

ORACLE®

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

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

August 2019



# 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 ➤ Guidelines for Secure Configuration and Auditing
- 2 ➤ Additional Secure Configuration When Running EBS in Oracle Cloud Infrastructure
- 3 ➤ Roadmap

# Program Agenda

- 1 ➤ Guidelines for Secure Configuration and Auditing
- 2 ➤ Additional Secure Configuration When Running EBS in Oracle Cloud Infrastructure
- 3 ➤ Roadmap

# Oracle E-Business Suite Security

## Documentation

- Security FAQ
  - MOS Note [2063486.1](#)
- Secure Configuration Guides
  - EBS 12.2: *Security Administration Guide, Secure Configuration Chapter*
  - EBS 12.1: [MOS Note 403537.1](#)
- Enabling TLS
  - EBS 12.2: [MOS Note 1367293.1](#)
  - EBS 12.1: [MOS Note 376700.1](#)
- EBS CPUs
  - MOS Note [2484000.1](#)

New

## EBS Security Features

- Secure Configuration Console ✓
  - Tool to assist with secure configuration
  - Easy to see where you are out of compliance
  - Use the console to enable security features or set secure configuration
  - Guidance is provided for items that cannot be turned on via the console
- Allowed Resources ✓
  - Key feature for reducing your attack surface
  - Defines whitelist of allowed resources for Oracle E-Business Suite Release 12.2
  - Prevents access to resources which are not used
- Allowed Redirects ✓
  - Defines whitelist of allowed redirects for Oracle E-Business Suite 12.2

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

# 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

## Follow Our Development Standards

- Developing and Deploying Customizations in Oracle E-Business Suite Release 12.2 (MOS Note 1577661.1)
- Guidance for Integrating Custom and Third-Party Products with Oracle E-Business Suite Release 12.2 (MOS Note 1916149.1)
- Guidance for Providing Access to the Oracle E-Business Suite Database for Extensions and Third-Party Products (MOS Note 2327836.1)



New



# 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 248400.1**

# 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 12.2.8
  - 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
- For EBS 12.2, enable TLS for the WLS Admin Port
- Optional Configurations
  - Configuring “TLS 1.2 Only”
  - Disabling HTTP Port
  - Enabling HTTP Strict Transport Security (HSTS)
  - Enabling TLS from Oracle HTTP Server (OHS) to Application Server (OC4J / WLS)

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

# 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

# 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
- Scripts are available
    - Review MOS Note 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*
    - Setup notification for updates to this MOS Note
  - Download EBSAuditScripts.zip
    - Contains multiple SQL scripts
    - Validate audit configuration
    - Query audit tables
    - Configure database auditing

Oracle E-Business Suite Security Guide Release 12.2, Auditing and Logging Chapter

# 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 %  
Code  
Critical Level  
Config Type  
Status  
☒ Include suppressed security configurations  
Go Clear

Check Fix Suppress Unsuppress |

Details	Status	Severity	Security Guideline	Description	Code	Type
<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"/>	✓	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"/>	✓	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"/>	✓	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"/>	✓	1	<a href="#">Diagnostic Web Pages Protected</a>	Check whether diagnostic web page protection is configured.	DIAG_WEB_PAGE_PROTEC	Manual
<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"/>	✓	1	<a href="#">PUBLIC Privileges</a>	Check whether the PUBLIC role privileges are restricted.	FND_APPS_IND_PUBLIC	Manual
<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"/>	✓	1	<a href="#">Clickjacking Protection</a>	Check whether clickjacking protection is configured.	CLICKJACK_PROTECTION	Manual
<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

<div>Check Configure Suppress Unsuppress</div>			
<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
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 ]			
<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
<b>Security Guideline</b>
Application Users Default Password
<b>Description</b>
Check whether all application users default passwords have been changed to non-default values.
<b>Detailed Info</b>
<p>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.</p> <p>Note that this will not list shipped accounts that cannot be used for login (disabled/end dated accounts).</p> <p>Refer to the following for additional information:</p> <ul style="list-style-type: none"><li>• Oracle E-Business Suite Security Guide, Release 12.2 &gt; Oracle E-Business Suite Security &gt; Authentication &gt; Change Passwords for Seeded Application User Account</li></ul>

# 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 Server security (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**

# Secure Configuration Console

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

The screenshot shows the 'Secure Configuration Console' interface. At the top, there are tabs for 'Security', 'Core Services', 'Personalization', 'File Manager', 'Portletization', 'Configuration Manager' (selected), and 'Allowed Resources'. Below the tabs, the 'Configuration Management' section is visible, followed by the 'Secure Configuration Console' title with a star icon. A search section contains filters for 'Name' (with a '%' wildcard), 'Code', 'Config Type' (dropdown), 'Status' (dropdown), and 'Critical Level' (dropdown). There is a checkbox for 'Include suppressed security configurations' and 'Go'/'Clear' buttons. Below the search section is a table with columns: 'Check', 'Fix', 'Suppress', 'Unsuppress', 'Details', 'Status', 'Severity', 'Security Guideline', 'Description', 'Code', and 'Type'. The table lists several security guidelines, with the first one, 'Database Password Profiles', having a status of 'x' (failed) and a severity of 2. The other guidelines have a status of '✓' (passed) and a severity of 1. The table also includes navigation links like 'Previous', '1-10', and 'Next 10'.

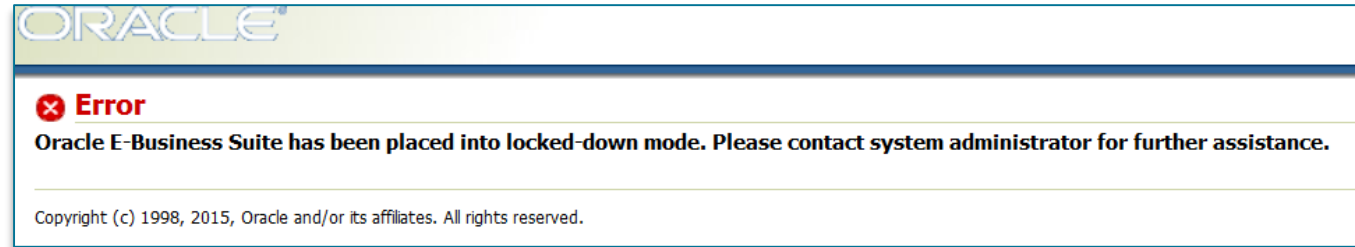
Check	Fix	Suppress	Unsuppress	Details	Status	Severity	Security Guideline	Description	Code	Type
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	x	2	Database Password Profiles	Check if secure configuration recommended database 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

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 Resources

# Feature Overview for Allowed Resources

- Allowed JSPs introduced in E-Business Suite 12.2.4
  - Enabled by default with E-Business Suite ATG 12.26
- 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 for Allowed Resources

## Principles

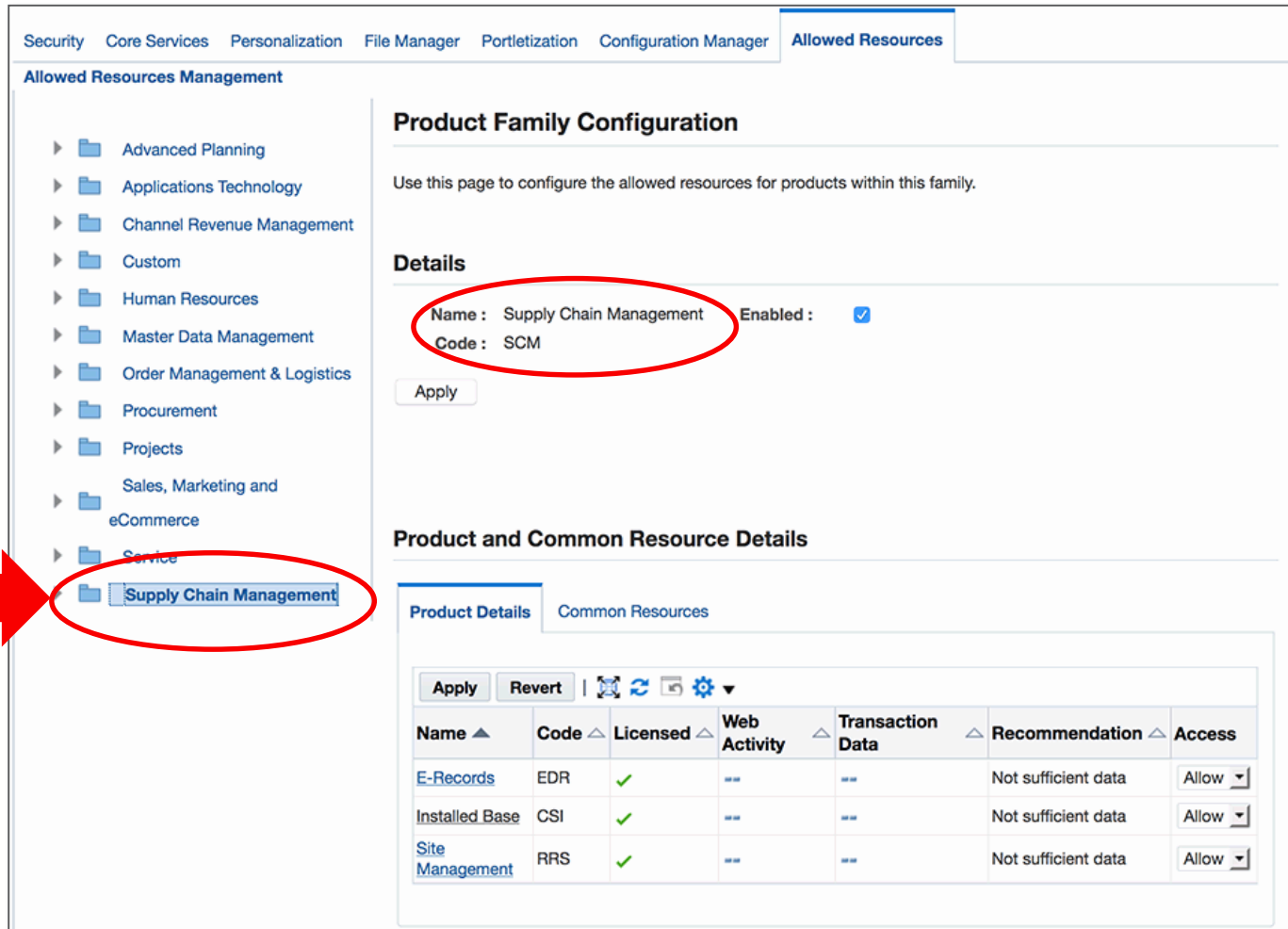
- Enhancements to Allowed JSPs feature
- Defines **whitelist** of web allowed resources
  - A whitelist is an explicit list of items that are allowed for access
- Prevents access to resources which are not used
- Enables configuration of actively allowed resources to avoid unnecessary exposure
- Allows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



# Feature Overview of Allowed Resources

- Whitelist resources including servlets and JSPs
- Metadata stored in the database (not in configuration files)
- User interface to manage resources by product hierarchy and by resource
- 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 are provided

# 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

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

**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	Not sufficient data	Not sufficient data	Allow ▼
<a href="#">Installed Base</a>	CSI	✓	Not sufficient data	Not sufficient data	Not sufficient data	Allow ▼
<a href="#">Site Management</a>	RRS	✓	Not sufficient data	Not sufficient data	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.

# 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
- Identity Cloud Service (IDCS) integration for single sign-on
- Any custom redirects used in your environment

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

# Recent Announcements

# Recent Announcements - Oracle E-Business Suite Security



## EBS Secure Configuration

1. Nosniff
2. HTTPOnly Cookie Flag
3. HTTP Strict Transport Security (HSTS)
4. Elliptic Curve Cryptography
5. Lockdown WLS Traffic  
Encrypt WLS Admin Port

## Defense Against

1. Meltdown/Spectre
2. Cross-site scripting (XSS)
3. Man-in-the-middle attacks
4. TLS cipher attacks
5. WLS attacks



# Features for HTTP Headers

- **Nosniff** - Header response code that prevents browsers from "reinterpreting" the mime type of a file
  - Available for all EBS 12.2.x releases and EBS 12.1.3
  - Apply October 2018 CPU, *Oracle E-Business Suite Release 12 Critical Patch Update Knowledge Document (October 2018)* (Doc ID 2445688.1)
- **HTTPOnly Cookie Flag** - EBS session (aka ICX session) cookie cannot be accessed from browser via script/code
  - Available for all EBS 12.2.x releases
    - Apply R12.ATG\_PF.C.DELTA.7 (24690680)
    - Enable Java Web Start, *Using Java Web Start with Oracle E-Business Suite* (Doc ID 2188898.1)
  - Backport in progress EBS 12.1.3

## Features for HTTP Headers

- **HTTP Strict Transport Security (HSTS)** - specifies a time period that browsers will communicate using only HTTPS
  - Optional configuration available for all EBS 12.2.x releases and EBS 12.1.3
  - Deployment recommendations:
    - This feature should be configured at the TLS termination point (for example: Oracle HTTP Server (OHS), Load-balancer)
    - Either use the default HTTPS port (443) or specify the HTTPS port in all URLs
    - When testing HSTS, start the configuration using short time periods

EBS 12.2: 1367293.1, EBS 12.1: 376700.1

# Recent Certificate Certifications for EBS 12.2 and 12.1.3

- Elliptic Curve Cryptography
  - 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
- Subject Alternative Name (SAN) & Wildcard Certificates
  - 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

# Lockdown WebLogic Server (WLS) Traffic

## Oracle E-Business Suite 12.2.x

- Apply April 2019 CPU (or perform manual configuration)
  - *Oracle E-Business Suite Release 12 CPU Knowledge Document (April 2019) (Doc ID 2514102.1)*
- Allow Direct Access to WLS from Trusted Hosts
  - Trusted hosts include known web entry points via the Oracle HTTP Server (OHS)  
Note: You will need to add trusted hosts for administrative access to WLS Admin Console
- Disable Web Services Atomic Transactions
  - Disables protocol not required by EBS
  - Perform required configuration steps as per the documentation

Oracle E-Business Suite 12.2 Setup Guide,  
Technical Configuration → Managing Configuration of Web Application Services

# Lockdown WebLogic Server (WLS) Traffic

## Oracle E-Business Suite 12.2.x – April 2019 CPU Configuration

### Required Configuration for WLS Administration Console Access

- Option 1: Adding Specific Trusted Hosts

Use the context variable **s\_wls\_admin\_console\_access\_nodes** to add trusted hosts used by administrators that require access to the Oracle WebLogic Server Administration Console

- Option 2: Allowing an IP Range

Allow a range of IP addresses access to Oracle WebLogic Administration ports by manually configure network connection filter rules in the Oracle WebLogic Server Administration Console.

- Option 3: Using SSH Tunneling

Setup SSH tunneling for administrators who have OS access and need to access the Weblogic Server Administration ports.

**MOS Note 2542826.1**

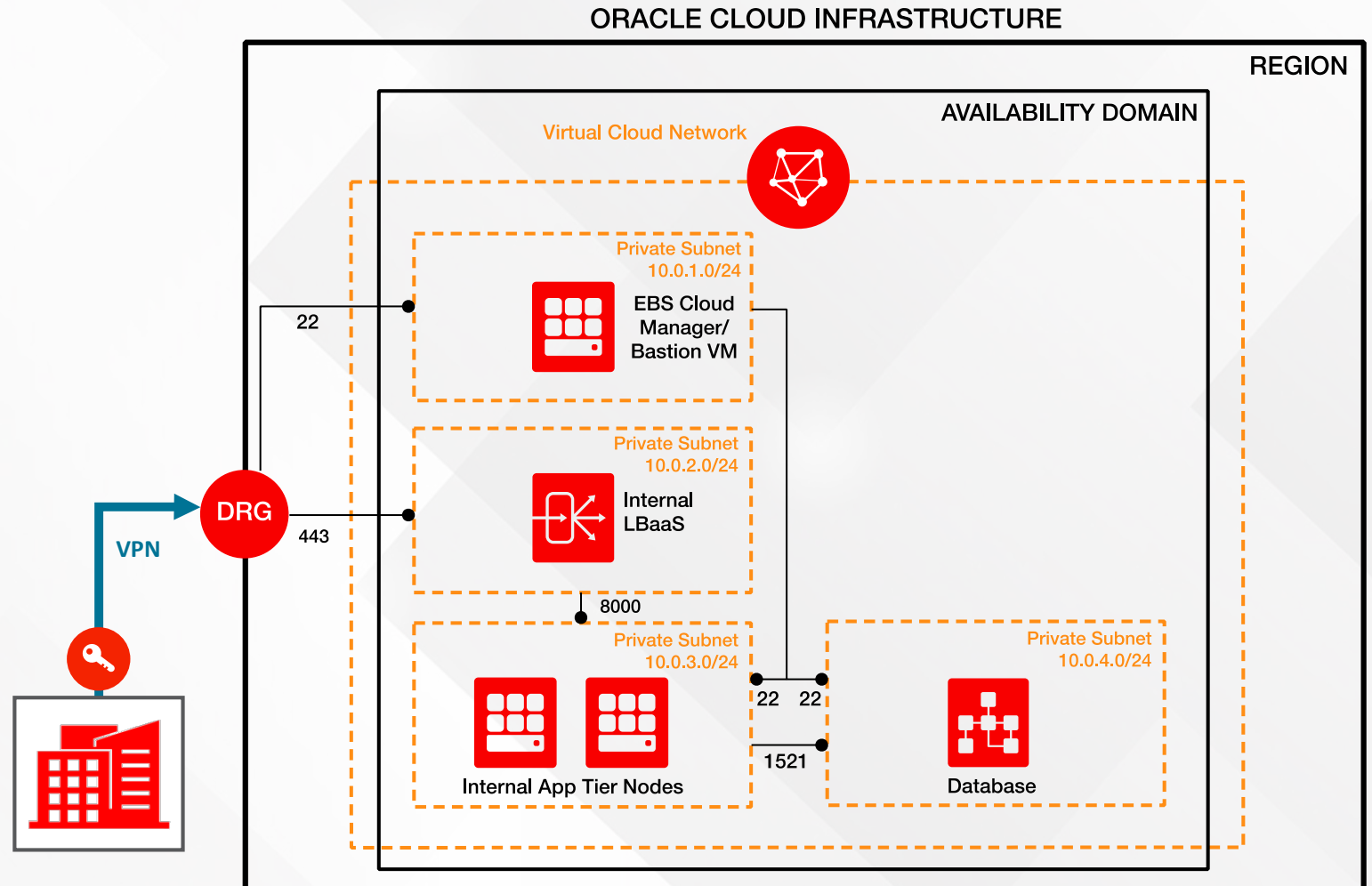
# Program Agenda

- 1 Guidelines for Secure Configuration and Auditing
- 2 Additional Secure Configuration When Running EBS in Oracle Cloud Infrastructure
- 3 Roadmap

# Oracle E-Business Suite on OCI – Secure Configuration

## Reduce Your Attack Surface

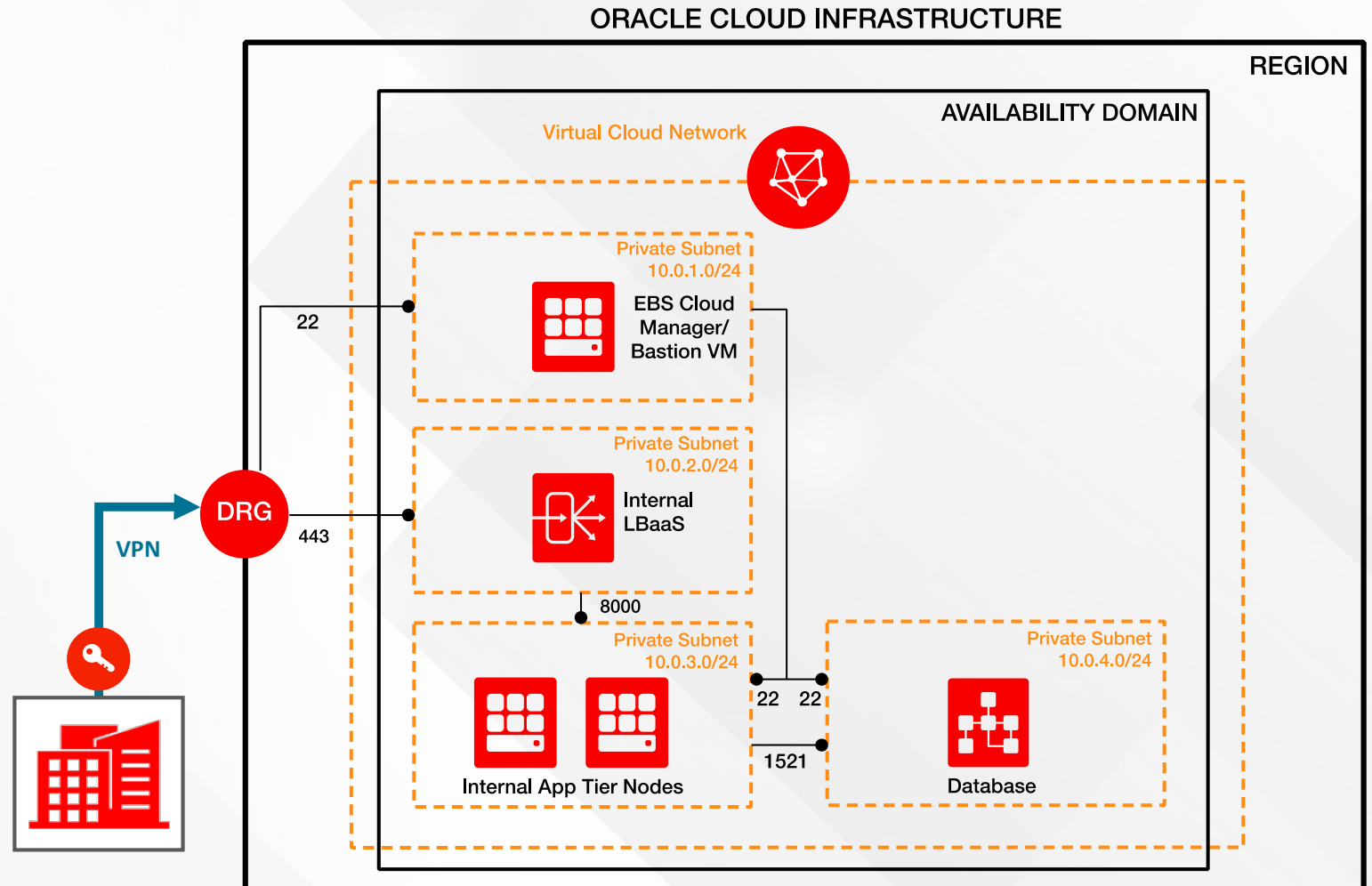
- Define Security Lists and Security Rules
  - Ensure that:
    - Ports are only accessible as required
    - Only the SSH and HTTPs ports are exposed externally
  - Never expose the following externally:
    - WLS Admin Ports
    - DB Listener Port



# Oracle E-Business Suite on OCI – Secure Configuration

## Reduce Your Attack Surface

- Use DRG with VPN
  - Alternatively, use IGW with Security IP Lists
- Deploy EBS components (VMs, LBRs) in private subnets
- Deploy each EBS component in a separate private subnet





# Guidance for Defining Network Resources

MOS Doc ID 2434500.1, Section 6

- [Section 1: Before You Begin](#)
- [Section 2: Create Oracle Cloud Infrastructure Accounts and Resources](#)
- [Section 3: Create Network Resources For Deploying Oracle E-Business Suite Cloud Manager](#)
- [Section 4: Create Oracle E-Business Suite Cloud Manager Compute Instance](#)
- [Section 5: Configure Oracle E-Business Suite Cloud Manager Compute Instance](#)
- [Section 6: Create Network Resources For Deploying Oracle E-Business Suite Instances](#)
- [Section 7: Prepare Oracle E-Business Suite Administrator Credentials \(Conditional\)](#)

# Guidance for Defining Network Resources

MOS Doc ID 2434500.1, Section 6

## Section 6: Create Network Resources For Deploying Oracle E-Business Suite Environments

**Note:** You must configure the Oracle E-Business Suite Cloud Manager Compute instance ([Section 5](#)) prior to performing these steps. The network administrator and the Oracle E-Business Suite Cloud Manager administrator perform these tasks as indicated in each task of this section.

Before the Oracle E-Business Suite Cloud Manager can be used to provision environments, a network and associated network profiles must be created. A network profile maps OCI network definitions with Oracle E-Business Suite instances network requirements.

When creating a network, the network administrator has two choices:

- **Default Network** - [Section 6.1](#) provides guidance for the network administrator who wishes to create a default network and two default network profiles, one for One-Click Provisioning and one for Advanced Provisioning using provided scripts ([Section 6.1.1](#)), and to the Oracle E-Business Suite Cloud Manager administrator who will subsequently upload the network profiles for One-Click Provisioning and Advanced Provisioning ([Section 6.1.2](#)).
- **Custom Network** - [Section 6.2](#) provides guidance for the network administrator who wishes to create custom network elements ([Section 6.2.1](#)), and to the Oracle E-Business Suite Cloud Manager Administrator who will subsequently use these elements in the definition of custom network profiles ([Section 6.2.2](#)).

# Guidance for Securing Admin Traffic

## MOS Doc ID 2517025.1, Section 6.2.1: Provisioning Oracle E-Business Suite

Table 2 - Options for One-Click Provisioning

Products Available for Deployment <sup>3</sup>	Cloud Service For Application and Database Tier
<b>Vision Demo Installation</b> <ul style="list-style-type: none"><li>• Oracle E-Business Suite Release 12.2.8 with Oracle Database 12.1.0.2</li></ul>	<ul style="list-style-type: none"><li>• Oracle Cloud Infrastructure Compute VM</li></ul>

<sup>3</sup> One-Click Provisioning has been enhanced to use an Oracle Cloud Infrastructure image and place the application and database tier on a single compute instance. Other Vision demo installation and fresh installation release combinations previously available from One-Click Provisioning are available from Advanced Provisioning.

Follow these Oracle by Example tutorials in the order shown below, for instructions related to provisioning a new Oracle E-Business Suite environment on Oracle Cloud Infrastructure using **One-Click Provisioning** in Oracle E-Business Suite Cloud Manager.

1. [Accessing Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure](#)
2. [Using One-Click Provisioning in Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure](#)
3. [Reviewing Activity Status in Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure](#)
4. [Reviewing Environment Details in Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure](#)
5. [Performing Post-Provisioning and Post-Cloning Tasks for Oracle E-Business Suite on Oracle Cloud Infrastructure](#)
6. [Accessing the Fusion Middleware Control and WebLogic Server Administration Console with SSH Port Forwarding for Oracle E-Business Suite on Oracle Cloud Infrastructure](#)

# Guidance for Securing Admin Traffic

## FMW Control and WLS Admin Console (WLS Admin Port)

### 1 Perform one-time configuration

Go to the following OBE to configure the required security and firewall rules

*Performing Post-Provisioning and Post-Cloning Tasks for Oracle E-Business Suite on Oracle Cloud Infrastructure*

For every Oracle E-Business Suite environment on OCI, perform the steps listed in the following section

*Configure Security and Firewall Rules for Secure Access to the Fusion Middleware Control and WebLogic Server*

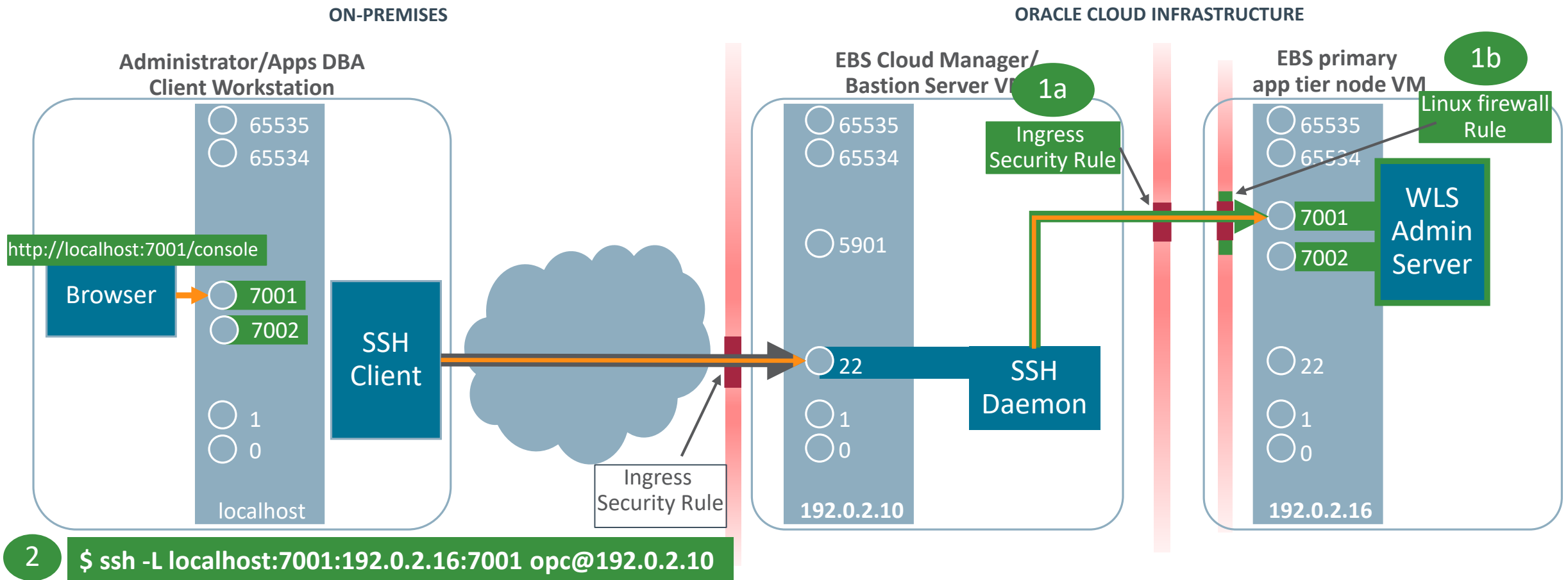
### 2 Repeat setup per every new client connection

Go to the following OBE and perform the instructions to establish an SSH tunnel from the client

*Accessing the Fusion Middleware Control and WebLogic Server Administration Console with SSH Port Forwarding for Oracle E-Business Suite on Oracle Cloud Infrastructure*

# Guidance for Securing Admin Traffic

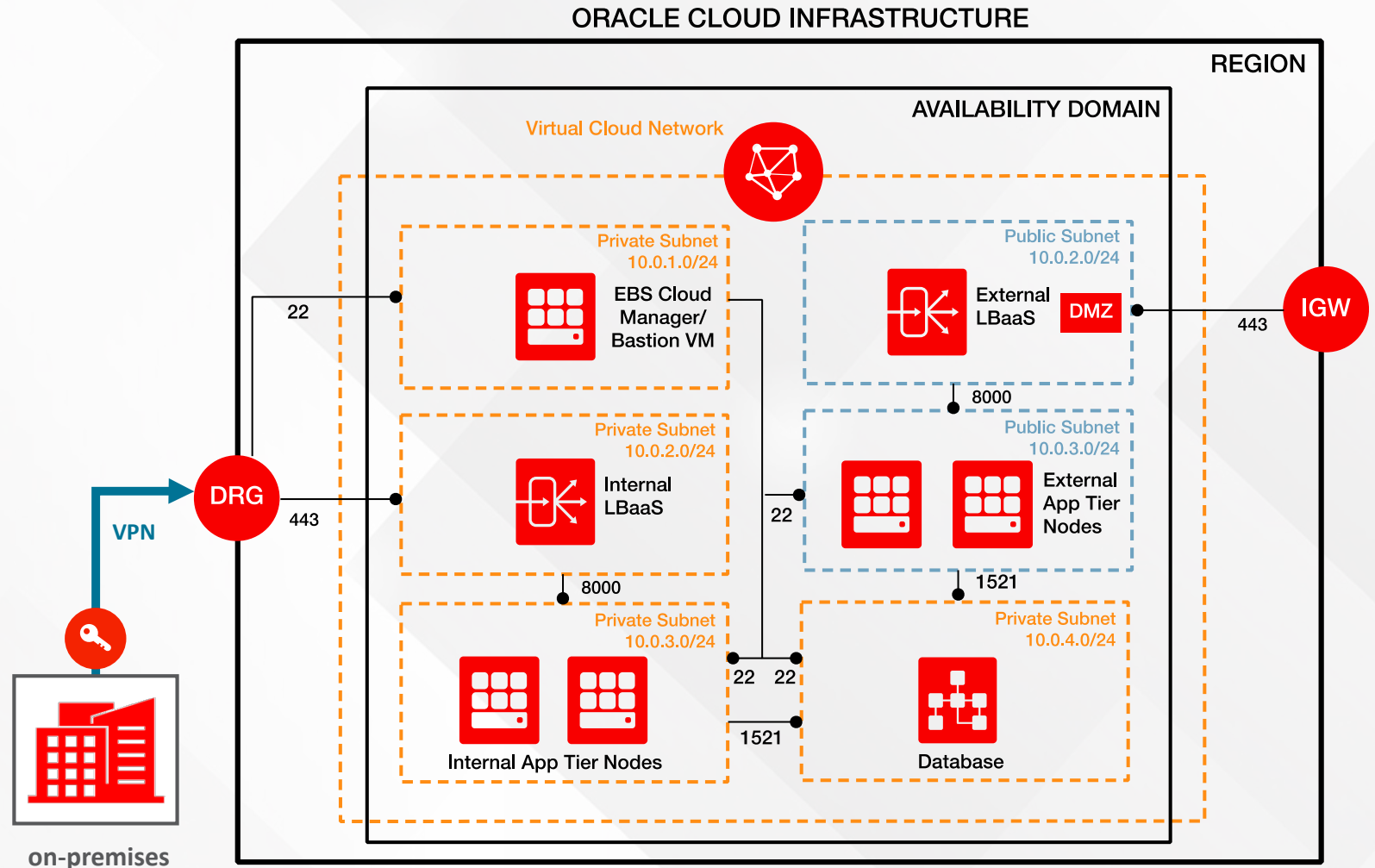
## FMW Control and WLS Admin Console (WLS Admin Port)



# Oracle E-Business Suite on OCI – Secure Configuration

## Reduce Your Attack Surface

- Follow DMZ guidelines for accessing EBS from the Internet
  - Limited number of Oracle E-Business Suite products certified for internet
  - MOS Notes
    - EBS 12.2: 1375670.1
    - EBS 12.1: 380490.1

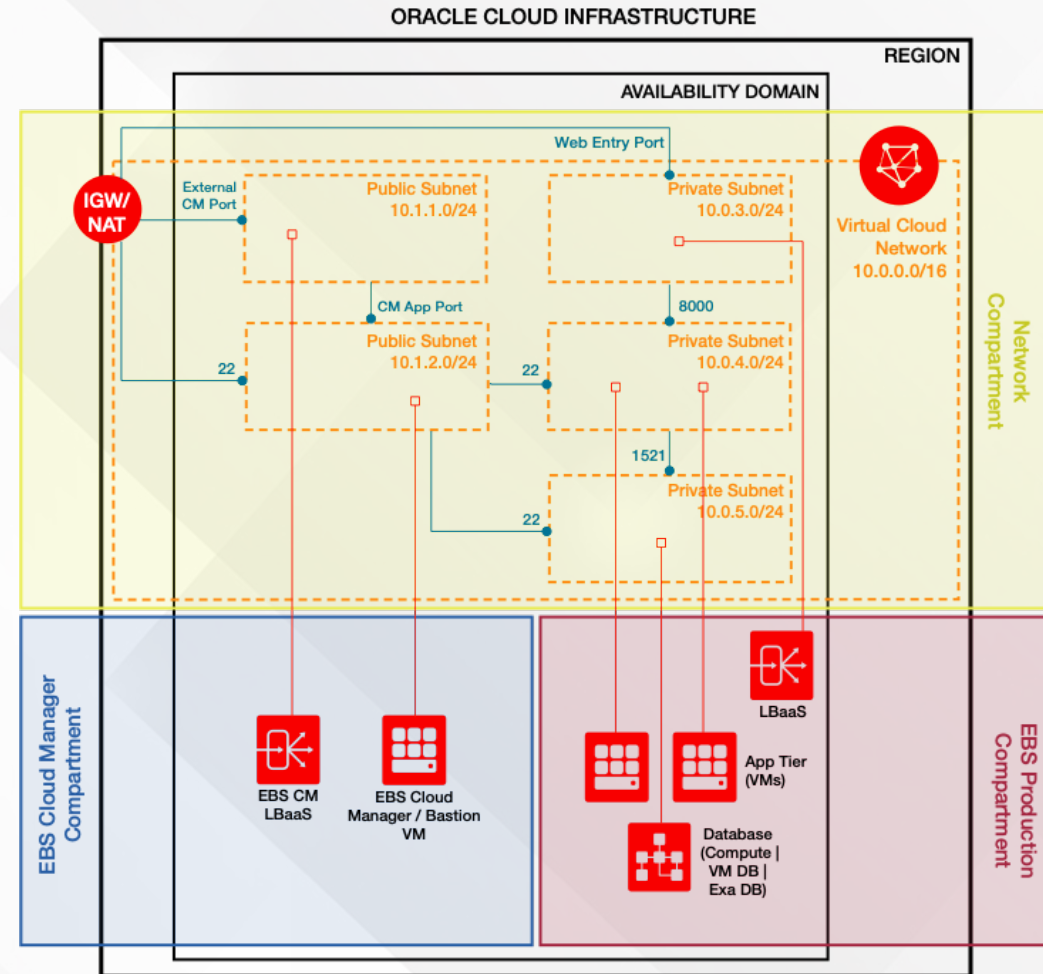




# Oracle E-Business Suite on OCI – Secure Configuration

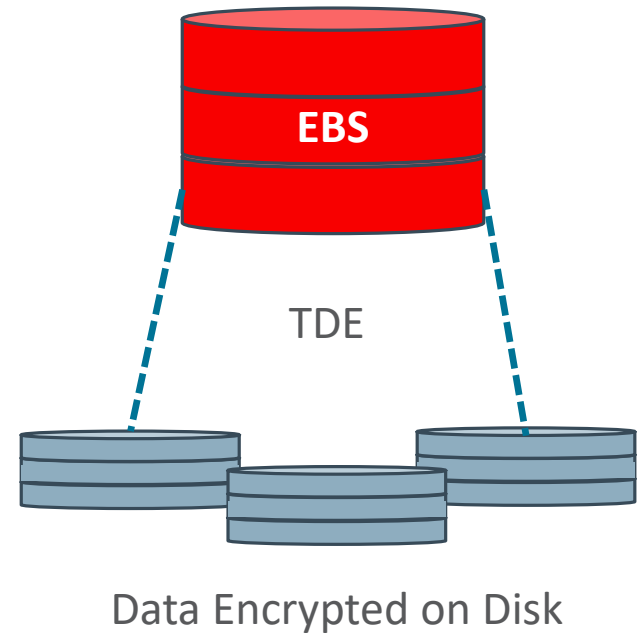
## Secure Administrative Access

- Follow the Principle of Least Privilege (PoLP)
  - Define Roles (Separation of Duties)
    - DBAs, Network Administrators
  - Use Compartments
- Route administrator access through a Bastion server



# Transparent Data Encryption

- Automatically enabled for all EBS Databases running on DBaaS
  - New installs, lift and shift
- Optionally enabled for EBS Databases deployed to Compute
  - Bring Your Own License (BYOL)





# Program Agenda

- 1 Guidelines for Secure Configuration and Auditing
- 2 Additional Secure Configuration When Running EBS in Oracle Cloud Infrastructure
- 3 Roadmap

# Oracle E-Business Suite Security

- Oracle E-Business Suite Release 12.1.3
  - Backport Allowed Resources Feature
- Oracle E-Business Suite Release 12.2 and Release 12.1
  - Ongoing updates to documented security guidelines (e.g., DB Access Control List)
  - Add more Secure Configuration Console checks (e.g., Default WLS Admin password)
  - Improve recommendations based upon activity for Allowed Resources
  - Automate configuration of resource level lockdown for Allowed Resources

# Allowed Resources – Management by Resource

## Ease of Configuration – Deny All Resources Not Accessed

**Resource Management**  
Access data collected since 2017-07-31

1075  
Allowed - but Never Accessed

40  
Allowed - Sorted by Last Access Date

40  
Allowed - Sorted by Access Count

1132  
Allowed Resources

1541  
Denied Resources

2669  
All Resources

Personalize Flow Layout: (neverUsedResourcesRN)  
Personalize Query: (neverUsedResourcesSearch)

New Search Hide Filters Table Diagnostics

**Filters**

Resource Name  
is ▼

Resource Type  
is ▼

Go Save Add ▼

<input type="checkbox"/> Deny	<input type="checkbox"/> Deny All	<input type="checkbox"/>
Resource Name ▲		Resource Type ▲
<input type="checkbox"/>	/OA_HTML/APECCTableActionsPost.jsp	JSP
<input type="checkbox"/>	/OA_HTML/APTableActionsPost.jsp	JSP
<input type="checkbox"/>	/OA_HTML/AnonymousLogin.jsp	JSP
<input type="checkbox"/>	/OA_HTML/AppsPwdChange	Servlet URL
<input type="checkbox"/>	/OA_HTML/AppsTCFServer	Servlet URL
<input type="checkbox"/>	/OA_HTML/AuthenticateUser	Servlet URL
<input type="checkbox"/>	/OA_HTML/BIExport	Servlet URL
<input type="checkbox"/>	/OA_HTML/BarcodeImageServlet	Servlet URL
<input type="checkbox"/>	/OA_HTML/BneAdminServlet	Servlet URL

◀ Previous 1 - 20 ▼ Next 20 ▶

# Allowed Resources – Management by Resource

## Ease of Configuration – See All Resources Used

**Resource Management**  
Access data collected since 2017-07-31

1075  
Allowed - but Never Accessed

40  
Allowed - Sorted by Last Access Date

40  
Allowed - Sorted by Access Count

1132  
Allowed Resources

1541  
Denied Resources

2669  
All Resources

Personalize Flow Layout: (allowedResByLastAccessRN)  
Personalize Query: (allowedResByLastAccessSearch)

New Search ▾ Hide Filters Table Diagnostics

**Filters**

Resource Name  
is ▾

Resource Type  
is ▾

Last Access Date  
is ▾

Access Count  
is ▾

Go Save Add ▾

Deny   ...	Resource Name ▴	Resource Type ▴	Access Count ▴	Last Access I
<input type="checkbox"/>	/OA_HTML/indgfm.jsp	JSP	1	05-Dec-2017
<input type="checkbox"/>	/OA_HTML/csiCreateInstMain.jsp	JSP	6	16-Feb-2018
<input type="checkbox"/>	/OA_HTML/csiLOV.jsp	JSP	19	16-Feb-2018
<input type="checkbox"/>	/OA_HTML/jtfalout.jsp	JSP	1	19-Feb-2018
<input type="checkbox"/>	/OA_HTML/jtfbookmark.jsp	JSP	1	19-Feb-2018
<input type="checkbox"/>	/OA_HTML/jtfdcall.jsp	JSP	6	22-Feb-2018
<input type="checkbox"/>	/OA_HTML/help	Servlet URL	1	05-Mar-2018
<input type="checkbox"/>	/OA_HTML/BneCreateDocumentService	Servlet URL	1	02-Apr-2018
<input type="checkbox"/>	/OA_HTML/oaj2se.exe	Executable	11	15-Jul-2018
<input type="checkbox"/>	/OA_HTML/jsp/fnd/AOLDataStreaming.jsp	JSP	43	28-Nov-2018
<input type="checkbox"/>	/OA_HTML/oags	Servlet URL	20	05-Jan-2019
<input type="checkbox"/>	/OA_HTML/jsp/edr/EDRRuleXMLPublisherHandler.jsp	JSP	41	18-Jan-2019

# Allowed Resources – Management by Resource

## Ease of Configuration – See All Denied Resources

**Resource Management**  
Access data collected since 2017-07-31

1075  
Allowed - but Never Accessed

40  
Allowed - Sorted by Last Access Date

40  
Allowed - Sorted by Access Count

1132  
Allowed Resources

1541  
Denied Resources

2669  
All Resources

Personalize Flow Layout: (deniedResourcesRN)  
Personalize Query: (deniedResourcesSearch)

New Search [Hide Filters](#) [Table Diagnostics](#)

**Filters**

Resource Name  
is

Resource Type  
is

Access Count  
is

Denied Date  
is

[Go](#) [Save](#) [Add](#)

<input type="checkbox"/>	Resource Name ▲	Resource Type ▲	Access Count ▲	Last Access Date ▲	Denie
<input type="checkbox"/>	/OA_HTML/AsiZipDownloadControl	Servlet URL	0		14-Me
<input type="checkbox"/>	/OA_HTML/CZIFrame.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrGrpDetail.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrGrpDetailProcess.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrGrpHierProcess.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrGrpHierarchy.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrGrpMbrShowHist.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrGrpShowAll.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrResRoleShowHist.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrRoleDetail.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrRoleSearch.jsp	JSP	0		14-Me
<input type="checkbox"/>	/OA_HTML/JtfrRoleSum.jsp	JSP	0		14-Me

# Additional Resources

# 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**

# 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 TLS in Oracle E-Business Suite Release 12.1	376700.1



# 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)**

<b>Home</b>	<b>Oracle E-Business Suite Release 12.2 Highlights</b>
<b>Reference Information</b>	<b>Start Here</b> <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>
-Product Release Notes 12.2.2 -Product Release Notes 12.2.3 -Product Release Notes 12.2.4 -Product Release Notes 12.2.5	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>
Globalization Center	<b>Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation</b>
Additional Resources	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>
Product Info Centers	<b>Information Center: Oracle E-Business Suite Extensions for Oracle Endeca Install &amp; Configure</b>
R11i Info Center	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>
R12.0 Info Center	<b>Oracle E-Business Suite Releases 12.1 and 12.2 Release Content Documents</b>
R12.1 Info Center	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>
<b>R12.2 Info Center</b>	<b>Using the Online Patching Readiness Report in Oracle E-Business Suite Release 12.2</b>
<b>Lifecycle Management</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>
Install	<b>Oracle E-Business Suite Release 12.2: Consolidated List of Patches and Technology Bug Fixes</b>
Implement	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>
Manage	<b>Applying the Latest AD and TXK Release Update Packs to Oracle E-Business Suite Release 12.2</b>
Upgrade	
Legislative Updates Center	

# Blog: Oracle E-Business Suite Technology Blog

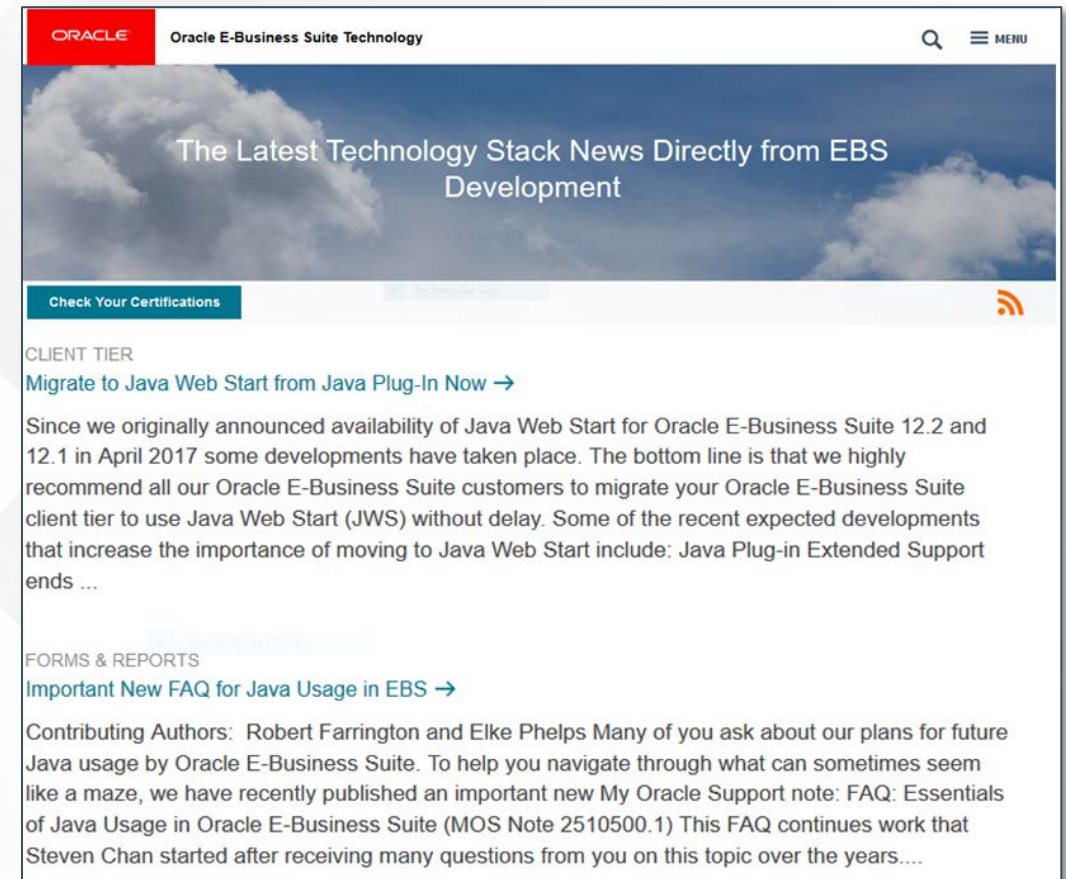
**New URL** <https://blogs.oracle.com/ebstech> (previously [blogs.oracle.com/stevenchan](https://blogs.oracle.com/stevenchan))

- Same blog, new URL

Note: [blogs.oracle.com/stevenchan](https://blogs.oracle.com/stevenchan) will automatically redirect to [blogs.oracle.com/ebstech](https://blogs.oracle.com/ebstech)

- News about EBS Technology
- Certification announcements
- Quarterly upgrade recommendations
- Primers, FAQs, tips
- Statements of Direction
- Desupport reminders

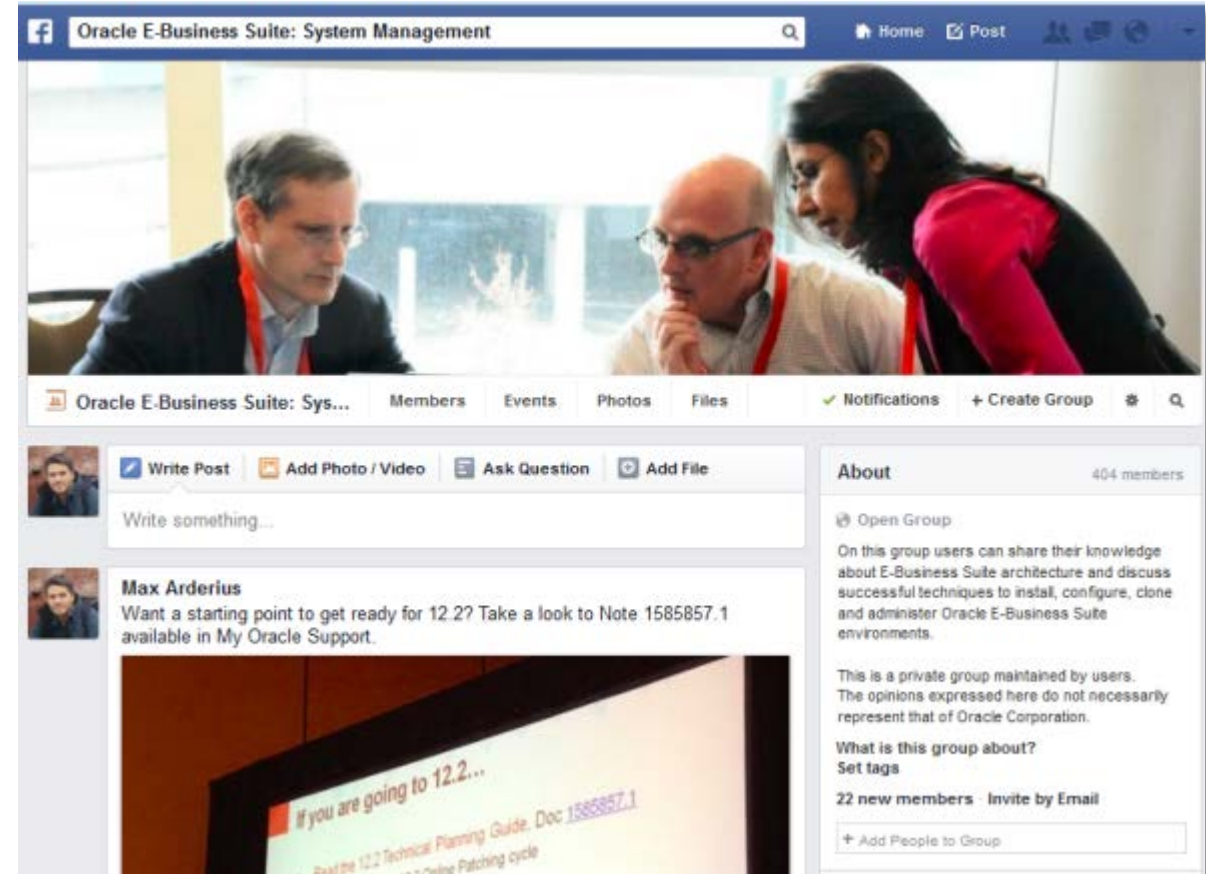
**Subscribe via RSS or email**



# E-Business Suite: System Management

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

## Join us on Facebook

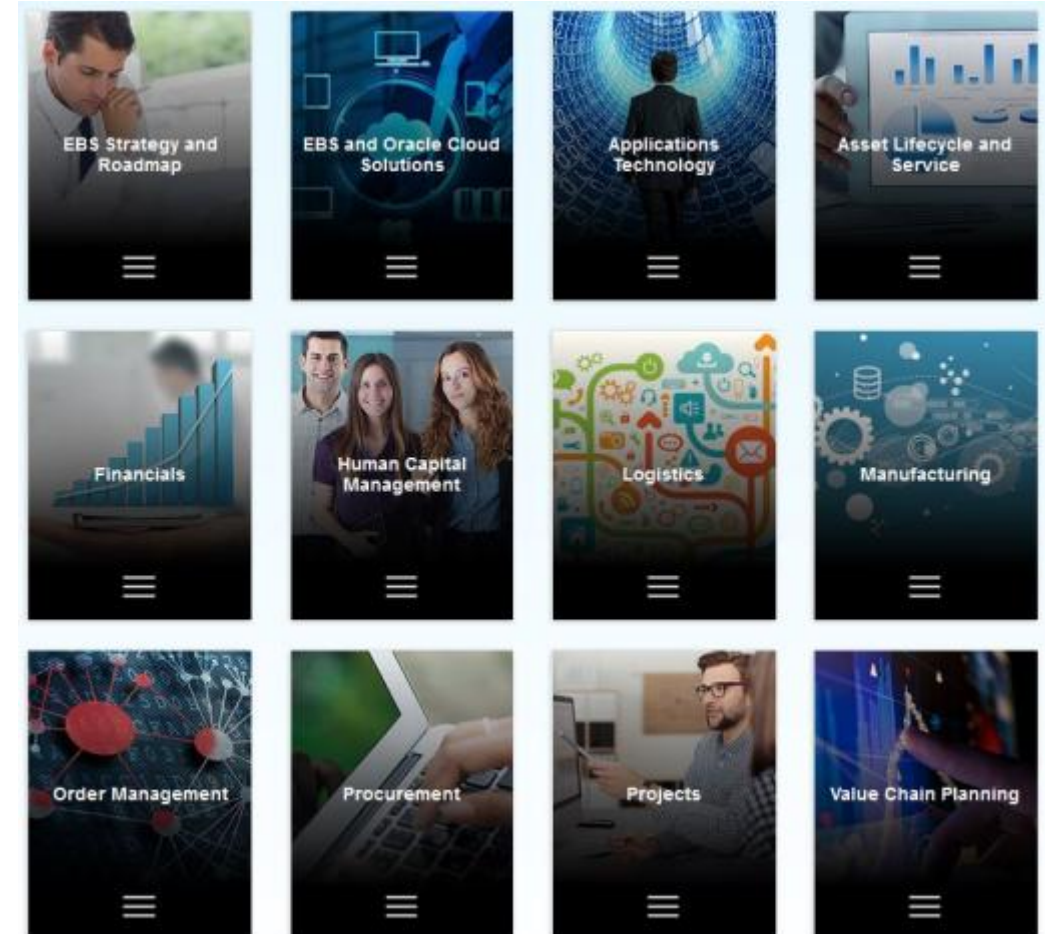


# Oracle E-Business Suite Learning Subscription

## 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

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



ORACLE®