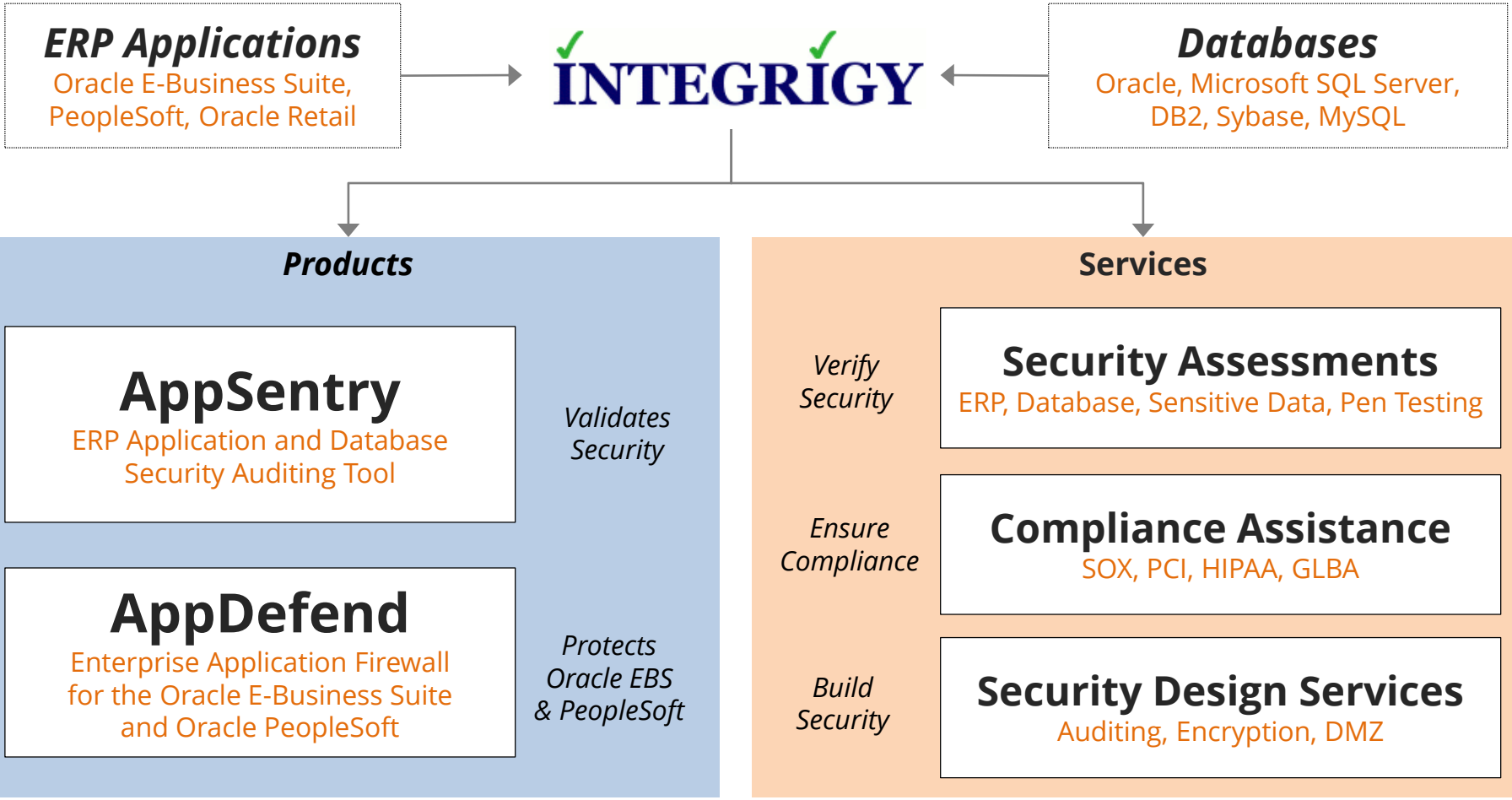
New Oracle EBS Security Features You Can Use Now

November 7, 2018

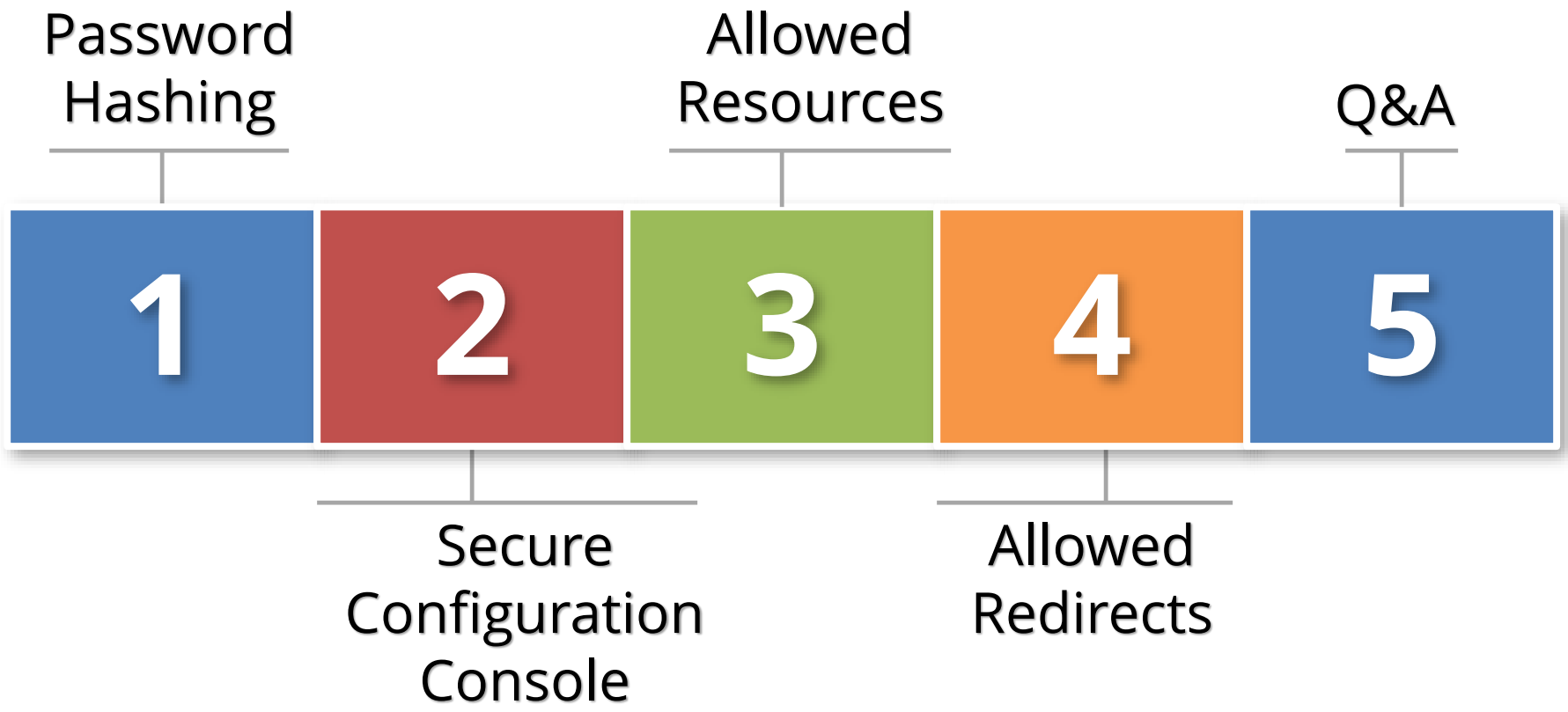
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

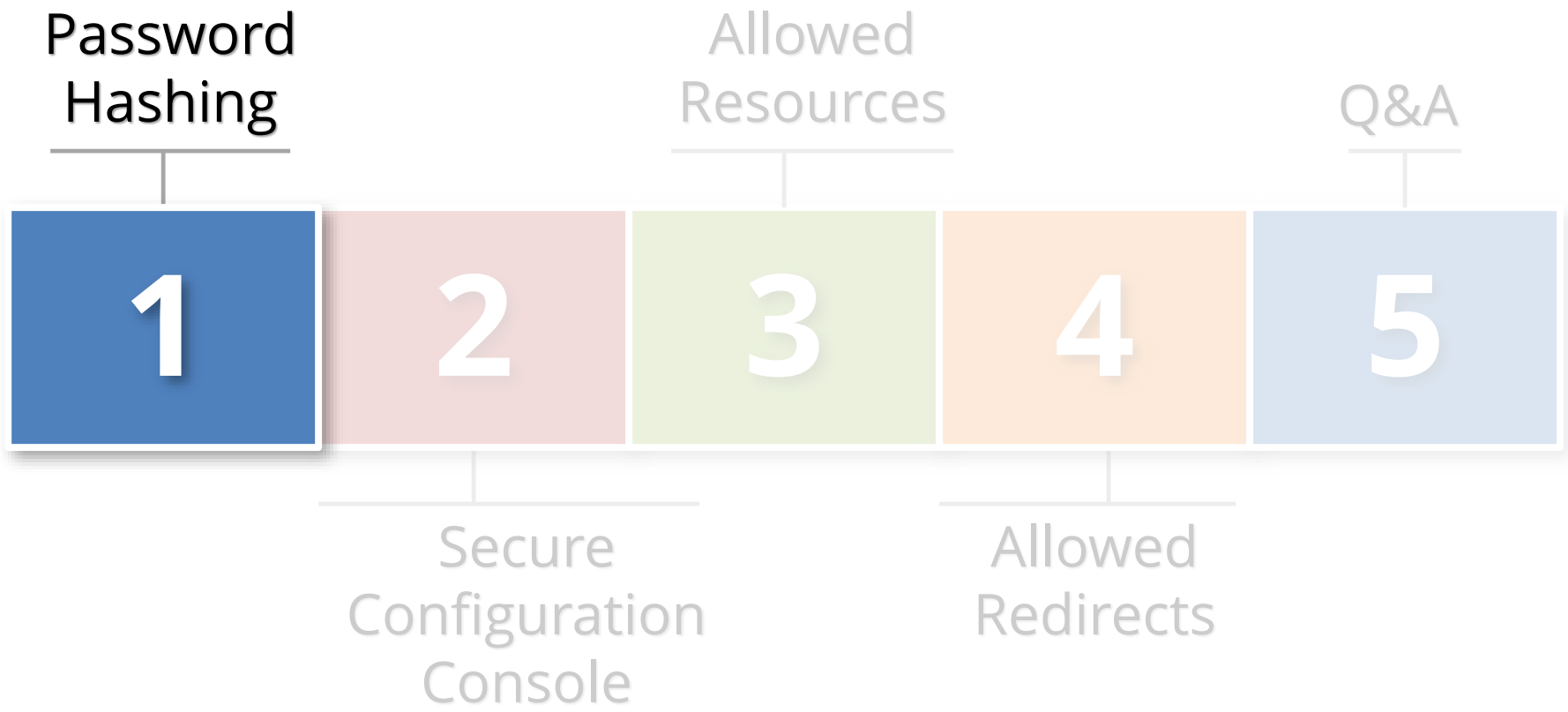
About Integrigy



Agenda

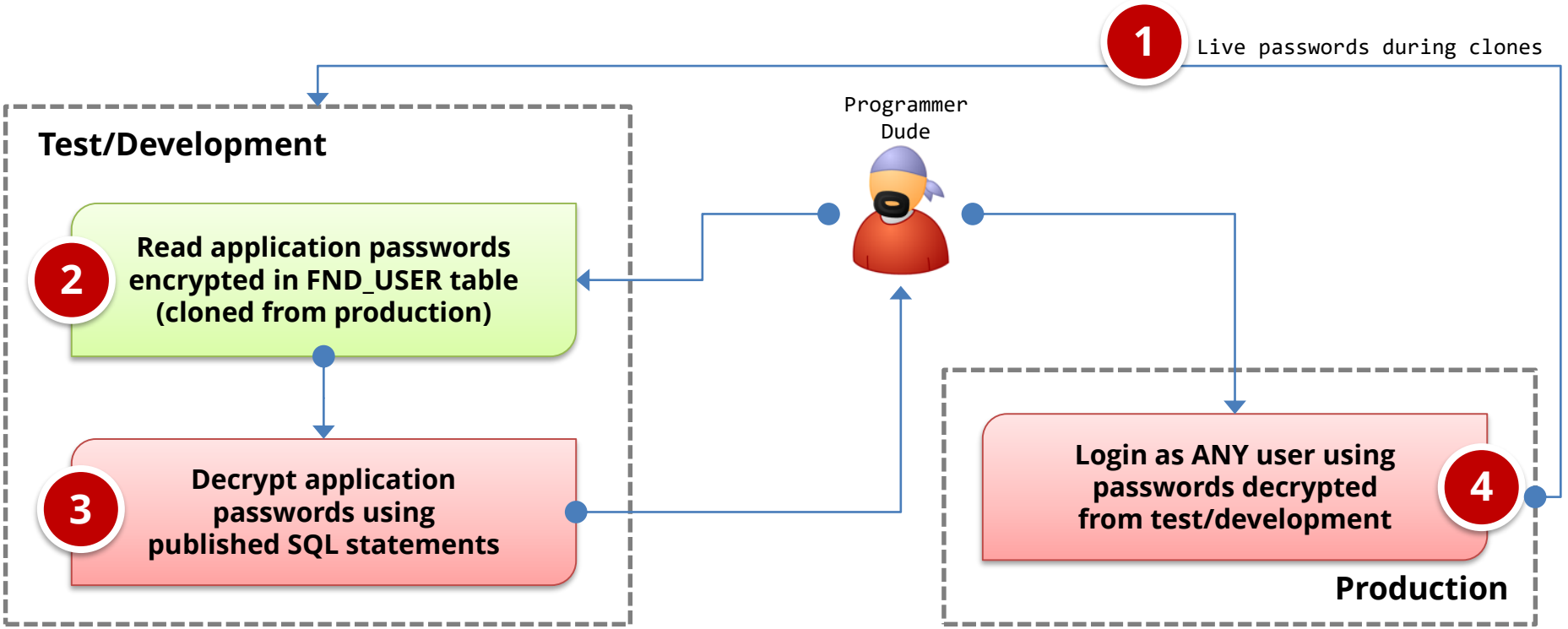

Password Hashing
Allowed Resources
Q&A
1
2
3
4
5
Secure Configuration Console
Allowed Redirects

Agenda


Password Hashing
Allowed Resources
Q&A
1
2
3
4
5
Secure Configuration Console
Allowed Redirects

Threat

Application user passwords may be **decrypted** and multiple other user accounts may be used to circumvent application controls.



Oracle EBS Password Encryption

FND_USER Table

USER_NAME	ENCRYPTED_FOUNDATION_PASSWORD	ENCRYPTED_USER_PASSWORD
GUEST	ZG6EBD472D1208B0CDC78D7EC7730F9B249496F825E761BA3EB2FEBB54F6915FADA757EF4558CF438CF55D23FE32BE0BE52E	ZG6C08D49D524A1551A3068977328B1AFD260400FB598E799A3A8BAE573777E7EE7262D1730366E6709524C95EC6BFA0DA06
SYSADMIN	ZH39A396EDCA4CA7C8D5395D94D8C915510C0C90DA198EC9CDA15879E8B547B9CDA034575D289590968F1B6B38A1E654DD98	ZHF57EAF37B1936C56755B134DE7C83AE40CADDD4AA83B1D7455E5533DC041773B494D2AA04644FB5A514E5C5614F3C87888
WIZARD	ZG2744DCFCCFFA381B994D2C3F7ADACF68DF433BADF59CF6C3DAB3C35A11AAAB2674C2189DCA040C4C81D2CE41C2BB82BFC6	ZGE9AAA974FB46BC76674510456C739564546F2A0154DCF9EBF2AA49FBF58C759283C7E288CC673044036E284042A8FE4451

APPS password encrypted user name + user password

User password encrypted using APPS password

R12 APPS Password Decryption SQL

```
select
(
  select
  decrypt(
    (select fnd_web_sec.get_guest_username_pwd from dual)
     , fu.encrypted_foundation_password
  )
  from dual
) as apps_password
from
  fnd_user fu
where
  fu.user_name like
  (select substr(fnd_web_sec.get_guest_username_pwd,1,
      instr(fnd_web_sec.get_guest_username_pwd,'/')-1)
   from dual
  )
```

Google: oracle applications password decryption

End-User Password Decryption SQL

```
select user_name,
       decrypt('APPSPASSWORD',
       encrypted_user_password)
from
  fnd_user;
```

Google: oracle applications password decryption

Access Oracle EBS Decrypt Function

```
create or replace
function decrypt(key in varchar2,
                 value in varchar2)
return varchar2
as language java name
'oracle.apps.fnd.security.WebSessionManagerProc.decrypt
(java.lang.String,java.lang.String)
return java.lang.String';
```

Decrypt is in a Java class in the database and must be published with a PL/SQL function in order to be called directly from SQL. This is only one method for using decrypt – there are many other ways this can be accomplished.

Oracle EBS Password Decryption and Hashing

- **Application passwords are encrypted by default, not hashed which is more secure**
  - Simple method to decrypt if able to access FND_USER table

- **Secure hashing of passwords is optional for ALL Oracle EBS versions and must be enabled by DBA**
  - Patch for earlier 11i versions and included with R12 but not enabled by default

EBS Password Hashing New Feature

- **Enable EBS application user password hashing**
  - See MOD ID 457166.1 for instructions
- **Use AFPASSWD rather FNDCPASS in order to enable stronger hash algorithms**
  - For 12.1.3+ and 12.2.3+, use **SHA512**
  - For all other versions, only option is SHA (uses SHA1)
- **Previously migrated, as of June 2017 improved hashing available**
  - 12.2.3+ = 26175708 FND SECURITY RUP JUN-2017
  - 12.1.3+ required
  - Run AFPASSWD again with PARTIAL option

EBS Password Hashing New Feature

- **Verify it has been run successfully for all users**
  - See MOS ID 1084956.1 for query

Release	Versions	SHA1	SHA256, 384, 512
11.5	11.5.10	RUP6	*Not available*
12.0	12.0.4 – 12.0.6	12.0.4	*Not available*
12.1	12.1.1 – 12.1.3	12.1.1+	12.1.3+
12.2	12.2.1 – 12.2.8	12.2.1+	12.2.3+ [26175708]

Oracle EBS Password Hash Feature

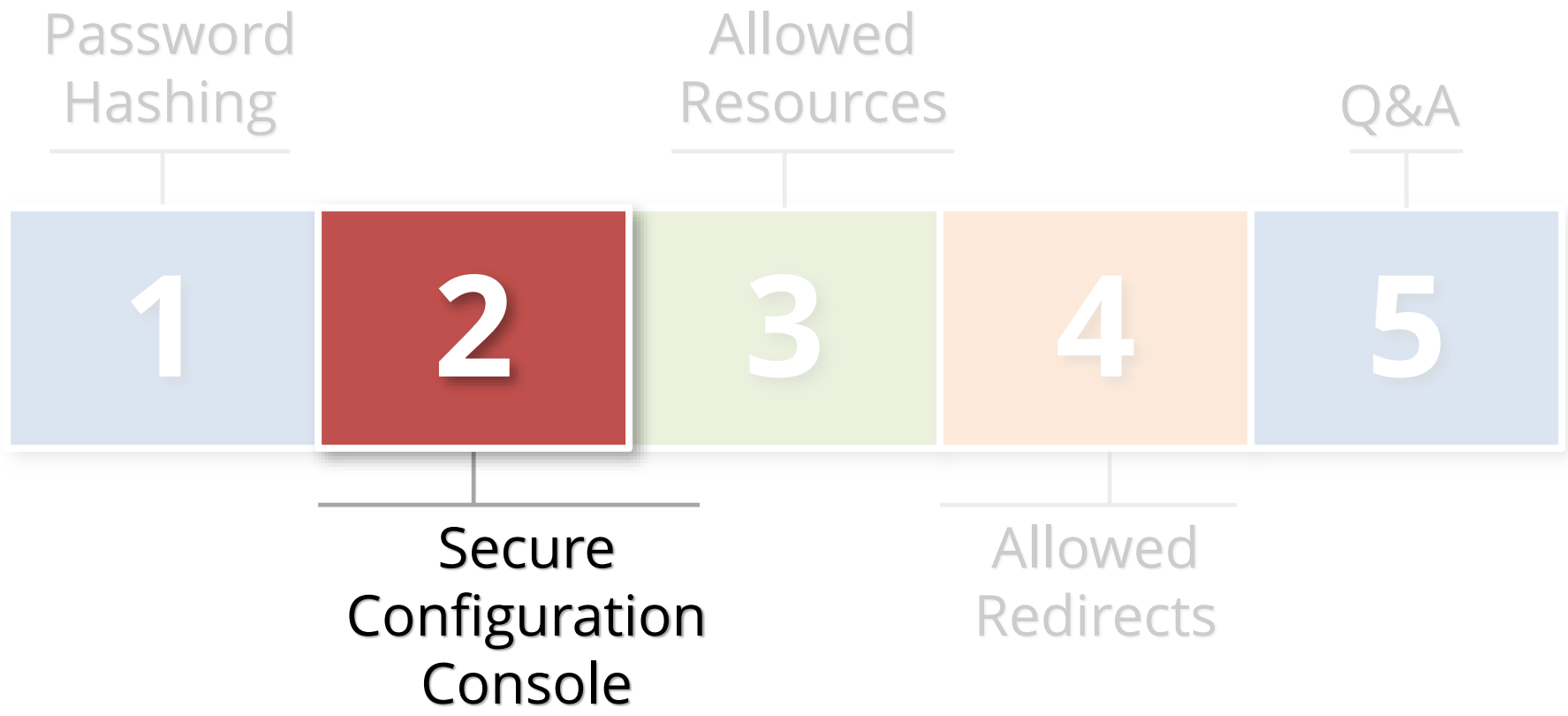
FND_USER Table

USER_NAME	ENCRYPTED_FOUNDATION_PASSWORD	ENCRYPTED_USER_PASSWORD
GUEST	XG{SHA1}	XG6C08D49D524A1551A3068977328B1AFD260400FB598E799A3A8BAE573777E7EE7262D1730366E6709524C95EC6BFA0DA06
SYSADMIN	XG{SHA1}	XGF57EAF37B1936C56755B134DE7C83AE40CADDD4AA83B1D7455E5533DC041773B494D2AA04644FB5A514E5C5614F3C87888
WIZARD	XG{SHA1}	XGE9AAA974FB46BC76674510456C739564546F2A0154DCF9EBF2AA49FBF58C759283C7E288CC673044036E284042A8FE4451

APPS password no longer encrypted and stored in FND_USER

User password now a SHA1 one-way hash

Agenda


Password Hashing
Allowed Resources
Q&A
1
2
3
4
5
Secure Configuration Console
Allowed Redirects

Secure Configuration Console

- **Secure Configuration Console performs basic Oracle EBS security checks**
  - 18 checks as of November 2018
- **Available for 12.1.3 and 12.2.6+**
  - 12.1.3 = Secure Configuration Console in Oracle E-Business Suite Release 12.1.3 (Doc ID 2311308.1) and Patch 26090737:R12.FND.B
  - 12.2.6 = Oracle E-Business Suite Security Guide
- **Access using Functional Administrator responsibility**
  - Functional Administrator → Configuration Manager

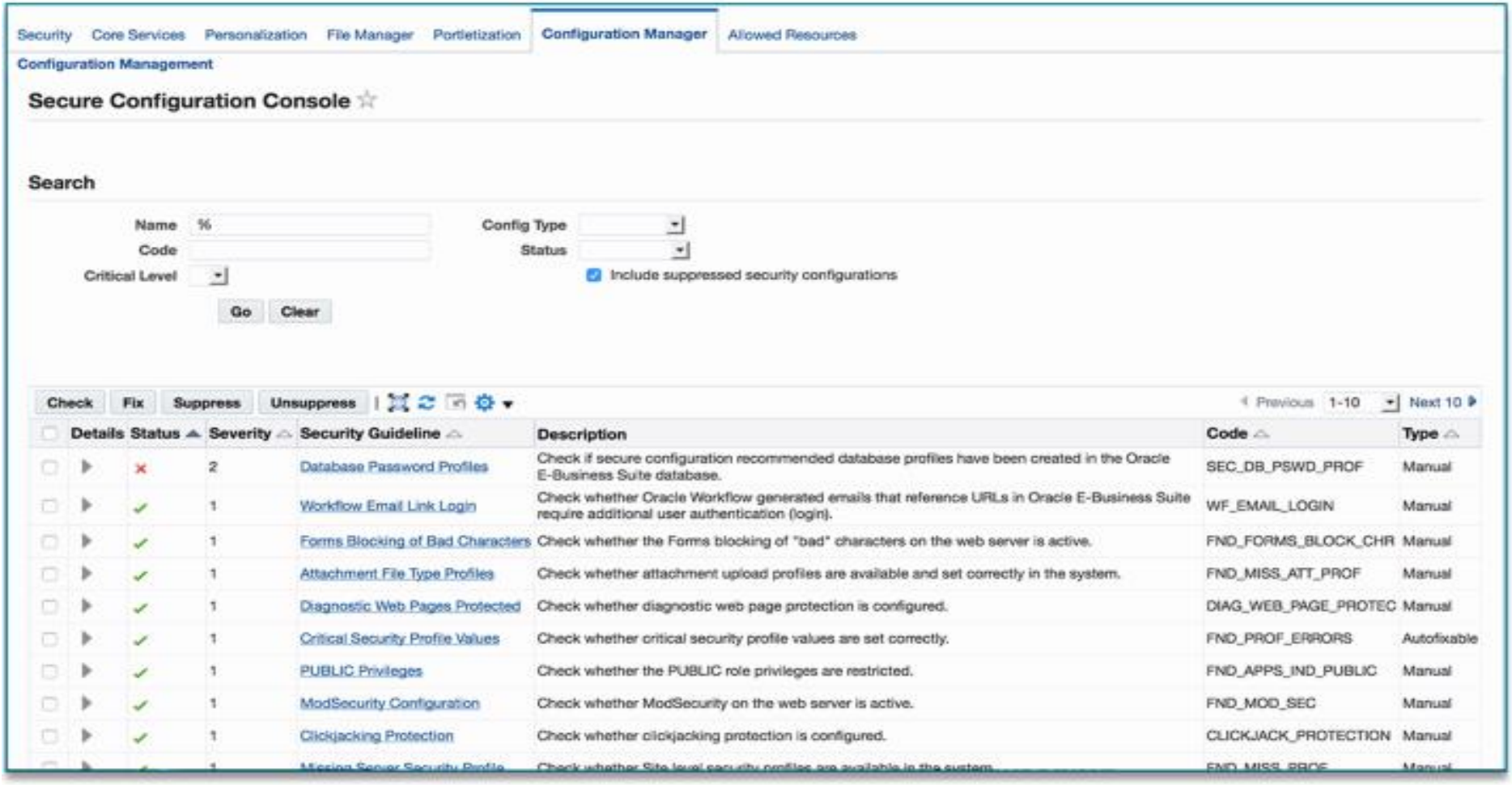
Secure Configuration Console

Secure Configuration Console performs basic Oracle EBS configuration security checks

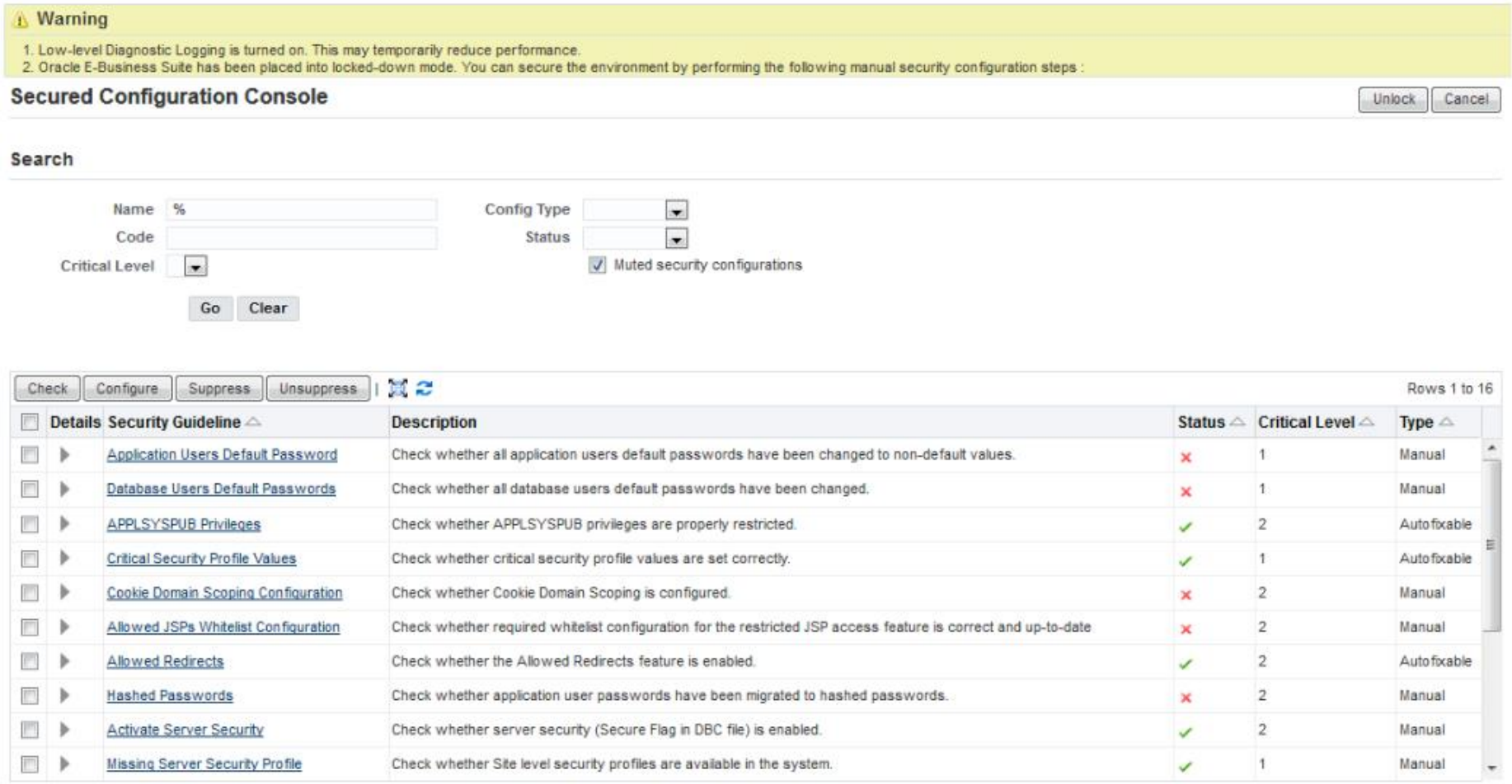
- 12.1.3 = 18 checks (26090737:R12.FND.B)
- 12.2.6 = 14 checks
- 12.2.7 = 24 checks

12.1	12.1.3	▪ Patch 26090737:R12.FND.B ▪ Secure Configuration Console in Oracle E-Business Suite Release 12.1.3 (MOS ID 2311308.1)
12.2	12.2.6+	▪ Included with 12.2.6+ ▪ See latest version *Oracle E-Business Suite Security Guide*

Secure Configuration Console



Secure Configuration Console



Warning

1. Low-level Diagnostic Logging is turned on. This may temporarily reduce performance.
2. Oracle E-Business Suite has been placed into locked-down mode. You can secure the environment by performing the following manual security configuration steps :

Secured Configuration Console

Unlock | Cancel

Search

Name: %
Code:
Critical Level:
Config Type:
Status:
Muted security configurations

Go | Clear

Check | Configure | Suppress | Unsuppress

Rows 1 to 16

Details	Security Guideline	Description	Status	Critical Level	Type
	Application Users Default Password	Check whether all application users default passwords have been changed to non-default values.	✗	1	Manual
	Database Users Default Passwords	Check whether all database users default passwords have been changed.	✗	1	Manual
	APPLSYSPUB Privileges	Check whether APPLSYSPUB privileges are properly restricted.	✓	2	Autofixable
	Critical Security Profile Values	Check whether critical security profile values are set correctly.	✓	1	Autofixable
	Cookie Domain Scoping Configuration	Check whether Cookie Domain Scoping is configured.	✗	2	Manual
	Allowed JSPs Whitelist Configuration	Check whether required whitelist configuration for the restricted JSP access feature is correct and up-to-date	✗	2	Manual
	Allowed Redirects	Check whether the Allowed Redirects feature is enabled.	✓	2	Autofixable
	Hashed Passwords	Check whether application user passwords have been migrated to hashed passwords.	✗	2	Manual
	Activate Server Security	Check whether server security (Secure Flag in DBC file) is enabled.	✓	2	Manual
	Missing Server Security Profile	Check whether Site level security profiles are available in the system.	✓	1	Manual

Secure Configuration Console Lock-Down

- **EBS is locked down and can not be used until the system administrator resolves any open issues or accepts the risks**
  - After applying a 12.2 ATG_PF RUP patch
  - 12.1.3 Secure Configuration Console patch
- **Access to limited to local EBS users only with responsibility such as System Administration or System Administrator**

"After you upgrade to the latest ATG_PF Release Update Pack, your system will be 'locked down' until a local system administrator resolves or acknowledges the recommended security configurations in the Secure Configuration Console."

Secure Configuration Console Lock-Down

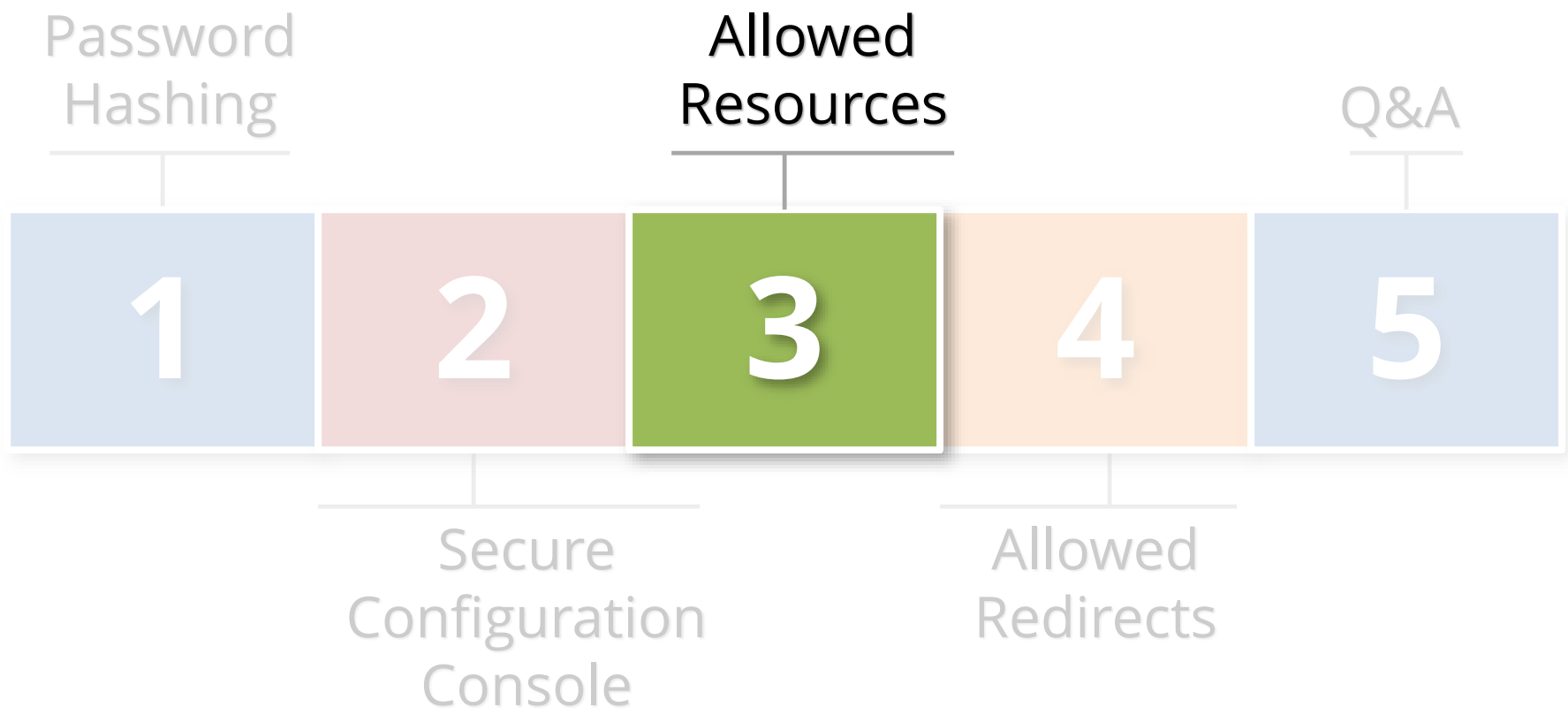
EBS may also be unlocked using a command line utility or by logging in as System Administrator

```
java oracle.apps.fnd.security.AdminSecurityCfg <APPS Username/APPS password[@<DB
Host>] [-check|-fix|-status|-lock|-unlock] [DBC=<DBC File Path>]
[CODES=<code1>,<code2>,<code3>...]
-unlock = To take the system out of locked down mode.
-check = To compute the status of a certain configuration or all configurations.
-fix = To configure a certain configuration or all configurations of type
'Autofixable’.
-status = To view the status of a certain configuration or all configurations
```

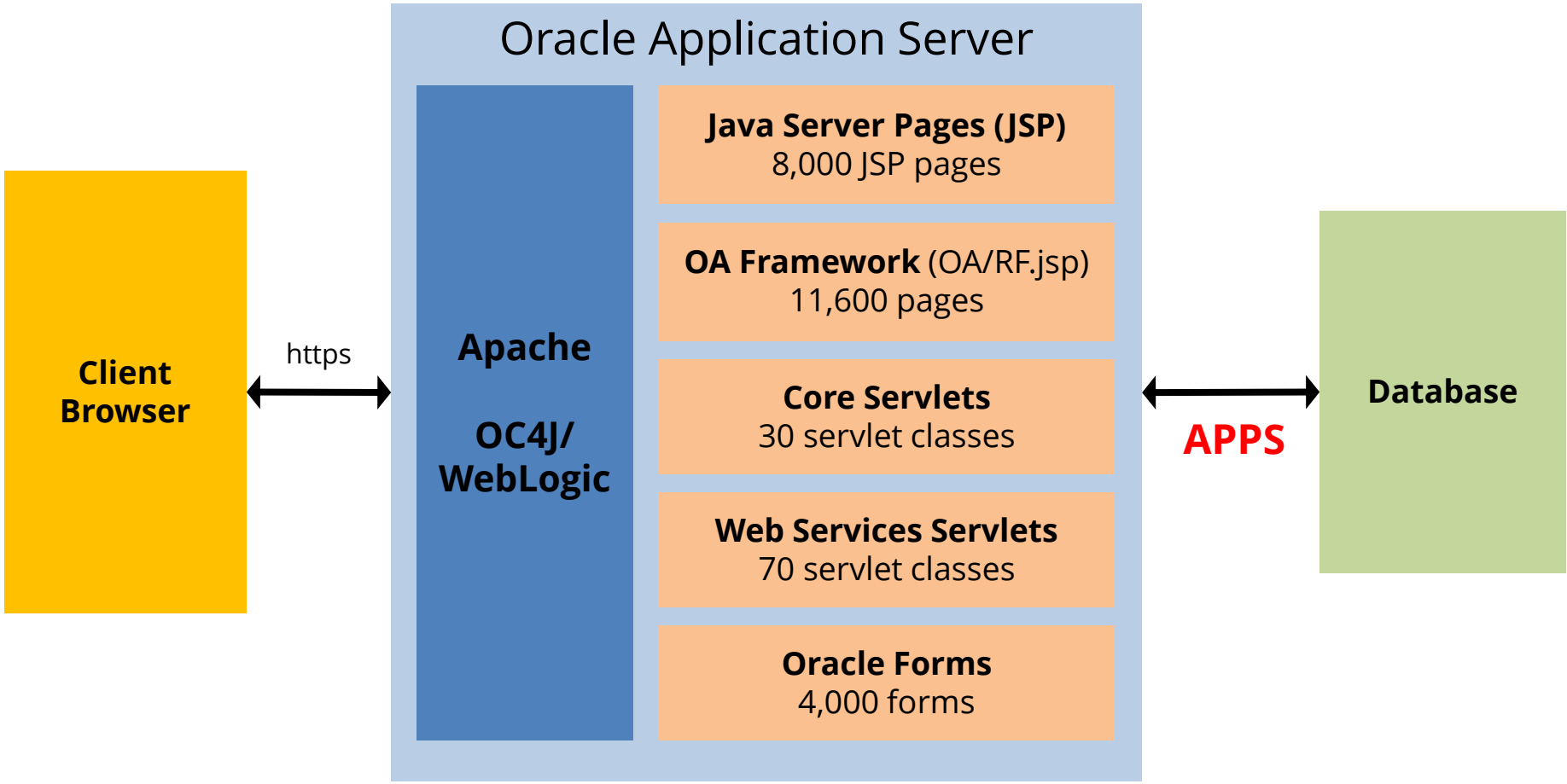
12.2 = How to Run Secure Configuration Console Non-Interactively(Doc ID 2312409.1)

12.1.3 = Secure Configuration Console in Oracle E-Business Suite Release 12.1.3 (MOS ID 2311308.1)

Agenda

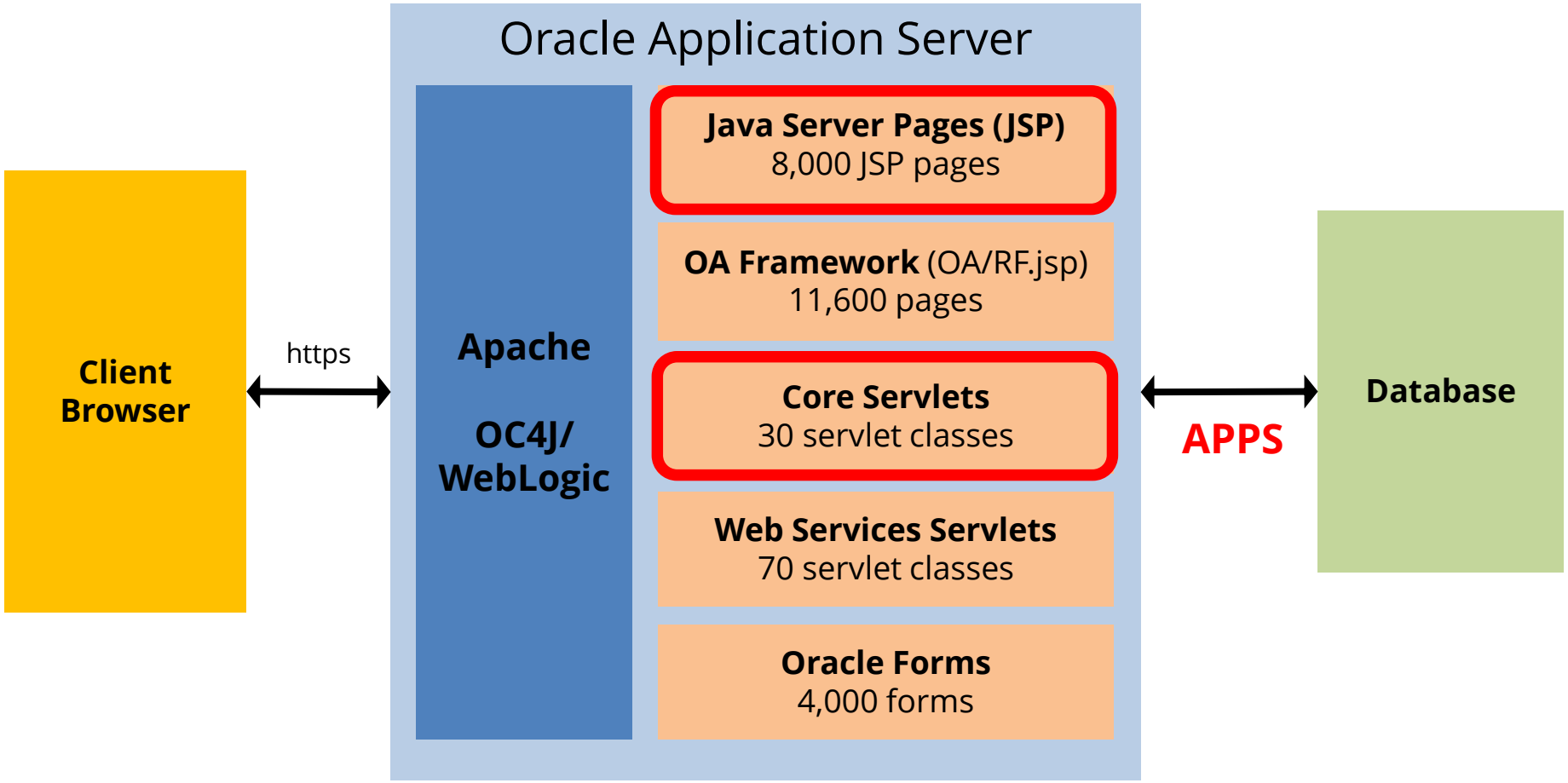

Password Hashing
Allowed Resources
Q&A
1
2
3
4
5
Secure Configuration Console
Allowed Redirects

Oracle EBS R12 Architecture



Threat

Large Oracle EBS application surface area with many unused modules and web page.



12.2 Allowed Resources (formerly known as Allowed JSPs)

- Explicit list of allowed JSP pages and servlets
- Limits access to unused JSP pages and servlets for modules not configured or licensed
- Initially released in 12.2.4 as Allowed JSPs
- Rebranded and enhanced in 12.2.6 from Allowed JSPs to Allowed Resources
- See the Oracle EBS Security Guide manual for instructions on usage
- See MOS Note “Significance of Profile Allow Unrestricted JSP Access” (Doc ID 2172584.1)

Allowed Resources – Configuration

- Allowed Resources enabled by default starting with 12.2.6
- Allowed JSPs in 12.2.4 and 12.2.5 not enabled by default
- New profile option for enabling of Allowed Resources
- Allowed Resources lists stored in database

Profile Option Name	Description
Security: Allowed Resources (FND_SEC_ALLOWED_RESOURCES)	Set at Site or Server Level **CONFIG** – Allow only whitelisted **(default)** **ALL** – Allow all web resources

Allowed Resources – Configuration

- **12.2.7 New web interface released to allow configuration**
  - Functional Administrator responsibility → Allowed Resources
- **12.2.4 and 12.2.5 Allowed JSP configuration is through the `allowed_jsp.conf` file.**

12.2.4/12.2.5 allowed_jsp.conf

```
# $Header: allowed_jsps.conf
120.0.12020000.3 2013/06/11 21:37:29
srveerar noship $
/OA_HTML/AppsLocalLogin.jsp
/OA_HTML/cabo/jsps/a.jsp
/OA_HTML/cabo/jsps/frameRedirect.jsp
/OA_HTML/fndgfm.jsp
/OA_HTML/jsp/fnd/close.jsp
/OA_HTML/jsp/fnd/fnderror.jsp
/OA_HTML/OADownload.jsp
/OA_HTML/OAErrorDetailPage.jsp
/OA_HTML/OAErrorPage.jsp
/OA_HTML/OAExport.jsp
/OA_HTML/OA.jsp
/OA_HTML/OALogout.jsp
/OA_HTML/OARegion.jsp
/OA_HTML/RF.jsp
/OA_HTML/GWY.jsp
/OA_HTML/runforms.jsp
/OA_HTML/xdo_doc_display.jsp
/OA_HTML/OAD.jsp
/OA_HTML/OAP.jsp

include allowed_jsps_FIN.conf
include allowed_jsps_HR.conf
include allowed_jsps_Leasing.conf
include allowed_jsps_Procurement.conf
include allowed_jsps_SCM.conf
include allowed_jsps_CRM.conf
include allowed_jsps_VCP.conf
include allowed_jsps_diag_tests.conf
```

Allowed JSPs – If Not Allowed (12.2.4/12.2.5)

Error
Requested resource or page is
not allowed in this site

Allowed JSPs – If Not Allowed (12.2.6+)

403 Forbidden
Requested resource or page is
not allowed in this site

Allowed JSPs – 12.2.6 Automatic Config

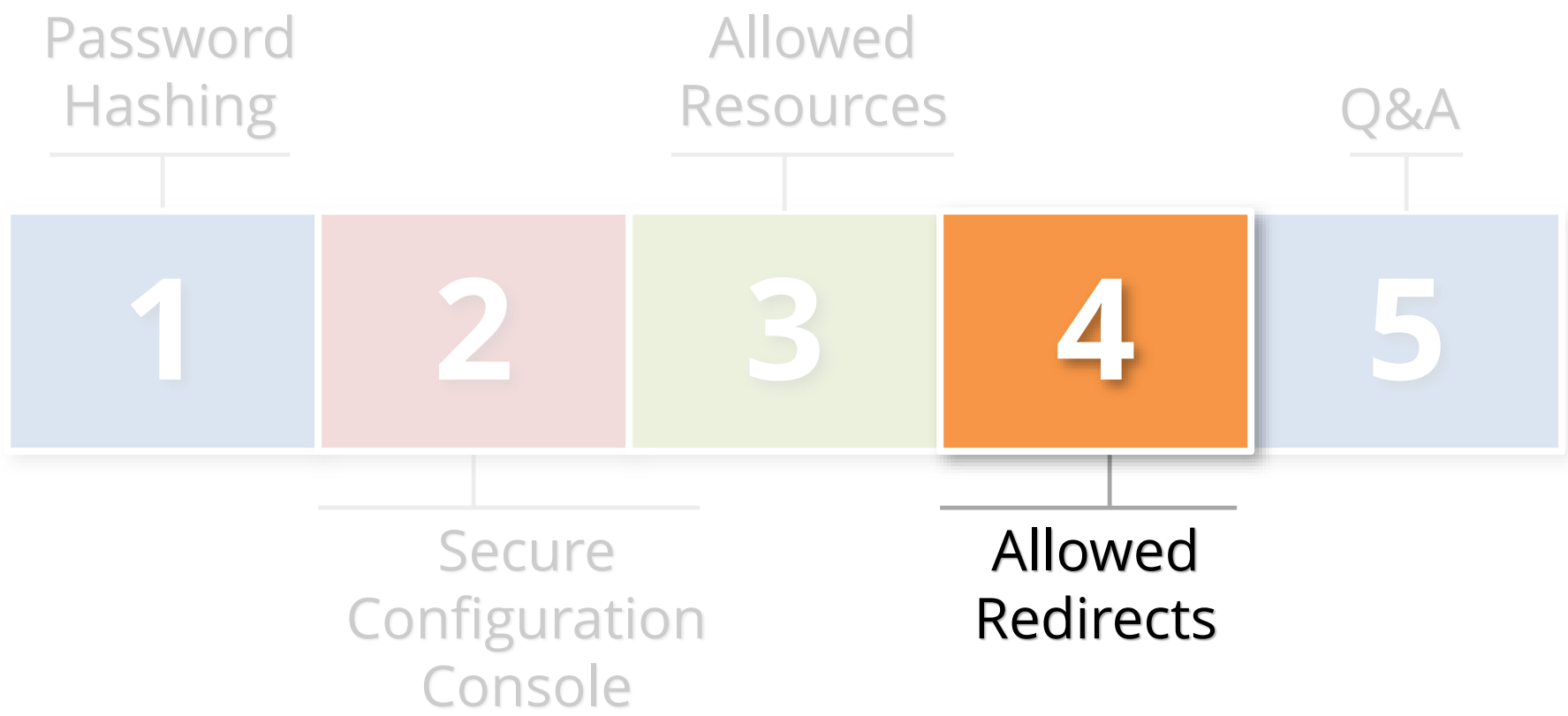
- 12.2.6 introduces an utility to automatically configure the allowed JSPs lists
- Script handles modules and pages – disabled inactive application modules

```
perl txkCfgJSPWhitelist.pl -contextfile=<path>
-mode=<report/update>
```

Allowed JSPs – Logging (12.2.4/12.2.5)

- **Logging is disabled by default – no visibility if a disallowed page is accessed**
  - No HTTP error
  - Redirects to `/jsp/fnd/fnderror.jsp?msg_app=FND&msg_name=FND_INVALID_RESOURCE`
- **Must enable Allowed JSPs logging in web.xml**
  - Logging is verbose and not recommended for production

Agenda


Password Hashing
Allowed Resources
Q&A
1
2
3
4
5
Secure Configuration Console
Allowed Redirects

Allowed Redirects

- **Introduced in 12.2.4 to protect against phishing redirect attacks**
- **Whitelist of allowed redirect locations located in `$FND_TOP/secure/allowed_redirects.conf`**
  - Can be host, domain, or profile option value

Profile Option Name	Description
Allow Unrestricted Redirects (FND_SEC_ALLOW_UNRESTRICTED_REDIRECT)	Set at Site or Server Level **Yes** – Allow any redirect **(default 12.2.4/12.2.5)** **No** – Use allowed list **(default 12.2.6+)**

Allowed Redirects – Standard EBS

- Report Launcher
- Self-Service Applications
- Help System
- Single sign-on integration with Oracle Access Manager using Oracle E-Business
- AccessGate and Oracle Directory Services
- Reporting with Oracle Discoverer Viewer, Oracle Discoverer Server and Oracle
- Business Intelligence Enterprise Edition
- Integration with Oracle Portal
- iRecruitment Background Check URL

Allowed Redirects – Custom

- **Oracle E-Business Suite iProcurement with Punchout (Add host or domain entry for each Punchout site)**
  - Only for Releases 12.2 through 12.2.5
  - Starting with Release 12.2.6, configuration of allowed redirects for Oracle E-Business Suite iProcurement is performed automatically
- **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**

Testing Allowed Redirects

- **Create and compile custom JSP page as follows –**

```
<html>
<head>
   <title>Testing a redirect</title>
</head>
<body>
   <%
     String redirectURL =
"https://example.org/wiki/HTTP_302";
     response.sendRedirect(redirectURL);
   %>
</body>
```

- **Remember to delete this page when done testing!!!**

Other New Security Features (SSL/TLS)

- **Oracle EBS TLS 1.2 certified**
  - Enabled in 12.1 (see 376700.1) and 12.2 (see 1367293.1)
  - Use an SSL termination point (load balancer/reverse proxy) for a much more robust TLS implementation
- **HTTP Strict Transport Security (HSTS) supported**
  - Tells browser to only communicate using HTTPS
  - Enabled in 12.1 (see 376700.1) and 12.2 (see 1367293.1)
  - Use an SSL termination point (load balancer/reverse proxy) for a much more robust TLS implementation

Other New Security Features (Web)

- **HTTP web header X-Content-Type-Options = Nosniff**
  - Prevents web browser from guessing the mime-type and prevents some types of web attacks
  - New feature included in the October 2018 Critical Patch Update for 12.1 and 12.2.4+
- **HTTP cookie flag HTTPOnly**
  - Flag set on cookies sent from the server to the browser to prevent scripts running in the browser from accessing session cookies
  - 12.2 = R12.ATG_PF.C.DELTA.7 (24690680)
  - 12.1.3 = backport in progress

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**