Informatica

White Paper

Informatica MDM – Reference 360

Security and Compliance Overview

ABOUT INFORMATICA

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category, or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities, or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

Table of Contents

Introduction

Business success depends on the open flow of information more than ever before. Yet this dependency exposes the organization to substantial liabilities. Striking that elusive balance between open and secure is a constant challenge. As organizations explore Master Data Management (MDM) as a means for bringing data from multiple applications and multiple sources into a single MDM system, the security model and governance requirements (and related potential liability) become exponentially more complex. As a result, it is only when you have the right security mechanisms in place that you have the confidence to share your critical business data among internal and external users, secure in the knowledge that each user will have the right kind of access to any resources they might require. Informatica MDM — Reference 360 meets these critical challenges and enables customers to master their reference data while also meeting any compliance requirements.

With a security framework built on into Informatica® Intelligent Cloud Services℠ (IICS), Informatica MDM — Reference 360 services have the most comprehensive and flexible security framework of any MDM Software as a Service (SaaS) offering in the marketplace. Our technology provides pinpoint data-access security, including the ability to control, access, and manage security down to the field level. The IICS security configuration enables security administrators and data stewards to customize user views according to roles, operational groups, and regulatory requirements. For organizations subject to data privacy governance regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), or comply with specific industry regulations—for instance, financial services firms with Know Your Customer (KYC), or retailers that need to meet the Payment Card Industry (PCI) privacy standards—this kind of functionality makes it far easier to bring operations in sync with regulatory guidelines, ensure policy compliance, and meet reporting requirements.

The Challenge

Today, a business must continually improve its processes to remain competitive. One essential requirement to achieve this goal is to better understand, manage, and report on risk. Organizations rely on their MDM programs to deliver a trusted single version of master data across an enterprise. However, few MDM programs protect this significant business asset, which creates an exposure to risk for the organization. This trend is critical, especially during a time when intelligent data-driven disruptions have become crucial in corporate strategies. As several companies turn to master data management to conduct their business-led initiatives around growth, compliance, efficiency, and customer experience, they should ensure that their MDM is secure.

Overview

Informatica offers a Master Data Management solution that is configurable and extensible to meet a variety of security requirements—including areas such as identity and access management, data security, and monitoring—driven by the customer's security policies, procedures, and best practices.

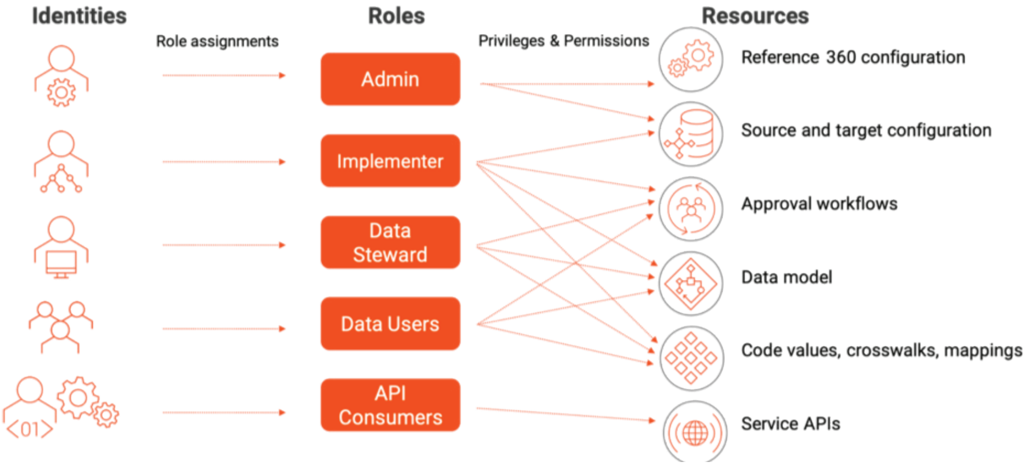
- For any industry (product-centric industries, service industries, and government), we provide the ability to express and enforce data authority policy directly in the data model and map that to role-based authorization system, ensuring access to and interaction with master data in a manner that conforms to the organization's privacy/compliance/data governance policies.
- For any data domain, we provide role-based security and access management for all data assets at any granularity across all modes of interaction, i.e. data model, APIs, services, UIs.

Identity and Access Management

For identity and access management, Informatica MDM — Reference 360 provides comprehensive and highly granular security access controls to ensure that only authenticated and authorized users have access to master data, resources, and functionality. This access control is role-based and defines the access rights, entitlements, and expertise for any user- or group-role participating in the lifecycle of master data, mapping those to express the internal security and access control policies of the organization that is managing the master data.

Administrators configure authorization policies by assigning privileges and permissions to roles and then assigning users to roles. The authorization policies allow for scalable deployment of security policies. Role privileges control access to features and functionality of an application (for example, whether the role can configure rules). Role permissions control access to data within the application (for example, whether the role can create, read, update, or delete records).

The following diagram logically illustrates Role-Based Access Control (RBAC).



Data Security

The security of customers' data for each of our Informatica MDM — Reference 360 customers is of primary importance for Informatica. This is why Informatica MDM — Reference 360 provides so many efficient and scalable security features.

A security key is stored in a "secret store" and a digital security certificate (signed by the Informatica Cloud's Certificate Authority) is used to encrypt data. Encrypting data this way ensures that data is secure, both in transit and at rest. The secret store secures access to tokens, passwords, certificates, and API keys (along with other confidential information), and handles leasing, key revocation, key rolling, and auditing. The secret store ensures that only customers can access their data. Informatica employees will not be able to access customer data through any mediums, including UIs and APIs.

Customer Data Separation

Each customer's data is separate, with a dedicated database instance and search indexes to ensure data isolation. The third-party products we use for the database instance and search indexes undergo independent verification of platform security, privacy, and compliance controls.

Both the database and search index stores are encrypted, and the keys are stored in the secret store to ensure that no one has access to customer data, including Informatica employees. Customers can only access their data based on security filtering applied by our authorization service.

Data in Transit and Data at Rest Encryption

Data in transit and rest uses TLS/SSL protocols and authentication (SCRAM) by default, which encrypts all connections. Traffic from clients to the database is authenticated and encrypted. Informatica MDM — Reference 360 cloud uses the TLS 1.1 protocol by default.

The Informatica Cloud® security team continuously monitors and updates transport protocols to ensure weak ciphers are deprecated.

Conclusion

Informatica MDM — Reference 360 is fully configurable to meet a variety of security needs including and not limited to privacy, compliance, and data governance policies. Informatica uses proven processes and procedures to harden our applications taking all aspects of data security into account with a dedicated team of experts.

We invite you to learn more at: https://www.informatica.com/trust-center.html

Informatica®

Worldwide Headquarters 2100 Seaport Blvd., Redwood City, CA 94063, USA   Phone: 650.385.5000, Toll-free in the US: 1.800.653.3871