Informatica® Multidomain MDM
10.4 HotFix 2

Security Guide

Informatica Multidomain MDM Security Guide
10.4 HotFix 2
December 2020

Publication Date: 2021-01-12

Table of Contents

Preface

Use the Informatica® *Multidomain MDM Security Guide* to learn how to enable security in Multidomain MDM. Understand how to use the Security Access Manager to secure MDM Hub resources and use Dynamic Data Masking to prevent access to sensitive data. Learn how to manage users and groups, and how to use permissions, privileges, and roles to manage user security.

This guide assumes that you have knowledge of operating systems, database environments, and your application server.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Introduction to MDM Hub Security

This chapter includes the following topics:

MDM Hub Security Overview

The MDM Hub secures data from unauthorized access and tampering to protect information privacy and data integrity.

You can use the Security Access Manager in the Hub Console to secure MDM Hub resources and enforce operational security policies, including user authentication and authorization.

You can use Dynamic Data Masking to prevent access to sensitive data. For example, you can use Dynamic Data Masking to conceal credit card numbers from all users who do not have administrative rights.

You can configure security in MDM Hub implementations in multiple ways. You can use third-party security providers to handle specific elements of security for your organization, or you can configure the MDM Hub manage all aspects of security. For more information about using the Services Integration Framework (SIF) to configure security, see the *Multidomain MDM Services Integration Framework Guide*.

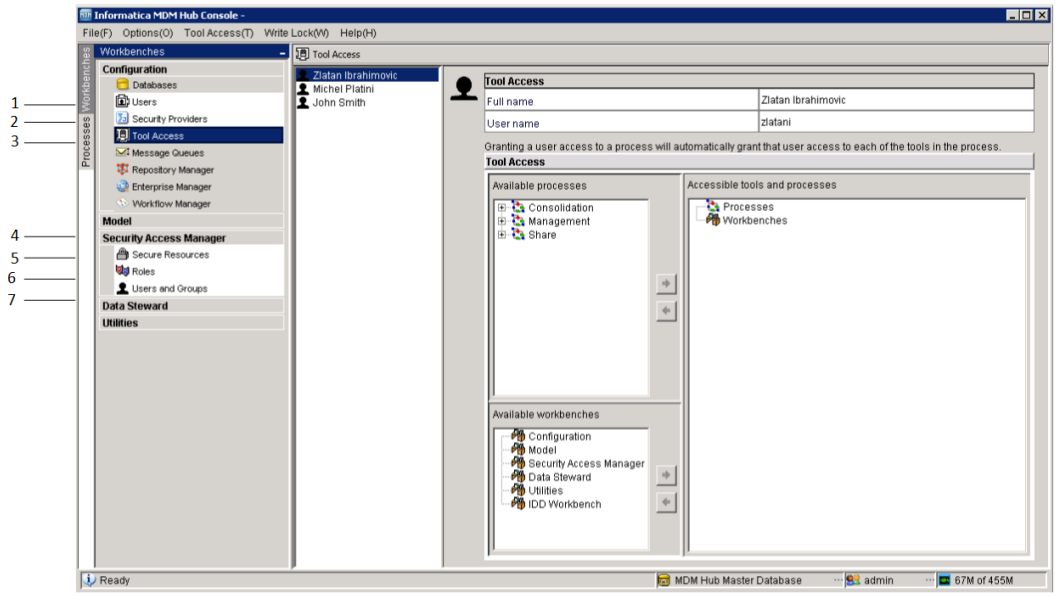
Important: Before you begin to secure Multidomain MDM, ensure that your application server and caching devices are secured.

MDM Hub Console

Use the Hub Console to configure security in the MDM Hub.

To control access privileges to Hub Console tools, you can use the Tool Access tool in the Configuration workbench. For example, you can use the Tool Access tool to deny data stewards access to all Hub Console tools except the Data Manager and Merge Manager tools.

The following image shows the Hub Console interface:



1. Users tool
2. Security Providers tool
3. Tool Access tool
4. Security Access Manager
5. Secure Resources tool
6. Roles tool
7. Users and Groups tool

Dynamic Data Masking

Informatica Dynamic Data Masking is a data security product that operates between a client and a database to prevent unauthorized access to sensitive information. Dynamic Data Masking intercepts requests sent to the database and applies data masking rules to the request to mask the data before it is sent back to the client.

You can use Dynamic Data Masking to mask or prevent access to sensitive data stored in production and non-production databases managed by the MDM Hub. You set up the connection rules to identify incoming requests and security rules to define how you want to mask the data. Dynamic Data Masking monitors incoming database requests from the MDM Hub and modifies the database request before it sends the

request to the database. The database processes the modified request and returns masked results to Dynamic Data Masking. Dynamic Data Masking then sends the results to the MDM Hub.

You can use Dynamic Data Masking to mask data for specific types of database requests or you can restrict access to data from certain groups within an organization. For example, you can create a rule to apply a masking function to credit card numbers when the database request comes from a support team member. When Dynamic Data Masking sends the data back to the MDM Hub, the support team member sees the masked numbers instead of the real credit card numbers.

Note: To use Dynamic Data Masking in the MDM Hub, you need to have Dynamic Data Masking 9.6.0 and Emergency Bug Fix 14590 installed. Earlier versions of Dynamic Data Masking are not compatible with the MDM Hub.

For more information about Dynamic Data Masking, see the Dynamic Data Masking documentation.

Security Access Manager

The Security Access Manager is the security module for the MDM Hub. The Security Access Manager protects MDM Hub resources from unauthorized access.

The Security Access Manager enforces the security policies of your organization in your MDM Hub implementation. The Security Access Manager manages user authentication and authorization according to your security configuration.

Note: You can use the Security Access Manager to configure user access to MDM Hub resources from third-party applications. However, you cannot configure security for Hub Console tools and resources through the Security Access Manager. The Hub Console authenticates users and authorizes user access to Hub Console tools and resources through a separate security mechanism.

Authentication

Authentication is the process of verifying the identity of a user.

The MDM Hub authenticates users based on their supplied credentials, such as a user name and password, or raw binary data in a security payload.

The MDM Hub uses the following types of authentication:

Internal

Authenticates users within the MDM Hub, where the user logs in with a user name and password.

External Directory

Authenticates users through an external user directory, with native support for LDAP-enabled directory servers, Microsoft Active Directory, and Kerberos.

External Authentication Providers

Authenticates users through third-party authentication providers.

MDM Hub implementations can use each type of authentication exclusively, or implementations can use a combination of authentications. The type of authentication that you use depends on how you configure security.

Authorization

Authorization is the process of determining whether a user has sufficient privileges to access a requested MDM Hub resource.

In the MDM Hub, you can use internal and external authorization:

Internal

Authorizes through the MDM Hub. The MDM Hub determines whether you can access secure resources by examining the privileges associated with any roles assigned to your user account.

External

Authorizes through third-party authorization providers.

You can configure the MDM Hub to use either type of authorization, or you can configure it to use both types of authorization.

Secure Resources and Privileges

You can configure multiple MDM Hub resources as secure resources.

The following resources are configurable:

- Base objects
- Mappings
- Packages
- Cleanse functions
- Match rule sets
- Metadata
- Profiles
- Users table

You can grant access to MDM Hub resources according to privileges. The MDM Hub can assign the following privileges:

- Read
- Create
- Update
- Merge
- Execute
- Delete

Resources can be either private or secure. By default, resources are secure. The MDM Hub can grant privileges only to secure resources.

When you configure security in the MDM Hub, consider the following facts:

- A specific resource is configured to be secure.
- A specific role is configured to have access to one or more secure resources.

- Each secure resource can be configured with specific privileges, such as read or write, that define access for that role to the secure resource.

To run a Services Integration Framework request, the logged-in user must have a role that has the required privileges to access the resource involved with the request.

Roles

A role represents a set of privileges to access secure MDM Hub resources. You assign a user a role in order for that user to gain privileges.

You can use the Roles tool in the Security Access Manager workbench to assign roles to users and user groups. The roles assigned to a user or user group determine the resource privileges of a user or user group. You cannot assign privileges to users directly.

The Security Access Manager enforces resource authorization for requests from external application users. Administrators and data stewards who use the Hub Console to access MDM Hub resources are not affected by resource privileges to the same extent.

Security Implementation Scenarios

You can configure security in MDM Hub implementations in multiple ways.

A policy decision point is a specific security check point that determines the identity of users at run time. This is called authentication. A policy decision point also confirms what MDM Hub resources users can access. This is called authorization. The degree to which policy decision points are handled internally by the MDM Hub, or externally by third-party security providers or other security services, depends on the MDM Hub implementation.

The following scenarios are examples of high-level ways that you can configure security in MDM Hub implementations:

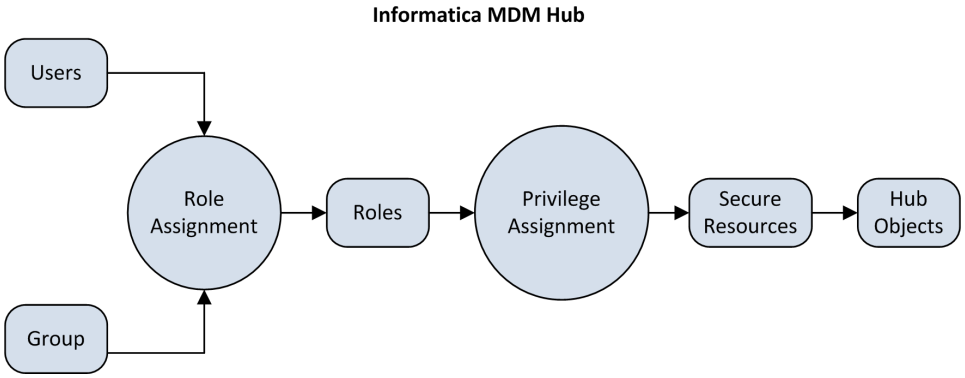
- Internal-only policy decision points
- External User Directory
- Roles-based Centralized policy decision points
- Comprehensive Centralized policy decision points

Note: The MDM Hub does not reflect changes to resource privileges from an external security provider. If you make changes to resource privileges by using an external security provider, use other means to synchronize the changes with the MDM Hub.

Internal Policy Decision Point

The MDM Hub can handle all policy decisions internally.

The following image shows a security deployment in which the MDM Hub handles all policy decisions internally:



In this scenario, the MDM Hub makes all policy decisions based on how users, groups, roles, privileges, and resources are configured using the Hub Console.

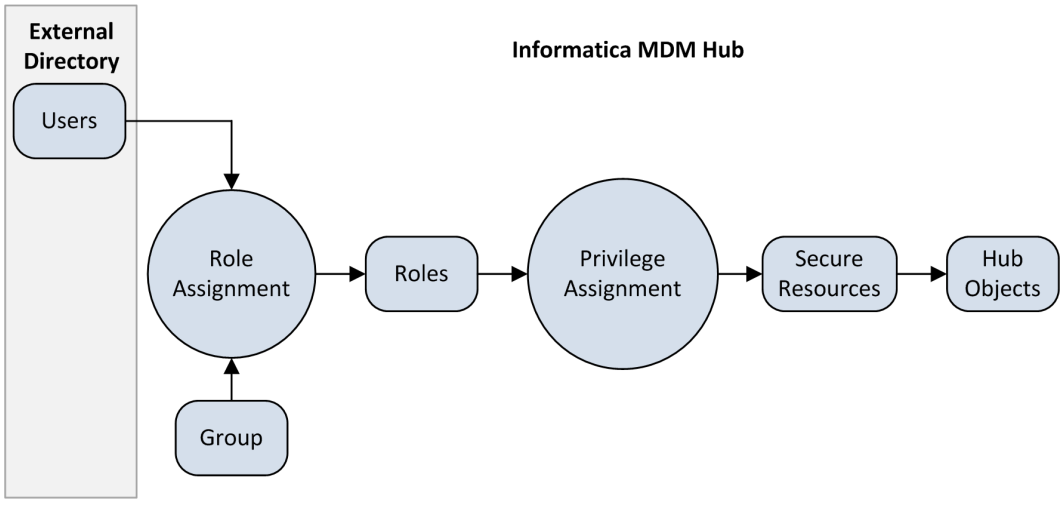
External User Directory

The MDM Hub can integrate with an external user directory.

Users or user groups that are maintained in the external user directory must still be registered in the MDM Hub. Registration is required before the MDM Hub can assign roles, and their associated privileges, to these users and groups.

Assign users from the external directory to groups in the MDM Hub. You must maintain the relationships between users and groups in the MDM Hub, even if you also maintain the relationships through the Lightweight Directory Access Protocol.

The following image shows a security deployment where you manage users in an external directory, but you manage the groups, role assignment, and privilege assignment in the MDM Hub.

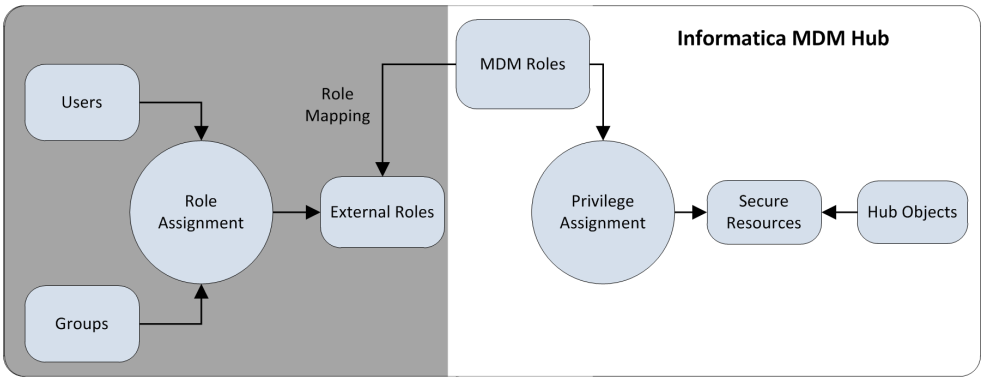


In this scenario, the external user directory manages user accounts, groups, and user profiles. The external user directory can authenticate users and provide information to the MDM Hub about group membership and user profiles.

Role-based Centralized Policy Decision

The MDM Hub can handle some policy decisions internally and receive external role assignments.

The following image shows a security deployment where role assignment, in addition to user accounts, groups, and user profiles, occurs externally to the MDM Hub:

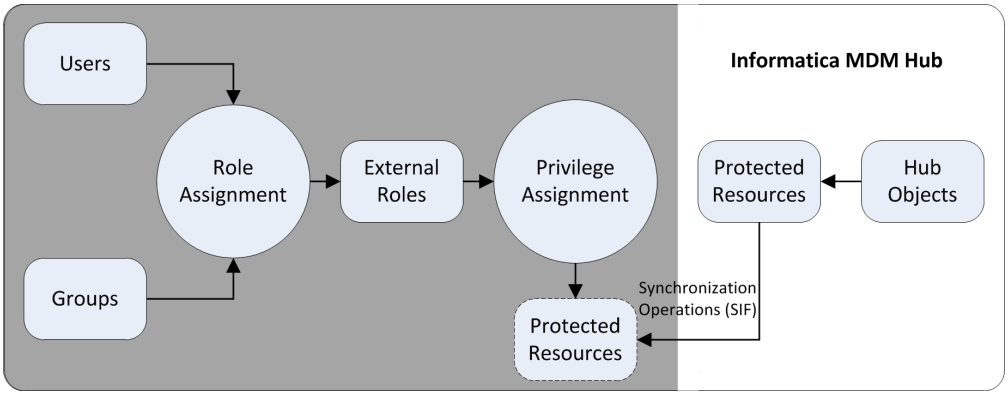


In this scenario, external roles are explicitly mapped to the MDM Hub roles.

Comprehensive Centralized Policy Decision

The MDM Hub can control protected resources internally but accept roles and privileges assigned from an external directory.

The following image shows a security deployment in which role definition and privilege assignment occur externally to the MDM Hub. The figure also shows that user accounts, groups, user profiles, and role assignment occur externally to the MDM Hub:



In this scenario, the MDM Hub simply exposes the protected resources using external proxies, which are synchronized with the internally protected resources using Services Integration Framework requests. All policy decisions are external to the MDM Hub.

Configuration Tasks for Security Scenarios

The following table shows the security configuration tasks that pertain to each of the security implementation scenarios. If a cell contains a "Yes" then the associated task occurs within the MDM Hub. If a cell contains a "No" then the associated task occurs externally to the MDM Hub.

Service / Task	Internal Policy Decision Points	External User Directory	RoleNobased Centralized Policy Decision Points	Comprehensive Centralized Policy Decision Points
Configure MDM Hub users	Yes	Yes	No	No
Use external authentication	No	Yes	No	No
Assign users to the current Operational Reference Store database	Yes	Yes	No	No
Manage the global password policy	Yes	No	No	No
Configure user groups	Yes	Yes	No	No
Secure MDM Hub resources	Yes	Yes	Yes	Yes
Set the status of a MDM Hub resource	Yes	Yes	Yes	Yes
Configure roles	Yes	Yes	Yes	No
Map internal roles to external roles	No	No	Yes	No
Assign resource privileges to roles	Yes	Yes	Yes	No
Manage security providers	No	Yes	Yes	Yes
Assign roles to users and user groups	Yes	Yes	No	No

Note: If you are using third-party security providers to handle any portion of security in your MDM Hub implementation, see configuration instructions from your security provider.

Disabling the default administrative user

You can disable the default administrative user account to prevent any external authentication for security purposes. As a result, external users cannot use this account to access the MDM system. You must create and configure a non-default administrative user in MDM Hub.

1. Create an administrative user in MDM Hub. Go to **Users > Add User > New**, create this new user account and select the **Enable Administrator** check box.
2. Assign the user to the registered ORS. Use the **Target Database** tab if you want to assign it to multiple ORSs.
3. To disable default administrative user account, connect to MDM Hub Master Database and run the following command:

```
update c_repos_user set user_enabled_ind = 0 where rowid_user = 'INST.0 ' ;
commit ;
```

4. Assign this user for use by the **Identity Service** in the ActiveVOS Console.
   a. Go to `<MDM Hub installation directory>/hub/server/bin` folder.
   b. Open the `build.properties` file.
   c. Add the following property for the user name that you created: `mdm.identity.user=<user name>`.
   d. Save the file.
5. Open a command prompt, and run the following script:
   - On Windows. `<MDM Hub installation directory>\hub\server\postInstallSetup.bat`
   - On UNIX. `<MDM Hub installation directory>/hub/server/postInstallSetup.sh`
6. Restart the application server.
7. Log into the ActiveVOS Console and update the password for this new user, added to **Identity Service**.
   a. On the **Admin** tab, go to **Configure Services > Identity Service**.
   b. On the **Connection** tab, in the **Connection Settings** section, specify and confirm the new password.
   c. Click **Update**.

   When you install a HotFix, the setting `mdm.identity.user=<user name>` will be removed from the `build.properties` file automatically. You must add this property manually. Open the `build.properties` file, add the property, and save the file. Run the `postInstallSetup` script. Restart the application server.

CHAPTER 2

Resources

This chapter includes the following topics:

Resources Overview

The Hub Console allows you to expose or hide MDM Hub resources to external applications.

A secure resource is a protected MDM Hub resource that is exposed to the Roles tool, which allows the resource to be added to roles with specific privileges. A resource group is a collection of secure resources that simplify privilege assignment. You can use the Secure Resources tool to define resources groups and create a hierarchy of resources.

You can configure the following MDM Hub resources as secure resources:

Base Object

User has access to all secure base objects, columns, and content metadata.

Cleanse Function

User can run all secure cleanse functions.

Hierarchy Manager Profile

User has access to all secure Hierarchy Manager profiles.

Business Entity Services

User has access to all secure Business Entity services.

Mapping

User has access to all secure mappings and their columns.

Package

User has access to all secure packages and their columns.

Remote Package

User has access to all secure remote packages.

Batch groups are secure by default. You cannot change the status of batch groups to private. The batch group has Read and Execute privileges.

In addition, you can use the Hub Console to protect other resources that are accessible by SIF requests, including metadata, match rule sets, the audit table, and the users table.

Note: If you use Informatica Data Director, you can use the HTTP methods GET or POST to access the Hub Server. Other HTTP methods, such as DELETE or PUT, return an HTTP error.

Secure and Private Resources

You can configure a protected MDM Hub resource as either secure or private.

Secure

Exposes this MDM Hub resource to the Roles tool, which allows the resource to be added to roles with specific privileges. When you assign a specific role to a user, then that user can use SIF requests to access the secure resources according to the privileges associated with that role. By default, MDM Hub designates a new resource, such as a base object, as secure.

Private

Hides the MDM Hub resource from the Roles tool. Prevents access of the resource from SIF requests.

A resource must be secure before external applications can use SIF requests to access an MDM Hub resource.

There are certain MDM Hub resources that you might not want to expose to external applications. For example, your MDM Hub implementation might have mappings or packages that are used only in batch jobs, and not in SIF requests, so these could remain private.

Note: The MDM Hub does not consider package columns to be secure resources. Package columns inherit the secure status and privileges from the parent base object columns. If package columns are based on system table columns, you do not need to set up security for them, because they are accessible by default.

Resource Groups

A resource group is a logical collection of secure resources.

You can use the Secure Resources tool to define resource groups, and then assign related resources to them. Resource groups simplify privilege assignment, which allows you to assign privileges to multiple resources and assign resource groups to a role.

To simplify administration, consider the creation of the following kinds of resource groups:

- Define an ALL_RESOURCES resource group that contains all secure resources, which allows you to set minimal privileges globally.
- Define resource groups by resource type so that you can set minimal privileges to those kinds of resources.
- Define resource groups by functional area, such as TRAINING_RESOURCES, for example.

- Define a catch-all resource group that you can then assign to many different roles that have similar privileges.

Resource Group Hierarchies

A resource group can also contain other resource groups, except a resource group to which it belongs. This means you can build a hierarchy of resource groups and simplify the management of a large collection of resources.

Secure Resources

Only secure resources can belong to resource groups. Private resources cannot belong to resource groups.

If you change the status of a resource to private, then the MDM Hub removes the resource from any resource groups to which it belongs. When you set the status of a resource to secure, the MDM Hub adds the resource to the appropriate resource group.

Secure Resources Tool

Use the Secure Resources tool in the Hub Console to manage security for MDM Hub resources in detail, including setting the status of any MDM Hub resource to secure or private. You can also use resource groups to configure a hierarchy of resources.

The Secure Resources tool contains the following tabs:

Resources

Used to set the status of individual MDM Hub resources as secure or private. MDM Hub displays the resources as a hierarchy that shows the relationships among resources. Global resources appear at the top of the hierarchy.

Resource Groups

Used to configure resource groups.

You can use the Secure Resources tool to expose resources to, or hide resources from, the Roles tool and SIF requests. You must connect to an Operational Reference Store before you use the tool.

Configuration of Secure Resources

To browse and configure MDM Hub resources, use the Resources tab in the Secure Resources tool.

Setting the Status of an MDM Hub Resource

You can configure the resource status as secure or private for any MDM Hub resource.

Note: This status setting does not apply to resource groups, which contain only secure resources, or to global resources.

1. Start the Secure Resources tool.

2. Acquire a write lock.
3. On the Resources tab, navigate the Resources tree to find the resources that you want to configure.
4. Double-click the resource name to toggle between secure or private. To change the status of multiple resources at one time, perform step 5 and 6.
5. Select the resources that require a status change. You can select multiple resources if you want.
6. Update the status of the resources you selected.
   - Click the **Secure** button to change the status of the selected resources to secure.
   - Click the **Private** button to change the status of the selected resources to private.
7. Click the **Save** button to save your changes.

Filtering Resources

To simplify changing the status of a collection of MDM Hub resources, you can specify a filter that displays only the resources that you want to change.

1. Start the Secure Resources tool.
2. Acquire a write lock.
3. Click the **Filter Resources** button.

   The Secure Resources tool displays the Resources Filter dialog box.
4. Select resource types.
   - Select the resource types that you want to include in the filter.
   - Clear the resource types that you want to exclude in the filter.
5. Click **OK**.

   The Secure Resources tool displays the filtered Resources tree.

Configuration of Resource Groups

You can use the Secure Resources tool to define resources groups and create a hierarchy of resources. You can then use the Roles tool to assign privileges to multiple resources in a single operation.

The Secure Resources tool differentiates visually between resources that belong directly to the current resource group and resources that belong indirectly. Resources explicitly added to a resource group have direct membership. Resources that belong to a resource group that was added to a resource group have indirect membership.

For example, you want to have two resource groups:

- Resource Group A contains the Consumer base object, which means that the Consumer base object is a direct member of Resource Group A.
- Resource Group B contains the Address base object.
- Resource Group A contains Resource Group B, which means that the Address base object is an indirect member of Resource Group A.

In this example, the Address base object is unavailable when you edit Resource Group A. You must edit Resource Group B to edit the Address base object.

Adding Resource Groups

Use the Secure Resources tool to add a resource group to the resources list.

1. Start the Secure Resources tool.
2. Acquire a write lock.
3. Click the **Resource Groups** tab.

   The Secure Resources tool displays the Resource Group tab.
4. Click the **Add** button.

   The Secure Resources displays the Add Resources to Resource Group dialog box.
5. Enter a unique, descriptive name for the resource group.
6. Click the plus (+) sign to expand the resource hierarchy as needed.

   Each resource has a check box indicating membership in the resource group. If you select a parent, all the children are selected as well. For example, if you select the Base Objects item in the tree then all base objects and their child resources are selected.
7. Select the resources that you want to assign to this resource group.
8. Click **OK**.

   The Secure Resources tool adds the new resource to the Resource Groups node.

Editing and Deleting Resource Groups

You can use the Secure Resources tool to edit or delete resource groups.

1. Start the Secure Resources tool.
2. Acquire a write lock.
3. Click the **Resource Groups** tab.
4. Select the resource group whose properties you want to edit or delete.
   - Click the **Edit** button to edit a resource group.
   - Click the **Remove** button to remove a resource group.

   The Secure Resources tool displays the Assign Resources to Resource Group dialog box. Or the Secure Resources tool removes the deleted resource from the Resource Groups node.
5. Edit the resource group name.
6. Click the plus (+) sign to expand the resource hierarchy.
7. Select the **Show Only Resources Selected for this Resource Group** check box.
8. Select the resources that you want to assign to this resource group.
9. Clear the resources that you want to remove from this resource group.
10. Click **OK**.

Refreshing the Resources List

After adding a resource, you can refresh the resources list to update it.

To refresh the Resources list, choose **Refresh** from the Secure Resources menu.

The Secure Resources tool updates the Resources list.

Refreshing Other Security Changes

You can also change the refresh interval for all other security changes.

To set the refresh rate for security changes, set the following parameter in the `cmxserver.properties` file:

```
cmx.server.sam.cache.resources.refresh_interval
```

Note: The default refresh interval is 5 clock ticks at a rate of 60,000 milliseconds for 1 clock tick, which is equivalent to 5 minutes.

Configuration of Security for Data Director Business Entity Services

Business entity services are secured resources and only user roles with privileges can access business entity services in Data Director.

You can configure the following business entity service resources in the MDM Hub console:

- Find-Replace
- File Import
- Adhoc Match

You must use the Secure Resource tool to configure business entity services as secure resources. You can then use the Roles tool to assign privileges to user roles.

Configuring Business Entity Services as a Secure Resource

Use the Secure Resources tool in the Security Access Manager workbench to configure the required resources as a secure resource.

1. Start the Secure Resources tool.
2. Acquire a write lock.
3. Click the **Resources** tab.
4. Navigate to the Resource tree and expand **Business Entity Services**.
5. Double-click the resource name to toggle between secure or private.
    a. Click the **Secure** button to change the status of the selected resources to secure.
    b. Click the **Private** button to change the status of the selected resources to private.
6. Click **Save**.

Assigning Role Privileges to Business Entity Services

Use the Roles tool in the Security Access Manager workbench to assign business entity service privileges to user roles.

1. Start the Roles tool.
2. Acquire a write lock.
3. Scroll through the roles list and select the required role.
4. Click the **Resource Privileges** tab.

5. Navigate to the Resource tree and expand **Business Entity Services**.
6. Select the **Execute** privilege for each business entity service resource.
7. Click **Save**.

CHAPTER 3

Roles

This chapter includes the following topics:

Roles Overview

A role is a collection of privileges that you assign to a user or group. A role represents a set of privileges to access secure MDM Hub resources.

For users to view or manipulate a secure MDM Hub resource, those users must be assigned roles that grant them sufficient privileges to access the resource. Roles determine what a user is authorized to access and which tasks they can perform in the MDM Hub.

MDM Hub roles are highly granular and flexible, which allows administrators to implement complex security safeguards according to the security policies of their organization. Some users, such as administrators, might be assigned a single role with access to everything. Other users, such as data stewards, might have a role with explicitly restricted privileges.

A role can also have other roles assigned to it, thereby inheriting the access privileges configured for those roles. Privileges are additive, meaning that, when you combine roles, you combine the privileges of those roles as well. For example, Role A has read privileges to an Address base object, and Role B has create and update privileges to it. If a user account is assigned Role A and Role B, then that user account will have read, create, and update privileges to the Address base object. A user account inherits the privileges configured for any role to which the user account is assigned.

Role Configuration

You can create, edit, and delete roles in the MDM Hub.

Note: If you use a comprehensive centralized security deployment, in which users are authorized externally, you do not need to configure roles.

Resource privileges vary based on the scope of access required for users to do their jobs. The best practice for administrators is to follow the principle of least privilege. Assign to users the lowest level of privilege needed to do their work.

Adding Roles

To configure roles and assign access privileges to MDM Hub resources, use the Roles tool in the Security Access Manager workbench.

Tip: Avoid spaces in role names. Spaces can cause errors when the MDM Hub communicates with ActiveVOS.

1. Start the Roles tool.
2. Acquire a write lock.
3. Point anywhere in the navigation pane, right-click, and choose **Add Role**.

   The Roles tool displays the Add Role dialog box.
4. Enter the name of the role.
5. Enter an optional description of the role.
6. Enter an external name, or alias, of the role.
7. Click **OK**.

   The new role appears in the roles list.

Editing and Deleting Roles

To edit or delete an existing role, use the Roles tool in the Security Access Manager workbench.

1. Start the Roles tool.
2. Acquire a write lock.
3. Scroll the roles list and select the role that you want to edit.
   - For each property that you want to edit, click the **Edit** button next to it, and specify the new value.
   - Point anywhere in the navigation pane, right-click, and choose **Delete Role**, and click **Yes** when prompted for confirmation.
4. Click the **Save** button to save your changes.

Privileges

With MDM Hub internal authorization, you can assign privileges to roles.

You can assign the following privileges to roles:

Read

User can view but not change data.

Create

User can create data records in the Hub Store

Update

User can update data records in the Hub Store.

Delete

User can delete data records in the Hub Store.

Merge

User can merge and unmerge data.

Execute

User can run cleanse functions and batch groups.

Privileges determine the access that external application users have to MDM Hub resources. For example, you can configure a role to have read, create, update, and merge privileges on particular packages.

Note: Each privilege is distinct and must be explicitly assigned. Privileges do not aggregate other privileges. For example, a user who has update access to a resource does not necessarily have read access to it. Both privileges must be individually assigned.

When you use the Hub Console, privileges are not enforced although the settings still affect the use of the Hub Console. For example, data stewards cannot view any packages in the Merge Manager and Data Manager except those for which they have read privileges. For data stewards to edit and save changes to data in a particular package, they must have update and create privileges for that package.

If data stewards do not have update or create privileges, then they cannot change any data in the Data Manager. Similarly, a data steward must have merge privileges to use the Merge Manager to merge or unmerge records. To learn more about the Merge Manager and Data Manager tools, see the *Multidomain MDM Data Steward Guide*.

Internal Roles and External Roles

In a role-based centralized security implementation, you must create a mapping between the MDM Hub internal role and the external role that is managed separately from the MDM Hub.

The name of the external role name might differ from the internal role name used in a MDM Hub environment.

Configuration details depend on the role mapping implementation of the security provider. You map roles in a configuration file. You can map one external role to more than one internal role.

Note: Although mappings are often created in XML, there is no predefined format for a configuration file. It might not be an XML file or even a file. The mapping is part of the custom user profile or authentication provider implementation. The purpose of the mapping is to populate a user profile object roles list with internal role IDs.

Assigning Resource Privileges to Roles

You can use the Roles tool in the Security Access Manager workbench to assign and edit resource privileges for roles.

1. Start the Roles tool.
2. Acquire a write lock.
3. Scroll the roles list and select the role to which you want to assign resource privileges.
4. Click the **Resource Privileges** tab.

5. Expand the Resources hierarchy to show the secure resources that you want to configure for this role.
6. For each resource that you want to configure:
   - Select any privilege that you want to grant to this role.
   - Clear any privilege that you want to remove from this role.
7. Click the **Save** button to save your changes.

Assigning Roles to Other Roles

A role can also inherit other roles, except a role to which it already belongs. For example, if you assign Role B to Role A, then Role A inherits the access privileges of Role B.

1. Start the Roles tool.
2. Acquire a write lock.
3. Scroll the roles list and select the role to which you want to assign other roles.
4. Click the **Roles** tab.

   The Roles tool displays any roles that can be assigned to the selected role.
5. Select any role that you want to assign to the selected role.
6. Clear any role that you want to remove from this role.
7. Click the **Save** button to save your changes.

Generating a Report of Resource Privileges for Roles

You can generate a report that describes the resource privileges granted to a particular role.

1. Start the Roles tool.
2. Acquire a write lock.
3. Scroll the roles list and select the role for which you want to generate a report.
4. Click the **Report** tab.
5. Click **Generate**.

   The Roles tool generates the report and displays it in the Report tab.

Saving the Generated Report as an HTML File

1. Click **Save**.

   The Roles tool prompts you to specify the target location for the saved report.
2. Navigate to the target location.
3. Click **Save**.

   The Security Access Manager saves the report using the following naming convention:

   <*ORS_Name*>-<*Role_Name*>-RolePrivilegeReport.html

   where:

   - *ORS_Name* is the name of the target database.
   - *Role_Name* is the role associated with the generated report.

   The Roles tool saves the current report as an HTML file in the target location. You can subsequently display this report using a browser.

CHAPTER 4

Users and User Groups

This chapter includes the following topics:

Users and User Groups Overview

An MDM Hub user is an individual who can access MDM Hub resources.

User accounts are defined in the Master Database in the Hub Store. For an introduction to MDM Hub users, see the *Multidomain MDM Overview Guide*.

A user account gains access to MDM Hub resources using the roles assigned to it, inheriting the privileges configured for each role.

You can use the Users tool in the Configuration workbench to configure user accounts for MDM Hub users, as well as to change passwords and enable external authentication. External applications with sufficient authorization can also register user accounts using SIF requests, as described in the *Multidomain MDM Services Integration Framework Guide*.

User Configuration

You can create, edit, and delete users in the MDM Hub.

Depending on how you have deployed security, your MDM Hub implementation might require that you add users to the Master Database.

You must configure users in the Master Database in the following scenarios:

- You are using internal authorization in the MDM Hub.
- You are using external authorization with the MDM Hub.
- Multiple users access the Hub Console using different accounts.

A user needs to be defined only once, even if the same user will access more than one Operational Reference Store associated with the Master Database.

User Access to MDM Hub Resources

Users, including administrators and data stewards, can access MDM Hub resources in the following ways:

MDM Applications

Users can interact with the MDM Hub by logging into the Hub Console and using the tools to which they have access. Users can also use IDD or the Provisioning tool to access data in base objects and business entities.

Third-Party Applications

Users can interact with MDM Hub data indirectly using third-party applications that use SIF classes. These users never log into the Hub Console. They log in to the MDM Hub using applications that can invoke SIF classes. These users are known as external application users. To learn more about the kinds of SIF requests that developers can invoke, see the *Multidomain MDM Services Integration Framework Guide*.

Adding User Accounts

Use the Users tool in the Security Access Manager workbench to add a user account to the MDM Hub.

1. Start the Users tool.
2. Acquire a write lock.
3. Click the **Users** tab.
4. Click the **Add user** button.

   The Users tool displays the **Add User** dialog box.
5. Enter a first, middle, and last name for the user.
6. Enter a user name for the user.

   Note: User names are case-insensitive and are stored as lowercase characters.
7. Enter a valid email address for the user. The MDM Hub sends the password for this user account to this email address.
8. Enter the default database for the user. This is the database that is selected by default when the user logs in to Hub Console.
9. If the user account is for an application, select the **Application user** check box.

   Note: Application users are used for certificate-based authentication of requests that are generated by a trusted application on behalf of the user.
10. Enter and verify a password for the user.
11. Choose the type of authentication.
    - Select the **Use external authentication** check box if your MDM Hub implementation uses authentication through a third-party security provider.
    - Clear the **Use external authentication** check box if you want to use the internal authentication in the MDM Hub.
12. Browse for a public certificate for the user. This certificate can be used by the MDM Hub for authentication of user requests.

    Note: If the user account is for an application user, you must select a certificate.

13. Click **OK**.

    The Users tool adds the new user to the list of users on the **Users** tab.

Editing and Deleting User Accounts

You can use the Users tool in the Security Access Manager workbench to edit or remove user accounts.

1. Start the Users tool.
2. Acquire a write lock.
3. Click the **Users** tab.
4. If you want to delete a user, select the user account that you want to remove.
5. Click the **Delete** button.

   The Users tool prompts you to confirm deletion.
6. Click **Yes** to confirm deletion.

   The Users tool removes the deleted user account from the list of users.
7. If you want to edit a user, select the user account that you want to configure.
8. To change a name, double-click the cell and type a different name.
9. Select a different login database and server, if you want.
10. Select the **Administrator** check box to give this user administrative access, which allows them to have access to all Hub Console tools and all databases.
11. Select the **Enable** check box to activate this user account and allow this user to log in.

    Note: If you use external authentication for a user, you cannot disable the user account through the Hub Console.
12. Click the **Save** button.

    The Users tool saves your changes to the user account.

Editing Supplemental User Information

You can use the MDM Hub to manage supplemental information for each user, such as an email address or phone numbers. The MDM Hub does not require that you provide this information, nor does the MDM Hub use this information in any special way.

Note: You cannot change the email address for the `admin` user in the Hub Console. To change the email address for the admin user, update the admin user entry directly in the C_REPOS_USER table under CMX_SYSTEM schema.

1. Start the Users tool.
2. Acquire a write lock.
3. Click the **Users** tab.
4. Select the user whose properties you want to edit.
5. Click the **Edit** button.

   The Users tool displays the **Edit User** dialog box.
6. Specify any of the properties of the user, such as title, email address, or login message. The login message is the message that the Hub Console displays after this user logs in.
7. Click **OK**.
8. Click the **Save** button to save your changes.

Changing Password Settings for User Accounts

You can change password settings for a user. The latest information about the latest password and who changed the password is maintained. Password history is not available.

1. Start the Users tool.
2. Acquire a write lock.
3. Click the **Users** tab.
4. Select the user whose password you want to change.
5. Click the **Change Password** button.

   The Users tool displays the **Change Password** dialog box for the selected user.
6. Specify and verify the new password.
7. Choose the type of authentication.
   - Select the **Use external authentication** check box if your MDM Hub implementation uses authentication through a third-party security provider.
   - Clear the **Use external authentication** check box if you want to use the internal authentication in the MDM Hub.
8. Click **OK**.

Configuring User Access to Operational Reference Store

You can configure user access to Operational Reference Store databases.

1. Start the Users tool.
2. Acquire a write lock.
3. Click the **Target Database** tab.

   The Users tool displays the Target Database tab.
4. Expand each database node to see which users that can access that database.
5. To change user assignments to a database, right-click the database name and choose **Assign User**.

   The Users tool displays the **Assign User to Database** dialog box.
6. Select the names of any users that you want to assign to the selected database.
7. Clear the names of any users that you do not want to assign to the selected database.
8. Click **OK**.

Password Policy Configuration

You can define global password policies for all users. Configure private password policies that override the global password policies for individual users. All passwords are case-sensitive.

Note: If you deploy the MDM Hub on the JBoss application server with security enabled, ensure that the password that you set adheres to the JBoss password policy. Your password must also adhere to the MDM Hub global password policy. This is important because the passwords for the Hub Console and for JBoss must match.

Password Policy Settings

You can specify password policy settings for the MDM Hub users.

The MDM Hub allows you to set users the following private password policies:

Password Length

Minimum and maximum length of a password in characters.

Password Expiry

Specifies whether a password expires or not, and the number of days for which a password is valid.

Select the **Password expires** check box to set an expiry period for passwords. Clear the **Password expires** check box to set passwords that do not expire.

If you select the **Password expires** check box, specify the number of days in which the password must expire. The minimum password expiry period that you can set is `10`.

Login Settings

Number of grace logins and maximum number of failed logins allowed.

Password History

Number of times that a password can be reused.

Password Requirements

Select the **Password pattern validation enabled** check box to enforce a password pattern. You can specify the following criteria for password pattern:

- Minimum number of unique characters
- Password must start with
- Password must contain
- Password must end with

Managing Global Password Policy

The global password policy applies to users who do not have private password policies specified for them.

1. Start the **Users** tool.
2. Acquire a write lock.
3. Click the **Global Password Policy** tab.

   The Global Password Policy window appears.
4. Specify the password policy settings.
5. Click **OK**.
6. Click the **Save** button to save your global settings.

Managing Private Password Policies

You can specify a private password policy that overrides the global password policy for any user.

Note: Best practise for password policy management is to ensure most user passwords are managed by a global policy instead of by many private policies.

1. Start the Users tool.

2. Acquire a write lock.
3. Click the **Users** tab.
4. Select the user for whom you want to set the private password policy.
5. Click the **Manage password policy** button.

   The **Private Password Policy** window for the selected user appears.
6. Enable the **Private password policy enabled** option.
7. Specify the password policy settings for the user.
8. Click **OK**.
9. Click the **Save** button to save your changes.

JDBC Data Sources Security Configuration

In MDM Hub implementations, if a JDBC data source uses application server security, you must configure settings in the cmxserver.properties file.

You must store the user name and password for the application server for the JDBC data source in the cmxserver.properties file. Passwords cannot appear as clear text. You must encrypted passwords before saving them in the cmxserver.properties file.

To learn more about secured JDBC data sources, see your application server documentation.

User Names and Passwords for a Secured JDBC Data Source

To configure user names and passwords for a secured JDBC data source in the cmxserver.properties file, use the following parameters:

```
databaseId.username=username
databaseId.password=encryptedPassword
```

where databaseId is the unique identifier of the JDBC data source.

Database ID for Oracle SID Connection Types

For an Oracle SID connection type, the databaseId consists of the following strings:

```
<database hostname>-<Oracle SID>-<schema name>
```

For example, with the following settings:

- `<database hostname>` = `localhost`
- `<Oracle SID>` = `MDMHUB`
- `<schema name>` = `Test_ORS`

the user name and password properties would be:

```
localhost-MDMHUB-Test_ORS.username=weblogic
localhost-MDMHUB-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Database ID for Oracle Service Connection Types

For an Oracle Service connection type, the databaseId consists of the following strings:

```
<service name>-<schema name>
```

For example, with the following settings:

- `<service name>` = `MDM_Service`
- `<schema name>` = `Test_ORS`

the user name and password properties would be:

```
MDM_Service-Test_ORS.username=weblogic
MDM_Service-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Database ID for IBM Db2 Connection Types

For an IBM Db2 connection type, the databaseId consists of the following strings:

```
<database hostname>-<database name>-<schema name>
```

For example, with the following settings:

- `<database hostname>` = `localhost`
- `<database name>` = `dsui2`
- `<schema name>` = `DS_UI2`

the user name and password properties would be:

```
localhost-dsui2-DS_UI2.username=weblogic
localhost-dsui2-DS_UI2.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Database ID for Microsoft SQL Server Connection Types

For a Microsoft SQL Server connection type, the databaseId consists of the following strings:

```
<database hostname>-<database name>
```

For example, with the following settings:

- `<database hostname>` = `localhost`
- `<database name>` = `ds_ui1`

the user name and password properties would be:

```
localhost-ds_ui1.username=weblogic
localhost-ds_ui1.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Database ID for the Master Database

If you want to secure the JDBC data source that accesses the Master Database, the `databaseId` is CMX_SYSTEM. In this case, the properties would be:

```
CMX_SYSTEM.username=weblogic
CMX_SYSTEM.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Password Encryption

To generate an encrypted password for a database schema, use the following commands:

```
C:\>java -cp siperian-common.jar com.siperian.common.security.Blowfish password
Plaintext Password: password
Encrypted Password: 9C03B113CD8E4BBFD236C56D5FEA56EB
```

User Group Configuration

A user group is a logical collection of user accounts.

User groups simplify security administration. For example, you can combine external application users into one user group, and then grant security roles to the user group instead of to each individual user. In addition to users, user groups can contain other user groups.

You use the Groups tab in the Users and Groups tool in the Security Access Manager workbench to configure users groups.

Starting the Users and Groups Tool

You start the Users and Groups tool in the Hub Console.

1. In the Hub Console, connect to an Operational Reference Store, if you have not already done so.
2. Expand the Security Access Manager workbench and click **Users and Groups**.

   The Hub Console displays the Users and Groups tool.

   The Users and Groups tool contains the following tabs:

   Groups

   Used to define user groups and assign users to user groups.

   Users Assigned to Database

   Used to associate user accounts with a database.

   Assign Users/Groups to Role

   Used to associate users and user groups with roles.

   Assign Roles to User / Group

   Used to associate roles with users and user groups.

Adding User Groups

You can use the Users and Groups tool in the Security Access Manager workbench to add user groups.

1. Start the Users and Groups tool.
2. Acquire a write lock.
3. Click the **Groups** tab.
4. Click the **Add** button.

   The Users and Groups tool displays the **Add User Group** dialog box.
5. Enter a descriptive name for the user group.
6. Optionally, enter a description of the user group.

7. Click **OK**.

   The Users and Groups tool adds the new user group to the list.

Editing and Deleting User Groups

You can also use the the Users and Groups tool to edit or remove user groups.

1. Start the Users and Groups tool.
2. Acquire a write lock.
3. Click the **Groups** tab.
4. Scroll the list of user groups and select the user group that you want to edit.
5. If you want to remove a user group, click the **Delete** button.

   The Users and Groups tool prompts you to confirm deletion.
6. Click **Yes**.

   The Users and Groups tool removes the deleted user group from the list.
7. If you want to edit a user group, click the **Edit** button next to each property that you want to edit, and specify the new value.
8. Click the **Save** button to save your changes.

Assigning Users and Users Groups to User Groups

To assign members to a user group:

1. Start the Users and Groups tool.
2. Acquire a write lock.
3. Click the **Group** tab.
4. Scroll the list of user groups and select the user group that you want to edit.
5. Right-click the user group that you just created and choose **Assign Users and Groups**.

   The Users and Groups tool displays the **Assign to User Group** dialog box.
6. Select the names of any users and user groups that you want to assign to the selected user group.
7. Clear the names of any users and user groups that you do not want to assign to the selected user group.
8. Click **OK**.

Assigning Users to the Current ORS Database

To assign users to the current Operational Reference Store database:

1. Start the Users and Groups tool.
2. Acquire a write lock.
3. Click the **Users Assigned to Database** tab.
4. Click the **Assign users to database** button to assign users to an Operational Reference Store database.

   The Users and Groups tool displays the **Assign User to Database** dialog box.
5. Select the names of any users that you want to assign to the selected Operational Reference Store database.

6. Clear the names of any users that you do not want to assign to the selected Operational Reference Store database.
7. Click **OK**.

Associations between Roles and Users and User Groups

You can associate roles with users and user groups. You can use the **Users and Groups** tool to associate roles with users in the following ways:

- Assign users and user groups to roles.
- Assign roles to users and user groups.

Choose the way that is most appropriate for your implementation.

Assigning Users and User Groups to Roles

To assign users and user groups to a role:

1. Start the Users and Groups tool.
2. Acquire a write lock.
3. Click the **Assign Users/Groups to Role** tab.
4. Select the role to which you want to assign users and user groups.
5. Click the **Edit** button.

   The Users and Groups tool displays the **Assign Users to Role** dialog box.
6. Select the names of any users and user groups that you want to assign to the selected role.
7. Clear the names of any users and user groups that you do not want to assign to the selected role.
8. Click **OK**.

Assigning Roles to Users and User Groups

To assign roles to users and user groups:

1. Start the Users and Groups tool.
2. Acquire a write lock.
3. Click the **Assign Roles to User/Group** tab.
4. Select the user or user group to which you want to assign roles.
5. Click the **Edit** button.

   The Users and Groups tool displays the **Assign Roles to User** dialog box.
6. Select the roles that you want to assign to the selected user or user group.
7. Clear the roles that you do not want to assign to the selected user or user group.
8. Click **OK**.

CHAPTER 5

Security Providers

This chapter includes the following topics:

Security Providers Overview

A security provider is a third-party application that provides security services, such as authentication and authorization, for users that access the MDM Hub. Security providers are part of some MDM Hub security deployment scenarios.

A provider file contains profile information for a security provider. If you want to use other third-party security providers, use the Security Providers tool to upload provider files to the MDM Hub. You can also use the Security Providers tool to modify, delete, enable, or disable security providers in the Providers list.

The MDM Hub comes with a set of default internal security providers. You can also add third-party security providers. Internal security providers cannot be removed.

Security Provider Management

You can manage security providers in the MDM Hub implementation through the Security Providers tool in the Configuration workbench of the Hub Console.

You can add security providers from the default selection internal to the MDM Hub or from you own custom-added selection of providers. Internal security providers cannot be removed.

The MDM Hub supports the following types of security providers:

Authentication provider

Authenticates a user by validating their identity. Informs the MDM Hub that users are who they claim to be. This type of security provider does not validate whether users have the required privileges to access particular MDM Hub resources.

Authorization provider

Informs the MDM Hub whether users have the required privileges to access particular MDM Hub resources.

User profile provider

Informs the MDM Hub about individual users, such as user-specific attributes and the roles to which the user belongs.

Internal providers represent internal MDM Hub implementations for authentication, authorization, and user profile services.

Some of the MDM Hub default providers are super providers. Super providers always return a positive response for authentication and authorization requests. Use a super provider in a development environment when you do not want to configure users, roles, and privileges. Super providers can also be used in a production environment in which security is provided as a layer on top of the SIF requests for performance gains.

Provider File Management

A provider file contains profile information for a security provider.

If you want to use your own third-party security providers, you must explicitly register them though the Security Providers tool. To register a security provider, you upload a provider file that contains the profile information needed for registration.

A provider file is a JAR file that contains the following data:

- A manifest that describes one or more external security providers. Each security provider has the following settings:
  - Provider Name
  - Provider Description
  - Provider Type
  - Provider Factory Class Name
  - Properties that specify configuration details for the provider. This can be a list of name-value pairs: property names with default values.
- Provider implementation and any required third-party libraries.

The InformaticaResource Kit copies a sample implementation of a provider file on the Hub Server. For more information about the sample provider file, see the *Multidomain MDM Resource Kit Guide*.

Uploading a Provider File

Upload a provider file to add or update provider information.

1. Start the Security Providers tool.
2. Acquire a write lock.

3. In the left navigation pane, right-click Provider Files and choose **Upload Provider File**.

   The Security Provider tool prompts you to select the JAR file for this provider.

4. Specify the JAR file, navigating the file system as needed and selecting the JAR file that you want to upload.
5. Click **Open**.

   The Security Provider tool checks the selected file to determine whether it is a valid provider file.

6. If the provider file you upload has the same name as an existing provider file, then the Security Provider tool asks you whether to overwrite the existing provider file. Click **Yes** to confirm.

   The Security Provider tool populates the Providers list with the additional provider information. After you upload the provider file, you can remove the original file from the file system.

Deleting a Provider File

You can delete a provider file if you no longer use that security provider.

1. Start the Security Providers tool.
2. Acquire a write lock.
3. In the left navigation pane, right-click the provider file that you want to delete, and then choose **Delete Provider File**.

   The Security Provider tool prompts you to confirm deletion.

4. Click **Yes**.

   The Security Provider tool removes the deleted provider file from the list.

   Note: You cannot delete the internal provider files that ship with the MDM Hub.

Security Provider Settings

The Security Providers tool displays a list of registered providers.

The list of registered providers is sorted by provider type. The sequence of providers in the Provider list also represents the order in which they are invoked. A user needs to be authenticated by at least one provider in the Provider list.

For example, when you attempt to log in and supply your user name and password, the MDM Hub submits your login credentials to each authentication provider in the authentication list. The MDM Hub proceeds sequentially through the list. If authentication succeeds with one of the providers in the list, then MDM Hub authenticates you. If authentication fails with all available authentication providers, then you are not authenticated.

Changing Security Provider Settings

To change the settings for a security provider, perform the following steps:

1. Start the Security Providers tool.
2. Acquire a write lock.
3. Select the security provider that you want to modify.
4. In the Properties panel, click the **Edit** button next to any setting that you want to edit.

5. Click the **Save** button to save your changes.

Enabling and Disabling Security Providers

1. Acquire a write lock.
2. Select the security provider that you want to enable or disable.
   - Check the **Enabled** check box to enable a disabled security provider.
   - Clear the **Enabled** check box to disable a security provider.

   Once disabled, the provider name is unavailable and moves to the end of the Providers list. You cannot rearrange disabled providers in the Providers list.
3. Click the **Save** button to save your changes.

Moving a Security Provider in the Processing Order

MDM Hub processes security providers in the order in which they appear in the Providers list. You can rearrange the order in which the security providers appear.

1. Start the Security Providers tool.
2. Acquire a write lock.
3. To move a provider up, right-click the provider you want to move and select **Move Provider Up**.

   The Security Provider tool moves the provider ahead of the previous one in the Providers list, and then refreshes the navigation pane.
4. To move a provider down, right-click the provider you want to move and select **Move Provider Down**.

   The Security Provider tool moves the provider under the previous one in the Providers list, and then refreshes the navigation pane.

Provider Properties

The Provider panel contains the following fields:

Name

Name of this security provider.

Description

Description of this security provider.

Provider Type

Type of security provider. They type can be one of the following values:

- Authentication
- Authorization
- User Profile

Provider File

Name of the provider file associated with this security provider, or **Internal Provider** for internal providers.

Enabled

Indicates whether this security provider is enabled or not. An enabled security provider is checked. A disabled security provider is not checked. Note that internal providers cannot be disabled.

Properties

Additional properties for this security provider, if defined by the security provider. Each property is a name-value pair. A security provider might require or allow unique properties that you can specify here.

Adding Provider Properties

To add provider properties, perform the following steps.

1. Start the Security Providers tool.
2. Acquire a write lock.
3. In the navigation pane, select the authentication provider for which you want to add properties.
4. Click the **Add** button.

   The Security Providers tool displays the Add Provider Property dialog box.
5. Specify the name of the property.
6. Specify the value to assign to this property.
7. Click **OK**.

Editing Provider Properties

To edit an existing provider property, perform the following steps.

1. Start the Security Providers tool.
2. Acquire a write lock.
3. In the navigation pane, select the authentication provider for which you want to edit properties.
4. For each property that you want to edit, click the **Edit** button next to it, and specify the new value.
5. Click the **Save** button to save your changes.

Custom Providers

You can package custom provider classes in the JAR or ZIP file that comprise the provider file.

Specify the settings for the custom providers in the `providers.properties` file. Then place the file within the JAR file in the META-INF directory. The settings are then translated by the loader to what appears in the Hub Console.

A provider.properties file has the following elements:

ProviderList

Comma-separated list of the contained provider names.

File-Description

Description of the package.

XXX-Provider-Name

Display name of the provider *XXX*.

XXX-Provider-Description

Description of the provider *XXX*.

XXX-Provider-Type

Type of the provider *XXX*. The possible values are `USER_PROFILE_PROVIDER`, `JAAS_LOGIN_MODULE`, and `AUTHORIZATION_PROVIDER`.

XXX-Provider-Factory-Class-Name

Implementation class of the provider, which is also in the same JAR or ZIP file.

XXX-Provider-Properties

Comma-separated list of name/value pairs that define provider properties.

Note: The provider archive file must contain all the classes required for the custom provider to be functional, in addition to the required resources. These resources are specific to your implementation.

Sample providers.properties File

Note: All of the settings are required except for *XXX*-Provider-Properties.

```
ProviderList=ProviderOne,ProviderTwo,ProviderThree,ProviderFour
ProviderOne-Provider-Name: Sample Role Based User Profile Provider
ProviderOne-Provider-Description: Sample User Profile Provider for roled-based management
ProviderOne-Provider-Type: USER_PROFILE_PROVIDER
ProviderOne-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleRoleBasedUserProfileProviderFactory
ProviderOne-Provider-Properties: name1=value1,name2=value2
ProviderTwo-Provider-Name: Sample Login Module
ProviderTwo-Provider-Description: Sample Login Module
ProviderTwo-Provider-Type: JAAS_LOGIN_MODULE
ProviderTwo-Provider-Factory-Class-Name: com.siperian.sam.sample.authn.SampleLoginModule
ProviderTwo-Provider-Properties:
ProviderThree-Provider-Name: Sample Role Based Authorization Provider
ProviderThree-Provider-Description: Sample Role Based Authorization Provider
ProviderThree-Provider-Type: AUTHORIZATION_PROVIDER
ProviderThree-Provider-Factory-Class-Name:
com.siperian.sam.sample.authz.SampleAuthorizationProviderFactory
ProviderThree-Provider-Properties:
ProviderFour-Provider-Name: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Description: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Type: USER_PROFILE_PROVIDER
ProviderFour-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleComprehensiveUserProfileProviderFactory
ProviderFour-Provider-Properties:
File-Description=The sample provider files
```

External Authentication

You can use external authentication with the MDM Hub for users through the Java Authentication and Authorization Service (JAAS).

MDM Hub provides templates for the following types of authentication standards:

- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory

These templates provide the settings, such as protocols, server names, and ports, that are required for these authentication standards. You can use these templates to add a new login module with the settings you need. For more information about these authentication standards, see the applicable vendor documentation.

Adding a Login Module

To set up external authentication in MDM Hub, you must create a login module.

1. Start the Security Providers tool.
2. Acquire a write lock.
3. Right-click Authentication Providers (Login Modules) and select **Add Login Module**.

   The Security Providers tool displays the Add Login Module dialog box.
4. Click the down arrow and select a template for the login module.

   OpenLDAP-template

   Based on LDAP authentication properties.

   MicrosoftActiveDirectory-template

   Based on Active Directory authentication properties.

   Kerberos-template

   Based on Kerberos authentication properties.
5. Click **OK**.

   The Security Providers tool adds the new login module to the list.
6. In the Properties panel, click the **Edit** button next to any property that you want to edit. Specify the settings for the type of login module you want to create.
7. Click the **Save** button to save your changes.

Deleting a Login Module

You can delete a login module if you want.

1. Start the Security Providers tool.
2. Acquire a write lock.
3. In the navigation pane, right-click a login module under Authentication Providers (Login Modules) and choose **Delete Login Module**.

   The Security Provider tool prompts you to confirm deletion.
4. Click **Yes**.

   The Security Provider tool removes the deleted login module from the list and refreshes the left navigation pane.

CHAPTER 6

Application Level Security

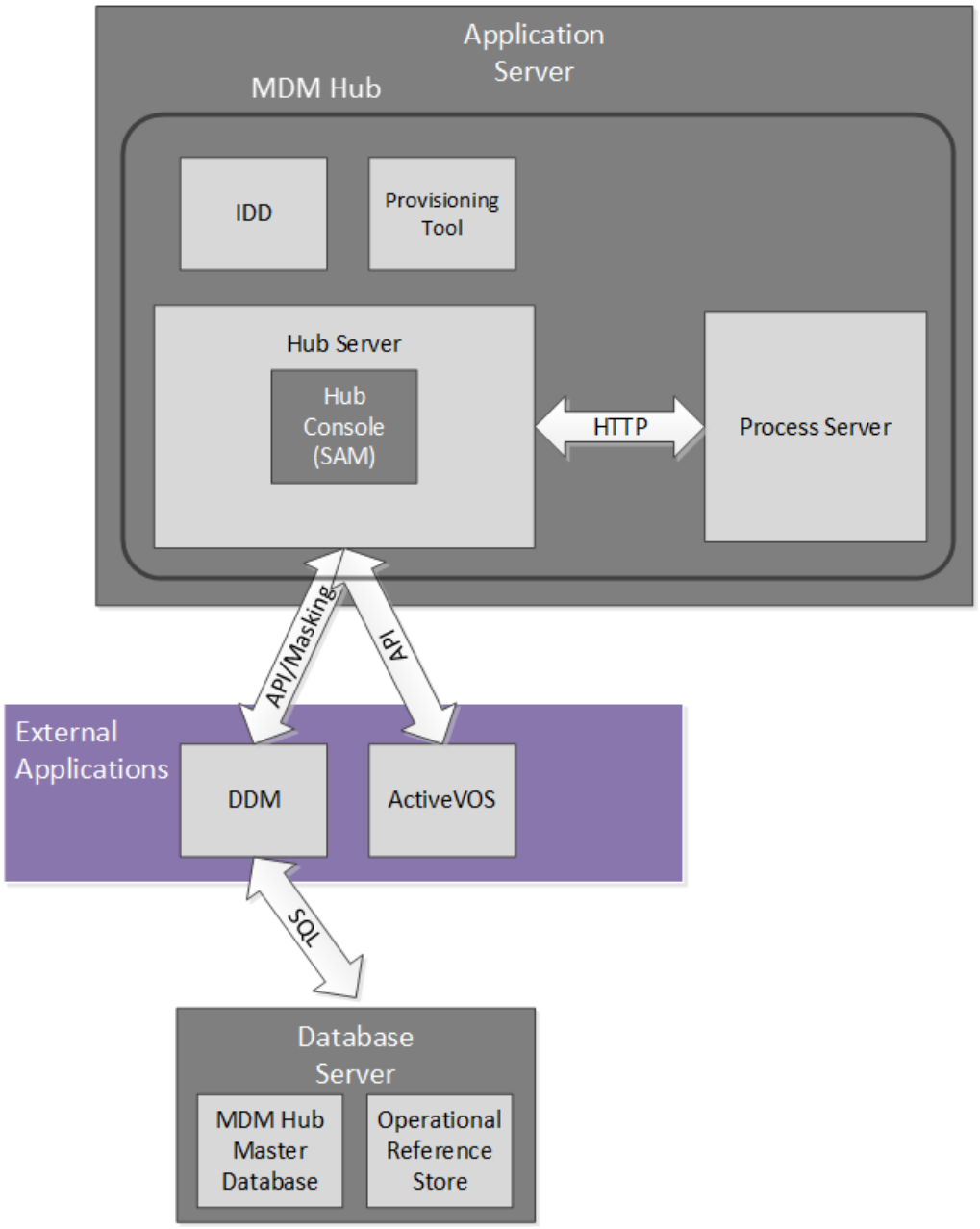
This chapter includes the following topics:

Application Level Security Overview

The Security Access Manager (SAM) is the security module for the MDM Hub, which controls user credentials and roles. Other applications and components within an MDM Hub implementation also have security settings to ensure that they communicate with the MDM Hub securely. For example, you can configure data-level security for Informatica Data Director.

Informatica conducts internal security tests of Informatica products. For example, Informatica uses industry-standard scanning applications to test products for security vulnerabilities, such as an SQL injection attack. Other Informatica security applications, used in conjunction with SAM, add an extra layer of security to an MDM Hub implementation. Informatica Dynamic Data Masking (DDM) applies a mask to data to prevent unauthorized access to sensitive information. The Informatica MDM Provisioning tool and Informatica ActiveVOS are not security applications but they still communicate securely with the MDM Hub.

The following image shows a sample MDM Hub implementation and how the components connect with one another:



Informatica Data Director

Informatica Data Director is a web-based data governance application for the MDM Hub. When you configure a Data Director application, business users can create, manage, consume, and monitor master data.

Informatica Data Director adheres to the top ten security recommendations of the Open Web Application Security Project (OWASP). Informatica uses IBM Security AppScan to test for security vulnerabilities, such as an SQL injection attack. The HTTP methods GET or POST can retrieve information from IDD, but other HTTP methods, such as DELETE or PUT, return an HTTP error.

When you configure a Data Director application, you can organize the tables in the Operational Reference Store into business entities or into subject areas. Both approaches provide a way to group related data that you want to treat as a unit, such as all data about a customer. Business entities are the recommended organizational approach since Multidomain MDM Version 10.1. Business entities are the core of the Entity 360 framework, which includes business entity services and modern entity views.

For data security, a Data Director application uses the user roles and resource privileges that are set on the Operational Reference Store. Recall that an MDM administrator uses the Security Access Manager workbench in the Hub Console to define resource privileges for each user role. In a Data Director application, users can perform the operations that are permitted by their user role.

The role privileges for business entities and subject areas are derived from the resource privileges in different ways, so the security might be slightly different. However, both approaches are equally secure. For more information about security for business entities, see the *Multidomain MDM Provisioning Tool Guide*. For more information about security configuration and data security for subject areas, see the *Multidomain MDM Data Director Implementation Guide*.

Provisioning Tool

Use the Provisioning tool to create business entity models based on the schema information that you defined in an Operational Reference Store (ORS). The business entity model is a foundational component of the Entity 360 framework in Data Director.

You must log in to the Provisioning tool before you can configure business entities.

As you work on the configuration files, you save your changes to a temporary workspace. The Provisioning tool does not apply changes until you publish your changes. If multiple users change the business entity configuration for an ORS simultaneously, the MDM Hub is updated with the most recently published configuration.

The Provisioning tool must run on the same application server as the Hub Server.

For more information, see the *Multidomain MDM Provisioning Tool Guide*.

ActiveVOS

Informatica ActiveVOS® is a business process management (BPM) tool that helps you to automate business processes. You can create process models that integrate people, processes, and systems, which increases the efficiency of your business.

You can use ActiveVOS to ensure that updated entity data goes through a change-approval workflow before the updated records contribute to the Best Version of the Truth (BVT) records. For example, a business process might require that a senior manager review and approve updates to customer data before it becomes master data.

To support a change-approval workflow, the MDM Hub and Data Director integrate with the ActiveVOS Server. Predefined MDM workflows, task types, and roles enable the components to synchronize with one another. You can configure your MDM implementation to work with the embedded ActiveVOS server. Alternatively, you can run a standalone instance of ActiveVOS in your environment.

Embedded ActiveVOS authenticates requests from Data Director and the MDM Hub by a specific principal that is trusted by both MDM and ActiveVOS. This principal is called the trusted user. The system administrator creates the credentials and roles for the trusted user in the application server.

The ActiveVOS server must run on the same application server as the MDM Hub. For more information, see the *Multidomain MDM Configuration Guide*.

Dynamic Data Masking

Informatica Dynamic Data Masking is a data security product that operates between a client and a database to prevent unauthorized access to sensitive information. Dynamic Data Masking intercepts requests sent to the database and applies a mask to the data before it sends the request results to the client.

Dynamic Data Masking provides an additional level of data security to databases that the MDM Hub manages. Use the Dynamic Data Masking Management Console to configure the Dynamic Data Masking connection to the Operational Reference Store and set up the masking rules for the data. You configure the MDM Hub connection to Dynamic Data Masking when you register an Operational Reference Store.

The MDM installer does not install Dynamic Data Masking with the MDM Hub. You must install Dynamic Data Masking separately. For more information about Dynamic Data Masking installation, see the Dynamic Data Masking documentation.

Note: To use Dynamic Data Masking in the MDM Hub, you must have Dynamic Data Masking 9.6.0 and Emergency Bug Fix 14590 installed. Earlier versions of Dynamic Data Masking are not compatible with the MDM Hub.

Integration Between Dynamic Data Masking and the MDM Hub

After you have Dynamic Data Masking installed and set up correctly, you can integrate Dynamic Data Masking with the MDM Hub.

The following steps describe the integration process:

1. In the Dynamic Data Masking Management Console, create a Dynamic Data Masking service. Configure the listener port number to match the port number where the client sends requests to the database.
2. Define the database connection properties for the database that requires data masking.
3. Create a connection rule. Configure the rule to identify the database requests that must be masked. Assign a database and a security rule set to the connection rule set.
4. Create a security rule set. Define the rules for masking the data sent back to the MDM Hub.
5. In the Hub Console, configure the connection to Dynamic Data Masking.

When you run processes for the Operational Reference Store, Dynamic Data Masking applies the rules on the database before it returns data to the MDM Hub.

Note: If you do not add the Dynamic Data Masking connection to the Operational Reference Store, the MDM Hub bypasses any Dynamic Data Masking rules that you define.

For more information about how to configure Dynamic Data Masking, see the *Informatica Dynamic Data Masking Administrator Guide*.

Dynamic Data Masking Best Practices for the MDM Hub

You can use Dynamic Data Masking effectively in the MDM Hub with the help of suggested best practices.

Best practice to create Dynamic Data Masking rules in the Rule Editor

Dynamic Data Masking evaluates rules in the Rule Editor from the top to the bottom. Therefore, if you create non-masking rules, you must put them above any masking rules you create so they can be effective.

Best practice to allow users to view unmasked data

Dynamic Data Masking does not mask data in the database. When you view data in the MDM Hub, the data appears masked. Use Create View statements in Dynamic Data Masking to give users privileges to view unmasked data.

Best practice to block users

To block users from adding a record to which masking is applied, you must create a separate rule for each affected base object. Define a text matcher as `%INSERT%<BO_NAME>%<ROLE NAME>%` and the Block Statement processing action.

Best practice to allow users to update masked data

By default, the Dynamic Data Masking engine prevents users from editing tables with masked data. If you want to update masked data in the MDM Hub, you can create a rule in the Dynamic Data Masking Rule Editor to allow a user to update masked columns.

Best practice to create rules with MDM_SYSTEM indicator

In the MDM Hub, the user MDM_SYSTEM is an internal indicator for system calls. MDM_SYSTEM does not appear in the roles list in the Hub Console. Dynamic Data Masking applies masking based on the MDM Hub roles that a user has. When you create Dynamic Data Masking rules in the Rule Editor, do not create rules for the MDM_SYSTEM indicator alone. YouChart of Accounts Installation and Configuration Guide must combine MDM_SYSTEM with a user name or roles that belong to a user. You can combine the MDM_SYSTEM indicator with any other rule to create fine-grained rules in Dynamic Data Masking.

Setting up Dynamic Data Masking for an Operational Reference Store

You configure the Dynamic Data Masking connection to the MDM Hub when you register an Operational Reference Store through the Hub Console.

1. Start the Hub Console.

   The **Change database** dialog box appears.
2. Select the MDM Hub Master database, and click **Connect**.
3. On the Configuration workbench, start the **Databases** tool.
4. Acquire a write lock.
5. Click the **Register database** button.

   The **Informatica MDM Hub Connection Wizard** appears and prompts you to select the database type.
6. Select the type of database, and click **Next**.
7. Configure connection properties for the database.
8. In the **Port** field, the port you enter must match the Dynamic Data Masking listener port for the database.
9. In the **DDM connection URL** field, enter the URL for the Dynamic Data Masking server.
10. Click **Finish**.

The **Registering Database** dialog box appears.

11. Click **OK**.

    The MDM Hub registers the Operational Reference Store.

12. Select the Operational Reference Store that you registered, and click the **Test database connection** button to test the database settings.

    If you use WebSphere, restart WebSphere before you test the database connection.

    The Test Database dialog box displays the result of the database connection test.

13. Click **OK**.

    Dynamic Data Masking connects to the Operational Reference Store that you registered.

Setting Up a WebLogic T3S Channel on Linux

The WebLogic T3S is a SSL based protocol, which you can set up for the MDM Hub.

The following steps assume that you are familiar with how to create and use a keystore, configure a server instance for SSL, and create a channel. For more information, see the WebLogic documentation.

1. Before you begin, you must have a keystore that you want to use for identity purposes.
2. In the WebLogic Administration Console, navigate to the server instance that you use with MDM and configure SSL with the following properties:
   - **Identity and Trust Location** = **Keystore**
   - **Private Key Location** = **from Custom Identity Keystore**
   - **Private Key Alias** = <Alias defined in the keystore>
   - **Private Key Passphrase** = <Passphrase defined in the keystore>
   - **Certificate Location** = **from Custom Identity Keystore**
   - **Trusted Certificate Authorities** = **from Java Standard Trust Keystore**
3. Open an Administrator Command Prompt (cmd) window and use the `keytool` command to import the keystore into the JDK and JRE directories under `lib/security/cacerts`.
   The following sample code shows the syntax:

   ```
   keytool -import -alias <SSL Private Key Alias> -keystore "<JDK installation
   directory>/jre/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/
   Oracle_Home/user_projects/domains/base_domain/servers/<WebLogic server instance>/
   keystores/wls12c_server.cer" -v

   keytool -import -alias <SSL Private Key Alias> -keystore "<JRE installation
   directory>/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/
   user_projects/domains/base_domain/servers/<WebLogic server instance>/keystores/
   wls12c_server.cer" -v
   ```

   Note: If you need help with the `keytool` command, see the Java documentation.
4. Navigate to the `<WebLogic domain>/bin/startWebLogic.sh` file and set the following Java option:

   ```
   -Doracle.jdbc.J2EE13Compliant=true
   ```
5. In the WebLogic Administration Console, create a T3S channel that matches the SSL configuration. Set the following properties:
   - **Name** = <Name for the channel>
   - **Protocol** = t3s

- **Listen Address** = <Host name defined in the keystore>
- **Listen Port** = <Port defined in the keystore>
- Select **Tunneling Enabled**
- Select **Two Way SSL**
- Verify that the **Server Private Key Alias** displays the alias that you specified when you configured SSL.

6. Save the channel, and verify that the channel appears in the list of network channels.
7. If you use Informatica Data Director with the Entity 360 views, navigate to the `<WebLogic domain>/bin/setDomainEnv.sh` file and set the following MDM options:
   - `e360.mdm.protocol=t3s`
   - `e360.mdm.host=<T3S channel Listen Address>`
   - `e360.mdm.port=<T3S channel Listen Port>`
8. Restart WebLogic.
9. Test that the channel is working by pinging it.

   ```
   java weblogic.Admin -url t3s://<T3S Channel Listen Address>:<T3S Channel Listen Port> -username <WebLogic username> -password <WebLogic password> PING
   ```
10. You can now launch the Hub Console by using HTTPS and the secure port.

    ```
    https://<T3S Channel Listen Address>:<T3S Channel Listen Port>/cmx/
    ```

Enabling Secure Siperian Bus in the WebSphere Application Server

To enable secure message communication over Siperian Bus, you must configure the WebSphere console, and then the relevant `cmxserver.properties`.

1. Open the WebSphere console.
2. Configure a new user, on the **Users and Groups** tab.
   a. Click **Manage Users**, and then click **Create**.
   b. On the **Create a New User** page, enter the required information to create a new user. Do not assign any privileges to this user.
   c. Click **Create**, to complete the action.
3. Configure the settings on the **Service Integration** tab.
   a. Go to **Buses**, and then click the **SiperianBus** link. The **Configuration** page appears.
   b. In the **Additional Properties** section, click **Security**. The **Buses > SiperianBus > Buses > Security for bus SiperianBus** page appears.
   c. In the **General Properties** section, select the **Enable bus security** check box.
   d. In the **Authorization Policy** section, click **Users and groups in the bus connector role**.
   e. Click **New**, select the **Users** radio button, and then click **Next**.
   f. Select the user, and then click **Next** again. The **Summary** page appears.
   g. Click **Finish**.

h. Go back to the **Buses > SiperianBus > Buses > Security for bus SiperianBus** page.

i. Under **Related Items**, click the **JAAS -J2C authenticate data** link, and then click **New**.

j. In the **General Properties** section, specify **Alias**, **User ID**, and **Password**. Click **OK**.

k. Go back to the **Buses > SiperianBus > Security for bus SiperianBus** page.

l. In the **General Properties** section, select this JAAS Alias from the **Inter-engine authentication alias** list. Click **OK**.

4. Configure the settings on the **Resources** tab.

   a. Go to **JMS > Queue connection factory**, and then click the connection factory link to open the factory. The **Configuration** page appears.

   b. In the **Security Settings** section, from the **Container-managed authentication alias** list, select the JAAS Alias you defined earlier. Click **OK**.

   c. Go to **JMS > Activation Specifications**, and then click the **SiperianActivation** link. The **Configuration** page appears.

   d. In the **Security Settings** section, from the **Authenticate alias** list, select the JAAS Alias you defined earlier. Click **OK**.

Proceed to configure the relevant properties in the `cmxserver.properties` file.

Configuring cmxserver.properties for Secure Siperian Bus

You must configure the relevant`cmxserver.properties` to complete secure Siperian Bus configuration. Then, generate the encrypted password. Before you begin, enable security for Siperian Bus in the WebSphere application server.

1. In MDM Hub, open the `cmxserver.properties` file.
   - On UNIX. `<infamdm installation directory>/hub/server/resources`
   - On Windows. `<infamdm installation directory>\hub\server\resources`
2. Set the user name to be stored:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.username=<user name>
   ```
3. Set the password to be stored:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.password=<password>
   ```

   For example:

   ```
   siperian.mrm.jms.xaconnectionfactory.qcf.password=UlRJz88k4O2EL5yDw2jypuCLAkEYHCwVg8F
   iNJavdfVvKnC8RFGIGE45IeKyQm5C2WJe2pX+ajXj1QeC/j
   +o7jQmItiaYoyrEMsIRWTvZiHg14ZKjYbFNJcwGSC3rpURvPqH+WMjaEWdXxcD8p7uZ1pphc7WXkE
   +VouCR6kRwy0=
   ```
4. Run the following command to generate the encrypted password in your environment:

   ```
   java -classpath siperian-api.jar;siperian-common.jar;siperian-server.jar
   com.delos.util.PublicKeyBasedEncryptionHelper <plain text password> <infa home
   server>
   ```

For example:

```
java -classpath siperian-api.jar;siperian-common.jar;siperian-server.jar
com.delos.util.PublicKeyBasedEncryptionHelper admin \<infamdm installation directory>
\hub\
```

CHAPTER 7

Certificate-Based Authentication

This chapter includes the following topics:

Certificate-Based Authentication Overview

The MDM Hub uses a certificate-based authentication mechanism for securing the communication between the MDM Hub components and trusted applications. The authentication mechanism is also supported for the Services Integration Framework (SIF) and Business Entity Services APIs.

By default, the certificate login module considers Informatica applications, such as Data Director, to be trusted applications. To use the certificate-based authentication for external applications, you must register the applications as trusted applications.

An external application that is registered as trusted application passes the MDM Hub a concatenation of the application name and user name. For example, `IDD/admin`. The external application must also pass a security payload.

Certificate-Based Authentication and External Clients

Clients external to the MDM Hub, such as SiperianClient API, can send requests using user name and password authentication. However, external clients can also use certificate-based authentication.

To configure certificate-based authentication for a client external to the MDM Hub, perform the following steps:

1. In the Hub Console, register the public certificate for users associated with the external client.
2. Use the external client to trigger a request.

Trusted Applications

In the MDM Hub, a trusted application has a user type called an application user that can run requests on behalf of any regular MDM Hub user, including the admin user. Trusted applications belong to the MDM Hub trusted application framework.

You must use the Hub Console to register each custom application that you want to use as a trusted application. By default, the MDM Hub considers Informatica applications, such as Data Director and ActiveVOS that are used in the MDM Hub implementations as trusted applications.

By default, each trusted application has a set of public and private keys configured. The MDM Hub authenticates the request from a trusted application through certificate-based authentication.

To configure a custom application as a trusted application, see "Adding User Accounts" on page 30.

Adding an External Application as a Trusted Application

You can add applications external to the MDM Hub trusted application framework as trusted applications.

1. In the Hub Console, add a user account for the application user that corresponds to the external application.

   Note: Ensure that you select the **Application user** check box in the **Add User** dialog box and that you use only lowercase characters for the name of the user account.
2. Register a public certificate with the application user account.
3. Use the external application to trigger a request.

   Note: If you want to use certificate-based authentication, set the request name as <application name>/<user name>. The <application name> must be the same as that used in step 1. The <user name> is the name of the MDM Hub user that triggers the request.

Management of Certificates and Keys

The MDM Hub uses a certificate-based authentication. You must maintain the certificate and private key pairs for each user in a secure location.

By default, the MDM Hub keeps private keys and certificates at the following location:

```
<MDM Hub installation directory>/server/resources/certificates
```

Also, you can configure a custom certificate provider during the installation of Multidomain MDM.

To implement a custom certificate provider, you must implement a `PKIUtil.java` interface in the `siperian-server-pkiutil.jar` file, which is in the following directory:

```
<MDM Hub installation directory>/hub/server/lib/pkiutils
```

If you use a custom certificate provider, you must maintain the keystore and public certificates that the PKIUtil implementation uses.

Note: If you need to change the certificate provider, contact Informatica Global Customer Support to request a security configuration utility.

Related Topics:

- "Security Configuration Utility" on page 57

Security Configuration Utility

You can use the security configuration utility to manage some of the security settings in the MDM Hub implementation.

You can use the security configuration utility to perform the following tasks:

- Change the certificate provider that is used for authentication.
- Reset a password for a user in the MDM Hub.
- Change the hashing algorithm that is used for password hashing.
- Change the customer hashing key that is used to create the hashing algorithm.

Note: To get the security configuration utility, contact Informatica Global Customer Support.

CHAPTER 8

Password Hashing

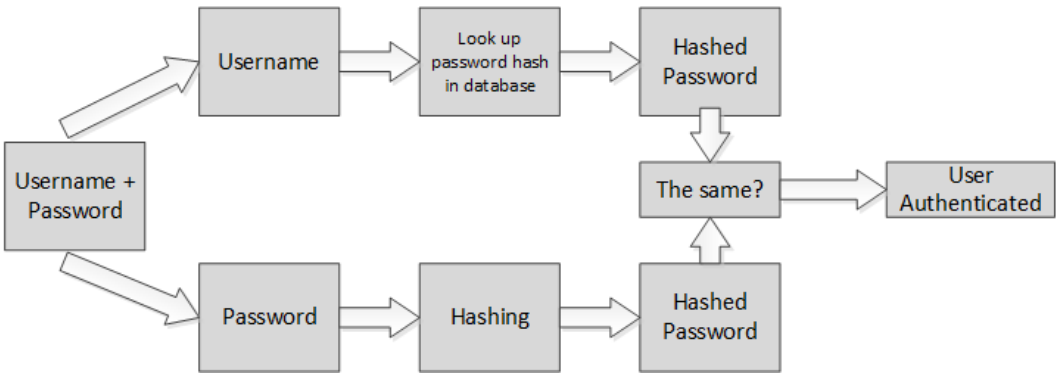
This chapter includes the following topics:

Password Hashing Overview

Password hashing is a way to irreversibly encrypt passwords through a cryptographic hash function. The MDM Hub uses a password hashing method to protect user passwords and ensure passwords are never stored in clear text form in a database. The MDM Hub administrator configures the password hashing options, such as the algorithm and customer hashing keys, during installation of the Hub Server.

Informatica provides a security configuration utility to manage some of the security settings in an MDM Hub implementation, including changing the hashing algorithm or resetting MDM Hub user passwords.

The following image shows how the MDM Hub authenticates user password:



Related Topics:

- "Security Configuration Utility" on page 57

Password Hashing Options

During the installation of the Hub Server, you configure the following password hashing options:

- Whether to create a custom hash key as part of the hashing algorithm
- Whether to use the default SHA3 hashing algorithm or create a custom hashing algorithm
- Whether to use the default certificate provider or use a custom certificate provider

Both SHA3 and custom hashing algorithms ensure that passwords of MDM Hub users are irreversibly encrypted and never stored in clear text form in a database. Regardless of which hashing algorithm you use, the algorithm has the following components:

- A hash function
- A salt value
- An optional pepper value or hash key, which is set during the MDM Hub installation. It is the responsibility of the MDM Hub administrator to generate this key and store it securely.

If you create a pepper value, Informatica recommends to use a key that contains a sequence of up to 32 hexadecimal characters with no delimiters.

Important: Protect the secrecy of the hash key to avoid the risk of data breach. If the hash key is stolen, you must reset all passwords.

The password hashing algorithm and the underlying implementation for the algorithm are stored in the Hub Server properties. For more information about Hub Server properties, see the *Multidomain MDM Configuration Guide*.

Custom Hashing Algorithm

Password Reset Process

If you forget your password, or if you believe the security of the secret components of your hashing algorithm might be compromised, you can reset your password. To reset your password, contact Informatica Global Customer Support.

When you reset your password, you receive an email with a temporary password. Use this password to log in to the MDM Hub and then change the password to something meaningful for you. You can change your password from the Hub Console or through Informatica Data Director.

Security Configuration Utility

You can use the security configuration utility to manage some of the security settings in the MDM Hub implementation.

You can use the security configuration utility to perform the following tasks:

- Change the certificate provider that is used for authentication.
- Reset a password for a user in the MDM Hub.
- Change the hashing algorithm that is used for password hashing.
- Change the customer hashing key that is used to create the hashing algorithm.

Note: To get the security configuration utility, contact Informatica Global Customer Support.

Troubleshooting

If you encounter problems, use the following information to troubleshoot issues.

MDM Hub users cannot login

If the MDM Hub re-creates the CMX_SYSTEM schema after installation of the Hub Server, the MDM Hub cannot recognize the hashed passwords. As a result, users cannot log in to the MDM Hub.

To resolve the issue, run the `postInstallSetup` script again manually. This script ensures that the passwords of the MDM Hub users are hashed again and users can log in.

For more information about the postInstallSetup script, see the *Multidomain MDM Installation Guide*.

APPENDIX A

Glossary

authentication

Process of verifying the identity of a user to ensure that they are who they claim to be. In Informatica MDM Hub, users are authenticated based on their supplied credentials—user name / password, security payload, or a combination of both. Informatica MDM Hub provides an internal authentication mechanism and also supports user authentication using third-party authentication providers.

authorization

Process of determining whether a user has sufficient privileges to access a requested Informatica MDM Hub resource. In Informatica MDM Hub, resource privileges are allocated to roles. Users and user groups are assigned to roles. A user's resource privileges are determined by the roles to which they are assigned, as well as by the roles assigned to the user group(s) to which the user belongs.

base object

A table that contains information about an entity that is relevant to your business, such as customer or account.

batch group

A collection of individual batch jobs (for example, Stage, Load, and Match jobs) that can be executed with a single command. Each batch job in a group can be executed sequentially or in parallel to other jobs.

Configuration workbench

Includes tools for configuring a variety of MDM Hub objects, including the Operational Reference Store, users, security, message queues, and metadata validation.

database

Organized collection of data in the Hub Store. Informatica MDM Hub supports two types of databases: a Master Database and an Operational Reference Store (ORS).

Data Manager

Tool used to review the results of all merges—including automatic merges—and to correct data content if necessary. It provides you with a view of the data lineage for each base object record. The Data Manager also allows you to unmerge previously merged records, and to view different types of history on each consolidated record.

Use the Data Manager tool to search for records, view their cross-references, unmerge records, unlink records, view history records, create new records, edit records, and override trust settings. The Data Manager displays all records that meet the search criteria you define.

data steward

Informatica MDM Hub user who has the primary responsibility for data quality. Data stewards access Informatica MDM Hub through the Hub Console, and use Informatica MDM Hub tools to configure the objects in the Hub Store.

Dynamic Data Masking

A data security product that operates between a client and a database to prevent unauthorized access to sensitive information. Dynamic Data Masking intercepts requests sent to the database and applies data masking rules to the request to mask the data before it is sent back to the client.

hierarchy

In Hierarchy Manager, a set of relationship types. These relationship types are not ranked based on the place of the entities of the hierarchy, nor are they necessarily related to each other. They are merely relationship types that are grouped together for ease of classification and identification.

Hierarchy Manager

The Hierarchy Manager allows users to manage hierarchy data that is associated with the records managed in the MDM Hub. For more information, see the *Multidomain MDM Configuration Guide*.

Hub Console

Informatica MDM Hub user interface that comprises a set of tools for administrators and data stewards. Each tool allows users to perform a specific action, or a set of related actions, such as building the data model, running batch jobs, configuring the data flow, running batch jobs, configuring external application access to Informatica MDM Hub resources, and other system configuration and operation tasks.

Hub Server

A run-time component in the middle tier (application server) used for core and common services, including access, security, and session management.

Hub Store

In a Informatica MDM Hub implementation, the database that contains the Master Database and one or more Operational Reference Store (ORS) database.

Kerberos

Computer network authentication protocol that allows nodes that communicate over a non-secure network to prove their identity to one another in a secure manner. The Massachusetts Institute of Technology developed the protocol and makes an implementation of Kerberos freely available.

metadata

Data that is used to describe other data. In Informatica MDM Hub, metadata is used to describe the schema (data model) that is used in your Informatica MDM Hub implementation, along with related configuration settings.

Operational Reference Store (ORS)

A database that contains master data and the rules that act on the master data. Rules include the rules for processing the master data, the rules for managing the set of master data objects, and the processing rules and auxiliary logic that the MDM Hub uses to define the best version of the truth. An MDM Hub configuration can have one or more Operational Reference Stores. The default name of an ORS is CMX_ORS.

package

A *package* is a public view of one or more underlying tables in Informatica MDM Hub. Packages represent subsets of the columns in those tables, along with any other tables that are joined to the tables. A package is based on a query. The underlying query can select a subset of records from the table or from another package.

password policy

Specifies password characteristics for Informatica MDM Hub user accounts, such as the password length, expiration, login settings, password re-use, and other requirements. You can define a global password policy for all user accounts in a Informatica MDM Hub implementation, and you can override these settings for individual users.

policy decision points (PDPs)

Specific security check points that authenticate user identity and authorize user access to MDM Hub resources.

policy enforcement points (PEPs)

Specific security check points that enforce, at run time, security policies for authentication and authorization requests.

private resource

A Informatica MDM Hub resource that is hidden from the Roles tool, preventing its access through Services Integration Framework (SIF) operations. When you add a new resource in Hub Console (such as a new base object), it is designated a PRIVATE resource by default.

privilege

Permission to access an MDM Hub resource. With MDM Hub internal authorization, each role is assigned one of the following privileges.

Privilege	Allows the User To....
READ	View data.
CREATE	Create data records in the Hub Store.
UPDATE	Update data records in the Hub Store.
MERGE	Merge and unmerge data.
EXECUTE	Execute cleanse functions and batch groups.
DELETE	Delete data records from the Hub Store.

Privileges determine the access that external application users have to MDM Hub resources. For example, a role might be configured to have READ, CREATE, UPDATE, and MERGE privileges on particular packages and package columns. These privileges are not enforced when using the Hub Console, although the settings still affect the use of Hub Console to some degree.

profile

In Hierarchy Manager, describes what fields and records an HM user may display, edit, or add. For example, one profile can allow full read/write access to all entities and relationships, while another profile can be read-only (no add or edit operations allowed).

provider

See *security provider* on page 64.

role

Defines a set of privileges to access secure Informatica MDM Hub resources.

security

The ability to protect information privacy, confidentiality, and data integrity by guarding against unauthorized access to, or tampering with, data and other resources in your Informatica MDM Hub implementation.

Security Access Manager (SAM)

Security Access Manager (SAM) is the security module for protecting MDM Hub resources from unauthorized access. At run time, SAM enforces your organization's security policy decisions for your MDM Hub implementation, handling user authentication and access authorization according to your security configuration.

Security Access Manager workbench

Includes tools for managing users, groups, resources, and roles.

security payload

Raw binary data supplied to an MDM Hub operation request that can contain supplemental data required for further authentication or authorization.

security provider

A third-party application that provides security services (authentication, authorization, and user profile services) for users accessing Informatica MDM Hub.

workbench

In the Hub Console, a mechanism for grouping similar tools. A workbench is a logical collection of related tools. For example, the Model workbench contains tools for modelling data such as Schema, Queries, Packages, and Mappings.

write lock

In the Hub Console, a lock that is required in order to make changes to the underlying schema. All non-data steward tools (except the Operational Reference Store security tools) are in read-only mode unless you acquire a write lock. Write locks allow multiple, concurrent users to make changes to the schema.

INDEX