



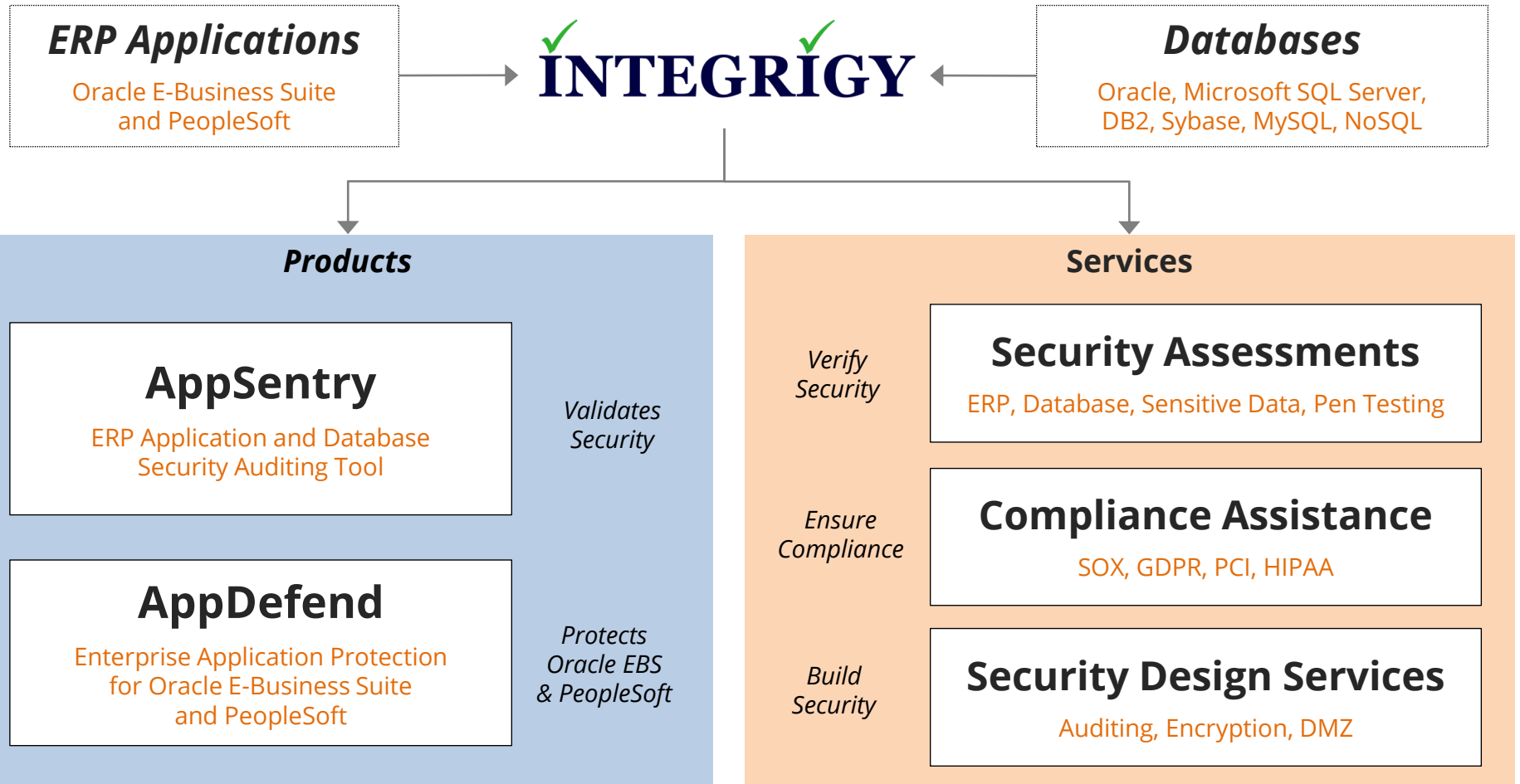
SSO and MFA for Oracle E-Business Suite without the Complexity

February 9, 2023

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Integrigy Research Team

ERP Application and Database Security Research



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 accessing 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 multiple application logins
 - Better application usability and employee satisfaction by reducing password fatigue
- **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
 - Enables enforcement of stronger and more realistic password policies
- **Improve compliance**
 - Single point of user termination across applications
 - Simplify user and password management
 - Implement additional account controls like risk-based authentication

SSO and Oracle E-Business Suite

- SSO is not supported natively by Oracle EBS
- Oracle solution requires implementation of a standalone identity management solution
 - Oracle Internet Directory (OID), Oracle Access Manager (OAM), or Oracle Cloud IDCS
- 3rd party solutions require implementation of a stand-alone identity management solution

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

Two-Factor Authentication and Oracle E-Business Suite

- 2FA is not supported natively by Oracle EBS
- Oracle 2FA solution requires implementation of SSO and an identity management solution
 - Oracle Internet Directory (OID), Oracle Access Manager (OAM), or Oracle Cloud IDCS
- 2FA is only when logging into 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 with hybrid protection using WAF and RASP

Limits EBS Modules

More flexibility and capabilities than URL firewall to identify EBS modules

Protects Mobile Applications

Detects and reacts to attacks against Oracle EBS mobile applications

Protects Web Services

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

SSO and two-factor (2FA/MFA)

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

Application Logging

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

AppDefend Oracle E-Business Suite Support

Oracle E-Business Suite

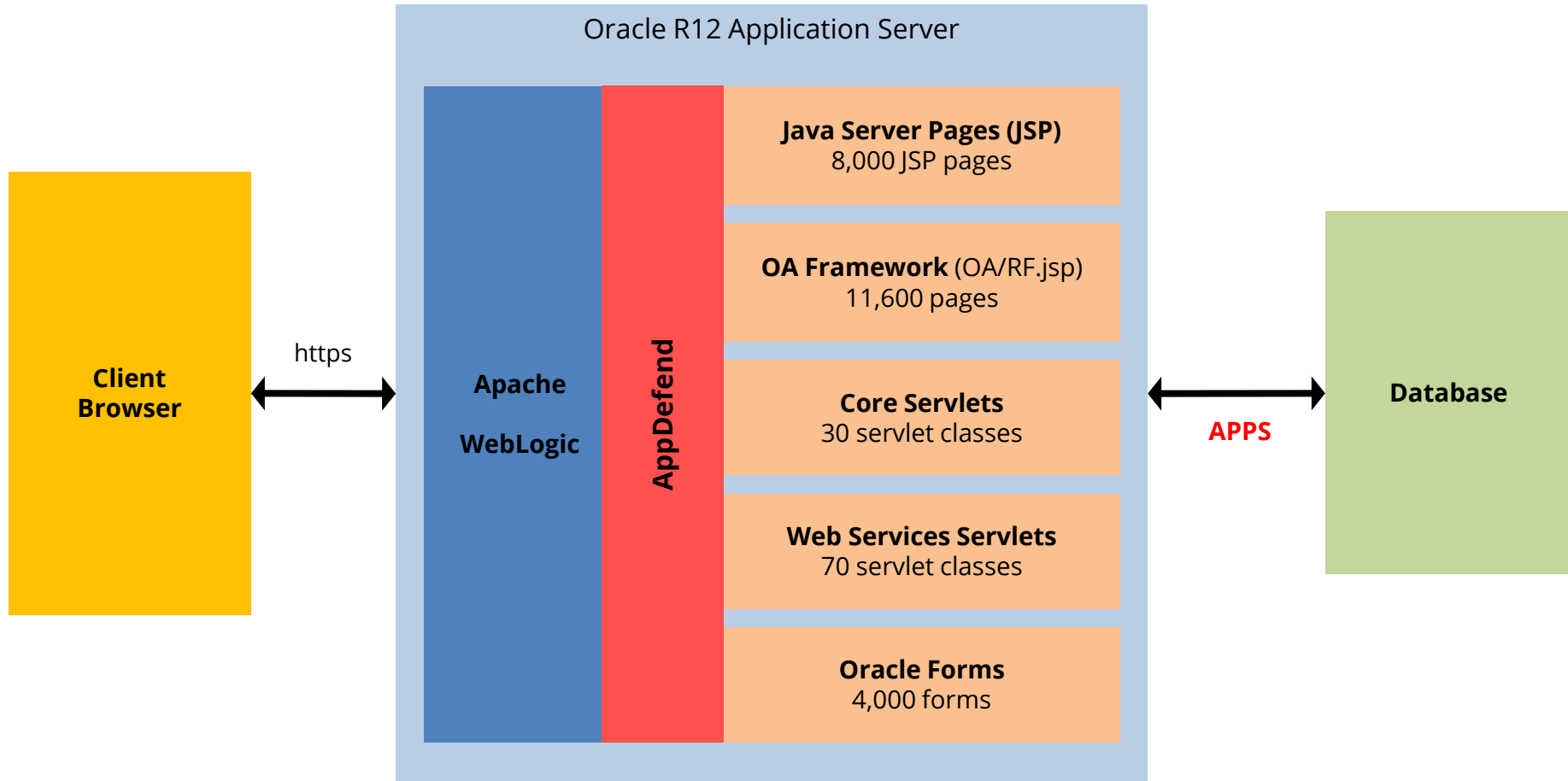
- 12.2.x
- 12.1.x
- 12.0.x

Operating Systems

Supported operating systems

- Linux x86 (Oracle Enterprise Linux, Red Hat Enterprise Linux AS/ES, SuSe)
- Sun SPARC Solaris
- HP PA-RISC HP/UX
- IBM AIX

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.

Oracle E-Business Suite User Populations – SSO and MFA

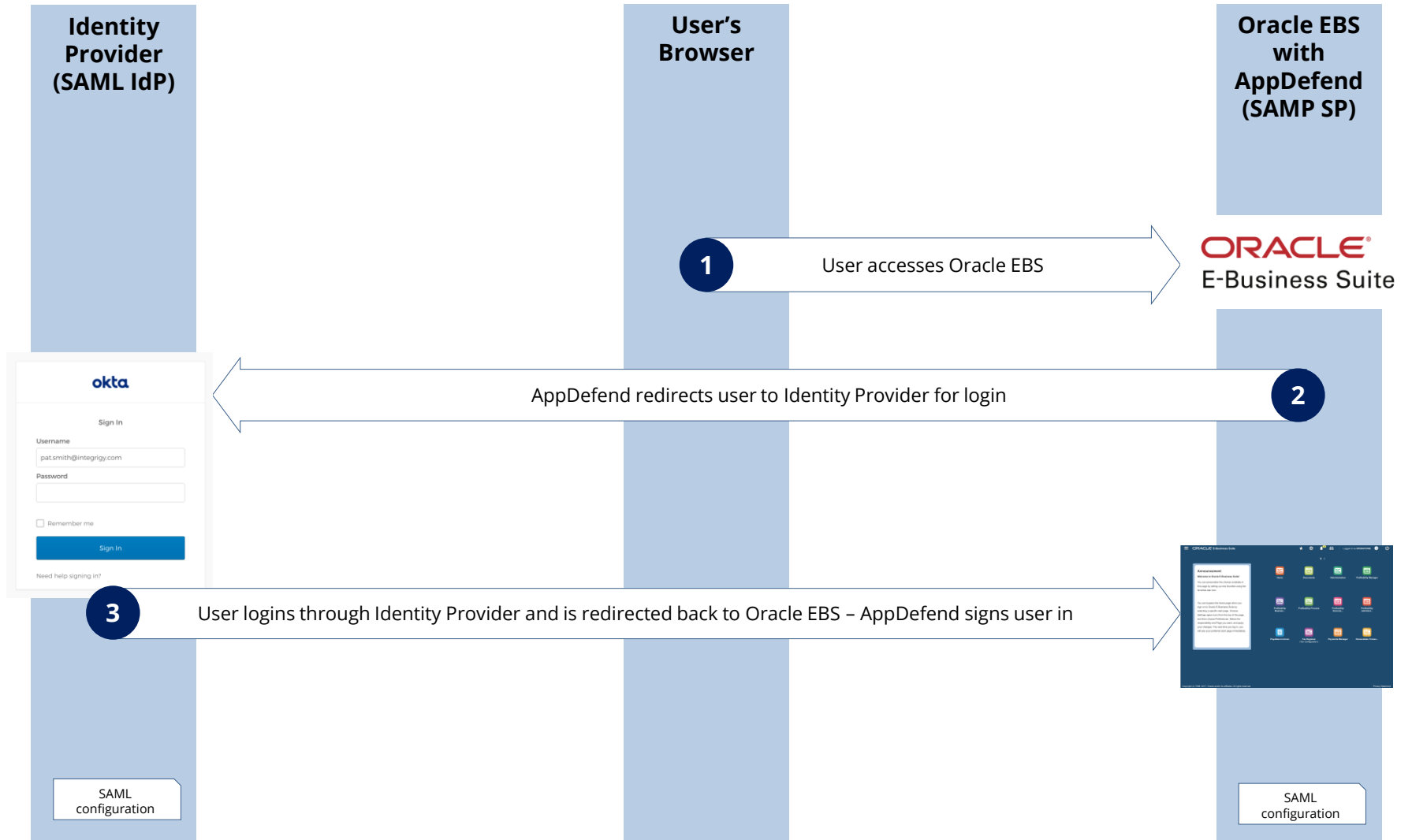
AppDefend SSO and MFA can be tailored to specific Oracle EBS user populations and configured with different SSO and MFA methods for each user population. Mix and match SSO and MFA even multiple SSO solutions for different groups of internal users.

	Typical Options for SSO/Authentication	Typical Options for MFA
Internal Users (SSO and/or MFA)	SAML (AD, Azure AD, Okta, etc.)	(1) with SAML (2) DUO, RSA, RADIUS, PKI, and SmartCard
Generic Internal Users (SYSADMIN, BATCH, JOB, ...)	SAML named user	(1) SAML named user (2) FND_USER named user (3) DUO
External Users – Suppliers (iSupplier)	FND_USER	(1) TOTP (2) SMS (3) Email (4) no MFA
External Users – Candidates/Customers (iRecruitment/iStore)	FND_USER	(1) TOTP (2) SMS (3) Email (4) no MFA

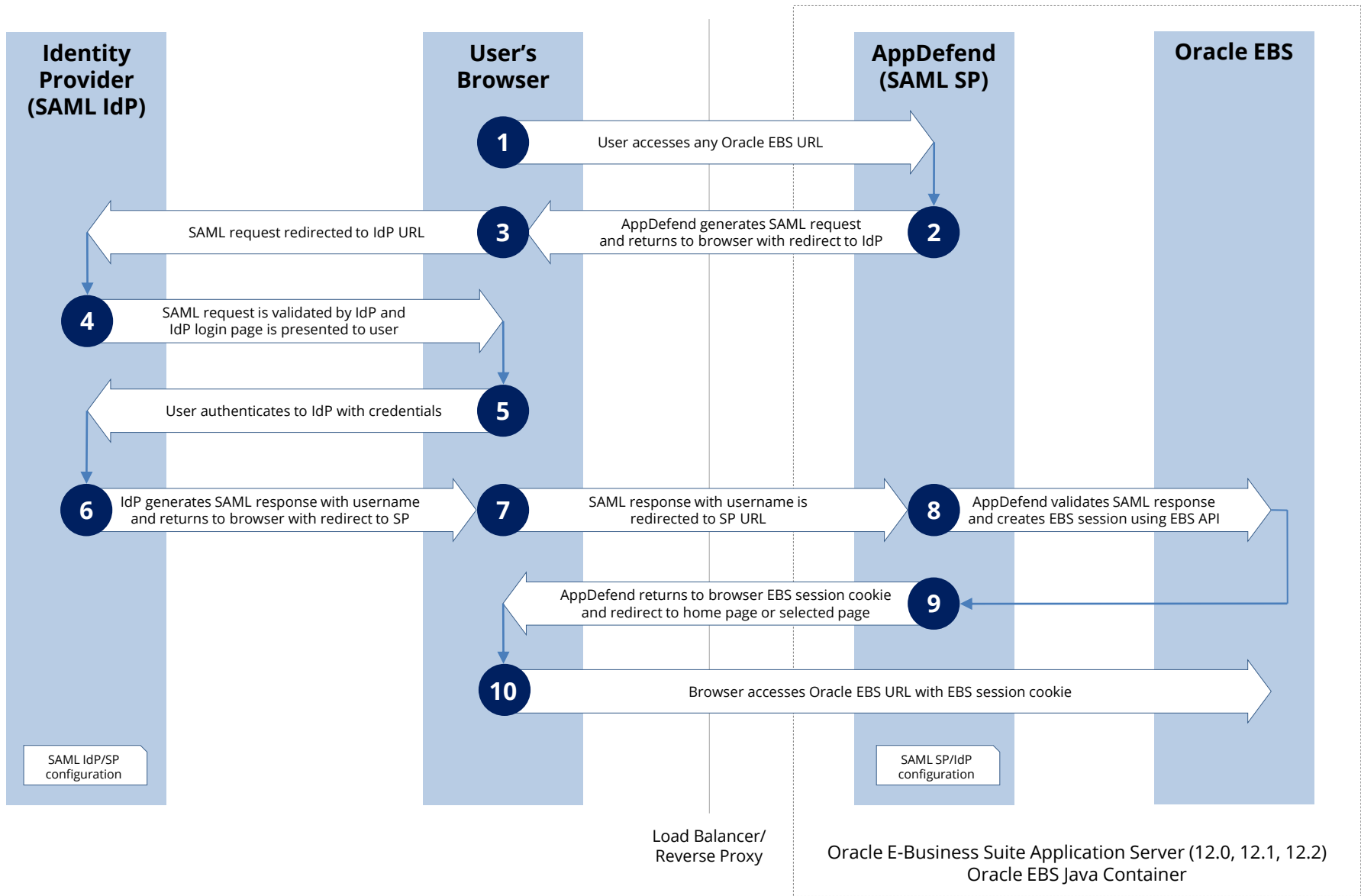
AppDefend SSO Feature (SAML)

- **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 any SAML 2.0 IdP such as –
 - Active Directory On-Premise (ADFS)
 - Azure AD (Microsoft Azure Active Directory)
 - Okta
 - AWS IAM Identity Center
 - 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”

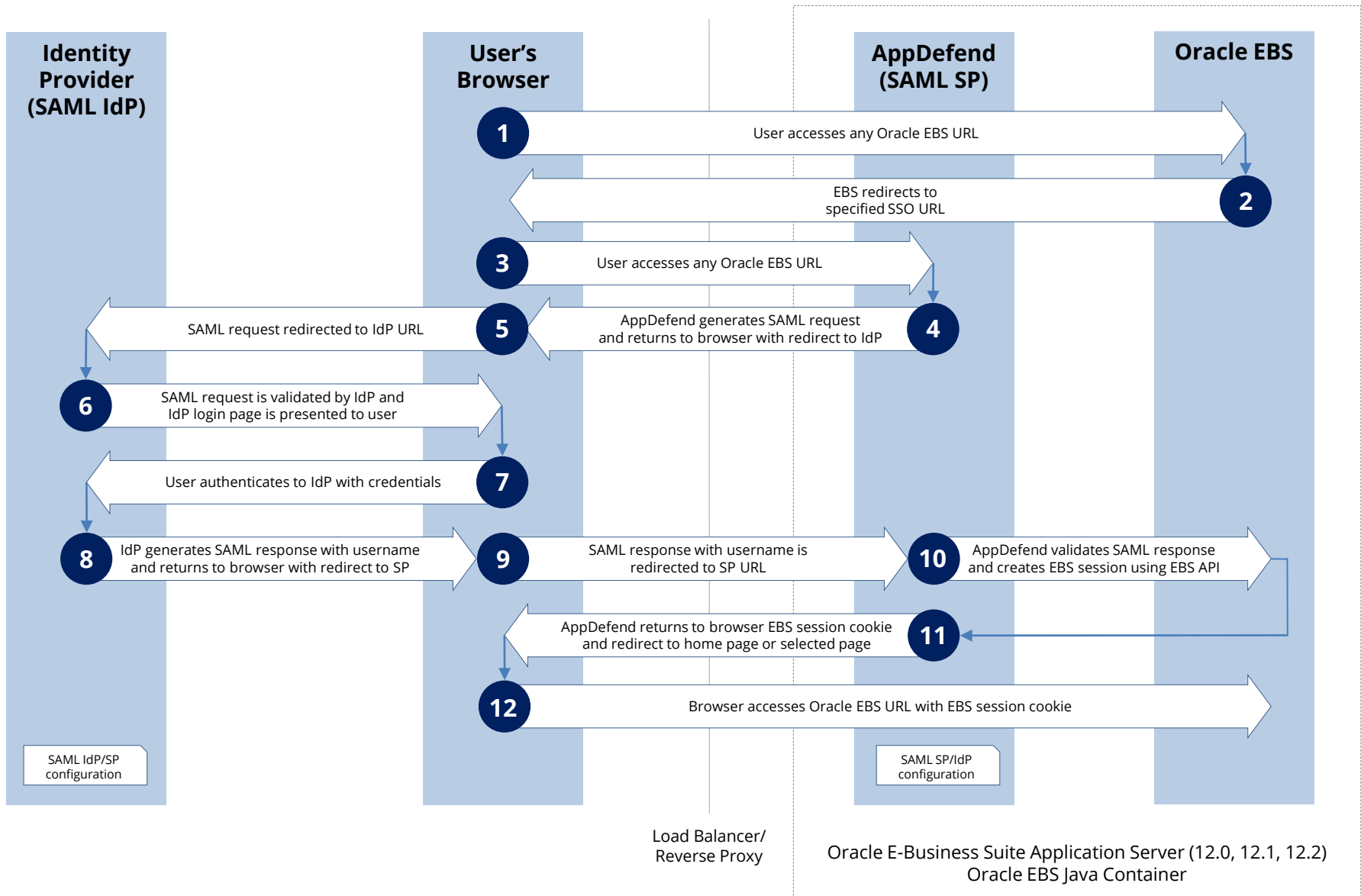
AppDefend SSO SAML Flow – High-level



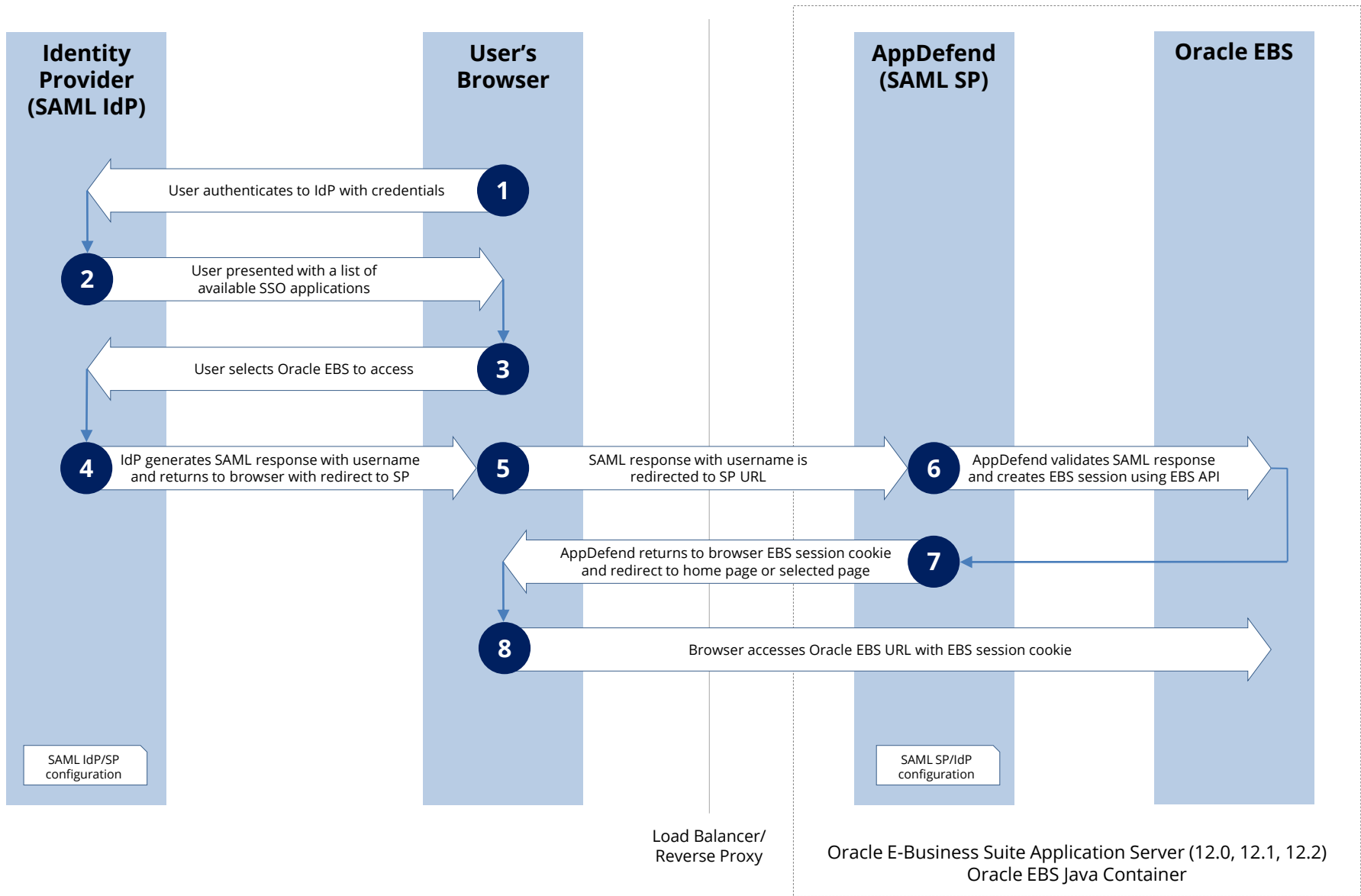
AppDefend SSO SAML Flow



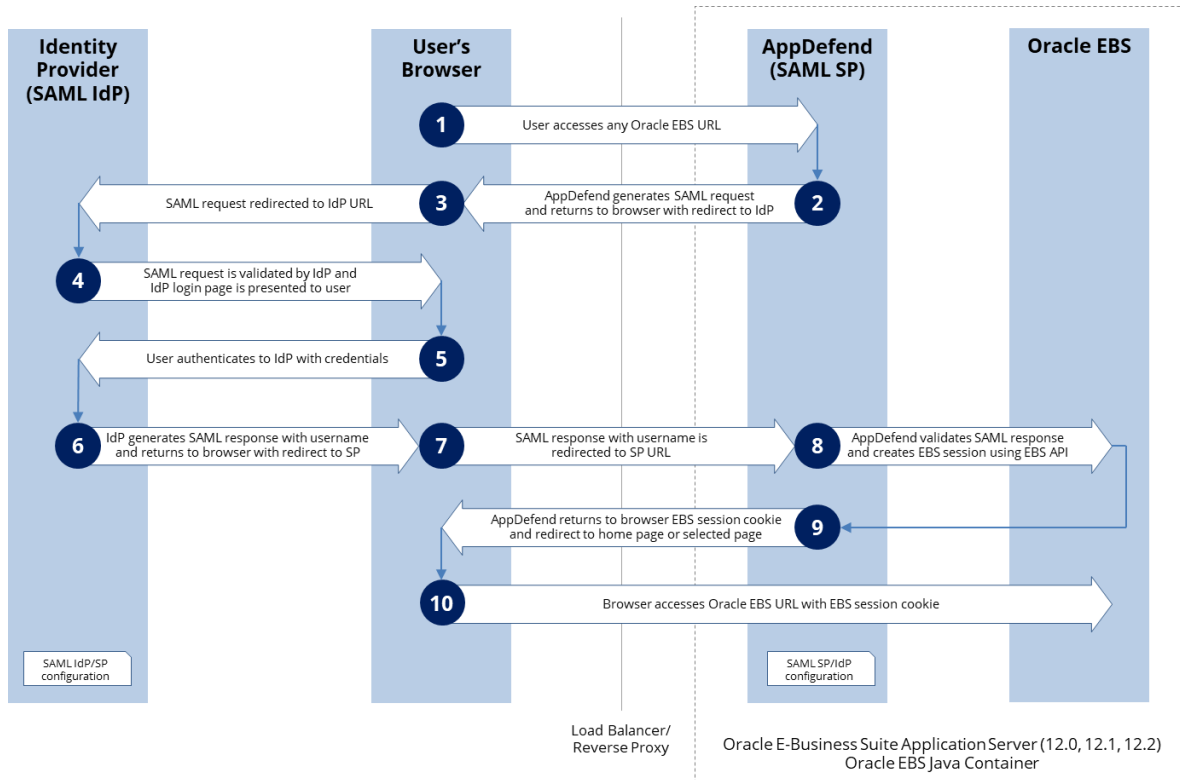
AppDefend SSO SAML Flow (EBS SSO Configuration)



AppDefend SSO SAML Flow (SSO Homepage)



AppDefend SSO SAML Security



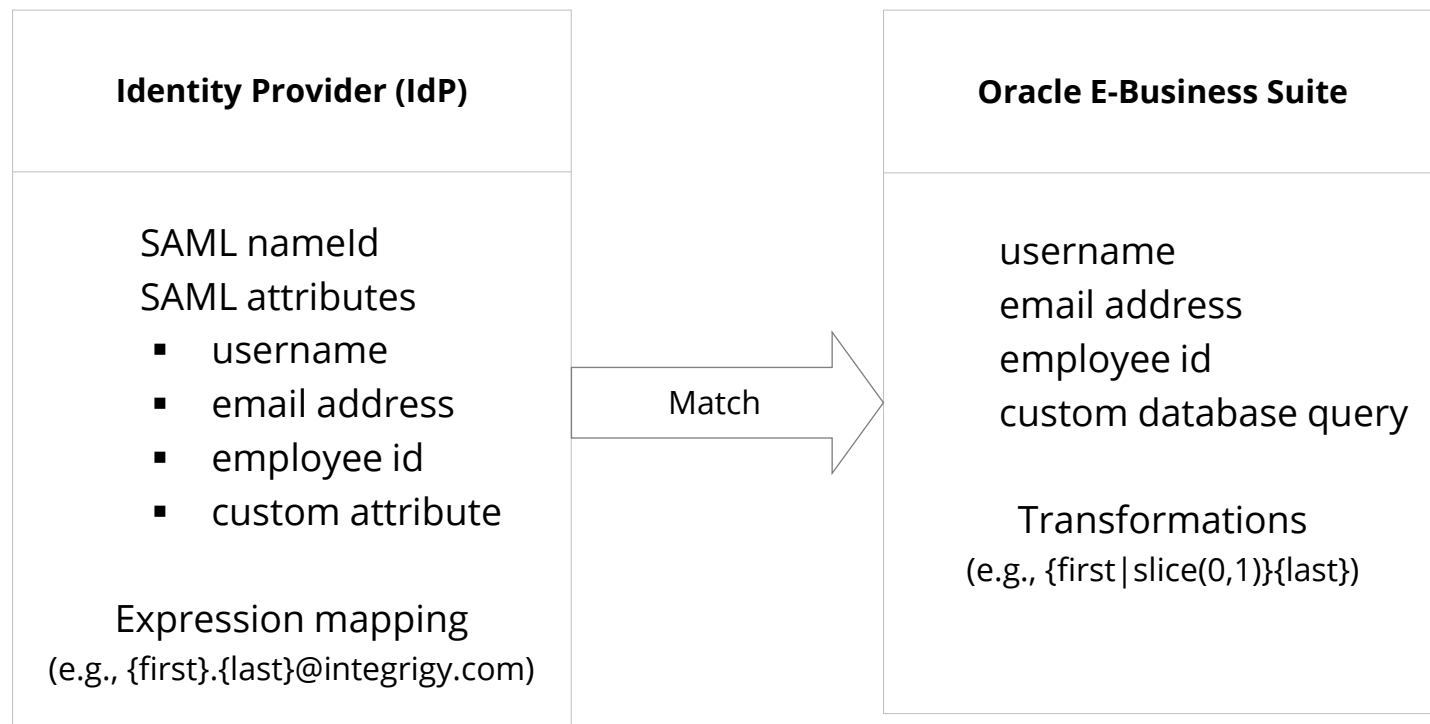
- 1
 - AppDefend protects access to all Oracle EBS URLs
 - Must be authenticated to access any URLs except specific pages such as iStore or iSupplier registration
- 2
 - SAML request is signed (SHA-512 if supported by IdP) and encrypted (AES-256) using IdP public key
 - SAML request should be communicated 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 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

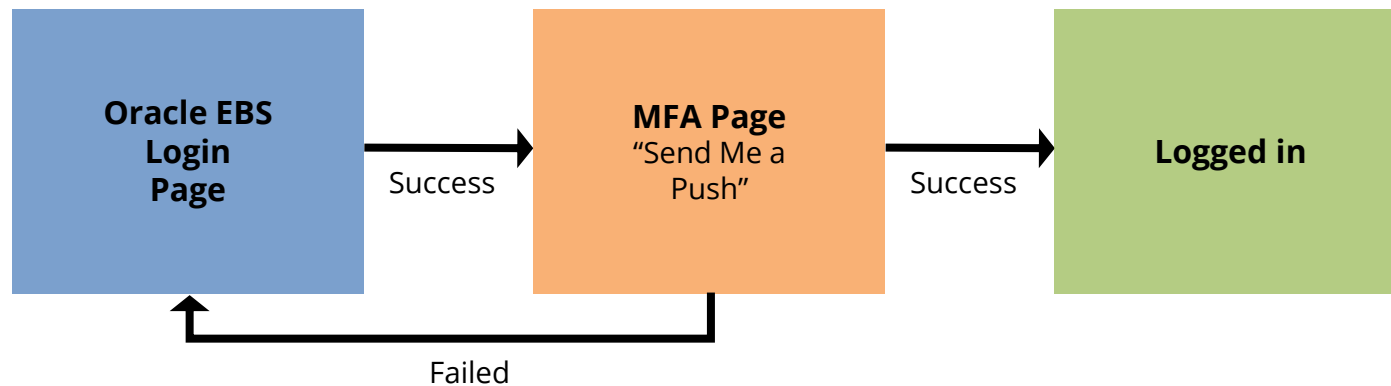
AppDefend SSO SAML User Mapping

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.



AppDefend Adaptive Multi-Factor Authentication

AppDefend enables adaptive multi-factor authentication (MFA/2FA) for Oracle EBS using DUO Security, RSA, RADIUS, TOTP, SMS, email, 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**

Two-Factor Authentication Use Cases

- **Entire Application**

- Require 2FA when logging into Oracle EBS

- **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



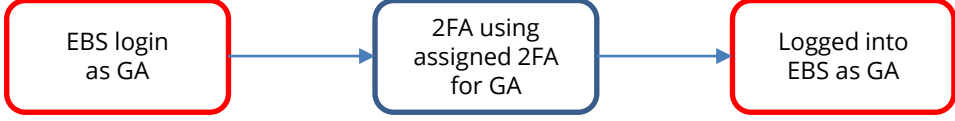

AppDefend MFA

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)	✓			

AppDefend Generic Account Protection

AppDefend MFA can be used to protect Oracle E-Business Suite privileged, generic accounts (GA), such as SYSADMIN. Multiple options to protect generic accounts and a different option may be used for each generic account.

Generic Account MFA Options	MFA Flow
1. SSO Named User profile option and/or authorized user list	 <pre>graph LR; A[EBS login as GA] --> B[IdP login page for named user]; B --> C[Logged into EBS as GA if user allowed];</pre>
2. FND_USER Named User profile option and/or authorized user list	 <pre>graph LR; A[EBS login as GA] --> B[Login page for named user]; B --> C[Logged into EBS as GA if user allowed];</pre>
3. MFA Solution such as DUO authorized in MFA solution	 <pre>graph LR; A[EBS login as GA] --> B[2FA using assigned 2FA for GA]; B --> C[Logged into EBS as GA];</pre>
4. Identity Provider (IdP) Direct authorized in IdP to access GA	 <pre>graph LR; A[IdP User's App Homepage] --> B[Click GA assigned Tile]; B --> C[Logged into EBS as GA];</pre>

AppDefend Generic Account Protection Example Scenarios

A client with about **30 generic accounts** used for various purposes configured AppDefend MFA to protect the generic accounts. Scenarios for one generic account to many named users, many generic accounts to one named user, and many generic accounts to many named users can all be easily configured and maintained. All logins including named user are monitored and logged.

Type of Generic Account	Generic Accounts	MFA and AppDefend Configuration
SYSADMIN	SYSADMIN	<ul style="list-style-type: none">▪ Tile in IdP▪ Assigned by IdP group▪ Tightly controlled, limited to DBAs▪ SYSADMIN password not known by DBAs
Job Scheduling	10 accounts, one per module, such as GL_JOB	<ul style="list-style-type: none">▪ One AppDefend rule for all 10 accounts▪ Access controlled using both an authorized user list (DBAs) and profile option set per named user (operations team)
Maintenance/Setups	12 accounts, one per module, such as GL_SETUP	<ul style="list-style-type: none">▪ One AppDefend rule for all 12 accounts▪ Access only allowed if AppDefend EBS maintenance feature is enabled▪ Access controlled using profile option set per named user
Upgrade/Patch Test	6 accounts, such as TEST1	<ul style="list-style-type: none">▪ An AppDefend rule for each of the 6 accounts▪ Access controlled using profile option set per named user and DBA team sets prior to testing as testers will change based on the patches applied▪ AppDefend logging enabled for these accounts to capture all activity

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**