Oracle® Healthcare Master Person Index

Data Manager User's Guide

Release 3.0

E62301-01

March 2015

ORACLE®

Oracle Healthcare Master Person Index Data Manager User's Guide, Release 3.0

E62301-01

Contents

3 Object Profile Searches on the MIDM

4 Object Profile Views on the MIDM

5 Object Profiles on the MIDM

6 MIDM Maintenance Tasks

7 MIDM Reports

8 Master Index Data Manager Security

Preface

This document provides conceptual information and procedures for managing Oracle Healthcare Master Person Index (OHMPI) applications using the web-based Master Index Data Manager (MIDM) and is accessed through an internet browser.

Audience

This document is intended for users who manage their OHMPI applications and projects using MIDM.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information and instructions for implementing and using a master person index application, see the following documents in the Oracle Healthcare Master Person Index documentation set:

- *Oracle Healthcare Master Person Index Data Manager User's Guide* [This document]
- *Oracle Healthcare Master Person Index Analyzing and Cleansing Data User's Guide*
- *Oracle Healthcare Master Person Index Australia Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index Command Line Reports and Database Management User's Guide*
- *Oracle Healthcare Master Person Index Configuration Guide*
- *Oracle Healthcare Master Person Index Configuration Reference*
- *Oracle Healthcare Master Person Index Installation Guide*
- *Oracle Healthcare Master Person Index Loading the Initial Data Set User's Guide*

- *Oracle Healthcare Master Person Index Match Engine Reference*
- *Oracle Healthcare Master Person Index Message Processing Reference*
- *Oracle Healthcare Master Person Index Provider Index User's Guide*
- *Oracle Healthcare Master Person Index Real-time Loader User's Guide*
- *Oracle Healthcare Master Person Index Release Notes*
- *Oracle Healthcare Master Person Index Security Guide*
- *Oracle Healthcare Master Person Index Standardization Engine Reference*
- *Oracle Healthcare Master Person Index United Kingdom Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index United States Patient Solution User's Guide*
- *Oracle Healthcare Master Person Index User's Guide*
- *Oracle Healthcare Master Person Index Working With HPD Profile Application User's Guide*
- *Oracle Healthcare Master Person Index Working With IHE Profiles User's Guide*

Note: These documents are designed to be used together when implementing a master index application.

Finding Information and Patches on My Oracle Support

Your source for the latest information about Oracle Healthcare Master Person Index is Oracle Support's self-service Web site My Oracle Support (formerly MetaLink).

Before you install and use Oracle Healthcare Master Person Index, always visit the My Oracle Support Web site for the latest information, including alerts, White Papers, installation verification (smoke) tests, bulletins, and patches.

Creating a My Oracle Support Account

You must register at My Oracle Support to obtain a user name and password account before you can enter the Web site.

To register for My Oracle Support:

1. Open a Web browser to `https://support.oracle.com`.
2. Click the **Register here** link to create a My Oracle Support account. The registration page opens.
3. Follow the instructions on the registration page.

Signing In to My Oracle Support

To sign in to My Oracle Support:

1. Open a Web browser to `https://support.oracle.com`.
2. Click **Sign In.**
3. Enter your user name and password.
4. Click **Go** to open the My Oracle Support home page.

Finding Information on My Oracle Support

There are many ways to find information on My Oracle Support.

Searching by Article ID

The fastest way to search for information, including alerts, White Papers, installation verification (smoke) tests, and bulletins is by the article ID number, if you know it.

To search by article ID:

1. Sign in to My Oracle Support at https://support.oracle.com.
2. Locate the Search box in the upper right corner of the My Oracle Support page.
3. Click the sources icon to the left of the search box, and then select **Article ID** from the list.
4. Enter the article ID number in the text box.
5. Click the magnifying glass icon to the right of the search box (or press the Enter key) to execute your search.

   The Knowledge page displays the results of your search. If the article is found, click the link to view the abstract, text, attachments, and related products.

Searching by Product and Topic

You can use the following My Oracle Support tools to browse and search the knowledge base:

- Product Focus — On the Knowledge page under Select Product, type part of the product name and the system immediately filters the product list by the letters you have typed. (You do not need to type "Oracle.") Select the product you want from the filtered list and then use other search or browse tools to find the information you need.
- Advanced Search — You can specify one or more search criteria, such as source, exact phrase, and related product, to find information. This option is available from the **Advanced** link on almost all pages.

Finding Patches on My Oracle Support

Be sure to check My Oracle Support for the latest patches, if any, for your product. You can search for patches by patch ID or number, or by product or family.

To locate and download a patch:

1. Sign in to My Oracle Support at https://support.oracle.com.
2. Click the **Patches & Updates** tab. The Patches & Updates page opens and displays the Patch Search region. You have the following options:
   - In the **Patch ID or Number is** field, enter the number of the patch you want. (This number is the same as the primary bug number fixed by the patch.) This option is useful if you already know the patch number.
   - To find a patch by product name, release, and platform, click the **Product or Family** link to enter one or more search criteria.
3. Click **Search** to execute your query. The Patch Search Results page opens.
4. Click the patch ID number. The system displays details about the patch. In addition, you can view the Read Me file before downloading the patch.
5. Click **Download.** Follow the instructions on the screen to download, save, and install the patch files.

Finding Oracle Documentation

The Oracle Web site contains links to all Oracle user and reference documentation. You can view or download a single document or an entire product library.

Finding Oracle Health Sciences Documentation

To get user documentation for Oracle Health Sciences applications, go to the Oracle Health Sciences documentation page at:

http://www.oracle.com/technetwork/documentation/hsgbu-154445.html

> **Note:** Always check the Oracle Health Sciences Documentation page to ensure you have the latest updates to the documentation.

Finding Other Oracle Documentation

To get user documentation for other Oracle products:

1. Go to the following Web page:

   http://www.oracle.com/technology/documentation/index.html

   Alternatively, you can go to http://www.oracle.com, point to the Support tab, and then click **Documentation**.
2. Scroll to the product you need and click the link.
3. Click the link for the documentation you need.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction to the Master Index Data Manager

This chapter provides an introduction to OHMPI and its features, including the function of the MIDM. It also provides conceptual information about MIDM object profiles.

This chapter includes the following sections:

Learning About OHMPI Applications and MIDM Functions

The MIDM is your primary tool to view and maintain the data stored in the master person index database and cross-referenced by a master person index application. It is a web-based interface that lets you access, monitor, and maintain the data stored by the master person index applications you create using OHMPI. You can use MIDM to search add, update, delete, deactivate, reactivate, merge, unmerge, and compare object profiles. You can also view and correct potential duplicate profiles, view transaction histories, view source records, view patient summary information, view an audit log, and print reports.

OHMPI provides a flexible framework, which lets you create matching and indexing applications called master person index applications. It is an application building tool to design, configure, and create a master person index application that uniquely identifies and cross-reference the business objects stored in your system databases. Business objects can be any type of entity for which you store information, such as patients, doctors, hospitals, healthcare facilities, pharmacies, and so on. OHMPI lets you define the data structure of the business objects to be stored and cross-referenced. In addition, you define the logic that determines how data is updated, standardized, weighted, and matched in the master person index database.

The following sections provide additional information about OHMPI, the master person index applications created by OHMPI, and the MIDM.

About Master Person Index Applications

The applications created by OHMPI are enterprise-wide master person index applications that maintain the most current information about the objects in your business enterprise. A master person index application creates a single, consistent view of all object data by providing an automatic, common identification process regardless of the location or system from which the data originates. Object profiles from various locations are cross-referenced using an enterprise-wide unique identifier (EUID) assigned to each profile by the master person index application. By creating EUIDs, a master person index application can identify many types of participants, such as customers, employees, contacts, and so on.

The identification and general information for all objects is centralized in one shared index. A master person index application is designed specifically to support scattered business locations, disparate information systems across an enterprise, and various applications from multiple vendors. Maintaining a centralized database for multiple systems enables a master person index application to integrate data throughout the enterprise while allowing local systems to continue operating independently. A master person index application makes it easy to find information that are previously scattered among multiple systems.

Features of Master Person Index Applications

The components of the master person index applications you create are configurable, letting customization of each master person index application for your specific data processing needs. Primary features of a master person index application include the following:

- **Centralized Information** - A master person index application maintains a centralized database, enabling the integration of data records throughout the enterprise while letting local systems continue operating independently. The index stores copies of local source records and the single best record (SBR), which represents the most accurate and complete data for each object. This database is the central location of all object information and identifiers, and is accessible throughout the enterprise. Records from various systems are cross-referenced using the EUID assigned by a master person index application to each object profile.
- **Configurability** - Before deploying a master person index application, you can customize the components and processing capabilities of the system. The configurable components include:
  - Types of objects to index
  - Types of data stored
  - Standardization and match engines to use
  - Matching, standardization, and phonetic conversion rules
  - Survivorship and weighting rules for determining the SBR
  - Types of queries available
  - How queries are blocked or grouped for match processing
  - MIDM appearance
  - Searches available to the MIDM
  - Local ID validation rules

You can deploy MIDM on single or multiple machines using the configurability feature. When you deploy MIDM on multiple machines, it isolates the web layer from the business layer. This makes the application more scalable.

- **Cross-referencing** - A master person index application serves as a global cross-reference, matching profiles across disparate source systems, and simplifying the process of sharing data between systems. A master person index application uses the local identifiers assigned by your existing systems as a reference that lets you maintain your current systems and practices.
- **Data Cleansing** - A master person index application uses configurable matching algorithm logic to uniquely identify object profiles, and duplicate and potential duplicate profiles. You can use master person index application to easily merge or resolve duplicates, and can be configured to automatically match profiles that are found to be duplicates of one another.
- **Data Updates** - A master person index application provides the ability to add, update, deactivate, merge, and delete data in the database tables through messages received from external systems or the MIDM. Messages received from external systems and the MIDM are checked for potential duplicates during processing.
- **Updates to External Systems** - The master person index application can publish updated information to external systems, provided the external systems can accept incoming messages. This is handled through a JMS Topic to which a master person index application publishes XML messages that contain the updates.
- **Identification** - A master person index application employs configurable probabilistic matching technology. This technology uses a matching algorithm to formulate an effective statistical measure of how closely profiles match. Using a state-of-the-art algorithm in the real-time mode and establishing a common method of locating profiles, a master person index application consistently and precisely identifies objects within an enterprise.
- **Matching Algorithm** - A master person index application uses the OHMPI match engine or a custom matching algorithm to provide a matching probability weight between object profiles. You can define matching thresholds, which control how potential duplicates and automatic merges are determined.
- **Unique Identifier** - A master person index application assigns an enterprise-wide unique identifier (EUID) to each object added to the database. The index uses the EUID to cross-reference the local IDs assigned to each object by various computer systems throughout the enterprise.
- **Security** - A master person index application provides secure access to the patient information. It also provides restricted access to patient records by masking and unmasking their sensitive data. This feature is configurable.

Functions of the Master Index Data Manager

While a master person index application cleanses data automatically as it is entered through external system messages or through the MIDM, there are instances where it cannot be determined automatically whether two object profiles truly match one another. In these cases, manually review through the MIDM to verify the status of two profiles, and join two potential duplicate profiles or separate two profiles that are automatically joined. The MIDM provides additional functions to maintain the data you store.

Using the MIDM, you can perform the following activities:

- **View an Object's History**: The system provides a complete transaction history of each object profile by recording all changes to each object's data. This lets you view before and after images of a profile for each change made. The table also records the user ID of the person who made the changes. This history is maintained for both local source records and SBR.
- **Search for Object Profiles**: Using the MIDM, you can search for specific objects or set of objects. The MIDM lets you perform different types of search using different combinations of data elements, which returns a list of potential matches to your search criteria. For certain searches, the results are assigned a matching weight that indicates the probability of a match.
- **Maintain Object Data**: The MIDM supports all necessary features for maintaining object profiles. It lets you add new profiles (view, update, delete, deactivate, or reactivate existing profiles), and compare profiles for similarities and differences. You can also view each local source record associated with an SBR.
- **Compare Object Data**: The MIDM lets you compare two or more object profiles in a side-by-side or tabular comparison to evaluate their differences or similarities. You can also compare different objects within one object profile in the same comparison view. For example, you can compare the SBR of a profile with a record from System A and compare the record of a profile from System A with its record from System B.
- **View and Resolve Potential Duplicates**: The data *deduplication* improves storage utilization by identifying and eliminating redundant data. Using algorithm matching logic, a master person index application identifies potential duplicate profiles, and the MIDM manually corrects the duplicate profiles. Profiles that are potential duplicates can be viewed online in a side-by-side or tabular comparison. Potential duplication is resolved by either merging the profiles in question or removing their potential duplicate flags.
- **Merge and Unmerge Profiles**: You can compare potential duplicate profiles and merge duplicate profiles. Using the merge feature, you can determine the profile to be retained as the active profile. The MIDM also lets you merge source records between object profiles and specify the information to be preserved from each source record in the resulting profile. If two object profiles or source records are merged in error, you can unmerge them. You can also view the history of merges for a profile by viewing the transactions page for the specified EUID or Local ID for the SBR. You can only unmerge the last merged transaction from the profiles.
- **Audit Log**: The system administrator can specify to maintain a log for each instance of the object data that is accessed from the MIDM. This log provides information such as the ID of the user who accessed the data, the type of action that is performed against the data, and the date and time of access.
- **Security**: Security is provided through the application server, which includes basic access to the database through user login IDs and passwords, and access to specific functions and actions of a master person index application. Access can be restricted by functions, actions within functions, data element, and user ID.

Learning About MIDM Object Profiles

The information about an object in a master person index application is stored in an object profile. The profile includes information from all source records for that object and a record that contains the best information about the object according to the master person index application.

The following sections describe object profiles and their components:

MIDM Object Profile Components

An object profile, also known as an enterprise record, is a set of information that describes characteristics of an individual object in the master person index application. An object profile includes information from one or more source systems. The information can be divided into child objects, which hold additional information about an object, such as address information, telephone information, or alias names.

A profile contains two types of records:

- **Source Records** - Also known as a system record is a set of information from an external system that shares data with a master person index application. A profile may contain several source records.
- **Single Best Record** -Is a set of information derived from the best information from each source record in an object profile (as determined by the survivor calculator). Each object profile has only one SBR.

Source Records

Source records are different from the SBR, in which each source record contains a system and local ID pair, and only contains data from a specific system. The information in the source records of an object profile determines the best values for the SBR in that profile. If an object profile only contains one source record, the SBR is identical to that source record. However, if an object profile contains multiple source records, the SBR may be identical to one source record but includes a combination of information from all source records. Certain actions (such as, updating, deleting, deactivating, merging, and unmerging a source record) against a source record changes the SBR. Each active object profile must have at least one active source record. If all source records in a profile are deactivated, the entire profile is deactivated.

Single Best Record

The SBR for an object profile is a combination of information from all active source records associated with that object profile. The SBR represents the information that is determined by the master person index application to be the most reliable and current of all source records in an object profile. The SBR is dynamic and is recalculated each time an update is made to an associated source record, a merge or an unmerge affects the object profile, or a source record in the profile is deactivated or reactivated. You can use the overwrite capability of the MIDM to update the SBR directly or update a source record, and let survivor calculator determine how to update the SBR. For more information, see Survivor Calculator on page 1-6.

You can override the survivor calculator by specifying values for the SBR in the following ways:

- Use the overwrite capability to update a field that remains locked, and cannot be updated by changing the source records until the field is unlocked.
- Link a field in the SBR to the same field in one of the profile's source systems, and that SBR field contains the same value as the source system until the link is removed.

For more information on overwrites and linked fields, see Linking Field Values in the SBR on page 6-4.

Survivor Calculator

The survivor calculator determines which information from each source record in an object profile is stored in the SBR for that profile. The calculator uses information defined by the system administrator to calculate the SBR. By default, the survivor calculator uses a weighted strategy for most fields, using the relative reliability assigned to each system in combination with the reliability given to the most recently updated value.

For some fields, such as alias and auxiliary IDs, a union strategy is used. This means that all unique alias names and auxiliary IDs from all systems are included in the SBR. For detailed information about the survivor calculator and configuring the survival strategy, see *Oracle Healthcare Master Person Index Configuration Reference* and *Oracle Healthcare Master Person Index Configuration Guide*.

Source Record and SBR Components in a Master Person Index

In a master person index application, each source record and SBR in an object profile contains a set of sub-objects that store different types of information about the object. Generally, a record contains a parent object and several child objects. A record can have only one parent object, but can have multiple child objects and multiple instances of each child object, with each instance being identified by a unique field. For example, in a master person index, a record can only contain one person name and social security number (contained in the parent object), but can have multiple addresses, telephone numbers, and aliases (contained in child objects). Each address must be a different type, such as a home address, billing address, or mailing address.

Identification Numbers for Each Entity in the Master Person Index

Each object profile in a master person index application is assigned a unique identification number and the local IDs assigned by individual systems. Each object has one unique identification number throughout your organization and a unique identification number within each system with which they are registered.

EUID

Every object profile in the master person index system is assigned a EUID number. This number is the same for that object regardless of the system from which the object information originates. This number is used to cross-reference object profiles to accurately identify the objects throughout your organization.

Local ID

A local ID is a unique local identification number that is assigned to an object in each system at which it is registered. These numbers are assigned using a numbering system unique to each local system, and are used internally by the systems to identify each object. A master person index application uses an object's EUID to cross-reference its local IDs in different systems.

Note: The name of the Local ID field is configurable and may be different for your implementation.

Auxiliary ID

An auxiliary ID is an identification code that does not necessarily uniquely identify a single object within the database, but may identify a group of objects. For example, if a family shares the same account or insurance policy, every family member has the same

identification code for that account or policy.

2

The Master Index Data Manager

This chapter provides information and procedures about MIDM, including logging in and out of the MIDM, using the dashboard, and learning about object queries.

This chapter includes the following sections:

Working With the Master Index Data Manager

The MIDM is the primary tool to view and maintain the data stored in the master person index database and cross-referenced by a master person index application. It is a web-based application. The MIDM uses standard web-based features, such as hyperlinks, data fields, icons, and action buttons, to help you enter information and navigate through the different pages.

The following sections provide basic information about the design of the MIDM and logging in and out of the application:

Requirements

The MIDM is supported on Mozilla Firefox 24 and higher, Internet Explorer 10 and higher, and Google Chrome 30 and higher. Oracle recommends that you use Internet Explorer or Mozilla Firefox to access the MIDM application in the WebLogic Clustering environment.

For the browser you use, ensure that pop-up windows are allowed for the MIDM URL, and that JavaScript is enabled. Additionally, if you are working with sensitive data, disable the feature that automatically fills in field values as you type. These options are configured on the Options (Mozilla Firefox) or Internet Options (Internet Explorer) window accessed from the Tools menu.

Logging into the Master Index Data Manager

Before using the MIDM, you must first log in to the application in your web browser. Ensure you have a user ID and password for the master person index application before logging in. The application server running the master person index application must be started before you can log in to the MIDM.

The URL for the MIDM is:

`http://`**`host`**`:`**`http_port`**`/`**`application_name`**`MIDM`

where,

- **`host`** is the name of the server machine.
- **`http_port`** is the HTTP port number of the application server.
- **`application_name`** is the name of the master person index application.

> **Note:** The application name is created when the project is created. The MIDM at the end of the URL is case-sensitive and must be entered in capital letters.

The HTTP port number for the application server is listed in the config.xml file in the *listen-port* element under the sever element (7001 by default). The config.xml file is located in the user_projects\domains\domain_name\config directory.

To Log into the MIDM

1. Launch a web browser.
2. In the **Address** field, enter the appropriate URL.

   The login page appears.
3. In the upper-right portion of the page, select the language for the MIDM display from the drop-down list.

   > **Note:** This performs only a partial translation and you must configure your system. For additional information, see *Oracle Healthcare Master Person Index Configuration Guide* and *Oracle Healthcare Master Person Index Configuration Reference*.

4. Enter your user ID and password in the appropriate fields.
5. Click **Login**.

   The initial page appears. By default, the initial page is the Record Details page, but this is configurable.

Note: After a certain period of inactivity, the session for the user terminates. The MIDM automatically logs off and returns you to the Login page when you try to perform an activity on the MIDM. To access the MIDM, re-enter your user name and password. The system administrator can set the inactivity period at the server level in the *session-timeout* element of `default-web.xml` (in appserver_home\domains\domain_name\config) or at the application level in `web.xml` in the master person index application `.war` file (located in the deployment `.ear` file) or in the deployment folder. The application level overrides any values set at the server level. The default inactivity period is 30 minutes.

Master Index Data Manager Security Permissions

Security for the MIDM is defined at the function level. You may not be able to perform all functions described in this guide depending on the security permissions you are assigned. For more information about functions you can perform, contact your system administrator. Security for the MIDM is defined in the application server. For information about defining security for the MIDM, see Defining Master Index Data Manager Security on page 8-1.

Master Index Data Manager Navigation Tips

The MIDM provides hyperlinks, icons, and command buttons to access and move through the MIDM pages. When you place the cursor over links, icons, and images on the MIDM pages, tooltips are displayed, which provide additional information. Information is also provided to facilitate the use of screen readers and other assistive technology.

Navigating the MIDM Functions

The actions you can perform on the MIDM are grouped into these primary functions: Dashboard, Duplicate Records, Record Details, Assumed Matched, Transactions (history), Source Record, Reports, and Audit Log. The main menu on all MIDM pages provides hyperlinks to each of these functions. The first page is the Search page that is displayed for each function, except the Source Record function. You can modify the names of these headings for your application.

- **Dashboard** - This provides a summary of recent transactions, quick links to commonly used functions, and quick lookup functions. The information, links, and lookup functions on this page can be configured by the system administrator.
- **Duplicate Records** - This lets you perform a search for potential duplicate profiles. Potential duplicate profiles are those whose matching probability weight indicates that they might match but is not high enough to automatically match the two profiles. From the associated pages, you can compare, merge, or resolve potential duplicate profiles.
- **Record Details** - This lets you perform a search for an object profile or set of object profiles in the master person index application. From the associated pages, you can compare two object profiles, compare records in one object profile, view all information for one object profile, view and print summary information for a profile, update an object profile or source record, delete an object profile, view a transaction history of an object profile, view potential duplicates of an object, and merge object profiles.

- **Assumed Matches** - This lets you perform a search for any profiles that are updated by an assumed match transaction. It also shows the transaction history that generated the assumed match. An assumed match occurs when the matching probability weight is high enough to indicate that two records represent the same object. From the associated pages, you can view and reverse assumed match transactions.
- **Transactions** - This lets you perform a search for transaction histories. From the Transaction History pages, you can compare information about an object before and after a transaction occurred, select object profiles to unmerge (the last merged transaction), and view a merge history for an object profile. From associated Transaction History pages, you can unmerge object profiles.
- **Reports** - This lets you display and print reports about certain transactions performed from the MIDM and from messages sent in from external systems. You can run reports from either the MIDM or from a command line.
- **Source Record** - The Create Source Record function lets you create new object profiles by creating a source record. When you save the information in the source record, the master person index application automatically generates the SBR using the survivor calculator. You can also edit, delete, or merge source records from the Source Record page.
- **Audit Log** - When enabled, this lets you perform a search for audit log entries. From the Audit Log pages, you can view information about transactions in which data about an object is accessed through the MIDM. This enforces HIPAA privacy rules for healthcare master indexes.

Navigating the MIDM Detail Pages

The detail pages display the SBR of the object profile on the left and summary information on the right side of the screen. You can further expand the pages to view source records on the right side. Child objects appear below the parent object, and you can expand and collapse the information for each type of object. If you are viewing a comparison of object profiles, you can expand the source records of one object profile at a time.

Navigating Through Icons

Table 2–1 displays the list of icons used in the MIDM application to provide enhanced usability to the end-users.

Table 2–1 Icons

Icon	Tool Tip	Description
	View Sources	Displays all the source objects associated with the Enterprise object.
	View History	Displays history of the Enterprise object.
	View Merge Tree	Displays the hierarchy of the merged records.
	View Transaction	Directs to the transactions page where you can view the transaction details for the assumed match record.
	View Summary	Displays the summary for the Enterprise object.

Table 2–1 (Cont.) Icons

Icon	Tool Tip	Description
	Print SBR	Displays details for the SBR in a report format.
	Delete	Deletes the source object.
	Potential Duplicate	Marks a record as potential duplicate.
	Different Records	Marks a record as different.
	System Record Transfer	Transfers system object to an Enterprise object.

Logging Out of the MIDM

Before you exit the MIDM, ensure you have saved the changes (if any). To exit the MIDM, click **Sign Out** in the upper-right corner of the page. The Login page reappears.

Using the MIDM Dashboard

The following sections provide step-by-step instructions to perform various functions available from the MIDM dashboard. The information in these topics is based on the default configuration.

- Viewing Summary Information From the Dashboard on page 2-5
- Accessing Reports and Audit Logs From the Dashboard on page 2-6
- Performing a Quick Search (EUID Lookup) on page 2-6
- Performing a EUID Comparison Lookup on page 2-6

Viewing Summary Information From the Dashboard

The dashboard provides a short summary of important transactions that have occurred in the past 24 hours. You can view how many transactions occurred and link to the search pages to view more information.

To View Summary Information

1. In the tabbed headings, click **Dashboard**.

   The Summary box displays the number of potential duplicate and assumed match transactions that have occurred in the past 24 hours.

2. To view additional information about potential duplicates, click **Potential Duplicates** in the Summary field, and then perform a search as described in the section Working with Potential Duplicate Profiles on the MIDM on page 6-16.

3. To view additional information about assumed match transactions, click **Assumed Matches** in the Summary field, and then perform a search as described in the section Working with Assumed Matches on the MIDM on page 6-22.

Accessing Reports and Audit Logs From the Dashboard

The dashboard provides quick links to the search pages for different type of production reports that gives information about the status of your data.

To Access Reports and Audit Logs From the Dashboard

1. In the tabbed headings, click **Dashboard**.
2. To view a merged record report, click **Merged Records**, and perform a search as described in the section Running MIDM Reports on page 7-3.
3. To view a deactivated record report, click **Deactivated EUIDs**, and perform a search as described in the section Running MIDM Reports on page 7-3.
4. To view an unmerged record report, click **Unmerged Records**, and perform a search as described in the section Running MIDM Reports on page 7-3.
5. To view an audit log report, click **Audit Log**, and perform a search as described in the section Viewing the MIDM Audit Log on page 4-10.

Performing a Quick Search (EUID Lookup)

To search for an object profile using only the EUID of an object, you can enter the EUID number in the Quick Search box of the dashboard. This type of search results in only one matching profile.

To Perform Quick Search

1. In the tabbed headings, click **Dashboard**.
2. In the **Quick Search** section, enter the EUID of the object.
3. Click **Search** to initiate the search.

   The Record Details page appears, displaying detailed information about the object.
4. To perform a more advanced search with multiple criteria fields and options, click **Advanced Search**.

Performing a EUID Comparison Lookup

You can perform a lookup of multiple EUIDs from the dashboard to compare object profiles in a side-by-side view on the Record Details page. To lookup multiple EUIDs, specify each EUID in the Compare EUIDs field on the dashboard. You can enter two to four EUIDs to compare in the search results list.

To Perform a EUID Comparison Lookup

1. In the tabbed headings, click **Dashboard**.
2. In the **Compare EUIDs** field, enter two to four EUIDs.
3. Click **Compare**.

   The Record Details page appears with each matching profile displayed side-by-side.

Learning About Object Queries on the MIDM

Before viewing or updating object information, you must perform a search for the object. There are several different search capabilities within the MIDM. You can

perform lookups for specific object profiles using unique identifiers, such as the EUID or local ID, and you can perform broader searches using data from the parent or child objects as criteria.

The following topics provide information about working with general searches that find specific records in the master person index database. Most of these searches are performed from the Record Details page, but some are performed from the dashboard. Searches for specific functions, such as finding potential duplicates or assumed matches, are described in the topics for those functions.

- About the MIDM Search Function on page 2-7
- Searching by Ranges on the MIDM on page 2-8
- Required Fields on the MIDM on page 2-9

About the MIDM Search Function

There are several different methods of searching for objects, depending on the search criteria you enter. By default, the Record Details page includes three different search types: Advanced ProjectName Lookup (Alpha), Advanced ProjectName Lookup (Phonetic), and Simple ProjectName Lookup. You can also perform a EUID lookup from the dashboard to view record details. The search functionality provides flexibility in designing database queries. You can narrow a search for a specific object or a range of objects using various fields on the search pages, and then view your search results in the search results list. When you select a specific object from the Search Result page, detailed information for that object appears on the Record Details page in the view mode.

> **Note:** The names of the search types are configurable. Searches are described in the following sections by their default names, and images show customized search criteria. Contact your system administrator if you have questions about how your search pages are configured.

Simple Lookup

The Simple Lookup on the Record Details page lets you perform lookups using unique identifiers to find a specific object profile. By default, the unique identifiers you can use as search criteria include the EUID, and the local ID and system. When you perform this type of search, the search results list is bypassed and the Record Details page appears in the view mode, displaying information about the matching profile.

You can perform a EUID lookup from either the Dashboard or the Record Details page. Other simple lookups include system and local ID lookups, which can be performed from the Record Details page or the Source Record page. To increase search accuracy, you can select only the system listed in the drop-down list and the Local ID field is case-sensitive.

Advanced Alphanumeric Lookup

The Advanced Alphanumeric Lookup on the Record Details page lets you perform various types of searches against the database using a field or combination of fields as criteria. This type of search is an exact match search, which returns profiles that exactly match the criteria you specify. You can specify any combination of fields as long as any fields that are required for the search are entered. Most fields in this search allow wildcard characters if the exact value is unknown.

The fields displayed on the Search page are configured by the system administrator. You can enter as much information as needed to narrow down the search appropriately.

Advanced Phonetic Lookup

The Advanced Phonetic Lookup on the Record Details page lets you perform various types of searches against the database using predefined combinations of fields as criteria. This type of search compares the phonetic values of certain fields entered as criteria. The object profiles returned by a phonetic search are assigned a matching probability weight to indicate how closely they match the search criteria. Phonetic searches are not exact match searches and allow for misspellings or data entry errors.

The fields displayed on the Search page are configured by the system administrator. You can enter as much information as needed to narrow down the search appropriately. For phonetic searches, certain combinations of criteria are required to perform a search. The search is only carried out for combinations that have complete data.

For example, in a master company index, a blocking search might be configured to search on the following combinations:

- Company Name and Sales Region
- Company Name and Address Line1
- Tax Payor ID
- Stock Symbol and Address Line1

If Company Name, Address Line1, and Stock Symbol are entered as criteria, only the second and fourth combinations are carried out. The returned result set includes any records that match on Company Name and Address Line1 **or** that match on Stock Symbol and Address Line1. If only Company Name is entered as the criteria, no records are returned since it does not fulfill any of the combination requirements.

The Search Results List

The search results list appears under the search fields and displays a list of object profiles found in the database that closely match the search criteria you entered. The results list appears in a table, with the number of profiles returned for the search displayed above the table. This page displays information to identify the object profile, such as the EUID or address information. The search results list appears differently depending on which type of search is performed and how the lists are configured. For more information about search results, see Working with Search Results on the MIDM on page 3-4.

Searching by Ranges on the MIDM

Your system administrator can configure the search pages to let you enter a range to search for certain fields. For example, you might want to search for profiles with a specific name, but with a date that falls within a five-year range. If a field is defined to search by a user-defined range, the MIDM displays a **from** field and a **to** field so you can specify the range (for example, Date From and Date To). If you enter a value only in the **from** field, the MIDM searches for profiles with a value greater than or equal to that value. If you only enter a value only in the **to** field, the MIDM searches for profiles with a value less than or equal to that value.

Ranges can also be defined as an entered value plus or minus a specific value. For example, a date field can be configured to search for dates that fall within a range five

years earlier than the date you enter, and five years later than the date you enter. Ranges can be defined as specific upper and lower limits. These limits are used when no value is entered. For example, if you perform a search without the date, the MIDM searches between the defined lower and upper limits. If you enter only the *from* date, the MIDM searches between the date you entered, and the defined upper limit. For more information about how your system is configured for range searching, contact your system administrator.

Required Fields on the MIDM

Certain fields are mandatory for searches on the MIDM. If a field is marked with an asterisk (*), it indicates that it is mandatory. If multiple fields are marked with daggers (†), at least one of these fields must be populated to perform the search. The required fields can vary depending on the type of search you perform.

3

Object Profile Searches on the MIDM

This chapter provides step-by-step instructions to perform the various types of searches for object profiles available on the MIDM.

This chapter includes the following section:

Searching for Object Profiles on the MIDM

See the following sections to perform searches for object profiles. To move from one field to another on the search pages without using the mouse, press the **Tab** key.

Performing a EUID Lookup

To search for an object profile using only the EUID of an object, you must enter the EUID number in the EUID Search section, either on the Dashboard or Record Details page. This type of search results in only one matching profile.

> **Note:** The following procedure performs the lookup from the Record Details page. For instructions on performing the lookup from the Dashboard, see Performing a Quick Search (EUID Lookup) on page 2-6.

To Perform a EUID Lookup

1. Click the **Record Details** tab and select **obj_name Lookup** from the **Select the Search Type** drop-down list (where, **obj_name** is the name of the master person index object).
2. In the EUID section, enter the object's EUID.

> **Note:** If you do not know the EUID, enter the local ID of the object.

3. In the **System** drop-down list, select the source system such as, a hospital for which the object's EUID or local ID is known.
4. Click **Search** to initiate the lookup.

   The Record Details page appears in the view mode, displaying details and summary information about the object whose EUID is entered.

Performing a Local ID Lookup

To search for an object profile by its local ID in a specific system, you must enter the search criteria in the local ID section of the Lookup page. This type of search results in only one matching profile. If the Local ID field contains alphabetic characters, the criterion is case-sensitive.

Note: The name of this section may be modified for your implementation. For more information, contact your system administrator.

To Perform a Local ID Lookup

1. Click the **Record Details** page and select **app_name Lookup** from the **Select the Search Type** drop-down list (where, **app_name** is the name of the master person index application).
2. In the **System** drop-down list, select the source system such as, a hospital for which the object's local ID is known.
3. In the Local ID field, enter the unique identification code of the object for the specified system.

   Note: If alphabetic characters are entered in this field, the search is case-sensitive. This field name may be modified for your implementation.

   ---

4. Click **Search** to initiate the lookup.

   The Search Result page is bypassed and the Record Details page appears in the view mode.

Performing an Alphanumeric Search

To perform an alphanumeric search for an object profile, you must specify identifying information for the object on the Alphanumeric Search page. This type of search results in several matching profiles.

Note: Make your search as specific as possible. This type of search allows wildcard characters. Use a percent sign (%) to indicate unknown characters. Mandatory fields are marked with an asterisk (*). If at least one field in a group of fields is required, the fields in that group are marked with a dagger (†).

In addition, range searching is supported for any field type that has two fields, one appended with **From** and the other with **To** to the name (for example, DOB From and DOB To). If your MIDM is set up for range search, contact the system administrator for more information about how it is configured.

To Perform an Alphanumeric Search

1. On the Record Details page, select **Advanced app_name Lookup (Alpha)** from the Search Type drop-down list (where, **app_name** is the name of the master person index application).
2. Enter the search criteria for the object you want to find.
3. Click **Search** to initiate the search.

   The search results list appears with a list of matching profiles. If only one matching profile is returned, the Record Details page appears in the view mode.

Note: The system administrator can select whether to display certain transaction-based fields on this page such as, the EUID, the local ID, and system fields, or the create date field. Any values entered in these optional fields take precedence over information entered in other search fields.

For example, if an invalid EUID is entered, but valid first and last names are entered, no results are returned due to the invalid EUID. The EUID field takes precedence over the local ID and system fields.

Performing a Phonetic Search

To perform a phonetic search for an object profile, you must specify identifying information for the object in the phonetic search fields. Only specific combinations of fields are used for queries. This search returns several profiles.

To Perform a Phonetic Search

1. On the Record Details page, select **Advanced app_name Lookup (Phonetic)** from the Search Type drop-down list (where, **app_name** is the name of the master person index application).
2. Enter the search criteria for the object you want to find.

Note: Certain combinations of data may be required to perform a phonetic search. For more information, contact your system administrator.

For more information about phonetic searches, see Advanced Phonetic Lookup on page 2-8.

3. Click **Search** to initiate the search.

   The search results list appears with a list of matching profiles. If only one matching profile is found, the results list is bypassed and the Record Details page appears in the view mode.

   Note: The system administrator can select whether to display the EUID field or the local ID, and system fields on this page. Any values entered in these optional fields take precedence over information entered in other search fields.

   For example, if an invalid EUID is entered, but valid first and last names are entered, no results are returned due to the invalid EUID. The EUID field takes precedence over the local ID and system fields.

Working with Search Results on the MIDM

The following topics describe the search results list for searches performed from most MIDM pages, sort, select the profiles that match the searches, and print a search result report. The results list appears below the search criteria. The number of records returned for the search, appear above the results list.

Viewing the Results of a Search

The matching profiles that result from an object search appear in the table format below the search criteria. The table displays a limited number of fields contained in the SBR of the object profile.

To View the Results of a Search

1. Using one of the searches described in Searching for Object Profiles on the MIDM on page 3-1, perform a search for the object whose profile you want to access.

   If more than one record matches the criteria, the search results list appears below the criteria.

2. In the results list, view the information presented for each returned profile to determine which profile you want to view.

3. To view additional address or telephone information for a profile, click the address component, or the telephone number you want to view.

   A pop-up window appears.

4. After viewing the additional address or telephone information, click **Close**.

5. To navigate through the results list pages, perform one of the following:

   - To view the following page of search results, click **Next>**.
   - To return to the previous page of results, click **<Previous**.
   - To view the first page of search results, click **<<First**.
   - To view the last page of search results, click **Last>>**.

6. To select a profile to display on the Record Details page in the view mode, click the EUID of that profile.
7. To select multiple profiles to compare on the Record Details page, select the check boxes next to the EUIDs you want to compare, and then click **Compare**.
8. To return to the Search Results list from the Record Details page, click **Back**.
9. To perform a new search, click **Clear** in the search criteria section of the page.
10. To print the results in a report, click **Print Report**.

Selecting a Profile from the Results List

From the Record Details results list, you can select one object profile to view the detailed information for that profile, or you can select two profiles to compare the information in both profiles.

To Select a Profile to View

1. Perform a search for the object profiles you want to view.
2. To view detailed information for one object profile, click the EUID of that profile.

   The View or Edit page appears, displaying the person object for that profile.
3. To compare object profiles, select the **check boxes** to the left of each profile you want to compare, and then click **Compare Records**.

   The Record Details page appears, displaying a side-by-side comparison of the profiles.

Sorting the Results of Your Search

By default, the results of a search are sorted by EUID, but you can sort the results by any column in the search results list table.

To Sort the Profiles on the Search Result Page

1. Using one of the searches described in Searching for Object Profiles on the MIDM on page 3-1, perform a search for the object whose profile you want to access.
2. In the results list that appears, click a column heading to sort results in ascending order by that column.
3. Click that column heading again to sort the results in descending order.

Selecting Profiles to View as Comparisons

1. Search for the object whose profile you want to access. For information on how to search for the object, see Searching for Object Profiles on the MIDM on page 3-1.
2. Select up to four check boxes against the objects in the result page.

   You can make the selections from different pages of the results.
3. Click **Compare**.

   The Record Details page appears with each selected profile displayed.

4

Object Profile Views on the MIDM

This chapter helps you understand and look at the profile views. It includes the following sections:

Learning About Object Profile Views on the MIDM

Once you retrieve a search results list, you can view detailed information of an object, print summary information, compare object profiles, view merge transaction history for a profile, delete a source record, and view history of all transactions for a profile.

You can view object information in any of the following formats:

Object Profile Details on the MIDM

When you select a profile to view from the search results list, detailed information about the selected object appears on the Record Details page in the view mode. This page displays the SBR of the profile you selected on the left and summary information on the right side of the page. You can further expand the view to include all source records contained in the profile. Parent object information appears first followed by the data for each child object. From the Record Details page, you can perform several actions, such as viewing a transaction history for the object, viewing potential duplicate profiles, viewing merged transactions for the profile, deactivating the profile, updating object information, deleting the profile, and so on.

Source Record Details on the MIDM

You can view source record details from the following:

- Record Details page - You can view all source records for an object profile. You can also edit the source records belonging to a profile.

- Source Record page - You can search and view a specific source record. You can perform several actions against a source record, including adding, editing, deleting, deactivating or reactivating a source record, and merging two to four source records.

Object Profile and Source Record Comparisons

You can compare multiple object profiles by performing a EUID comparison lookup for the profiles to compare from the dashboard or by selecting multiple profiles in a search results list. The profiles are displayed in a side-by-side view or tabular format on the Record Details page. Once the profiles are displayed on the Record Details page, you can compare the source records of each object profile.

The Record Details comparison view lets you view the selected profiles in a side-by-side comparison with the differences between the profiles highlighted. You can compare the SBR of a profile with its own source records, and source records in one profile or between multiple profiles. This provides a complete comparison between object profiles and source records.

On the Source Record page, you can compare up to four source records from multiple profiles if they are all from the same source system.

Object Profile Transaction Histories

You can view a history of all transactions performed against object profiles either by performing a search for specific records as described in Searching for Object Profiles on the MIDM on page 3-1, or by performing a Transaction History search on the Transactions page as described in Viewing Transaction Histories on the MIDM on page 4-6. You can trace the events that modified an object profile from the time the profile is added to the master person index application to the most previous transaction, including merged and deactivated profiles.

The Transaction History page lets you view a side-by-side comparison of an object profile before and after a transaction occurred against that profile. You can also compare an SBR against an SBR, an SBR against a source record, and a source record against a source record. From associated Transaction History pages, you can unmerge the most recent merged profiles.

Object Profile Merge Histories on the MIDM

You can display a history of the merges that have affected a specific object profile. The merge history for a EUID or Local ID is available to view a transactions page for the specified SBR. The top level displays the EUID of the current active profile. The EUIDs at the second level indicate the profiles that are merged into the top-level EUID to form the top-level profile of the SBR. If there are Local IDs listed, they indicate profiles that are merged to form the profile above them. There may be several levels of merges displayed in the merge history of an object.

The right side of the page displays information about the merge transactions that involved the EUID that is selected in the EUID tree on the left. You can select a specific transaction to view a transaction history comparison for that merge transaction.

The Master Person Index Audit Log

The audit log lets you track and view all instances, in which information about the objects in the master person index application is accessed through the MIDM. If audit logging is enabled, an audit log entry is created each time the MIDM accesses database

tables that contain object information. The audit log keeps a record of each time the tables are accessed, along with the database function used to access the tables, the login ID of the user accessing the tables, the date and time the tables are accessed, and the EUIDs of the object profiles that are accessed. The audit log is enabled and disabled in the midm.xml file in the master person index project.

Viewing Object Information on the MIDM

The MIDM displays object profiles in a series of pages from which you can search, select, and view object profiles. You can view information associated with any of the SBR or source record components in an object profile. The SBR contains the most current and accurate information about that object from all external systems.

The source records associated with a profile contain information that is stored in the external systems that share information with the master person index application. The information in a source record may not match the information in the SBR. You can view information about an object in different ways, including the following:

- Viewing Object Profiles on the MIDM on page 4-3
- Viewing a Source Record on the MIDM on page 4-4
- Comparing Object Information on the MIDM on page 4-5
- Viewing Transaction Histories on the MIDM on page 4-6
- Viewing a Profile's Merge History on the MIDM on page 4-9
- Viewing the MIDM Audit Log on page 4-10

Viewing Object Profiles on the MIDM

The Record Details page displays object profiles in a series of pages from which you can select and view profiles. You can view information associated with any of the SBR or source record components in an object profile. The SBR contains the most current and accurate information about that object from all local systems.

To View an Object Profile

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to view on the Record Details page.
2. To view different types of information in the SBR for the displayed object, scroll through the visible data fields.
3. To view source records belonging to the profile, click  .

   All source records for the profile appear in a side-by-side comparison view.
4. From the Record Details page, perform any of the following functions.
   - To modify object information, click **Edit EUID** and follow the appropriate procedure under Modifying Profile Information on the MIDM on page 6-5.
   - To view a history of transactions for the displayed profile, click  .

     For more information, see Viewing Transaction Histories on the MIDM on page 4-6.
   - To deactivate a profile, click **Deactivate**. For more information, see Deactivating a Profile or Source Record on page 6-14.

- To delete a source record, click on the top-right corner of the source record.
- To view a merge history tree for the profile, click .

  A Transaction page with a merge tree on the left side of the screen and the merged transaction on the right side appears. This option is only available if the displayed profile is currently merged with another profile.

5. After viewing a profile, perform any of the following. The buttons you click are located at the top of the page.
   - To return to the search results list, click **Back**.
   - To look up another profile by EUID, enter the EUID in the field in the upper-left side and click **Search.**
   - To perform an advanced search for another profile, click **Advanced Search**.

Viewing a Source Record on the MIDM

The Source Record page displays source records in a series of search and view pages. You can view information associated with any of the SBR or source record components in an object profile. The source records associated with a profile contain the information that is stored in the external systems that share information with the master person index application. The information in the source records of an object may not match the information stored in the SBR of the object.

To View a Source Record

1. In the tabbed headings, click **Source Record**.
2. Click the **View/Edit** subtab, if it is not already selected.
3. In the **System** drop-down list, select the system from which the source record originated.
4. In the **Local ID** field, enter the local ID number for the source record you want to view.

   Note: If the Local ID field allows alphabetic characters, the search is case-sensitive.

5. Click **Search**.

   If the local ID is found, the source record fields appear in the view mode.

6. From the **Source Record View/Edit** page, perform any of the following functions.
   - To modify field values in the source record, click **Edit**, and follow the appropriate procedure in Modifying Profile Information on the MIDM on page 6-5.
   - To view the object profile that contains the displayed source record, click **View EUID**. For more information, see Viewing Object Profiles on the MIDM on page 4-3.
   - To deactivate the source record, click **Deactivate.**
   - To delete a source record, click **Delete.**

Comparing Object Information on the MIDM

The MIDM lets you compare two or more object profiles side-by-side to check for similarities and differences. You can also compare different components of the same object profile, and two or more source records from the same or different profiles.

Comparing Two or More Object Profiles

To compare two or more object profiles, you can either perform a EUID comparison lookup from the dashboard, or select multiple records from a Record Details search. From the resulting comparison page, you can compare the resulting profiles, and view the source records for the displayed profiles.

To Compare Two or More Object Profiles

1. Perform a search for the object profiles you want to compare, using one of the following methods:
   - If you know the EUIDs of the profiles you want to compare, look up the EUIDs from the dashboard as described in Performing a EUID Comparison Lookup on page 2-6.
   - If you do not know the EUIDs of the profiles to compare, perform a search on the Record Details page as described in Searching for Object Profiles on the MIDM on page 3-1. Select the check boxes next to the EUIDs to compare and click **Compare**.

     The records appear on the Record Details page in a side-by-side comparison view.
2. To view the source records for a displayed profile, click  .

   After viewing the source records for a profile, click  to return to the comparison view.
3. To view a transaction history for one of the displayed profiles, click  .

   After viewing the transaction history for a profile, click  to return to the comparison view.
4. To merge object information, click the EUIDs of the profiles you want to merge, and then click **Preview**. Follow the instructions in Merging Object Profiles on the MIDM on page 6-25.

Comparing Source Records From Object Profile Views

You can view the source records from one or more object profiles displayed on the Record Details page in either the view or comparison mode. This page does not provide merge functionality for source records. To merge source records, compare the records on the Source Record page as described in Viewing a Source Record on the MIDM on page 4-4.

To Compare Source Records From Object Profile Views

1. Perform a search for the object profile containing the source records you want to view, as described in Searching for Object Profiles on the MIDM on page 3-1.
2. In the search results list, select the EUIDs of the profiles you want to view, and click **Compare**.

   The Record Details page appears with SBR information displayed.
3. For each SBR whose source records you want to compare, click  .

The source record that belongs to the profile appears.

4. To edit any of the displayed source records, click **Edit EUID** and follow any of the procedures in Modifying Profile Information on the MIDM on page 6-5.
5. To merge source records in the displayed object profile, make a note of their local IDs, and follow the instructions in Merging Source Records on the MIDM on page 6-26.

Comparing Source Records From One Source System

To compare source records directly without accessing them from an object profile, you need to know the system and local ID numbers for the records. On the Source Record page, you can only compare records that originated from the same system.

To Compare Source Records From One Source System

1. In the tabbed headings, click **Source Record**.
2. Click the **Merge** subtab.
3. In the **Source** drop-down list, select the name of the source system from which the records you want to compare originated.
4. In the **Local ID** fields, enter one to four local IDs.

> **Note:** If any of the Local ID fields allows alphabetic characters, the search is case-sensitive.

5. Click **View Records**.

   Any matching source records appear side-by-side in a comparison view.
6. To view the object profile for one of the source records, click **View EUID** for that source record.

   This takes you to the Record Details page. To return to the Source Record comparison page, click **Back**.
7. To merge any of the displayed source records, see Merging Source Records on the MIDM on page 6-26.

Viewing Transaction Histories on the MIDM

Using the Transactions function, you can view historical information for a specific object, and compare the profile of the object before and after a specific transaction occurred to determine what information is modified. You can access the transaction history for a profile from the Record Details page, or for one or more profiles from the Transactions page.

When you display a transaction history from the Record Details page, all transactions for the displayed object profile appear in chronological order, with the earliest transaction on the left, and the most recent transaction on the right. When you display a transaction history record from the Transactions page, the image of the profile as it was before the transaction appears on the left side of the comparison page. The image on the right reflects the information of the object after the transaction occurred.

To View a Complete Transaction History for an Object Profile

1. Perform a search for the object profile whose history you want to view using one of the search procedures described in Searching for Object Profiles on the MIDM on page 3-1.
2. If necessary, select the profile to view from the search results list.

   The profile appears on the Record Details page.
3. Click  .

   A history of all transactions performed against the object profile appears.

To View Transaction History Records from the Transactions Page

You must obtain information about the object profile whose history you want to view, such as the EUID, a system in which the object is registered, or a specific transaction performed against the object's profile.

1. In the tabbed headings, click **Transactions.**
2. Enter values in any of the search fields as criteria. For more information about these fields, see Table 4–1.

   Note: The EUID field takes precedence over all other search fields on this page. You can only enter a Local ID as search criteria after entering the corresponding system. You can also search for all transactions related to all objects in a particular system by providing the system code.
3. Click **Search**.

   The Transaction History search results list appears with a list of matching transactions. For more information, see Table 4–1.
4. Click a transaction number of a result to view the transaction on the Transactions comparison page.

   Note: If you are viewing an unmerge transaction, the active record before unmerge is displayed on the left. The after-image of the two records that are unmerged during the transaction is displayed on the right.
5. To view the source records for either the before or after profile, click  .
6. If you are viewing a merge transaction that is not unmerged, you can unmerge the records here. For more information, see Unmerging Object Information on the MIDM on page 6-27.
7. To print the transactions, click **Print Report**.

About Transaction History Search Fields on the MIDM

The fields located on the Transaction History Search page lets you specify search criteria for the transactions you want to view. Note that the label for the Local ID field is customizable and may be changed for your implementation. The search page can also be configured to display additional transaction fields. Table 4–1 lists the fields that are defined by default for a transaction history search.

Table 4–1 Transaction History Search Fields

Field Name	Description
EUID	The enterprise-wide unique identifier of an object assigned by the master person index application.
System	The system in which the local ID is known.
Local ID	The local ID corresponding to the record you want to find and the system selected in the previous field. This field name may be different for your implementation.
From Date	The start date for the search. The query is performed for transactions that fall between the From Date and To Date.
From Time	The start time for the search using 24-hour notation. The query is performed for transactions that fall between the From Time and To Time on the specified dates. If no time is entered, the default value is 00:01 (12:01 AM).
To Date	The end date for the search.
To Time	The end time for the search using 24-hour notation. If no time is entered, the default value is 24:00.
System User	The login ID of the user who performed the transaction for which you are searching.
Function	The type of transaction that caused the object's profile to change. See Table 4–3 for more information about transaction types.

About Transaction History Results Fields on the MIDM

The fields located in the Transaction History search results list identifies a specific object profile and transaction to view. Additional fields may be added to this page by the system administrator. The Local ID labels are configurable and may be changed for your implementation.

Table 4–2 Transaction History Results Fields

Field Name	Description
Transaction No.	The sequential identification code of the transaction that caused the transaction history record.
EUID1	The enterprise-wide unique identification number of the first object profile involved in the transaction.
EUID2	The enterprise-wide unique identification number of the second object profile involved in the transaction, if appropriate.
System	The name of the system in which the transaction that created the history record occurred.
Local ID1	The local ID of the first source record involved in the transaction.
Local ID2	The local ID of the second source record involved in the transaction, if appropriate.
Function	The type of transaction that changed the object profile and caused the history record to be written. See Table 4–3 for a description of each transaction type.
System User	The login ID of the user who performed the transaction.
TimeStamp	The date and time the transaction occurred.

Transaction History Transaction Types on the MIDM

Each transaction performed by the master person index application is assigned a transaction type, indicating the type of action that is performed against the profile. Table 4–3 lists and describes each transaction type:

Table 4–3 Transaction Type Descriptions

Transaction Type	Description
Add	This transaction type is assigned when a new object profile is added to the database, whether it is through a direct add or through reversing an assumed match.
EUID Activate	This transaction type is assigned when a deactivated object profile is reactivated.
EUID Deactivate	This transaction type is assigned when an active object profile is deactivated.
EUID Merge	This transaction type is assigned when two object profiles are merged.
EUID Unmerge	This transaction type is assigned when two object profiles are unmerged.
SO Delete	This transaction type is assigned when a system object is deleted from the application.
System Record Merge	This transaction type is assigned when two source records are merged.
System Record Transfer	This transaction type is assigned when a source record is transferred from one object profile to another.
System Record Unmerge	This transaction type is assigned when two source records are unmerged.
Update	This transaction type is assigned when an object profile is modified in any way other than those described above. This includes such transactions as modifying an object profile, reversing an assumed match, deactivating or reactivating a source record, and adding or removing a child object (such as an address or telephone number).

Viewing a Profile's Merge History on the MIDM

When an object profile that is currently merged is displayed on the Record Details page, you can display a history of all merges performed against the profile, and trace the origin of certain information contained in the profile. The master person index application tracks all merges performed against each object profile in the database. You can view a history of merges that affect a specific object profile and view each EUID that is merged to form the final merge result profile. The merge history appears in a tree structure on the left side of the Transaction page. The right side of the page displays each pair of profiles that are merged for the selected merged transaction.

To View the Merge History of an Object

1. Using one of the search procedures described in Searching for Object Profiles on the MIDM on page 3-1, perform a search for the object whose merge history you want to view.
2. If necessary, select the object profile you want to view from the search results list.

   The Record Details page appears.
3. Under the SBR, click  .

A Transaction page with a merge tree on the left side of the screen and the merged transaction on the right side appears.

4. Expand the tree structure to view the EUIDs or LIDs that are combined to create the current record.
5. To view transaction information for any of the merge transactions, click any of the EUIDs involved in the transaction.

Viewing Merged Profiles for an Object Profile

If the profile you are viewing on the Record Details page is merged, you can view the merged profiles that are combined to create the currently displayed profile.

To View Merged Profiles for an Object Profile

1. Using one of the search procedures described in Searching for Object Profiles on the MIDM on page 3-1, perform a search for the object whose merge history you want to view.
2. If necessary, select the object profile you want to view from the search results list.

   The Record Details page appears.
3. Click **View Merged Records**.

   The profiles that are merged to create the current profile are displayed.

Viewing the MIDM Audit Log

Using the Audit Log function, you can view a record of each instance an MIDM user accessed information about any object in the master person index database. The audit log includes instances in which an object profile appeared in a search results list, viewed or compared, added, updated, deleted, or deactivated, and merged or unmerged. The system administrator can enable or disable the audit log.

Note: You must enable the MIDM Audit Log for it to function.

To View the Audit Log

You must obtain information about the instances you want to view such as, the EUID, a time frame when they occurred, the type of function that caused the audit log entries, the user who performed the functions, and so on.

1. In the tabbed headings, click **Audit Log.**
2. Enter values into any of the search fields as criteria. For more information about these fields, see About Audit Log Results Fields on the MIDM on page 4-11.

   Note: The EUID field takes precedence over all other search fields on this page. You can only enter a local ID as search criteria after you have entered the corresponding system.
3. Click **Search**.
4. On the Audit Log search results list, view the instances in which the data is accessed. For information about the fields displayed on this page, see About Audit Log Results Fields on the MIDM on page 4-11.

About Audit Log Search Fields on the MIDM

The fields located on the Audit Log Search page lets you enter search criteria about the audit log entries you want to view. These fields are configurable. Table 4–4 describes the fields that are displayed by default.

Table 4–4 Audit Log Search Fields

Field Name	Description
EUID	The object's enterprise-wide unique identifier assigned by the master person index application.
System	The system of the system in which the local ID is known.
Local ID	The local ID corresponding to the record you want to find and the system selected in the previous field. This field name might be different for your implementation.
From Date	The start date for the search. The query is performed for audit log entries that fall between the From Date and To Date.
To Date	The end date for the search.
From Time	The start time for the search using 24-hour notation. The query is performed for audit log entries that fall between the From Time and To Time on the specified dates. If no time is specified, the default value is 00:01 (12:01 AM).
To Time	The end time for the search using 24-hour notation. If no time is specified, the default value is 24:00.
System User	The login ID of the user whose transactions you want to view
Function	The type of transaction that created the audit log entries you want to view. For more information about transaction types, see Audit Log Functions on the MIDM on page 4-12.

About Audit Log Results Fields on the MIDM

The fields located on the Audit Log Result page display information about the instances in which object data is accessed, where those instances match the search criteria you entered. These fields are configurable. Table 4–5 describes the fields that are displayed by default.

Table 4–5 Audit Log Results Fields

Field Name	Description
Audit ID	The unique ID code in the audit log for the audit log entry.
EUID1	The EUID of the first object profile whose information was accessed.
EUID2	The EUID of the second object profile whose information was accessed in the same transaction (as in the case of a profile comparison or merge).
Function	The primary transaction type that is used to access information. For more information about transaction types, see Audit Log Functions on the MIDM on page 12.
Detail	Specific information about the actions taken against the profile such as, the MIDM page that is accessed or the type of function performed against a profile.
Create Date	The date and time that the information is accessed.
Create User	The login ID of the user who accessed the information.

Audit Log Functions on the MIDM

The audit log creates an audit entry whenever data is accessed through the MIDM. Table 4–6 lists and describes each audit log function. Some of these functions refer to the actual viewing of data on an MIDM page. Others refer to an action taken against that data, such as clicking the merge or unmerge Confirm button or resolving a potential duplicate pair.

Table 4–6 Audit Log Function Descriptions

Audit Log Function	Description
Add	A user added a new object profile to the database from the Create Source Record page or by reversing an assumed match.
Associated Potential Duplicates	A user viewed profile summaries on the Associated Records page of a potential duplicate search.
Assumed Match Comparison	A user viewed two assumed match profiles on the Assumed Match page.
Assumed Match Search Result	A user viewed the results of a search for assumed matches.
Auto Resolve or Resolve Permanently	A user permanently resolved two potential duplicate records on the Potential Duplicate Comparison page.
EO Comparison	A user viewed two object profiles on the Comparison page.
EO Search Result	A user viewed profile summaries on the Search Results page after performing a search for object profiles.
EO View/Edit	A user viewed an object profile on the View/Edit page.
EUID Merge Confirm	A user initiated a merge of two object profiles. This function refers to when the user views the merge result before clicking Confirm.
EUID Unmerge	A user finalized an unmerge of two object profiles.
EUID Unmerge Confirm	A user initiated an unmerge of two object profiles. This function refers to when the user views the unmerge result before clicking Confirm.
History Comparison	A user compared the before and after image of an object profile on the Transaction History Comparison page.
History Search Result	A user viewed the results of a transaction history search on the Transaction History Search Results page.
LID Merge - Selection	A user initiated a merge of two source records. This function refers to when the user has selected LID Merge but has not finalized the merge.
LID Merge Confirm	A user finalized a merge of two source records.
LID Unmerge	A user finalized an unmerge of two source records.
LID Unmerge Confirm	A user initiated an unmerge of two source records. This function refers to when the user views the unmerge result record before clicking Confirm.
Matching Review Search Result	A user viewed the results of a search for potential duplicates.
Merge	A user finalized a merge of two object profiles or two source records.
Merge Tree Comparison	A user viewed merge transactions using the merge tree. This function appears for each object profile included in the merge tree.

Table 4–6 (Cont.) Audit Log Function Descriptions

Audit Log Function	Description
Potential Duplicate Comparison	A user viewed two object profiles on the Potential Duplicate Comparison page.
Resolve or Resolve Temporary	A user resolved two potential duplicate records on the Potential Duplicate Comparison page.
SO Delete	A user performed the System Object Delete operation.
Undo Assumed Match	A user reversed an assumed match.
Unmerge Comparison	A user initiated an unmerge of two source records or two object profiles. This function refers to when the user views the unmerge result record before clicking Confirm.
Unresolve	A user changed the status of two object profiles on the Potential Duplicate Comparison page from Resolved to Unresolved.
Update	A user modified a profile on the View/Edit page. Updates include any changes made to a profile, including activating and reactivating source records, adding or removing child objects, and so on.
View Merge Tree	A user viewed a merge tree.

5

Object Profiles on the MIDM

This chapter provides step-by-step instructions to add object profiles to a master person index database. It includes the following section:

Adding an Object Profile and Creating a Source Record

When you add an object profile, you are creating a source record. When you create a source record, the master person index either adds the new record to the database or updates an existing record if a match is found. The master person index application calculates the SBR portion of the object profile when you commit the source record to the database.

Adding an object profile includes the following steps:

Step 1: Obtain Information about the Object

Before you add a new object to the master person index application, you must obtain certain information about the object. If necessary, review the fields displayed on the pages of the MIDM to learn what type of information you need to enter about the object. You must provide as much information available for each object.

Step 2: Specify a System and Local ID

Each object profile is associated with at least one source record. Before you add data to an object profile, you must specify the local ID of the object in a specific system. This creates the source record component of the object profile.

To Specify a System and Local ID

1. In the MIDM tabbed headings, select **Source Record**.

   The Source Record page appears.

2. Click the **Add** tab on the Source Record page.

3. In the **System** drop-down list, select the name of the source system from which the new record originated.
4. In the **Local ID** field, enter the local ID assigned to the new record by the specified system.

> **Note:** The name of the Local ID field may be modified for your use. For more information, contact your system administrator.

5. Click **Validate**.

   If the record does not exist, the page changes to display profile fields.

Step 3: Specify Parent Object Information

When you add a new object profile to the master person index database, you must enter certain information about the object. The required information varies depending on the type of objects in the index and the configuration of the application. An asterisk appears for mandatory field.

To Specify Parent Object Information

1. On the Source Record page, enter the details in the fields.
2. Click **Submit**.
3. Repeat steps 2 and 3 as needed.

Step 4: Specify Child Object Information

After specifying information for the parent object in the object profile, you can add child objects to the profile.

To Specify Child Object Information

1. On the Source Record page, scroll down until you see Add child_type, where child_type is the type of child object you want to add (for example, Add Address).
2. Click **Add child_type**.

   The page changes to display the fields associated with that child object type.
3. Enter the data for the child object.
4. Click **Save child_type**.
5. Repeat the above steps for each child object to add.

Step 5: Save the Object Profile

After specifying the required information for an object profile, save the profile to the database, else you may lose the information entered.

To Save the Object Profile

1. Scroll to the bottom of the page and click **Submit**.

Note: When the transaction completes, the MIDM returns to the initial Add page and a message displays whether a new profile is added to the database, a new profile is added and it has potential duplicates, or an existing profile is updated with the information you entered.

2. To add another source record, repeat the steps from Step 1: Obtain Information about the Object on page 5-1.

6

MIDM Maintenance Tasks

This chapter introduces you to the Master Index Data Manager maintenance tasks that include adding, editing, and deleting information, finding duplicate profiles, merging and unmerging profiles and records, and deactivating profiles and records. It also provides procedures on how to use the MIDM to perform these tasks and keep your master person index database accurate. It includes the following sections:

Learning About MIDM Maintenance Tasks

Object profile maintenance involves a number of tasks you can perform to ensure that your database contains the most current and accurate information. These tasks include editing, adding, and deleting information, detecting and fixing profiles that are potential duplicates of each other, merging and unmerging object profiles or source records, and deactivating object profiles or source records that are no longer active.

The following sections provide additional information to help you understand data maintenance tasks for the master person index application.

Matching Probability Weights

When you add a new object profile to the master person index application, the new profile is automatically checked for any similarities to profiles that already exist in the database. Matching probability weights between existing profiles and the new profile

are then calculated using matching algorithm logic. This weight indicates how closely two profiles match each other. If the matching probability weight for two profiles is above a specific number (defined in the master person index application configuration files), the profiles are considered to be potential duplicates. If the weight between two profiles is high enough, they are assumed to be a match and the existing profile is updated with the new information. For more information, see Assumed Matches on page 6-3.

Merging Profiles on the MIDM

You can merge object profiles that represent the same object, and merge source records within the same object profiles or between different object profiles. The source records you merge must be from the same source system. While merging, you can specify which fields from each record to retain in the final merged source record. After an object profile merge, all information from all source records involved in the merge is stored in the surviving profile. You may need to review the final merge result profile to determine which source records must be deactivated or merged (if any).

After an object profile merge, the SBR for the surviving profile is determined by the survivor calculator, taking into account all source records involved in the merge. If you merge profiles that have duplicate child objects (for example, each profile has an Office address), and the union survivor calculator is used, the most recently modified of the two child objects is stored in the SBR. After a source record merge, the SBRs for both object profiles are determined by the survivor calculator if both profiles are still active.

Surviving and Non-Surviving Profiles

You can perform an object profile merge on two to four object profiles. The *non-surviving profiles* are the profiles that are not retained after the merge. These profiles are also referred to as merged profiles. The *surviving profile* is retained after the merge. This profile is also referred to as the main profile. During an object profile merge, the source records in the non-surviving profiles are transferred to the surviving profile, and the non-surviving profiles are given a status of **Merged**. The SBR for the surviving object profile is recalculated based on the existing source records for that profile along with the newly merged source records. The EUID of the surviving profile is always retained. The information that is discarded during a merge is stored in the transaction table, making it possible to restore the profiles to their original EUIDs if they are merged in error. You can specify which profile to retain during a merge and select fields from the non-surviving source record to be retained in the surviving source record.

Source Record Merges

You can merge source records together only if they originated from the same external system. The source records can belong to the same object profile or different profiles. When the merge includes different object profiles, the profile from which the source record is merged is called the *merge from* profile. The object profile into which the source records are merged is called the *merge to* profile. If you merge the only active source record in one object profile into a source record in a different object profile, the merge from profile is deactivated (since there are no active source records remaining, it is not possible to create the SBR). During a source record merge, you can select fields from the non-surviving source record to be retained in the surviving source record.

Unmerging

If you merge object profiles or source records in error, you can unmerge the profiles or records, moving the information back into the original object profiles or source

records. Any modifications that are made to the surviving object profile or source record after the merge are retained after the profiles or records are unmerged. If a source record merge caused a **merge from** object profile to be deactivated, unmerging the source records reactivates that profile.

Assumed Matches

If you add a new object profile and the master person index application determines that the object you are adding already exists in the database, the master person index application assumes the profiles are a match and updates the existing object profile. This is known as an *assumed match*. An assumed match only occurs when the probability of a match between the new profile and the existing profile is above the match threshold specified by your system administrator. You can view assumed match transactions on the MIDM and reverse the match if needed. Reversing an assumed match creates a new object profile from the record that caused the assumed match and reverts the profile that is updated by the assumed match to its previous state.

Potential Duplicates

Potential duplicates are object profiles that possibly represent the same object. If you add a new object, and the master person index application determines that the object might already exist in the database, the profiles are listed as potential duplicates of one another. Profiles are listed as potential duplicates if the probability of a match between the two profiles is above the duplicate threshold but below the match threshold. Because object information is entered from various sources, an object profile may have several potential duplicates. In this case, it is important to identify the potential duplicates and to determine whether the profiles represent the same object.

Handling Potential Duplicates on the MIDM

The Duplicate Records function lets you locate any profiles that are similar enough that they could represent the same object. You can compare potential duplicate profiles side-by-side or tabular format to determine if they represent the same object. Once you have determined whether the profiles are duplicates, you can use one of the following methods to correct the potential duplicate listing.

Merge

If you conclude that the profiles represent the same object, you need to determine which EUID to retain and then merge the profiles. For a description of the merge process, see Merging Profiles on the MIDM on page 6-2.

Resolve

If you conclude that two potential duplicate profiles do not represent the same object, you can mark the profiles as being resolved. Performing this does not change any information for either profile, but it flags them as not being potential duplicates of one another. There are two methods of resolving potential duplicates.

- **Resolve or Resolve Until Recalculation** - This type of resolution lets the profiles be listed as potential duplicates again if one of the profiles is updated. After its potential duplicates are re-evaluated, the profiles still have a matching weight above the duplicate threshold.
- **Resolve Permanently** - This type of resolution marks the profiles as not being duplicates and does not let the pair be listed as duplicates after any future updates to either record. This is a permanent resolution.

Mark as Different Records

If the profiles represent different objects, you can mark them as different records.

Survivor Calculator Overrides

Every time a source record is updated, the survivor calculator determines whether the new information must be populated into the SBR. This includes updates from the MIDM and from local systems. When you update information in an object profile, you update the source record, which initiates the survivor calculator. The MIDM provides two methods to override the survivor calculator for the SBR. You can update the SBR directly and lock that field for editing, or you can link the value of an SBR field to the value of a source record field.

Linking Source Record Fields to the SBR

You can use MIDM to link the value of a specific source record field to the same field in the SBR. When you link an SBR and source record field, the value of the SBR field is always the same as the field in that source record. If the field value is subsequently updated in the source record, the changes are shown in the SBR. The link icon (for example, the open link) also appears in the system record The field values remain the same until the link is removed, at which point the survivor calculator immediately recalculates the best value for the field based on the source records in the profile. You can only link SBR and source record fields in the parent object and only if you have explicit security permissions to do so.

Linking Field Values in the SBR

When you update an SBR field directly, the link icon to the database must be closed for you to add your changes. After you make changes, open the link icon to prevent an SBR field from being updated by any source record changes or by the survivor calculator. When a field has an open link, the survivor calculator immediately recalculates the best value for that field based on the source records in the profile.

Note: Use this capability cautiously, since fields updated in the SBR cannot be overwritten by new information from local systems until you close the link icon, which lets you overwrite the information. You can only update an SBR and overwrite parent object fields, only if you have explicit security permissions to do so.

Note: A closed link indicates an unlinked field that can be linked. An open link indicates a linked field that can be unlinked.

Concurrent Users on the MIDM

If you have the same object profile open for editing as another MIDM user, only the user who commits their changes first can save their changes. If you try to commit changes after the first user clicks **Commit**, an error message appears and you will be unable to commit your changes. To update the profile with your changes, you must reload the profile by performing a search for that profile. You can then edit the profile and commit your changes.

Modifying Profile Information on the MIDM

Once an object profile is added to the master person index application, you can modify information about that object, update the SBR of the object, add or delete source records to or from the profile, or change the status of a source record or object profile. If you make any of these modifications, the survivor calculator determines what changes, if any, must be made to the SBR. You can only modify the SBR directly if you have access permission to do so.

Perform any of the following tasks to update profile information:

Modifying Information in an Object Profile

If the information for an object profile changes, you can update the information in either the SBR or the affected source record. If you update the source record, the survivor calculator determines what changes, if any, must be made to the SBR. You must have overwrite permissions to update the SBR directly. If you know the local ID and system of the source record you want to modify, you can access the source record directly, as described in Modifying Information Directly in a Source Record on page 6-7.

Perform any of the following tasks to modify information in an object profile:

Modifying Parent Object Information in a Profile

The Record Details page has an edit mode, where you can modify field values in the displayed object profile.

To Modify a Parent Object in a Profile

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to modify on the Record Details page.
2. Click **Edit EUID**.
3. To update the SBR, perform the following:
   - For each field in the parent object you want to modify, click the **padlock** icon to the left of the field to modify, and then modify the value of the field.
   - Click **Update** *parent_object* under the fields you modified (where, *parent_object* is the name of the parent object.

Note: You can only modify SBR fields directly if you have permissions to do so.

4. To update a source record, modify the parent object fields in any of the displayed system objects.
5. After modifying information, click **Update** *parent_object* (where, *parent_object* is the name of the parent object).
6. Click **Save** at the bottom of the page, and click **OK** on the information dialog box that appears.

   The page refreshes and if you have modified a source record, the SBR is recalculated based on the new information.

Adding a Child Object to an Object Profile

If additional information becomes available about an object, you need to add a new child object to the object profile. For example, if additional address information becomes available, you need to add a new address record to the affected source record. You cannot add a child object to the SBR.

To Add a Child Object to an Object Profile

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to modify on the Record Details page.
2. Click **Edit EUID**.
3. Click **View** *child_type* in the column containing the source record you want to modify.

   For example, to add an address record, select **View Addresses**.
4. In the empty field, enter the new information for the child object.
5. Below the updated record, click **Save** *child_type*.
6. Scroll to the bottom of the page and click **Save**.
7. Click **OK** on the information dialog box that appears.

   The page refreshes and the SBR is recalculated based on the new information.

Modifying a Child Object in a Profile

If information about a child object changes, you may need to modify information for an existing child object. You cannot modify information in child object in the SBR.

To Modify a Child Object in a Profile

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to modify on the Record Details page.
2. Click **Edit EUID**.
3. In the source record you want to modify, click **View** *child_type*, where *child_type* is the name of the child object type you want to modify. For example, to modify an address record, select **View Addresses**.

Empty child object fields appear along with a list of existing child objects of the selected type.

4. In the child object list, click the **pencil** icon next to the child object you want to modify.

   The field values for the selected child object are populated into the child object fields.

5. Modify any fields for the child object.
6. Below the updated record, click **Save** *child_type*.
7. Scroll to the bottom of the page and click **Save**.
8. Click **OK** on the information dialog box that appears.

   The page refreshes and if you have modified a source record, the SBR is recalculated based on the new information.

Deleting a Child Object From a Profile

If a child object is entered incorrectly or becomes obsolete, you can delete the object from the affected object profile. Child objects cannot be deleted from the SBR. Deleting a child object cannot be undone.

To Delete a Child Object

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to modify on the Record Details page.
2. Click **Edit EUID**.
3. Click **View** *child_type* in the source record you want to modify, where *child_type* is the name of the child object type you want to delete. For example, to delete an address record, select **View Addresses**.

   Empty child object fields appear along with a list of existing child objects of the selected type.

4. In the child object list, click the **delete (X)** icon next to the child object you want to modify.
5. Scroll to the bottom of the page and click **Save**.
6. Click **OK** on the information dialog box that appears.

   The page refreshes and if you have modified a source record, the SBR is recalculated based on the new information.

Modifying Information Directly in a Source Record

If the object information for a specific source record changes, you can update the information by accessing either the object profile or the affected source record. If you update the source record, the survivor calculator determines what changes, if any, must be made to the SBR. This section describes how to modify information by accessing the source record directly. For information about modifying an object profile, see Modifying Information in an Object Profile on page 6-5.

Perform any of the following tasks to modify information in a source record directly:

- Modifying the Parent Object in a Source Record on page 6-8
- Adding a Child Object to a Source Record on page 6-8

- Modifying a Child Object in a Source Record on page 6-9
- Deleting a Child Object From a Source Record on page 6-9

Modifying the Parent Object in a Source Record

If parent object for a particular source record changes, you can update the source record directly on the Source Record page.

To Modify the Parent Object in a Source Record

1. In the MIDM tabbed headings, click **Source Record**.
2. If necessary, click the **View/Edit** subtab.
3. In the **System** drop-down list, select the name of the system for the source record you want to modify.
4. In the **Local ID** field, enter the local ID for the record you want to modify.
5. Click **Search**.

   If a matching source record is found, it appears on the Source Record page in the view mode.
6. Click **Edit**.
7. Modify the parent object fields in the upper portion of the page.
8. Scroll to the bottom of the page and click **Save.**
9. Click **OK** on the information dialog box that appears.

   The page refreshes and if you have modified a source record, the SBR is recalculated based on the new information.

Adding a Child Object to a Source Record

If additional information becomes available about an object, you need to add a new child object to a source record. For example, if additional address information becomes available, you need to add a new address record to the affected source record.

To Add a Child Object to a Source Record

1. In the MIDM tabbed headings, click **Source Record**.
2. If necessary, click the **View/Edit** subtab.
3. In the **System** drop-down list, select the name of the system for the source record you want to modify.
4. In the **Local ID** field, enter the local ID for the record you want to modify.
5. Click **Search**.

   If a matching source record is found, it appears on the Source Record page in the view mode.
6. Click **Edit**.
7. Click **View** *child_type*, where *child_type* is the name of the type of child you want to add.

   The child object section expands to display empty fields for the object.
8. Enter information into the empty child object fields.
9. Click **Save** *child_type*.

10. After adding information, click **Save** at the bottom of the page.
11. Click **OK** on the information dialog box that appears.

    The page refreshes and if you have modified a source record, the SBR is recalculated based on the new information.

Modifying a Child Object in a Source Record

If information about an object changes, you may need to modify information for an existing child object. You can make those changes on the Source Record page.

To Modify a Child Object in a Source Record

1. In the MIDM tabbed headings, click **Source Record**.
2. If necessary, click the **View/Edit** subtab.
3. In the **System** drop-down list, select the name of the system for the source record you want to modify.
4. In the **Local ID** field, enter the local ID for the record you want to modify.
5. Click **Search**.

   If a matching record is found, it appears on the Source Record page in the view mode.
6. Click **Edit**.
7. Click **View** *child_type*, where *child_type* is the name of the type of child you want to modify.

   The child object section expands to display empty fields for the object along with a list of existing child objects.
8. Click the **pencil** icon next to the child object you want to modify.

   The child object fields are populated with the values from the child object you selected.
9. Modify any of the child object fields.
10. Click **Update** *child_type*.
11. After modifying information, click **Save**.
12. Click **OK** on the information dialog box that appears.

    The page refreshes and if you have modified a source record, the SBR is recalculated based on the new information.

Deleting a Child Object From a Source Record

If a child object is entered incorrectly or becomes obsolete, you can delete the object from the affected source record. Deleting a child object cannot be undone.

To Delete a Child Object From a Source Record

1. In the MIDM tabbed headings, click **Source Record**.
2. If necessary, click the **View/Edit** subtab.
3. In the **System** drop-down list, select the name of the system for the source record you want to modify.
4. In the **Local ID** field, enter the local ID for the record you want to modify.

5. Click **Search**.

   If a matching record is found, it appears on the Source Record page in the view mode.

6. Click **Edit**.

7. Click **View** *child_type* (where, *child_type* is the name of the type of child you want to delete).

   The child object section expands to display a list of existing child objects.

8. Click the **delete (X)** icon next to the child object you want to modify.

9. After modifying information, click **Save**, and then click **OK** on the information dialog box that appears.

   The page refreshes and the SBR of the object profile is recalculated based on the new information.

Overwriting SBR Field Values

Locking an SBR field for overwrite ensures that the value for that field is not recalculated by the survivor calculator each time the object profile is updated. If you determine that a value in the SBR is the most accurate data and must not be updated, you can lock the field, and no updates can be made to that SBR field by the survivor calculator until it is unlocked. If you unlock a locked field, the value of that field is automatically recalculated by the survivor calculator once the unlock action is committed. Parent and child object fields can be locked.

Locking an SBR Field

When you lock a field in an SBR, that field can only be updated through the MIDM by a user who has overwrite permissions. Locking a field in the SBR removes the survivor calculator from the update process for that field, and any updates made to or by source records will not update the locked fields in the SBR. You can lock fields in the parent and child objects.

To Lock a Field in the SBR

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile containing the field you want to lock on the Record Details page.

2. Click **Edit EUID**.

3. Scroll to the SBR field you want to lock. Parent and child object fields can be locked.

4. If necessary, change the value of the field to be locked.

5. Click the **padlock icon** to the left of the field.

   Note: A closed padlock indicates an unlocked field that can be locked. An open padlock indicates a locked field that can be unlocked.

6. Click **OK** on both dialog boxes that appear.

7. Click **Save** at the bottom of the page, and then click **OK** on the confirmation dialog box.

The field is now locked and cannot be edited by updates to source records until the lock is removed. The link icon is also removed since a locked field cannot be linked to a source record field.

Unlocking an SBR Field

Once you unlock a field for overwrite in an SBR, the SBR is recalculated by the survivor calculator, and the field can be updated by changes made to source records.

To Unlock an SBR Field

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile containing the field you want to unlock on the Record Details page.
2. Click **Edit EUID**.
3. Scroll to the SBR field you want to unlock.
4. Click the **unlocked padlock** icon to the left of the field.

   Note: A closed padlock indicates an unlocked field that can be locked. An open padlock indicates a locked field that can be unlocked.

5. On both dialog boxes that appear, click **OK.**
6. Click **Save** at the bottom of the page, and then click **OK** on the confirmation dialog box.

   The field is now unlocked and can be edited by updates to source records. The link icon appears next to the field indicating that the field can be linked to a source record field.

Overriding the SBR of the Survivor Calculator

Linking an SBR field to a field in a source record ensures that the value for that field is not recalculated by the survivor calculator each time the object profile is updated. If you determine that a value in a specific source system is the most accurate data and must always be used in the SBR, you can link the field values and override the survivor calculator's version of the SBR.

If you unlink a linked field, the value of that field is automatically recalculated by the survivor calculator once the unlink action is performed. You can link field values from the parent and child objects.

Linking an SBR Field to a Specific Source Record

When you link a field in an SBR to a field in one of the profile's source records, the value of the field is always equal to the value of the field in the source record, even when the source record field is updated. Linking a field in the SBR to a source record removes the survivor calculator from the update process for that field. Any updates made to or by other source records in the profile will not update the linked field in the SBR. Use linking if the field value from a specific source record is most accurate and current value. You cannot link an SBR field if it is locked for editing.

Linked fields in an object profile are indicated by the link icons to the left of the fields in the source record. All other fields have the link icon in the SBR.

To Link an SBR Field to a Source Record Field

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile containing the field you want to link on the Record Details page.
2. Click **Edit EUID**.
3. Scroll to the SBR field you want to link.
4. Click the **chain-link** icon to the far left of the field.

   A pop-up window appears where you can specify the source record to link.

   Note: A closed link indicates an unlinked field that can be linked. An open link indicates a linked field that can be unlinked.

5. On the pop-up window, select the source system code and the local ID of the source record to which you want to link the selected field.
6. Click **OK** on the dialog boxes that appear.
7. Click **Save** and then click **OK** on the confirmation dialog box.

   The link icon moves from the SBR field to the source record field and the link icon is removed (because a field cannot be both linked and unlinked). The SBR field is now linked and can only be edited by updates to the source record to which it is linked.

Unlinking an SBR Field From a Source Record

Once you unlink a field in the SBR from the corresponding field in the source record, the SBR is recalculated by the survivor calculator, and the field can be updated by changes made to other source records. An SBR with no fields linked are indicated by all link icons next to the SBR fields (in the column below the red arrow).

To Unlink an SBR Field From a Source Record

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile containing the field you want to unlink on the Record Details page.
2. Click **Edit EUID**.
3. Scroll to the field you want to unlink.
4. Click the **chain-link** icon to the left of the field in the source object.
5. Click **OK** on both dialog boxes that appear.
6. Click **Save** at the bottom of the page, and then click **OK** on the confirmation dialog box that appears.

   The icon is moved from the source record field to the SBR field that is no longer linked. The SBR is recalculated by the survivor calculator.

Adding a Source Record to an Object Profile

If an object has local IDs in addition to those already recorded in the master person index application, you can add the local IDs to the object's profile by adding a source record to the profile.

To add a local ID to an object profile, you need to specify information such as, the system that assigned the local ID, certain parent object information, and the local ID

itself. When you add a source record to an object profile, the survivor calculator determines what changes, if any, must be made to the SBR.

You cannot add a new local ID and system pair to an object profile if that same local ID and system pair already exists in another object profile.

To Add a Source Record to an Object Profile

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to modify on the Record Details page.
2. Click **Edit EUID**.
3. At the bottom of the page, click **Add SO**.

   A new column appears to the right of the existing records to add the new source record.
4. Enter the system and local ID for the new source record, and then click **Validate**.

   If no existing record matches the system and local ID you entered, and the local ID is of a valid format, a validation succeeded message appears.
5. Enter information in the parent object fields.
6. For each child object to add, perform the following:
   a. Click **Add** *child_type* in the column containing the new source record.

      For example, to add an address record, select **Add Addresses**.
   b. Enter the new information for the child object.
   c. Below the child object you updated, click **Save** *child_type*.
7. Scroll to the bottom of the column and click **Save**.
8. Click **OK** on the dialog box that appears.
9. At the bottom of the page, click **Save.**
10. Click **OK** on the dialog box that appears.

    The page refreshes and the SBR is recalculated based on the new information.

> **Note:** You only need to enter required fields to save the new source record. Required fields are indicated by an asterisk (*).

To Delete a Source Record from an Object Profile

You can delete a source record from an object profile by performing one of the following:

- Deleting a Source Record Using the Record Details Tab on page 6-13
- Deleting a Source Record Using the Source Record Tab on page 6-14

Deleting a Source Record Using the Record Details Tab

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to modify on the Record Details page.
2. Click **Edit EUID** or  .

3. At the top-right corner of the column for the source record that you want to delete, click ✕.

   The Confirmation dialog box appears.

4. Click **OK** on the dialog boxes that appear.

Deleting a Source Record Using the Source Record Tab

1. In the tabbed headings, click **Source Record**.
2. Click the **View/Edit** subtab if it is not already selected.
3. In the **System** drop-down list, select the system from which the source record originated.
4. In the **Local ID** field, enter the local ID number for the source record you want to view.

   Note: If the Local ID field allows alphabetic characters, the search is case-sensitive.

5. Click **Search**.

   If the local ID is found, the source record fields appear in the view mode.

6. Click **Delete.**

Deactivating a Profile or Source Record

If an object profile or source record is no longer active, you can either delete the profile or deactivate it. Once you deactivate a record, you can reactivate it if needed. Deactivating an object profile removes the potential duplicate listings for that profile. If you deactivate a source record, the survivor calculator determines what changes, if any, must be made to the SBR.

Deactivating an Object Profile

Deactivated profiles cannot be modified, and in some cases, cannot be viewed. If you deactivate a profile in error, you can reactivate it if needed.

To Deactivate an Object Profile

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to deactivate on the Record Details page.
2. Click **Deactivate**.

   The profile is deactivated in the database and the EUID appears on the MIDM screen.

Deactivating a Source Record

If an existing local ID for an object becomes obsolete, you can deactivate the source record with that local ID for the object profile. An object profile must have at least one active local ID. If you deactivate an object's last active source record, the entire profile is deactivated. When you deactivate a source record from an object profile, the survivor calculator determines what changes, if any, must be made to the SBR.

You can deactivate a source record from the Record Details page, where you can view the source record within the context of its profile.

To Deactivate a Source Record (by EUID)

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile containing the source record you want to deactivate on the Record Details page.
2. Click **Edit EUID**.
3. Below the source record you want to deactivate, click **Deactivate**.
4. Click **OK** on the information dialog box that appears.

   The page refreshes and the SBR for the object profile containing the source record is recalculated based on the new information.

Reactivating a Profile or Source Record

Once an object profile or source record is deactivated, you can reactivate it if needed. Reactivating a profile causes the potential duplicates for the profile to be recalculated. Reactivating a source record causes the SBR to be recalculated.

Reactivating an Object Profile

If an object profile is deactivated in error or becomes active again, you can reactivate that profile. Reactivating a profile returns the profile to its status before it was deactivated.

To Reactivate an Object Profile

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile you want to reactivate on the Record Details page.
2. Click **Activate.**
3. Click **OK** on the information dialog box that appears.

   The profile is reactivated in the database.

Reactivating a Source Record

If a source record was deactivated in error or is no longer active, you can reactivate the source record. You can activate the source record from the Record Details page, where you can view the source record within the context of its profile.

To Reactivate a Source Record (by EUID)

1. Using one of the search methods described in Searching for Object Profiles on the MIDM on page 3-1, display the object profile containing the source record you want to deactivate on the Record Details page.
2. Click **Edit EUID**.
3. Below the source record you want to deactivate, click **Activate**.
4. Click **OK** on the information dialog box that appears.

   The page refreshes and the SBR for the object profile containing the source record is recalculated based on the new information.

Working with Potential Duplicate Profiles on the MIDM

The Duplicate Records function of the MIDM lets you view any object profiles that are marked as potential duplicates of each other by the master person index application. You can search and view potential duplicate profiles on the MIDM, and then fix the potential duplication by either merging or resolving the two profiles. You can view potential duplicates that are resolved, but not those that are merged.

Perform any of the following tasks to monitor and fix potential duplicate profiles.

Finding Potential Duplicate Profiles on the MIDM

Potential duplicate profiles are determined based on the matching probability weight that indicates how closely two profiles match. You can find and compare potential duplicate profiles using the MIDM Duplicate Record function.

To Find Potential Duplicates

1. Obtain information about the object whose potential duplicates you want to view such as, a system in which they are registered, or the login ID of the user who created the object profile.
2. In the MIDM tabbed headings, click **Duplicate Records**.

   The Duplicate Records basic search page appears.
3. Perform one of the following:
   - To search by date range only, enter the date range in the basic search fields, and then click **Search**.
   - To search by system only, select the system code from the drop-down list, and then click **Search**.

     This provides all the potential duplicate records that are generated by the selected source system.
   - To use additional criteria for the search, select **Advanced Search** from the Search Type field, enter your search criteria, and then click **Search**.

     For more information about advanced search fields, see About Duplicate Records Search Fields on the MIDM on page 6-17.

     The Duplicate Records results list appears with key information for each potential duplicate record displayed.
4. In the results list, compare the displayed information to determine whether you want to view a detailed comparison of the potential duplicate profiles.

   You can configure the result list in the tabular format.
5. To view a detailed comparison for a set of potential duplicate profiles, click **Preview** to the right of the profiles.
6. To view the source records associated with any of the displayed profiles, click  .

   To return to the duplicate record comparison view, again click  .

7. To view a transaction history for a displayed profile, click .

   To return to the comparison page, again click .

8. To mark a profile as not duplicate of the main profile, see Resolving Potential Duplicate Profiles on the MIDM on page 6-20.

9. To merge two or more profiles, see Merging Potential Duplicate Profiles on page 6-19.

10. To start a new search for potential duplicate records, click **Advanced Search** at the top of the page.

About Duplicate Records Search Fields on the MIDM

The fields located on the Duplicate Records search page lets you specify information about the potential duplicate profiles you want to view.

Table 6–1 Duplicate Records Search Fields

Field Name	Description
EUID	The enterprise-wide unique identification number of one of the profiles you want to view.
System	The external system with which the object profile that caused the potential duplicate flag is associated.
Local ID	The local ID associated with the object profile in the specified system. The name of this field may be different for your implementation.
Create Date From	The start create date for the profiles you want to view. The query is performed for transactions that are created between the Create Date From (and Create Time From) and the To Create Date (and To Create Time).
To Create Date	The end create date for the profiles you want to view.
Create Time From	The start create time for the profiles you want to view (using 24-hour notation). If no time is entered, the default value is 00:01 (12:01 AM).
To Create Time	The end create time for the profiles you want to view (using 24-hour notation). If no time is entered, the default value is 24:00.
Status	The potential duplicate status of the profiles you want to view. The values for this field are Unresolved, Resolved, or Permanently Resolved.

Understanding the Types of Merges on the MIDM

There are two types of merges in master person index, a EUID merge and an Local ID merge.

EUID Merges

A EUID merge is performed between two enterprise objects, EUID1 and EUID2. This type of merge is MPI wide, which means that it is directed by knowledge that is only known outside the given hospital or clinic. For example,

Hospital 1 has a patient named John Smith (Local ID 123456) and Hospital 2 has a patient named John Smyth (Local ID 147258). In the MPI database, these records are given EUIDs as follows:

- John Smith (Hospital 1; Local ID 123456) is assigned EUID1 0000000128

- John Smyth (Hospital 2; Local ID 147258) is assigned EUID2 0000012457

In theory, these hospitals do not know anything about the other patients, and the MPI evaluates them and recommends one of the following:

- The patients are two different people as described in this example.
- Their demographics are close enough that a human needs to evaluate them (potential duplicate).
- The first record is updated with information from the second record as an assumed match. In this example, this is not the case since the records are given different EUIDs.

If a human has decided that these patients are the same person, at the MPI level, a merge of EUID1 may be made into EUID2. This information is broadcast to the two hospitals to know the set of medical records that is common to their patient, but the merge remains with the MPI.

The processing for this merge at the MPI level is:

- EUID1 receives a status of *Merged*.
- The system record from EUID1 is transferred to EUID2, leaving EUID1 without a system object
- EUID2 (0000012457) now have two active system records:
  - Local ID 147258
  - Local ID 123456

Local ID Merges

A local ID merge can have different origins, but is focused within a single hospital, and has more than one scenario as follows:

Scenario 1

Jane Doe checks into the hospital with a Local ID 963852. The information is sent to the MPI and EUID is assigned:

- Jane Doe (Local ID 963852) is assigned EUID3/0000065412

After marriage, Jane Doe changes her name to Jane Brown. She checks into the same hospital with the Local ID 333555. The information is sent to the MPI and an EUID is assigned:

- Jane Brown (Local ID 333555) is assigned EUID4/0000005623

The hospital discovers that these two Local IDs (963852 and 333555) belong to the same patient. They combine the records into a single file with a single local ID (for example, 333555) and notify the MPI. At the MPI level, a local ID merge is triggered by two Local IDs that are identified by the hospital.

The processing for this merge at the MPI level is as follows:

- Local ID 963852 and Local ID 333555 are sent to the MPI and EUID3 and EUID4 are identified.
- A Local ID merge is performed.
- The Local ID from EUID3 is transferred to EUID4.
- EUID3/0000065412 is deactivated.
- The Local ID from EUID3 (963852) is deactivated.

- EUID4/0000005623 now has two system records:
  - Local ID 333555 (active)
  - Local ID 963852 (deactivated)

> **Note:** The MIDM performs field level selections as to which data remains from the merge. For OHMPI, all data will come from one record.

Scenario 2

The second scenario is similar, but arises from a different set of inputs.

Paul Black checks into the hospital with a Local ID 444999. The information is sent to the MPI and an EUID is assigned:

- Paul Black (Local ID 444999) is assigned EUID5/0000226541

Paul Black checks into the hospital again, with a different Local ID (222777), but is identified with the same MPI EUID5/0000226541. This results in the following EUID5 record:

- EUID5/0000226541
  - Local ID 222777 (active)
  - Local ID 444999 (active)

The hospital consolidates the two Local IDs (222777 and 444999) that belong to the same patient. They combine the records into a single file with a single Local ID (for example, 222777) and notify the MPI. At the MPI level, this is a straight Local ID merge identified by the hospital.

The processing for this merge at the MPI level follows:

- Local ID 444999 and Local ID 222777 are sent to the MPI and EUID5 is identified.
- A Local ID merge is performed.
- The Local ID 444999 is deactivated.
- EUID5 now has two system records:

  EUID5/0000226541:
  - Local ID 222777 (active)
  - Local ID 444999 (deactivated)

> **Note:** The MIDM performs field level selections as to which data remains from the merge. For OHMPI, all data comes from one record.

Merging Potential Duplicate Profiles

When you compare potential duplicate profiles, you may find that the object profiles represent the same entity, or that a source record from one profile belongs to the other profile. You can perform either an object profile merge or a source record merge to correct this. When you merge profiles, the SBR of the surviving profile is automatically recalculated based on the source records involved in the merge. You can combine up to four profiles.

This section only describes object profile merges. For more information about merging object profiles, see Combining Object Information on the MIDM on page 6-25. To learn how to merge source records, see Merging Source Records on the MIDM on page 6-26.

To Combine Duplicate Profiles From the Comparison Page

1. Perform a search for potential duplicates on the Duplicate Records page as described in Finding Potential Duplicate Profiles on the MIDM on page 6-16.
2. To view a detailed comparison for a set of potential duplicate profiles, click **Preview** to the right of the profiles.
3. On the Duplicate Records comparison page, determine which of the displayed profiles you want to keep, and then click the EUID of that profile.
4. Click the EUIDs of any other associated profile you want to merge into the profile you selected above.

   Each profile changes color to indicate it is selected.
5. Under the far right column, click **Preview**.

   The merge preview profile appears, which lets you view the profile as it appears after the merge.
6. Compare the field values in the profiles to be merged to determine which values to populate into the kept profile. Click any values you want to keep.

   Note: Selecting a value to keep in the merge result profile creates a link from the SBR to the source record field that populated the field.

   For example, if the first name field from Record A is populated from Source Record 1, and you merge Record A into Record B, and select the first name value from Record A, a link is created from the first name field in the resulting SBR to the first name field in Source Record 1. For more information on linking SBR fields to source record fields, see Overriding the SBR of the Survivor Calculator on page 6-11.
7. Review the merge preview profile and click **Merge** to finalize the merge.
8. On the confirmation dialog box that appears, click **OK**.

   The surviving profile appears.
9. Review the surviving object profile to determine whether to merge any source records or deactivate.

Resolving Potential Duplicate Profiles on the MIDM

When you compare two potential duplicate profiles and determine that they do not represent the same object, you can resolve the two profiles to flag the profiles as not being potential duplicates. There are two types of resolution.

- *Resolve* - Removes a potential duplicate flag, but if one of the resolved profiles is updated, the records might be listed as potential duplicates again.
- *Resolve Permanently* - Flags the two profiles as being permanently resolved regardless of whether one of the resolved profiles is updated.

To Resolve Potential Duplicate Profiles from the Results List

If the fields on the Duplicate Records search results list are sufficient to determine that two profiles do not represent the same object, you can resolve the profiles from the search results list.

1. Perform a search for potential duplicates on the Duplicate Records page as described in Finding Potential Duplicate Profiles on the MIDM on page 6-16, and display the results list.

   The results list displays key identification fields that provide enough information to determine whether the profiles must be resolved.

2. Scroll through the results until you see the profiles you want to resolve.
3. To resolve the duplicate profile from the Main EUID (the profile in the far left column), click  .
4. On the confirmation dialog box that appears, perform one of the following:
   - To flag the potential duplicate profiles as resolved but still allow the potential duplicate listing to be reinstated in the future, select **Resolve Until Recalculation**.
   - To flag the potential duplicate profiles as resolved and never allow the potential duplicate listing to be reinstated, click **Resolve Permanently**.
5. On the confirmation dialog box, click **OK**.

   The status of the potential duplicate entry is changed to Resolved and the profiles are no longer regarded as potential duplicates of one another.

6. Repeat this for each duplicate profile you want to resolve from the main profile.
7. If you resolve a profile in error, click  in the results list to mark it as a potential duplicate again.

To Resolve Potential Duplicate Profiles from the Comparison Page

If you want to view detailed information about two profiles to determine whether they are a match, view them on the Duplicate Records comparison screen before you resolve them.

1. Display a set of potential duplicates on the Duplicate Records comparison page as described in Finding Potential Duplicate Profiles on the MIDM on page 6-16.
2. To resolve the duplicate profile from the Main EUID (the profile in the far left column), click  .
3. On the confirmation dialog box that appears, perform one of the following:
   - To flag the potential duplicate profiles as resolved but still allow the potential duplicate listing to be reinstated in the future, select **Resolve Until Recalculation**.
   - To flag the potential duplicate profiles as resolved and never allow the potential duplicate listing to be reinstated, click **Resolve Permanently**.
4. On the confirmation dialog box, click **OK**.

   The status of the potential duplicate entry is changed to Resolved and the profiles are no longer possible duplicates of one another.

5. Repeat this for each duplicate profile you want to resolve from the main profile.

6. If you resolve a profile in error, click  in the results list to mark it as a potential duplicate again.

Unresolving Potential Duplicate Profiles on the MIDM

If two profiles are resolved and flagged as not potential duplicates in error, you can undo the resolve transaction, and mark them as potential duplicates. You can perform this from either the results list or the comparison page.

To Unresolve Potential Duplicate Profiles From the Results List

If the fields on the Duplicate Records search results list are sufficient to determine that a resolve transaction is performed in error, you can unresolve the profiles in the search results list.

1. Perform a search for potential duplicates on the Duplicate Records page as described in Finding Potential Duplicate Profiles on the MIDM on page 6-16, and display the results list.

   The results list displays key identification fields that provide enough information to determine whether the profiles must be unresolved.

2. Scroll through the results until you see the profiles you want to unresolve.
3. To mark the profile as duplicate with the Main EUID (the profile in the far left column), click  .

   The status of the potential duplicate entry is changed from Resolved and the profiles are again potential duplicates of one another.

To Unresolve Potential Duplicate Profiles From the Comparison Page

If you want to view detailed information about two profiles to determine whether they must be unresolved, view them on the Duplicate Records comparison screen.

1. Display a set of potential duplicates on the Duplicate Records comparison page as described in Finding Potential Duplicate Profiles on the MIDM on page 6-16.
2. To mark the profile as duplicate with the Main EUID (the profile in the far left column), click  .
3. On the confirmation dialog box, click **OK**.

   The status of the potential duplicate entry is changed from Resolved and the profiles are again possible duplicates of one another.

Working with Assumed Matches on the MIDM

The Assumed Matches function of the MIDM lets you view any object profiles that are automatically updated by the master person index application as a result of an assumed match. You can use MIDM to search for assumed matches originating from the same source system. You can reverse the assumed match, if necessary. The following sections provide instructions for finding profiles updated by an assumed match and then reversing the update if necessary.

Perform the following tasks to work with profiles that are automatically matched.

- Finding Assumed Matches on the MIDM on page 6-23
- Reversing an Assumed Match on the MIDM on page 6-24

Finding Assumed Matches on the MIDM

You can find object profiles that are updated by an assumed match using the Assumed Matches function of the MIDM. When you search for assumed matches, you can select an object profile to view from a results list to determine whether the assumed match is done correctly.

To Find Assumed Matches

1. Obtain information about the object profile you want to view such as, their EUID, a system in which they are registered, or the login ID of the user who added the record that caused the update.
2. In the tabbed headings, select **Assumed Matches**.

   The Assumed Matches search page appears.
3. Enter the search criteria. For more information, see About Assumed Matches Search Fields on page 6-23.
4. Click **Search**.

   The Assumed Match Result page appears. For more information, see About Assumed Match Results Fields on the MIDM on page 6-24.
5. In the Results list, click the EUID of the assumed match profile you want to view.

   The Assumed Matches page appears with the assumed match profile displayed.
6. To view a transaction history of the profile, click  .
7. To view the transaction details, click  .
8. To undo the assumed match transaction, follow the instructions provided in Reversing an Assumed Match on the MIDM on page 6-24.

About Assumed Matches Search Fields

The fields located on the Assumed Matches search page lets you specify information about the assumed match profiles you want to view.

Table 6–2 Assumed Matches Search Fields

Field Name	Description
EUID	The enterprise-wide unique identification number of the profile you want to view.
System	The external system with which the object profile that caused the assumed match is associated.
Local ID	The local ID associated with the object profile in the specified system. The name of this field might be different for your implementation.
Create Date From	A start create date for the profiles you want to view. The query is performed for transactions that are created between the Create Date From (and Create Time From) and the To Create Date (and To Create Time).
To Create Date	The end create date for the profiles you want to view.
Create Time From	The start create time for the profiles you want to view (using 24-hour notation). If no time is entered, the default value is 00:01 (12:01 AM).

Table 6–2 (Cont.) Assumed Matches Search Fields

Field Name	Description
To Create Time	The end create time for the profiles you want to view (using 24-hour notation). If no time is entered, the default value is 24:00.

About Assumed Match Results Fields on the MIDM

The fields located in the assumed match results list identify an assumed match transaction to display on the Assumed Matches comparison page. The fields described in the following table always appear in the results list, but the list can be configured to include additional fields.

Table 6–3 Assumed Match Results Fields

Field Name	Description
ID	The assumed match ID of the transaction that caused the assumed match.
EUID	The enterprise-wide unique identification number of the object profile that is updated by the assumed match.
Weight	The matching probability weight between the updated profile and the record that caused the assumed match.
System	The system with which the record that caused the assumed match is associated.
Local ID	The local ID in the above system for the record that caused the assumed match. The name of this field may be different for your implementation.
Create User	The login ID of the user who added the profile that created the assumed match.
Create Date	The date and time the transaction that caused the assumed match occurred.

Reversing an Assumed Match on the MIDM

If you find that an assumed match is made in error, you can reverse the assumed match. This process returns the updated object profile to its status before the assumed match update, creates a new object profile for the record that caused the assumed match, and recalculates the SBR for the existing profile.

To Reverse an Assumed Match

1. View the assumed match profile as described in Finding Assumed Matches on the MIDM on page 6-23.
2. Click **Undo Match**.

   A confirmation dialog box appears, providing the EUID number of the new profile that is created as a result of reversing the match.
3. On the confirmation dialog box, click **OK**.

   The assumed match is reversed, the updated profile is returned to its state before the assumed match, and a new object profile is created for the source record that caused the assumed match. Any changes that are made after the assumed match but before reversing the assumed match are retained.
4. On the information dialog box, click **OK** to view the newly created profile.

Combining Object Information on the MIDM

When you determine that two or more profiles represent the same object, you can merge the profiles to form one profile that contains the object's most current information. You can also merge source records within one profile or from one profile to another. The resulting profile of a profile level merge is called the Merge Result Record. The SBR for the surviving profile is automatically recalculated based on the source records involved in the merge. In a source record merge, the SBRs for all affected profiles are automatically recalculated based on the resulting source records in each profile.

You can display the object profiles to merge using the Search or the Duplicate Records function. This section describes how to merge records using the Search function. For information about merging records using the Duplicate Records function, see Merging Potential Duplicate Profiles on page 6-19.

You can merge profiles from either the Duplicate Records or the Record Details page. The following sections provide instructions for merging profiles or source records from the Record Details or Source Record page. For information about merging profiles from the Duplicate Records page, see Merging Potential Duplicate Profiles on page 6-19.

Merging Object Profiles on the MIDM

When you merge object profiles, all source records associated with the non-surviving object profiles are transferred to the surviving object profile. The non-surviving profiles are given a status of merged and are no longer active. The SBR of the surviving profile is recalculated based on the new source records that are added to the profile due to the merge. After merging profiles, review the source records in the active profile to determine whether any of them must be deactivated or merged.

Note: Use caution when merging more than two object profiles as the entire merge process cannot be reversed.

To Merge Object Profiles

1. Perform a search for the object profiles you want to merge using any of the search procedures described in Searching for Object Profiles on the MIDM on page 3-1.
2. In the results list, select the check boxes to the left of the profiles you want to merge.

   You can select from two to four profiles.
3. Click **Compare**.

   The Comparison page appears.
4. Determine which of the displayed profiles you want to keep, and then click the EUID of that profile.
5. Determine which of the displayed profiles you want to merge into the profile you selected, and then click their EUIDs.
6. Click **Preview**.

The merge preview profile appears so you can review the results of the merge before finalizing it.

Note: If you merge more than two profiles, you can only unmerge the last two profiles that are merged (as determined by the master person index application). Before proceeding, make sure that the profiles must be merged.

7. Compare the highlighted field values to determine which to keep in the final profile. Select each value you want to keep in the merge preview profile.

   Selecting a value to keep in the merge result profile creates a link from the SBR to the source record field that populated the field. For example, if the first name field from Record A is populated from Source Record 1, and you merge Record A into Record B, and select the first name value from Record A, a link is created from the first name field in the resulting SBR to the first name field in Source Record 1. For more information on linking SBR fields to source record fields, see Overriding the SBR of the Survivor Calculator on page 6-11.

8. Click **Merge**.
9. Click **OK** on the confirmation dialog box that appears.
10. Review the surviving profile of the merge to ensure no source records need to be deactivated or merged.

Merging Source Records on the MIDM

You can merge source records from one object profile to a source record from another object profile, or you can merge source records within one profile, as long as both source records originated from the same system. You can also specify which (if any) information to save from the non-surviving source record. When you merge source records, the non-surviving source record is transferred into the object profile of the surviving source record and is given a status of merged. The SBRs of the surviving profiles are automatically recalculated.

To Merge Local ID Source Records

1. In the tabbed headings, select **Source Record**.
2. Click the **Merge** subtab.
3. In the **Source Record** search fields, select the source system for the records.
4. Enter two local IDs for the source records you want to merge and then click **View Records**.

   The source record comparison page appears.

5. Determine which source records you want to merge and click their local IDs.

   Click **View EUID** for the record you want to view to examine the profiles of the source records. After viewing a profile, click **Back** to return to the Source Record page.

6. Click **Keep Local ID#**, where **#** is the heading number of the source record you want to retain after the merge.

   The merge preview record appears.

7. Compare the highlighted fields in the source records to determine which value you want to keep. Click a highlighted value to add it to the merge preview record.
8. At the bottom of the page, click **Merge**.
9. On the confirmation dialog box that appears, click **OK**.

   After you merge two source records, the surviving source record is updated, and the non-surviving source records are transferred to the **merge to** profile and are marked as merged. The SBRs for the object profiles involved in the merge are recalculated. If a merge from profile no longer has any source records, it is deactivated.

Unmerging Object Information on the MIDM

The following sections provide instructions for unmerging profiles and source records.

- Unmerging Object Profiles on the MIDM on page 6-27
- Unmerging Source Records on the MIDM on page 6-28

Unmerging Object Profiles on the MIDM

If object profiles are merged in error, the profiles can easily be separated by unmerging the profiles. When you unmerge object profiles, the information is returned to the original profiles, the source records are returned to their original profiles, and any changes made after the merge are retained. Any source records that are added while the profiles are merged are associated with the profile that was active at the time. After you unmerge object profiles, verify that the source records are distributed correctly in the resulting records.

To Unmerge Object Profiles

1. In the MIDM tabbed headings, click **Transactions**.
2. Perform a search for the object profiles to unmerge.

   For information about the search fields on this page, see About Transaction History Search Fields on the MIDM on page 4-7.
3. Select a transaction to unmerge from the search results list.

   Note: This must be an EUID merge transaction.
4. Review the two displayed profiles to verify that they are unmerged.

   Note: If you are unmerging profiles that are merged in a transaction that included three or four profiles, only the last two profiles merged are unmerged. The remaining profiles cannot be unmerged.
5. Click **Preview Unmerge**.

   A preview of the unmerged record appears.
6. Verify the preview and click **Unmerge**.
7. On the confirmation dialog box that appears, click **OK**.

Unmerging Source Records on the MIDM

If two source records are merged in error, the records can be separated by unmerging the two source records. When source records are unmerged, the source record that is inactive is reactivated. If the source record is merged from a different object profile, it is returned to its original profile. The SBR is recalculated for all affected object profiles. Any changes made to the surviving source record following the merge are retained after the unmerge transaction.

To Unmerge Two Merged Source Records

1. Perform a search for the transaction to unmerge.

   For information about the search fields on this page, see About Transaction History Search Fields on the MIDM on page 4-7.

2. Select a transaction to unmerge from the search results list.

   Note: This must be a system object merge transaction.

3. Review the displayed system records and profiles to verify the system records must be unmerged.

   Note: If you are unmerging system records that are merged in a transaction that included three or four records, only the last two system records that are merged are unmerged. The remaining records cannot be unmerged.

4. Click **Preview Unmerge**.

   A preview of the unmerged record appears.

5. Verify the preview and click **Unmerge**.

   To preview the source records involved in the transaction, click  .

6. On the confirmation dialog box that appears, click **OK**.

7

MIDM Reports

This chapter introduces you to MIDM reports and provides a procedure on how to run the reports. It includes the following sections:

Learning About MIDM Reports

OHMPI provides a set of production and activity reports that can be generated from the MIDM. The production reports provide information about the current state of the data in the master person index application to monitor stored data and determine how that data needs to be updated. This information helps to verify if the matching logic and weight thresholds are defined correctly. Activity reports provide statistical information for transactions over specific period of time.

The following sections provide additional information on how to work with the default reports:

MIDM Production Reports

Production reports provide information about the transactions that are processed through the master person index database. These reports provide lists of potential duplicate profiles, merge transactions, unmerge transactions, assumed matches, updates, and deactivated profiles for a specified time period. These reports provide valuable information about how data is processed with the current configuration. In addition to running the production reports daily, you must run them against any data that is loaded from existing systems into the master person index database in the batch format. Production reports are run based on a date range you specify.

- **Assumed Match Report** - This report displays information about any profiles that are automatically updated by incoming data during the specified time period. The information in this report along with data from the potential duplicate report, determines the accuracy of the threshold for assumed matches. You must review this report daily to ensure that no assumed matches are made in error.
- **Deactivated Record Report** - This report displays a list of all profiles that are deactivated during the specified time period. Review this report daily to ensure

that no profiles are deactivated in error. Master person index applications provide the ability to reactivate any deactivated profile.

- **Potential Duplicate Report** - This report displays information about object profiles that are marked as potential duplicates of one another during the specified time period. The information provided in this report determines if the matching threshold and the duplicate threshold are configured accurately. Review this report daily to ensure potential duplicates are managed in a timely manner, and use this report as a work list when processing potential duplicates.
- **Merge Transaction Report** - This report displays a list of all object profiles and their source records that are merged during the specified time period. Review this report daily to ensure that no profiles are merged in error. You can unmerge any merged profiles using the Master person index applications.
- **UnMerge Transaction Report** - This report displays a list of all object profiles that are unmerged during the specified time period.
- **Update Report** - This report displays object profiles whose information is updated during the specified time period. Review this report daily to verify the updates for a given day. This report details the reason why a resolved potential duplicate listing was reinstated to the potential duplicate list.

MIDM Activity Reports

Activity reports must be run weekly, monthly, and yearly to obtain statistical data about the transactions that are processed through the master person index database. These reports give the number of each type of transaction performed for the specified week, month, or year. They also provide cumulative information for the week, month, or year to date. The information you find in these reports help you analyze the condition of the data by providing the number of potential duplicates created, the number of assumed matches, and so on.

- **Weekly Activity Report** - This report displays a summary of transactions that occurred against the database on each day for the specified calendar week (always Sunday through Saturday). The information provided in this summary includes the number of each of the following transactions performed each day.
  - Add
  - EUID Deactivate
  - EUID Merge
  - EUID Unmerge
  - LID Merge
  - LID Unmerge
  - LID Delete
  - Unresolved Potential Duplicates
  - Resolved Duplicates

  Monthly Activity Report - This report displays a summary of transactions that occurred against the database during the specified month. You can run this report for any calendar month. The information provided in this report includes a summary of each transaction listed for the weekly activity report above.

  Yearly Activity Report - This report displays a summary of transactions that occurred against the database for the specified calendar year. You can run this

report for any calendar year. The information provided in this report includes a summary of each transaction listed for the weekly activity report above.

Configuring MIDM Reports

The report files are configured in the midm.xml file in the master person index project. For detailed information and instructions on configuring the reports, see *Oracle Healthcare Master Person Index Configuration Guide* and *Oracle Healthcare Master Person Index Configuration Reference.*

Masked Data and MIDM Reports

Though the MIDM can be configured to hide certain fields from users who do not have the appropriate security permissions, reports generated from the MIDM displays the hidden data if those fields are configured to appear on the reports. Ensure to grant access to users who can view this information, or do not include hidden fields in the reports.

Running MIDM Reports

Reports are run from the Reports page of the MIDM. You need appropriate security permissions to run the production and activity reports from the MIDM. Production and activity reports require a time period to be defined in the search criteria, and certain reports take additional search criteria.

To Run Reports From the MIDM

1. In the MIDM tabbed headings, click the **Reports** tab.

   The Reports Search page appears.

2. On the Reports Search page, select the type of report to run from the **Reports** subtab.

3. Enter the search criteria. For more information, see About Report Search Fields on the MIDM on page 7-3.

4. Click **Search**.

   The selected report appears.

5. To sort the report by a single column, click that column name.

6. To change whether the column is sorted by ascending or descending order, click again on the column.

7. To print the report, click **Print Report.**

About Report Search Fields on the MIDM

The report search fields let you specify a date range for each report. For Potential Duplicate reports, you can also specify the status of the potential duplicates returned by the search.

Table 7–1 Report Search Fields

Field Name	Description
From Date	The start date for the report. The report retrieves transaction that occurred starting on this date through the date specified in the To Date field.
From Time	The start time for the report in the HHmmss format.
To Date	The end date for the report.
To Time	The end time for the report in the HHmmss format.
Report Maximum Size	The number of records to display. This is applicable only for Potential Duplicate and Assumed Match reports. This lets you limit the size of the report, which can be large in some cases.
System	The source system of the potential duplicate profiles to retrieve. This is applicable only for Potential Duplicate reports and is not visible for other reports. You can specify all systems by leaving this field blank.

8

Master Index Data Manager Security

This chapter provides guidelines for setting up security for the Master Index Data Manager, including defining MIDM user roles and EJB user roles, and creating MIDM user accounts. It includes the following section:

Defining Master Index Data Manager Security

OHMPI supports security for the Master Index Data Manager at the user and function level, and also supports Secure Sockets Layer (SSL) authentication. Security is defined at the following levels:

- EJB level - provides access at the user and function level to the methods of the master controller (com.sun.mdm.index.ejb.master).
- Presentation level - provides access at the function and user level for the actions that can be performed from the MIDM.

A secure user name and password must be defined for each master person index application user to connect to the database, and to log on to the MIDM. For each user account you define, specify one or more roles to let that user perform any functions in the MIDM. You must define roles in the midm-security.xml file in the master person index project. This is the presentation layer security.

In addition, each user must also be assigned at least one EJB security role. EJB security roles are defined in the security.xml file. A default role that grants access to all functions of the master controller is predefined, but is not included in the file. The role is named MasterIndex.Admin.

User permissions for master person index applications are granted using the Admin Console. You can also define security using a Lightweight Directory Access Protocol (LDAP) server, using the roles you define in Defining Master Index Data Manager User Roles on page 8-2.

To configure security for the master person index application, perform the following tasks:

These sections provide additional information to perform the above tasks:

Defining Master Index Data Manager User Roles

OHMPI provides sample user roles for granting multiple permissions to a user. You can define additional user roles and assign combinations of access permissions to each role. By doing this, you can assign a user account to one or two user roles instead of assigning them several access permissions.

To Define a User Role

1. In the NetBeans Project window, expand the master person index project, and then expand **Configuration**.
2. Open **midm-security.xml** in an XML editor.
3. Define user groups and their permissions using the elements described in Master Index Data Manager User Permissions on page 8-8.

   The permissions you can assign are listed and described in Master Index Data Manager User Role Properties on page 8-8.
4. Save and close the file.
5. Continue to Defining EJB User Roles on page 8-2.

Defining EJB User Roles

EJB user roles control access at the master controller level. OHMPI provides a sample role for granting multiple permissions at a time without giving access to all functions. An additional role **MasterIndex.Admin** is predefined that provides access to all functions. You can define additional roles and assign combinations of functional permissions to each role. By doing this, you can assign a user account to one or two roles instead of assigning them several permissions.

Note: This step is optional. You can use the **MasterIndex.Admin** role for MIDM users if you only need to restrict access at the presentation level.

To Define an EJB User Role

1. In the NetBeans Projects window, expand the master person index project, and then expand **Configuration**.
2. Open **security.xml** in an XML editor.
3. Define user roles and the permissions using the elements described in EJB User Role Properties on page 8-10.

   The permissions you can assign are listed and described in EJB Security Functions on page 8-11.
4. Save and close the file.

   You can use these roles when you create the user accounts.

Changing the midm.xml for SSN Masking

For SSN masking, use the plug-in **object-sensitive-plug-in-class** in OHMPI.

To Change the midm.xml for SSN Masking

Perform the following to set the configuration.

1. Add `<is-sensitive>`**true**`</is-sensitive>` to the SSN field in the `midm.xml` file.

```
<field>
  <name>SSN</name>
  <display-name>SSN</display-name>
  <display-order>11</display-order>
  <max-length>16</max-length>
  <gui-type>TextBox</gui-type>
  <value-type>string</value-type>
  <input-mask>DDD-DD-DDDD</input-mask>
  <value-mask>DDDxDDxDDDD</value-mask>
  <is-sensitive>true</is-sensitive>
  <key-type>false</key-type>
</field>
```

   Or

   Add `<is-global-sensitive>`**true**`</is-global-sensitive>` to the SSN field in the `midm.xml` file.

```
<field>
  <name>SSN</name>
  <display-name>SSN</display-name>
  <display-order>11</display-order>
  <max-length>16</max-length>
  <gui-type>TextBox</gui-type>
  <value-type>string</value-type>
  <input-mask>DDD-DD-DDDD</input-mask>
  <value-mask>DDDxDDxDDDD</value-mask>
  <is-global-sensitive>true</is-global-sensitive>
  <key-type>false</key-type>
</field>
```

2. In the `<impl-details>` part of `midm.xml`, specify the `<object-sensitive-plug-in-class><impl-details>`:

```
<master-controller-jndi-name>
     ejb/PersonMasterController
  </master-controller-jndi-name>
  <validation-service-jndi-name>
     ejb/PersonCodeLookup
  </validation-service-jndi-name>
  <usercode-jndi-name>
     ejb/PersonUserCodeLookup
  </usercode-jndi-name>
  <reportgenerator-jndi-name>
     ejb/PersonReportGenerator
  </reportgenerator-jndi-name>
  <object-sensitive-plug-in-class>
     oracle.hsgbu.ohmpi.plugin.SensitiveFieldMaskPlugIn
  </object-sensitive-plug-in-class>
</impl-details>
```

3. To implement SensitiveFieldMaskPlugIn, copy the following `SensitiveFieldMaskPlugIn.java` to the ejb project at oracle.hsgbu.ohmpi.plugin:

```
public class SensitiveFieldMaskPlugIn implements ObjectSensitivePlugIn
{
 public boolean isDataSensitive(ObjectNode objectNode) throws Exception
{
 return true;
}
}
```

4. In the `midm-security.xml` file, there is operation called **Field_VIP**. If a user role has this operation (for example, Administrator role), the user can view the SSN.
5. In the `web_project\web\WEB-INF\classes\com\sun\mdm\index\edm\presentation\messages\midm.properties`, set the SENSITIVE_FIELD_MASKING property (for example, SENSITIVE_FIELD_MASKING=XXXXXXXXX).

Setting Up the Master Index Data Manager User for Application Server

Use the user for MIDM access using the WebLogic Admin Console. In the following steps, you create the MasterIndex.Admin and Administrator groups, and then create a new user within the two groups.

To Set Up the User for Application Server

1. On the left panel, under Domain Structure, expand **Services**, and then select **Security Realms**.
2. In the table on the Summary of Security Realms panel, click **myrealm**, which is the name of the realm.

   The Settings for myrealm panel appears.
3. Select the **Users and Groups** tab and then click **Groups**.
4. In the Groups table, click **New**.
5. In the Name field, enter `MasterIndex.Admin`, and click **OK**.
6. In the Groups table, click **New**.
7. In the Name field, enter `Administrator`, and click **OK**.
8. On the Settings for myrealm panel, select **Users and Groups**, and then **Users**.
9. In the Users table, click **New**.
10. Type a name and password for the new user you are creating and click **OK**.
11. Select **User Group**.
12. To add the two groups you created to the user, from the Available list, drag **MasterIndex.Admin** to the **Chosen** list, and then drag **Administrator** to the **Chosen** list.

Making Required Changes for SSN Masking in Application Server

For SSN masking, use the **object-sensitive-plug-in-class**.

To Input the Required Changes for SSN Masking

Perform the following to make the required changes:

1. Add `<is-sensitive>`**true**`</is-sensitive>` to the SSN field in the `midm.xml` file.

```
<field>
  <name>SSN</name>
  <display-name>SSN</display-name>
  <display-order>11</display-order>
  <max-length>16</max-length>
  <gui-type>TextBox</gui-type>
  <value-type>string</value-type>
  <input-mask>DDD-DD-DDDD</input-mask>
  <value-mask>DDDxDDxDDDD</value-mask>
  <is-sensitive>true</is-sensitive>
  <key-type>false</key-type>
</field>
```

Or

Add `<is-global-sensitive>`**true**`</is-global-sensitive>` to the SSN field in the `midm.xml` file.

```
<field>
  <name>SSN</name>
  <display-name>SSN</display-name>
  <display-order>11</display-order>
  <max-length>16</max-length>
  <gui-type>TextBox</gui-type>
  <value-type>string</value-type>
  <input-mask>DDD-DD-DDDD</input-mask>
  <value-mask>DDDxDDxDDDD</value-mask>
  <is-global-sensitive>true</is-global-sensitive>
  <key-type>false</key-type>
</field>
```

2. In the `<impl-details>` part of `midm.xml`, specify the `<object-sensitive-plug-in-class>`.

```
<impl-details>
  <master-controller-jndi-name>
     ejb/PersonMasterController
  </master-controller-jndi-name>
  <validation-service-jndi-name>
     ejb/PersonCodeLookup
  </validation-service-jndi-name>
  <usercode-jndi-name>
     ejb/PersonUserCodeLookup
  </usercode-jndi-name>
  <reportgenerator-jndi-name>
     ejb/PersonReportGenerator
  </reportgenerator-jndi-name>
  <object-sensitive-plug-in-class>
     oracle.hsgbu.ohmpi.plugin.SensitiveFieldMaskPlugIn
  </object-sensitive-plug-in-class>
</impl-details>
<impl-details>
        <master-controller-jndi-name>ejb/PersonMasterController
</master-controller-jndi-name>
        <validation-service-jndi-name>ejb/PersonCodeLookup
</validation-service-jndi-name>
        <usercode-jndi-name>ejb/PersonUserCodeLookup</usercode-jndi-name>
        <reportgenerator-jndi-name>ejb/PersonReportGenerator
</reportgenerator-jndi-name>
        <object-sensitive-plug-in-class>oracle.hsgbu.ohmpi.plugin.
SensitiveFieldMaskPlugIn</object-sensitive-plug-in-class>
```

```
    </impl-details>
```

3. To implement SensitiveFieldMaskPlugIn, copy the following `SensitiveFieldMaskPlugIn.java` to the EJB project:

```
package com.sun.mdm.index.ejb.util;
import com.sun.mdm.index.objects.ObjectNode;
import com.sun.mdm.index.util.ObjectSensitivePlugIn;
public class SensitiveFieldMaskPlugIn implements ObjectSensitivePlugIn {
    public boolean isDataSensitive(ObjectNode objectNode) throws Exception {
        return true;
    }
}
```

4. In the `midm-security.xml` file, there is an operation called **Field_VIP**. If a user role has this operation (for example, Administrator role), the user can view the SSN.
5. In the `web_project\web\WEB-INF\classes\com\sun\mdm\index\edm\presentation\messages\midm.properties`, set the SENSITIVE_FIELD_MASKING property (for example, SENSITIVE_FIELD_MASKING=XXXXXXXXX).
6. Build the project and redeploy the new ear into the application server.

Masking Sensitive Fields in the MIDM

The `midm.xml` file contains configuration details of all screens in the MIDM. As some fields are sensitive and must not be viewed by everyone, they need to be set so that only users with the appropriate permissions can view certain fields. To do this, the MIDM uses the role-based security tags `<is-sensitive>`**true**`</is-sensitive>` or `<is-global-sensitive>`**true**`</is-global-sensitive>`. Set these tags to **true** for any field that must be masked in the `midm.xml` file.

For example,

```
<?xml version="1.0" encoding="UTF-8"?>
<midm xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:noNamespaceSchemaLocation="schema/midm.xsd">
    <node>
    <name>Person</name>
         <field>
            <name>PersonCatCode</name>
            <display-name>Person Cat Code</display-name>
            <display-order>1</display-order>
            <max-length>8</max-length>
            <gui-type>TextBox</gui-type>
            <value-type>string</value-type>
            <is-sensitive>true</is-sensitive>
            <is-global-sensitive>true</is-global-sensitive>
            <key-type>false</key-type>
         </field>
```

Setting Conditional Masking on the MIDM

You can set the conditional masking for each record in the MIDM in the field VIPFlag in the `<impl-details>` section of the `midm.xml` file. Use the VIPFlag field (see the example below) to control the masking of fields that have `<is-sensitive>` set to **true**. For example,

- If a record's field such as SSN has `is-sensitive` set to **true**, and if the VIPFlag value is set to **false** in the `midm.xml` file, the SSN (123-12-1234) is not masked in the MIDM.
- If a record's SSN has `is-sensitive` set to **true**, and if the VIPFlag value is set to **true** in the `midm.xml` file, the SSN (xxx-xx-xxxx) is masked in the MIDM.

> **Note:** The field VIPFlag is a placeholder and you can change this field name based on your configuration requirements (for example, MVP). You can also change the values **true** or **false** (for example, **yes** or **no**).

```
<impl-details>
  <master-controller-jndi-name>
     ejb/PatientMasterController
  </master-controller-jndi-name>
  <validation-service-jndi-name>
     ejb/PatientCodeLookup
  </validation-service-jndi-name>
  <usercode-jndi-name>
     ejb/PatientUserCodeLookup
  </usercode-jndi-name>
  <reportgenerator-jndi-name>
     ejb/PatientReportGenerator
  </reportgenerator-jndi-name>
  <object-sensitive-plug-in-class></object-sensitive-plug-in-class>
  <sensitive-mask-condition>
     <sensitive-field>
        <name>VIPFlag</name>
        <value>true</value>
     </sensitive-field>
  </sensitive-mask-condition>
</impl-details>
```

> **Note:** `<sensitive-mask-condition>` is used with the `<is-sensitive>` attribute to provide conditional masking for sensitive fields. For example, if you want to mask the SSN of certain patients, you can add `<is-sensitive>` to the `<SSN field>` and provide a mask condition. In the above example `<sensitive-mask-condition>`, the SSN for all patient records whose VIPFlag is set to **true** or **yes** are masked.

Configuring Search Result Pages

The sensitive field added to the `<sensitive-mask-condition>` tag needs to be added to the `<search-result-pages>`. In the following example, the **Person.VIPFlag** sensitive field is added to the `<search-result-pages>` tag.

```
<search-result-pages>
       <search-result-list-page>
             <search-result-id>0</search-result-id>
             <item-per-page>10</item-per-page>
             <max-result-size>100</max-result-size>
             <field-group>
                    <description></description>
                    <field-ref>Person.FirstName</field-ref>
                    <field-ref>Person.LastName</field-ref>
```

```
                    <field-ref>Person.SSN</field-ref>
                    <field-ref>Person.DOB</field-ref>
                    <field-ref>Person.Gender</field-ref>
                    <field-ref>Person.VIPFlag</field-ref> <-- sensitive mask
                    field needs to be added to the search result pages.
                </field-group>
            </search-result-list-page>
</search-result-pages>
```

Master Index Data Manager User Role Properties

You can define user roles for the MIDM to assign multiple security permissions to a user account at once. Roles are defined in the midm-security.xml file. Table 8–1 describes the elements of the security configuration file.

Table 8–1 MIDM User Role Configuration Elements

Element	Description
role	A definition for a user role. Each role element contains a name for the user role, a list of security permissions, and, optionally, a user role from which permissions are inherited along with any exceptions to the inheritance.
role-name	The name of the user role, such as Administrator.
inheritance	A definition of how permissions are inherited from another user role. The definition includes the parent user role and any permission that must not be inherited. This group of elements is optional, and a role can inherit from multiple user roles. **Note:** The role from which permissions are inherited must be defined earlier in the XML file than the role that inherits the permissions.
inherits-from	The name of the user role from which the current role inherits permissions. If permissions are added to this user role at any time, the new permissions are also inherited by the current role.
excluded-operations	A list of permissions assigned to the parent role that the current role must not have access. Any permission assigned to the parent role that are not listed here are assigned to the current role. **Note:** If a role inherits from multiple parent roles and each parent is assigned an excluded permission, you need to specify that the permission must be excluded for each parent role.
excluded-operations/name	The name of a security permission that is not inherited from the parent user role. Security permissions are listed under Master Index Data Manager User Permissions on page 8-8.
operation	A list of security permissions to assign to the user role. If the role inherits permissions from another role, the permissions listed here are in addition to the inherited permissions.
operation/name	The name of a security permission to add to the current user role. Security permissions are listed under Master Index Data Manager User Permissions on page 8-8.

Master Index Data Manager User Permissions

Table 8–2 lists and describes user permissions for the MIDM. The user permission names are case-sensitive.

Table 8–2 MIDM User Permissions and Descriptions

User Permission	Description
AssumedMatch_Print	Gives access permission to print the results of an assumed match search.
AssumedMatch_SearchView	Gives access permission to search for and view records that are automatically matched by the master person index application. This permission is required to perform any assumed match functions.
AssumedMatch_Undo	Give access permission to reverse an assumed match, separating the two records.
AuditLog_Print	Gives access permission to print an audit log search results report. This permission also requires AuditLog_SearchView.
AuditLog_SearchView	Gives access permission to search and view audit log entries.
EO_Activate	Gives access permission to activate enterprise records.
EO_Compare	Gives access permission to compare enterprise records.
EO_Create	Gives access permission to create new enterprise records.
EO_Deactivate	Gives access permission to deactivate enterprise records.
EO_Edit	Gives access permission to modify the SBR in enterprise records.
EO_LinkSBRFields	Gives access permission to link a field in a system record with a field in the enterprise record's SBR so the value of the SBR field is the same as the system object field.
EO_LockSBRFields	Give access permission to modify the SBR directly and lock SBR fields for overwrite.
EO_Merge	Gives access permission to merge enterprise records.
EO_OverwriteSBR	Gives access permission to choose an SBR field to retain during a merge. After the merge transaction, the field is locked for editing.
EO_PrintComparison	Reserved for future functionality.
EO_PrintSBR	Reserved for future functionality.
EO_SearchViewSBR	Gives access permission to search and view single best records, and generate and print the search results report. This permission is needed to perform any functions on the details page.
EO_UnlinkSBRFields	Gives access permission to unlink an SBR field and system record field that are previously linked.
EO_UnlockSBRFields	Gives access permission to unlock an SBR field that is previously locked for editing.
EO_Unmerge	Gives access permission to unmerge enterprise records.
EO_ViewMergeTree	Gives access permission to view a merge history of an enterprise object.
Field_VIP	Gives permission to view fields masked by any custom masking logic specified by midm.xml.
PotDup_Print	Gives permission to print results of a potential duplicate search.
PotDup_ ResolvePermanently	Gives access permission to permanently resolve potential duplicate records.
PotDup_ResolveUntilRecalc	Gives access permission to resolve potential duplicate records.

Table 8–2 (Cont.) MIDM User Permissions and Descriptions

User Permission	Description
PotDup_SearchView	Gives access permission to search and view potential duplicate records. This permission is needed to perform any functions on the Duplicate Records page.
PotDup_Unresolve	Gives access permission to unresolve potential duplicate records that are previously resolved.
Reports_Activity	Gives access permission to run an activity report.
Reports_AssumedMatches	Gives access permission to run an assumed match report.
Reports_DeactivatedEUIDs	Gives access permission to run a deactivated record report.
Reports_Duplicates	Gives access permission to run a potential duplicate report.
Reports_MergedRecords	Gives access permission to run a merge transaction report.
Reports_UnmergedRecords	Gives access permission to run an unmerge transaction report.
Reports_Updates	Gives access permission to run an update report.
Reports_View	Gives access permission to the reports page. This permission is needed to run any of the production or activity reports.
SO_Activate	Gives access permission to reactivate a deactivated system record.
SO_Add	Gives access permission to add system records.
SO_Compare	Gives access permission to compare system records.
SO_Edit	Gives access permission to modify system records.
SO_Deactivate	Gives access permission to deactivate system records.
SO_Merge	Gives access permission to merge system records.
SO_Print	Gives access permission to print results of a system record search.
SO_Remove	Gives access permission to delete system records.
SO_Transfer	Gives access permission to transfer system records.
SO_SearchView	Gives access permission to search for and view system records.
SO_Unmerge	Gives access permission to unmerge system records.
TransLog_Print	Gives permission to print results of a transaction history search.
TransLog_SearchView	Gives access permission to search and view the transaction history of enterprise records and view merged records.
View_Sensitive	Gives permission to view **is-sensitive** field values that are hidden on the MIDM.
View_Global_Sensitive	Gives permission to view **is-global-sensitive** field values that are hidden on the MIDM.

EJB User Role Properties

You can define access roles for the EJB layer to assign multiple security permissions to a user or web client at once. EJB roles can be used to secure MIDM users and other clients accessing the master person index application, such as web services. Roles are defined in the security.xml file.

Table 8–3 describes the elements of the security configuration file. The default user, MasterIndex.Admin, is not defined in this file, but it gives access to all functions.

Table 8–3 EJB User Role Configuration Elements

Element	Description
ejbSecurity	An indicator of whether EJB security is enabled. Enter **ON** to enable web service security and enter **OFF** to disable web service security.
role	A definition for one EJB user role. Each role element contains a name for the user role and a list of security permissions.
role-name	The name of the EJB user role, such as DataProcessor.
operation	A list of master controller functions to assign to the user role.
name	The name of a master controller function to add to the current user role. Functions are listed under EJB Security Functions on page 8-11.

EJB Security Functions

Table 8–4 lists and describes each security function in the master controller. The permission names are case-sensitive. For more information about these functions, see the Javadocs provided with Oracle Healthcare Master Person Index. These functions are defined in com.sun.mdm.index.ejb.master.MasterController.

Table 8–4 EJB Security Functions and Descriptions

User Permission	Description
activateEnterpriseObject	Gives access permission to change the status of a deactivated enterprise object back to active.
activateSystemObject	Gives access permission to change the status of a deactivated system object back to active.
addSystemObject	Give access permission to add a system object to an enterprise object.
calculatePotentialDuplicates	Gives access permission to calculate potential duplicates for a transaction.
calculateSBR	Gives access permission to calculate a new SBR for an enterprise object that is updated.
createEnterpriseObject	Gives access permission to create a new enterprise object in the master person index application.
deactivateEnterpriseObject	Gives access permission to change the status of an enterprise object to inactive.
deactivateSystemObject	Gives access permission to change the status of a system object to inactive.
deleteSystemObject	Gives access permission to delete a system object from an enterprise object.
executeMatch	Gives access permission to process a system object using the standardization and matching logic defined for the master person index application.
executeMatchDupRecalc	Gives access permission to process a system object using the standardization and matching logic defined for the master person index application and lets you defer potential duplicate processing.
executeMatchGui	Gives access permission to process a system object using the standardization and matching logic defined for the master person index application.

Table 8–4 (Cont.) EJB Security Functions and Descriptions

User Permission	Description
executeMatchUpdate	Gives access permission to process a system object using the standardization and matching logic defined for the master person index application.
executeMatchUpdateDupRecalc	Gives access permission to process a system object using the standardization and matching logic defined for the master person index application and lets you defer potential duplicate processing.
getConfigurationValue	Gives access permission to retrieve the configuration of a master controller parameter.
getDatabaseStatus	Give access permission to retrieve the status of the master person index database.
getEnterpriseObject	Gives access permission to retrieve an enterprise object.
getEUID	Gives access permission to retrieve the EUID associated with a system and local ID.
getMergeHistory	Gives access permission to retrieve a tree structure of the merge transactions associated with a specific enterprise object.
getRevisionNumber	Gives access permission to retrieve the SBR revision number for an enterprise object.
getSBR	Gives access permission to retrieve the SBR for an enterprise object.
getSystemObject	Gives access permission to retrieve a system object based on the system and local ID information.
insertAuditLog	Gives access permission to add an audit log record to the master person index database.
lookupAssumedMatches	Gives access permission to retrieve a list of assumed matches based on the search criteria specified.
lookupAuditLog	Gives access permission to retrieve an audit log record.
lookupPotentialDuplicates	Gives permission to retrieve a list of potential duplicate records.
lookupSystemDefinition	Gives permission to retrieve the attributes of a source system in the master person index database.
lookupSystemObjectPKs	Gives access permission to retrieve an array of system object keys.
lookupSystemObjects	Gives access permission to retrieve the active system objects in an enterprise object.
lookupTransaction	Gives access permission to retrieve a transaction summary.
lookupTransactions	Gives access permission to retrieve an array of transaction summaries.
mergeEnterpriseObject	Gives access permission to merge two or more enterprise objects.
mergeSystemObject	Gives access permission to merge two or more system objects.
ResolvePotentialDuplicates	Gives access permission to flag a potential duplicate pair as resolved.
searchEnterpriseObject	Gives access permission to retrieve an iterator of enterprise objects based on the specified search criteria.
transferSystemObject	Gives access permission to transfer a system object from its current enterprise object to a different enterprise object.

Table 8–4 (Cont.) EJB Security Functions and Descriptions

User Permission	Description
UndoAssumedMatch	Gives access permission to reverse an assumed match transaction, unmerging the two objects that are matched, and creating a new enterprise object.
unmergeEnterpriseObject	Gives access permission to unmerge two previously merged enterprise objects.
unmergeSystemObject	Gives access permission to unmerge two previously merged system objects.
unresolvePotentialDuplicate	Gives access permission to mark as unresolved two potential duplicate records that are previously flagged as resolved.
updateEnterpriseDupRecalc	Gives access permission to update the master person index database to reflect new values for an enterprise object and optionally to defer potential duplicate processing.
updateEnterpriseObject	Gives access permission to modify enterprise objects.
updateSystemObject	Gives access permission to modify system objects.