INTEGRIGY

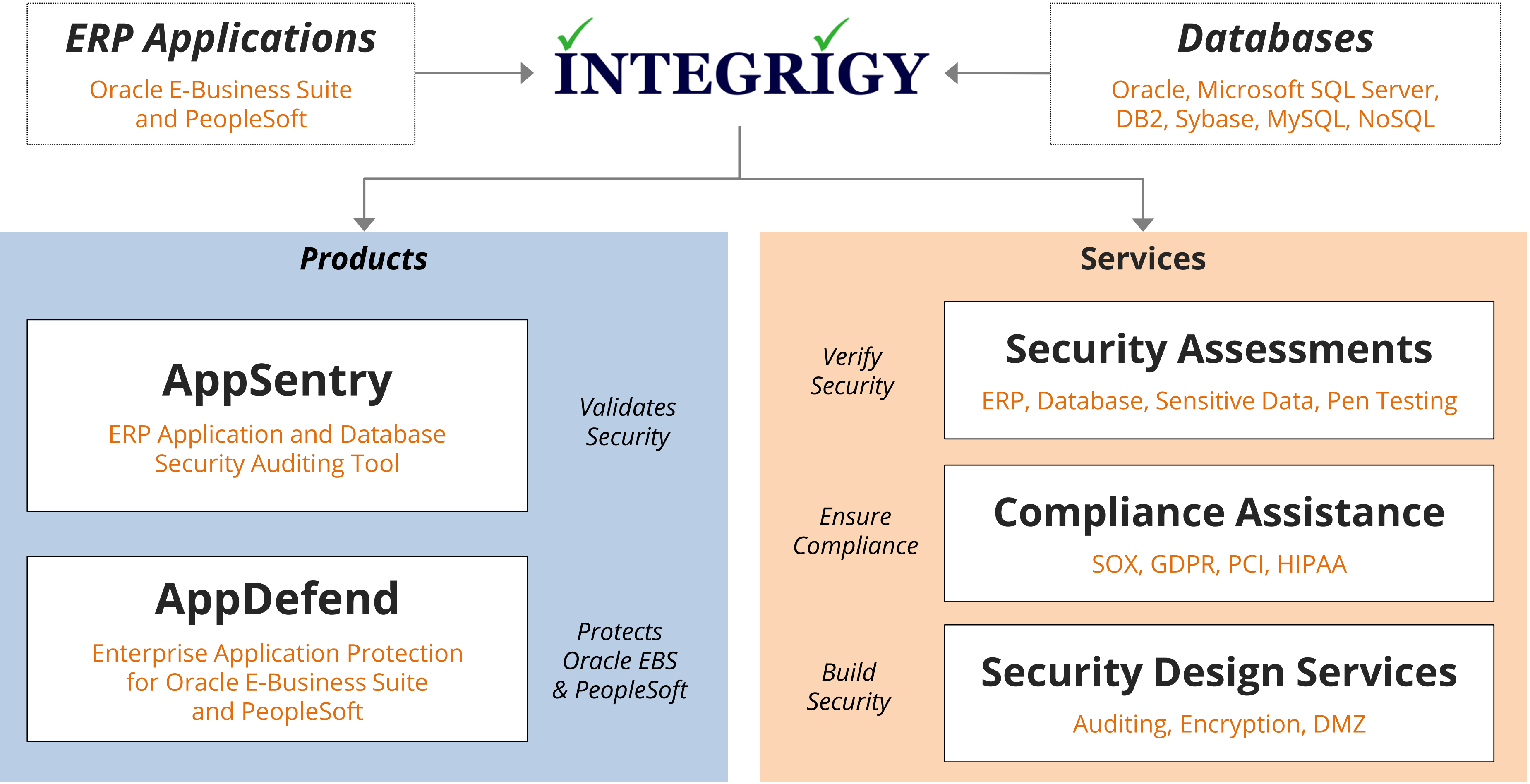
SSO and MFA for Oracle E-Business Suite without the Complexity

March 16, 2022

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications

Oracle E-Business Suite and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server, DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database Security Auditing Tool

Validates Security

AppDefend

Enterprise Application Protection for Oracle E-Business Suite and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, GDPR, PCI, HIPAA

Build Security

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

Definitions

Single Sign-On (SSO)

A session and user authentication scheme that allows a user to use one set of login credentials, such as username and password, to access multiple applications and often does not require re-entering of those credentials when access a new application.

Multi-Factor Authentication (MFA)

Access control method in which a user is only granted access after successfully presenting two or more pieces of information or data (factors) to an authentication mechanism

Two-Factor Authentication (2FA)

2FA is a subset of MFA where only two factors are required such as a password and a hardware token

Factors

Pieces of information or data such as –

- Knowledge = something you know like a password
- Possession = something you have like a hardware token or device
- Inherence = something you are like a biometric such as a fingerprint

SSO Benefits for Oracle E-Business Suite

- **Increase Employee and IT productivity**
  - Improve user experience by eliminating logins and multiple passwords
  - Better application usability and employee satisfaction
- **Reduce IT costs**
  - Fewer support calls for password resets and authentication issues
- **Improve security**
  - Reduce risk of password theft due to password fatigue
  - Enhance password strength with fewer passwords
- **Improve compliance**
  - Single point of user termination across all applications
  - Implement additional account controls like risk-based authentication

Oracle EBS SSO Solutions

Oracle Access Manager/ Oracle Internet Directory	▪ Oracle SSO solution for Oracle EBS ▪ Requires Oracle Internet Directory or Oracle Unified Directory ▪ MFA using Oracle Mobile Authenticator, SMS, email, …
Oracle Identity Cloud Service	▪ Cloud-based authentication, SSO, and MFA solution ▪ Integrates with Oracle EBS using EBS Asserter
Okta	▪ Cloud-based authentication, SSO, and MFA solution
SSOgen	▪ Integration solution between Oracle EBS and other identity management such as Active Directory, Azure AD, Siteminder, OpenID, …
miniOrange	▪ Integration solution between Oracle EBS and other identity management such as Active Directory, Azure AD, Siteminder, OpenID, …
Integrigy AppDefend	▪ SSO native integration solution that authentications Oracle EBS with an external identity provider like Active Directory of Azure AD

SSO and Oracle E-Business Suite

- SSO is not supported natively by Oracle EBS
- SSO requires implementation of an identity management solution
- Uses Oracle EBS Access Gate to integration to identity management
- Redirects from EBS login page to identity management login page

MFA Benefits

- **Prevent fraud and phishing attacks**
  - Two or more methods of identity verification makes account take-over harder
- **Improve security**
  - Enable strong authentication
  - Reduce risk of compromised passwords
- **Improve compliance**
  - PCI-DSS requires MFA required for access in some situations
  - GDPR, HIPAA, and other standards require strong authentication
- **Contextualize authentication**
  - MFA can be when specific data is accessed or actions performed like employee self-service direct deposit changes

Popular Multi-Factor Authentication Solutions

Duo Security	▪ Mobile app, hardware token, U2F, biometrics, SMS, phone call, …
RSA SecurID	▪ Hardware and software tokens
Okta Adaptive MFA	▪ Mobile app, hardware token, U2F, biometrics, SMS, phone call, …
Symantec VIP	▪ Mobile app, hardware token, U2F
Ping Identity MFA	▪ Mobile app, hardware token, U2F, biometrics, …
Microsoft Authenticator	▪ Mobile-based with Azure AD integration
Google Authenticator	▪ Mobile-based and application-level

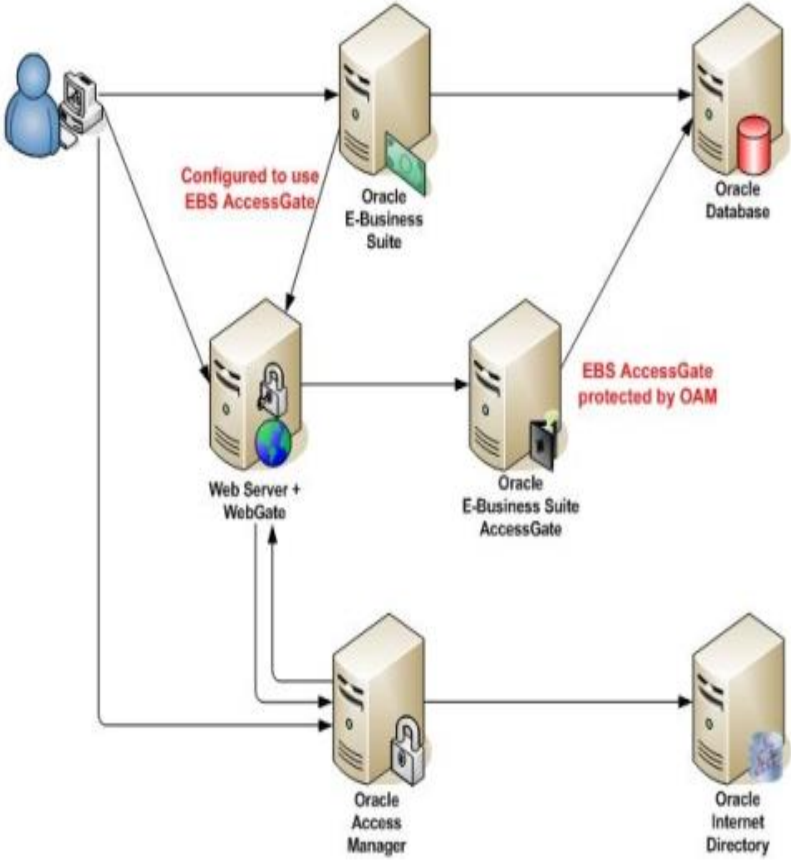
Oracle E-Business Suite and Two-Factor Authentication

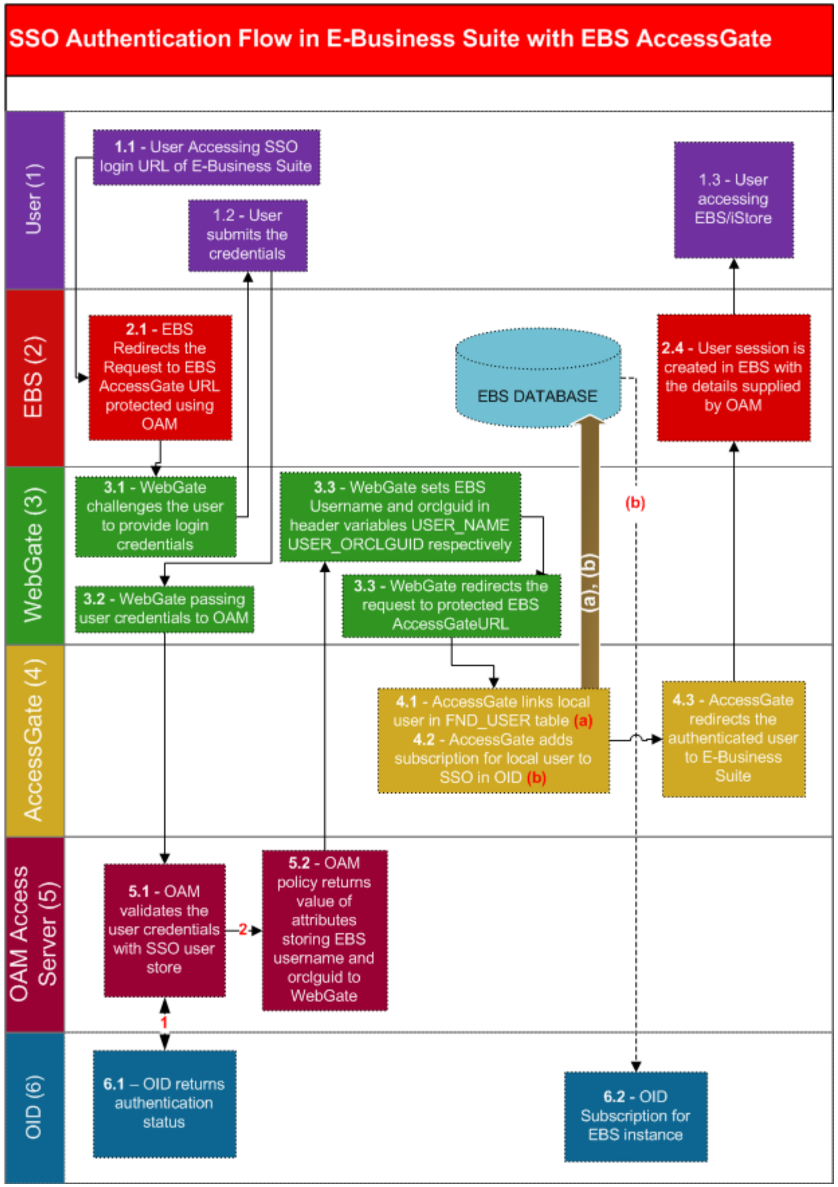
- 2FA is not supported natively by Oracle EBS
- 2FA requires implementation of an identity management solution
- Uses Oracle EBS Access Gate to integration to identity management
- Redirects from EBS login page to identity management login page
- 2FA is only when logging into Oracle EBS

Oracle EBS 2FA Solutions

Oracle Access Manager	▪ Oracle SSO solution for Oracle EBS ▪ Requires Oracle Internet Directory or Oracle Unified Directory ▪ MFA using Oracle Mobile Authenticator, SMS, email, …
Oracle Identity Cloud Service	▪ Cloud-based authentication, SSO, and MFA solution ▪ Integrates with Oracle EBS using EBS Asserter
Okta	▪ Cloud-based authentication, SSO, and MFA solution
SSOgen	▪ Integration solution between Oracle EBS and other identity management such as Active Directory, Azure AD, Siteminder, OpenID, …
Integrigy AppDefend	▪ 2FA integration solution that protects Oracle EBS including users, responsibilities, functions, and pages

Oracle Access Manager for Oracle EBS


Oracle E-Business Suite
Oracle Database
Configured to use EBS AccessGate
Web Server + WebGate
Oracle E-Business Suite AccessGate
EBS AccessGate protected by OAM
Oracle Access Manager
Oracle Internet Directory



SSO Authentication Flow in E-Business Suite with EBS AccessGate

User (1)

1.1 - User Accessing SSO login URL of E-Business Suite

1.2 - User submits the credentials

1.3 - User accessing EBS/iStore

EBS (2)

2.1 - EBS Redirects the Request to EBS AccessGate URL protected using OAM

EBS DATABASE

2.4 - User session is created in EBS with the details supplied by OAM

WebGate (3)

3.1 - WebGate challenges the user to provide login credentials

3.2 - WebGate passing user credentials to OAM

3.3 - WebGate sets EBS Username and orclguid in header variables USER_NAME USER_ORCLGUID respectively

3.3 - WebGate redirects the request to protected EBS AccessGateURL

AccessGate (4)

4.1 - AccessGate links local user in FND_USER table (a)
4.2 - AccessGate adds subscription for local user to SSO in OID (b)

(a), (b)

(b)

4.3 - AccessGate redirects the authenticated user to E-Business Suite

OAM Access Server (5)

5.1 - OAM validates the user credentials with SSO user store

2

5.2 - OAM policy returns value of attributes storing EBS username and orclguid to WebGate

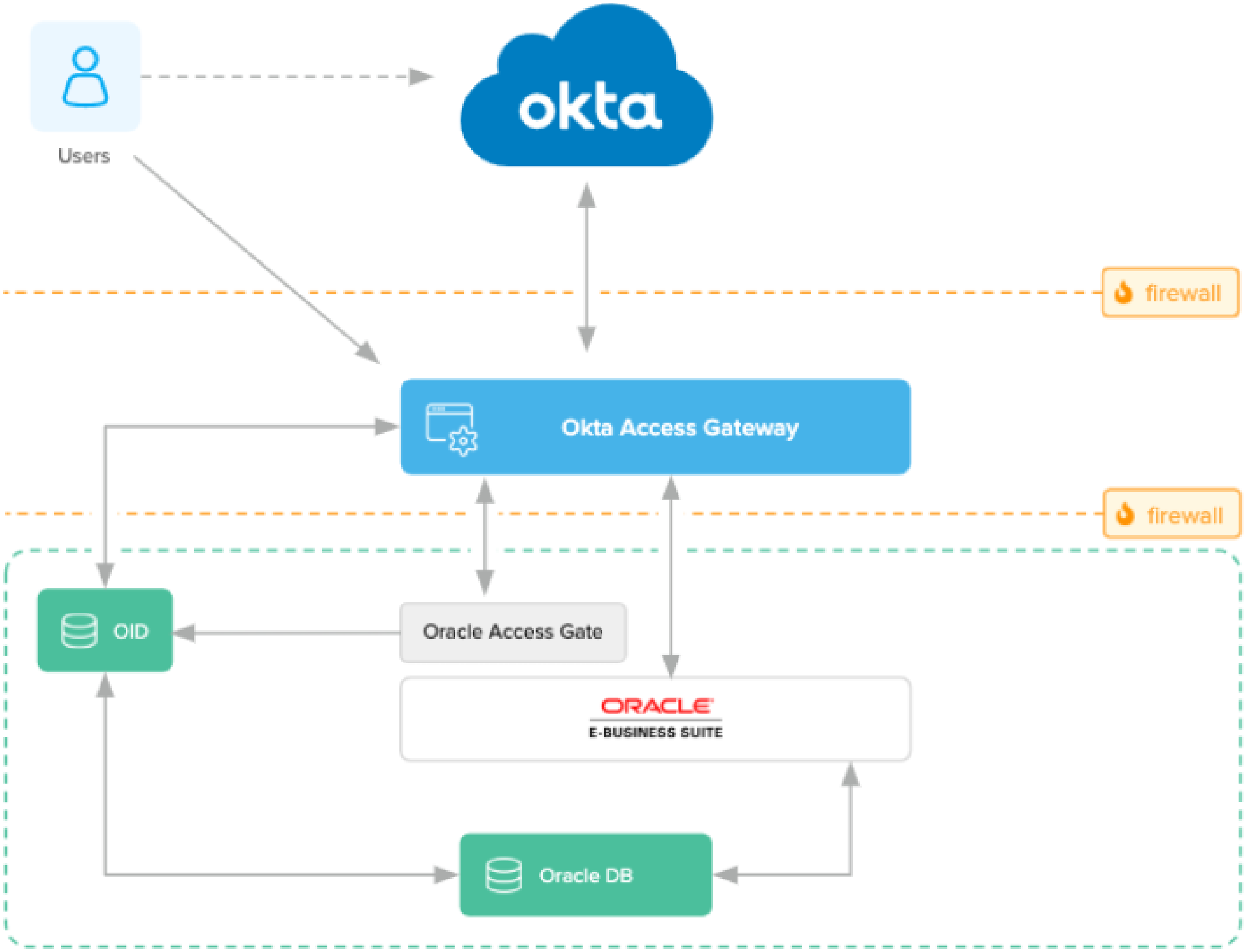
1

OID (6)

6.1 – OID returns authentication status

6.2 - OID Subscription for EBS instance

Okta for Oracle EBS



Integrigy AppDefend

AppDefend is an **enterprise application firewall** designed and optimized for the Oracle E-Business Suite.

Prevents Web Attacks

Detects and reacts to SQL Injection, XSS, and known Oracle EBS vulnerabilities

Application Logging

Enhanced application logging for compliance requirements like SOX, GDPR, PCI-DSS 10.2

SSO and two-factor (2FA/MFA)

Enables SSO and two-factor authentication for login, user, responsibility, or function

Limits EBS Modules

More flexibility and capabilities than URL firewall to identify EBS modules

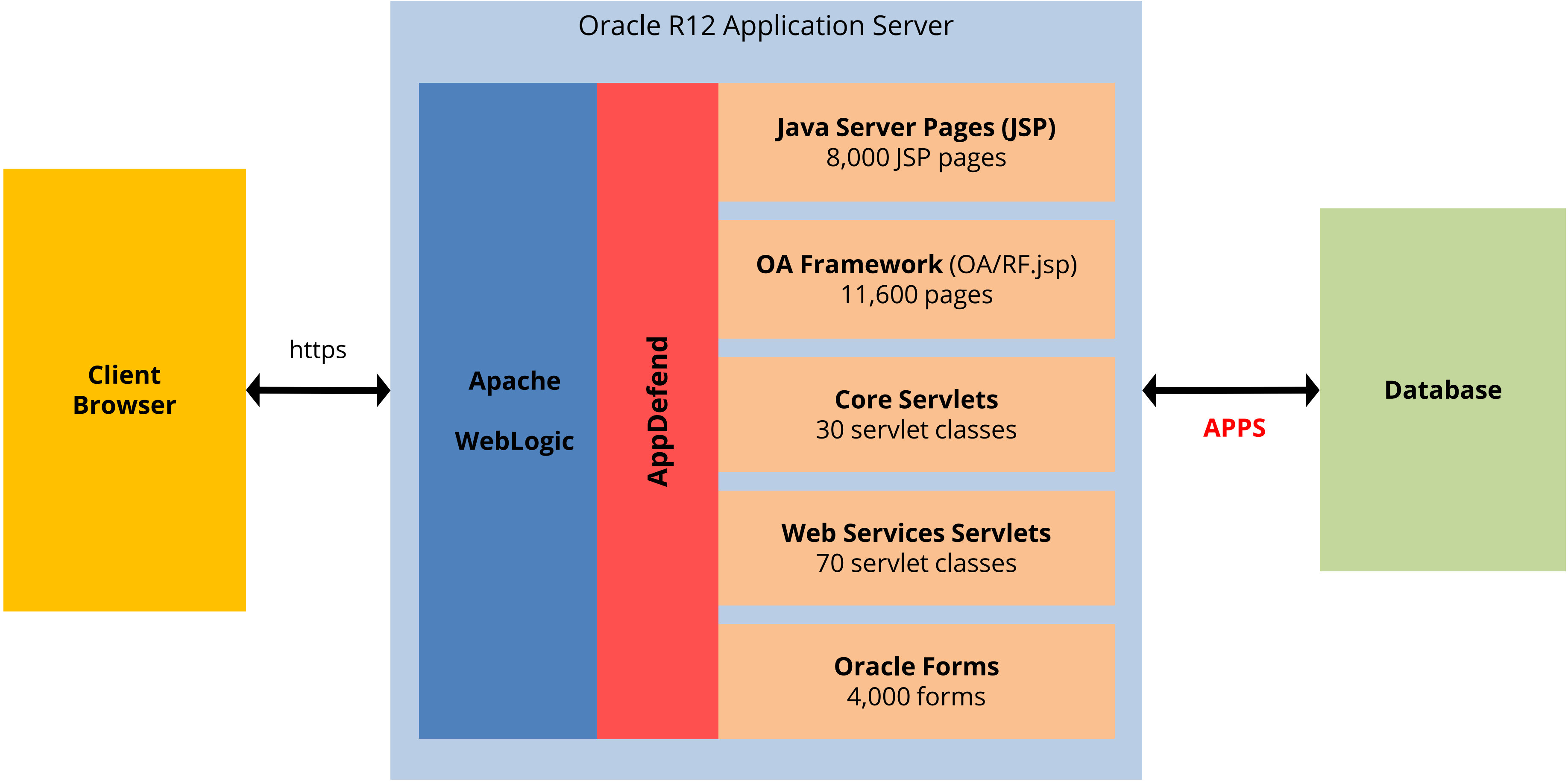
Protects Web Services

Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST)

Protects Mobile Applications

Detects and reacts to attacks against Oracle EBS mobile applications

AppDefend and Oracle EBS 12.2



AppDefend runs within the WebLogic Java containers as a servlet filter and monitors all incoming requests and out-going responses. Being in the Java container, AppDefend can access all session state, attributes, error messages, and the database.

AppDefend SSO Feature (SAML)

- **AppDefend adds single sign-on (SSO) for Oracle E-Business Suite**
  - SAML 2.0 support for Oracle EBS as a service provider (SP)
  - No additional hardware or servers
  - No additional identity management software

- **Direct integration with SAML 2.0 Identity Providers (IdP)**
  - Supports all SAML 2.0 IdPs such as –

    Active Directory Federation Services (ADFS)

    Azure AD (Microsoft Azure Active Directory)

    Okta

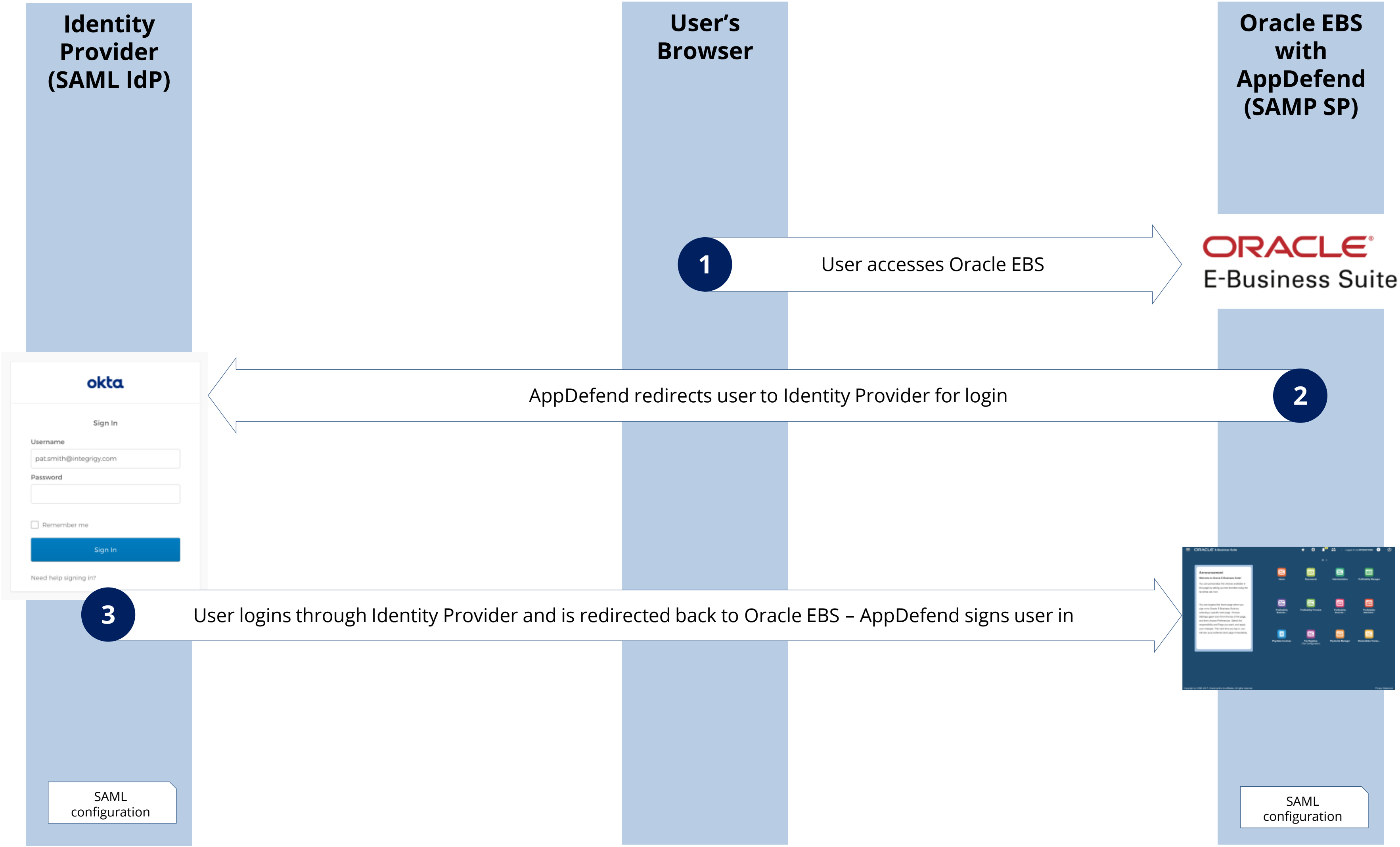
    OneLogin

    Ping Identity

- **Multiple Modes**
  - Oracle E-Business Suite SSO Provider (system profile options)
  - AppDefend servlet filter
  - Direct SSO to Oracle E-Business Suite
  - WebADI and EBS mobile applications are fully supported

- **Secure Implementation**
  - Oracle EBS Session cookie set to “host” rather than “domain”

AppDefend SSO SAML Flow – High-level



Identity Provider (SAML IdP)

User's Browser

Oracle EBS with AppDefend (SAMP SP)

1 User accesses Oracle EBS

2 AppDefend redirects user to Identity Provider for login

3 User logins through Identity Provider and is redirected back to Oracle EBS – AppDefend signs user in

okta

Sign In

Username

pat.smith@integrigy.com

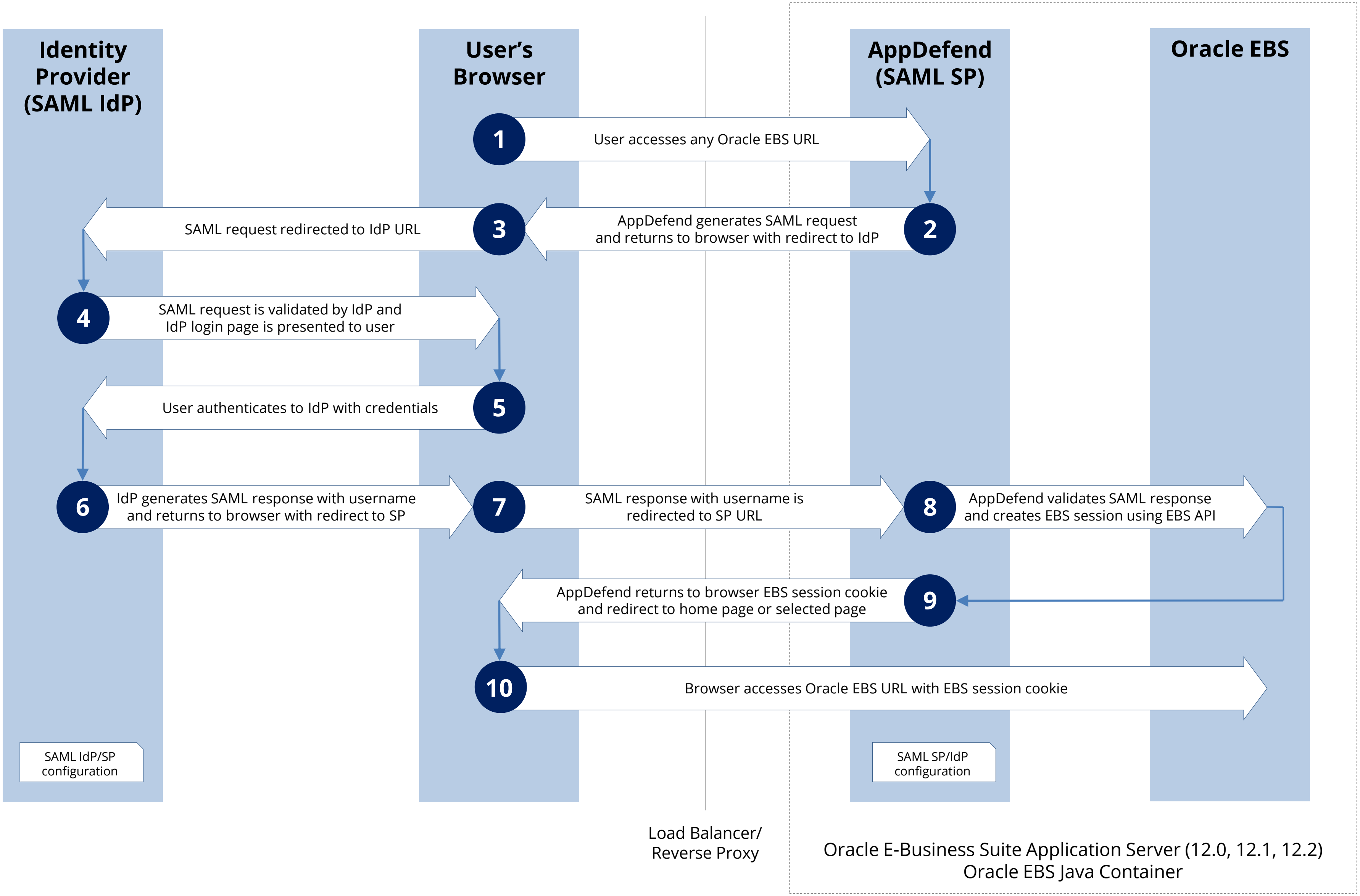
Password

□ Remember me

Sign In

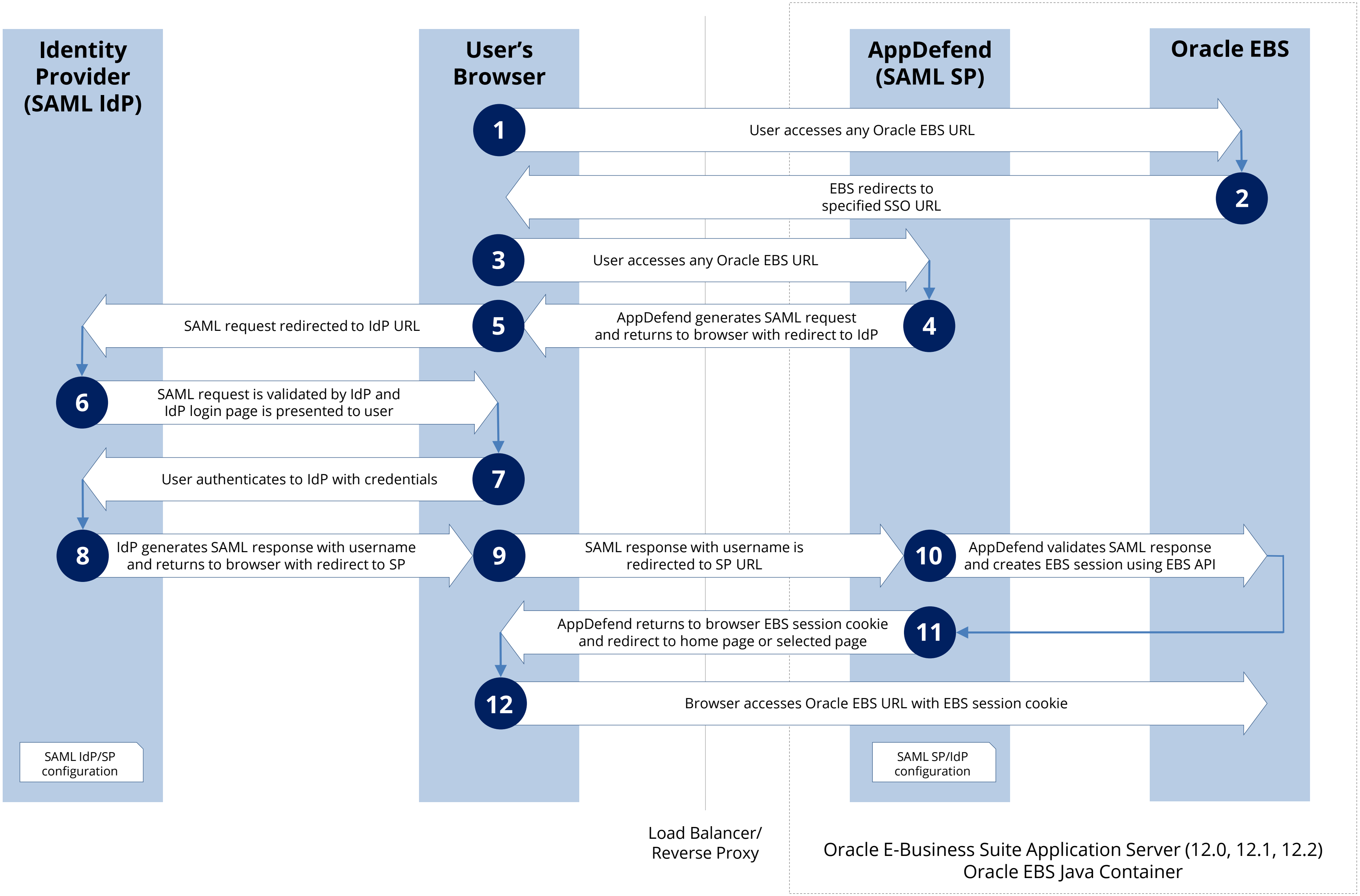
Need help signing in?

AppDefend SSO SAML Flow



Identity Provider (SAML IdP)
User's Browser
AppDefend (SAML SP)
Oracle EBS
1
User accesses any Oracle EBS URL
2
AppDefend generates SAML request and returns to browser with redirect to IdP
3
SAML request redirected to IdP URL
4
SAML request is validated by IdP and IdP login page is presented to user
5
User authenticates to IdP with credentials
6
IdP generates SAML response with username and returns to browser with redirect to SP
7
SAML response with username is redirected to SP URL
8
AppDefend validates SAML response and creates EBS session using EBS API
9
AppDefend returns to browser EBS session cookie and redirect to home page or selected page
10
Browser accesses Oracle EBS URL with EBS session cookie
SAML IdP/SP configuration
SAML SP/IdP configuration
Load Balancer/ Reverse Proxy
Oracle E-Business Suite Application Server (12.0, 12.1, 12.2)
Oracle EBS Java Container

AppDefend SSO SAML Flow (EBS SSO Configuration)



Identity Provider (SAML IdP)

User's Browser

AppDefend (SAML SP)

Oracle EBS

1 User accesses any Oracle EBS URL

2 EBS redirects to specified SSO URL

3 User accesses any Oracle EBS URL

4 AppDefend generates SAML request and returns to browser with redirect to IdP

5 SAML request redirected to IdP URL

6 SAML request is validated by IdP and IdP login page is presented to user

7 User authenticates to IdP with credentials

8 IdP generates SAML response with username and returns to browser with redirect to SP

9 SAML response with username is redirected to SP URL

10 AppDefend validates SAML response and creates EBS session using EBS API

11 AppDefend returns to browser EBS session cookie and redirect to home page or selected page

12 Browser accesses Oracle EBS URL with EBS session cookie

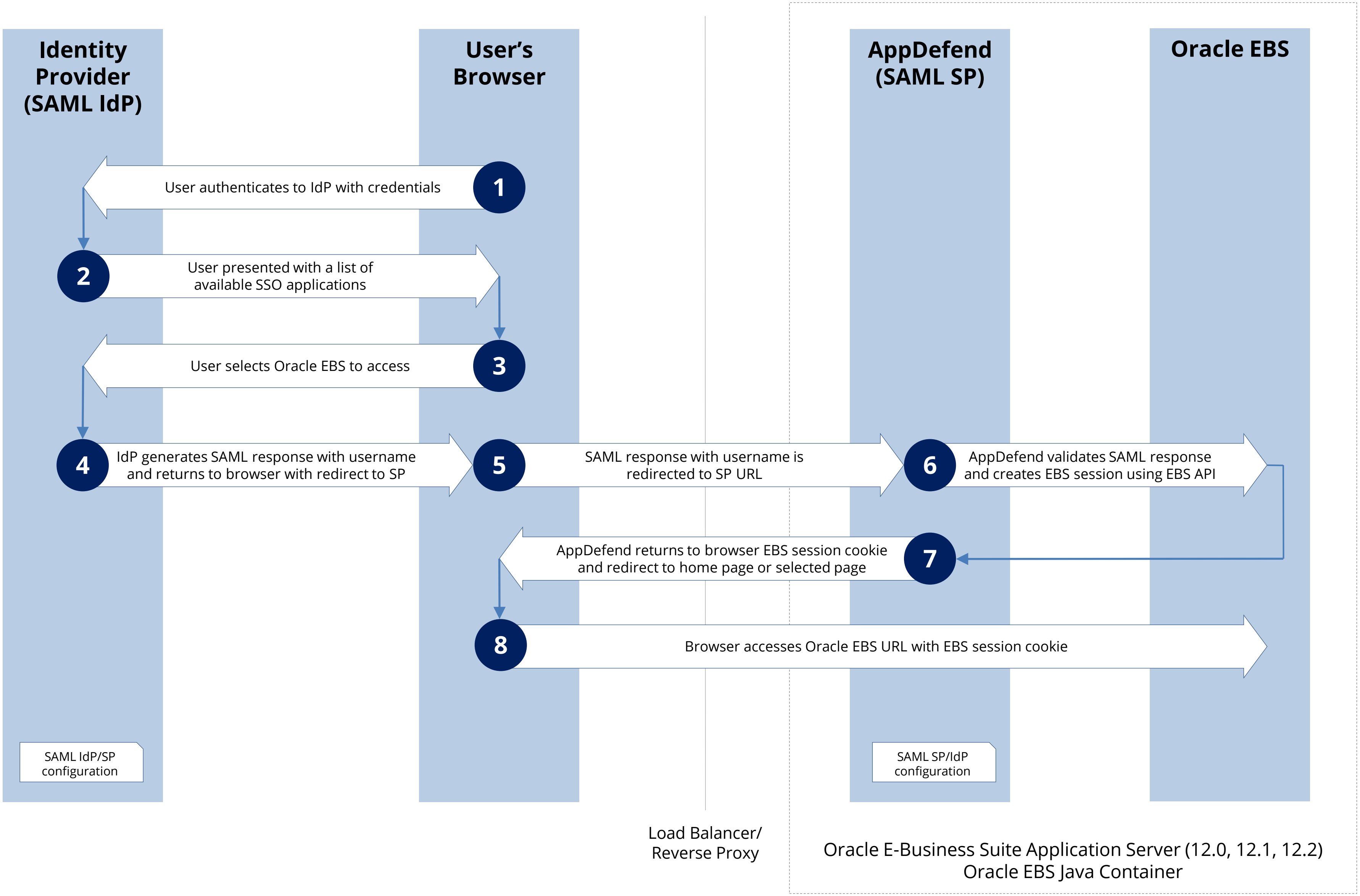
SAML IdP/SP configuration

SAML SP/IdP configuration

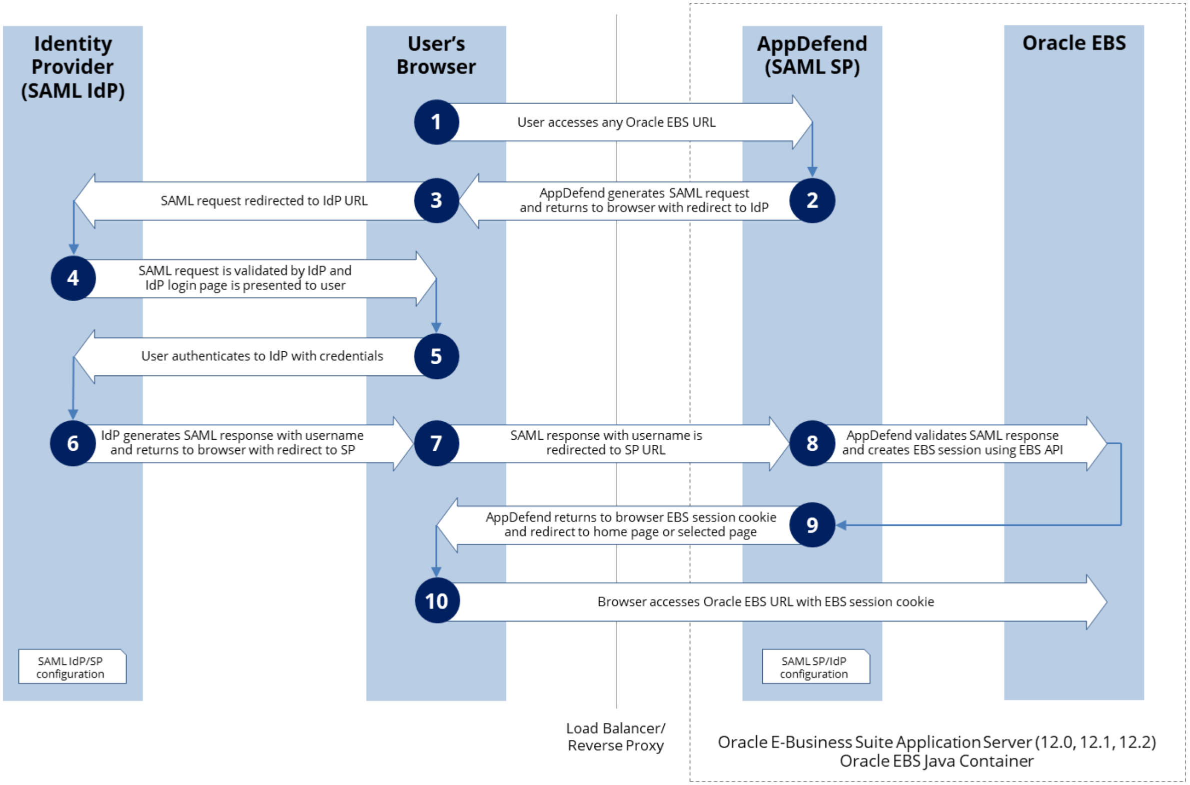
Load Balancer/
Reverse Proxy

Oracle E-Business Suite Application Server (12.0, 12.1, 12.2)
Oracle EBS Java Container

AppDefend SSO SAML Flow (SSO Homepage)


Identity Provider (SAML IdP)
User's Browser
AppDefend (SAML SP)
Oracle EBS
1 User authenticates to IdP with credentials
2 User presented with a list of available SSO applications
3 User selects Oracle EBS to access
4 IdP generates SAML response with username and returns to browser with redirect to SP
5 SAML response with username is redirected to SP URL
6 AppDefend validates SAML response and creates EBS session using EBS API
7 AppDefend returns to browser EBS session cookie and redirect to home page or selected page
8 Browser accesses Oracle EBS URL with EBS session cookie
SAML IdP/SP configuration
SAML SP/IdP configuration
Load Balancer/ Reverse Proxy
Oracle E-Business Suite Application Server (12.0, 12.1, 12.2)
Oracle EBS Java Container

AppDefend SSO SAML Security



Identity Provider (SAML IdP)

User's Browser

AppDefend (SAML SP)

Oracle EBS

1 User accesses any Oracle EBS URL

2 AppDefend generates SAML request and returns to browser with redirect to IdP

3 SAML request redirected to IdP URL

4 SAML request is validated by IdP and IdP login page is presented to user

5 User authenticates to IdP with credentials

6 IdP generates SAML response with username and returns to browser with redirect to SP

7 SAML response with username is redirected to SP URL

8 AppDefend validates SAML response and creates EBS session using EBS API

9 AppDefend returns to browser EBS session cookie and redirect to home page or selected page

10 Browser accesses Oracle EBS URL with EBS session cookie

SAML IdP/SP configuration

SAML SP/IdP configuration

Load Balancer/ Reverse Proxy

Oracle E-Business Suite Application Server (12.0, 12.1, 12.2)
Oracle EBS Java Container

1

- AppDefend protects access to all Oracle EBS URLs
- Must be authenticated to access any URLs except specific pages such as iStore or iSupplier registration

2

- SAML request is signed (SHA-512 if supported by IdP) and encrypted (AES-256) using IdP public key
- SAML request should be communicated using TLS 1.2 or 1.3 based on your configuration

6

- SAML response is signed (SHA-512 if supported by IdP) and encrypted (AES-256) using AppDefend public key

8

- AppDefend validates the integrity of the SAML response by decrypting using the AppDefend private key and verifying the signature against the IdP public key
- AppDefend prevents XML entity and schema attacks and by blocking entity tags and whitelisting schemas
- SAML replay attacks are prevented with a distributed accepted assertion caching, narrow expiration window, matching SAML request id for request and response as well as to JSESSIONID, and blocking already accepted assertions

9

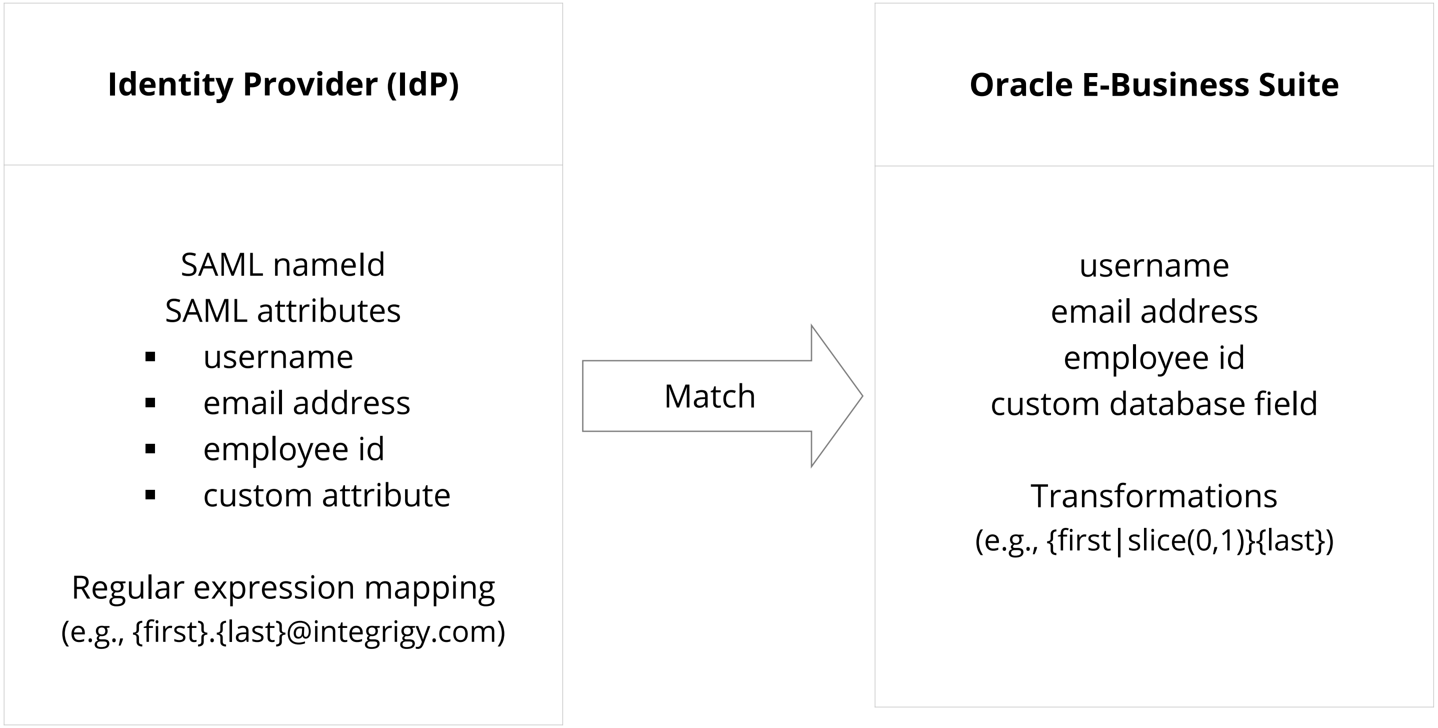
- AppDefend sets the Oracle EBS session cookie scope to **host** to prevent session hijacking
- All other Oracle EBS SSO solutions require session cookie scope to be set to **domain** which allows for potential session hijacking attacks

10

- AppDefend can maintain a mapping of EBS session cookies to IP address in order to prevent session hijacking attacks

AppDefend SSO SAML User Mapping

AppDefend can map Identity Provider user to Oracle E-Business Suite user using different attributes or values from both the Identity Provider and Oracle E-Business Suite. Multiple match rules can be defined and evaluated per login.



Identity Provider (IdP)

SAML nameId
SAML attributes

- username
- email address
- employee id
- custom attribute

Regular expression mapping
(e.g., {first}.{last}@integrigy.com)

Match

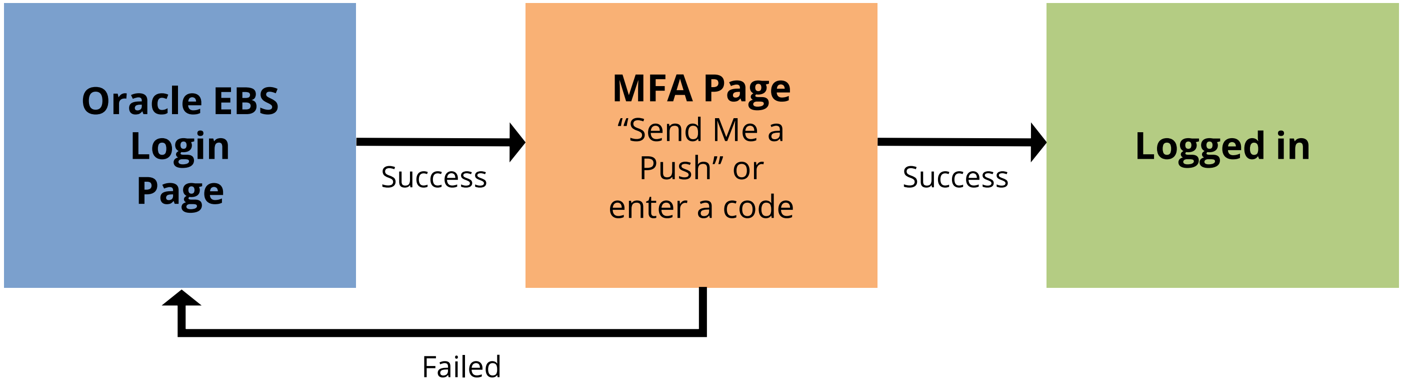
Oracle E-Business Suite

username
email address
employee id
custom database field

Transformations
(e.g., {first|slice(0,1)}{last})

AppDefend Contextual Multi-Factor Authentication

AppDefend enables contextual multi-factor authentication (MFA/2FA) for Oracle EBS using DUO Security, TOTP, SMS, or PKI (smartcards).



- **Multi-Factor Authentication**
  Enhances Oracle EBS login security by integrating with 2FA to provide secondary authentication
- **Per Page, Responsibility, Function**
  Require 2FA when user selects or accesses specific pages, responsibilities, or functions through menus or directly

AppDefend Two-Factor Authentication

- **Application-aware**
  - 2FA for login, user, responsibility, function, or page
  - Multiple 2FA authentications can be configured for different use cases and controls
- **Context-aware**
  - 2FA may be triggered based on session context such as time, location, device, etc.
- **Single 2FA request per application session**
  - 2FA authentications only when required
- **Enhanced logging and audit trail for all authentications**
- **Supports local EBS authentication or single-signon**
- **No additional hardware or single point of failure**
- **Support for WebADI, Configurator, Mobile Apps, etc.**

Two-Factor Authentication Use Cases

- Entire Application
  - Require 2FA when logging into Oracle EBS
  - Different 2FA can be used for internal vs suppliers as an example
- Privileged Responsibilities
  - Require 2FA when user accesses specific responsibilities like **System Administrator**
  - Protect highly privileged responsibilities from malicious use
- Privileged Users
  - Require 2FA when highly privileged users like **SYSADMIN** login
  - Preventative control for privileged, generic users accounts for SOX compliance
  - Limit access to generic user accounts by 2FA devices
  - Audit trail of named users accessing generic user accounts
- High Risk Functions or Pages
  - Require 2FA when user access specific functions or pages
  - Prevent fraud by requiring 2FA when user accesses self-service HR bank accounts

AppDefend MFA

AppDefend provides contextual **multi-factor authentication** for logins (SSO and non-SSO users, responsibilities, pages, and/or functions. MFA options are Duo Security, TOTP, SMS, and PKI (smartcards).

	Contextual Multi-factor Authentication			
	SSO User Login	**Non-SSO User Login**	**Responsibility**	**Page/Function**
AppDefend MFA (with or without SSO SAML)	✓	✓	✓	✓
AppDefend SSO SAML with IdP MFA	✓			
Legacy Oracle EBS SSO (such as OID/OAM or Oracle IDCS)	✓			

Integrigy Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**