Informatica

07 Jan, 2025

MDM SaaS Onboarding: Essential Steps for a Seamless Implementation

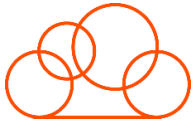
- Sourya Dass, Principal Customer Success Architect, CSA
- Kamal Abrol, Senior Principal Customer Success Architect, CSA

Where data & AI come to LIFE

Housekeeping Tips

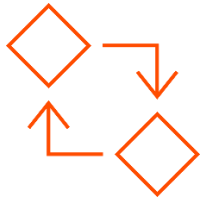
- Today's Webinar is scheduled for 1 hour
- The session will include a webcast and then your questions will be answered live at the end of the presentation
- All dial-in participants will be muted to enable the speakers to present without interruption
- Questions can be submitted to "All Panelists" via the Q&A option and we will respond at the end of the presentation
- The webinar is being recorded and will be available on our Success Portal - where you can download the slide deck for the presentation. The link to the recording will be emailed as well.
- Please take time to complete the post-webinar survey and provide your feedback and suggestions for upcoming topics.

Feature Rich Success Portal



Bootstrap trial and POC Customers

Enriched Customer Onboarding experience



Product Learning Paths and Weekly Expert Sessions

Informatica Concierge

Tailored training and content recommendations

More Information

Success Portal

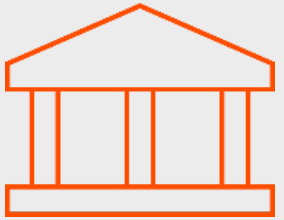
https://success.informatica.com

Communities & Support

https://network.informatica.com

Documentation

https://docs.informatica.com



University

https://www.informatica.com/in/services-and-training/informatica-university.html

Safe Harbor

The information being provided today is for informational purposes only. The development, release, and timing of any Informatica product or functionality described today remain at the sole discretion of Informatica and should not be relied upon in making a purchasing decision.

Statements made today are based on currently available information, which is subject to change. Such statements should not be relied upon as a representation, warranty or commitment to deliver specific products or functionality in the future.

Informatica

Customer Onboarding

Sourya Sekhar Dass

Kamal Abrol

Where data & AI come to LIFE

Disclaimer: The information being provided herein is for informational purposes only. The development, release and timing of any Informatica product, service or functionality described herein remain at the sole discretion of Informatica and should not be relied upon in making a purchasing decision. Statements made herein are based on information currently available, which is subject to change. Such statements should not be relied upon as a representation, warranty or commitment to deliver specific products, services or functionality in the future.

SaaS Architecture

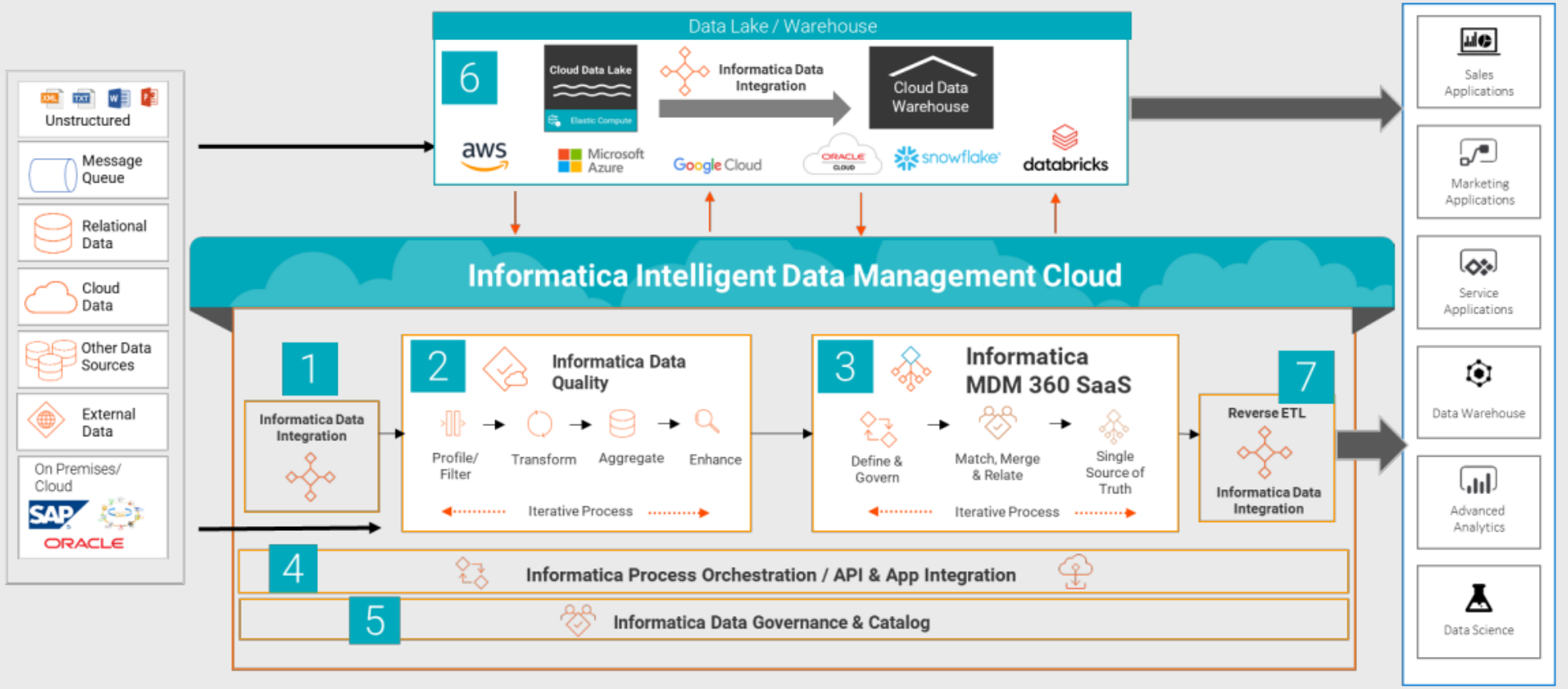
MDM SaaS Architecture

Informatica

Reference Architecture

Master Data Management

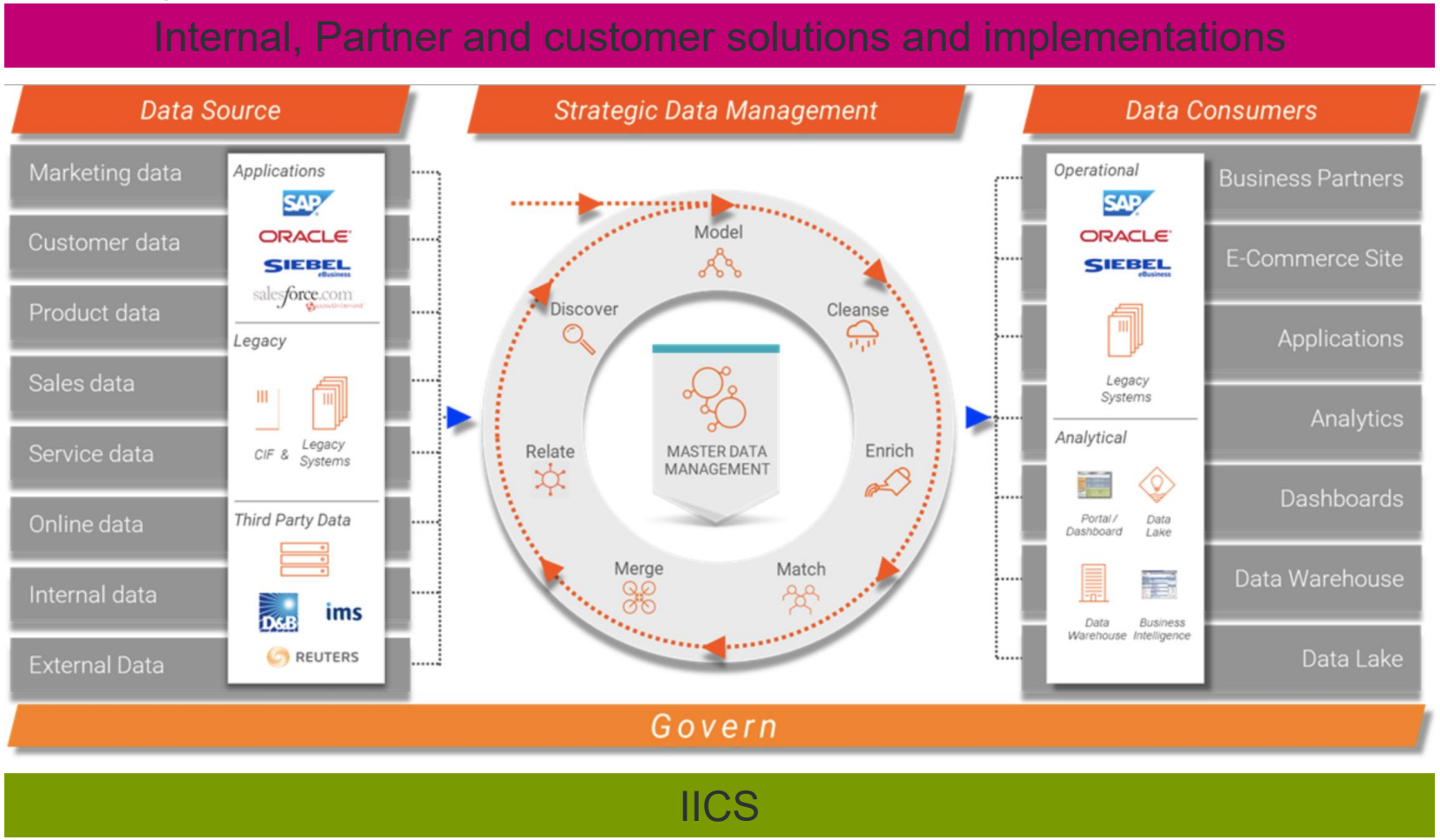
The next-generation master data management reference architecture delivers a trusted, actionable view of master data and its relationships across a business. It also provides a framework where organizations can onboard and safeguard critical master data, expose relationships across entities, and enrich, verify and validate information so the business can engage relevantly with key master data domains such as customers, products, suppliers, employees, etc.



1. **Data Integration** — Ingest and integrate master data from various source systems and applications across enterprises at the speed of business.
2. **Data Quality** — Cleanse, profile, standardize, remediate and monitor data quality to create accurate, consistent and complete master data.
3. **Master Data Management (MDM)** — Informatica MDM 360 SaaS governs, matches and merges duplicate master records, providing a single, trusted version of the truth.
4. **Process Orchestration & API/App Integration** — Orchestrate end-to-end processes and manage the enterprise metadata and business facets beyond applications. API/app integration helps in gathering and enriching master data from various internal business applications as well as third-party applications.
5. **Data Governance & Catalog** — Data governance manages enterprise data proactively. The data catalog identifies data across the business and assesses its relevance for master data and defines data lineage. Data privacy and protection secure data access in compliance with regulations.
6. **Data Lake/Warehouse** — Integrate and enrich cloud data lakes/warehouses with rich master data published from MDM software as well as with relevant information shared from data lakes/warehouses for AI and analytics use cases.
7. **Reverse ETL** — Integrate MDM with other applications including operational applications, data warehouses, advanced analytics, and AI and data science use cases.

MDM on Cloud – user view

Core functionality to deliver in multi-tenant context



© Informatica. Proprietary and Confidential.

Stages of MDM SaaS journey

Key ROI & Outcomes for use cases determination

- Improve customer retention, loyalty, and profitability
- Optimize supply chain resiliency, flexibility, and continuity
- Increase product conversion rates, basket size, and profitability
- Accelerate financial consolidation and reporting
- Define Business & Technical concepts
- Gain greater accuracy from forecasting, planning, and analysis

Informatica

Best practices & Recommendations

- Vision & Strategy for business & technical use cases – Project Stakeholders
- Define Success Criteria for ROI
- Identify Current Challenges that need to be solved with MDM SaaS
- Budgeting & Cost
- Design phases & iterations of each deployment with timelines
- Procure and set up environments
- Invite PDOs, Data Governors, Architects, Developers to Governance Council meetings

Informatica

Logical Steps to MDM SaaS Implementation

- Data Governance Councils
- Finalize the source systems
- Finalize the Lookup Code values
- Finalize the Business attributes
- Define Business & Technical concepts
- Finalize MDM Data Model
- Profile Data Quality

Informatica

Logical Steps to MDM SaaS Implementation

- Finalize MDM use cases based on requirements and business feedback & inputs
- Design conceptual Match Rules in MDM
- Design Ingress & Egress mechanism
- Finalize Data Quality rules based on use cases
- Design MDM UI
- Finalize User Roles & Privileges
- Start test data load in Development environment

Informatica

Drilling down to the technical details

CDQ use cases	CDI use cases	MDM use cases	Downstream data syndication	Reporting & Analytics requirements
• Business rules • Technical validations • Exception report • Data corrections	• Source to Target mappings • Data transformations • DnB, Address Doctor integration	• Data Load Strategy • Match rules • Survivorship • Hierarchy • UI	• API (real time) • Message Queue (near real time) • Batch driven • Publish format	• Target system • Schedule • Giving access to teams

Informatica

Business 360 SaaS: Informatica Responsibilities

Typical Informatica Project Roles and Responsibilities	
Delivery Manager	✓ Assist Project Team with establishing project approach and detailed project plan ✓ Provide expert advice and counsel to the project team ✓ Collaborate with Informatica project team to review design decisions and quickly resolve software related issues ✓ Provide assistance with implementing solution review recommendations ✓ Participate in project status review meetings ✓ Primary liaison to Informatica support, product management and engineering during engagement ✓ Risk management, assessing risks in an informed and considered manner plan for the mitigation of these risks
MDM SaaS Solution Architect	✓ Provide expert advice, counsel, and technical expertise to the project team to help assure that Informatica MDM and Data Governance solutions are designed and developed in the optimal manner and in accordance with industry and Informatica best practices. ✓ Architecture assistance and guidance ✓ Validates the requirements and feasibility of designs for MDM and Data Governance ✓ Design and architect modular integrations ✓ Guides the team on all integration patterns and serves as the technical lead ✓ Provide optimal design and guidance on designs, build and testing of IICS transformations and data quality rules for the MDM and Data Governance implementations
Integration Specialist (CDI /CAI)	✓ Design and development of Batch and API programs/modules ✓ Develops source to target design specifications ✓ Designs, builds and unit tests integrations ✓ Assists with testing defect resolution and initial data loads
CDI Consultant	✓ Performs Data Profiling on source data ✓ Presents Data Profiling Analyses to stakeholders ✓ Develops DQ Business Rules design specification

Business 360 SaaS: Customer Responsibilities

Typical customer Project Roles and Responsibilities			Initial Involvement	Steady-state
Executive Sponsor	✓ ✓ ✓	Provides the business sponsorship for the project Champions the project within the business Guides the Project Managers in understanding business requirements and priorities	10% (3-4 hours)	5% (1-2 hours)
I/T Leadership	✓ ✓	Provides Executive oversight of the project from an I/T perspective Provides advice and guidance to the technical team	20% (6-8 hours)	10% (3-4 hours)
Technical Project Manager	✓ ✓ ✓	Defines and implements the methodology adopted for the project Liaises with the Project Sponsor, Business Project Manager, Technical Delivery Manager, Engagement Advisor Manages project resources within the project scope, timeline and budget	50% (20 hours)	25% (10 hours)
System Administrator	✓ ✓ ✓ ✓	Configures required hardware and infrastructure software Coordinates the sizing, purchase and installation of all servers and OS installations for all environments Supports and maintains all environments Manages the daily execution of workflows and sessions in the production environment	25-50% during Installs/execution (10-20 hours)	10% (4 hours)
Database Administrator	✓	Configures databases for the Informatica integrations and provides connection information to the end points	25% during Installs (10 hours)	10% (4 hours)
Data Stewards	✓ ✓ ✓ ✓	Oversee the life cycle of a particular set of data Establishing data-quality metrics and requirements, including defining the values, ranges, and parameters that are acceptable for each data element. Establish guidelines and protocols that govern the proliferation of data to ensure that privacy controls are enforced Define policies and procedures for access to data	50% (20 hours)	20% (8 hours)
Business SME	✓ ✓	Helps define business requirements Participates in UAT and final deployment acceptance	50% (20 hours)	20% (8 hours)
Infrastructure Architect	✓ ✓	Responsible for technical infrastructure In conjunction with Project and IICS Architects, determines requirements for supporting hardware, software and network resources.	25-50% (10-20 hours)	20% (8 hours)

Secure Agent

Informatica

How Secure Agent Works

- The Informatica Cloud Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services. When the Secure Agent runs a task, it connects to the Informatica Cloud hosting facility to access task information. It connects directly and securely to sources and targets, transfers data between them, orchestrates the flow of tasks, runs processes, and performs any additional task requirement. If the Secure Agent loses connectivity to Informatica Intelligent Cloud Services, it tries to reestablish connectivity to continue the task. If it cannot reestablish connectivity, the task fails. The Secure Agent uses pluggable microservices for data processing. For example, the Data Integration Server runs all data integration jobs, and Process Server runs application integration and process orchestration jobs. Each service has a unique set of configuration properties, such as Tomcat and Tomcat JRE settings. For more information about Secure Agent services, see Secure Agent Services. You can install and run one Secure Agent on a physical or virtual machine. After you install a Secure Agent, all users in the organization share the Secure Agent. You can configure the Secure Agent properties and move it to a different Secure Agent group. To improve scalability, you can also add multiple agents to a Secure Agent group.

More Information on SA

- In IICS, the Secure Agent component and/or the Informatica managed cloud runtime is responsible for processing data. The Secure Agent plays a major role in securing customer data and applications and contains several security features. The Secure Agent as a platform by itself supports microservice characteristics like pluggable engines, load balancing, scalability and high availability. It consists of data integration, process server, and mass ingestion engines and connectors to external data sources to execute both batch and real-time integrations and other forms of integrations in the future The Secure Agent can be flexibly deployed on-premise or on a public cloud (AWS, Azure, etc.) by the customer to meet the customer's specific needs, or it can be managed on the IICS host by Informatica.
- The Secure Agent is attached to the customer organization at the time of its registration. The Secure Agent installer supports basic authentication and token-based authentication. When using basic authentication, the customer needs to supply the user name and password to register the agent to the customer's IICS organization. When using token-based authentication, the customer needs to supply the token granted at the time of the Secure Agent installation. Customers can also optionally configure a proxy server at the time of Secure Agent registration for its communication with cloud applications. Upon successful authentication, the Secure Agent will be attached to the customer organization. Once the Secure Agent is attached to the customer organization, it downloads binaries associated with services and connectors that the customer is licensed to and initiates the corresponding service engines. The agent also downloads any updates to engines or packages associated with the connectors during the customer subscription and service upgrade life cycle.

Secure Agent Groups

- Secure Agent groups Use a Secure Agent group as the runtime environment when you need to access data on-premises or when you want to access data in a cloud computing services environment without using the Hosted Agent. When you select a Secure Agent group as the runtime environment for a connection or task, a Secure Agent within the group runs the tasks. Create Secure Agent groups to accomplish the following goals: Prevent the activities of one department from affecting another department. To prevent the activities of one department from impacting a different department, create separate Secure Agent groups for each department. For example, users in the sales department run 10 times as many tasks as users in the finance department, but the finance tasks are more time critical. To prevent the sales tasks from impacting the finance tasks, create separate Secure Agent groups for each department. Then assign the sales tasks to one runtime environment and the finance tasks to the other runtime environment. Separate tasks by environment. You can create different Secure Agent groups for test and production environments. When you configure a connection, you can associate it with the test or production database by choosing the appropriate Secure Agent group as the runtime environment.

- When you create a Secure Agent group, all users in the organization can select the Secure Agent group as the runtime environment. You can add and remove Secure Agents from a group. Based on your license, you can also perform the following actions: • If you have the Secure Agent Cluster license, you can add multiple agents to a Secure Agent group. • If you have the Organization Hierarchy license, you can share a Secure Agent group with your suborganizations. Note: If you use the runtime environment to run a mapping task that is based on an elastic mapping, the Secure Agent group must have only one Secure Agent. If you need to access output files on the Secure Agent machine, you can view the All Jobs page in Monitor or the My Jobs page in Data Integration to determine where a task ran.

Secure Agent Group with Multiple SA

- When you create a Secure Agent, it is added to its own group by default. If you have the Secure Agent Cluster license, you can add multiple agents to one Secure Agent group. All agents within a group must be of the same type, for example, all agents that run within your network or all agents that run on Amazon EC2 machines. Add multiple agents to a group to achieve the following goals: Balance the workload across machines. Add multiple agents to a group to balance the distribution of tasks across machines. When the runtime environment is a Secure Agent group with multiple agents, the group dispatches tasks to the available agents in a round-robin fashion. Improve scalability for connections and tasks. When you create a connection or task, you select the runtime environment to use. If the runtime environment is a Secure Agent group with multiple agents, the tasks can run if any Secure Agent in the group is up and running.
- You do not need to change connection or task properties when you add or remove an agent or if an agent in the group stops running. When you add multiple agents to a group, ensure that all of the Secure Agents are of the same type. For example, your organization installs four Secure Agents on physical machines within your network and two Secure Agents on Amazon EC2 machines.
- You can create a Secure Agent group that contains some or all of the local agents and a different group that contains the EC2 agents. Do not create a group that contains both a local agent and an EC2 agent. If you need to access output files on the Secure Agent machine, you can view the job details to determine which Secure Agent ran the task. To view job details, open Monitor, select All Jobs, and click the job name.

Secure Agent Installation

Informatica

Download & Install Secure Agent

Requirements

- Secure Agent may be installed and operated on a multi-core CPU machine with up to four (4) physical Cores (Not Logical/ vCPUs). Linux or Windows.
- Minimum of 16 GB RAM. Recommended to have up to 32 GB RAM with 8 Cores using FEP to accommodate all IICS services up and running like a process server, OI Data Collector, Mass Ingestion, common integration services, File Integration Services, etc.
- At least 250 GB disk space to run your tasks and store caches and logs with success.
- And more…Minimum requirements and best practices

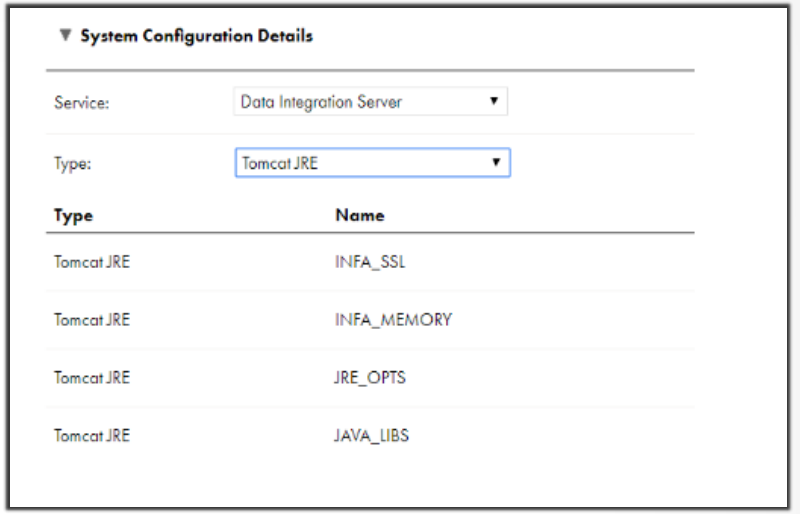
Other Considerations

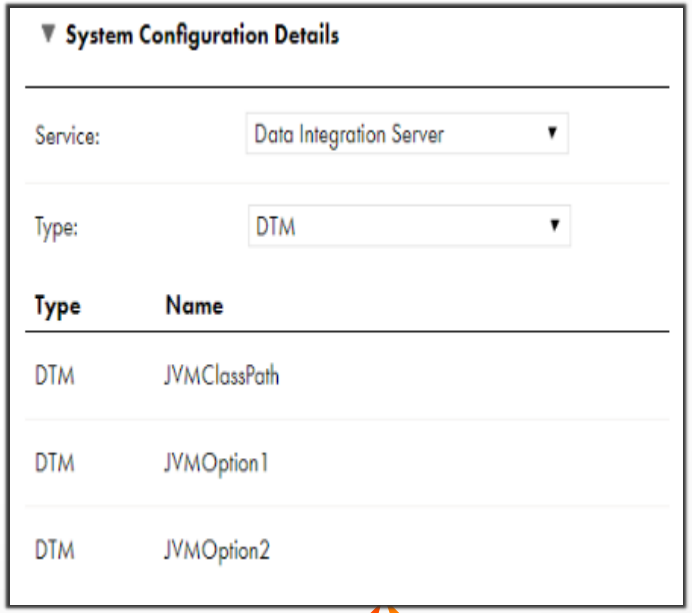
- Consideration for installing extra Secure Agents in an Org:
  - Grouped: H.A./Load Balancing, Separate Memory Resources (vertical scaling)
  - Adding Cores: Fast and Parallel Jobs (Horizontal scaling)
  - Separate: Dividing by Services, LOBs, or optimized for Source/Target
- Secure Agent Links
  - FAQs – Secure Agent Group, Cluster Server Considerations, Increase Java heap size and other memory attributes
  - Admin Guide – Secure Agent Services and Grouping Details

Secure Agent Key Points

- **DIS** service heap space. Need to increase if we see java heap space related message in :
  - Test connection
  - Metadata fetch
  - Agent logs(tomcat logs or tomcat out)
  - Designing mapping
  - Recommended value 4192 MB

- **DTM** - If you hit java out of memory or java heap error messages at run time of a mapping task execution(observed in session log), then memory attributes need to be defined as JVMOptions under DTM.
  - Need to defined under JVMOption like under JVMOption1, JVMOption2 and so on.
  - Each JVMOption parameter accepts one JVM parameter only.
  - JVMOption5 is the last default one, custom property under Type DTM and subtype INFO can be added to add further JVM parameter.
  - -Xmx****m. 2048m is enough.



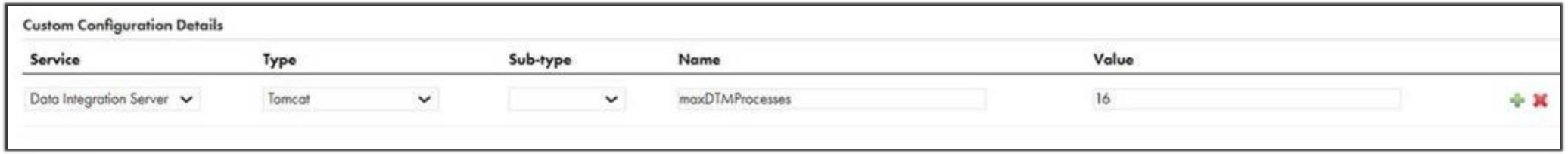


Secure Agent Contd..

maxDTMProcesses Custom Property

Background:

- By default, a SA schedule only two mapping tasks for execution.
- Additional tasks are Queued and becomes eligible for execution when slot is free.



Configuring **maxDTMProcesses** results in :

- Better CPU utilization
- Higher degree of concurrency

Recommended value = 0.75 of the No. of CPU cores on SA machine.

Guidelines:

- Do not exceed the terms of your license agreement (from compliance perspective).
- Setting property value > No. of CPU can increase parallelism but can cause performance bottlenecks in execution time.

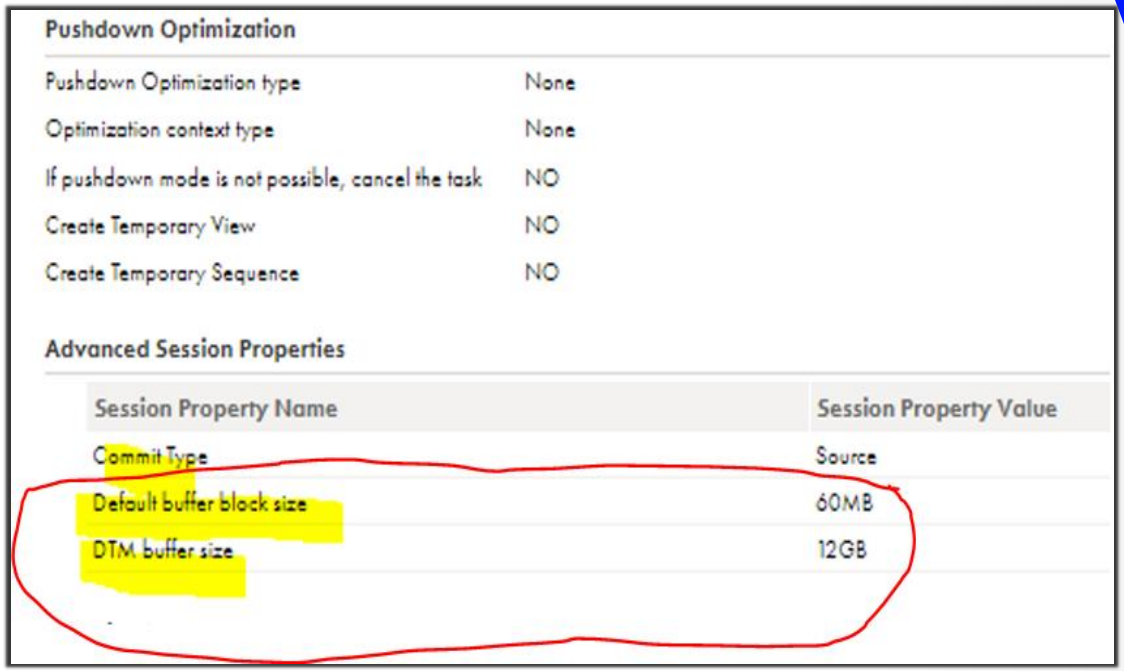
Secure Agent Contd..

DTM Buffer Size

- DTM Buffer size holds the actual data in blocks for processing.
- DTM Buffer size is automatically calculated based on Buffer block size.
- DTM Buffer Size = (DTM Buffer Block Size) * 10* N, where N is the number of partitions.
- Can be increased to increase number of blocks.

DTM Buffer Block Size

- Generally calculated as 2*X, where X is the maximum row size of any transformation.



Pushdown Optimization

Pushdown Optimization type	None
Optimization context type	None
If pushdown mode is not possible, cancel the task	NO
Create Temporary View	NO
Create Temporary Sequence	NO

Advanced Session Properties

Session Property Name	Session Property Value
Commit Type	Source
Default buffer block size	60MB
DTM buffer size	12GB

Informatica

Secure Agent Contd..

- **Use SA Group is recommended**.
  - High availability.
  - Load Balancing.

- **SA behind proxy**, below JVM parameters needs to set :

  - JVMOption1= **-Dhttps.proxySet**=True
  - JVMOption2= **-Dhttps.proxyHost**=<proxy_server_hostname>
  - JVMOption3= **-Dhttps.proxyPort**=<proxy_server_portnumber>
  - JVMOption4= **-Dhttps.proxyUser**=<user name>
  - JVMOption5= **-Dhttps.proxyPassword**=<password>
  - JVMOption6= **-Db360.datastore.useProxy**=true

  Administrator –> Runtime Environment -> System Configuration Details -> DTM Type -> JVMOptions

- For each org, we need to have separate Secure agent server. It cannot be shared.

IP Whitelisting

Informatica

Informatica Intelligent Cloud Services (IICS) implements security as a design principle. Security is considered at every step during product development life cycle. This design approach ensures that IICS is resistant to attack and resilient against failure. IICS may be used in systems compliant with SOC2, SOC3, HIPAA, and U.S.-EU Privacy Shield. Security program supporting IICS system is aligned with international security standards such as ISO27000.

IICS is built on microservices-based technology architecture and cloud native frameworks. The diagram below shows all major components of the IICS security domain and lays out the areas of metadata and data persistence and data movement. Users interact with IICS through a web client via the HTTPS protocol. The IICS host contains services such as Data Integration, Application Integration, API Management, and Integration Hub that can be accessed by users. These services are built on microservices and multi-tenant repositories on the back end with a common login page and user interface shell on the front end.

IICS security architecture is logically divided into IICS Platform and Data Center Infrastructure layers. IICS security provides protection across both platform and infrastructure layers with careful attention paid to the security of each layer. This layered, holistic security structure provides resistance to attack and resilience against failure. The entire stack becomes secure for each customer, with partners and customers easily able to complement Informatica Intelligent Cloud Services.

IICS Platform Security deals with securing access to Informatica Intelligent Cloud Services, which in turn ensures customer’s data processing is always protected and secure during the entire batch and real-time integration and data management life cycle. Data Center Infrastructure Security deals with security of the Informatica multi-tenant data center infrastructure that hosts Informatica Intelligent Cloud Services.

Controlling and auditing user access can often prevent security problems and help pinpoint and analyze any issues that do arise. Towards that, first and foremost, IICS requires each user in the customer organization to have an identity, which in turn supports role-based access management. IICS supports a variety of authentication mechanisms – password-based, SSO-based, certificate-based, and token-based authentication. Multi-factor authentication mechanisms like trusted IP address ranges also enable stringent security. For native password-based authentication, user credentials are hashed and securely stored in the IICS host. Administrators of the customer organization can configure policies for password strength and rotation to suit their business needs.

IP address to be whitelisted as per your POD -

POD Availability and Networking | Current Version

ORG Structure

Organizations

An organization is a secure area within the
Informatica Intelligent Cloud Services
repository that stores your licenses, user accounts, data integration assets such as mappings and tasks, and information about jobs and security.

You might have access to one or more organizations.

By default, the organization that you create when you start your free trial is a production organization.

Based on your licenses, you might also have access to the following organizations:

Sub-organizations

Administrators in the production organization can create one or more sub-organizations. Sub-organizations are child organizations of the production organization. They are automatically linked to the parent organization.

Each sub-organization has its own set of assets, connections, runtime environments, and users. However, the parent organization can share runtime environments and add-on connectors with a sub-organization. Administrators in the parent organization can switch to a sub-organization unless the sub-organization forbids this.

You cannot create any other organizations from a sub-organization.

Additional production organizations and sandbox organizations

Administrators in the production organization can create additional production organizations and sandbox organizations.

These organizations are automatically linked to the production organization for IPU usage, but they are otherwise completely independent organizations. They do not share assets, connections, runtime environments, or users with the production organization. Administrators in the production organization cannot switch into an additional production organization or a sandbox organization.

If the production organization has the license to create sub-organizations, administrators in the additional production organizations and sandbox organizations can create sub-organizations for their organizations.

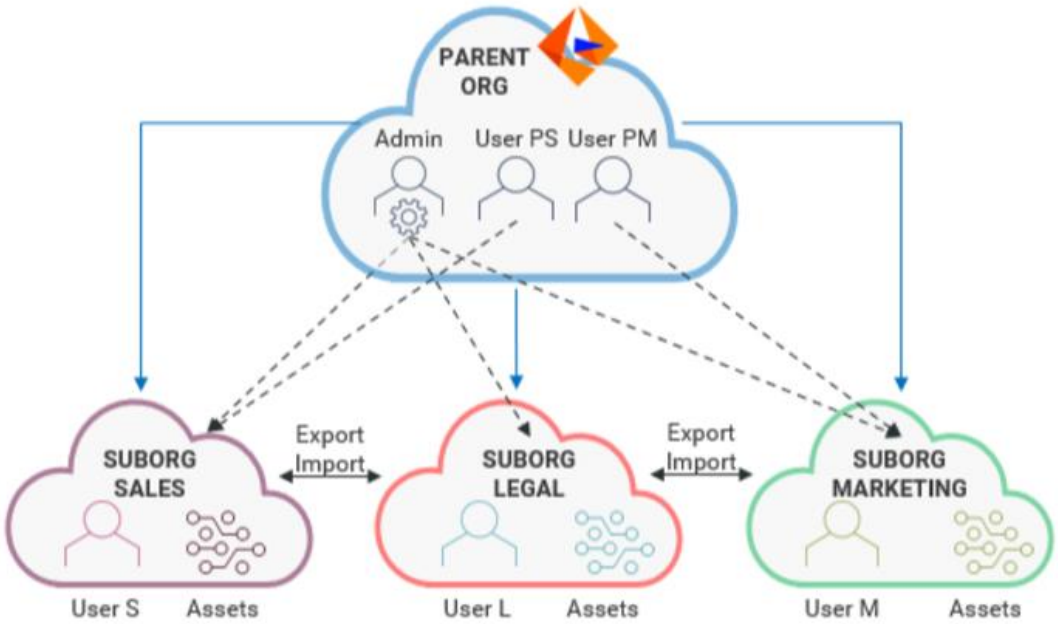
The administrator of an organization maintains the organization and its sub-organizations

More useful links –

1. Setting up a ORG - Setting up an organization
2. Adding a Sub Org - Adding a sub-organization

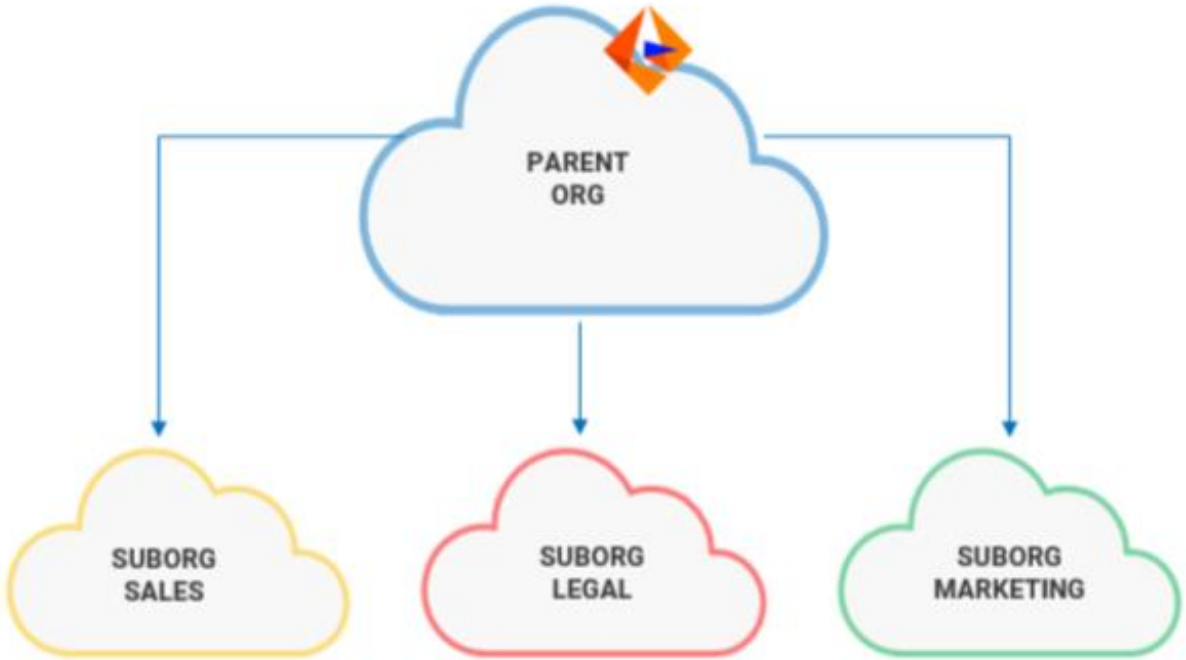
ORG & Sub Orgs

SubOrgs – Users/Assets



All IDMC orgs - parent orgs, sub orgs, additional orgs, sandbox orgs - are isolated, tenanted boundaries. Suborgs are logically linked to the parent org and can be navigated to, from a parent org login - they are NOT a part of the parent org.

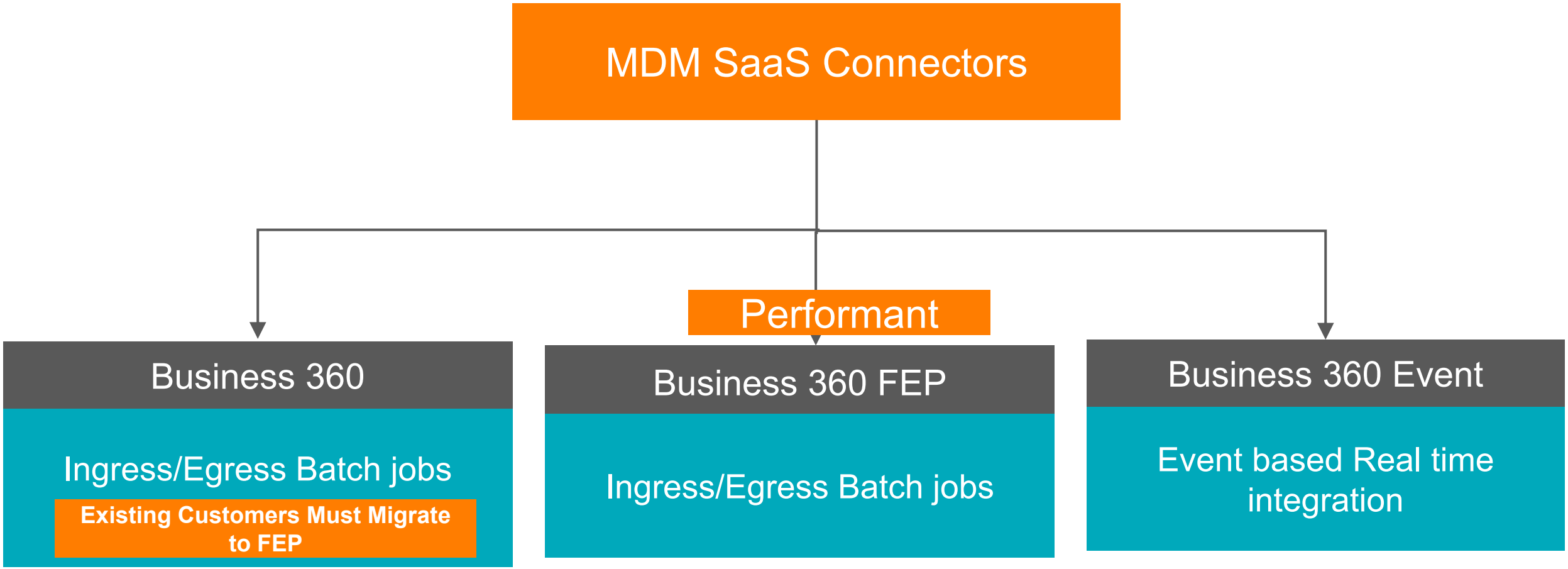
Organizations



- An organization is a secure area within the IDMC repository that stores your licenses, user accounts, assets such as mappings and tasks, and information about jobs and security
- SUBORGS
  - Administrators in the production organization can create one or more sub-organizations. SubOrgs are child organizations of the prod organization. They are automatically linked to the parent org
  - Each sub-org has its own set of assets, connections, runtime environments, and users. However, the parent org can share runtime environments and add-on connectors with a sub-org. Admins in the parent org can switch to a sub-org unless the sub-org forbids this
  - You cannot create any other orgs from a sub-org
- SANDBOXES
  - Admins in the prod org can create additional production organizations and sandbox organizations
  - These orgs are automatically linked to the prod org for IPU usage, but they are otherwise completely independent orgs. They do not share assets, connections, runtime environments, or users with the prod org. Admins in the prod org cannot switch into an additional prod or sandbox org

MDM SaaS Connectivity

Types of Connectivity



User Roles walkthrough

Informatica

User and User Roles Overview

- A user is an individual account in Informatica Intelligent Cloud Services.
- Customer 360 and Business 360 Console users must have an Informatica Intelligent Cloud Services user account.
- You can create and manage users in Administrator service.
- A role is a collection of privileges that you assign to users to allow access to Customer 360 and Business 360 Console.

Customer 360 Roles

- Customer 360 user roles have the privileges to access Customer 360 Service.

Customer 360 Analyst	Customer 360 Manager	Customer 360 Data Steward	MDM Business User
• Create and edit records in Customer 360. • When a Customer 360 Analyst creates or edits a record, the changes trigger a review process that requires approval from a Customer 360 Manager.	• Review and approve customer records or update customer records. • They can also create or edit records without approval.	• Role for creating records and hierarchies. • They can create and edit records without approval, run jobs, and review and approve customer records.	• View records in Customer 360. • They cannot create or edit records in Customer 360.

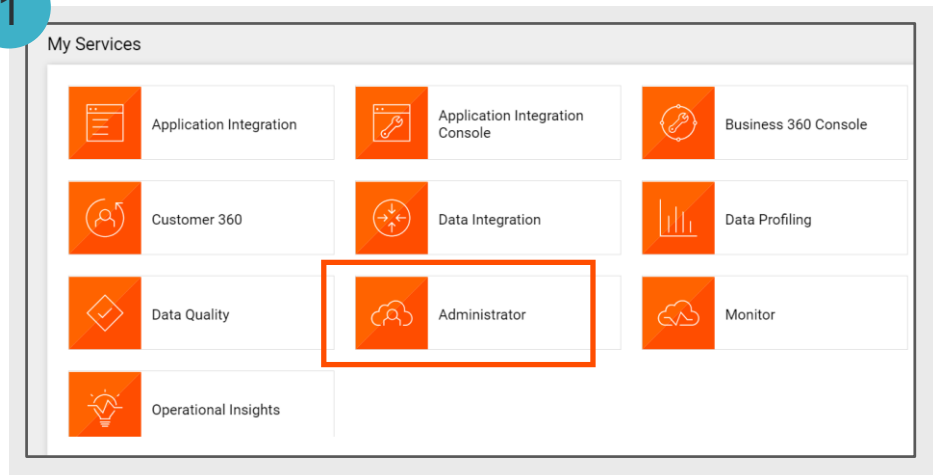
Business 360 Roles

- Business 360 user roles have the privileges to access Business 360 Service.

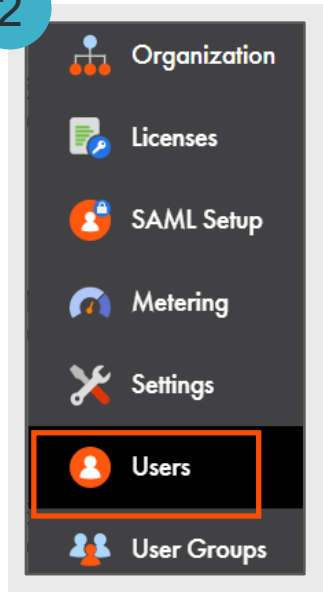
Admin	Designer	MDM Designer	Business 360 Process Executor	Job Executor
Provides full access to Business 360 Console . Allows users to perform solution upgrades. Allows users to create reports in business applications.	• Allows users to perform tasks in Business 360 Console that require integration with other services such as Data Integration and Data Quality.	• Allows users to perform the MDM SaaS specific assets in Business 360 Console like modelling, match merge config, ingress/egress job definition.	• Allow users with custom user roles to perform tasks in Business 360 Console and business applications like Import records , Hierarchy view, Workflow task	• Allows users to run ingress and egress jobs in Business 360 Console.

Steps to Create a User in the Administrator

1

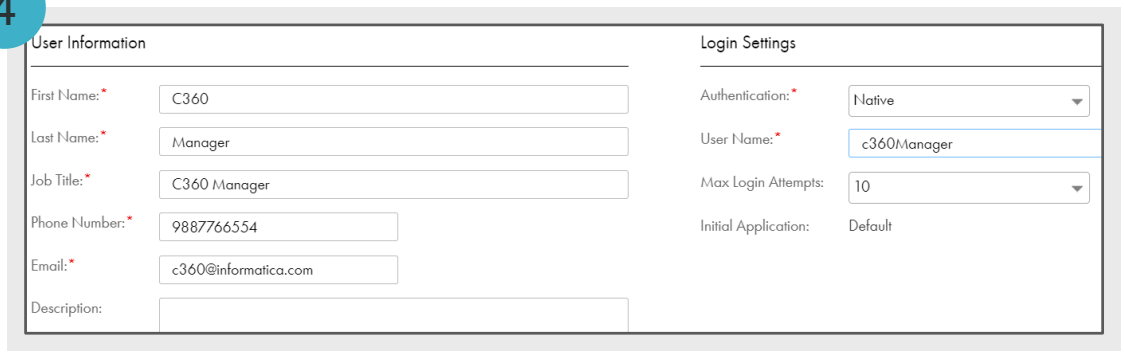


2

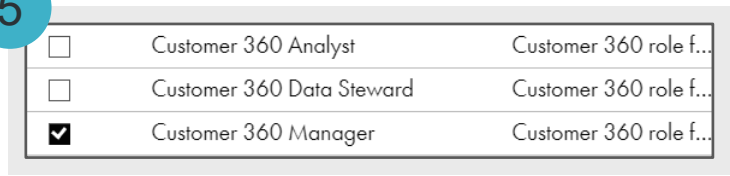


3

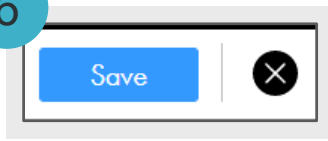
4



5



6



Set up Business Applications / Application Initialization

Informatica

Best Practices for Application Initialization

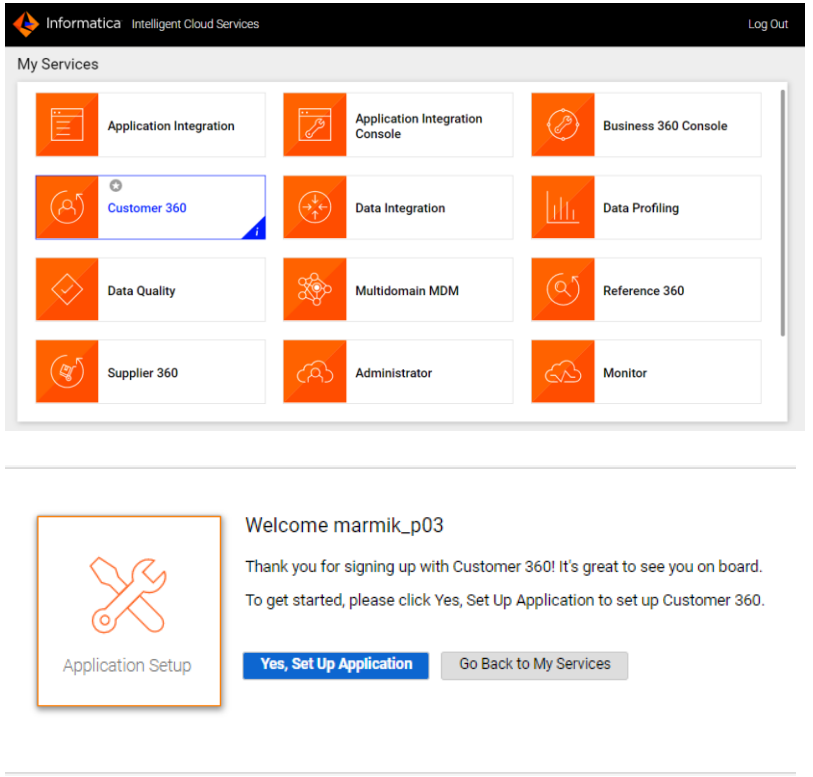
- Ensure all Business 360 processes under Application Integration should be in published state
- Org should be upgraded to latest release from Business 360
- Org state should be “ORG_PROVISIONED”-Optional
- Activate Admin user via CSM and assign the admin role and a group to users required for setting up application
- Create projects for additional assets that you require, such as mappings, mapping tasks, task flows, and other MDM SaaS assets. Avoid using predefined projects, such as Business360, Reference360, and Customer360, for these assets.
- Don't add any permissions to the predefined projects on the Explorer page in MDM SaaS.

Set up Business Applications / Application Initialization

After all the pre-requisites and best practices are taken care of, you can set up the business applications.

1. Log in to Informatica Intelligent Cloud Services.
2. Click the business application that requires setup.
3. Click **Yes, Set Up Application**.

- It might take several minutes for the setup to complete. You can click **Go Back to My Services** while waiting.
- Congratulations! Setup is now complete. You can now configure the business application.




Thank
you