

# Oracle HCM Security

What Clients Should Know *Before*  
They Implement



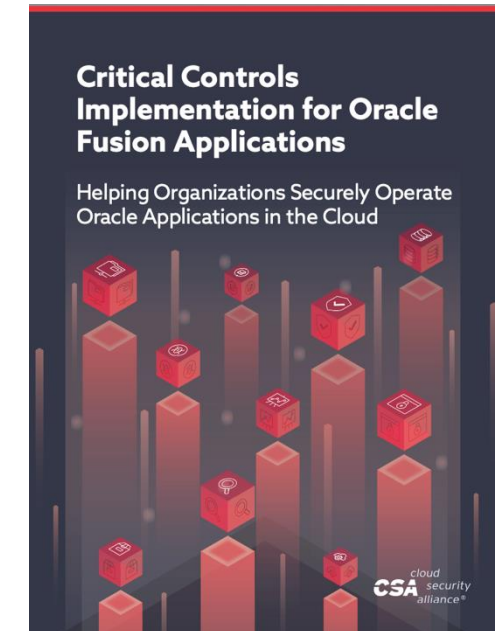
# Speaker – Moderator



## Mike Miller

Syntax Senior Solution Architect

- Over 25 years of working with enterprise software and information security technologies
- Experience with enterprise software implementation and support, cloud operations, and executing compliance and risk management programs.
- A CISSP, Certified Information Systems Security Professional
- Oracle ACE Associate



# Syntax



- Founded in 1972 in Montreal, Canada, Syntax is a global company with 3,600+ employees across 15 countries
- Syntax provides full-stack, full-lifecycle Cloud Managed Services and Application Managed Services focused on leading ERP solutions such as JD Edwards, Oracle E-Business Suite, and SAP
- Syntax is a multicloud partner and supports OCI, AWS, Azure, GCP, and Syntax Enterprise Cloud®
- Our ERP solutions include an array of value-add services, including our AI-driven monitoring and automation platform, CxHub customer experience portal, security management, and FinOps



*Expertise in*  
**Cloud Service Solution  
OCI Migration**  
in NAMED-North America



*Expertise in*  
**Oracle E-Business Suite  
Applications to Oracle Cloud**  
in North America



*Expertise in*  
**JD Edwards Applications  
to Oracle Cloud**  
in North America



*Expertise in*  
**Oracle Cloud Platform -  
Oracle Cloud Platform Integration**  
in North America



*Expertise in*  
**CSPE: Oracle Cloud Platform -  
Oracle Cloud Platform  
Data Management**  
in North America



*Expertise in*  
**CSPE: Oracle Cloud Platform -  
Oracle Database to Oracle Cloud**  
in North America

# Agenda



- HCM Security Basics:
  - Authentication
  - Authorization and Role-Based Security
  - Auditing
  - Data security and scrambling
- Security for Different Implementation Phases
  - Data Scrambling and Testing
  - Implementation vs Day-2 Security Needs
- 25B is Big
  - What you should know
- Lessons Learned
  - Use Cases for Small and Large Clients
- Key takeaways and questions to ask



A vibrant, stylized illustration of a city skyline. In the foreground, there's a body of water reflecting the sky. Behind it, a dense line of green trees and palm trees separates the water from the city. The city features several tall, modern skyscrapers in shades of blue and grey. Three hot air balloons with colorful, geometric patterns (red, orange, yellow, green, blue) are floating in the sky. The sky is a bright blue with large, white, fluffy clouds. The overall style is flat and graphic, typical of modern digital art.

# Introduction to Oracle HCM Cloud Security

## The Basics

# Authentication and Physical Access



- Single Sign-On (SSO):
  - Integrates with organizational identity providers.
  - Simplifies user authentication
- Multi-Factor Authentication (MFA):
  - Adds an additional layer of security to user logins.
  - Recommend: use your IDP's MFA

## Location-Based and IP Restrictions

- Oracle HCM supports location-based security, allowing organizations to restrict access (by role) based on geographic location or IP address
- This is useful for limiting system access to specific offices or trusted networks

# Role-Based Authorization



## Roles

- Role Based Access Control and Assignment-level security ensures that users can access only the records of employees or data relevant to their assigned scope.

## Areas of Responsibility (AOR)

- AOR allows organizations to define specific responsibilities for users, such as managing employees in particular departments or geographic regions.

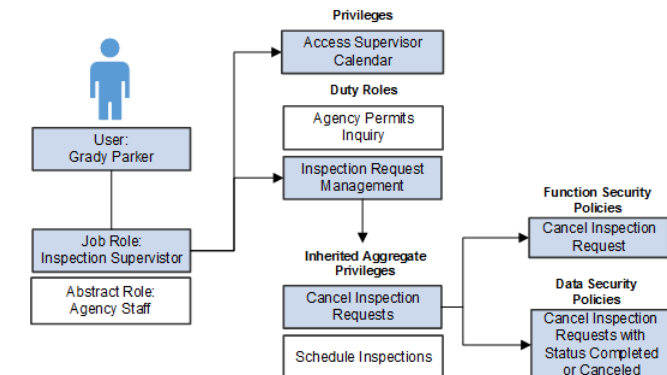
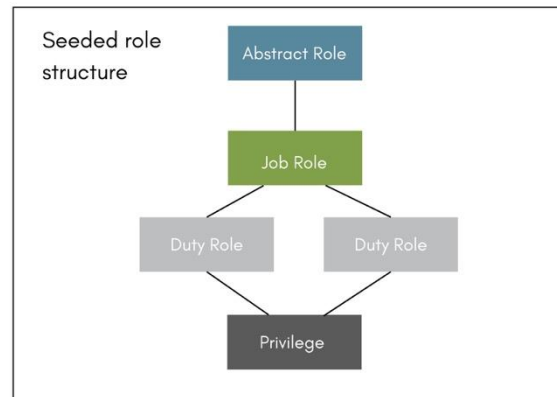
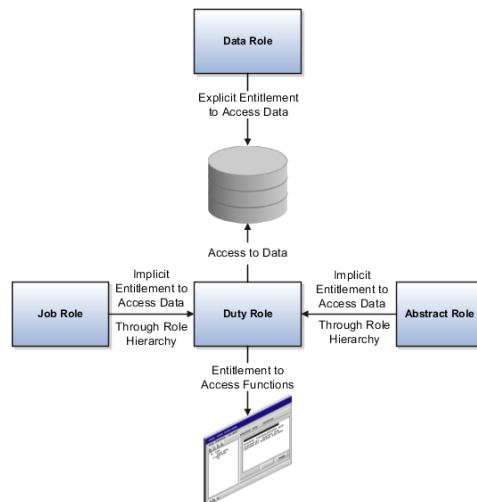
## Data Security Policies

- Data security policies define which rows of data users can access based on their roles.
- These policies control access to sensitive information like salaries, benefits, and performance data.
- Assigned to roles

# Types Of Roles



- Security roles define **access permissions** and control **what users can see and do** in Oracle HCM Cloud.
- Types of roles:
  - **Seeded Roles:** Predefined roles provided by Oracle.
  - **Custom Roles:** Tailored roles created to meet specific business needs.
  - **Abstract Roles:** High-level roles for user categories (e.g., Employee, Manager).
  - **Job Roles:** Associated with specific job functions (e.g., HR Specialist, Payroll Administrator).
  - **Duty Roles:** Granular roles tied to specific tasks (e.g., Manage Absence Records).





# Seeded Roles: Predefined by Oracle



- Examples:
  - **Human Resource Specialist**
  - **Employee**
  - **Line Manager**
- Characteristics:
  - Provided by Oracle to cover common use cases.
  - Designed to work "out-of-the-box."
- Use Cases:
  - Small organizations with straightforward security needs.
- **Pros:**
  - Easy to implement.
  - No need for initial customization.
- **Cons:**
  - May not meet complex requirements.

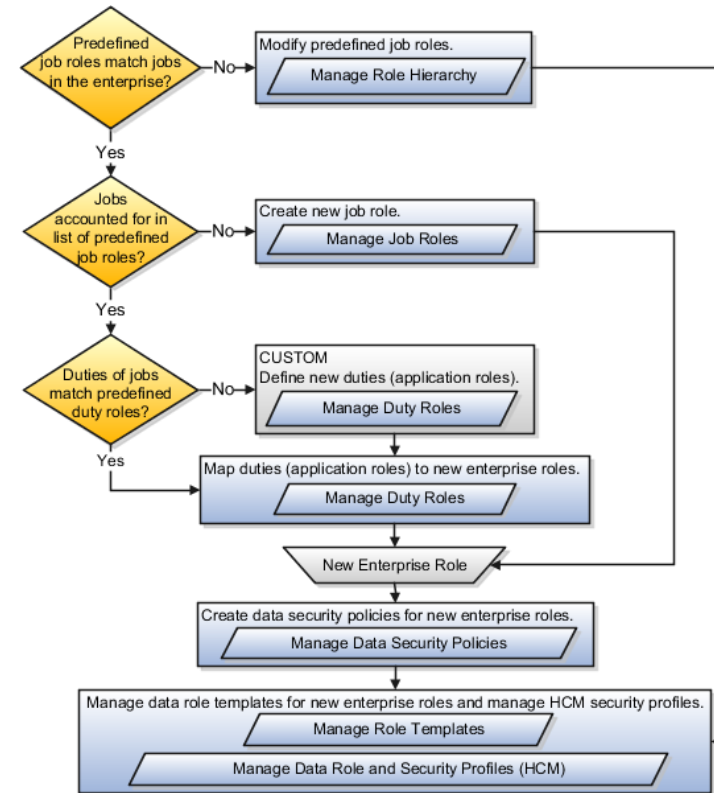
# Custom Roles: Tailored for Business Needs



- **Definition:**  
Created by administrators to meet specific organizational requirements.
- **Benefits:**
  - Provides flexibility for unique workflows and access requirements.
  - Can combine multiple abstract, job, and duty roles.
- **Example:**  
A custom role for a **Regional HR Manager** that combines access to payroll, employee records, and absence approval.

- **Best Practice:**

- Avoid excessive customization to reduce maintenance overhead.



# Abstract Roles: Broad User Categories



- **employee**
- **Manager**
- Characteristics:
  - Represents **high-level access** for user categories.
  - Assigned automatically based on predefined rules (e.g., when an employee is onboarded).
- Use Cases:
  - Basic access control for large organizations.
- **Important:** Abstract roles are **not job-specific**.

# Seeded Roles: Predefined by Oracle



- **Specialist**
- **Payroll Administrator**
- Characteristics:
  - Aligned with specific job functions and responsibilities.
  - Provides access to relevant modules (e.g., payroll, benefits).
- Use Cases:
  - Assign access based on the organizational hierarchy.
- **Tip:**
  - Regularly review job roles to ensure they align with changing job functions.

# *Duty Roles: Access Granularity for Tasks*



- **Definition:**  
Represents specific tasks users can perform within the system.
- Examples:
  - **Manage Absence Records**
  - **View Employee Compensation**
- Characteristics:
  - Assigned **within job roles** to provide granular access.
- **Best Practice:** Combine duty roles effectively to avoid overlapping permissions.



# Optimizing Role Assignment



- Use **seeded roles** for standard use cases.
- Create **custom roles** only if necessary.
- Avoid assigning **duty roles directly**—bundle them into job roles.
- Regularly audit role assignments to ensure compliance.
- Use **role hierarchies** for efficient permission management.

# Auditing is Off: Turn It On



Fusion audit logs are disabled by default and must first be enabled. Once enabled, they are retained indefinitely.

- There is no expiry or purge of audit logs nor currently no known storage fees due to accumulated audit logs.
- No performance impact
- Once enabled, Fusion Application audit logs can be viewed within the applications by using Navigator > Tools > Audit Reports. The privilege Manage Audit Policies (FND\_MANAGE\_AUDIT\_POLICIES\_PRIV) is required to see the audit logs

# Enable Auditing for APIs Too



- Diagnostic logging of APIs is not enabled by default. API authentication is logged separately from end-users:
  - API authentication is logged separately from end-users. Diagnostic logging of APIs is not enabled by default. Enable it by Security Console -> API Authentication -> View Diagnostic Logs -> Edit -> Enable
  - Once enabled, the same page can be used to view API diagnostic information. Similar but not as detailed information is also available in the table FND\_SESSIONS

# Enable HCM Sensitive Data Auditing



Verify sensitive data auditing is enabled within Fusion HCM. Fusion HCM pages can audit who has viewed “read” sensitive PII data such as National Identifier Numbers and Drivers Licenses:

Ensure that the profile option `ORA_HCM_SENSITIVE_DATA_VIEW_AUDIT_ENABLED` is enabled.

Once enabled audit data can be viewed by users with the privilege.  
`PER_VIEW_SENSITIVE_DATA_ACCESS_AUDIT_PRIV` using My Client Groups > Quick Actions > Show More > Transaction Configuration and Audit > Sensitive Data Access Audit.

Likewise a BI Publisher report can be used to query the table  
'`PER_SENSITIVE_DATA_AUDIT`.'

# Data Scrambling Is Now Free



- Data Scrambling for Testing
  - Protects sensitive employee data during testing phases
  - Ensures compliance with data privacy regulations
- Masking for non-production Data Masking Standalone MOS Note 2092389.1
  - As of April 2024 is FREE!
  - Standalone
  - Part of a Refresh

## What is Data Masking?



Data masking, also known as data scrambling, is the process of obscuring sensitive information copied from a production database with internally-consistent, scrubbed data based on masking rules, to a test or non-production database.

Fusion data masking is a process of applying a pattern or algorithm designed to scramble data in a non-production environment with the goal to reduce exposing personally identifiable information (PII) to unauthorized people. Data will look different every time you mask it.

## Why Data Masking?

Remove sensitive data from test, development, analytics, and other non-production environments.

Some customers desire non-production environments for activities such as staging and training. In these non-production environments, customers may not want to use actual production data but would still like to use internally consistent data sets. Fusion data masking process is designed to mask specific entities and fields in non-production environments in a way that is designed to protect the original data from being exposed while maintaining production-like views.

## How Does This Impact Customers?

As of April 11th, **Data Masking** became a free feature included in the base subscription for all Fusion SKUs. This exciting change has several implications:

- 1. Cost Savings:** Fusion customers no longer need to pay extra for Data Masking. It's now part of the standard offering.
- 2. Enhanced Security:** By enabling Data Masking, organizations can protect sensitive data during development, testing, and other non-production activities.
- 3. Streamlined Workflows:** Refreshing non-production environments (e.g., copying data from production) becomes simpler and more secure.

<https://blogs.oracle.com/saas/post/oracle-data-masking-for-fusion-applications-environment-management>



A vibrant, stylized illustration of a city skyline. In the foreground, there's a body of water reflecting the sky. Behind it, a dense line of green trees and palm trees separates the water from the city. The city features several tall, modern skyscrapers in shades of blue and grey. Three hot air balloons with colorful, geometric patterns (red, orange, yellow, green, blue) are floating in the sky. The sky is a bright blue with large, white, fluffy clouds. The overall style is flat and colorful, reminiscent of a digital painting or a modern graphic design.

# Security for Implementation vs Day-2 Operations

Sins of the Past Will Haunt You!

# Implementation Phase



- Build security from day one - design foundational security
- Prioritize role creation and OAR configuration
- Limit who has full “God” access for OCI Console:
  - Cloud Account Administrator
  - Identity Domain Administrator
  - Service Administrator

# Day-2 Security Needs



- How will and who will be responsible for ongoing monitoring and updates?
- How will you adapt to organizational changes, mergers, or restructuring
- Have a pre-built project play for flipping security “on” day-2
  - Do not let your implementor off the hook

# Day Two Security Plan



- Implementation accounts
  - Should never be used after the implementation
  - Change password, lock and end-date the implementation roles – breakglass if required
  - After Hypercare, delete if possible
  - Run the User and Role Access Audit Report to for “\_IMPL%” users
- Review and revoke users with:
  - Application Developer
  - Application Administrator
  - Application Implementation Administrator
  - Application Composer
  - Application Implementation Consultant
  - BI Administrator
  - Integration Specialist
  - IT Security Manager
  - Workflow Administration
- Who has BI Admin?





# 25B Is BIG!

Release 25B Changes How Authentication Is Done



# 25B Is Big

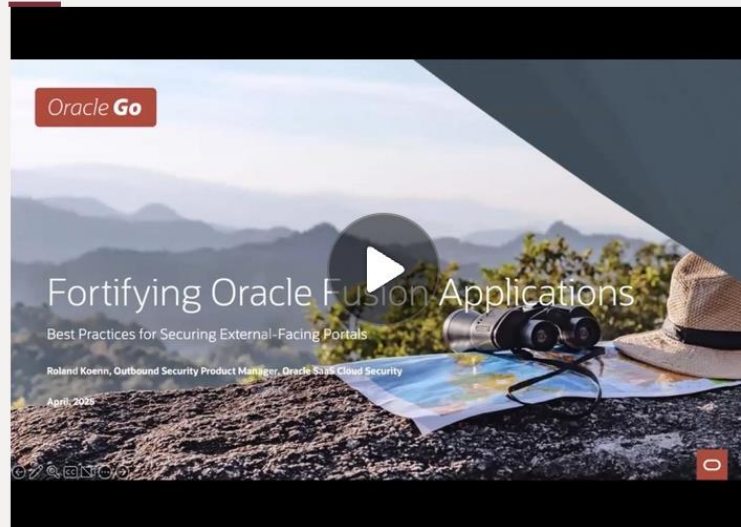


## Roland Koenn

Outbound Security Product Manager,  
Oracle SaaS Cloud Security

- Based in Melbourne, Australia
- Joined Oracle in 2011
- Part of the A-Team for 11 years
- SCS Outbound PM since April 2024

## < Oracle Go – FAQ: Fortifying Oracle Fusion Applications Best Practices for Securing External Facing Portals



### When

Apr 2, 6:00 PM - 7:00 PM

### Organizer

Tamara Fairbanks-Oracle

### About the event

#### Event PDF:

Oracle Go – FAQ Fortifying Oracle Fusion Applications Best Practices for Securing External Facing Portals.pdf  
Uploaded Apr 2, 2025 1.65 MB

#### Description:

[https://community.oracle.com/customerconnect/events/606391-oracle-go-faq-fortifying-oracle-fusion-applications-best-practices-for-securing-external-facing-portals?trk=public\\_post\\_comment-text](https://community.oracle.com/customerconnect/events/606391-oracle-go-faq-fortifying-oracle-fusion-applications-best-practices-for-securing-external-facing-portals?trk=public_post_comment-text)

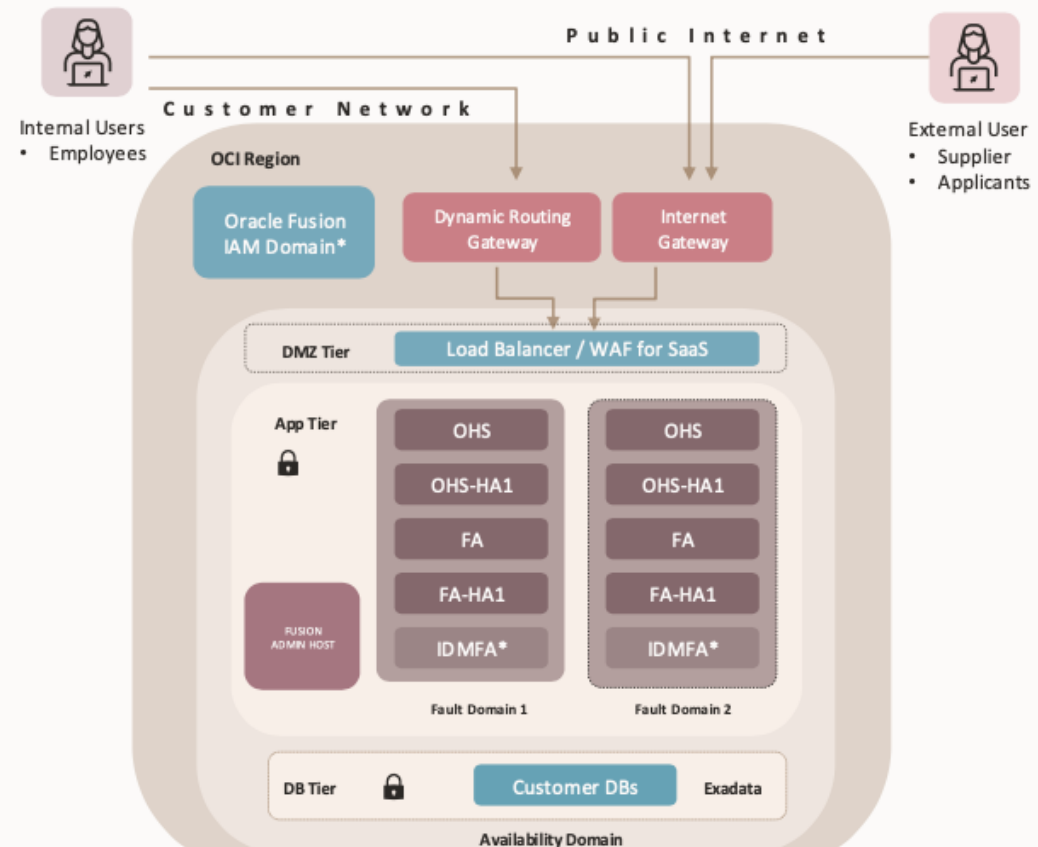
# Oracle Cloud Application Architecture



## Oracle Portal Architecture Overview

### Simplified View

- Oracle Fusion allows secure access for both internal employees and external users such as suppliers and applicants
- Internal users access Fusion through customer networks, e.g. via FastConnect or VPN from known IPs or the public internet
- External users access Fusion portals via the public internet generally from unknown IPs
- Web Application Firewall for SaaS provides IP filtering, traffic inspection and threat protection
- High Availability is ensured across fault domains in the application tier
- Customer data is securely stored in Exadata databases within the database tier



# Identity Services Moving to OCI IAM Domains



## Fusion Identity Upgrade in a Nutshell

### Highlights

#### Key Changes

- Identity services will move to OCI IAM Domains over the coming months
- Built-in support for MFA, included at no extra cost

#### Rollout Timeline

- Begins after the 25B release
- Customers will be notified
  - 90 days in advance (if using Federation)
  - 30 days in advance (if not using Federation)



Some customer with SSO will require action check here for details [here](#).  
Oracle Go Session [here](#).

Sign In  
Oracle Applications Cloud

Company Single Sign-On

or

User ID  
User ID

Password  
Password

Forgot Password

Sign In

Select Language  
English



ORACLE Cloud  
fascpgpintnext

Oracle Cloud Account Sign In

Identity domain fa-cpaabraczy-w2owe

User Name  
User name or email

Password  
Password

Forgot Password?

Sign In

Or sign in with

email-idp

Need help signing in?

English



## Fusion Identity Upgrade in a Nutshell

### Key Enhancements

#### Modern Authentication Features

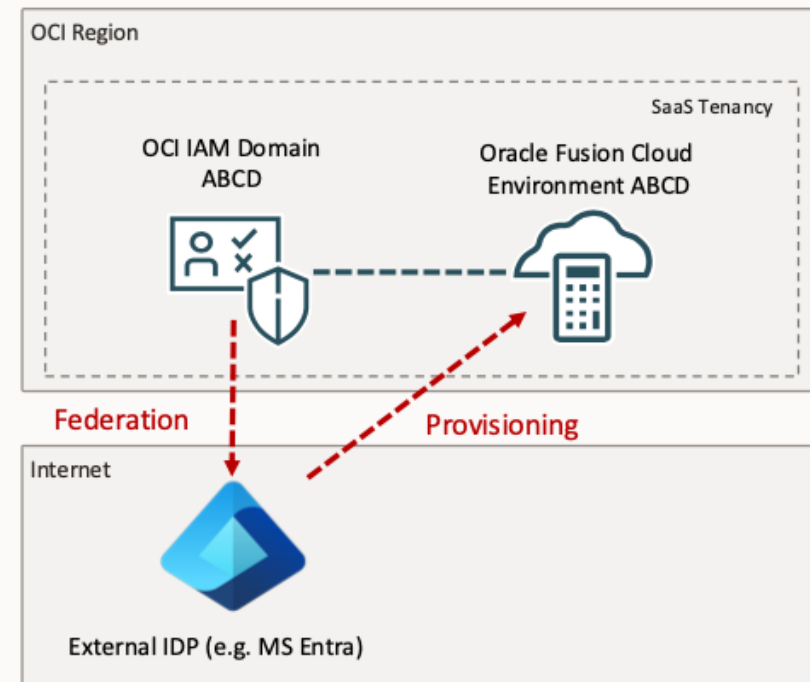
- Enhanced sign-on and IDP policy support
- End users will see a new, modern login page

#### User Experience

- A fully customizable new login experience
- Seamless migration of user attributes, including usernames, email addresses, credentials, and Federated SSO.

#### Architectural Changes

- All Identity Providers (IDPs) are now federated directly with the IAM Domain, rather than with Fusion.
- No more Local Fusion without MFA - these accounts are IAM based.

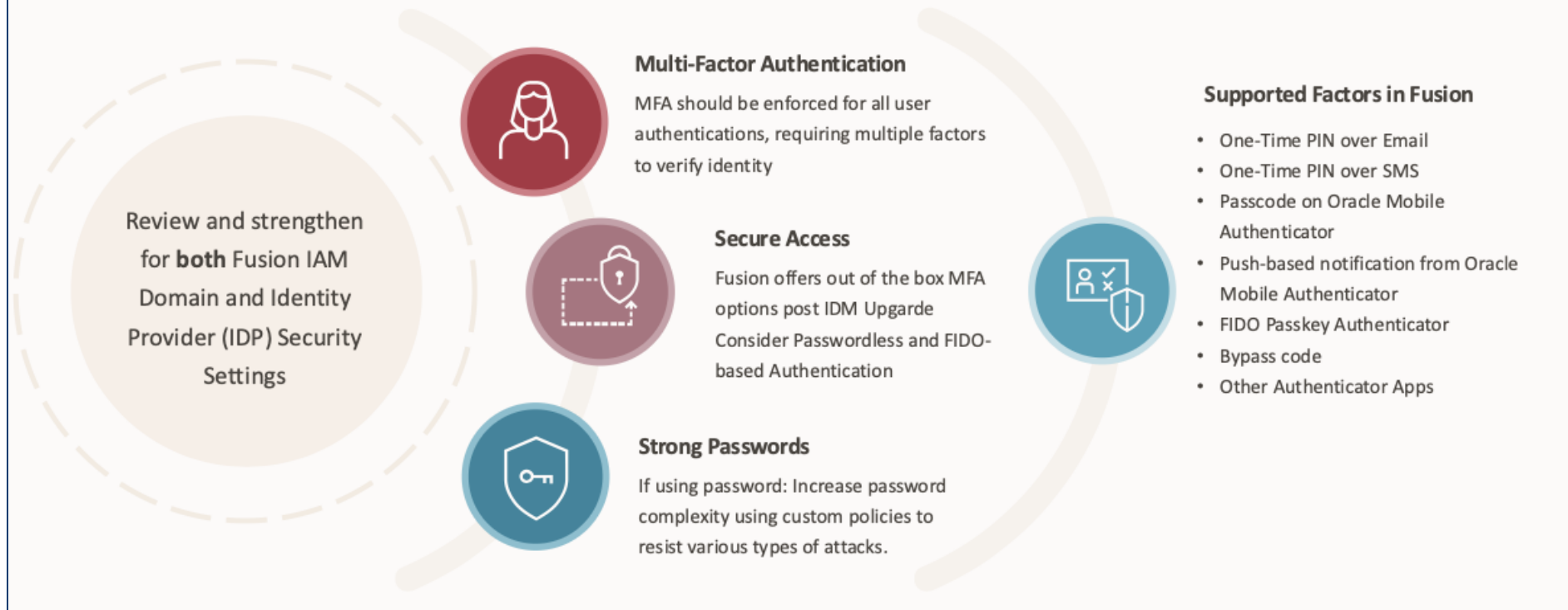


# Multi-Factor Authentication



## Enhancing Security: Multi Factor Authentication

Strengthening Fusion Accounts with MFAs & external Identity Providers



*Recommendation:  
Use your Identity  
provider for MFA  
instead*



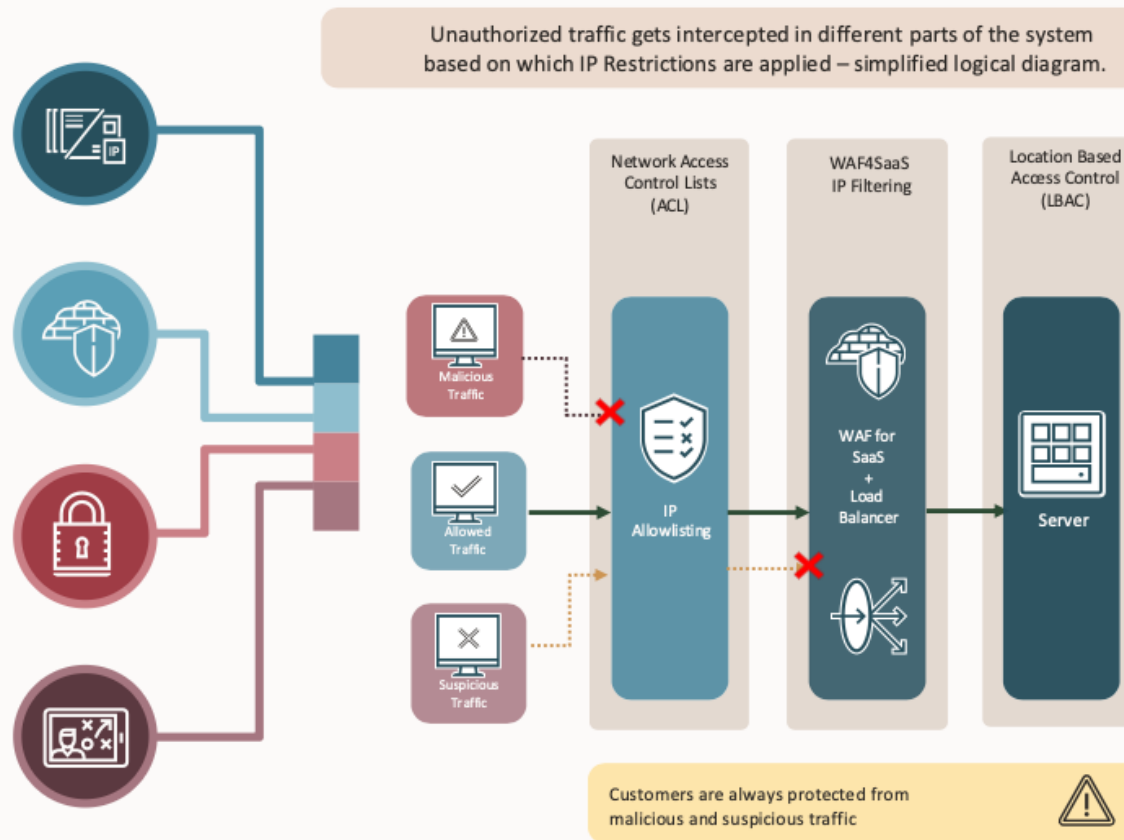
# Filter Who Can Connect



## Enhancing Security: IP Filtering Overview

### The Strategic Role of IP Filtering

- IP Filtering Options**  
Oracle advises using at least one IP Filtering option for enhanced security.
- Maximum Protection**  
WAF for SaaS, LBAC and Network ACLs can be used simultaneously; choose the based on your needs  
ACLs do not support access to Fusion Portals from unknown IPs.
- Built-in Protection**  
Customers are protected from malicious and suspicious traffic even without specific IP Filtering.  
Implements OWASP-Based Policies  
24x7 SOC Monitoring
- Traffic Interception**  
Unauthorized traffic is intercepted at multiple points, depending on the IP Restrictions applied.



# Deploy The Web Application Firewall



## WAF in Action: Controlling Access to Oracle Fusion

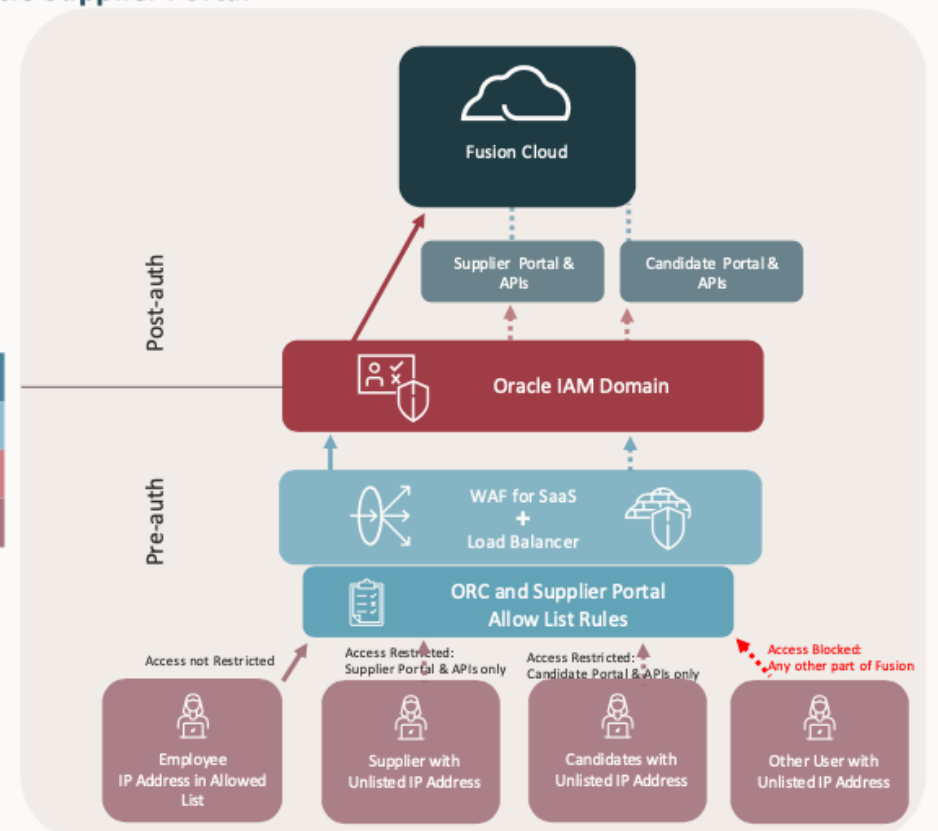
Utilizing WAF for SaaS to protect Oracle Recruitment Cloud and Oracle Supplier Portal

**Approved Access**  
Allowed IPs or employee IP ranges on the Allow List enable full access to all Oracle Fusion Cloud Applications Suite functions.

**Blocked Access**  
Unlisted or blocked IPs are denied access to Oracle Fusion Cloud Applications Suite functions due to WAF policies.

**Supplier Portal Access for Suppliers**  
External applicants with unlisted IPs can only access the Recruitment Portal and APIs.  
**Qualified Target <Oracle Supplier Portal>**

**ORC Applicant Access**  
External applicants with unlisted IPs can only access the Recruitment Portal and APIs.  
**Qualified Target <Oracle Recruitment Cloud Portal>**



# Don't Forget About API (Non-Humans)



## Enhancing Security: Oracle Fusion API Safeguards

### Disable Basic Authentication to Increase Protection

#### IP-Based Access Control

Enforce API access restrictions by allowing only trusted IP addresses, minimizing exposure to unauthorized requests.



#### Disable Basic Authentication for APIs

Basic Authentication for API access should be blocked to enhance protection against common vulnerabilities especially with external portal users in the system.



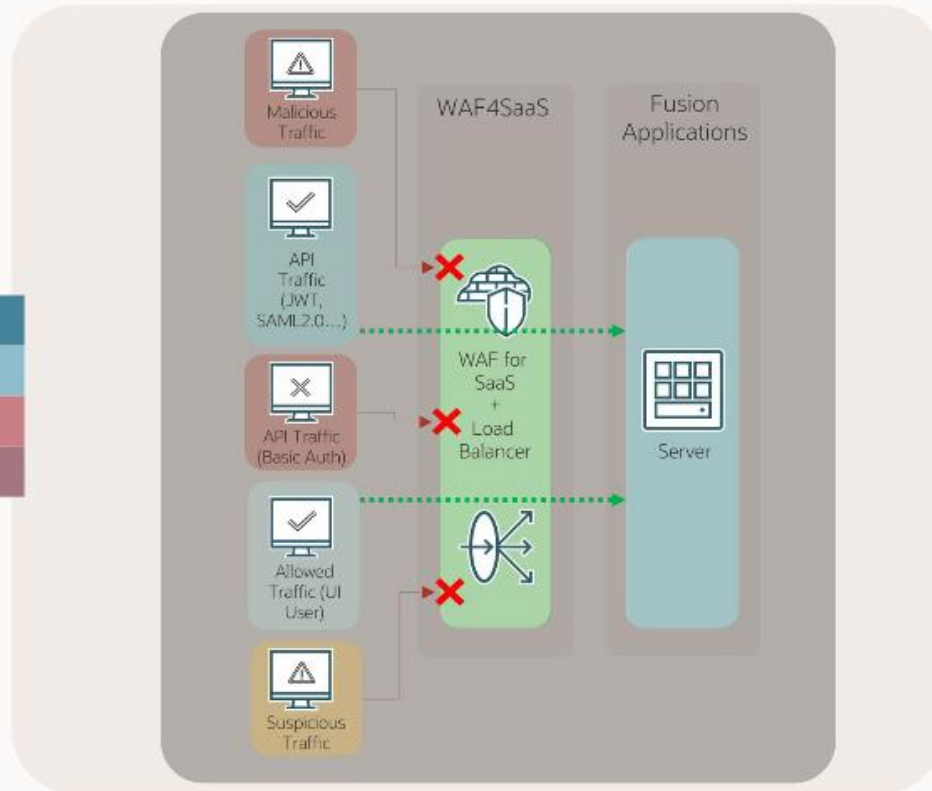
#### Service Request Integration

Easily request the removal of Basic Authentication by raising a Service Request for targeted API security adjustments.



#### Safe Rollout Process

Test the implementation in a staging environment to ensure all systems function properly before deploying in production.







# Lessons Learned

Big and Small Lessons


# Common Challenges

- Role design
  - Is hard, testing is harder
  - Over-permissioning due to poorly designed custom roles
- Lack of alignment between security policies and business processes
- Oracle is not infallible

# Lots of Details: Use A Tool: ConfigSnapshot for Fusion



- Automatically created setup documentation Create setup baseline
- ICompare operating units
- Report on changes to configurations



## ConfigSnapshot

The most **comprehensive & flexible** configuration management software available for the E-Business Suite

Generate setup documentation including BR108 style in just minutes

Identify & analyse customisations  
Identify the impact of upgrades & patching

Compare settings across environments, entities & even versions (11.5.3 to current release)

Review / monitor user access including segregation of duties conflicts

Identify changes over time via point to point baselines or full audit change tracking

Migrate setup across environments / entities: Extract -> Transform -> Load -> Compare

Document

Comply

Track

Baseline

Full Audit

Analyse

Compare

Migrate

**Seeded data is clearly highlighted to make it distinct from data set up for the implementation**

Field Name	Value
From	WACOR TYPE
From/To/From Name	WACOR TYPE
Organization	Oracle Purchasing
Department	WACOR TYPE
Account Level	WACOR TYPE
Security Group	WACOR TYPE

**Receiving Options**

Field Name	VSI11510	R12
Receipt Date		
Receipt Date Early	5	5
Receipt Date Late	5	5
Receipt Date Action	Warning	Warning
Over Receipt Control		
Tolerance	5	5
Over Receipt Action	Warning	Warning
Miscellaneous		
Allow Substituted Receipts	Yes	Yes
Allow Unordered Receipts	Yes	Yes
Allow Express Transactions	Yes	Yes
Allow Cascade Transactions	Yes	Yes
Allow Blind Receiving	No	No
Validate Serial Numbers on RMA Receipts	Yes	No
Receipt Routing	Direct Delivery	Direct Delivery
Enforce Ship-To	Warning	Warning
RMA Receipt Routing	Warning	Warning
Validate Lots on RMA Receipts	Direct Delivery	Direct Delivery
Receipt Number Options		
Receipt Number Generation	Automatic	Automatic
Receipt Number Type	Numeric	Numeric
Next Receipt Number	9999	9999
Accounting		
Receiving Inventory Account	01-000-1410-0000-000	01-000-1410-0000-000
Retrospective Price Adjustment Account	01-000-1230-0000-000	01-000-1230-0000-000
Clearing Account	01-000-1410-0000-000	01-000-1410-0000-000

**Differences clearly highlighted**

<https://www.configsnapshot.com/>



# Lessons Learned (Often)



## Large Clients

- Complexity in managing multiple roles and OARs
- Importance of automation for efficiency.

## Smaller Clients

- Need for simplicity in role design
- Value of leveraging seeded roles to save time



# Key Takeaways and Questions To Ask

Design corrections are much LESS expensive

# Key Takeaways



## Functional

1. Get Roles Right:
  - Understand the differences between seeded, custom, abstract, job, and duty roles.
  - Don't be afraid of custom roles done right!
2. Protect sensitive data during testing
  - Scramble if you can
  - Get your users accustomed to scrambled data
3. Have a Day-Two security plan drafted BEFORE go-live
  - Test with day-two security enabled
  - End-date/delete the implementation roles
  - Revoke "God" Access
4. Be leery of who has BI Admin Role
5. Use ConfigSnapshot

## Technical

- Use MFA in our IDP
- Enable LBAC day one
- Restrict network access as tight as possible (WAF, LBAC, IAM Network Perimeter)
- Use WAF for SaaS Portal exceptions to reduce your attack surface
- Enable auditing on day one of implementation

# Questions to Ask Before Implementation

1. What are our organization's security requirements?
  - Auditing? Logging? SSO? MFA?
  - Are there any compliance or regulatory concerns?
2. How many custom roles do we need, and why?
3. What is our plan for testing and data protection?
  - Test real transactions with real roles
4. What will be included in the day-2 security project plan?
  - How will we ensure roles are not overprovisioned



# Thank You For Attending!

Please complete the session survey  
in the conference app.



# Q&A

Mike Miller

[Michael.Miller@syntax.com](mailto:Michael.Miller@syntax.com)

