



HYPERION® SYSTEM™ 9

MASTER DATA MANAGEMENT SERVICES™

RELEASE 9.2

NEW FEATURES



- Overview 2
- Ntier Architecture..... 2
- Installer 3
- External Authentication..... 3
- Master Data Management Services Console 3
- Component Version Checking 4
- Client-Server Functionality Migration..... 4
- Improved Orphan Node Management..... 5
- Transaction Logging of Metadata Changes 5
- Enhanced Password and user controls for Internal Authentication..... 5
- Memory Utilization Enhancement..... 6
- Master Data Management Services Account Changes 6
- Where to Get More Information..... 7

OVERVIEW

Hyperion® System™ 9 Master Data Management Services™ release 9.0 represents the initial release of the Master Data Management Services Ntier system from Hyperion. The release includes the following major features:

- Ntier architecture release—The initial release of the Master Data Management Services Ntier from Hyperion
- Installer—Automated installation capability for the client and server layers of Master Data Management Services
- External authentication—The ability to utilize an external source such LDAP, NTLM, or MSAD for username/password authentication
- Master Data Management Services Console—The ability to monitor and control the Master Data Management Services application layers
- Component version checking—Checking of appropriate components to prevent an incomplete upgrade or install from causing stability issues
- Client server functionality migration—Functionality added to the client-server code during the development of the Ntier model. This includes database export, ID generation, node type glyphs, and model after functionality
- Improved orphan node management—Ease in managing orphan nodes in a version
- Transaction logging of metadata changes—Auditing changes to the Master Data Management Services system
- Enhanced password and user controls for internal authentication—Controls to enforce password and user management when using the internal authentication model of Master Data Management Services
- Enhanced memory utilization—MDM Services no longer requires an expired or finalized version to be opened by the main engine
- Master Data Management Services account changes—Creation of separate accounts by function to improve control and reduce confusion

NTIER ARCHITECTURE

The Ntier architecture represents a major change from the original two-tier client-server architecture. It provides the following benefits:

- Scalability—The server layer for Master Data Management Services can include multiple engines and Web layers across multiple servers if needed to scale the performance of the system
- Full API—The server layer provides a full SOAP and COM+ API to allow interfacing from external enterprise applications
- Thin Client—The Win32 client for Master Data Management Services is now a thin client requiring less client resources. The thin client is a simple executable requiring no additional dlls or files
- User Concurrency—In the Ntier environment, the server layer tracks concurrency between users and allows users to see changes made by other users without having to restart the application as in the client-server architecture.

INSTALLER

An installer is now available to automate and streamline the Master Data Management Services installation process. The server installer offers two installation options:

- Complete—Installs all server components on the current machine
- Custom—Installs only certain components on the current machine

This allows the Master Data Management Services server functionality to be spread across multiple machines if desired. For example, separate machines could be used for the web server and application server functions.

The installer also includes the ability to either create a new Master Data Management Services database or automatically update an existing Master Data Management Services database from a previous release. It is no longer necessary to manually apply database scripts to an existing database. Also, the installer can remove or modify an existing Master Data Management Services installation. For additional details, refer to the *Hyperion System 9 Master Data Management Services Installation Guide*.

EXTERNAL AUTHENTICATION

External Authentication via Hyperion Shared Services—Master Data Management Services users can be authenticated via external sources such as LDAP, NTLM or MSAD. This feature requires access to the Common Security Services component of Hyperion Shared Services to perform the authentication. This feature can be controlled by setting the system preference AuthMethod as follows:

- Internal—Users are only authenticated internally within Master Data Management Services as in previous releases. This is the default setting.
- CSS (External)—Users are only authenticated externally. Requires access to Common Security Services found in HSS.
- Mixed—Users are authenticated internally or externally based on a setting for each individual user.

MASTER DATA MANAGEMENT SERVICES CONSOLE

A new tool is available for monitoring and configuring Master Data Management Services operation. The Master Data Management Services Console provides the ability to start and stop the service, monitor the various Master Data Management Services components that are running, and view the event log messages generated by Master Data Management Services. In addition, this tool allows all necessary configurations to be done from a single place. The Console replaces both the DAL Configuration tool and the Process Manager configuration tool. Master Data Management Services configuration data is now stored in an XML file (config.xml) rather than in the registry. While it is possible to edit config.xml manually, it is strongly recommended that configuration changes be made via the Console.

COMPONENT VERSION CHECKING

Previously, it was possible to log in to the Master Data Management Services server with a client application from a different release that may not have been fully compatible with the server release. Now, when a user attempts a login, the client version is verified to be the same as the server version. Attempting to log in to a Master Data Management Services release 9.0.1 server with an older client version will display an error message. Each of the server components is also checked for compatibility at startup.

CLIENT-SERVER FUNCTIONALITY MIGRATION

Many enhancements added to the Client / Server Master Data Management Services system have been migrated to the Ntier Architecture. They include the following:

MODEL AFTER FEATURE FOR CREATING NEW NODES

When creating new nodes that share many characteristics with existing nodes, an existing node can be selected as the "model" for the new node selected properties and relationships can be copied to the new node. This can save considerable time as compared to creating each new node from scratch.

NEXT ID FUNCTION

Node names can be generated automatically using sequential numerical IDs and node prefixes. For example, a set of nodes can be created, each having a name like Org000xxx, where:

- Org is the node prefix and can be any desired character string
- 000xxx is the sequential ID and increments by 1 starting at 1

This feature must be enabled by a System Administrator for it to be visible to Master Data Management Services users.

EXPORT TO DATABASE TABLE

Export output can be written directly to an external database table. Each column in the export can be mapped to a column in the target database table. This option is available for these export types: Hierarchy, Hierarchy Compare, Version, Transaction Log, and Merge Log.

CUSTOMIZED NODE TYPE GLYPHS

Master Data Management Services has always included default glyphs to distinguish limb nodes and leaf nodes in the hierarchy window. Now there is the ability to load custom glyphs and apply them to specific node types. This feature, previously only available in the Client Server version of Master Data Management Services, will allow the node type of a given node to be quickly determined based on the glyph displayed. This applies to all places where nodes are displayed including the hierarchy window and hot lists.

IMPROVED ORPHAN NODE MANAGEMENT

Several new features are available to improve the process of managing orphan nodes. Previously, orphan nodes that had children could not be deleted without first manually removing the children. Now the deletion process for orphan nodes will automatically remove any children and then delete the orphan node. Multiple nodes can be selected from the orphan list for deletion. Users can also now insert orphan nodes by dragging them from the orphan list directly into a hierarchy window.

TRANSACTION LOGGING OF METADATA CHANGES

In addition to logging all hierarchy data operations, the Transaction History now also records all changes to metadata such as property definitions, system preferences, export profiles, etc. Due to the increased data being stored in these metadata history records, a special viewer is available to review the contents of each.

ENHANCED PASSWORD AND USER CONTROLS FOR INTERNAL AUTHENTICATION

When using the Internal Authentication mechanism, the following enhancements allow for tighter control of the users activity and passwords allowing the enterprise to maintain standards needed for compliance.

PASSWORD LENGTH REQUIREMENTS

Two new system preferences, PasswordMinLength and PasswordMaxLength, are used to specify the minimum and maximum length for user passwords. Once these values are set, any new passwords will have to meet the length requirements. Existing user passwords will not be subject to the limits until the next time they are changed. If the system preferences are set to a value of 0, then no limits will be enforced.

USER LOCKOUT FOR ENHANCED SECURITY

Master Data Management Services administrators now have the ability, via the User Management dialog, to lockout users from accessing the system. Lockouts can also be configured to occur automatically when certain constraints are violated. Once a user is locked out, their access can only be restored by a Master Data Management Services administrator.

The following new system preferences can be used to trigger automatic lockout:

- LockoutInvalidLogins—Defines the maximum number of consecutive invalid login attempts allowed for a given user. Once the invalid attempts exceed this value, the user will be locked out of the system. If a user has a successful login before exceeding the limit, then no lockout will occur.
- LockoutInactivity—Defines the maximum number of days of inactivity allowed between valid login attempts. If a given user has not logged in within the specified number of days, they will be locked out on their next attempt.

While these system preferences affect all user levels, there are also options to exclude certain users from the automatic lockout conditions. The following new system preferences are available:

- LockoutExcludeSysAdmin—If set to True, then all System Admin users will not be subject to lockout based on invalid logins or inactivity.
- LockoutExcludeFuncAdmin—If set to True, then all Functional Admin users will not be subject to lockout based on invalid logins or inactivity.
- LockoutExcludeSeccAdmin—If set to True, then all Security Admin users will not be subject to lockout based on invalid logins or inactivity.
- LockoutExcludeUsers—Can be set to a comma-delimited list of users that will not be subject to lockout based on invalid logins or inactivity.

All user levels will still be subject to manual lockouts performed via the User Management dialog regardless of how these system preferences are set.

Note on invalid login attempts: Prior to the implementation of the user lockout feature, the NTier client application would only allow 3 invalid login attempts before shutting down. This is now controlled by the LockoutInvalidLogins system preference rather than having a fixed limit of 3. Thus, if this system preference is set to 5, the user will be able to continue the invalid login attempts up to 6 times before the client application shuts down and the user is locked out.

MEMORY UTILIZATION ENHANCEMENT

The main read/write engine no longer opens a read only version as it did in the past. This is due to the ability now for the system to edit changes to Version and Hierarchy level properties without loading the full set of version nodes. With this enhancement, a client can open many finalized and expired versions and they are balanced across multiple read only engines, thus allowing greater scalability and memory management for the Master Data Management Services system.

Since each version being used within Master Data Management Services has to be loaded into memory on the application server and can require substantial system resources based on the size of the version, it is important to only load versions when absolutely necessary. Administrative users can now view and update properties at the version or hierarchy level without having to fully load that version into memory. Also, since Finalized or Expired versions cannot be updated, versions with this status will no longer be opened in the Read/Write Engine. This allows more efficient use of existing system resources on the application server.

MASTER DATA MANAGEMENT SERVICES ACCOUNT CHANGES

Designated User Accounts—Previously, the Master Data Management Services installation would set up a default administrative user such as MDMAAdmin. This account would then be used for the database connection, the default client login, and server logins. Now the Master Data Management Services installation creates distinct users for each of these three functions. The following Master Data Management Services user accounts are created (each with default password "razza"):

- MDM_ADMIN—the default Master Data Management Services System Administrator. Can be used to login to the client tool and has full system access.

- MDM_DB—the database login. The system will always attempt to connect to the database using this account. If an MDM_DB database user already exists in the target database, then it will be necessary after installation to access the Master Data Management Services Console and update MDM_DB with the correct password.
- MDM_SYSTEM—the account used by Master Data Management Services server processes to communicate with each other. The default password set during installation can be updated via the Master Data Management Services Console if desired. This user should not be edited other than in the Console.

WHERE TO GET MORE INFORMATION

Except for the most recent information, each topic in this booklet is described in more detail in the documentation.

For answers to questions about the product, contact your authorized technical support provider or visit the Hyperion Solutions Web site.

COPYRIGHT NOTICE

Copyright 2005-2006 Hyperion Solutions Corporation.
All rights reserved.

“Hyperion,” the Hyperion logo, and Hyperion’s product names are trademarks of Hyperion. References to other companies and their products use trademarks owned by the respective companies and are for reference purpose only.

No portion hereof may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the recipient’s personal use, without the express written permission of Hyperion.

The information contained herein is subject to change without notice. Hyperion shall not be liable for errors contained herein or consequential damages in connection with the furnishing, performance, or use hereof.

Any Hyperion software described herein is licensed exclusively subject to the conditions set forth in the Hyperion license agreement.

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable Hyperion license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14, as applicable.

Printed in the U.S.A.

HYPERION WORLDWIDE HEADQUARTERS

HYPERION SOLUTIONS CORPORATION

5450 GREAT AMERICA PARKWAY, SANTA CLARA, CA 95054 TEL: 1.408.588.8000 FAX: 1.408.588.8500

