

ORACLE®

# Securing Oracle E-Business Suite with the Latest Features and Tools

Elke Phelps, Product Management Director  
Oracle E-Business Suite Development  
Applications Technology

GLOC 2018  
May 2018

Contributor: Eric Bing, Senior Director, Applications Security

ORACLE®

# Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

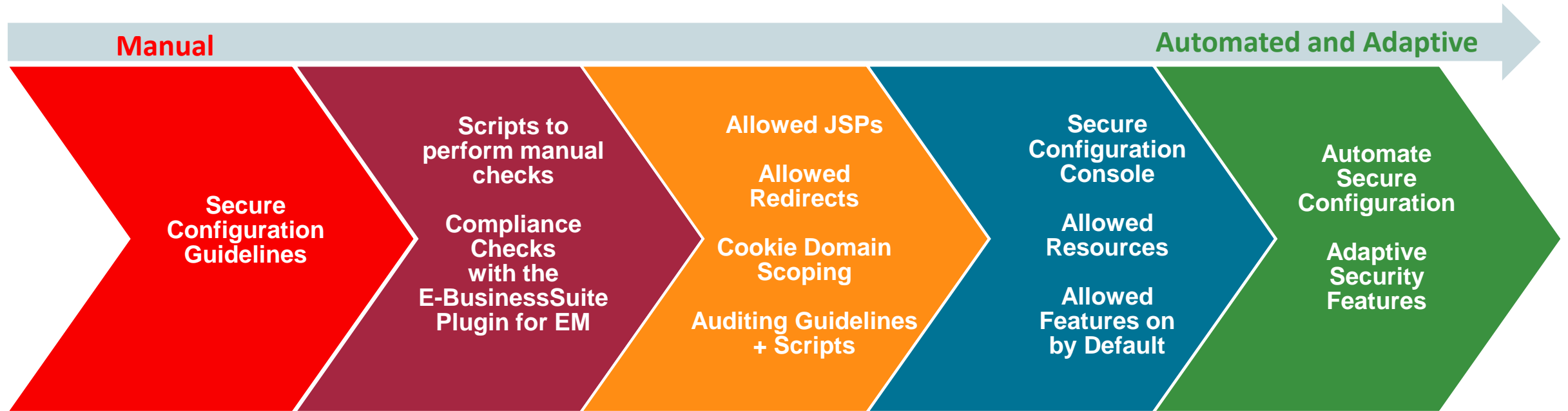
# Program Agenda

- 1 Adaptive Controls for Securing Your Oracle E-Business Suite Environment
- 2 Guidelines for Secure Configuration and Auditing
- 3 Additional Secure Configuration When Running EBS in Oracle Cloud Infrastructure
- 4 Roadmap

# Adaptive Controls for Securing Your Oracle E-Business Suite Environment

# Oracle E-Business Suite Secure Configuration Timeline

## Adding Features and Utilities to Simplify Secure Configuration



# Reduce Your Attack Surface

- **Secure Configuration Console**

- New tool to assist with secure configuration
- Easy to see where you are out of compliance
- Enable features via the console
- Guidance is provided for features that cannot be turned on via the console

- **Allowed JSPs/Resources**

- Defines whitelist of allowed JSPs/resources for Oracle E-Business Suite Release 12.2
- Prevents access to JSPs which are not used
- Enables configuration of allowed JSPs to avoid unnecessary exposure

- **Allowed Redirects**

- Defines whitelist of allowed redirects for Oracle E-Business Suite 12.2
- Prevents redirects that are not listed as allowed
- Enables configuration of allowed redirects to avoid unnecessary exposure

**Oracle E-Business Suite Security Guide Release 12.2**

# Reduce Your Attack Surface

- **Secure Configuration Console**

- New tool to assist with secure configuration
- Easy to see where you are out of compliance
- Enable features via the console
- Guidance is provided for features that cannot be turned on via the console

- **Allowed JSPs/Resources**

- Defines whitelist of allowed JSPs/resources for Oracle E-Business Suite Release 12.2
- Prevents access to JSPs which are not used
- Enables configuration of allowed JSPs to avoid unnecessary exposure

- **Allowed Redirects**

- Defines whitelist of allowed redirects for Oracle E-Business Suite 12.2
- Prevents redirects that are not listed as allowed
- Enables configuration of allowed redirects to avoid unnecessary exposure

**Enabled by default with Oracle E-Business Suite 12.2.6**



# Secure Configuration Console

# Secure Configuration Console

## Automatic Assessment of Your Environment

Security Core Services Personalization File Manager Portletization **Configuration Manager** Allowed Resources

Configuration Management

### Secure Configuration Console ☆

Search

Name %  Config Type

Code  Status







Critical Level   Include suppressed security configurations

Check	Fix	Suppress	Unsuppress						
Details	Status	Severity	Security Guideline	Description	Code	Type			
<input type="checkbox"/>	<input type="checkbox"/>	×	2	<a href="#">Database Password Profiles</a>	Check if secure configuration recommended database profiles have been created in the Oracle E-Business Suite database.	SEC_DB_PSWD_PROF	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">Workflow Email Link Login</a>	Check whether Oracle Workflow generated emails that reference URLs in Oracle E-Business Suite require additional user authentication (login).	WF_EMAIL_LOGIN	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">Forms Blocking of Bad Characters</a>	Check whether the Forms blocking of "bad" characters on the web server is active.	FND_FORMS_BLOCK_CHR	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">Attachment File Type Profiles</a>	Check whether attachment upload profiles are available and set correctly in the system.	FND_MISS_ATT_PROF	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">Diagnostic Web Pages Protected</a>	Check whether diagnostic web page protection is configured.	DIAG_WEB_PAGE_PROTEC	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">Critical Security Profile Values</a>	Check whether critical security profile values are set correctly.	FND_PROF_ERRORS	Autofixable		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">PUBLIC Privileges</a>	Check whether the PUBLIC role privileges are restricted.	FND_APPS_IND_PUBLIC	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">ModSecurity Configuration</a>	Check whether ModSecurity on the web server is active.	FND_MOD_SEC	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">Clickjacking Protection</a>	Check whether clickjacking protection is configured.	CLICKJACK_PROTECTION	Manual		
<input type="checkbox"/>	<input type="checkbox"/>	✓	1	<a href="#">Missing Server Security Profile</a>	Check whether Site level security profiles are available in the system.	FND_MISS_PROF	Manual		

- Review and implement secure configuration recommendations from a dashboard
- Access via the “Functional Administrator” responsibility, “Configuration Manager” tab
- Check your configuration
- Automatically configure items that are out of compliance
- Checks are assigned a severity level
- Suppress checks that are not relevant to your system

# Secure Configuration Console

## Details: Failed Configuration

<input type="checkbox"/> Check		<input type="checkbox"/> Configure	<input type="checkbox"/> Suppress	<input type="checkbox"/> Unsuppress	 
<input type="checkbox"/> Details	Security Guideline 			Description	
<input type="checkbox"/>		<a href="#">Application Users Default Password</a>			Check whether all application users default passwords have been changed to non-default
<p>Failed. This check has identified that some application users have default passwords. You should change application user passwords from defaults. obtained from /u01/R122_EBS/fs1/inst/apps/au64xb10_rws3260128/logs/adminsecuritycfg_25_07_2016_08_56.log ]</p>					
<input type="checkbox"/>		<a href="#">Database Users Default Passwords</a>			Check whether all database users default passwords have been changed.
<input type="checkbox"/>		<a href="#">APPLSYSPUB Privileges</a>			Check whether APPLSYSPUB privileges are properly restricted.

# Secure Configuration Console

## Security Guideline Details

### Security Guideline Details

#### Security Guideline

Application Users Default Password

#### Description

Check whether all application users default passwords have been changed to non-default values.

#### Detailed Info

This check will list the default (seeded) applications users that still have their default passwords. You should change all the default passwords, even if the user is end dated.

Note that this will not list shipped accounts that cannot be used for login (disabled/end dated accounts).

Refer to the following for additional information:

- Oracle E-Business Suite Security Guide, Release 12.2 > Oracle E-Business Suite Security > Authentication > Change Passwords for Seeded Application User Account

# Secure Configuration Console

## Security Checks

- 1 Default application users passwords have been changed to non-default values
- 2 Attachment upload profiles are available and set correctly
- 3 Critical profile values are set correctly
- 4 Default database users default passwords have been changed to non-default values
- 5 Forms blocking of bad characters on the web server is active
- 6 Site level security profiles are available in the system
- 7 ModSecurity on the web server is active
- 8 Serversecurity (Secure Flag in DBC file) is enabled
- 9 Allowed Redirects feature is enabled
- 10 APPLSYSPUB privileges are properly restricted
- 11 Auditing profiles are set
- 12 Cookie Domain scoping is configured
- 13 Application user passwords have been migrated to hashed passwords
- 14 HTTPS is enabled

# Secure Configuration Console

## 10 Additional Checks for a Total of 24 Checks

- 15 Clickjacking protection is configured
- 16 Diagnostic web page protection is configured
- 17 PUBLIC role privileges are restricted
- 18 Oracle Workflow generated emails that reference URLs in EBS require additional user authentication
- 19 Allowed Resources feature is enabled
- 20 Required whitelist configuration for the allowed resources feature is correct and up-to-date
- 21 Recommended Database initialization parameters have been set
- 22 Database profiles have been created in the EBS database for password management
- 23 iRecruitment file upload security profile value is set
- 24 Oracle Workflow Admin access is restricted

**Oracle E-Business Suite Security Guide Release 12.2**

New

# Secure Configuration Console

## Backport to Oracle E-Business Suite 12.1.3 with Patch 26090737

The screenshot displays the 'Secure Configuration Console' interface. At the top, there are navigation tabs: Security, Core Services, Personalization, File Manager, Portletization, Configuration Manager (selected), and Allowed Resources. Below the tabs, the page title is 'Secure Configuration Console' with a star icon. A search section includes fields for Name (with a '%' wildcard), Code, Config Type, Status, and Critical Level. There is a checked checkbox for 'Include suppressed security configurations' and 'Go' and 'Clear' buttons. Below the search section is a table of security checks with columns for Check, Fix, Suppress, Unsuppress, Details, Status, Severity, Security Guideline, Description, Code, and Type. The table shows 10 rows of checks, with the first one marked as failed (red X) and the others as passed (green checkmarks).

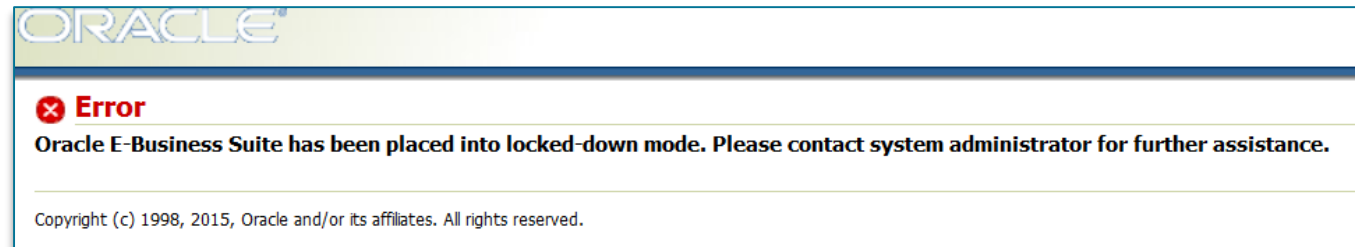
Check	Fix	Suppress	Unsuppress	Details	Status	Severity	Security Guideline	Description	Code	Type
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✖	2	Database Password Profiles	Check if secure configuration recommended database profiles have been created in the Oracle E-Business Suite database.	SEC_DB_PSWD_PROF	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	Workflow Email Link Login	Check whether Oracle Workflow generated emails that reference URLs in Oracle E-Business Suite require additional user authentication (login).	WF_EMAIL_LOGIN	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	Forms Blocking of Bad Characters	Check whether the Forms blocking of "bad" characters on the web server is active.	FND_FORMS_BLOCK_CHR	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	Attachment File Type Profiles	Check whether attachment upload profiles are available and set correctly in the system.	FND_MISS_ATT_PROF	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	Diagnostic Web Pages Protected	Check whether diagnostic web page protection is configured.	DIAG_WEB_PAGE_PROTEC	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	Critical Security Profile Values	Check whether critical security profile values are set correctly.	FND_PROF_ERRORS	Autofixable
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	PUBLIC Privileges	Check whether the PUBLIC role privileges are restricted.	FND_APPS_IND_PUBLIC	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	ModSecurity Configuration	Check whether ModSecurity on the web server is active.	FND_MOD_SEC	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	Clickjacking Protection	Check whether clickjacking protection is configured.	CLICKJACK_PROTECTION	Manual
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✔	1	Missing Server Security Profile	Check whether Site level security profiles are available in the system.	FND_MISS_PROF	Manual

- Review and implement secure configuration recommendations from a dashboard
- Performs 23 secure configuration checks
- Configures items that are out of compliance
- Suppress checks that are not relevant to your system
- System is locked down after application of patch 26090737

MOS Note 2311308.1

# Secure Configuration Console

## Configure or Acknowledge and Accept Warnings



Please select the appropriate option below:

I am done with the Security Configurations

Ignore the Security Configurations

Proceed

By Clicking this Button you Agree that you have reviewed the current security configurations and are willing to Unlock EBS for normal usage.

Note: Your system will be locked down until the system administrator configures or acknowledges the recommended security configurations.



# Allowed JSPS/Resources

# History of Allowed JSPs / Resources

- Allowed JSPs introduced in E-Business Suite 12.2.4
  - Enabled by default in E-Business Suite ATG 12.2.6
- Rebranded to Allowed Resources in 12.2.6+ with the following patches:
  - ENABLE ALLOWED RESOURCES (24737426:R12.FND.C)
    - This patch will turn the Allowed Resources feature ON.
  - ATG 12.2.6 (21900895:R12.ATG\_PF.C.DELTA.6)
  - TKX Delta 9 (25180736:R12.TXK.C.DELTA.9)
- User interface and configuration metadata stored in the database in E-Business Suite ATG 12.2.7

# Feature Overview of Allowed Resources

## Principles

- Defines **whitelist** of web allowed resources
  - A whitelist is an explicit list of items that are allowed for access
- Enhancements to Allowed JSPs feature
  - Whitelist resources including servlets and JSPs
- Prevents access to resources which are not used
- Enables configuration of actively allowed resources to avoid unnecessary exposure
- Allows custom resources to be defined in the list of allowed resources

# Feature Overview of Allowed Resources

## What Additional Features are Available?

- Metadata now stored in the database (not in configuration files)
- New user interface
- With configuration metadata stored in the database, allowed resources configuration will be preserved when upgrading and patching
- Whitelist configuration recommendations are provided based upon products used and underlying resource usage
- Utilities to identify custom resources and populate usage data

# Configuration Overview of Allowed Resources

## Patch 24737426:R12.FND.C

- Profile: **Security: Allowed Resources**  
( **FND\_SEC\_ALLOWED\_RESOURCES** )
- Profile may be set at site or server level
- Default value: **CONFIG**
- Turn off feature and allow all resources to be accessible by setting the profile to: **All**
- New profile overrides profile: **Allow Unrestricted JSP Access**  
( **FND\_SEC\_ALLOW\_JSP\_UNRESTRICTED\_ACCESS** )

# Configuration Overview of Allowed Resources

## On By Default as of Oracle E-Business Suite 12.2.6

1. Populate web usage data (optional)
2. Identify and configure custom resources
3. Configure allowed resources products based upon recommendations
4. Continue to refine the list based upon recommendations (ongoing)
  - As a result of improved recommendations based upon usage data
  - With the deployment of new features or products

# Configuration Overview of Allowed Resources

## Start with an Introduction of the Configuration in the New UI

1. Populate web usage data (optional)
2. Identify and configure custom resources
3. Configure allowed resources products based upon recommendations
4. Continue to refine the list based upon recommendations (ongoing)
  - As a result of improved recommendations based upon usage data
  - With the deployment of new features or products

# Configuration Overview of Allowed Resources

## 3 Levels of Granularity for Configuring Access

- If you are not using any products in a particular product family, ensure that the **Enabled** check box is not selected in the Details section of the Product Family Configuration page.
- To restrict access at the product level, deny access to the appropriate product-level resources on the **Product Details** tab in the Product and Common Resources section.
- To restrict access at the individual resource level, deny access to the resources in question by drilling down to the **Resource Details** or denying access in **Common Resources** tab.



# User Interface for Allowed Resources

Security Core Services Personalization File Manager Portletization Configuration Manager **Allowed Resources**

**Allowed Resources Management**

- Advanced Planning
- Applications Technology
- Channel Revenue Management
- Custom
- Human Resources
- Master Data Management
- Order Management & Logistics
- Procurement
- Projects
- Sales, Marketing and eCommerce
- Service
- Supply Chain Management**

**Product Family Configuration**

Use this page to configure the allowed resources for products within this family.

**Details**

Name : Supply Chain Management Enabled :

Code : SCM

Apply

**Product and Common Resource Details**

Product Details Common Resources

Name ▲	Code ▲	Licensed ▲	Web Activity ▲	Transaction Data ▲	Recommendation ▲	Access
E-Records	EDR	✓	--	--	Not sufficient data	Allow ▾
Installed Base	CSI	✓	--	--	Not sufficient data	Allow ▾
Site Management	RRS	✓	--	--	Not sufficient data	Allow ▾

UI is accessible via the Functional Administrator responsibility → Functional Administrator page → Allowed Resources tab

Easily allow or deny access to products and underlying resources

A family name may be selected from the left menu to view the Product Family Configuration

# User Interface for Allowed Resources

**Allowed Resources Management**

**Product Family Configuration**

Use this page to configure the allowed resources for products within this family.

**Details**

Name : Supply Chain Management    Enabled :     Code : SCM

Apply

**Product and Common Resource Details**

Product Details    Common Resources

Name ▲	Code ▲	Licensed ▲	Web Activity ▲	Transaction Data ▲	Recommendation ▲	Access
<a href="#">E-Records</a>	EDR	✓	--	--	Not sufficient data	Allow ▼
<a href="#">Installed Base</a>	CSI	✓	--	--	Not sufficient data	Allow ▼
<a href="#">Site Management</a>	RRS	✓	--	--	Not sufficient data	Allow ▼

## Details section

Enabled check box indicates whether or not the product family resources are used and allowed.

## Product and Common Resources Details Section

Use this section of the page to configure products.

# User Interface for Allowed Resources

Product and Common Resource Details → Product Details tab

**Product and Common Resource Details**

Product Details | Common Resources

Apply Revert | [Icons: Refresh, Undo, Settings]





Name ▲	Code ▲	Licensed ▲	Web Activity ▲	Transaction Data ▲	Recommendation ▲	Access
<a href="#">E-Records</a>	EDR	✓	--	--	Not sufficient data	Allow ▼
<a href="#">Installed Base</a>	CSI	✓	--	--	Not sufficient data	Allow ▼
<a href="#">Site Management</a>	RRS	✓	--	--	Not sufficient data	Allow ▼

# User Interface for Allowed Resources

Product and Common Resource Details → Common Resources Tab

**Product and Common Resource Details**

Product Details | **Common Resources**

Apply Revert |     ▼

◀ Previous 1-10 ▶ Next 10 ▶

Name ▲	Type ▲	Application ▲	Web Activity ▲	Access
/OA_HTML /CreateWaveBookmarkable.jsp	JSP	GLOBAL_SCM	--	Allow for product ▼
/OA_HTML/EamLamEsri.jsp	JSP	GLOBAL_SCM	--	Allow for product ▼
/OA_HTML/EamLamSpatial.jsp	JSP	GLOBAL_SCM	--	Allow for product ▼
/OA_HTML/EbiServlet	SERVLET_URL	GLOBAL_SCM	--	Allow for product ▼
/OA_HTML/LcmEndecaPost.jsp	JSP	GLOBAL_SCM	--	Allow for product ▼
/OA_HTML/MOBookmarkable.jsp	JSP	GLOBAL_SCM	--	Allow for product ▼

# User Interface for Allowed Resources

Product and Common Resource Details → Product Details tab → Click on Product Name

**Product and Common Resource Details**

Product Details | Common Resources

Apply Revert | [Icons: Refresh, Undo, Settings]

Name ▲	Code ▲	Licensed ▲	Web Activity ▲	Transaction Data ▲	Recommendation ▲	Access
<a href="#">E-Records</a>	EDR	✓	--	--	Not sufficient data	Allow ▼
<a href="#">Installed Base</a>	CSI	✓	--	--	Not sufficient data	Allow ▼
<a href="#">Site Management</a>	RRS	✓	--	--	Not sufficient data	Allow ▼








# User Interface for Allowed Resources

Product Details tab → Click on Product Name → Used Tab

### Resource Details

Used Owned

Apply Revert |     

Name ▲	Type ▲	Application ▲	Web Activity ▲	Access
/OA_HTML/jsp/edr/EDRRuleXMLPublisherHandler.jsp	JSP	EDR	--	Allow for product ▼
/OA_HTML/jsp/edr/FilePreview.jsp	JSP	EDR	--	Allow for product ▼
/OA_HTML/jsp/edr/iSignPublisherHandler.jsp	JSP	EDR	--	Allow for product ▼

# Configuration Overview of Allowed Resources

Review How to Populate Usage Data and Custom Resources

1. Populate web usage data (optional)
2. Identify and populate custom resources
3. Configure allowed resources products based upon recommendations
4. Continue to refine the list based upon recommendations (ongoing)
  - As a result of improved recommendations based upon usage data
  - With the deployment of new features or products

# Utilities for Allowed Resources

## Step 1. Generate Web Usage File

- Download **webusage.awk**

- Delivered with auditing scripts , MOS [Document ID 2069190.1](#)
- Generates a web usage file from Apache access logs
- Execute the **webusage.awk** script against your Apache access logs:

```
$ cat access_log* | tr '?' ' ' | awk -f webusage.awk > webusage.out
```

```
===== WEB USAGE: 324512 lines, 1358 counted hits 2016-09-11 - 2016-12-09
First hit seen   Most recent hit   #Hits URL
-----
2016-11-08_19:38 2016-11-08_20:36     3 /OA_HTML/amsActMetricsHistLOV.jsp
2016-11-08_19:42 2016-11-08_19:42     1 /OA_HTML/amsApprFuncLOV.jsp
...
2016-09-29_00:36 2016-12-08_18:06    308 /OA_HTML/AppsLocalLogin.jsp
2016-11-04_20:27 2016-11-04_21:02     6 /OA_HTML/AppsLocalLogin.jsp/%2e./jtffmeqq.jsp
...
2016-11-04_19:29 2016-11-04_19:31     5 /OA_HTML/cabo/jsps/a.jsp
2016-10-27_21:03 2016-11-08_00:08    195 /OA_HTML/cabo/jsps/frameRedirect.jsp
2016-09-11_11:12 2016-09-11_11:12     1 /OA_HTML/fake.jsp
```



# Utilities for Allowed Resources

## Step 2. Populate Web Usage and Custom Configurations

- Populate web usage data or custom configuration with `WLDataMigration`
- Execute Loader utility to populate web usage data for already seeded resources and generate **CUSTOM.out** for unknown resources

```
$ java oracle.apps.fnd.security.resource.WLDataMigration MODE=seed \  
  INPUT_FILE=webusage.out DBC=$FND_SECURE/<SID>.dbc
```

```
2016-09-11_11:12 2016-09-11_11:12          1 /OA_HTML/fake.jsp  
2017-06-14_03:24 2017-06-14_03:27      538 /OA_HTML/CustLogin.jsp
```

# Load Custom Configuration for Allowed Resources

## Step 3 – Review **CUSTOM.out** and Load

- **Option 1:** Use the **CUSTOM.out** file generated from **WLDataMigration**

- Review the CUSTOM.out file before uploading to ensure that entries are legitimate

```
$ java oracle.apps.fnd.security.resource.WLDataMigration MODE=custom \  
INPUT_FILE=CUSTOM.out DBC=$FND_SECURE/<SID>.dbc
```

- **Option 2:** Use the **custom.conf** file from prior configuration of Allowed JSPs or Allowed Resources (pre-12.2.7)

```
$ java oracle.apps.fnd.security.resource.WLDataMigration MODE=custom \  
INPUT_FILE=custom.conf DBC=$FND_SECURE/<SID>.dbc
```

# Allowed Redirects

# Feature Overview for Allowed Redirects

## Principles

- Provides “*defense-in-depth*” protection against phishing redirect attacks
- Defines **whitelist** of allowed redirects for Oracle E-Business Suite 12.2
  - A whitelist is an explicit list of hosts that are allowed for redirects
- Prevents redirects that are not listed as allowed
- Enables configuration of allowed redirects to avoid unnecessary exposure
- Allows custom redirects to be defined in the list of allowed redirects
- Allows **all redirects by default**

Oracle E-Business Suite Security Guide Release 12.2

# Which Redirects Should Be Allowed?

## Configuration You Need to Add to the Configuration File

- Oracle E-Business Suite iProcurement with Punchout
  - Add host or domain entry for each Punchout site
- Oracle E-Business Suite Configurator integration with Agile or Siebel using Oracle Application Integration Architecture
  - Add host or domain entry for each integration point
- Any custom redirects used in your environment

# Transfer of Information (TOI) Online Training

## Learn More About Oracle E-Business Suite 12.2 New Features

- Implement and Use Application Object Library - Secure Configuration Console
- Implement and Use E-Business Suite Secure Configuration - Allowed Resources
- Implement and Use Application Object Library - SECURITY: Redirect Filter
- Implement and Use E-Business Suite Secure Configuration - Cookie Domain Scoping

**MOS Note 807319.1**

# Guidelines for Secure Configuration and Auditing

# How to Deploy Oracle E-Business Suite Securely

## Follow Our Secure Configuration Guidelines

- Secure Configuration Guide for Oracle E-Business Suite
  - Previously known as “Best Practice” documents
  - Release **12.2**, *Security Administration Guide, Secure Configuration Chapter*
  - Release **12.1**, MOS Note **403537.1**
- Secure Configuration Scripts
  - *Security Configuration and Auditing Scripts for Oracle E-Business Suite*, MOS Note **2069190.1**



# How to Deploy Oracle E-Business Suite Securely

## Stay Current with Patching

- Review the Critical Patch Updates Advisory Page on a quarterly basis  
<http://www.oracle.com/technetwork/topics/security/alerts-086861.html>
- Review the Latest CPU document for Oracle E-Business released with CPU,
  - Covers Oracle E-Business Suite Release 12.1 and 12.2
  - Apply to Oracle E-Business Suite
  - Apply to Oracle E-Business Suite technology stack

**MOS Note 2270270.1**

# How to Deploy Oracle E-Business Suite Securely

## Stay Current with Latest Oracle E-Business Suite Code

- Update to the latest release or release update pack
  - Yes, Oracle E-Business Suite releases and release updates improve security as well
- Release Upgrade
  - Oracle E-Business Suite Release 12.2.7
  - Oracle E-Business Suite Release 12.1.3 + Recommended Patch Collection 5

**Oracle E-Business Suite 12.2 Information Center: [MOS Note 1583092.1](#)**

# Implement or Migrate to TLS 1.2

## For Oracle E-Business Suite Inbound, Outbound and Loopback Connections

- Oracle E-Business Suite Release 12.2 and 12.1 Certified with TLS 1.2
- Optional Configurations
  - Configuring “TLS 1.2 Only”
  - Disabling HTTP Port
  - Enabling TLS from Oracle HTTP Server (OHS) to Application Server (OC4J / WLS)

**EBS 12.2: 1367293.1, EBS 12.1: 376700.1**

# Recent Certificate Certifications

- Elliptic Curve Cryptography certified with EBS 12.2
  - Elliptic Curve Cryptography supports both forward secrecy and stronger cipher suites
  - Apple's [App Transport Security](#) mandates forward secrecy, and we expect this to be a requirement for mobile clients
  - Roadmap for EBS 12.2
- Subject Alternative Name (SAN) & Wildcard Certificates certified with EBS 12.1.3
  - Use of the SAN field in a certificate request (CSR) allows you to specify multiple host names to be protected by a single public key certificate
  - Use of SAN will also allow for using a single certificate for multiple domains.
  - Wildcard Certificates can be used with multiple sub-domains of a domain.
  - Roadmap for EBS 12.2

# Oracle E-Business Suite DMZ Features

## Reduce Attack Surface

- Limited number of Oracle E-Business Suite products certified for internet
- External Oracle E-Business Suite application tier access limited by setting **Node Trust Level**
- Responsibilities available for external use only upon configuration
- URL Firewall exposes only the pages that are required

**EBS 12.2: 1375670.1, EBS 12.1: 380490.1**

# Feature Overview for Cookie Domain Scoping

## Principles

- Reduces the attack surface of Oracle E-Business Suite
- Provides additional protection for communication between the browser and the Oracle E-Business Suite web tier
- Provides the ability to define the scope for cookie sharing to avoid unnecessary exposure
- Allows for a custom scope to be defined

Oracle E-Business Suite Security Guide Release 12.2

# What is a Cookie?

- If a domain is not specified, the browser does not send the cookie beyond the originating host
- If you explicitly set the cookie domain scope this tells the browser where the cookie can be sent



Oracle E-Business Suite Security Guide Release 12.2

# Enable Auditing and Logging

- Detect suspicious activity and attacks
- Investigate incidents after an attack
- Adhere to compliance standards (SOX, HIPAA, PCI-DSS)
- Implement business process monitoring and controls
- Debug application problems
- Performance monitoring

**Oracle E-Business Suite Security Guide Release 12.2**



# Enable Auditing and Logging

- Documentation
  - Oracle E-Business Suite 12.2 Security Guide, *Auditing and Logging* Chapter
  - MOS Note 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*
- Scripts
  - Download EBSAuditScripts.zip (contains multiple SQL scripts)
    - Validate audit configuration
    - Query audit tables
    - Configure database auditing
  - Check periodically for updates to EBSAuditScripts.zip

**Oracle E-Business Suite Security Guide Release 12.2**

# Additional Secure Configuration When Running EBS in Oracle Cloud Infrastructure

# Provisioning Oracle E-Business Suite 12.2.6

## Default Configuration for Oracle Cloud

- Oracle E-Business Suite accounts are locked down
  - Must reset passwords and enable Oracle E-Business Suite accounts (FND\_USERS)
- Products turned off for both production and vision installs using Allowed JSPs feature
  - Complex Maintenance, Repair & Overhaul
  - Oracle Marketing
  - Oracle Marketing Encyclopedia System
  - Oracle Sales Online
  - Oracle Sales Offline
  - Oracle Sales for Handhelds
  - Oracle Field Service
  - Oracle Field Service / Handheld
  - Oracle Knowledge Management
  - Oracle iStore
  - Oracle iSupport
  - Oracle Advanced Outbound Telephony
  - Oracle Email Center
  - Oracle Call Center Technology
  - Oracle One-to-One Fulfillment
  - Oracle Partner Management

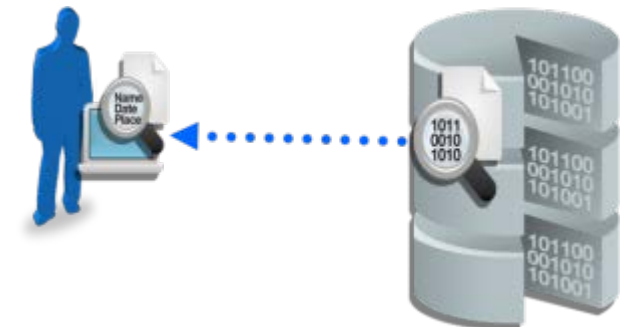
# Transparent Data Encryption (TDE)

## What is it?

- Encrypt data at rest
- Decrypt data on-the-fly while E-Business Suite is running
- Encrypt tablespaces or individual columns
- Store keys in Oracle Wallet Hardware Device

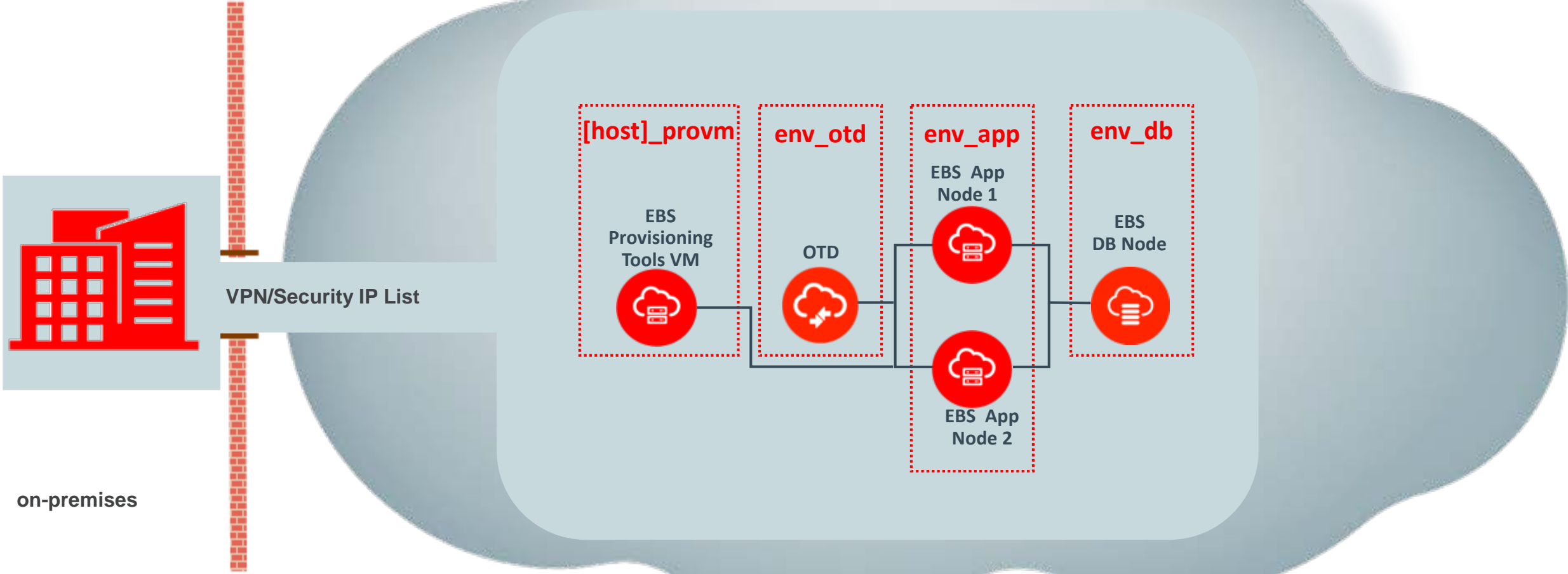
## What's automated with Lift and Shift?

- Maintain TDE enabled on-premises with lift and shift from on-premises to compute, DBCS or ExaCS
- Enable TDE automatically with lift and shift from on-premises to DBCS and ExaCS



# E-Business Suite on Oracle Cloud Infrastructure - Classic

## Additional Security with **Security Lists** and **Security Rules**

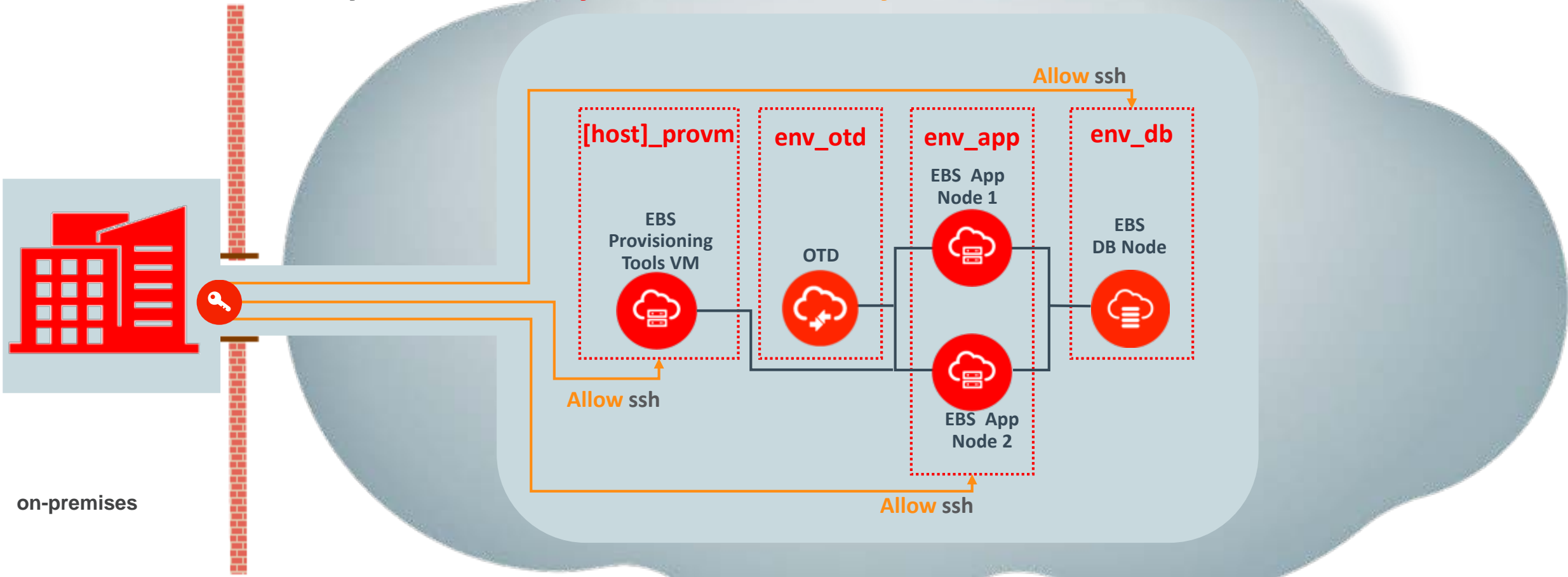


on-premises



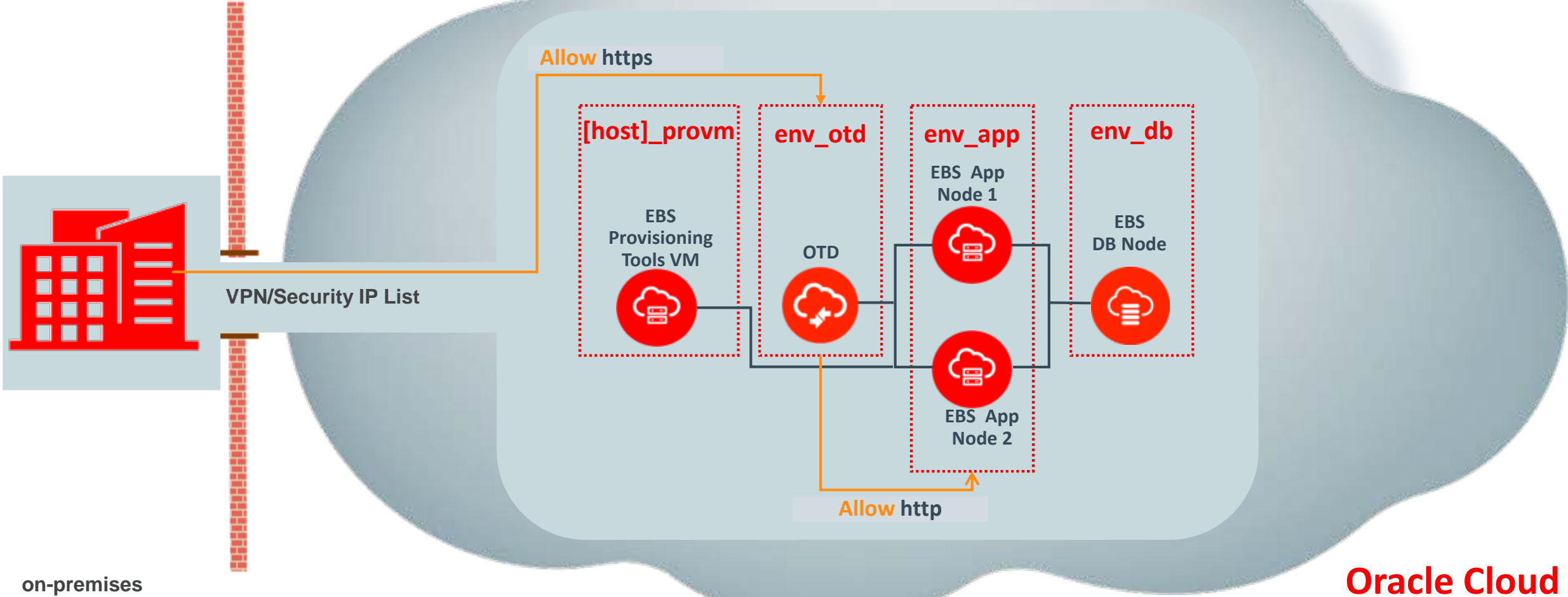
# E-Business Suite on Oracle Cloud Infrastructure - Classic

## Additional Security with **Security Lists** and **Security Rules**



# E-Business Suite on Oracle Cloud Infrastructure - Classic

## Additional Security with **Security Lists** and **Security Rules**



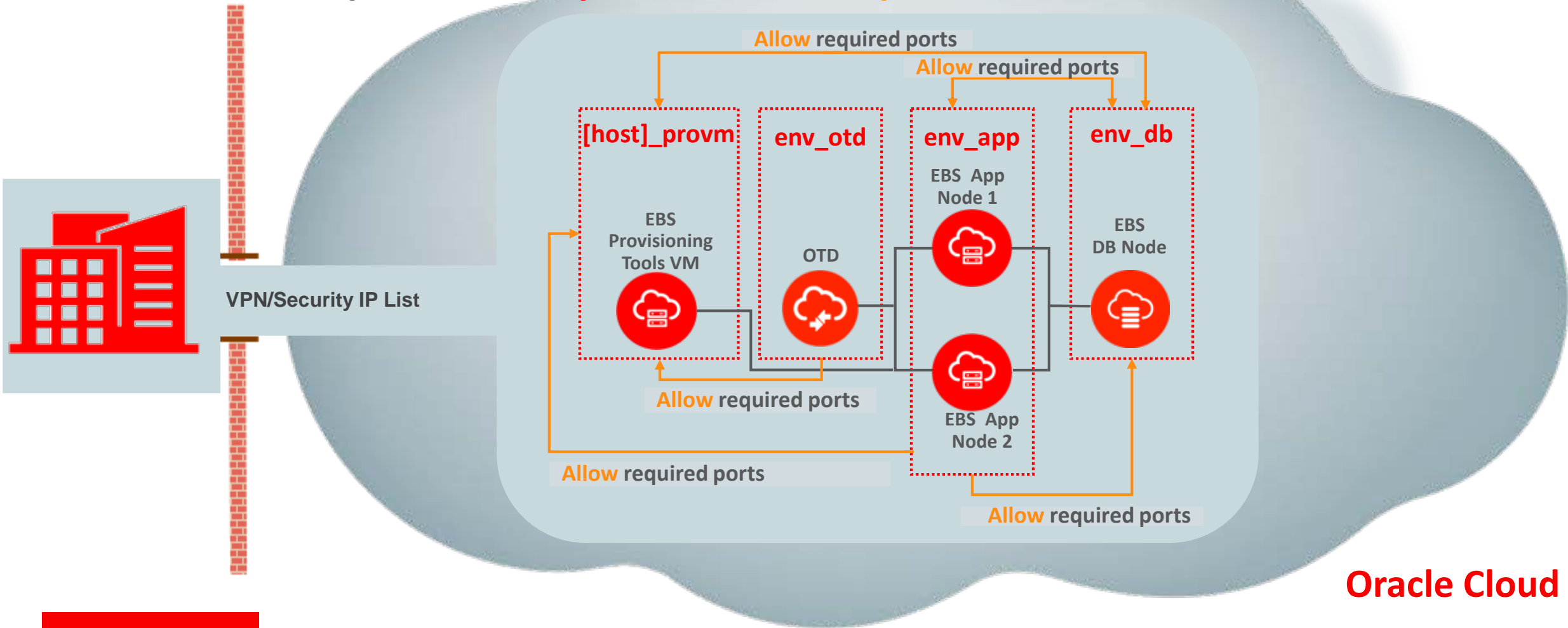
on-premises

Oracle Cloud



# E-Business Suite on Oracle Cloud Infrastructure - Classic

## Additional Security with **Security Lists** and **Security Rules**



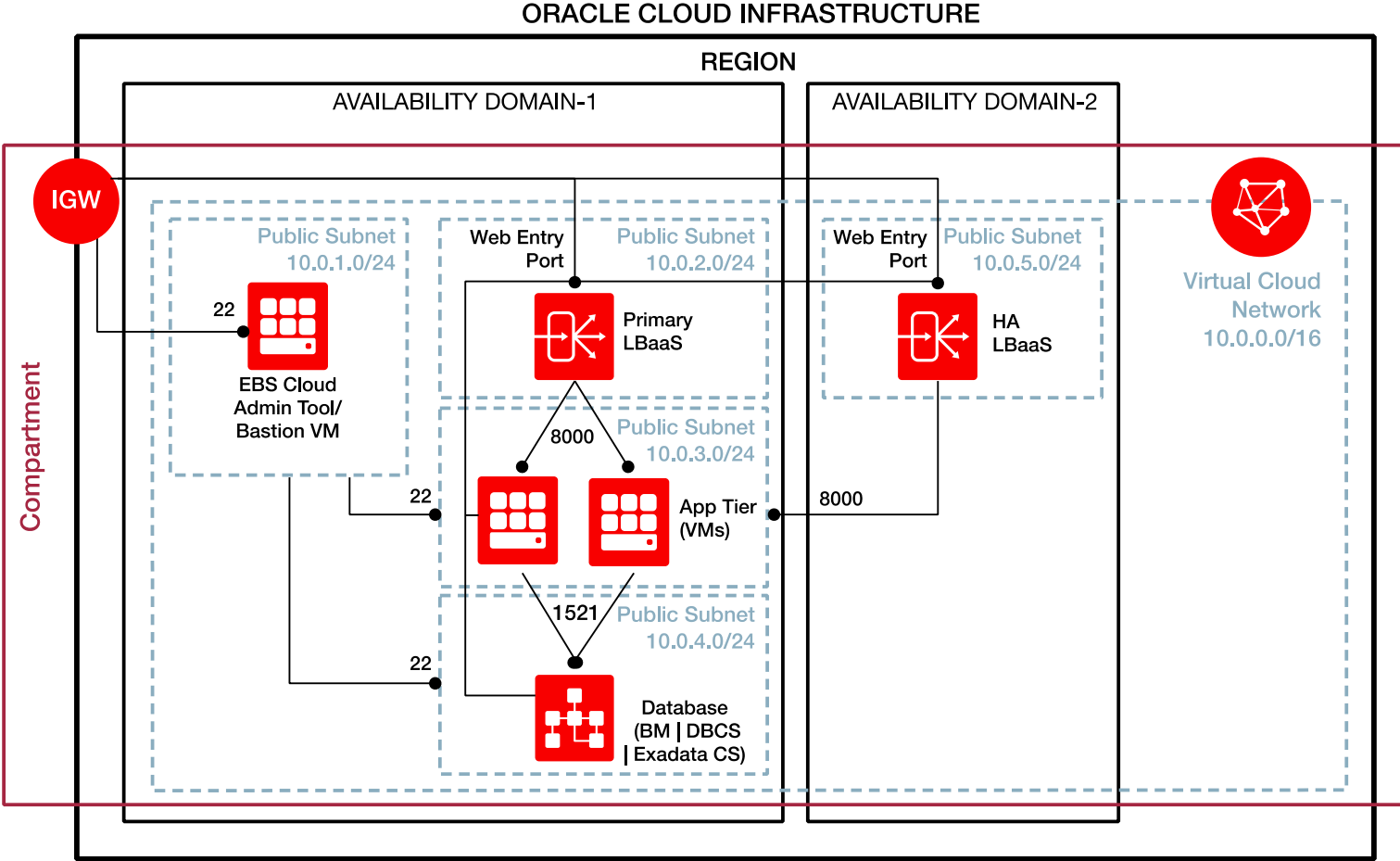
Oracle Cloud





# E-Business Suite on Oracle Cloud Infrastructure\*

## Enhanced Provisioning using the EBS Cloud Admin Tool



\*formerly Bare Metal



# Roadmap

# Oracle E-Business Suite Security

## Oracle Cloud & On-Premises

- ✓ Turn additional security features on by default
- ✓ Whitelisted Resources
- ✓ Add additional checks to the Secure Configuration Console
- ✓ Certify EBS 12.1 Data Masking Templates with EM13cR1

## Oracle Cloud

- Certify Database 12c Database Vault (DBCS) with EBS 12.2
- ✓ Provide an improved process for enabling TDE with EBS 12.1.3 and EBS 12.2 on DBCS

## On-Premises

- ✓ Certify Database Vault for EBS 12.2 with Database 12c and 11gR2
- ✓ Certify Database Vault for EBS 12.1.3 and Database 12c

# Oracle E-Business Suite Security

- Backport to Oracle E-Business Suite Release 12.1.3
  - Secure Configuration Console
  - Allowed Resources
- Oracle E-Business Suite Release 12.2 and Release 12.1
  - TLS configuration prerequisite checker
  - Automation of TLS configuration
  - Elliptic curve cipher suites certification
  - Allowed Resources
    - Improve recommendations based upon activity
    - Automate configuration of resource level lockdown

# Documentation

Title	Doc ID
FAQ: Oracle E-Business Suite Security	2063486.1
Oracle E-Business Suite Security Guide, Release 12.2 – Secure Configuration Chapter	N/A
Secure Configuration for Oracle E-Business Suite Release 12	403537.1
Enabling TLS in Oracle E-Business Suite Release 12.2	1367293.1
Enabling SSL or TLS in Oracle E-Business Suite Release 12.2	2143101.1
Enabling TLS in Oracle E-Business Suite Release 12.1	376700.1
Enabling SSL or TLS in Oracle E-Business Suite Release 12	2143099.1
CVE-2014-3566 - Instructions to Mitigate the SSLv3 Vulnerability ("POODLE Attack") in Oracle E-Business Suite	1937646.1

# Where to Find More Information

## Oracle E-Business Suite Release 12.2

- EBS Documentation and Training
  - [EBS 12.2 Information Center](#)  
MOS Note 1581299.1  
Includes link to the EBS Documentation Web Library
  - [EBS Release Content Documents](#)  
MOS Note 1302189.1
  - [EBS Transfer of Info \(TOI\) Online Training](#)  
MOS Note 807319.1

## EBS 12.2 Information Center

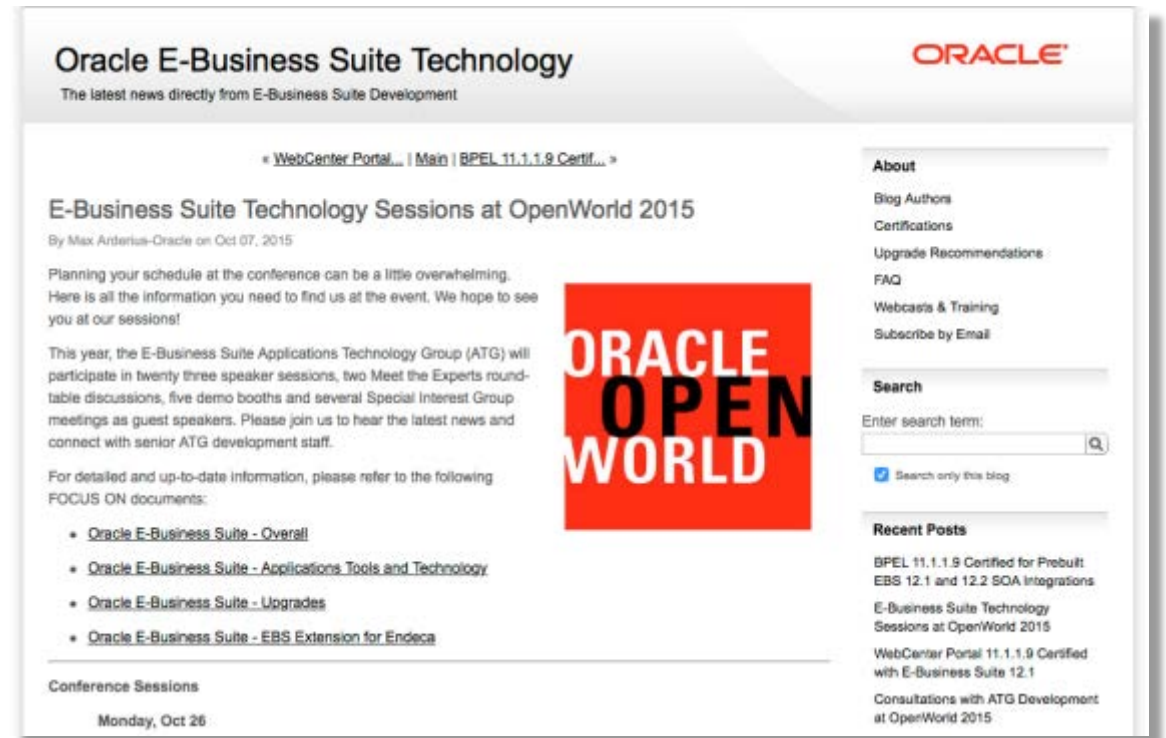
### ★ Oracle E-Business Suite Release 12.2 Information Center (Doc ID 1581299.1)

Home	<b>Oracle E-Business Suite Release 12.2 Highlights</b>
<b>Reference Information</b>	<a href="#">Start Here</a> <a href="#">Oracle E-Business Suite Release 12.2 Technology Stack Documentation Roadmap</a>
Announcements	This document acts as a central list of My Oracle Support knowledge documents that describe the recommended use and deployment of various optional and required components of the technology stack that underpins the overall Oracle E-Business Suite Release 12.2 architecture.
Documentation	<b>Oracle E-Business Suite Release 12.2: Technical Planning, Getting Started, and Go-Live Checklist</b> The Technical Planning Guide is designed to provide a starting point for customers moving to Oracle E-Business Suite Release 12.2. Much of the content of this book has been drawn from other Release 12.2 books, to provide a convenient high-level summary for DBAs and developers before they move on to the more detailed descriptions in those books. It is not intended to replace or be a substitute for any of those books. The go-live readiness checklist helps you identify and meet the high-level requirements that are needed for a successful go-live on Release 12.2. <a href="#">Read full details</a>
-Product Release Notes 12.2.2 -Product Release Notes 12.2.3 -Product Release Notes 12.2.4 -Product Release Notes 12.2.5	<b>Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation</b> The purpose of this document is to communicate implementation, configuration, and administration information specific to Oracle E-Business Suite Mobile Apps currently available for the iOS operating system and the Android operating system. <a href="#">Read full details</a>
Globalization Center	<b>Information Center: Oracle E-Business Suite Extensions for Oracle Endeca Install &amp; Configure</b> This Index is designed to provide you with simple and quick navigation between the E-Business Suite and the Information Discovery integration. <a href="#">Read full details</a>
Additional Resources	<b>Oracle E-Business Suite Releases 12.1 and 12.2 Release Content Documents</b> These Release Content Documents (RCDs) communicate information about new or changed functionality introduced in Oracle E-Business Suite Releases 12.1 and Release 12.2, subsequent Release Update Packs (RUPs), and off-cycle patches. For your convenience, they also include new or changed functionality introduced in the RUPs for Release 12, including 12.0.2 through 12.0.7. <a href="#">Read full details</a>
Product Info Centers	<b>Using the Online Patching Readiness Report in Oracle E-Business Suite Release 12.2</b> This document introduces the Global Standards Compliance Checker (GSCC) and Readiness Report, and outlines how it is used with Oracle E-Business Suite Release 12.2. <a href="#">Read full details</a>
R11i Info Center	<b>Oracle E-Business Suite Release 12.2: Consolidated List of Patches and Technology Bug Fixes</b> This document provides a consolidated list of the latest technology bugfixes required for Oracle E-Business Suite Release 12.2 and a set of recommended patches to install the technology bugfixes. <a href="#">Read full details</a>
R12.0 Info Center	<b>Applying the Latest AD and TXK Release Update Packs to Oracle E-Business Suite Release 12.2</b>
R12.1 Info Center	
<b>R12.2 Info Center</b>	
<b>Lifecycle Management</b>	
Install	
Implement	
Manage	
Upgrade	
Legislative Updates Center	

# E-Business Suite Technology Stack Blog

[blogs.oracle.com/stevenChan](https://blogs.oracle.com/stevenChan)

- Direct from EBS Development
- Latest news
- Certification announcements
- Primers, FAQs, tips
- Desupport reminders
- Latest upgrade recommendations
- Statements of Direction
- Subscribe via email or RSS



The screenshot shows a blog post from the Oracle E-Business Suite Technology blog. The page header includes the Oracle logo and the text "Oracle E-Business Suite Technology" and "The latest news directly from E-Business Suite Development". The main content area features a navigation bar with links for "WebCenter Portal...", "Main", and "BPEL 11.1.1.9 Certif...". The article title is "E-Business Suite Technology Sessions at OpenWorld 2015" by Max Arterias-Oracle on Oct 07, 2015. The article text discusses planning for the conference and lists several sessions. A large red "ORACLE OPEN WORLD" logo is positioned to the right of the text. Below the article, there is a "Conference Sessions" section with a date of "Monday, Oct 26". The right sidebar contains sections for "About" (with links for Blog Authors, Certifications, Upgrade Recommendations, FAQ, Webcasts & Training, and Subscribe by Email), "Search" (with a search input field and a "Search only this blog" checkbox), and "Recent Posts" (listing "BPEL 11.1.1.9 Certified for Prebuilt EBS 12.1 and 12.2 SOA Integrations", "E-Business Suite Technology Sessions at OpenWorld 2015", "WebCenter Portal 11.1.1.9 Certified with E-Business Suite 12.1", and "Consultations with ATG Development at OpenWorld 2015").

# Blog: Oracle E-Business Suite and Oracle Cloud

<https://blogs.oracle.com/EBSandOracleCloud/>

- Live since 1<sup>st</sup> June 2016
- 40+ Articles since 1<sup>st</sup> June 2016
- Dedicated to EBS and Oracle Cloud Topics
- Sponsored by EBS Development Executives

[Subscribe by Email](#)

## Oracle E-Business Suite and Oracle Cloud

The latest news direct from E-Business Suite Development


**ORACLE**

[Main](#) | [What is Oracle E-Bus...](#) »

### Welcome to Oracle E-Business Suite and Oracle Cloud Blog

By Nadia Bendjedou-EBS-Oracle on Jun 01, 2016

*[Publisher's note: We are pleased to launch this new blog with the following introductory article by Cliff Godwin, Senior Vice President, Oracle E-Business Suite Development.]*



Welcome to the Oracle E-Business Suite and Oracle Cloud Blog, which will cover all aspects of running Oracle E-Business Suite on Oracle Cloud - including what you can do right now, and what you can plan for as our offerings evolve.

Larry Ellison, Founder and Executive Chairman of Oracle stated, "Coexistence of cloud and on-premises computing is going to be a decades-long process, if not forever".

Oracle has invested extensively in providing solutions to help customers realize the benefits of cloud computing at the infrastructure, platform, and business application levels. These cloud services are broadly grouped as follows:

- Oracle's Infrastructure as a Service (IaaS)
- Oracle's Platform as a Service (PaaS)
- Oracle's Software as a Service (SaaS)

While each Oracle product line (including Oracle E-Business Suite) continues its development roadmap to serve its target markets and customer base, Oracle is actively promoting a coexistence or hybrid model that enables customers to adopt Oracle's cloud services in ways that complement and augment their existing enterprise applications.

Most Oracle E-Business Suite customers will think about embracing cloud computing as a journey, rather than a "big

#### About

- This Blog
- The Authors
- FAQ: EBS on Oracle Cloud
- Oracle Cloud Marketplace
- Subscribe by Email

#### Search

Enter search term:

Search only this blog

#### Recent Posts

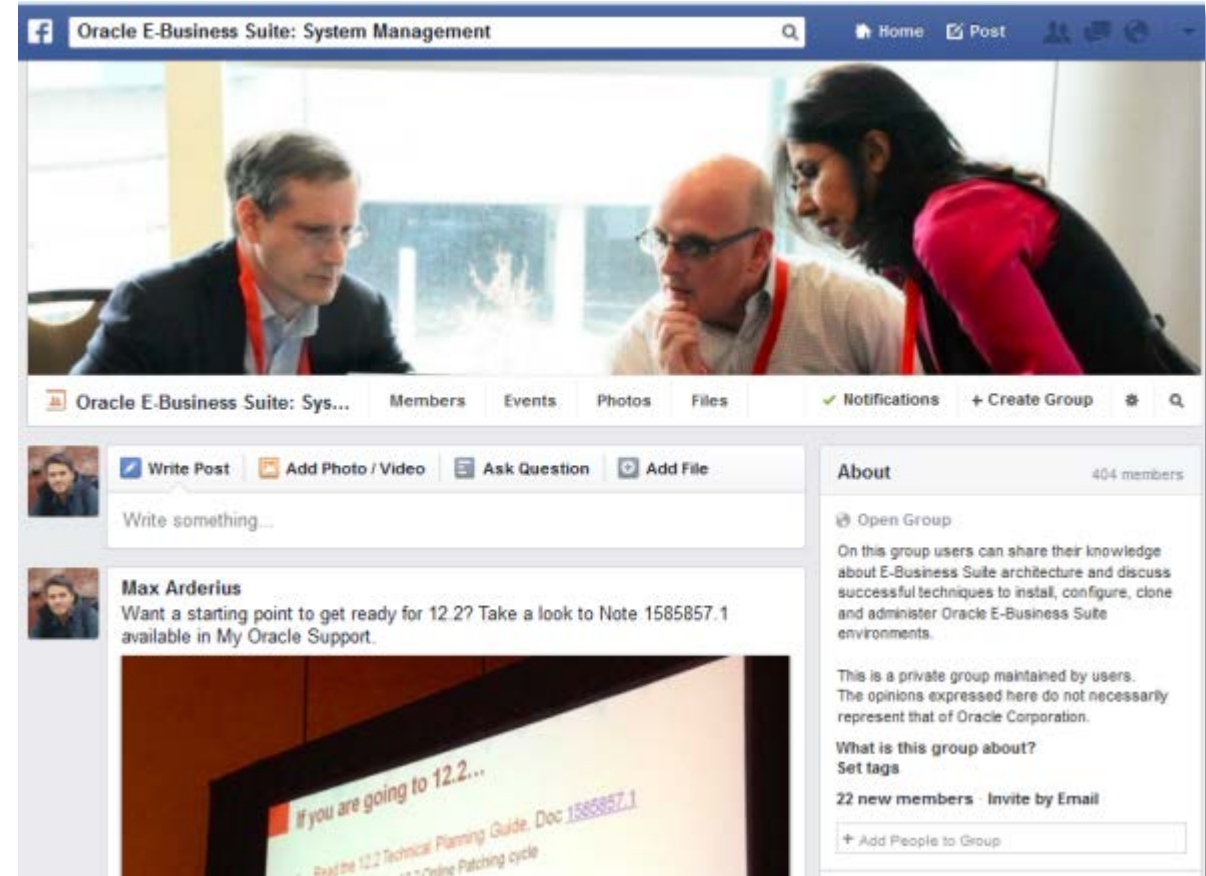
- Provisioning EBS in Oracle Compute Cloud
- EBS Deployment Options on Oracle Cloud
- Getting Started with EBS on Oracle Cloud
- Oracle E-Business Suite on Oracle Cloud - Offerings Available Today



# E-Business Suite: System Management

[facebook.com/groups/EBS.SysAdmin](https://facebook.com/groups/EBS.SysAdmin)

## Join us on Facebook

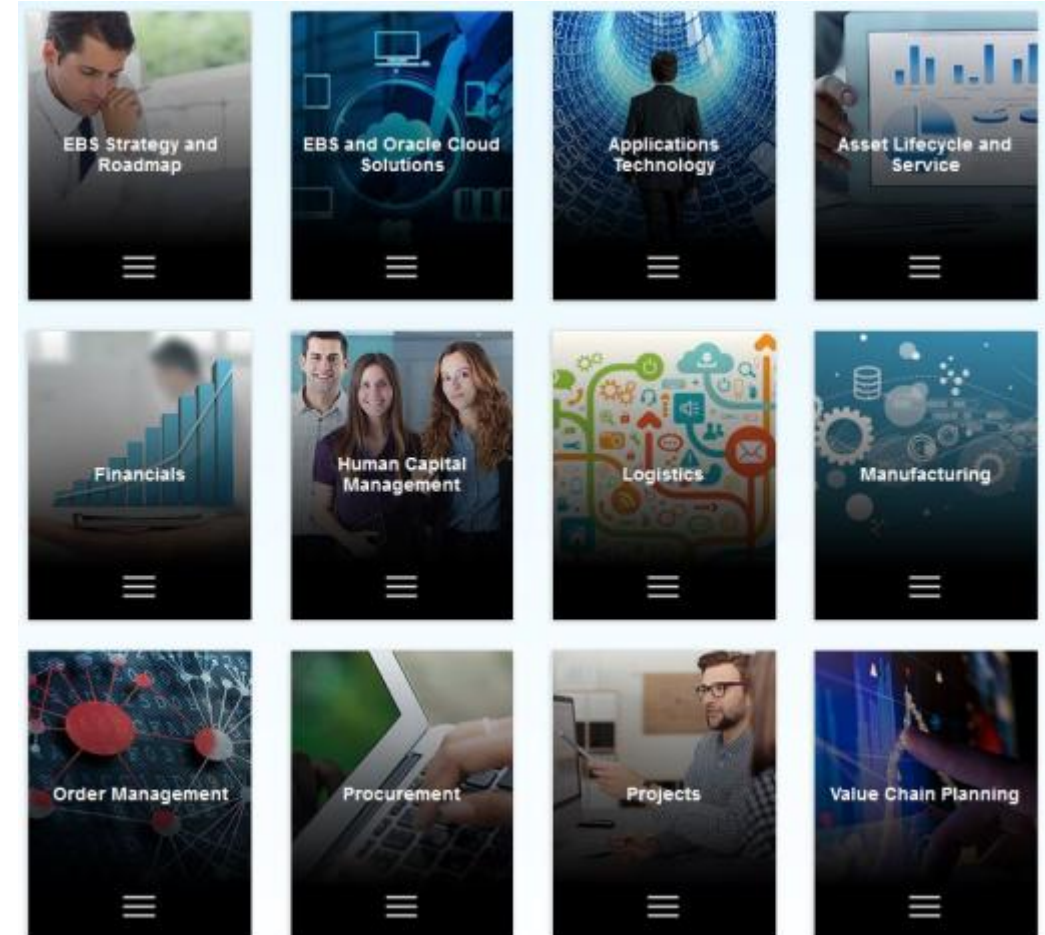


# Oracle E-Business Suite Learning Subscription

## Stay Up-to-Date on Everything Oracle E-Business Suite

- **Free access** to hundreds of videos
  - What's New, Virtual Conference, User Experience, Advice from Development
- Subscription access to over 500 technical and functional training sessions
- Continuous updates and additions

[education.oracle.com/subscriptions/ebs](https://education.oracle.com/subscriptions/ebs)



ORACLE®