Fall 2022

SafePaaS™

Leading Policy-based Access Governance Platform

A message from SafePaaS CTO

SafePost Quarterly

Hennie Vermeulen

SafePaaS continues to provide innovative capabilities on the platform to meet the growing needs of our customers. In the third quarter, we released 27 new enhancements across product suites including enhanced API Services, simplified data transfer for Oracle E-Business Suite customers, and Configuration change tracking for Oracle ERP Cloud customers.

As a growing number of organizations aim to adopt a zero-trust approach to enterprise cybersecurity and access risks, SafePaaS continues to innovate and invest deeply in R&D to protect our customers from the avalanche of security challenges they face. Our mission is to safeguard our customers from risk so that they can achieve business objectives.

As our customers increase cloud application adoption and implement multi-cloud infrastructures, secure and encrypted data integration services are paramount to provide continuous protection across the enterprise in real time.

The hype around cloud computing leaves on-premise customers feeling "abandoned". A large number of enterprise customers still have on-premise applications that require protection and security. Oracle E-Business Suite PeopleSoft and JD Edwards customers can now simplify data transfer through JDBC connection secured by VPN Tunnel to ensure segregation of duties compliance.

Oracle ERP Cloud customers can now use Change Tracking capabilities in SafePaaS to ensure accurate and timely evidence of control incidents for audit.

Until December 31, 2022, we are offering all customers a one-time discount to purchase and provision new SafePaaS applications to mitigate risks and address any Governance, Audit, and Compliance needs. We encourage all customers to contact their account executive to find out more.

WHAT'S INSIDE THIS ISSUE?

One-time offer only - use your RiskReward Credits to purchase and provision new SafePaaS applications before December 31, 2022.

RiskReward customers are **rewarded by being given priority on enhancement requests, software trials as well as live knowledge transfer workshops by product experts.**

RiskReward customers can earn reward points based on:

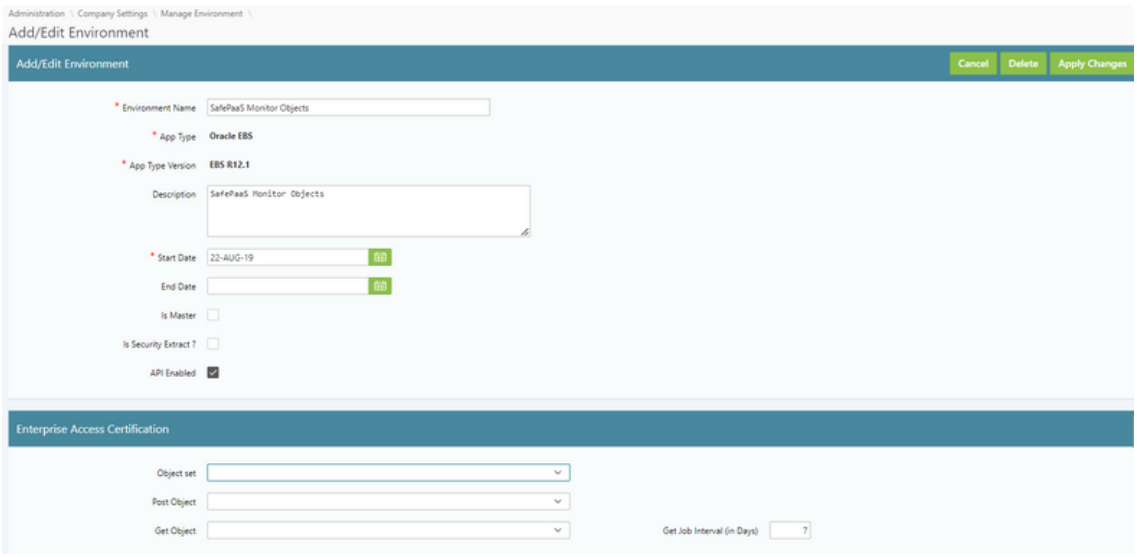
- Total spend with SafePaaS per calendar year
- Level of SafePaaS platform adoption
- SafePaaS usage for risk reduction
- Participation in Quarterly Business Reviews
- Providing product references and assisting with business case studies
- Feedback on product enhancements and bugs
- Trial period of 90 days on new software

Securely Bring in Data from any Application, ERP, and Infrastructure using enhanced API services

DataProbe™ is a versatile ETL tool that provides secure and encrypted data integration services. DataProbe™ allows you to extract, transform and load data into SafePaaS from external data sources, including on-premise ERP database and cloud enterprise applications as well as IDM and ITSM systems. DataProbe™ supports many popular APIs standards to integrate with multiple data sources, including JDBC, SOAP Web Services, REST Services, and flat file upload.

Customers can now use the POST API services to transfer security, centrifugation, master data, and transaction snapshots from any enterprise application using meta-data objects available with DataProbe™. Customers can also add new data sources using object management capabilities, including data discovery and sampling methods.

The following shows the new API page to enable POST services:

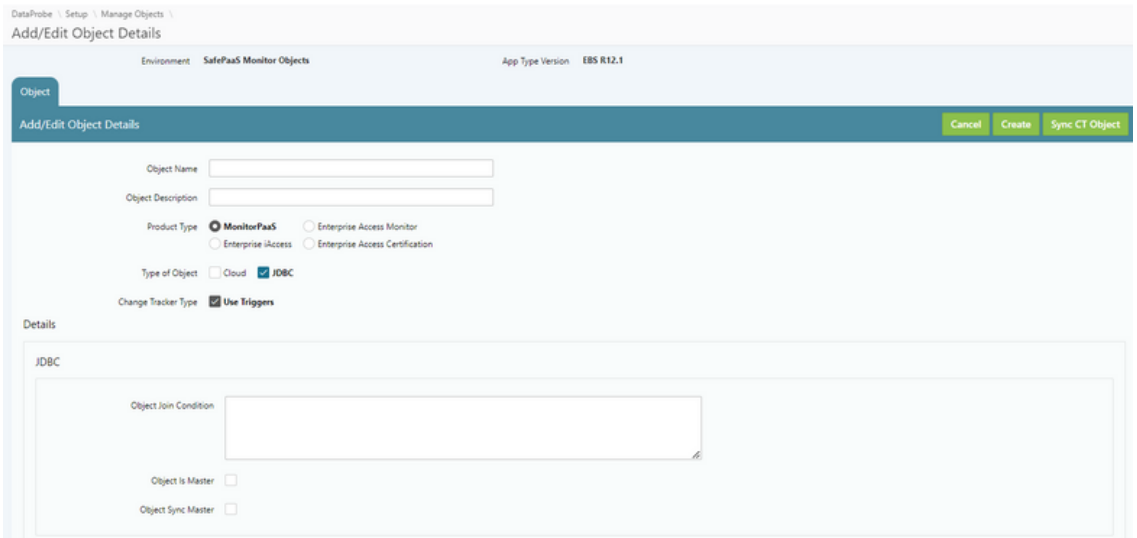


Enhanced JDBC services enable on-premise ERP customers to schedule automated data synchronization from SafePaaS

Customers that are continuing to operate on-premise ERP systems such as Oracle E-Business Suite, PeopleSoft, SAP and JD Edwards can automate the ERP security snapshot upload process within SafePaaS to reduce manual efforts required to extract the snapshots using database scripts and load the data into SafePaaS. Many customers perform this task weekly or monthly to ensure compliance with Segregation of Duty policies. Some customers have automated this step using the batch processing tools such as secure File Transfer Protocol (sFTP) and Concurrent Managers in Oracle EBS.

JDBC (Java Database Connectivity) is the Java API that manages connecting to a database, issuing queries and commands, and handling result sets obtained from the database. TLS/SSL is configured using connection properties for clients connecting via the JDBC interface.

See the JDBC page setup below:

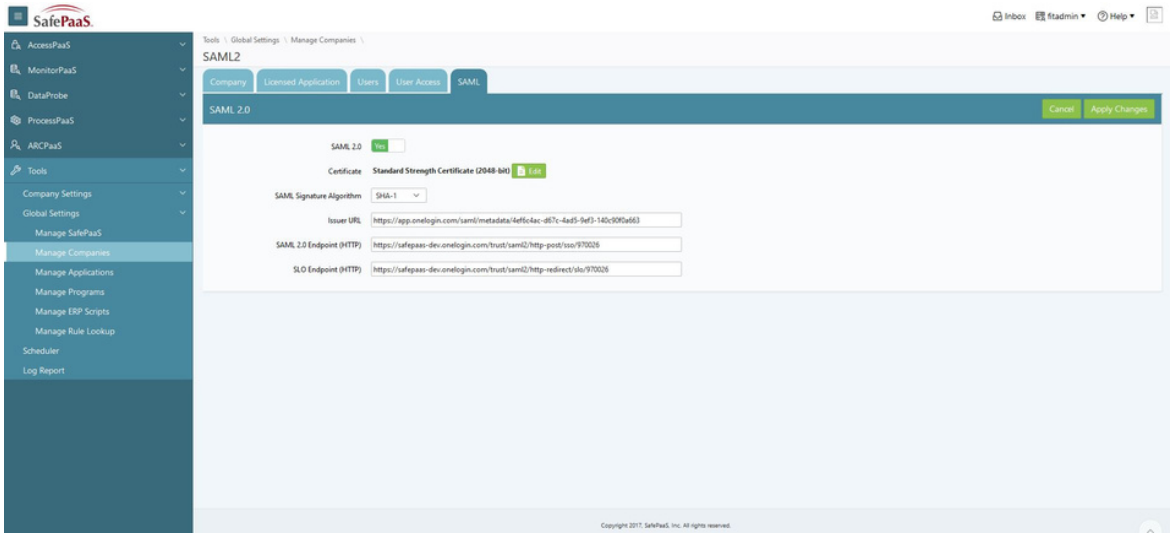


Policy-based Access Governance for Microsoft Azure AD

SafePaaS' cloud-native platform is now available to govern Identity Lifecycle Management in Microsoft Azure AD by automatically synchronizing the identities using API services. SafePaaS goes beyond enabling authentication and role-based access to help our customers achieve comprehensive identity access governance with attribute visibility based on zero trust.

SafePaaS' identity access governance hub for Microsoft Azure AD gives you the visibility and control your security team needs to support your compliance, risk, and governance efforts without slowing down or putting your business at risk. If you are currently using Azure AD for identity authentication, please contact our support team to enable single sign-on (SSO) in SafePaaS.

You can setup SSO in SafePaaS under the Company Setting as shown below:



Track Configuration Changes in Oracle Cloud

Oracle ERP Cloud customers face a number of challenges when it comes to maintaining audit policies. The challenges with audit policies in the cloud include the following:

- Lack of Control over Audit Policies – Privileged users can change the audit level. Some audit levels cannot be reset once changed.
- Data Fragmentation – Requires custom reports to view complete changes to business objects such as suppliers, security roles, and journal categories.
- Limited Visibility – Missing audit policies and analytics to track changes over a financial period across all audit objects.
- Manual Control – Evidence of control active – response to changes, reconciliation with ITSM to ensure control evidence is offline/manual.

SafePaaS allows customers to:

- Tracking changes in base tables, as well as audit policies, improves the completeness of control evidence.
- Select, extend or create business objects in SafePaaS to monitor changes across related entities in the Cloud.
- Closed-loop workflow ensures accurate and timely evidence of control incidents is available for audit.
- Fast track controls deployments with auto-generated BI reports directly into ERP – no BI/coding skills required.
- Controls evidence is tamper-proof and securely “vaulted” outside the ERP.

Access Governance for OCI (Oracle Cloud Infrastructure)

Cloud governance is an ongoing problem that burdens security, compliance, and management. As organizations move to Oracle Cloud Infrastructure to run their on-premise applications such as E-Business Suite in the Cloud, they need to ensure that access to OCI and all applications on OCI is secure and governed. The problem is that infrastructure accounts, administrative accounts and middle-layer accounts that are used by technical teams are accounts with high risk privileges, in other words, they are “keys to the kingdom” accounts. Access to these accounts needs to be governed, monitored, and /or certified to ensure risk is mitigated. SafePaaS can connect to OCI and provide access governance for these accounts that if not monitored, can cause chaos.

Proactively prevent Financial Misstatement Risk with Segregation of Duty Controls Monitoring

Staying true to our company mission, we wanted to highlight one of the principal reasons customers choose SafePaaS as an audit platform. The platform has been built and designed by former auditors with audit and compliance in mind.

The most effective way to avoid financial reporting errors is to prevent them with robust controls. Controls are policies, procedures, and technical precautions that safeguard an organization’s resources by avoiding mistakes and inappropriate actions. Controls, such as the segregation of duties, access controls, automated process controls, and internal audits, can help prevent errors and increase the ability to detect mistakes and fraud.

SafePaaS provides a robust controls platform for the automated detection, mitigation, remediation, and prevention of access risk and segregation of duties to mitigate financial misstatement errors. Implementing effective automated segregation of duties is critical to efficiently managing and mitigating material misstatement risk.

Read How to mitigate financial misstatement risk with effective segregation of duties.

READ EBOOK

Solve Multi-cloud security and governance challenges

We recognize that our customers are implementing multi-cloud strategies. There are many benefits to a multi-cloud strategy, but operating in multiple clouds also introduces complexity. If not managed carefully, a multi-cloud architecture can rob the cost-saving component of the cloud and hinder your performance goals. Multi-cloud vulnerabilities can manifest because each Cloud provider has a different method of managing identity, privileges, and entitlements. These differences in security models complicate visibility, governance, and security across multi-cloud environments. And if left unaddressed, your organization is vulnerable to attacks, breaches, and additional security incidents.

When securing multi-cloud environments, remember that each cloud service provider has its own model for managing identities and privileges. Those models each have different roles and security controls, requiring a single solution to manage identities across all clouds.

One of multi-cloud management's most significant security risks is privileged access sprawl. A converged platform that can reduce privileged access sprawl with access certification is necessary to curb the accumulation of privileges. Converged identity platforms consolidate this effort and perform tasks with a single set of credentials and a consistent policy.

LEARN MORE

Industry Insight

The following recent cases, highlight the importance of how effective access governance can mitigate risk.

Toyota Data Breach

Japanese carmaker Toyota suffered a breach of customer records and disclosed a security incident. The root cause of the data breach was found to be a subcontractor uploading Toyota source code to a GitHub repository that was inadvertently set to public access between 2017 and 2022.

Insider Bank fraud - Africa

As a result of preliminary investigations, 12 bankers were arrested. It is suspected that they allegedly stole funds from **dormant accounts** in a branch of an old-generation bank in Enugu, Nigeria.

Insider Fraud - lack of segregation of duties

An investigation by Comptroller's Office in Tennessee revealed that a former director of the Meigs County Emergency Communications District misappropriated more than $1,000,000 between July 2011 and February 2021.

Investigators determined the former director misappropriated the majority of the district's money by falsifying invoices from real and fictitious vendors and cashing district checks that were written to pay these fake invoices.

Forward-thinking events

We continue to attend industry-leading events and host insight sessions with industry experts.

September 20 saw the SafePaaS team in Chicago at the **ISACA Chicago Annual Conference Convergence** where we announced Policy-based Access Controls (PBAC) Governance for SAP S/4 HANA. Rapidly growing cybersecurity risks along with the continuously changing SAP landscapes, regulatory environments, and cloud are challenging the most forward-thinking organizations. Measures to safeguard critical systems include access review to limit access to sensitive privileges and data to only authorized users. Any unauthorized access can be terminated to eliminate any threat to critical applications, data, or infrastructure. Without effective access governance, businesses cannot ensure the sensitive data they are responsible for is kept safe from hackers and cybercriminals.

On September 28, SafePaaS joined forces with **ERP Risk Advisors for How to Design Roles for an effective Oracle ERP Cloud audit** and announced our **strategic new partnership** that aims to simplify audit for Oracle ERP customers.

September 29 VP Solution Specialist Robert Enders and our CEO Adil Khan exhibited at the Cyber Security Conference in Dallas where we announced cutting-edge enhancements to our Policy-Based Access Controls management SaaS platform. SafePaaS customers have unmatched advantage to control all identity risks across the enterprise and all data sources including, cloud infrastructure, ERP, vertical applications, ITSM, databases, and servers to protect businesses from continued insider external and cyber threats.

New hires

The SafePaaS team continues to grow. This quarter we welcome:

In Q3 we welcome Pablo Stahlhamer to the SafePaaS Family. Pablo joins us as a Senior Consultant - Consulting Services and joins our growing team in Argentina. Pablo brings extensive Oracle Technical expertise and more than 20 years of experience to the team.

We also welcome Maria Isabel Brum who joins as QA Analyst. Based in Colombia, Maria Isabel brings a wealth of experience to ensure the platform is reliable, fully functional, and user-friendly.