the following information to configure the local directory server:

Note: If you configure the local directory server before you use the EIM Configuration wizard, the **Specify User for Connection** page displays instead. Use this page to specify the distinguished name and password for the LDAP administrator to ensure that the wizard has enough authority to administer the EIM domain and the objects in it and continue with the next step in this procedure. Click **Help**, if necessary, to determine what information to provide for this page.

- In the **Port** field, accept the default port number 389, or specify a different port number to use for nonsecure EIM communications with the directory server.
 - In the **Distinguished name** field, specify the LDAP distinguished name (DN) that identifies the LDAP administrator for the directory server. The EIM Configuration wizard creates this LDAP administrator DN and uses it to configure the directory server as the domain controller for the new domain that you are creating.
 - In the **Password** field, specify the password for the LDAP administrator.
 - In the **Confirm password** field, specify the password a second time for validation purposes.
 - Click **Next**.
7. On the **Specify Domain** page, 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**.
8. On the **Specify Parent DN for Domain** page, select **Yes** to specify a parent DN for the domain that you are creating, or specify **No** to have EIM data stored in a directory location with a suffix whose name is derived from the EIM domain name.

Note: When you create a domain on a local directory server, a parent DN is optional. By specifying a parent DN, you can specify where in the local LDAP namespace EIM data should reside for the domain. When you do not specify a parent DN, EIM data resides in its own suffix in the namespace. If you select **Yes**, use the list box to select the local LDAP suffix to use as the parent DN, or enter text to create and name a new parent DN. It is not necessary to specify a parent DN for the new domain. Click **Help** for further information about using a parent DN.

9. On the **Registry Information** page, specify whether to add the local user registries to the EIM domain as registry definitions. Select one or both of these user registry types:

Note: You do not have to create the registry definitions at this time. If you choose to create the registry definitions later, you need to add the system registry definitions and update the EIM configuration properties.

- a. Select **Local i5/OS** to add a registry definition for the local registry. In the field provide, accept the default value for the registry definition name or specify a different value for the registry definition name. The EIM registry name is an arbitrary string that represents the registry type and specific instance of that registry.
 - b. Select **Kerberos** to add a registry definition for a Kerberos registry. In the field provided, accept the default value for the registry definition name or specify a different value for the registry definition name. The default registry definition name is the same as the realm name. By accepting the default name and using the same Kerberos registry name as the realm name, you can increase performance in retrieving information from the registry. Select **Kerberos user identities are case sensitive**, if necessary.
 - c. Click **Next**.
10. On the **Specify EIM System User** page, select a **User type** that you want the system to use when performing EIM operations on behalf of operating system functions. These operations include mapping lookup operations and deletion of associations when deleting a local i5/OS 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**. Which user types you can select vary based on the current system configuration. For example, if Network Authentication Service is not configured for the system, then Kerberos user types may not be available for selection. The user type that you select determines the other information that you must provide to complete the page as follows:

Note: You must specify a user that is currently defined in the directory server which is hosting the EIM domain controller. The user that you specify must have privileges to perform mapping lookup and registry administration for the local user registry at a minimum. If the user that you specify does not have these privileges, then certain operating system functions related to the use of single sign-on and the deletion of user profiles may fail.

If you have not configured the directory server prior to running this wizard, the only user type you can select is **Distinguished name and password** and the only distinguished name you can specify is the LDAP administrator's DN.

- If you select **Distinguished name and password**, provide the following information:
 - In the **Distinguished name** field, specify the LDAP distinguished name that identifies the user for the system to use when performing EIM operations.
 - In the **Password** field, specify the password for the distinguished name.
 - In the **Confirm password** field, specify the password a second time for verification purposes.
- If you select **Kerberos principal and password**, provide the following information:
 - In the **Principal** field, specify the Kerberos principal name for the system to use when performing EIM operations
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal `jsmith` in the realm `ordept.myco.com` is represented in the keytab file as `jsmith@ordept.myco.com`.
 - In the **Password** field, enter the password for the user.
 - In the **Confirm password** field, specify the password a second time for verification purposes.
- If you select **Kerberos keytab file and principal**, provide the following information:
 - In the **Keytab file** field, specify the fully qualified path and keytab file name that contains the Kerberos principal for the system to use when performing EIM operations. Or, click **Browse** to browse through directories in the System i integrated file system to select a keytab file.

- In the **Principal** field, specify the Kerberos principal name for the system to use when performing EIM operations.
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal `jsmith` in the realm `ordept.myco.com` is represented in the keytab file as `jsmith@ordept.myco.com`.
 - Click **Verify Connection** to ensure that the wizard can use the specified user information to successfully establish a connection to the EIM domain controller.
 - Click **Next**.
11. In the **Summary** panel, review the configuration information that you have provided. If all information is correct, click **Finish**.

Finalize your EIM configuration for the domain

When the wizard finishes, it adds the new domain to the **Domain Management** folder and you have created a basic EIM configuration for this server. However, you must complete these tasks to finalize your EIM configuration for the domain:

1. Use the EIM Configuration wizard on each additional server that you want to have join the domain.
2. Add EIM registry definitions to the EIM domain, if necessary, for other non-System i platforms and applications that you want to participate in the EIM domain. These registry definitions refer to the actual user registries that must participate in the domain. You can either add system registry definitions or add application registry definitions depending on your EIM implementation needs.
3. Based on your EIM implementation needs, determine whether to:
 - Create EIM identifiers for each unique user or entity in the domain and create identifier associations for them.
 - Create policy associations to map a group of users to a single target user identity.
 - Create a combination of these.
4. Use the EIM test a mapping function to test the identity mappings for your EIM configuration.
5. If the only EIM user you have defined is the DN for the LDAP administrator, then your EIM user has a high level of authority to all data on the directory server. Therefore, you might consider creating one or more DNs as additional users that have more appropriate and limited access control for EIM data. To learn more about creating DNs for the directory server, review Distinguished names in the i5/OS Information Center. The number of additional EIM users that you define depends on your security policy's emphasis on the separation of security duties and responsibilities. Typically, you might create at least the two following types of DNs:
 - **A user that has EIM administrator access control**
 This EIM administrator DN provides the appropriate level of authority for an administrator who is responsible for managing the EIM domain. This EIM administrator DN could be used to connect to the domain controller when managing all aspects of the EIM domain by means of System i Navigator.
 - **At least one user that has all of the following access controls:**
 - Identifier administrator
 - Registry administrator
 - EIM mapping operations
 This user provides the appropriate level of access control required for the system user that performs EIM operations on behalf of the operating system.

Note: To use this new DN for the system user instead of the LDAP administrator DN, you must change the EIM configuration properties for the System i platform. Review Manage EIM configuration properties to learn how to change the system user DN.

Additionally, you might want to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to configure a secure connection to the EIM domain controller to protect the transmission of EIM data. If you enable SSL for the directory server, you must update EIM configuration properties to specify that the System i platform uses a secure SSL connection. Also, you must update the properties for the domain to specify that EIM uses SSL connections for managing the domain through System i Navigator.

Note: You might need to perform additional tasks if you created a basic network authentication service configuration, especially if you are implementing a single sign-on environment. You can find information on these additional steps by reviewing the complete configuration steps demonstrated by the scenario, *Enable single sign-on for i5/OS*.

Creating and joining a new remote domain

When you use the EIM Configuration wizard to create and join a new domain, you can choose to configure a directory server on a remote system to act as the EIM domain controller as part of creating your EIM configuration.

You must specify the appropriate information for connecting to the remote directory server to allow you to configure EIM. If Kerberos is not currently configured on the System i platform, the wizard prompts you to start the Network Authentication Service Configuration wizard.

Note: The directory server on the remote system must provide EIM support. EIM requires that the domain controller be hosted by a directory server that supports Lightweight Directory Access Protocol (LDAP) Version 3. Additionally, the directory server product must have the EIM schema configured. For example, the IBM Directory Server V5.1 provides this support. For more detailed information about EIM domain controller requirements, review “Planning an Enterprise Identity Mapping domain controller” on page 54.

When you complete the EIM Configuration wizard, you can accomplish these tasks:

- Create a new EIM domain.
- Configure a remote directory server to act as the EIM domain controller.
- Configure network authentication service for the system.
- Create EIM registry definitions for the local i5/OS registry and the Kerberos registry.
- Configure the system to participate in the new EIM domain.

To configure your system to create and join a new EIM domain, you must have all the following special authorities:

- Security administrator (*SECADM).
- All object (*ALLOBJ).
- System configuration (*IOSYSCFG).

To use the EIM Configuration wizard to create and join a domain on a remote system, complete these steps:

1. Verify that the directory server on the remote system is active.
2. In System i Navigator, select the system for which you want to configure EIM and expand **Network > Enterprise Identity Mapping**.
3. Right-click **Configuration** and select **Configure** to start the EIM Configuration wizard.

Note: This option is labeled **Reconfigure** if EIM has been previously configured on the system.

4. On the **Welcome** page of the wizard, select **Create and join a new domain**, and click **Next**.
5. On the **Specify EIM Domain Location** page, select **On the local Directory server** and click **Next**.

Note: This option configures the local directory server to act as the EIM domain controller. Because this directory server stores all EIM data for the domain, it must be active and remain active to support EIM mapping lookups and other operations.

If network authentication service is not currently configured on the System i platform, or additional network authentication configuration information is needed to configure a single sign-on environment, the **Network Authentication Services Configuration** page displays. This page allows you start the Network Authentication Service Configuration wizard so that you can configure network authentication service. Or, you can configure Network Authentication Service at a later time by using the configuration wizard for this service through System i Navigator. When you complete network authentication service configuration, the EIM Configuration wizard continues.

6. To configure network authentication service, complete these steps:
 - a. On the **Configure Network Authentication Service** page, select **Yes** to start the Network Authentication Service Configuration wizard. With this wizard, you can configure several i5/OS interfaces and services to participate in a Kerberos realm as well as configure a single signon environment that uses both EIM and network authentication service.
 - b. On the **Specify Realm Information** page, specify the name of the default realm in the **Default realm** field. If you are using Microsoft Active Directory for Kerberos authentication, select **Microsoft Active Directory is used for Kerberos authentication**, and click **Next**.
 - c. On the **Specify KDC Information** page, specify the fully qualified name of the Kerberos server for this realm in the **KDC** field, specify 88 in the **Port** field, and click **Next**.
 - d. On the **Specify Password Server Information** page, select either **Yes** or **No** for setting up a password server. The password server allows principals to change passwords on the Kerberos server. If you select **Yes**, enter the password server name in the **Password server** field. In the **Port** field, accept the default value of 464, and click **Next**.
 - e. On the **Select Keytab Entries** page, select **i5/OS Kerberos Authentication**, and click **Next**.

Note: In addition you can also create keytab entries for the IBM Tivoli Directory Server for i5/OS, i5/OS NetServer, and IBM HTTP Server for i5/OS server if you want these services to use Kerberos authentication. You may need to perform additional configuration for these services before they can use Kerberos authentication.

- f. On the **Create i5/OS Keytab Entry** page, enter and confirm a password, and click **Next**. This is the same password you will use when you add the i5/OS principals to the Kerberos server.
- g. Optional: On the **Create Batch File** page, select **Yes**, specify the following information, and click **Next**:
 - In the **Batch file** field, update the directory path. Click **Browse** to locate the appropriate directory path, or edit the path in the **Batch file** field.
 - In the **Include password** field, select **Yes**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is essential that you delete the batch file from the Kerberos server and from the PC immediately after you use it. If you do not include the password, you will be prompted for the password when you run the batch file.

Note: You can also manually add the service principals that are generated by the wizard to Microsoft Active Directory. To learn how to do this, review **Add i5/OS principals to the Kerberos server**.

- On the **Summary** page, review the network authentication service configuration details, and click **Finish** to return to the EIM Configuration wizard.
7. Use the **Specify EIM Domain Controller** page to specify connection information as follows for the remote EIM domain controller that you want to configure:

- a. In the **Domain controller name** field, specify the name of the remote directory server that you want to configure as the EIM domain controller for the domain that you are creating. The EIM domain controller name can be the directory server TCP/IP host and domain name or the directory server address.
 - b. Specify connection information for the connection to the domain controller as follows:
 - Select the **Use secure connection (SSL or TLS)** to use a secure connection to the EIM domain controller. When this is selected, the connection uses either Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to establish a secure connection to protect EIM data transmission over an untrusted network, such as the Internet.
- Note:** You must verify whether the EIM domain controller is configured to use a secure connection. Otherwise, the connection to the domain controller may fail.
- In the **Port** field, specify the TCP/IP port on which the directory server listens. If **Use secure connection** is selected, the default port is 636; otherwise, the default port is 389.
 - c. Click **Verify Connection** to test that the wizard can use the specified information to successfully establish a connection to the remote EIM domain controller.
 - d. Click **Next**.
8. On the **Specify User For Connection** page, 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**, **Kerberos principal and password**, or **User profile and password**. The two Kerberos user types are available only if network authentication service is configured for the local System i platform. The user type that you select determines the other information that you must provide to complete the dialog as follows:

Note: To ensure that the wizard has enough authority to create the necessary EIM objects in the directory, select **Distinguished name and password** as the user type and specify the LDAP administrator DN and password as the user.

You can specify a different user for the connection; however, the user you specify must have the equivalent of LDAP administrator authority for the remote directory server.

- a. If you select **Distinguished name and password**, provide the following information:
 - In the **Distinguished name** field, specify the LDAP administrator's distinguished name (DN) and password to ensure the wizard has enough authority to administer the EIM domain and the objects in it.
 - In the **Password** field, specify the password for the distinguished name.
 - In the **Confirm password** field, specify the password a second time for validation purposes.
- b. If you select **Kerberos keytab file and principal**, provide the following information:
 - In the **Keytab file** field, specify the fully qualified path and keytab file name that contains the Kerberos principal for the wizard to use when connecting to the EIM domain. Or, click **Browse** to browse through directories in the i5/OS integrated file system to select a keytab file.
 - In the **Principal** field, specify the name of the Kerberos principal to be used to identify the user.
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal `jsmith` in the realm `ordept.myco.com`, is represented in the keytab file as `jsmith@ordept.myco.com`.
- c. If you select **Kerberos principal and password**, provide the following information:
 - In the **Principal** field, specify the name of the Kerberos principal for the wizard to use when connecting to the EIM domain.

- In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
 - In the **Password** field, specify the password for the Kerberos principal.
 - In the **Confirm password** field, specify the password a second time for validation purposes.
- d. If you select **User profile and password**, provide the following information:
 - In the **User profile** field, specify the user profile name for the wizard to use when connecting to the EIM domain.
 - In the **Password** field, specify the password for the user profile.
 - In the **Confirm password** field, specify the password a second time for validation purposes.
 - e. Click **Verify Connection** to test that the wizard can use the specified user information to successfully establish a connection to the EIM domain controller.
 - f. Click **Next**.
9. On the **Specify Domain** page, provide the following information:
 - a. 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 *.
 - b. In the **Description** field, enter text to describe the domain.
 - c. Click **Next**.
 10. On the **Specify Parent DN for Domain** dialog, select **Yes** to specify the parent DN the wizard should use for the location of the EIM domain that you are creating. This is the DN that represents the entry immediately above your domain name entry in the directory information tree hierarchy. Or specify **No** to have EIM data stored in a directory location with a suffix whose name is derived from the EIM domain name.
- Note:** When you use the wizard to configure a domain on a remote domain controller you should specify an appropriate parent DN for the domain. Because all necessary configuration objects for the parent DN must already exist or the EIM configuration may fail, you should browse for the appropriate parent DN rather than manually enter the DN information. Click **Help** for further information about using a parent DN.
11. On the **Registry Information** page, specify whether to add local user registries to the EIM domain as registry definitions. Select one or both of these user registry types:

Note: You do not have to create the registry definitions at this time. If you choose to create the registry definitions later, view adding a system registry definition and EIM configuration properties.

 - a. Select **Local i5/OS** to add a registry definition for the local registry. In the field provide, accept the default value for the registry definition name or specify a different value for the registry definition name. The EIM registry name is an arbitrary string that represents the registry type and specific instance of that registry.
 - b. Select **Kerberos** to add a registry definition for a Kerberos registry. In the field provided, accept the default value for the registry definition name or specify a different value for the registry definition name. The default registry definition name is the same as the realm name. By accepting the default name and using the same Kerberos registry name as the realm name, you can increase performance in retrieving information from the registry. Select **Kerberos user identities are case sensitive**, if necessary.
 - c. Click **Next**.
 12. On the **Specify EIM System User** page, select a **User type** that you want the system to use when performing EIM operations on behalf of operating system functions. These operations include mapping lookup operations and deletion of associations when deleting a local i5/OS 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**. Which user types you can select vary based on the current system configuration. For example, if Network Authentication Service is not configured for the system, then Kerberos user types may not be available for selection. The user type that you select determines the other information that you must provide to complete the page as follows:

Note: You must specify a user that is currently defined in the directory server which is hosting the EIM domain controller. The user that you specify must have privileges to perform mapping lookup and registry administration for the local user registry at a minimum. If the user that you specify does not have these privileges, then certain operating system functions related to the use of single sign-on and the deletion of user profiles may fail.

If you have not configured the directory server prior to running this wizard, the only user type you can select is **Distinguished name and password** and the only distinguished name you can specify is the LDAP administrator's DN.

- a. If you select **Distinguished name and password**, provide the following information:
 - In the **Distinguished name** field, specify the LDAP distinguished name that identifies the user for the system to use when performing EIM operations.
 - In the **Password** field, specify the password for the distinguished name.
 - In the **Confirm password** field, specify the password a second time for verification purposes.
 - b. If you select **Kerberos principal and password**, provide the following information:
 - In the **Principal** field, specify the Kerberos principal name for the system to use when performing EIM operations
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal `jsmith` in the realm `ordept.myco.com` is represented in the keytab file as `jsmith@ordept.myco.com`.
 - In the **Password** field, enter the password for the user.
 - In the **Confirm password** field, specify the password a second time for verification purposes.
 - c. If you select **Kerberos keytab file and principal**, provide the following information:
 - In the **Keytab file** field, specify the fully qualified path and keytab file name that contains the Kerberos principal for the system to use when performing EIM operations. Or, click **Browse** to browse through directories in the System integrated file system to select a keytab file.
 - In the **Principal** field, specify the Kerberos principal name for the system to use when performing EIM operations.
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal `jsmith` in the realm `ordept.myco.com` is represented in the keytab file as `jsmith@ordept.myco.com`.
 - d. Click **Verify Connection** to ensure that the wizard can use the specified user information to successfully establish a connection to the EIM domain controller.
 - e. Click **Next**.
13. In the **Summary** panel, review the configuration information that you have provided. If all information is correct, click **Finish**.

Finalize your EIM configuration for the domain

When the wizard finishes, it adds the new domain to the **Domain Management** folder and you have created a basic EIM configuration for this server. However, you must complete these tasks to finalize your EIM configuration for the domain:

1. Use the EIM Configuration wizard on each additional server that you want to have join an existing domain. Review the "Joining an existing domain" on page 78 topic for more information.

2. Add EIM registry definitions to the EIM domain, if necessary, for other non-System i platforms and applications that you want to participate in the EIM domain. These registry definitions refer to the actual user registries that must participate in the domain. Depending on your EIM implementation needs you should view either “Adding a system registry definition” on page 89 or “Adding an application registry definition” on page 90.
3. Based on your EIM implementation needs, determine whether to:
 - a. “Creating an EIM identifier” on page 96 for each unique user or entity in the domain and “Creating EIM identifier association” on page 99 for them.
 - b. “Creating a policy association” on page 100 to map a group of users to a single target user identity.
 - c. Create a combination of these.
4. Use the EIM “Testing EIM mappings” on page 86 function to test the identity mappings for your EIM configuration.
5. If the only EIM user you have defined is the DN for the LDAP administrator, then your EIM user has a high level of authority to all data on the directory server. Therefore, you might consider creating one or more DNs as additional users that have more appropriate and limited access control for EIM data. To learn more about creating DNs for the directory server, review Distinguished names in the i5/OS Information Center. The number of additional EIM users that you define depends on your security policy’s emphasis on the separation of security duties and responsibilities. Typically, you might create at least the two following types of DNs:
 - **A user that has EIM administrator access control**

This EIM administrator DN provides the appropriate level of authority for an administrator who is responsible for managing the EIM domain. This EIM administrator DN could be used to connect to the domain controller when managing all aspects of the EIM domain by means of System i Navigator.
 - **At least one user that has all of the following access controls:**
 - Identifier administrator
 - Registry administrator
 - EIM mapping operations

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

Note: To use this new DN for the system user instead of the LDAP administrator DN, you must change the EIM configuration properties for the System i platform. Review “Managing EIM configuration properties” on page 113 to learn how to change the system user DN.

You might need to perform additional tasks if you created a basic network authentication service configuration, especially if you are implementing a single sign-on environment. You can find information about these additional steps by reviewing the complete configuration steps demonstrated by the scenario, Enable single sign-on for i5/OS.

Joining an existing domain

Use the Enterprise Identity Mapping (EIM) Configuration wizard on one System i platform to configure a domain controller and create an EIM domain, then you can use the wizard to configure other systems to participate in the domain.

After you create an EIM domain and configure a domain controller on one system, you can configure all additional System i platforms to join the existing EIM domain. As you work through the wizard you must supply information about the domain, including connection information to the EIM domain controller. When you use the EIM Configuration wizard to join an existing domain, the wizard still provides you with the option of launching the Network Authentication Service Configuration wizard if you choose to configure Kerberos as part of configuring EIM on the system.

When you complete the EIM Configuration wizard to join an existing domain, you can accomplish these tasks:

- Configure network authentication service for the system.
- Create EIM registry definitions for the local i5/OS registry and the Kerberos registry.
- Configure the system to participate in an existing EIM domain.

To configure your system to join an existing EIM domain, you must have all of the following special authorities:

- Security administrator (*SECADM).
- All object (*ALLOBJ).

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

1. Verify that the directory server on the remote system is active.
2. In System i Navigator, select the system for which you want to configure EIM and expand **Network > Enterprise Identity Mapping**.
3. Right-click **Configuration** and select **Configure...** to start the EIM Configuration wizard.

Note: This option is labeled **Reconfigure...** if EIM has been previously configured on the system.

4. On the **Welcome** page of the wizard, select **Join an existing domain**, and click **Next**.

Note: If network authentication service is not currently configured on the System i model, or additional network authentication configuration information is needed to configure a single sign-on environment, the **Network Authentication Services Configuration** page displays. This page allows you start the Network Authentication Service Configuration wizard so that you can configure network authentication service. Or, you can configure Network Authentication Service at a later time by using the configuration wizard for this service through System i Navigator. When you complete network authentication service configuration, the EIM Configuration wizard continues.

5. To configure network authentication service, complete these steps:
 - a. On the **Configure Network Authentication Service** page, select **Yes** to start the Network Authentication Service Configuration wizard. With this wizard, you can configure several i5/OS interfaces and services to participate in a Kerberos realm as well as configure a single signon environment that uses both EIM and network authentication service.
 - b. On the **Specify Realm Information** page, specify the name of the default realm in the **Default realm** field. If you are using Microsoft Active Directory for Kerberos authentication, select **Microsoft Active Directory is used for Kerberos authentication**, and click **Next**.
 - c. On the **Specify KDC Information** page, specify the fully qualified name of the Kerberos server for this realm in the **KDC** field, specify 88 in the **Port** field, and click **Next**.
 - d. On the **Specify Password Server Information** page, select either **Yes** or **No** for setting up a password server. The password server allows principals to change passwords on the Kerberos server. If you select **Yes**, enter the password server name in the **Password server** field. In the **Port** field, accept the default value of 464, and click **Next**.
 - e. On the **Select Keytab Entries** page, select **i5/OS Kerberos Authentication**, and click **Next**.

Note: In addition you can also create keytab entries for the IBM Tivoli Directory Server for i5/OS, i5/OS NetServer, and IBM HTTP Server for i5/OS if you want these services to use Kerberos authentication. You may need to perform additional configuration for these services before they can use Kerberos authentication.

- f. On the **Create i5/OS Keytab Entry** page, enter and confirm a password, and click **Next**. This is the same password you will use when you add the i5/OS principals to the Kerberos server.
- g. Optional: On the **Create Batch File** page, select **Yes**, specify the following information, and click **Next**:

- In the **Batch file** field, update the directory path. Click **Browse** to locate the appropriate directory path, or edit the path in the **Batch file** field.
- In the **Include password** field, select **Yes**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is essential that you delete the batch file from the Kerberos server and from the PC immediately after you use it. If you do not include the password, you will be prompted for the password when you run the batch file.

Note: You can also manually add the service principals that are generated by the wizard to Microsoft Active Directory. To learn how to do this, review *Add i5/OS principals to the Kerberos server*

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

6. On the **Specify Domain Controller** page provide the following information:

Note: The directory server that acts as the domain controller must be active to successfully complete this EIM configuration.

- 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 System i platform to join.
- Click **Use secure connection (SSL or TLS)** if you want to use a secure connection to the EIM domain controller. When this is selected, the connection uses either Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to establish a secure connection to protect EIM data transmission over an untrusted network, such as the Internet.

Note: You must verify whether the EIM domain controller is configured to use a secure connection. Otherwise, the connection to the domain controller may fail.

- In the **Port** field, specify the TCP/IP port on which the directory server listens. If **Use secure connection** is selected, the default port is 636; otherwise, the default port is 389.
- Click **Verify Connection** to test that the wizard can use the specified information to successfully establish a connection to the EIM domain controller.
- Click **Next**.

7. On the **Specify User For Connection** page, 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**, **Kerberos principal and password**, or **User profile and password**. The two Kerberos user types are available only if network authentication service is configured for the local System i platform. The user type that you select determines the other information that you must provide to complete the dialog as follows:

Note: To ensure that the wizard has enough authority to create the necessary EIM objects in the directory, select **Distinguished name and password** as the user type and specify the LDAP administrator DN and password as the user.

You can specify a different user for the connection; however, the user you specify must have the equivalent of LDAP administrator authority for the remote directory server.

- If you select **Distinguished name and password**, provide the following information:
 - In the **Distinguished name** field, specify the LDAP distinguished name (DN) that identifies the user who is authorized to create objects in the local namespace of the LDAP server. If you used this wizard to configure the LDAP server in an earlier step, you should enter the distinguished name of the LDAP administrator that you created in that step.
 - In the **Password** field, specify the password for the distinguished name.
 - In the **Confirm password** field, specify the password a second time for validation purposes.

- If you select **Kerberos keytab file and principal**, provide the following information:
 - In the **Keytab file** field, specify the fully qualified path and keytab file name that contains the Kerberos principal for the wizard to use when connecting to the EIM domain. Or, click **Browse...** to browse through directories in the System i integrated file system to select a keytab file.
 - In the **Principal** field, specify the name of the Kerberos principal to be used to identify the user.
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com, is represented in the keytab file as jsmith@ordept.myco.com.
 - If you select **Kerberos principal and password**, provide the following information:
 - In the **Principal** field, specify the name of the Kerberos principal for the wizard to use when connecting to the EIM domain.
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal jsmith in the realm ordept.myco.com is represented in the keytab file as jsmith@ordept.myco.com.
 - In the **Password** field, specify the password for the Kerberos principal.
 - In the **Confirm password** field, specify the password a second time for validation purposes.
 - If you select **User profile and password**, provide the following information:
 - In the **User profile** field, specify the user profile name for the wizard to use when connecting to the EIM domain.
 - In the **Password** field, specify the password for the user profile.
 - In the **Confirm password** field, specify the password a second time for validation purposes.
 - Click **Verify Connection** to test that the wizard can use the specified user information to successfully establish a connection to the EIM domain controller.
 - Click **Next**.
8. On the **Specify Domain** page, select the name of the domain that you want to join and click **Next**.
9. On the **Registry Information** page, specify whether to add local user registries to the EIM domain as registry definitions. Select one or both of these user registry types:
- Select **Local i5/OS** to add a registry definition for the local registry. In the field provide, accept the default value for the registry definition name or specify a different value for the registry definition name. The EIM registry name is an arbitrary string that represents the registry type and specific instance of that registry.

Note: You do not have to create the local i5/OS registry definition at this time. If you choose to create the i5/OS registry definition later, you need to add the system registry definition and update the EIM configuration properties.

- Select **Kerberos** to add a registry definition for a Kerberos registry. In the field provided, accept the default value for the registry definition name or specify a different value for the registry definition name. The default registry definition name is the same as the realm name. By accepting the default name and using the same Kerberos registry name as the realm name, you can increase performance in retrieving information from the registry. Select **Kerberos user identities are case sensitive**, if necessary.

Note: If you have used the EIM Configuration wizard on another system to add a registry definition for the Kerberos registry for which this System i model has a service principal, then you do not need to add a Kerberos registry definition as part of this configuration. However, you will need to specify the name of that Kerberos registry in the configuration properties for this system after you finish the wizard.

- Click **Next**.

10. On the **Specify EIM System User** page, select a **User type** that you want the system to use when performing EIM operations on behalf of operating system functions. These operations include mapping lookup operations and deletion of associations when deleting a local i5/OS 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**. Which user types you can select vary based on the current system configuration. For example, if Network Authentication Service is not configured for the system, then Kerberos user types may not be available for selection. The user type that you select determines the other information that you must provide to complete the page as follows:

Note: You must specify a user that is currently defined in the directory server which is hosting the EIM domain controller. The user that you specify must have privileges to perform mapping lookup and registry administration for the local user registry at a minimum. If the user that you specify does not have these privileges, then certain operating system functions related to the use of single sign-on and the deletion of user profiles may fail.

- If you select **Distinguished name and password**, provide the following information:
 - In the **Distinguished name** field, specify the LDAP distinguished name that identifies the user for the system to use when performing EIM operations.
 - In the **Password** field, specify the password for the distinguished name.
 - In the **Confirm password** field, specify the password a second time for verification purposes.
- If you select **Kerberos principal and password**, provide the following information:
 - In the **Principal** field, specify the Kerberos principal name for the system to use when performing EIM operations
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal `jsmith` in the realm `ordept.myco.com` is represented in the keytab file as `jsmith@ordept.myco.com`.
 - In the **Password** field, enter the password for the user.
 - In the **Confirm password** field, specify the password a second time for verification purposes.
- If you select **Kerberos keytab file and principal**, provide the following information:
 - In the **Keytab file** field, specify the fully qualified path and keytab file name that contains the Kerberos principal for the system to use when performing EIM operations. Or, click **Browse...** to browse through directories in the System i integrated file system to select a keytab file.
 - In the **Principal** field, specify the Kerberos principal name for the system to use when performing EIM operations.
 - In the **Realm** field, specify the fully qualified Kerberos realm name for which the principal is a member. The name of the principal and realm uniquely identify the Kerberos users in the keytab file. For example, the principal `jsmith` in the realm `ordept.myco.com` is represented in the keytab file as `jsmith@ordept.myco.com`.
- Click **Verify Connection** to ensure that the wizard can use the specified user information to successfully establish a connection to the EIM domain controller.
- Click **Next**.

11. On the **Summary** page, review the configuration information that you have provided. If all information is correct, click **Finish**.

Finalize your EIM configuration for the domain

When the wizard finishes, it adds the domain to the **Domain Management** folder and you have created a basic EIM configuration for this server. However, you may need to complete these tasks to finalize your EIM configuration for the domain:

1. Add EIM registry definitions to the EIM domain, if necessary, for systems not running i5/OS systems and applications that you want to participate in the EIM domain. These registry definitions refer to

the actual user registries that must participate in the domain. You can either Add system registry definitions or Add application registry definitions depending on your EIM implementation needs.

2. Based on your EIM implementation needs, determine whether to:
 - Create EIM identifiers for each unique user or entity in the domain and create identifier associations for them.
 - Create policy associations to map a group of users to a single target user identity.
 - Create a combination of these.
3. Use the EIM test a mapping function to test the identity mappings for your EIM configuration.
4. If the only EIM user you have defined is the DN for the LDAP administrator, then your EIM user has a high level of authority to all data on the directory server. Therefore, you might consider creating one or more DNs as additional users that have more appropriate and limited access control for EIM data. To learn more about creating DNs for the directory server, review Distinguished names in the i5/OS Information Center. The number of additional EIM users that you define depends on your security policy's emphasis on the separation of security duties and responsibilities. Typically, you might create at least the two following types of DNs:

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

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

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

- Identifier administrator
- Registry administrator
- EIM mapping operations

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

Note: To use this new DN for the system user instead of the LDAP administrator DN, you must change the EIM configuration properties for the System i platform. Review Manage EIM configuration properties to learn how to change the system user DN.

You might need to perform additional tasks if you created a basic network authentication service configuration, especially if you are implementing a single sign-on environment. You can find information on these additional steps by reviewing the complete configuration steps demonstrated by the scenario, Enable single sign-on for i5/OS.

Configuring a secure connection to the EIM domain controller

You may want to use Secure Sockets Layer (SSL) or Transport Layer Security Protocol (TLS) to establish a secure connection to the Enterprise Identity Mapping (EIM) domain controller to protect the transmission of EIM data.

To configure SSL or TLS for EIM, you must complete these tasks:

1. If necessary, use Digital Certificate Manager (DCM) to create a certificate for the directory server to use for SSL.
2. Enable SSL for the local directory server that hosts the EIM domain controller.
3. Update EIM Configuration properties to specify that the System i model uses a secure SSL connection. To update the EIM Configuration properties, complete these steps:
 - a. In System i Navigator, select the system on which you configured EIM and expand **Network → Enterprise Identity Mapping**.
 - b. Right-click **Configuration** and select **Properties**.

- c. On the **Domain** page, select **Use secure connection (SSL or TLS)**, specify the secure port on which your directory server listens or accept the default value of 636 in the **Port** field, and click **OK**.
4. Update EIM Domain properties for each EIM domain to specify that EIM uses an SSL connection when managing the domain through System i Navigator. To update the EIM Domain properties, complete these steps:
 - a. In System i Navigator, select the system on which you configured EIM and expand **Network** → **Enterprise Identity Mapping** → **Domain Management**.
 - b. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review **Add an EIM domain to Domain Management**.
 - If you are not currently connected to the EIM domain in which you want to work, review **Connect to the EIM domain controller**.
 - c. Right-click the EIM domain to which you are now connected and select **Properties**.
 - d. On the **Domain** page, select **Use secure connection (SSL or TLS)**, specify the secure port on which your directory server listens or accept the default value of 636 in the **Port** field, and click **OK**.

Managing Enterprise Identity Mapping

After you configure Enterprise Identity Mapping (EIM) on your System i platform, there are many administrative tasks that you will need to perform over time to manage your EIM domain and data for the domain.

To learn more about managing EIM in your enterprise, review these pages.

Managing Enterprise Identity Mapping domains

Use System i Navigator to manage all of your EIM domains.

To manage any EIM domain, the domain must be listed in, or you must add it to, the **Domain Management** folder under the **Network** folder in System i Navigator. When you use the EIM Configuration wizard to create and configure a new EIM domain, the domain is added to the **Domain Management** folder automatically so that you can manage the domain and information in the domain.

You can use any System i connection to manage an EIM domain that resides anywhere in the same network, even when the system that you are using is not a participant in the domain.

You can perform the following management tasks for a domain:

Adding an EIM domain to the Domain Management folder

To add an EIM domain to the Domain Management folder, you must have *SECADM special authority and the domain that you want to add must exist prior to adding it to the Domain Management folder.

To add an existing Enterprise Identity Mapping (EIM) domain to the **Domain Management** folder, complete these steps:

1. Expand **Network** > **Enterprise Identity Mapping** .
2. Right-click **Domain Management** and select **Add Domain**.
3. In the **Add Domain** dialog, specify the required domain and connection information. Or, click **Browse** to view a list of domains that the specified domain controller manages.

Note: If you click **Browse**, the **Connect to EIM Domain Controller** dialog displays. To view the list of domains, you must connect to the domain controller with either LDAP administrator access control or EIM administrator access control. The contents of the domain list vary based on the EIM access control that you have. If you have LDAP administrator access control, you can view

a list of all domains that the domain controller manages. Otherwise the list displays only those domains for which you have EIM administrator access control.

4. Click **Help**, if necessary, to determine what information to specify for each field.
5. Click **OK** to add the domain.

Connecting to an EIM domain

Before you can work with an Enterprise Identity Mapping (EIM) domain, you must first connect to the EIM domain controller for the domain. You may connect to an EIM domain even if your System i model is not currently configured to participate in this domain.

To connect to the EIM domain controller, the user with which you connect must be a member of an EIM access control group. Your EIM access control group membership determines what tasks you can perform in the domain and what EIM data you can view or change.

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

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Right-click the domain to which you want to connect.

Note: If the domain with which you want to work is not listed under **Domain Management**, you must add an EIM domain to the domain management folder.

3. Right-click the EIM domain to which you want to connect and select **Connect**.
4. On the **Connect to EIM Domain Controller** dialog, specify the **User type**, provide the required identification information for the user, and select a password option for connecting to the domain controller.
5. Click **Help**, if necessary, to determine what information to specify for each field in the dialog.
6. Click **OK** to connect to the domain controller.

Enabling policy associations for a domain

A policy association provides a means of creating many-to-one mappings in situations where associations between user identities and an Enterprise Identity Mapping (EIM) identifier do not exist.

You can use a policy association to map a source set of multiple user identities (rather than a single user identity) to a single target user identity in a specified target user registry. Before you can use policy associations, however, you must first ensure that you enable the domain to use policy associations for mapping lookup operations.

To enable mapping policy support to use policy associations for a domain, you must be connected to the EIM domain in which you want to work and you must have EIM administrator access control.

To enable mapping lookup support to use policy associations for a domain, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Right-click the EIM domain in which you want to work and select **Mapping Policy**.
 - If the EIM domain you want to work with is not listed under **Domain Management**, you must add an EIM domain to the domain management folder.
 - If you are not currently connected to the EIM domain in which you want to work, you need to connect to the EIM domain controller. (The **Mapping Policy** option is not available until you connect to the domain.)
3. On the **General** page, select **Enable mapping lookups using policy associations for domain**.
4. Click **OK**.

Note: You must enable mapping lookups and the use of policy associations for each target registry definition for which there are policy associations defined. If you do not enable mapping lookups for the target registry definition, that registry cannot participate in EIM mapping lookup

operations. If you do not specify that the target registry can use policy associations, then any defined policy associations for that registry are ignored by EIM mapping lookup operations.

Related concepts

“EIM mapping policy support and enablement” on page 35

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain. You can use policy associations instead of, or in combination with, identifier associations.

Testing EIM mappings

Enterprise Identity Mapping (EIM) mapping testing allows you to issue EIM mapping lookup operations against your EIM configuration. You can use the test to verify that a specific source user identity maps correctly to the appropriate target user identity. Testing ensures that EIM mapping lookup operations can return the correct target user identity based on the specified information.

To use the test a mapping function to test your EIM configuration, you must be connected to the EIM domain in which you want to work and you must have EIM access control at one of these levels:

- EIM administrator
- Identifier administrator
- Registry administrator
- EIM mapping lookup operations

To use mapping test support to test your EIM configuration, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review Add an EIM domain to Domain Management.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Right-click the EIM domain to which you are connected and select **Test a Mapping**
4. In the **Test a Mapping** dialog, specify the following information:
 - a. In the **Source registry** field, provide the registry definition name that refers to the user registry that you want to use as the source of the test mapping lookup operation.
 - b. In the **Source user** field, provide the user identity name that you want to use as the source of the test mapping lookup operation.
 - c. In the **Target registry** field, provide the registry definition name that refers to the user registry that you want to use as the target of the test mapping lookup operation.
 - d. Optional: In the **Lookup information** field, provide any lookup information defined for the target user.
5. Click **Help**, if necessary, for more details about what information is needed for each field in the dialog.
6. Click **Test** and review the results of the mapping lookup operation when they display.

Note: If the mapping lookup operation returns ambiguous results, the Test a Mapping - Results dialog is displayed indicating an error message and a list of the target users that the lookup operation finds.

- a. To troubleshoot ambiguous results, select a target user and click **Details**.
 - b. The Test a Mapping - Details dialog is displayed indicating information about the mapping lookup operation results for the specified target user. Click **Help** for more detailed information about the mapping lookup operation results.
 - c. Click **Close** to exit the **Test a Mapping - Results** dialog.
7. Continue testing your configuration, or click **Close** to exit.

Related concepts

“Troubleshooting EIM mapping problems” on page 117

There are a number of common problems that may cause Enterprise Identity Mapping (EIM) mappings to fail entirely or not to work as expected. Review the following table to find information about what problem may be causing an EIM mapping to fail and potential solutions for that problem. If EIM mappings are failing, you may need to work through each solution in the table to ensure that you find and solve the problem or problems which are causing the mappings to fail.

Working with test results and resolving problems:

When the test runs, a target user identity is returned if the test process finds an association between the source user identity and target user registry that the administrator supplied. The test also indicates the type of association that it found between the two user identities. When the test process does not find an association based on the information supplied, the test returns a target user identity of none.

The test, like any EIM mapping lookup operation, searches for and returns the first appropriate target user identity, by searching in the following order:

1. Specific identifier association
2. Certificate filter policy association
3. Default registry policy association
4. Default domain policy association

In some cases, the test returns no target user identity results although associations are configured for the domain. Verify that you supplied the correct information for the test. If the information is correct and the test returns no results, then the problem may be caused by one of the following:

- Policy association support is not enabled at the domain level. You may need to enable policy associations for a domain.
- Mapping lookup support or policy association support is not enabled at the individual registry level. You may need to enable mapping lookup support and the use of policy associations for the target registry.
- A target or source association for an EIM identifier is not configured correctly. For example, there is no source association for the Kerberos principal (or windows user) or it is incorrect. Or, the target association specifies an incorrect user identity. Display all identifier associations for an EIM identifier to verify associations for a specific identifier.
- A policy association is not configured correctly. Display all policy associations for a domain to verify source and target information for all policy associations defined in the domain.
- The registry definition and user identities do not match because of case sensitivity. You can delete and re-create the registry, or delete and re-create the association with the proper case.

In other cases, the test may have ambiguous results. In such a case, an error message indicating this displays. The test returns ambiguous results when more than one target user identity matches the specified test criteria. A mapping lookup operation can return multiple target user identities when one or more of the following situations exist:

- An EIM identifier has multiple individual target associations to the same target registry.
- More than one EIM identifier has the same user identity specified in a source association and each of these EIM identifiers has a target association to the same target registry, although the user identity specified for each target association may be different.
- More than one default domain policy association specifies the same target registry.
- More than one default registry policy association specifies the same source registry and the same target registry.
- More than one certificate filter policy association specifies the same source X.509 registry, certificate filter, and target registry.

A mapping lookup operation that returns more than one target user identity can create problems for EIM-enabled applications, including i5/OS applications and products. Consequently, you need to determine the cause of the ambiguous results and what action needs to be taken to resolve the situation. Depending on the cause, you can do one or more of the following:

- The test returns unwanted multiple target identities. This indicates that association configuration for the domain is not correct, due to one of the following:
 - A target or source association for an EIM identifier is not configured correctly. For example, there is no source association for the Kerberos principal (or windows user) or it is incorrect. Or, the target association specifies an incorrect user identity. Display all identifier associations for an EIM identifier to verify associations for a specific identifier.
 - A policy association is not configured correctly. Display all policy associations for a domain to verify source and target information for all policy associations defined in the domain.
- The test returns multiple target user identities and these results are appropriate for the way you configured associations, then you need to specify lookup information for each target user identity. You need to define unique lookup information for all target user identities that have the same source (either an EIM identifier for identifier associations or a source user registry for policy associations). By defining lookup information for each target user identity, you ensure that a lookup operation returns a single target user identity rather than all possible target user identities. Review Add lookup information to a target user identity. You must specify this lookup information about the mapping lookup operation.

Note: This approach only works if the application is enabled to use the lookup information. However, base i5/OS applications such as System i Access for Windows can not use lookup information to distinguish among multiple target user identities returned by a lookup operation. Consequently, you might consider redefining associations for the domain to ensure that a mapping lookup operation can return a single target user identity to ensure that base i5/OS applications can successfully perform lookup operations and map identities.

Removing an EIM domain from the Domain Management folder

You can remove an EIM domain that you no longer want to manage from the **Domain Management** folder. However, removing the domain from the **Domain Management** folder is **not** the same as deleting the domain and it does not delete the domain data from the domain controller.

You do not need any EIM access control to remove a domain.

To remove an Enterprise Identity Mapping (EIM) domain that you no longer want to manage from the **Domain Management** folder, complete these 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.

Related tasks

“Deleting an EIM domain and all configuration objects”

Before you can delete an EIM domain, you must delete all registry definitions and all Enterprise Identity Mapping (EIM) identifiers in the domain. If you do not want to delete the domain and all domain data, but no longer want to manage the domain, you can remove the domain instead.

Deleting an EIM domain and all configuration objects

Before you can delete an EIM domain, you must delete all registry definitions and all Enterprise Identity Mapping (EIM) identifiers in the domain. If you do not want to delete the domain and all domain data, but no longer want to manage the domain, you can remove the domain instead.

To delete an EIM domain, you must have EIM access control at one of these levels:

- LDAP administrator.
 - EIM administrator.
1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
 2. If necessary, delete all registry definitions from the EIM domain.
 3. If necessary, 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.

Note: The Delete in Progress dialog displays to indicate the status of the domain deletion until the process is complete.

Related tasks

“Removing an EIM domain from the Domain Management folder” on page 88

You can remove an EIM domain that you no longer want to manage from the **Domain Management** folder. However, removing the domain from the **Domain Management** folder is **not** the same as deleting the domain and it does not delete the domain data from the domain controller.

Managing Enterprise Identity Mapping registry definitions

To have user registries and the user identities that they contain participate in an EIM domain you must create registry definitions for them. You can then manage how the user registries and their user identities participate in EIM by managing these EIM registry definitions.

You can perform the following management tasks for registry definitions:

Related concepts

“Creating a policy association” on page 100

A policy association provides a means to directly define a relationship between multiple user identities in one or more registries and an individual target user identity in another registry.

Related tasks

“Deleting a policy association” on page 112

To delete a policy association, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM access control for either Registry administrator or EIM administrator.

Adding a system registry definition

To create a system registry definition, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM administrator access control.

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

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under Domain Management, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.
3. Expand the EIM domain to which you are now connected.
4. Right-click **User Registries**, select **Add Registry**, then select **System**.
5. In the **Add system Registry** dialog box, provide information about the system registry definition, as follows:
 - a. A name for the system registry definition.
 - b. A registry definition type.
 - c. A description of the system registry definition.

- d. (Optional.) The user registry URL.
 - e. One or more aliases for the system registry definition, if necessary.
6. Click **OK** to save the information and add the registry definition to the EIM domain.

Adding an application registry definition

To create an application registry definition, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM administrator access control.

To add an application registry definition to an EIM domain, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under Domain Management, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.
3. Expand the EIM domain to which you are now connected.
4. Right-click **User Registries**, select **Add Registry**, then select **Application**.
5. In the **Add Application Registry** dialog, provide information about the application registry definition, as follows:
 - a. A name for the application registry definition.
 - b. The name of the system registry definition of which the application user registry that you are defining is a subset. The system registry definition that you specify must already exist in EIM, otherwise creation of the application registry definition fails.
 - c. A registry definition type.
 - d. A description of the application registry definition.
 - e. One or more aliases for the application registry definition, if necessary.
6. Click **Help**, if necessary, to determine what information to provide for each field.
7. Click **OK** to save the information and add the registry definition to the EIM domain.

Related concepts

“System registry definitions” on page 13

A system registry definition is an entry that you create in Enterprise Identity Mapping (EIM) to represent and describe a distinct user registry within a workstation or server.

Adding a group registry definition

To create a group registry definition, you must be connected to the EIM domain in which you want to work and you must have EIM administrator access control.

To add a group registry definition to an EIM domain, complete these steps:

1. Expand **Network → Enterprise Identity Mapping → Domain Management**.
2. Select the EIM domain in which you want to work.
 - a. If the EIM domain you want to work with is not listed under Domain Management, review Adding an EIM domain to Domain Management.
 - b. If you are not currently connected to the EIM domain in which you want to work, review Connecting to the EIM domain controller.
3. Expand the EIM domain to which you are connected.
4. Right-click **User Registries**, select **Add Registry**, then select **Group**.
5. In the **Add Group Registry** dialog, provide information about the group registry definition, as follows:
 - a. A name for the group registry definition.

- b. Select **Group registry members are case sensitive** if all members of the group registry definition are case sensitive.
 - c. A description of the group registry definition.
 - d. One or more aliases for the group registry definition, if necessary.
6. Click **Help**, if necessary, to determine what information to provide for each field.
7. Click **OK** to save the information and add the registry definition to the EIM domain.

Adding an alias to a registry definition

You, or an application developer, may want to specify additional distinguishing information for a registry definition. You can do this by creating an alias for the registry definition. You, or others, can then use the alias for the registry definition to better distinguish one user registry from another.

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

To add an alias to a registry definition, you must be connected to the EIM domain in which you want to work and you must have EIM access control at one of these levels:

- Registry administrator.
- Administrator for selected registries (for the registry that you are modifying).
- EIM administrator.

To add an alias to an EIM registry definition, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under Domain Management, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.
3. Expand the EIM domain to which you are now connected.
4. Click **User Registries** to display the list of registry definitions within the domain.

Note: If you have Administrator for selected registries access control, the list contains only those registry definitions to which you are specifically authorized.

5. Right-click the registry definition for which you want to add an alias and select **Properties**.
6. Select the **Aliases** page and specify the name and type of alias you want to add.

Note: You can specify an alias type that is not included in the list of types.

7. Click **Help**, if necessary, to determine what information to specify for each field.
8. Click **Add**.
9. Click **OK** to save your changes to the registry definition.

Defining a private user registry type in EIM

When you create an Enterprise Identity Mapping (EIM) registry definition you can specify one of a number of predefined user registry types to represent an actual user registry that exists on a system within the enterprise.

The predefined registry definition types cover most operating system user registries, you may need to create a registry definition for which EIM does not include a predefined registry type. You have two

options in this situation. You can either use an existing registry definition which matches the characteristics of your user registry or you can define a private user registry type.





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

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

There are two ways of obtaining OIDs:

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

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

- American National Standards Institute (ANSI) is the registration authority for the United States for organization names under the global registration process established by International Standards Organization (ISO) and International Telecommunication Union (ITU). A fact sheet in Microsoft Word format about applying for a Registered Application Provider Identifier (RID) is located at the ANSI Public Document Library Web site <http://public.ansi.org/ansionline/Documents/> . You can find the fact sheet by selecting **Other Services > Registration Programs**. 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) to create a new OID arc; for example: 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.wssn.net/WSSN/listings/links_national.html . The information includes postal address and electronic mail. In many cases, a Web site is specified as well.
- The Internet Assigned Numbers Authority (IANA) assigns private enterprise numbers, which are OIDs, in the arc 1.3.6.1.4.1. IANA has assigned arcs to over 7500 companies to date. The application page is located at <http://www.iana.org/cgi-bin/enterprise.pl> , under Private Enterprise Numbers. The IANA usually takes about one week. An OID from IANA is free. IANA will assign a number (NEWNUM) so that the new OID arc will be 1.3.6.1.4.1.NEWNUM.
- The U.S. Federal Government maintains the Computer Security Objects Registry (CSOR). The CSOR is the naming authority for the arc 2.16.840.1.101.3, and is currently registering objects for security labels, cryptographic algorithms, and certificate policies. The certificate policy OIDs are defined in the arc 2.16.840.1.101.3.2.1. The CSOR provides policy OIDs to agencies of the U.S. Federal Government. For more information about the CSOR, review <http://www.csrc.nist.gov/pki/CSOR/csor.html> .

Related concepts

“EIM registry definitions” on page 11

An Enterprise Identity Mapping (EIM) registry definition is an entry within EIM that you create to represent an actual user registry that exists on a system within the enterprise. A user registry operates like a directory and contains a list of valid user identities for a particular system or application.

Enabling mapping lookup support and the use of policy associations for a target registry

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as a means of creating many-to-one mappings in situations where associations between user identities and an EIM identifier do not exist. You can use a policy association to map a source set of multiple user identities (rather than a single user identity) to a single target user identity in a specified target user registry.

Before you can use policy associations, however, you must first ensure that you enable mapping lookups using policy associations for the domain. You must also enable one or two settings for each registry:

- **Enable mapping lookups for registry** Select this option to ensure that the registry can participate in EIM mapping lookup operations, regardless of whether the registry has any policy associations defined for it.
- **Use policy associations** Select this option to allow this registry to be the target registry of a policy association and ensure that it can participate in EIM mapping lookup operations.

If you do not enable mapping lookups for the registry, the registry cannot participate in EIM mapping lookup operations at all. If you do not specify that the registry use policy associations, then EIM mapping lookup operations ignore any policy associations for the registry when the registry is the target of the operation.

To enable mapping lookups to use policy associations for a target registry, you must be connected to the EIM domain in which you want to work and you must have “EIM access control” on page 36 at one of these levels:

- EIM administrator
- Registry administrator
- Administrator for selected registries (for the registry that you want to enable)

To enable mapping lookup support in general, and to allow the use policy associations in specific, for a target registry, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Select **User Registries** to display a list of registry definitions for the domain.

Note: If you have Administrator for selected registries access control, the list contains only those registry definitions to which you are specifically authorized.

4. Right-click the registry definition for which you want to enable mapping policy support for policy associations and select **Mapping Policy**
5. On the **General** page, select **Enable mapping lookups for registry**. Selecting this option allows the registry to participate in EIM mapping lookup operations. If this option is not selected, a lookup operation cannot return data for the registry, regardless of whether the registry is the source registry or the target registry in a lookup operation.
6. Select **Use policy associations**. Selecting this option allows lookup operations to use policy associations as the basis for returning data when the registry is the target of the lookup operation.

7. Click **OK** to save your changes.

Note: Before any registry can use policy associations, you must also ensure that you enable policy associations for a domain.

Related concepts

“EIM mapping policy support and enablement” on page 35

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain. You can use policy associations instead of, or in combination with, identifier associations.

Deleting a registry definition

When you delete a registry definition from an Enterprise Identity Mapping (EIM) domain you do not affect the user registry to which the registry definition refers, but that user registry can no longer participate in the EIM domain.

You need to consider these things when you delete a registry definition:

- When you delete a registry definition, you lose all associations for that user registry. If you redefine the registry to the domain, you must create any needed associations again.
- When you delete an X.509 registry definition, you also lose all certificate filters defined for that registry. If you redefine the X.509 registry to the domain, you must create any needed certificate filters again.
- You can not delete a system registry definition if there are application registry definitions that specify the system registry definition as a parent registry.

To delete a registry definition, you must be connected to the EIM domain in which you want to work and you must have EIM administrator access control.

To delete an EIM registry definition, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review **Connect** to the EIM domain controller.
3. Expand the EIM domain to which you are connected.
4. Click **User Registries** to display a list of registry definitions for the domain.

Note: If you have Administrator for selected registries access control, the list contains only those registry definitions to which you are specifically authorized.

5. Right-click the user registry that you want to delete and select **Delete**.
6. Click **Yes** on the **Confirmation** dialog to delete the registry definition.

Removing an alias from a registry definition

To remove an alias from an Enterprise Identity Mapping (EIM) registry definition, you must be connected to the EIM domain in which you want to work and you must have EIM access control as Registry administrator, Administrator for selected registries, or EIM administrator.

To remove an alias to an EIM registry definition, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.

- If you are not currently connected to the EIM domain in which you want to work, review **Connect** to the EIM domain controller.
3. Expand the EIM domain to which you are connected.
 4. Click **User Registries** to display a list of registry definitions for the domain.

Note: If you have Administrator for selected registries access control, the list contains only those registry definitions to which you are specifically authorized.

5. Right-click a registry definition and select **Properties**.
6. Select the **Alias** page.
7. Select the alias you want to remove and click **Remove**.
8. Click **OK** to save the changes.

Adding a member to a group registry definition

To add a member to a group registry definition, you must be connected to the EIM domain in which you want to work and you must have EIM access control as EIM administrator, Registry administrator, Administrator for selected registries (for both the group registry definition to which you want to add the member and to the individual member that you want to add).

To add a member to a group registry definition, complete these steps:

1. **Expand Network → Enterprise Identity Mapping → Domain Management.**
2. Select the EIM domain in which you want to work.
 - a. If the EIM domain you want to work with is not listed under Domain Management, review Adding an EIM domain to Domain Management.
 - b. If you are not currently connected to the EIM domain in which you want to work, review Connecting to the EIM domain controller.
3. Expand the EIM domain to which you are connected.
4. Click **User Registries** to display the list of registry definitions in the domain.
5. Right-click the group registry definition to which you want to add a member and select **Properties**.
6. Select the **Members** page and click **Add**.
7. In the **Add EIM Group Registry member dialog**, select one or more registry definitions and click **OK**. The contents of the list varies based on the type of EIM access control that you have and is restricted to registry definitions with the same case sensitivity as other members of the group.
8. Click **OK** to exit.

Managing Enterprise Identity Mapping identifiers

Use this information to learn how to create and manage Enterprise Identity Mapping (EIM) identifiers for a domain.

Creating and using EIM identifiers that represent the users in your network can be very useful for helping you track which person owns a particular user identity. Users within the enterprise are nearly always changing, with some coming, some going, and others moving between areas. These changes add to the ongoing administrative problem of keeping track of users' identities and passwords for systems and applications in the network. Additionally, password management takes a large amount of time in an enterprise. By creating Enterprise Identity Mapping (EIM) identifiers and associating them with the user identities for each user, you can make the process of tracking who owns a particular user identity. Doing so can also make password management much easier.

Implementing a single sign-on environment makes the process of managing user identities easier for users as well, especially when they move to another department or area within the enterprise. Single sign-on enablement can eliminate the need for these users to remember new user names and passwords for new systems.

Note: How you create and use EIM identifiers depends on the needs of your organization. To learn more, review “Developing an EIM identifier naming plan” on page 61.

You can manage EIM identifiers for any EIM domain that is available under the **Domain Management** folder. You can perform any of the following tasks to manage the EIM identifiers in an EIM domain:

Related information

Single sign-on

Creating an EIM identifier

To create an EIM identifier, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM access control as either Identifier administrator or EIM administrator.

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

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.
3. Expand the EIM domain to which you are connected.
4. Right-click **Identifiers**, and select **New identifier**.
5. In the **New EIM Identifier** dialog, provide information about the EIM identifier, as follows:
 - a. A name for the identifier.
 - b. Whether to have the system generate a unique name, if necessary.
 - c. A description of the identifier.
 - d. One or more aliases for the identifier, if necessary.
6. Click **Help**, if necessary, to determine what information to specify for each field.
7. After you enter the required information, click **OK** to create the EIM identifier.

Note: If you create a large number of EIM identifiers, it sometimes takes a long time before the list of identifiers displays when you expand the **Identifiers** folder. To improve performance when you have a large number of EIM identifiers, review “Customizing the EIM identifiers view” on page 98.

Adding an alias to an EIM identifier

You may want to create an alias to provide additional distinguishing information for an EIM identifier. Aliases can aid in locating a specific Enterprise Identity Mapping (EIM) identifier when performing an EIM lookup operation. For example, aliases can be useful in situations where someone’s legal name is different from the name that person is known as.

EIM identifier names must be unique within an EIM domain. Aliases can help address situations where using unique identifier names can be difficult. For example, different individuals within an enterprise can share the same name, which can be confusing if you are using proper names as EIM identifiers. For example, if you have two users named John J. Johnson, you could create an alias of John Joseph Johnson for one and an alias of John Jeffrey Johnson to make it easier to distinguish the identity of each user. The additional aliases might contain each user’s employee number, department number, job title, or other distinguishing attribute.

To add an alias to an EIM identifier, you must be connected to the EIM domain in which you want to work and you must have “EIM access control” on page 36 at one of these levels:

- EIM administrator.

- Identifier administrator.

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

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.
3. Expand the EIM domain to which you are connected.
4. Click **Identifiers** to display, in the right pane, a list of EIM identifiers available in the domain.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, review “Customizing the EIM identifiers view” on page 98.

5. Right-click the EIM identifier for which you want to add an alias and select **Properties**.
6. In the **Alias** field, specify the name of the alias you want to add to this EIM identifier, and click **Add**.
7. Click **OK** to save your changes to the EIM identifier.

Removing an alias from an EIM identifier

To remove an alias from an Enterprise Identity Mapping (EIM) identifier, you must be connected to the EIM domain in which you want to work and you must have EIM access control as either Identifier administrator or EIM administrator.

To remove an alias from an EIM identifier, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.
3. Expand the EIM domain to which you are connected.
4. Click **Identifiers** to display, in the right pane, a list of EIM identifiers available in the domain.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, review “Customizing the EIM identifiers view” on page 98.

5. Right-click the EIM identifier for which you want to add an alias and select **Properties**.
6. Select the alias you want to remove and click **Remove**.
7. Click **OK** to save your changes.

Deleting an EIM identifier

To delete an EIM identifier, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM administrator access control.

To delete an EIM identifier, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.

- If you are not currently connected to the EIM domain in which you want to work, review **Connect to the EIM domain controller**.
3. Expand the EIM domain to which you are now connected.
 4. Click **Identifiers**.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, you can “Customizing the EIM identifiers view.”

5. Select the EIM identifier you want to delete. To delete multiple identifiers, press the **Ctrl** key as you select EIM identifiers.
6. Right-click the selected EIM identifiers and select **Delete**.
7. On the **Delete Confirmation** dialog, click **Yes** to delete the selected EIM identifiers.

Customizing the EIM identifiers view

Sometimes when you attempt to expand the Identifiers folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of Enterprise Identity Mapping (EIM) identifiers in the domain, you can customize the view for the Identifiers folder.

To customize the **Identifiers** folder view, follow these steps:

1. Expand **Network** —> **Enterprise Identity Mapping** —> **Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.
3. Right-click the **Identifiers** folder and select **Customize this View**.
4. Specify the criteria that you want to use to display EIM identifiers in the domain. To narrow the number of EIM identifiers displayed, specify the characters that you want to use for sorting the identifiers. You can specify one or more wildcard characters (*) in the identifier name. For example, you could enter *JOHNSON* as your sorting criteria in the **Identifiers** field. The results will return all the EIM identifiers where the character string JOHNSON is defined as part of the EIM identifier name and will also return the EIM identifiers where the character string JOHNSON is defined as part of the alias for an EIM identifier.
5. Click **OK** to save your changes.

Managing EIM associations

EIM allows you to create and manage two kinds of associations, which define direct or indirect relationships between user identities: identifier associations and policy associations. EIM allows you to create and manage identifier associations between EIM identifiers and their user identities, which allow you to define indirect, but specific, individual relationships between user identities.

EIM also allows you to create policy associations to describe a relationship between multiple user identities in one or more registries and an individual target user identity in another registry. Policy associations use EIM mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier. Because both types of associations define relationships between user identities in an enterprise, managing associations is an important element in managing EIM.

Maintaining the associations within a domain is key to simplifying the administrative tasks required to keep track of which users have accounts on the various systems in the network. You need to keep identifier associations and policy associations current when you implement a secure single sign-on network.

You can perform the following management tasks for associations:

Creating EIM associations

There are two different types of EIM associations you can create. You can create either an identifier association or a policy association.

You can create an identifier association to indirectly define a relationship between two user identities that a single individual uses. An identifier association describes a relationship between an EIM identifier and a user identity in a user registry. Identifier associations allow you to create one-to-one mappings between an EIM identifier and each of the various user identities that are related to the user that the EIM identifier represents.

You can create a policy association to directly define a relationship between multiple user identities in one or more registries and an individual target user identity in another registry. Policy associations use EIM mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier. Policy associations allow you to quickly create a large number of mappings between related user identities in different user registries.

Whether you choose to create identifier associations, create policy associations, or use a mix of both methods depends on your EIM implementation needs.

Related concepts

“Developing an identity mapping plan” on page 58

A critical part of the initial Enterprise Identity Mapping (EIM) implementation planning process requires that you determine how you want to use identity mapping in your enterprise.

Creating EIM identifier association:

Identifier associations define a relationship between an Enterprise Identity Mapping (EIM) identifier and a user identity in your enterprise for the person or entity to whom the EIM identifier refers.

You can create three types of identifier association: target, source, and administrative. To prevent potential problems with associations and how they map identities, review “Developing an identity mapping plan” on page 58.

To create an identifier association, you must be connected to the EIM domain in which you want to work and you must have the EIM access control required by the type of association that you want to create.

To create a source or an administrative association, you must have EIM access control at one of these levels:

- Identifier administrator.
- EIM administrator.

To create a target association, you must have EIM access control at one of these levels:

- Registry administrator.
- Administrator for selected registries (for the registry definition that refers to the user registry that contains the target user identity)
- EIM administrator.

To create an identifier association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review “Connecting to an EIM domain” on page 85.

3. Expand the EIM domain to which you are now connected.
4. Click **Identifiers** to display the list of EIM identifiers for the domain.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, review “Customizing the EIM identifiers view” on page 98.

5. Right-click the EIM identifier for which you want to create an association and select **Properties...**
6. Select the **Associations** page and click **Add...**
7. In the **Add Association** dialog, provide information to define the association, as follows:
 - The name of the registry that contains the user identity that you want to associate with the EIM identifier. Specify the exact name of an existing registry definition or browse to select one.
 - The name of the user identity that you want to associate with the EIM identifier.
 - The type of association. You can create one of three different types of associations:
 - Administrative
 - Source
 - Target
8. Click **Help**, if necessary, to determine what information to specify for each field.
9. Optional. For a target association, click **Advanced...** to display the **Add Association - Advanced** dialog. Specify lookup information for the target user identity and click **OK** to return to the **Add Association** dialog.
10. After you provide the required information, click **OK** to create the association.

Creating a policy association:

A policy association provides a means to directly define a relationship between multiple user identities in one or more registries and an individual target user identity in another registry.

Policy associations use Enterprise Identity Mapping (EIM) mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier. Because you can use policy associations in a variety of overlapping ways, you need to have a thorough understanding of EIM mapping policy support before you create and use policy associations. Also, to prevent potential problems with associations and how they map identities, you need to develop an overall identity mapping plan for your enterprise before you begin defining associations.

Whether you choose to create identifier associations, create policy associations, or use a mix of both methods depends on your EIM implementation needs.

How you create a policy association varies depending on the type of policy association. To learn more about how to create a policy association, see:

Related concepts

“Managing Enterprise Identity Mapping registry definitions” on page 89

To have user registries and the user identities that they contain participate in an EIM domain you must create registry definitions for them. You can then manage how the user registries and their user identities participate in EIM by managing these EIM registry definitions.

“EIM mapping policy support and enablement” on page 35

Enterprise Identity Mapping (EIM) mapping policy support allows you to use policy associations as well as specific identifier associations in an EIM domain. You can use policy associations instead of, or in combination with, identifier associations.

“Developing an identity mapping plan” on page 58

A critical part of the initial Enterprise Identity Mapping (EIM) implementation planning process requires that you determine how you want to use identity mapping in your enterprise.

Creating a default domain policy association:

To create a default domain policy association, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM access control to either EIM administrator or Registry administrator.

A policy association describes a relationship between multiple user identities and a single user identity in a target user registry. You can use a policy association to describe a relationship between a source set of multiple user identities and a single target user identity in a specified target user registry. Policy associations use EIM mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier.

Note: Because you can use policy associations in a variety of overlapping ways, you need to have a thorough understanding of EIM mapping policy support before you create and use policy associations. Also, to prevent potential problems with associations and how they map identities, you need to develop an overall identity mapping plan for your enterprise before you begin defining associations.

In a default domain policy association, all users in the domain are the source of the policy association and are mapped to a single target registry and target user. You can define a default domain policy association for each registry in the domain. If two or more domain policy associations refer to the same target registry, you can define unique lookup information for each of these policy associations to ensure that mapping lookup operations can distinguish between them. Otherwise, mapping lookup operations may return multiple target user identities. As a result of these ambiguous results, applications that rely on EIM may not be able to determine the exact target identity to use.

To create a default domain policy association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Right-click the EIM domain in which you want to work and select **Mapping Policy**
 - If the EIM domain you want to work with is not listed under **Domain Management**, see “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, see Connect to the EIM domain controller.
3. Select **Enable mapping lookups using policy associations for domain** on the General page.
4. Select the **Domain** page and click **Add**.
5. In the **Add Default Domain Policy Association** dialog, specify the following required information:
 - The registry definition name of the **Target registry** for the policy association.
 - The user identity name of the **Target user** for the policy association.
6. Click **Help**, if necessary, for more details about how to complete this and subsequent dialogs.
7. Optional. Click **Advanced** to display the **Add Association - Advanced** dialog. Specify **Lookup information** for the policy association and click **OK** to return to the **Add Default Domain Policy Association** dialog.

Note: If two or more default domain policy associations refer to the same target registry, you must define unique lookup information for each of the target user identities in these policy associations. By defining lookup information for each target user identity in this situation, you ensure that mapping lookup operations can distinguish between them. Otherwise, mapping lookup operations may return multiple target user identities. As a result of these ambiguous results, applications that rely on EIM may not be able to determine the exact target identity to use.

8. Click **OK** to create the new policy association and return to the **Domain** page. The new policy association now displays in the **Default policy associations** table.
9. Verify that the new policy association is enabled for the target registry.

10. Click **OK** to save your changes and exit the **Mapping Policy** dialog.

Note: Verify that mapping policy support and the use of policy associations for target user registry are properly enabled. If it is not enabled, the policy association can not take effect.

Creating a default registry policy association:

To create a default registry policy association, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM access control as either a Registry administrator or EIM administrator.

A policy association describes a relationship between multiple user identities and a single user identity in a target user registry. You can use a policy association to describe a relationship between a source set of multiple user identities and a single target user identity in a specified target user registry. Policy associations use EIM mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier.

Note: Because you can use policy associations in a variety of overlapping ways, you need to have a thorough understanding of EIM mapping policy support before you create and use policy associations. Also, to prevent potential problems with associations and how they map identities, you need to develop an overall identity mapping plan for your enterprise before you begin defining associations.

In a default registry policy association, all users in a single registry are the source of the policy association and are mapped to a single target registry and target user. When you enable the default registry policy association for the target registry, the policy association ensures that these source user identities can all be mapped to a single specified target registry and target user.

To create a default registry policy association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Select **Enable mapping lookups using policy associations for domain** on the General page.
4. Select **Enable mapping lookups using policy associations for domain** on the General page.
5. In the **Add Default Registry Policy Association** dialog, specify the following required information:
 - The registry definition name of the **Source registry** for the policy association.
 - The registry definition name of the **Target registry** for the policy association.
 - The user identity name of the **Target user** for the policy association.
6. Click **Help**, if necessary, for more details about how to complete this and subsequent dialogs.
7. Optional. Click **Advanced** to display the **Add Association - Advanced** dialog. Specify **lookup information** for the policy association and click **OK** to return to the **Add Default Registry Policy Association** dialog. If two or more policy associations with the same source registry refer to the same target registry, you must define unique lookup information for each of the target user identities in these policy associations. By defining lookup information for each target user identity in this situation, you ensure that mapping lookup operations can distinguish between them. Otherwise, mapping lookup operations may return multiple target user identities. As a result of these ambiguous results, applications that rely on EIM may not be able to determine the exact target identity to use.
8. Click **OK** to create the new policy association and return to the **Registry** page. The new default registry policy association now displays in **Default policy associations**.

9. Verify that the new policy association is enabled for the target registry.
10. Click **OK** to save your changes and exit the **Mapping Policy** dialog.

Note: Verify that mapping policy support and the use of policy associations for target user registry are properly enabled. If it is not enabled, the policy association can not take effect.

Creating a certificate filter policy association:

To create a certificate filter policy association, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM access control as either a Registry administrator or EIM administrator.

A policy association describes a relationship between a source set of multiple user identities and a single target user identity in a specified target user registry. Policy associations use EIM mapping policy support to create many-to-one mappings between user identities without involving an EIM identifier.

Note: Because you can use policy associations in a variety of overlapping ways, you need to have a thorough understanding of EIM mapping policy support before you create and use policy associations. Also, to prevent potential problems with associations and how they map identities, you need to develop an overall identity mapping plan for your enterprise before you begin defining associations.

In a certificate filter policy association, you specify a set of certificates in a single X.509 registry as the source of the policy association. These certificates are mapped to a single target registry and target user that you specify. Unlike a default registry policy association in which all users in a single registry are the source of the policy association, the scope of a certificate filter policy association is more flexible. You can specify a subset of certificates in the registry as the source. The certificate filter that you specify for the policy association determines its scope.

Note: Create and use a default registry policy association when you want to map all certificates in an X.509 user registry to a single target user identity.

The certificate filter controls how a certificate filter policy association maps one source set of user identities, in this case digital certificates, to a specific target user identity. Therefore, the certificate filter that you want to use must exist before you can create a certificate filter policy association.

Before you can create a certificate filter policy association, you must first create a certificate filter to use as the basis of the policy association.

To create a certificate filter policy association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Right-click the EIM domain in which you want to work and select **Mapping Policy**
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Select **Enable mapping lookups using policy associations for domain** on the General page.
4. Select the **Certificate Filter** page and click **Add** to display the **Add Certificate Filter Policy Association** dialog.
5. Click **Help**, if necessary, for more details about how to complete this and subsequent dialogs.
6. Specify the following required information to define the policy association:
 - a. Enter the registry definition name of an X.509 user registry to use as the **Source X.509 Registry** for the policy association. Or, click **Browse** to select one from a list of registry definitions for the domain

- b. Click **Select** to display the **Select Certificate Filter** dialog and select an existing certificate filter to use as the basis for the new certificate filter policy association.

Note: You **must** use an existing certificate filter. If the certificate filter that you want to use is not listed, click **Add** to create a new certificate filter.

- c. Specify the registry definition name of the **Target registry** or click **Browse** to select one from a list of existing registry definitions for the domain.
- d. Specify the name of the **Target user** to which to map all certificates in the **Source X.509 Registry** that match the certificate filter. Or, click **Browse** to select one from a list of users known to the domain.
- e. Optional. Click **Advanced** to display the **Add Association - Advanced** dialog. Specify **Lookup information** for target user identity and click **OK** to return to the **Add Certificate Filter Policy Association** dialog.

Note: If two or more policy associations with the same source X.509 registry and the same certificate filter criteria refer to the same target registry, you must define unique lookup information for the target user identities in each of these policy associations. By defining lookup information for each target user identity in this situation, you ensure that mapping lookup operations can distinguish between them. Otherwise, mapping lookup operations may return multiple target user identities. As a result of these ambiguous results, applications that rely on EIM may not be able to determine the exact target identity to use.

7. Click **OK** to create the certificate filter policy association and return to the **Certificate Filter** page. The new policy association displays in the list.
8. Verify that the new policy association is enabled for the target registry.
9. Click **OK** to save your changes and exit the **Mapping Policy** dialog.

Note: Verify that mapping policy support and the use of policy associations for target user registry are properly enabled. If it is not enabled, the policy association can not take effect.

Creating a certificate filter:

A certificate filter defines a set of similar distinguished name certificate attributes for a group of user certificates in an X.509 source user registry. You can use the certificate filter as the basis of a certificate filter policy association.

The certificate filter in a policy association determines which certificates in the specified source X.509 registry to map to the specified target user. Those certificates that have Subject DN and Issuer DN information that satisfy the criteria of the filter are mapped to the specified target user during Enterprise Identity Mapping (EIM) mapping lookup operations.

To create a certificate filter, you must be connected to the EIM domain in which you want to work and you must have "EIM access control" on page 36 at one of these levels:

- EIM administrator
- Registry administrator
- Administrator for selected registries (for the registry definition that refers to the X.509 user registry for which you want to create the certificate filter)

You create a certificate filter based on specific distinguished name (DN) information from a digital certificate. The DN information that you specify can be either the subject distinguished name, which designates the owner of the certificate, or the issuer distinguished name, which designates the issuer of the certificate. You can specify either full or partial DN information for a certificate filter.

When you add the certificate filter to a certificate filter policy association, the certificate filter determines which certificates in an X.509 registry are mapped to the target user identity specified by the policy

association. When a digital certificate is the source user identity in an EIM mapping lookup operation (after the requesting application uses the `eimFormatUserIdentity()` EIM API to format the user identity name) and the certificate filter policy association applies, EIM compares the DN information in the certificate against the DN or partial DN information specified in the filter. If the DN information in the certificate matches the filter, EIM returns the target user identity that the certificate filter policy association specified.

When you create the certificate filter you can supply the required distinguished name information in one of three ways:

- You can enter a specific certificate's full or partial DNs for the **Subject DN**, the **Issuer DN**, or both.
- You can copy information from a specific certificate into your clipboard and use it to generate the a list of certificate filter candidates based on the distinguished name information in the certificate. You can then select which DNs to use for the certificate filter.

Note: If you want to generate the required distinguished name information to create a certificate filter, you must copy the certificate's information into your clipboard prior to performing this task. Also, the certificate must be base64 encoded format. For more detailed information regarding methods of obtaining a certificate in the proper format, see Certificate filter.

- You can generate a list of certificate filter candidates based on the distinguished name information from a digital certificate for which there is an existing source association with an EIM identifier. You can then select which DNs to use for the certificate filter.

To create a certificate filter to use as the basis for a certificate filter policy association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Right-click the EIM domain in which you want to work and select **Mapping Policy**
 - If the EIM domain you want to work with is not listed under **Domain Management**, see "Adding an EIM domain to the Domain Management folder" on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, see Connect to the EIM domain controller.
3. Select the **Certificate Filter** page and click **Certificate Filters** to display the **Certificate Filters** dialog.

Note: If you click **Certificate Filters** without selecting a policy association, then the **Browse EIM Registries** dialog displays. This dialog allows you to select an X.509 registry from a list of X.509 registry definitions in the domain for which you want to view certificate filters. The contents of the list varies based on the type of EIM access control that you have.

4. Click **Add** to display the **Add Certificate Filter** dialog.
5. In the **Add Certificate Filter** dialog, you must select whether to add a single certificate filter or to generate a certificate filter based on a specific digital certificate. Click **Help**, if necessary, for more details about how to complete this and subsequent dialogs.
 - a. If you select **Add a single certificate filter**, you can enter specific full or partial **Subject DN**, full or partial **Issuer DN** information, or both. Click **OK** to create the certificate filter and return to the **Certificate Filters** dialog. The filter now appears in the list.
 - b. If you select **Generate certificate filter from a digital certificate**, click **OK** to display the **Generate Certificate Filters** dialog.
 - 1) Paste the base64 encoded version of the certificate information that you earlier copied to your clipboard into the **Certificate information** field.
 - 2) Click **OK** to generate a list of potential certificate filters based on the certificate's **Subject DN** and **Issuer DN**.
 - 3) From the **Browse Certificate Filters** dialog, select one or more of these certificate filters. Click **OK** to return to the **Select Certificate Filters** dialog where the selected certificate filters now display.

- c. If you select **Generate certificate filter from a source association for an X.509 user**, click **OK** to display the **Generate Certificate Filters** dialog. This dialog displays a list of X.509 user identities that have a source association with an EIM identifier in the domain.
 - 1) Select the X.509 user identity whose digital certificate you want to use to generate one or more certificate filter candidates and click **OK**.
 - 2) Click **OK** to generate a list of potential certificate filters based on the certificate's **Subject DN** and **Issuer DN**.
 - 3) From the **Browse Certificate Filters** dialog, select one or more of these potential certificate filters. Click **OK** to return to the **Select Certificate Filters** dialog where the selected certificate filters now display.

You can now use the new certificate filter as the basis for creating a certificate filter policy association.

Adding lookup information to a target user identity

Lookup information is optional unique identifying data for the target user identity defined in an association. This association can be either an identifier target association or a policy association.

Lookup information is necessary only when a mapping lookup operation can return more than one target user identity. This situation can create problems for Enterprise Identity Mapping (EIM) enabled applications, including i5/OS applications and products, that are not designed to handle these ambiguous results.

When necessary, you can add unique lookup information for each target user identity to provide more detailed identifying information to further describe each target user identity. If you define lookup information for a target user identity, this lookup information must be provided to the mapping lookup operation to ensure that the operation can return a unique target user identity. Otherwise, applications that rely on EIM may not be able to determine the exact target identity to use.

Note: If you do not want EIM lookup operations to be able to return more than one target user identity, then you should correct your EIM associations configuration instead of using looking information to resolve the situation. Review “Troubleshooting EIM mapping problems” on page 117 for more detailed information.

How you add lookup information to further define a target user identity varies based on whether the target user identity is defined in an identifier association or a target association. Regardless of the method that you use to add the lookup information, the information that you specify is tied to the target user identity, not the identifier associations or policy associations in which that user identity is found.

Add lookup information to a target user identity in an identifier association:

To add lookup information to the target user identity in an identifier association, you must be connected to the EIM domain in which you want to work and you must have “EIM access control” on page 36 at one of these levels:

- Registry administrator.
- Administrator for selected registries (for the registry definition that refers to the user registry that contains the target user identity).
- EIM administrator.

To add lookup information to the target user identity in an identifier association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.

- If you are not currently connected to the EIM domain in which you want to work, review **Connect** to the EIM domain controller.
- 3. Expand the EIM domain to which you are connected.
- 4. Click **Identifiers** to display the list of EIM identifiers for the domain.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, you can customize the **Identifiers** folder view by restricting the search value used for displaying identifiers. Right-click **Identifiers**, select **Customize this view** > **Include**, and specify the display criteria to use for generating the list of EIM identifiers to include in the view.

5. Right-click an EIM identifier and select **Properties**.
6. Select the **Associations** page, select the target association to which you want to add lookup information, and click **Details**. Click **Help**, if necessary, to determine what information to specify for each field.
7. In the **Association - Details** dialog, specify the **Lookup information** that you want to use to further identify the target user identity in this association and click **Add**.
8. Repeat this step for each lookup information entry that you want to add to the association.
9. Click **OK** to save your changes and to return to the **Association - Details** dialog.
10. Click **OK** to exit.

Add lookup information to a target user identity in a policy association:

To add lookup information to the target user identity in a policy association, you must be connected to the EIM domain in which you want to work and you must have “EIM access control” on page 36 at one of these levels:

- Registry administrator.
- Administrator for selected registries (for the registry definition that refers to the user registry that contains the target user identity (ID)).
- EIM administrator.

To add lookup information to the target user identity in a policy association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review **Connect** to the EIM domain controller.
3. In the **Mapping Policy** dialog, use the pages to view policy associations for the domain.
4. Find and select the policy association for the target registry that contains the target user identity for which you want to add lookup information.
5. Click **Details** to display the appropriate **Policy Association - Details** dialog for the type of policy association that you selected. Click **Help**, if necessary, to determine what information to specify for each field.
6. Specify the **Lookup information** that you want to use to further identify the target user identity in this policy association and click **Add**. Repeat this step for each lookup information entry that you want to add to the association.
7. Click **OK** to save your changes and to return to the original **Policy Association - Details** dialog.
8. Click **OK** to exit.

Removing lookup information from a target user identity

Lookup information is optional unique identifying data for the target user identity defined in an association. This association can be either an identifier target association or a policy association.

Lookup information is necessary only when a mapping lookup operation can return more than one target user identity. This situation can create problems for Enterprise Identity Mapping (EIM) enabled applications, including i5/OS applications and products, that are not designed to handle these ambiguous results.

This lookup information must be provided to the mapping lookup operation to ensure that the operation can return a unique target user identity. However, if previously defined lookup information is no longer necessary, you may want to remove the lookup information so that it no longer needs to be supplied for lookup operations.

How you remove lookup information from a target user identity varies based on whether the target user identity is defined in an identifier association or a target association. Lookup information is tied to the target user identity, not the identifier associations or policy associations in which that user identity is found. Consequently, when you delete the last identifier association or policy association that defines that target user identity, both the user identity and the lookup information are deleted from the EIM domain.

Remove lookup information for a target user identity in an identifier association:

To remove lookup information for the target user identity in an identifier association, you must be connected to the EIM domain in which you want to work and you must have “EIM access control” on page 36 at one of these levels:

- Registry administrator.
- Administrator for selected registries (for the registry definition that refers to the user registry that contains the target user identity).
- EIM administrator.

To remove lookup information for the target user identity in an identifier association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Expand the EIM domain to which you are connected.
4. Click **Identifiers** to display the list of EIM identifiers for the domain.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, you can customize the **Identifiers** folder view by restricting the search value used for displaying identifiers. Right-click **Identifiers**, select **Customize this view > Include**, and specify the display criteria to use for generating the list of EIM identifiers to include in the view.

5. Right-click an EIM identifier and select **Properties**.
6. Select the **Associations** page, select the target association for the user identity for which you want to remove lookup information, and click **Details**.
7. In the **Association - Details** dialog, select the lookup information that you want to remove from the target user identity and click **Remove**.

Note: There is no confirmation prompt when you click **Remove**.

8. Click **OK** to save your changes and to return to the **Association - Details** dialog.
9. Click **OK** to exit.

Remove lookup information for a target user identity in a policy association:

To remove lookup information for the target user identity in a policy association, you must be connected to the EIM domain in which you want to work and you must have “EIM access control” on page 36 at one of these levels:

- Registry administrator.
- Administrator for selected registries (for the registry definition that refers to the user registry that contains the target user identity (ID)).
- EIM administrator.

To remove lookup information for the target user identity in a policy association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. In the **Mapping Policy** dialog, use the pages to view policy associations for the domain.
4. Find and select the policy association for the target registry that contains the target user identity for which you want to remove lookup information.
5. Click **Details** to display the appropriate **Policy Association - Details** dialog for the type of policy association that you selected.
6. Select the lookup information that you want to remove from the target user identity and click **Remove**.

Note: There is no confirmation prompt when you click **Remove**.

7. Click **OK** to save your changes and to return to the original **Policy Association - Details** dialog.
8. Click **OK** to exit.

Displaying all identifier associations for an EIM identifier

To display all associations for an Enterprise Identity Mapping (EIM) identifier you must be connected to the EIM domain in which you want to work and you must have some level of EIM access control to perform this task.

You can view all associations with any access control level except Administrator for selected registries access control. This access control level allows you to list and view only those associations to registries for which you have explicit authority, unless you also have EIM mapping lookup operations access control.

To display all the associations between an EIM identifier and the user identities (IDs) for which associations have been defined for the EIM identifier, complete these steps:

To display the associations for an identifier, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.

- If you are not currently connected to the EIM domain in which you want to work, review **Connect** to the EIM domain controller.
3. Expand the EIM domain to which you are connected.
 4. Click **Identifiers** to display the list of EIM identifiers for the domain.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, you can customize the **Identifiers** folder view by restricting the search value used for displaying identifiers. Right-click **Identifiers**, select **Customize this view** > **Include**, and specify the display criteria to use for generating the list of EIM identifiers to include in the view.

5. Select an EIM identifier, right-click the EIM identifier, and select **Properties**.
6. Select the **Associations** page to display a list of associated user identities for the selected EIM identifier.
7. Click **OK** to finish.

Displaying all policy associations for a domain

To display all policy associations defined for a domain, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have some level of EIM access control to perform this task.

You can view all policy associations with any access control level except Administrator for selected registries access control. This access control level allows you to list and view only those associations to registries for which you have explicit authority. Consequently, with this access control you cannot list or view any default domain policy associations, unless you also have EIM mapping lookup operations access control.

To display all the policy associations for a domain, complete these steps:

1. Expand **Network** > **Enterprise Identity Mapping** > **Domain Management**.
2. Right-click the EIM domain in which you want to work and select **Mapping Policy**
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review **Connect** to the EIM domain controller.
3. Select a page to display the policy associations defined for the domain, as follows:
 - a. Select the **Domain** page to view the default domain policy associations defined for the domain and whether a policy association is enabled at the registry level.
 - b. Select the **Registry** page to view the default registry policy associations defined for the domain. You can also view which source registries and target registries the policy associations affect.
 - c. Select the **Certificate Filter** page to view the certificate filter policy associations defined and enabled at the registry level.
4. Click **OK** to finish.

Displaying all policy associations for a registry definition

To display all policy associations defined for a specific registry, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have some level of EIM access control to perform this task.

You can view all policy associations with any access control level except Administrator for selected registries access control. This access control level allows you to list and view only those associations to registries for which you have explicit authority. Consequently, with this access control you cannot list or view any default domain policy associations, unless you also have EIM mapping lookup operations access control.

To display all the policy associations for a registry definition, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Right-click the registry definition that you want to work with and select **Mapping Policy**.
4. Select a page to display the policy associations defined for the specified registry definition, as follows:
 - Select the **Domain** page to view the default domain policy associations defined for the registry.
 - Select the **Registry** page to view the default registry policy associations defined and enabled for the registry.
 - Select the **Certificate Filter** page to view the certificate filter policy associations defined and enabled for the registry.
5. Click **OK** to finish.

Deleting an identifier association

To delete an identifier association, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have the EIM access control required by the type of association that you want to delete.

To delete a source or an administrative association, you must have EIM access control at one of these levels:

- Identifier administrator.
- EIM administrator.

To delete a target association, you must have EIM access control at one of these levels:

- Registry administrator.
- Administrator for selected registries (for the registry definition that refers to the user registry that contains the target user identity).
- EIM administrator.

To delete an identifier association, complete the following steps.

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Expand the EIM domain to which you are connected.
4. Click **Identifiers** to display the list of EIM identifiers for the domain.

Note: Sometimes when you attempt to expand the **Identifiers** folder, it may take a long time before the list of identifiers displays. To improve performance when you have a large number of EIM identifiers in the domain, you can customize the **Identifiers** folder view by restricting the search criteria used for displaying identifiers. Right-click **Identifiers**, select **Customize this view > Include**, and specify the display criteria to use for generating the list of EIM identifiers to include in the view.

5. Select an EIM identifier, right-click the EIM identifier, and select **Properties**.

6. Select the **Associations** page to display a list of associated user identities for the selected EIM identifier.
7. Select the association that you want to delete and click **Remove** to delete the association.

Note: There is no confirmation prompt when you click **Remove**.

8. Click **OK** to save your changes.

Note: When you remove a target association, any mapping lookup operations to the target registry that rely on the use of the deleted association may fail if other associations (either policy associations or identifier associations) do not exist for the affected target registry.

The only way to define a user identity to EIM is when you specify the user identity as part of creating an association, either an identifier association or a policy association. Consequently, when you delete the last target association for a user identity (whether by removing an individual target association or by removing a policy association), that user identity is no longer defined in EIM. Consequently, the user identity name and any lookup information for that user identity is lost.

Deleting a policy association

To delete a policy association, you must be connected to the Enterprise Identity Mapping (EIM) domain in which you want to work and you must have EIM access control for either Registry administrator or EIM administrator.

To delete a policy association, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Select the appropriate page for the type of policy association that you want to delete.
4. On that page, select the appropriate policy association and click **Remove**.

Note: There is no confirmation prompt when you click **Remove**.

5. Click **OK** to exit the **Mapping Policy** dialog and save your changes.

Note: When you remove a target policy association, any mapping lookup operations to the target registry that rely on the use of the deleted policy association may fail if other associations (either policy associations or identifier associations) do not exist for the affected target registry.

The only way to define a user identity to EIM is when you specify the user identity as part of creating an association, either an identifier association or a policy association. Consequently, when you delete the last target association for a user identity (whether by removing an individual target association or by removing a policy association), that user identity is no longer defined in EIM. Consequently, the user identity name and any lookup information for that user identity is lost.

Related concepts

“Managing Enterprise Identity Mapping registry definitions” on page 89

To have user registries and the user identities that they contain participate in an EIM domain you must create registry definitions for them. You can then manage how the user registries and their user identities participate in EIM by managing these EIM registry definitions.

Managing EIM user access control

An Enterprise Identity Mapping (EIM) user is a user who possesses EIM access control based on their membership in predefined Lightweight Directory Access Protocol (LDAP) user groups. Specifying EIM access control for a user adds that user to a specific LDAP user group.

Each LDAP group has authority to perform various EIM administrative tasks in a domain. Which and what type of administrative tasks, including lookup operations, an EIM user can perform is determined by the access control group to which the EIM user belongs.

Only users with either LDAP administrator access control or EIM administrator access control can add other users to an EIM access control group or change access control settings for other users. Before a user can become a member of an EIM access control group, that user must have an entry in the directory server that acts as the EIM domain controller. Also, only specific types of users can be made a member of an EIM access control group: Kerberos principals, distinguished names, and i5/OS user profiles.

Note: To have the Kerberos principal user type available in EIM, network authentication service must be configured on the system. To have the i5/OS user profile type available in EIM, you must configure a system object suffix on the directory server. This allows the directory server to reference i5/OS system objects, such as i5/OS user profiles.

To manage access control for an existing directory server user or to add an existing directory user to an EIM access control group, complete these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Select the EIM domain in which you want to work.
 - If the EIM domain you want to work with is not listed under **Domain Management**, review “Adding an EIM domain to the Domain Management folder” on page 84.
 - If you are not currently connected to the EIM domain in which you want to work, review Connect to the EIM domain controller.
3. Right-click the EIM domain to which you are connected and select **Access Control**
4. In the **Edit EIM Access Control** dialog, select the **User type** to display the fields required to provide identifying information for the user.
5. Enter the required user information to identify the user for whom you want to manage EIM access control and click **OK** to display the **Edit EIM Access Control** panel. Click **Help**, if necessary, to determine what information to specify for each field.
6. Select one or more **Access Control** groups for the user and click **OK** to add the user to the selected groups. Click **Help** for more detailed information about what authority each group has and to learn about any special requirements.
7. After you provide the required information, click **OK** to save your changes.

Related concepts

“EIM access control” on page 36

An Enterprise Identity Mapping (EIM) user is a user who possesses EIM access control based on their membership in a predefined Lightweight Directory Access Protocol (LDAP) user group for a specific domain.

Related information

Network authentication service

Managing EIM configuration properties

You can manage several different EIM configuration properties for your server. Typically, this is not something you need to do often.

However, there are some situations that require you to make changes to the configuration properties. For example, if your system goes down and you need to re-create your EIM configuration properties you can

either rerun the EIM Configuration wizard or change the properties here. Another example is if you chose not to create the registry definitions for the local registries when you ran the EIM Configuration wizard, you can update the registry definition information here.

The properties that you can change include:

- The EIM domain in which the server is participating.
- The connection information for the EIM domain controller.
- The user identity that the system uses to perform EIM operations on behalf of operating system functions.
- The registry definition names that refer to the actual user registries that the system can use when performing EIM operations on behalf of operation system functions. These registry definition names refer to the local user registries that you can create when you run the EIM Configuration wizard.

Note: If you chose not to create the local registry definition names when you ran the EIM Configuration wizard either because the registries were already defined to the EIM domain or because you chose to define them to the domain later, you need to update the system configuration properties with these registry definition names here. The system needs this registry definition information to perform EIM operations on behalf of operating system functions.

To change EIM configuration properties, you must have these special authorities:

- Security administrator (*SECADM).
- All object (*ALLOBJ).

To change EIM configuration properties for your System i platform, complete these steps:

1. Expand **Network > Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Properties**.
3. Make your changes to the EIM configuration information.
4. Click **Help** to determine what information to specify for each field in the dialog.
5. Click **Verify Configuration** to ensure that all specified information allows the system to successfully establish a connection to the EIM domain controller.
6. Click **OK** to save your changes.

Note: If you have not used the EIM Configuration wizard to create or join a domain, do not attempt to create an EIM configuration by manually specifying configuration properties. By using the wizard to create your basic EIM configuration, you can prevent potential configuration problems because the wizard does more than configure these properties.

Troubleshooting Enterprise Identity Mapping

Use the following troubleshooting methods to solve some of the basic problems you might experience while configuring and using Enterprise Identity Mapping (EIM).

EIM is composed of multiple technologies and many applications and functions. Consequently, problems can occur in a number of areas. The following information describes some common problems and errors that you may encounter when you are using EIM and some suggestions for how to correct these errors and problems.

Related information

Troubleshoot single signon configuration

Troubleshooting domain controller connection problems

A number of factors can contribute to connection problems when trying to connect to the domain controller. Review the following table to determine how to resolve potential domain controller connection problems

Table 27. Common EIM domain controller connection problems and solutions

| Possible problem | Possible solutions |
|---|--|
| You can not connect to the domain controller when using System i Navigator to manage EIM. | <p>Domain controller connection information may be incorrectly specified for the domain that you want to manage. Complete these steps to verify domain connection information:</p> <ul style="list-style-type: none"> Expand Network-->Enterprise Identity Mapping-->Network->Domain Management. Right-click the domain that you want to manage and select Properties. Verify that the name of the Domain controller is correct and that Parent DN, if specified, is correct. Verify that Connection information for the domain controller is correct. Ensure that the Port number is correct. If Use secure connection (SSL or TLS) is selected, the directory server must be configured to use SSL. Click Verify Connection to verify that the you can use the specified information to establish a connection to the domain controller successfully. Verify that the user information in the Connect to Domain Controller panel is correct. |
| The operating system or applications can not connect to the domain control to access EIM data. For example, EIM mapping lookup operations performed on behalf of the system are failing. This may be happening because the EIM configuration is incorrect on the system or systems. | <p>Verify your EIM configuration. Expand Network-->Enterprise Identity Mapping-->Configuration on the system that you are trying to authenticate with. Right-click the Configuration folder and select Properties and verify the following:</p> <ul style="list-style-type: none"> Domain page: <ul style="list-style-type: none"> The domain controller name and port numbers are correct. Click Verify Configuration to verify that the domain controller is active. The local registry name is specified correctly The Kerberos registry name is specified correctly. Verify that Enable EIM operations for this system is selected. System user page: <ul style="list-style-type: none"> The specified user has sufficient EIM access control to perform a mapping lookup, and the password is valid for the user. See the online help to learn more about the different types of user credentials. <p>Note: If you have changed the password for the specified system user in the directory server, you must change the password here as well. If these passwords do not match, then the system user can not perform EIM functions for the operating system and mapping lookup operations fail.</p> Click Verify Connection to confirm that the user information specified is correct. |

Table 27. Common EIM domain controller connection problems and solutions (continued)

| Possible problem | Possible solutions |
|---|---|
| Configuration information appears to be correct but you can not connect to the domain controller. | <ul style="list-style-type: none"> Ensure that the directory server that acts as the EIM domain controller is active. If the domain controller is a System i platform, you can use System i Navigator and follow these steps: <ol style="list-style-type: none"> Expand Network > Servers > TCP/IP. Verify that the Directory Server has a status of Started. If the server is stopped, right-click Directory Server and select Start |

After you verify connection information and that the directory server is active, try to connect to the domain controller by following these steps:

1. Expand **Network > Enterprise Identity Mapping > Domain Management**.
2. Right-click the EIM domain to which you want to connect and select **Connect**.
3. Specify the user type and the required user information that should be used to connect to the EIM domain controller.
4. Click **OK**.

Troubleshooting general EIM configuration and domain problems

There are a number of general problems that you may encounter as you configure EIM for your system, as well as problems that you may encounter as you access an EIM domain. Review the following table to learn more about some common problems and potential solutions that you can use to resolve these problems.

Table 28. Common EIM configuration and domain problems and solutions

| Possible problem | Possible solutions |
|---|---|
| EIM Configuration wizard appears to hang during Finish processing. | <p>The wizard may be waiting for the domain controller to start. Verify that no errors occurred during the startup of the directory server. For System i platforms, check the job log for the QDIRSRV job in the QSYSWRK subsystem. To check the job log, follow these steps:</p> <ol style="list-style-type: none"> 1. In System i Navigator, expand Work Management > Subsystems > Qsyswrk. 2. Right-click Qdirsrv and select Job Log. |
| While using the EIM Configuration wizard to create a domain on a remote system, you received the following error message: "The parent distinguished name (DN) you entered is not valid. The DN must exist on the remote directory server. Specify or select a new or existing parent DN." | The parent DN specified for the remote domain does not exist. See "Creating and joining a new remote domain" on page 73 to learn more about how to use the EIM Configuration wizard. Also, see the online help for detailed information about specifying a parent DN when creating a domain. |
| You receive a message indicating that the EIM domain does not exist. | If you have not created an EIM domain, use the EIM Configuration wizard. This wizard creates an EIM domain for you, or enables you to configure an existing EIM domain. If you have created an EIM domain, ensure that the specified user is a member of an "EIM access control" on page 36 group with sufficient authority to access it. |
| You receive a message indicating that an EIM object (identifier, registry, association, policy association, or certificate filter) is not found, or that you are not authorized to EIM data. | Verify that the EIM object exists and whether the specified user is a member of an "EIM access control" on page 36 group with sufficient authority to that object. |

Table 28. Common EIM configuration and domain problems and solutions (continued)

| Possible problem | Possible solutions |
|--|--|
| When you expand the Identifiers folder, it takes a long time before the list of identifiers displays. | <p>This may happen if there are a large number of EIM identifiers in the domain. To resolve this, you can customize the Identifiers folder view by restricting the search criteria used for displaying identifiers. To customize the view for EIM identifiers, follow these steps:</p> <ol style="list-style-type: none"> 1. In System i 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 to use for generating the list of EIM identifiers to include in the view. Note: You can use the asterisk (*) as a wildcard character. 5. Click OK. <p>The next time you click Identifiers, only those EIM identifiers that match the criteria that you specified display.</p> |
| While managing EIM through System i Navigator, you receive an error indicating that the EIM handle is no longer valid. | <p>The connection to the domain controller has been lost. To reconnect to the domain controller, follow these steps:</p> <ol style="list-style-type: none"> 1. In System i 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. |
| When using the Kerberos protocol for authentication with EIM, diagnostic message CPD3E3F is written to the job log. | <p>This message is generated whenever authentication or identity mapping operations fail. The diagnostic message contains both major and minor status codes to indicate where the problem occurred. The most common errors are documented in the message along with the recovery. Refer to the help information associated with the diagnostic message to begin troubleshooting the problem. You may also find it helpful to review Troubleshoot single sign-on configuration.</p> |

Troubleshooting EIM mapping problems

There are a number of common problems that may cause Enterprise Identity Mapping (EIM) mappings to fail entirely or not to work as expected. Review the following table to find information about what problem may be causing an EIM mapping to fail and potential solutions for that problem. If EIM mappings are failing, you may need to work through each solution in the table to ensure that you find and solve the problem or problems which are causing the mappings to fail.

Table 29. Common EIM mapping problems and solutions

| Possible problem | Possible solutions |
|---|---|
| Connection information for the domain controller may not be correct or the domain controller may not be active. | Review Domain controller connection problems to learn how to verify connection information for the domain controller and how to verify that the domain controller is active. |
| EIM mapping lookup operations performed on behalf of the system are failing. This may be happening because the EIM configuration is incorrect on the system or systems. | <p>Verify your EIM configuration. Expand Network-->Enterprise Identity Mapping-->Configuration on the system that you are trying to authenticate with. Right-click the Configuration folder and select Properties and verify the following:</p> <ul style="list-style-type: none"> • Domain page: <ul style="list-style-type: none"> – The domain controller name and port numbers are correct. – Click Verify Configuration to verify that the domain controller is active. – The local registry name is specified correctly – The Kerberos registry name is specified correctly. – Verify that Enable EIM operations for this system is selected. • System user page: <ul style="list-style-type: none"> – The specified user has sufficient EIM access control to perform a mapping lookup, and the password is valid for the user. Review the online help to learn more about the different types of user credentials. <p>Note: If you have changed the password for the specified system user in the directory server, you must change the password here as well. If these passwords do not match, then the system user can not perform EIM functions for the operating system and mapping lookup operations fail.</p> <ul style="list-style-type: none"> – Click Verify Connection to confirm that the user information specified is correct. |

Table 29. Common EIM mapping problems and solutions (continued)

| Possible problem | Possible solutions |
|--|---|
| <p>A mapping lookup operation may be returning multiple target user identities. This can occur when one or more of the following situations exist:</p> <ul style="list-style-type: none"> • An EIM identifier has multiple individual target associations to the same target registry. • More than one EIM identifier has the same user identity specified in a source association and each of these EIM identifiers has a target association to the same target registry, although the user identity specified for each target association may be different. • More than one default domain policy association specifies the same target registry. • More than one default registry policy association specifies the same source registry and the same target registry. • More than one certificate filter policy association specifies the same source X.509 registry, certificate filter, and target registry. | <p>Use the Test EIM Mapping function to verify that a specific source user identity maps correctly to the appropriate target user identity. How you correct the problem depends on what results you get from the test, as follows:</p> <ul style="list-style-type: none"> • The test returns unwanted multiple target identities for one of the following reasons: <ul style="list-style-type: none"> – This might indicate that association configuration for the domain is not correct, due to one of the following: <ul style="list-style-type: none"> - A target or source association for an EIM identifier is not configured correctly. For example, there is no source association for the Kerberos principal (or windows user) or it is incorrect. Or, the target association specifies an incorrect user identity. Display all identifier associations for an EIM identifier to verify associations for a specific identifier. - A policy association is not configured correctly. Display all policy associations for a domain to verify source and target information for all policy associations defined in the domain. – This might indicate that group registry definitions that contain common members are the source or target registries for EIM identifier associations or policy associations. Use the details provided by the test mapping lookup operation to determine whether the source or target registries are group registry definitions. If they are, check the group registry definition properties to determine whether the group registry definitions contain common members. – The test returns multiple target identities and these results are appropriate for the way you configured associations. If this is the situation, then you need to specify lookup information for each target user identity to ensure that a lookup operation returns a single target user identity rather than all possible target user identities. Review Add lookup information to a target user identity. <p>Note: This approach only works if the application is enabled to use the lookup information. However, base i5/OS applications such as System i Access for Windows can not use lookup information to distinguish among multiple target user identities returned by a lookup operation. Consequently, you might consider redefining associations for the domain to ensure that a mapping lookup operation can return a single target user identity to ensure that base i5/OS applications can successfully perform lookup operations and map identities.</p> |

Table 29. Common EIM mapping problems and solutions (continued)

| Possible problem | Possible solutions |
|---|---|
| EIM lookup operations return no results and associations are configured for the domain. | <p>Use the Test EIM Mapping function to verify that a specific source user identity maps correctly to the appropriate target user identity. Verify that you supplied the correct information for the test. If the information is correct and the test returns no results, then the problem may be caused by one of the following:</p> <ul style="list-style-type: none"> • Association configuration is incorrect. Verify your association configuration by using the problem resolution information provided in the previous entry. • Policy association support is not enabled at the domain level. You may need to enable policy associations for a domain. • Mapping lookup support or policy association support is not enabled at the individual registry level. You may need to enable mapping lookup support and the use of policy associations for the target registry. • The registry definition and user identities do not match because of case sensitivity. You can delete and recreate the registry, or delete and recreate the association with the proper case. |

Related tasks

“Testing EIM mappings” on page 86

Enterprise Identity Mapping (EIM) mapping testing allows you to issue EIM mapping lookup operations against your EIM configuration. You can use the test to verify that a specific source user identity maps correctly to the appropriate target user identity. Testing ensures that EIM mapping lookup operations can return the correct target user identity based on the specified information.

Enterprise Identity Mapping APIs

Enterprise Identity Mapping (EIM) provides the mechanics for cross-platform user identity management. EIM has multiple application programming interfaces (APIs) that applications can use to conduct EIM operations on behalf of the application or an application user.

You can use these APIs to conduct identity mapping lookup operations, various EIM management and configuration functions, as well as information changes and query capabilities. Each of these APIs are supported across IBM platforms.

EIM APIs fall into multiple categories, as follows:

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

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

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

Related concepts

“Planning for Enterprise Identity mapping application development” on page 64

For an application to use Enterprise Identity Mapping (EIM) and participate in a domain, that application must be able to use the EIM APIs.



Related information

Enterprise Identity Mapping (EIM) APIs

Related information for Enterprise Identity Mapping

IBM Redbooks™ publications and other information center topic collections contain information that relates to the Enterprise Identity Mapping (EIM) topic collection. You can view or print any of the PDF files.

IBM Redbooks

- Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server 
- iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos 

Other information

- Single signon
- Network authentication service
- IBM Tivoli Directory Server for i5/OS (LDAP)

Terms and conditions

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

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

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

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

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

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

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

Appendix. Notices

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

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

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

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

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

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

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

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

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

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

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

IBM Corporation

Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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

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

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

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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

COPYRIGHT LICENSE:

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

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

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

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

Trademarks

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

AIX
Distributed Relational Database Architecture
Domino
DRDA
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400
pSeries
RACF
RDN
System i
Tivoli
WebSphere
xSeries
z/OS

- | Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- | Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

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

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

Terms and conditions

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

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

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

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

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

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

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



Printed in USA