



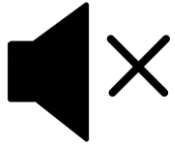
Mar 12, 2024

IDMC - Secret Manager Service

- Ravibabu Tubati, Sr Solution Architect, CSA
- Aracely Salazar, Associate Solutions 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.

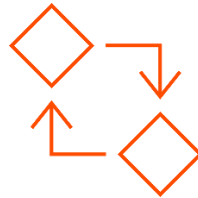
Feature Rich Success Portal



**Bootstrap trial and
POC Customers**



**Enriched Customer
Onboarding
experience**



**Product
Learning Paths
and Weekly
Expert Sessions**

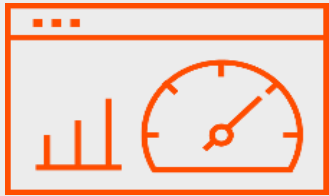


**Informatica
Concierge**



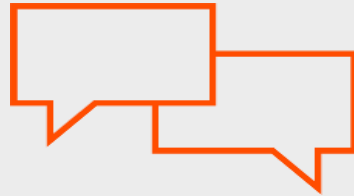
**Tailored training
and content
recommendations**

More Information



Success Portal

<https://success.informatica.com>



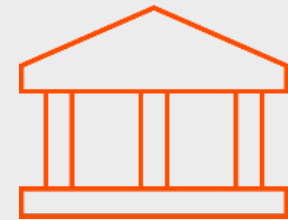
Communities & Support

<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.



Secret Manager Service

Ravibabu Tubati, Solutions Architect

Aracely Salazar, Associate Solutions Architect

Where data
& AI come to 

Secret Vault Integration

Summary: Ability to retrieve connection credentials from external secret vault



Key Highlights

Problem

Customers need to create connection object for every single endpoint they want to connect. This turns into very sensitive information duplicated and managed in multiple places

Solution

Integration with ecosystem secret vaults to retrieve connection credentials from there



Benefits

Customers manage credentials in vault as part of their governance policy/procedures in a centralized manner, avoiding duplication and mitigating risk

Sensitive customer technology credentials never persisted in Informatica

The screenshot displays the Informatica Administrator web interface. On the left is a navigation sidebar with options: Organization, Licenses, SAML Setup, Metering, Settings (highlighted), Users, User Groups, User Roles, Runtime Environ..., Connections, Add-On Connectors, Schedules, Add-On Bundles, Swagger Files, and Logs. The main content area is titled 'Settings' and has a 'Security' sub-tab selected. A modal window titled 'Secret Vault' is open, containing the following configuration options:

- Enable Secret Vault
- Type:
- Authentication Type:
- Access Key ID:
- Secret Access Key:
- Region:
-

Below the configuration fields, there is a note: "Configure this organization to retrieve connection credentials from an external secret vault. To test the vault connection, the SecretManagerApp service must be running on a Secure Agent in at least one runtime environment."

Configuration of Feature

Existing Auth and Payload Assessment

Vault Configuration

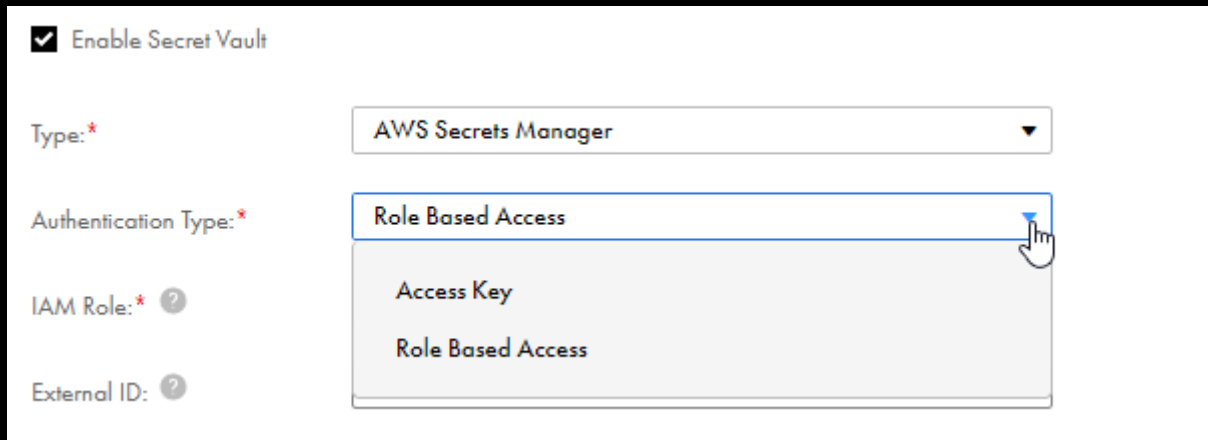
The screenshot shows the Informatica Administrator interface. The left sidebar contains navigation options: Organization, Licenses, SAML Setup, Metering, Settings (selected), Users, User Groups, User Roles, Runtime Environmen..., Connections, Add-On Connectors, Schedules, Add-On Bundles, Swagger Files, and Logs. The main content area is titled 'Settings' and has tabs for 'General' and 'Security'. Under the 'Security' tab, there is a 'Secret Vault' section. A message states: 'Configure this organization to retrieve connection credentials from an external secret vault. To test the vault connection, the SecretManagerApp service must be running on a Secure Agent in at least one runtime environment.' Below this, there is a checkbox for 'Enable Secret Vault' which is checked. The configuration fields are: Type (AWS Secrets Manager), Authentication Type (Access Key), Access Key ID (masked with dots), Secret Access Key (masked with dots), and Region (us-east-1). A 'Test Vault Connection' button is located at the bottom right of the configuration area.

Connection Configuration

The screenshot shows the 'Connection Details' configuration page for a SQL Server connection. The 'Connection Name' is 'SQLServer2008_02'. The 'Description' field is empty. The 'Type' is 'SQL Server'. Under the 'SQL Server Connection Properties' section, the 'Use Secret Vault' checkbox is checked and highlighted with a red box. Other properties include: Runtime Environment (redhat8ptfmqa.informatica.com), SQL Server Version (SQL Server 2008), Authentication Mode (SQL Server Authentication), Domain (empty), User Name (jsmith), Password (masked with dots and highlighted with a red box), Host (psv46impqa), and Port (1433).

Ways to Authenticate Vault/Manager

- Depending on the ecosystem you are integrating with, you will have different options to authenticate to connect to the Secret Vault:
- AWS
 - Role Based (based out of IAM roles)
 - Access Key (requires Access Key ID and Secrets Access Key)
- Azure
 - App Based: requires Client ID, Client Secret and Tenant ID



Enable Secret Vault

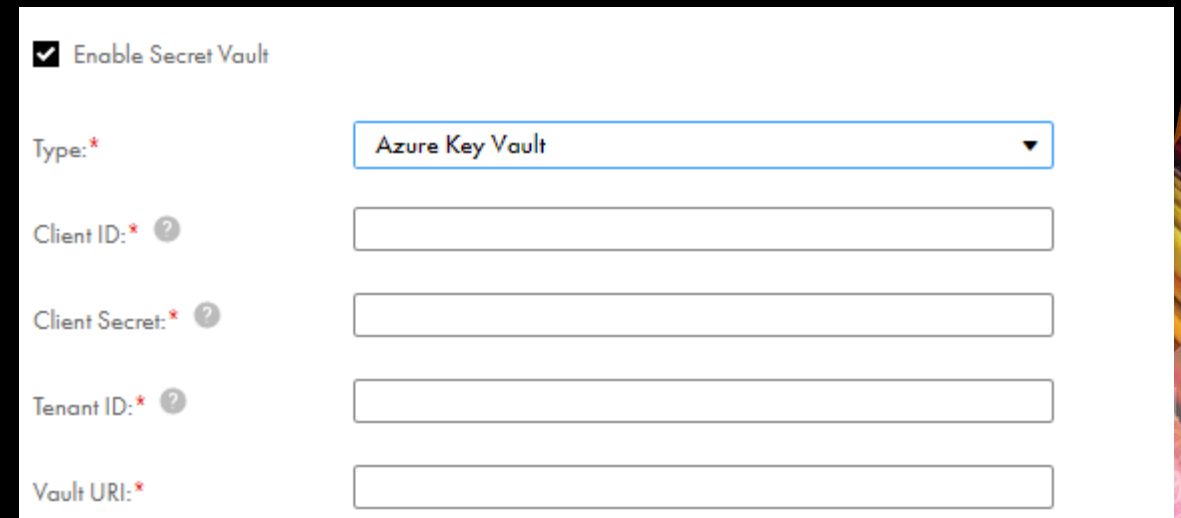
Type: *

Authentication Type: *

IAM Role: * ?

External ID: ?

The screenshot shows the AWS Secrets Manager configuration interface. The 'Type' dropdown is set to 'AWS Secrets Manager'. The 'Authentication Type' dropdown is open, showing 'Role Based Access' as the selected option. There are also fields for 'IAM Role' and 'External ID'.



Enable Secret Vault

Type: *

Client ID: * ?

Client Secret: * ?

Tenant ID: * ?

Vault URI: *

The screenshot shows the Azure Key Vault configuration interface. The 'Type' dropdown is set to 'Azure Key Vault'. There are four input fields for 'Client ID', 'Client Secret', 'Tenant ID', and 'Vault URI'.

Pre-Requisites/Roles for Secret Vault

Pre-Requisites:

- Licenses: Secret Manager, SecretManagerApp
- Secret Manager Service to be up and running in Agent
- Create Secret Vault Setting

Roles:

- Key Admin role (can configure the vault)
- Designer (can configure the connection)

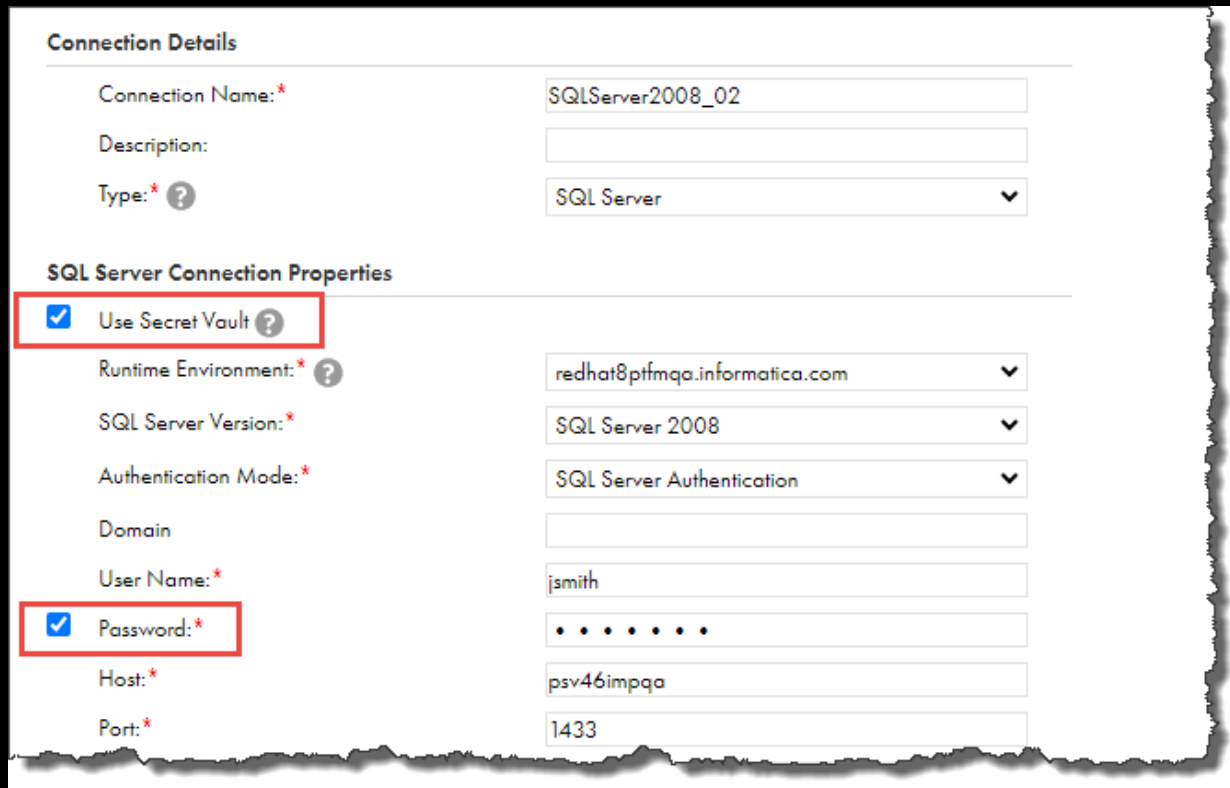
Custom Licenses (6)	
Custom License Name	Service Name
Data Loader Task	Data Integration
Dynamic Mapping Task	Data Integration
RESTSwaggerGenerator	Platform
SDKPatch	Platform
Secret Manager	Platform
SecretManagerApp_R1	Platform

Agent Service Details			
Service Name	Enabled/Disabled	Status	Version
OI Data Collector	Enabled	✓ Up and Running	25.1
SecretManagerApp	Enabled	✓ Up and Running	1.0.2
Mass Ingestion	Enabled	✓ Up and Running	20.4
Common Integration Components	Enabled	✓ Up and Running	18.0.2

The screenshot shows the Informatica Administrator interface. On the left is a navigation menu with options: Organization, Licenses, SAML Setup, Metering, Settings (selected), Users, User Groups, User Roles, Runtime Environ..., Serverless Environ..., Connections, and Schedules. The main content area is titled 'Settings' and has tabs for 'General' and 'Security'. Under the 'Security' tab, there is a section for 'Secret Vault'. It includes a checkbox for 'Enable Secret Vault' which is checked. Below this, there are several configuration fields: 'Type:' set to 'AWS Secrets Manager', 'Authentication Type:' set to 'Access Key', 'Access Key ID:' with a masked value '*****', 'Secret Access Key:' with a masked value '*****', and 'Region:' set to 'us-east-1'.

Connection Definition

Feature Details



Connection Details

Connection Name:* SQLServer2008_02

Description:

Type:* ? SQL Server

SQL Server Connection Properties

Use Secret Vault ?

Runtime Environment:* ? redhat8ptfmqa.informatica.com

SQL Server Version:* SQL Server 2008

Authentication Mode:* SQL Server Authentication

Domain:

User Name:* jsmith

Password:*

Host:* psv46impqa

Port:* 1433

- Customer will have the ability to select which connections they want to enable the feature for.
- Edit Connection using IDMC Administrator only
- Customers are charged by connection definition therefore we did not want to enable blanketly for all
- Currently we have selected fields which are sensitive limited to Username and Password as such.

SMS Meter

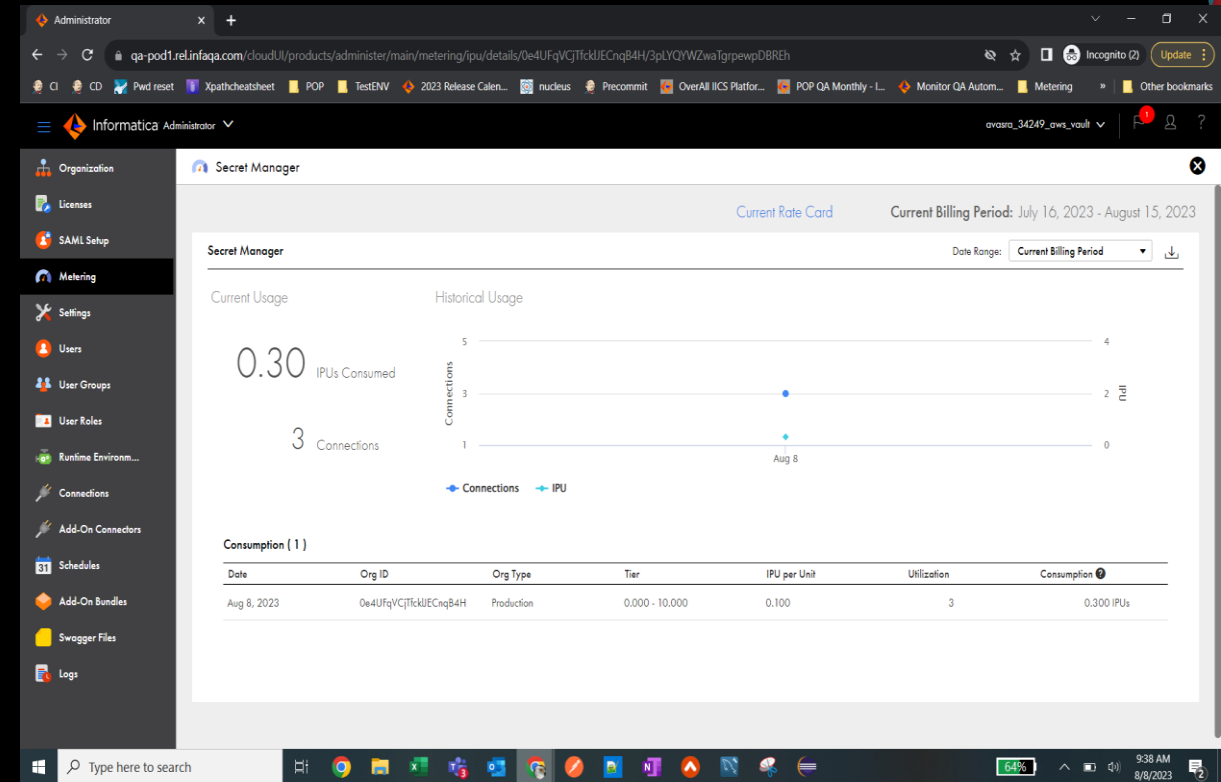
Secrets Manager Service Meter

Secrets Manager provides the ability for a customer to use their own cloud key secrets manager vaults to store and retrieve source/target credentials during run time. Customers can select which connections they would this feature is turned on for within their Connection Definitions.

- **Scaler:** Connection Definitions
- **Metric:** Daily Connection Definitions
- **IPU Per Metric Unit:**
 - 0.016 IPU for the first 600 Daily Connection Definitions
 - 0.0011 IPU for the next 601 -to 3,000 Daily Connection Definitions
 - 0.0006 IPU for each > 3,001 Daily Connection Definitions

Definition:

Connection Definitions: Source or /Target connections which are defined and configured with secret manager parameters toggled on.



DEMO

Guidelines for Usage

- Org must be configured to store connection credentials on the Cloud.
- Log in to SubOrg directly to see and enable Secret Vault
- AWS Secrets Manager:
 - To use role-based authentication, the Secure Agent must be in an EC2 instance.
 - <secret name>:<secret key>, Secret Key is the Key Value in AWS.
- Restrictions for secret names for AWS and Azure
 - AWS, alphanumeric and only these special characters: / _ + = . @ - “
 - Azure, alphanumeric characters and dashes.
- When Switching from Vault to non-Vault, you have to re-renter username and password.
- For more information, please visit Informatica Documentation, Under Administrator you will find Secret Manager Configuration.

