This document shows the description of all checks which are executed by the SAP Security Optimization Service for a Java system.

The check ids are marked in red.

Author: Global Service and Support – Security Services
Contact: securitycheck@sap.com
Date: 10.03.2016
| 1 SC_INIT - INITIALIZATIONS FOR SECURITY CHECK | ................................................................. 5 |
| 1.0.1 Preface | ................................................................. 5 |
| 2 SC_J2EE - J2EE CHECKS I | ................................................................. 6 |
| 2.1 J2EE - BACKEND CHECKS (DUAL STACK SYSTEM) | ................................................................. 6 |
| 2.2 J2EE - BACKEND CHECKS (DUAL STACK SYSTEM) | ................................................................. 6 |
| 2.2.1 Users with Role "SAP_J2EE_ADMIN" (0813) | ................................................................. 6 |
| 2.2.2 Profile of User SAPJSF (0796) | ................................................................. 7 |
| 2.2.3 Type of Users in the Jco RFC Provider (0877) | ................................................................. 8 |
| 2.2.4 Authorization of Users in the Jco RFC Provider (0878) | ................................................................. 9 |
| 2.2.5 J2EE Engines Allowed to Access the Application Server (0881) | ................................................................. 10 |
| 2.2.6 Other J2EE Systems Allowed to Connect to the SAP Database for User Replication (0863) | ................................................................. 10 |
| 2.2.7 Users Authorized to Maintain the Sending Systems for User Replication (0864) | ................................................................. 11 |
| 2.3 J2EE - COMMUNICATION SECURITY | ................................................................. 12 |
| 2.3.1 SSL is Not Working (JE143) | ................................................................. 12 |
| 2.3.2 Secure Attribute for System Cookie (JE166) | ................................................................. 12 |
| 2.3.3 Secure Attribute for Security Session ID Cookie (JE167) | ................................................................. 13 |
| 2.3.4 RFC Connections JCo Provider (JE157) | ................................................................. 13 |
| 2.3.5 Http Connections JCo Provider (JE168) | ................................................................. 14 |
| 2.3.6 Communication J2EE RA to SAP Sys (JE077) | ................................................................. 15 |
| 2.4 J2EE - ADMINISTRATION <;GENERAL;SID> | ................................................................. 15 |
| 2.4.1 J2EE Server Administration with Admin Tools (JE027) | ................................................................. 16 |
| 2.4.2 J2EE Server Remote Administration with Telnet (JE028) | ................................................................. 16 |
| 2.4.3 Additional Data Sources (JE031) | ................................................................. 17 |
| 2.4.4 Restriction of HTTP PUT Method (JE032) | ................................................................. 17 |
| 2.4.5 Restriction of Download Functions (JE144) | ................................................................. 19 |
| 2.4.6 HTTP Based Browsing (JE033) | ................................................................. 19 |
| 2.4.7 Security of SAP Logon tickets (JE137) | ................................................................. 20 |
| 2.4.8 HTTPONLY Setting for SAP Logon Tickets (JE138) | ................................................................. 21 |
| 2.4.9 Enforce SSL encryption for Transfer of SAP Logon Tickets(JE139) | ................................................................. 22 |
| 2.4.10 Control Lifetime of SAP Logon Tickets (JE140) | ................................................................. 23 |
| 2.4.11 Verify Setting for Domain Relaxing (JE141) | ................................................................. 24 |
| 2.4.12 HTTPONLY Setting for Session and Load Balancing Cookies (JE145) | ................................................................. 24 |
| 2.4.13 Session Fixation Protection (JE146) | ................................................................. 25 |
| 2.4.14 Invoker Servlet (JE165) | ................................................................. 26 |
| 2.5 J2EE - USER STORE - GENERAL CHECKS <;GENERAL;SID> | ................................................................. 27 |
| 2.5.1 Users of Standard User Group "Administrators" (JE045) | ................................................................. 27 |
| 2.5.2 Security of User Mapping Data (JE147) | ................................................................. 27 |
| 2.5.3 Users of Standard User Group "Guests" (JE046) | ................................................................. 28 |
| 2.5.4 Guest User "GUEST" should be Locked (JE148) | ................................................................. 29 |
| 2.5.5 Critical UME Actions of Role "Everyone" (JE149) | ................................................................. 29 |
| 2.6 J2EE - UME USER STORE <;GENERAL;SID> | ................................................................. 29 |
| 2.6.1 Disabling of SAP* as User Administrator (JE064) | ................................................................. 30 |
| 2.6.2 Password Authentication Allowed (JE070) | ................................................................. 30 |
| 2.6.3 Lock Time After Failed Logon Attempts (JE048) | ................................................................. 31 |
| 2.6.4 Number of Allowed Failed Logon Attempts (JE049) | ................................................................. 32 |
2.6.5 New Password Includes Old Password (JE050) ................................................. 33
2.6.6 Password Contains Alphabetic and Numeric Characters (JE051) ..................... 34
2.6.7 Regular Password Change (JE052) .................................................................. 34
2.6.8 Minimum Password Length (JE053) .................................................................. 35
2.6.9 Password Contains Upper and Lower Case Letters (JE054) .......................... 36
2.6.10 Password Contains Special Characters (JE055) ............................................. 37
2.6.11 Password Includes the User-ID (JE056) ......................................................... 38
2.6.12 Trivial Passwords are Not Sufficiently Prohibited (JE150) ......................... 39
2.6.13 Self-Registration (JE158) .............................................................................. 39
2.6.14 Self-Registration of Guest User is Enabled (JE151) ....................................... 40
2.6.15 Self-Management (JE152) ............................................................................ 41
2.6.16 SPML check of HTTP Header (JE169) ......................................................... 42
2.6.17 Disabling of URL logon (JE170) ................................................................. 42

2.7 J2EE - Change Management <;GENERAL;SID> .................................................. 43
2.7.1 Password DTR Emergency User (JE084) .......................................................... 43
2.7.2 Users Authorized to Administer the SLD (JE085) .......................................... 44
2.7.3 Users Authorized to Activate Software in the CBS (JE086) .......................... 44
2.7.4 Users Authorized to Administer the CBS (JE087) ........................................ 45

2.8 SAP ENTERPRISE PORTAL <;GENERAL;SID> ................................................. 46
2.8.1 EP - General ................................................................................................... 46
   2.8.1.1 Use of SSL for Communication with the Portal (EP103) ......................... 46
   2.8.1.2 Use of Multiple Authentication Schemes (EP108) ............................ 46
   2.8.1.3 Security Mode for production systems (EP171) .................................. 47
2.8.2 EP - User Administration .............................................................................. 48
   2.8.2.1 Portal Super Administrators Found (EP153) ........................................... 48
   2.8.2.2 Nested Roles are Used (2019) ............................................................... 48
   2.8.2.3 Additional Portal Administrators Found (EP115) .............................. 49
   2.8.2.4 Additional Portal User Administrators Found (EP117) ...................... 49
   2.8.2.5 Additional Portal Content Administrators Found (EP116) .............. 50
   2.8.2.6 Anonymous Logon (EP113) ................................................................. 50
2.8.3 Knowledge Management <;GENERAL;SID> ................................................... 51
   2.8.3.1 Use of HTML Text Editor (KM109) ..................................................... 51
   2.8.3.2 Assignments of System Principal Privileges (KM155) ....................... 52
   2.8.3.3 Security of KM Repositories (KM159) ............................................... 52
   2.8.3.4 Security of KM Reports (KM156) ....................................................... 53
   2.8.3.5 Use of HTML Text Editor ................................................................. 53
   2.8.3.6 Assignments of System Principal Privileges....................................... 54
   2.8.3.7 Security of KM Repositories ............................................................. 54

2.9 SYSTEM RECOMMENDATIONS (JAVA) (SY124) .............................................. 55

<Service Name>, <Customer Name> <date of session>
1 SC_INIT - Initializations for Security Check

1.0.1 Preface

The SAP Security Optimization service is a comprehensive support service that identifies security risks for your SAP system and helps you to determine the appropriate measures to protect it from these risks.

Objective of the SAP Security Optimization Service

The objectives of SAP Security Optimization are:
- To analyze the technical configuration of your SAP system for security risks
- To provide recommendations for implementing measures to mitigate security risks
- To provide a compressed overview of the implemented security level
- To enable you to protect your business systems from typical security risks

The security checks of SAP Security Optimization are performed for the following security aspects:
- **Availability**: ensuring that a system is operational and functional at any given moment
- **Integrity**: ensuring that data is valid and cannot be compromised
- **Authenticity**: ensuring that users are who they claim to be
- **Confidentiality**: ensuring that information is not accessed by unauthorized persons
- **Compliance**: ensuring that the system security setup is in accordance with established guidelines

Scope of SAP Security Optimization

SAP Security Optimization includes a collection of several hundred checks. These checks identify security vulnerabilities in the current setup and configuration of your SAP system. The checks are performed on the SAP software layer. For a security analysis of the underlying operating system and database, consult your vendor; for a security analysis of the network, contact your preferred network security provider.

The SAP Security Optimization service cannot cover customer-specific aspects that require a detailed on-site analysis, such as the following checks:
- Segregation of duties for business-critical processes
- Security organization (organizational security)
- Security administration processes (operational security)

For a complete overview of existing security risks to your business system, the topics listed above have to be taken into consideration. SAP's Security Consulting Team can assist you with individual on-site consulting services to obtain guidance on aspects of security.
2 SC_J2EE - J2EE Checks I

2.1 J2EE - Backend Checks (Dual Stack System)

**Purpose:**
To control the upload of data from the Configuration Change Database (CCDB) to the J2EE checks and check the validity of the uploaded data based on the timestamp.

**Procedure:**
This check is carried out automatically when the check group is initialized.
However, there are two options to control the check group:
- a) You can reload the CCDB data by choosing 'Reload DDCB data'.
- b) The default validity period of the uploaded data is three days. This period is stored in the 'Validity of Store Content' table by default and should not be changed.

**Rating:**
Set the rating to GREEN if all required CCDB data stores are up to date.
Set the rating to YELLOW if no stores are found.
Set the rating to RED if stores are found but some are missing or outdated

**Background:**
A yellow rating indicates that SAP Diagnostics is not configured.
A red rating indicates that SAP Diagnostics is configured but does not work correctly.
If this check is not green, several follow-on checks that could otherwise be carried out automatically with current CCDB data must be executed manually.
You can use the 'Check ID' column to identify which CCDB stores are used in which checks.
Use the function 'Goto -> technical information' in a check to display the check ID of the check.

**RED:**
The service data could not be retrieved from Solution Manager Configuration and Change Database (CCDB) into the session.
To analyze and resolve issues of missing data in CCDB please refer to the SAP Note 1777750 for Solution Manager 7.0 and 1777751 for Solution Manager 7.1.
If no issue has been found in CCDB, please open a message on component SV-SMG-SER.

2.2 J2EE - Backend Checks (Dual Stack System)

2.2.1 Users with Role "SAP_J2EE_ADMIN" (0813)

**Purpose**
To check if any users other than the system administrators have the role SAP_J2EE_ADMIN (Add-In installation) or the role defined during the installation (for example, J2EE_ADM_<SID>).

**Procedure**
List the users with this role in the check table.

**Rating**
Rating takes place automatically as follows:
GREEN: Only system administrators have the role.
RED: Other users have the role.

**Purpose**
To check if any users other than the system administrators have the role SAP_J2EE_ADMIN (Add-In installation) or the role defined during the installation (for example, J2EE_ADM_<SID>).

**Procedure**
List the users with this role in the check table.
Rating
Rating takes place automatically as follows:
GREEN: Only system administrators have the role.
RED: Other users have the role.

Recommended Risk - High RED:

Recommendation: The following users have either the role SAP_J2EE_ADMIN (Add-In installation) or J2EE_ADMIN_<SID>, which allows system administration. Please review these users and consider removing all users who do not need system administration rights. Check whether user is assigned to the system Java Administrators group:
- AS Java only (with DB or LDAP as DataSource): List users (and groups) assigned to Java group "Administrators"
- Dual stack: List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"
- AS Java only (with ABAP as DataSource): List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"

Recommendation: The following users have either the role SAP_J2EE_ADMIN (Add-In installation) or J2EE_ADMIN_<SID>, which allows system administration. Please review these users and consider removing all users who do not need system administration rights. Check whether user is assigned to the system Java Administrators group:
- AS Java only (with DB or LDAP as DataSource): List users (and groups) assigned to Java group "Administrators"
- Dual stack: List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"
- AS Java only (with ABAP as DataSource): List users (and groups) assigned to Java group "SAP_J2EE_ADMIN"

2.2.2 Profile of User SAPJSF (0796)
Purpose:
To check whether the communication user SAPJSF has the appropriate rights only.

Procedure:
Automatic check:
The system checks whether the SAPJSF user has the profile SAP_ALL.

Risk Rating:
Rating takes place automatically as follows:
GREEN: User SAPJSF does not have the profile SAP_ALL or does not exist.
RED: User SAPJSF has the profile SAP_ALL.

Recommendation: The SAPJSF user should only have the role SAP_BC_JSF_COMMUNICATION and not SAP_ALL. You should also rename this user. To rename this user, change the "ume.r3.connection.master.user" in the sapum.properties file (or in the file that you specified as ume.cfg.file.).

Recommendation: The SAPJSF user should only have the role SAP_BC_JSF_COMMUNICATION and not SAP_ALL. You should also rename this user. To
SC J2EE - J2EE Checks I

rename this user, change the "ume.r3.connection.master.user" in the sapum.properties file (or in the file that you specified as ume.cfg.file).

2.2.3 Type of Users in the Jco RFC Provider (0877)

**Purpose:**
To check whether the users specified in the JCo RFC Provider are of type "Communication"; only "UMEBackendConnection" connection should be available.

**Procedure:**
1. Log on to the Visual Administrator as administrator.
2. On the left side of the screen, expand Cluster -> Server -> Services.
3. Select the JCo RFC Provider from the list of services.
4. Check the available RFC destinations pointing at the ABAP stack of your system on the "Runtime" tab page.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).

**Command Line:**

```plaintext
IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 730
1. Log on to the NWA as administrator.
3. Filter for RFC destination.
4. For each destination found, check the user in the "Logon Data" tab destination detail.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).
ENDIF
```

**Risk Rating:**
Set the rating manually as follows:

**GREEN:** Only "UMEBackendConnection2 and well-known connections are available.

**RED:** Unknown connections are available.

To check whether the users specified in the JCo RFC Provider are of type "Communication"; only "UMEBackendConnection" connection should be available.

**Procedure:**
1. Log on to the Visual Administrator as administrator.
2. On the left side of the screen, expand Cluster -> Server -> Services.
3. Select the JCo RFC Provider from the list of services.
4. Check the available RFC destinations pointing at the ABAP stack of your system on the "Runtime" tab page.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).

**Command Line:**

```plaintext
ELSEIF "YSAP-SERVERCORE" >= 730 AND "YSAP-SERVERCORE" <= 740
1. Log on to the NWA as administrator.
3. Filter for RFC destination.
4. For each destination found, check the user in the "Logon Data" tab destination detail.
5. Check whether the user exists in the check table (containing all communication users of the back-end system).
ENDIF
```

**Risk Rating:**
Set the rating manually as follows:

**GREEN:** Only "UMEBackendConnection2 and well-known connections are available.

**RED:** Unknown connections are available.
**Evaluated Risk - High RED:**

**Recommendation:** Use only users of type "Communication" for your JCo RFC connections to prevent dialog logon with communication users. There is at least one RFC connection with a user of another user type in your system.

**Recommendation:** Use only users of type "Communication" for your JCo RFC connections to prevent dialog logon with communication users. There is at least one RFC connection with a user of another user type in your system.

### 2.2.4 Authorization of Users in the Jco RFC Provider (0878)

**Purpose:**
To check whether the users specified in the JCo RFC Provider have surplus authorizations.

**Procedure:**

- **Command Line:** IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 720
  1. Log on to the Visual Administrator as administrator.
  2. On the left side of the screen, expand Cluster -> Server -> Services.
  3. Select the JCo RFC Provider from the list of services.
  4. Check the available RFC destinations on the "Runtime" tab page.
  5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).

- **Command Line:** ELSEIF "YSAP-SERVERCORE" >= 720 AND "YSAP-SERVERCORE" <= 740
  1. Log on to the NWA as administrator.
  3. Filter for RFC destination.
  4. For each destination found, check the user in the "Logon Data" tab destination detail.
  5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).

**Risk Rating:**
Set the rating manually as follows:

- **GREEN:** Users in JCo RFC Provider are well-known.
- **RED:** Users in JCo RFC Provider are not well-known.

**Purpose:**
To check whether the users specified in the JCo RFC Provider have surplus authorizations.

**Procedure:**

- **Command Line:** IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 720
  1. Log on to the Visual Administrator as administrator.
  2. On the left side of the screen, expand Cluster -> Server -> Services.
  3. Select the JCo RFC Provider from the list of services.
  4. Check the available RFC destinations on the "Runtime" tab page.
  5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).

- **Command Line:** ELSEIF "YSAP-SERVERCORE" >= 720 AND "YSAP-SERVERCORE" <= 740
  1. Log on to the NWA as administrator.
  3. Filter for RFC destination.
  4. For each destination found, check the user in the "Logon Data" tab destination detail.
  5. Check whether the user exists in the check table (containing all SAP_ALL users and all users with more than 80% of authorizations in the back-end system).

**Risk Rating:**
Set the rating manually as follows:
GREEN: Users in JCo RFC Provider are well-known.
RED: Users in JCo RFC Provider are not well-known.

**Recommendation:** Do not give too many authorizations to the users used for JCo RFC connections. There is at least one RFC user with the profile SAP_ALL in your system or a user with more than 80% of all authorizations.

--

**2.2.5 J2EE Engines Allowed to Access the Application Server (0881)**

**Purpose:**
To check which J2EE Engines are allowed to access the application server.

**Procedure:**
Automatic check:
The J2EE Engines in table SNCSYSAACL are listed.

**Risk Rating:**
No rating for this check. The J2EE Engines are listed.

**Recommendation:** These J2EE Engines are allowed to access the application server. Check the list.

--

**2.2.6 Other J2EE Systems Allowed to Connect to the SAP Database for User Replication (0863)**

**Purpose:**
To check for J2EE systems that are allowed to connect to the SAP database of the back-end system. The UME replication functionality still exists in newer releases, but is no longer documented since it is obsolete as of NW 7.00.

**Procedure:**
List the systems specified in SMUM_ACL of the back-end system. Check whether all of these systems exist in the property file ume.r3.sync.sender in the Visual Administrator.

**Risk Rating:**
No rating for this check. Include the following information in the report: 1) If more systems appear in the table than in ume.r3.sync.sender, indicate any additional systems. 2) If user replication is not used but entries exist in the table SMUM_ACL, indicate the entries as displayed in the table SMUM_ACL. To include this information in the report, choose "Show".

**Purpose:**
To check for J2EE systems that are allowed to connect to the SAP database of the back-end system. The UME replication functionality still exists in newer releases, but is no longer documented since it is obsolete as of NW 7.00.

**Procedure:**
List the systems specified in SMUM_ACL of the back-end system. Check whether all of these systems exist in the property file ume.r3.sync.sender in the Visual Administrator.

**Risk Rating:**
No rating for this check. Include the following information in the report: 1) If more systems appear in the table than in ume.r3.sync.sender, indicate any additional systems. 2) If user replication is not used but entries exist in the table SMUM_ACL, indicate the entries as displayed in the table SMUM_ACL. To include this information in the report, choose "Show".

**YELLOW: Recommendation:** We found values in the SMUM_ACL file in your back-end system that do not exist in the property file ume.r3.sync.sender. Check your configuration. If you do use user replication, this file should be empty.

**YELLOW: Recommendation:** We found values in the SMUM_ACL file in your back-end system that do not exist in the property file ume.r3.sync.sender. Check your configuration. If you do use user replication, this file should be empty.

### 2.2.7 Users Authorized to Maintain the Sending Systems for User Replication (0864)

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

- **Green:** No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red:** More users with exceeding authorizations were found. The rating depends on the severity of this check.

**Purpose**
To find users with more authorizations than needed for their tasks.

**Procedure**
ST14 download data is analyzed and rated automatically but individually for each check.

**Risk Rating**
The rating is done automatically as follows, but does not always include all three possible values (Green / Yellow / Red):

- **Green:** No users found (except specified in the questionnaire) with exceeding authorizations.
- **Yellow/Red:** More users with exceeding authorizations were found. The rating depends on the severity of this check.

**RED:**

#### Evaluated Risk - High

**Evaluated Risk - High**

This authorization allows a user to maintain the access control list for sending systems. Currently, it is possible to create users from a malicious external system.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check, you should inspect the roles or profiles that include the authorization objects listed below.

Authorization objects:
- **Object 1:** S_TCODE with TCD = SE16, SE17, SM30, or SM31 [and all relevant parameter transactions]
- **Object 2:** S_TABU_DIS with ACTVT = 2 and DICBERCLS = SUSR

This authorization allows a user to maintain the access control list for sending systems. Currently, it is possible to create users from a malicious external system.

Recommendation: Use the Profile Generator (PFCG) to correct roles and/or transactions SU02 (Maintain Profiles) / SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. With the authorization info system (SUIM) you can check the results. For this check, you should inspect the roles or profiles that include the authorization objects listed below.
Authorization objects:
Object 1: S_TCODE with TCD = SE16, SE17, SM30, or SM31 [and all relevant parameter transactions]
Object 2: S_TABU_DIS with ACTVT = 2 and DICBERCLS = SUSR

2.3 J2EE - Communication Security

Purpose: To enter a chapter header in the report
Procedure: Perform the subchecks if the section is applicable to the analyzed system.
Rating: Set the rating to NOT PERFORMED if the section is not applicable. Otherwise, do not set a rating or set TOOL RATING.

2.3.1 SSL is Not Working (JE143)

Purpose:
To check whether systems can be accessed only via a secured connection.
Procedure:
Try to access via SSL and without SSL.
1...Try to access the J2EE/Portal with the url https://<host:port>/
2...If this works, download the certificate by clicking the "lock" icon at the left of the address bar and choose "View Certificates".
3...Check whether the certificate is not issued by the system itself (under Details, compare issuer and subject).
Risk Rating:
GREEN: Only SSL is available; certificate is not default/not self-signed.
RED: At least one of the following points is not true:
- Only SSL is available.
- Certificate used is not default/self-signed.
RED:
Evaluated Risk - High
Description: To check whether Secure Sockets Layer (SSL) communication is possible. SSL ensures secure transactions between Web servers and browsers.

Result: We found that SSL communication is not set up or the default (self-signed) certificate is used.

Recommendation: Ensure secure communication by using SSL certificates only. A default certificate should be replaced by a "real" certificate, signed by a proper certification authority. After applying the recommendation for SSL configuration, several parameters should be adjusted accordingly. Please refer to the following two sections.

2.3.2 Secure Attribute for System Cookie (JE166)

Procedure:
1. NWA: => Configuration => Infrastructure =>Java System properties.
2. Select the "Services" tab and search for the HTTP provider service.
3. Check the value of SystemCookiesHTTPSProtection.
Risk Rating:
The check is rated automatically when you save:
GREEN if value is TRUE.
RED if value is FALSE.

YELLOW:
Evaluated Risk - Medium
Description: If the property is set to true, then the secure attribute is set to the system cookies and the cookies marked as secure will only be transmitted if the communications channel is a secure one (https).

Result: The settings for secure attribute is not configured correctly.

Recommendation: If encryption is set up, please set the parameter to the recommended value so that the system cookies are transferred via SSL.

2.3.3 Secure Attribute for Security Session ID Cookie (JE167)
Procedure:
1. NWA: => Configuration => Infrastructure => Java System properties.
2. Select the "Services" tab and search for the HTTP provider service.
3. Check the value of SecuritySessionIDHTTPSProtection.

Risk Rating:
The check is rated automatically when you save:
GREEN if value is TRUE.
RED if value is FALSE.
YELLOW: Evaluated Risk - Medium

Description: If the property is set to true, then the secure attribute is set to the security session id cookie and the cookie marked as secure will only be transmitted if the communications channel is a secure one (https).

Result: The settings for secure attribute is not configured correctly.

Recommendation: If encryption is set up, please set the parameter to the recommended value so that the system cookies are transferred via SSL.

2.3.4 RFC Connections JCo Provider (JE157)
Purpose:
To check whether only the required RFC connections are specified in the JCo service provider.

Procedure:
Command Line: IF "YSAP-SERVERCORE" < 710
1. Log on to SAP NetWeaver Administrator as an administrator.
2. Navigate to System Management -> Configuration -> Destinations.
3. Get the available RFC destinations and enter them in the check table.
Alternatively:
1. Log on to SAP NetWeaver Administrator as an administrator.
3. Navigate to "Destinations" and navigate to RFC.
4. Check the available RFC destinations and enter them in the check table.

Then select each of the RFC destinations and check the following settings in the "Destination Detail" area -> connections and Transport/Logon Data:
- SNC: Enter "Yes" into the check table if SNC is activated, otherwise enter "No".
- Client SID: Enter the value of the "System ID" into the check table.
- Client User: Enter the value of the "User Name" into the check table.

Command Line: ENDIF

Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to SAP NetWeaver Administrator as an administrator.
3. Get the available RFC destinations and enter them in the check table.
Alternatively:
1. Log on to SAP NetWeaver Administrator as an administrator.
2. Navigate to Configuration->Infrastructure->Java Configuration Browser.
3. Navigate to "Destinations" and navigate to RFC.
4. Check the available RFC destinations and enter them in the check table.

Then select each of the RFC destinations and check the following settings in the "Destination Detail" area -> connections and Transport/Logon Data:
- SNC: Enter "Yes" into the check table if SNC is activated, otherwise enter "No".
- Client SID: Enter the value of the "System ID" into the check table.
- Client User: Enter the value of the "User Name" into the check table.

Command Line: ENDIF

Risk Rating:
The check is rated automatically when you save:
GREEN if no RFC connection is found.
YELLOW if RFC connections are found.

YELLOW:
Evaluated Risk - Medium
Description: To check whether only the required RFC connections are specified in the JCo service provider. We also checked whether communication between the J2EE system and back-end system is encrypted.
Result: The table below shows all configured RFC connections:

Command Line: IF "YSAP-SERVERCORE" < 710

Recommendation: To prevent unauthorized access to SAP systems via JCo, you should delete all unused RFC connections in the JCo Provider Service. Check the list of RFC connections found in the Visual Administrator.
To prevent eavesdropping of confidential information, use SSL or SNC for communication between the J2EE system and back-end systems as well as for communication between the J2EE and the ABAP stacks for dual stacks.
Command Line: ENDIF.

Command Line: IF "YSAP-SERVERCORE" >= 710

Recommendation: To prevent unauthorized access to SAP systems via JCo, you should delete all unused RFC connections in the JCo. Check the list of RFC connections found in SAP NetWeaver Administrator.
To prevent eavesdropping of confidential information, use SSL or SNC for communication between the J2EE system and back-end systems as well as for communication between the J2EE and the ABAP stacks for dual stacks.
Command Line: ENDIF.

2.3.5 Http Connections JCo Provider (JE168)

Purpose:
To check whether only the required HTTP connections are specified in the JCo service provider.

Procedure:
1. Log on to SAP NetWeaver Administrator as an administrator.
3. Get the available HTTP destinations and enter them in the check table.

Risk Rating:
The check is rated automatically when you save:
GREEN if no HTTP connection is found.
YELLOW if HTTP connections are found.

YELLOW:
Evaluated Risk - Medium
Description: To check whether only the required Http connections are specified in the JCo service provider. We also checked whether communication between the J2EE system and the destination system is encrypted.
Result: The table below shows all configured HTTP connections:

Recommendation: To prevent unauthorized access to SAP systems via JCo, you should delete all unused HTTP connections in the JCo Provider Service. Check the list of HTTP connections found in SAP NetWeaver Administrator.
To prevent eavesdropping of confidential information, use SSL for communication between the J2EE system and destination systems as well as for communication between the J2EE and the ABAP stacks for dual stacks.

2.3.6 Communication J2EE RA to SAP Sys (JE077)
Purpose:
To check communication encryption between the resource adapter of the J2EE Engine and the SAP application servers over the JCo via SNC.
SAP Help:
- 7.0, 7.1, 7.2: Resource Adapter Security and SAP JRA Configuration
- 7.3: Java Resource Adapter
- 7.4: JRA Configuration
Procedure:
Command Line: IF "YSAP-SERVERCORE" < 710
1. Log on to SAP NetWeaver Administrator as an administrator.
3. Navigate to "deploy".
4. Under sap.com, check whether sap.com/sapjra.rar is available.
Command Line: ENDIF.
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the SAP NetWeaver Administrator as an administrator.
2. Navigate to Configuration -> Infrastructure -> Application Resources.
3. Filter or search in the "Owner Name" for "sap.com/tc~sapjra".
4. On the pane below, choose the JCA Connection Factory Details pushbutton.
Command Line: ENDIF.
Risk Rating:
GREEN: Connector is not deployed or uses SNC.
RED: Connector is deployed but does not communicate securely.

Evaluated Risk - High
Description: To check communication encryption between the resource adapter of the J2EE Engine and the SAP application servers over the JCo via SNC (Secure Network Communication).
Result: We found that the connector is deployed but does not communicate securely.
Recommendation: Use SNC to encrypt the communication between the resource adapter of the J2EE Engine and the SAP application servers via the JCo.

2.4 J2EE - Administration <;GENERAL;SID>
Purpose: To enter a chapter header in the report
Procedure: Perform the subchecks if the section is applicable to the analyzed system.
Rating: Set the rating to NOT PEFORMED if the section is not applicable. Otherwise, do not set a rating or set TOOL RATING.
2.4.1 J2EE Server Administration with Admin Tools (JE027)

**Purpose:** To prevent unauthorized administration of the J2EE Engine.

**Procedure:**

**Command Line:** IF "YSAP-SERVERCORE" >= 710
1. Log on to SAP NetWeaver Administrator as an administrator.
2. Navigate to Configuration->Infrastructure->Java Configuration Browser.
3. Navigate to security - roles -> UME User Store->administrators and open the nodes group and user.
4. Enter something other than J2EE administrator in the check table.
5. Choose the "Evaluate questionnaire" button to exempt accounts from the questionnaire.

**Command Line:** ENDIF.

**Command Line:** IF "YSAP-SERVERCORE" < 710
1. Log on to SAP NetWeaver Administrator as an administrator.
3. Navigate to "security" -> roles -> UME User Store -> administrators and open the nodes group and user.
4. Enter something other than J2EE administrator in the check table.
5. Choose the "Evaluate questionnaire" button to exempt accounts from the questionnaire.

**Command Line:** ENDIF.

**Risk Rating**
The check is rated automatically when you save:
- **GREEN:** Only J2EE system administrators have the "Administrators" security role.
- **RED:** Other users have the "Administrators" security role.
- **RED:** Evaluated Risk - High

**Description:** To prevent unauthorized administration of the J2EE Engine.

**Result:** The following users have been found to have administrator authorizations.

**Recommendation:** To prevent unauthorized administration of the J2EE Engine, assign the security role "administrator" only to the appointed administrators of the J2EE Engine. Review the users listed above to ensure that only those users that require such a high level of authorization are assigned the role of administrator.

2.4.2 J2EE Server Remote Administration with Telnet (JE028)

**Procedure:**

**Command Line:** IF "YSAP-SERVERCORE" < 710
1. Log on to SAP NetWeaver Administrator as an administrator.

**Command Line:** ENDIF.

**Command Line:** IF "YSAP-SERVERCORE" >= 710
1. Log on to SAP NetWeaver Administrator as an administrator.
2. Navigate to Configuration->Infrastructure->Java Configuration Browser

**Command Line:** ENDIF.

**Risk Rating:**
The check is rated automatically when you save:

No rating is required for this check. Add any users with telnet authorization to the check table. If there is no Telnet_Login, remove the check.

**Description:** To prevent unauthorized administration of the J2EE Engine via telnet.
Result: The following users have been found to have the security role telnet_login.

Evaluated Risk – Information

Recommendation: To prevent unauthorized administration of the J2EE Engine via telnet, assign the security role "telnet_login" only to the administrators of the J2EE Engine.

2.4.3 Additional Data Sources (JE031)

Purpose: To prevent unauthorized access to non-SAP databases.

Procedure:

Command Line: IF "YSAP-SERVERCORE" < 710
1. In NWA, choose System Management > Configuration > Application Resources.
2. Select JDBC DataSources from the Show dropdown menu.
3. Add any additional data sources found (other than SAP<SID>DB).

Command Line: ENDIF.

Command Line: IF "YSAP-SERVERCORE" >= 710
1. In NWA, choose Configuration > Infrastructure -> Application Resources.
2. Select JDBC System DataSources from the resource type filter.
3. Add any additional data sources found (other than SAP<SID>DB).

Command Line: ENDIF.

Risk Rating:
The check is rated automatically when you save:
Do not rate this check but include it if any additional data sources are found (other than SAP<SID>DB).

Description: To prevent unauthorized access to non-SAP databases.

Result: The table below shows the additional data sources that are maintained in your J2EE Engine.

Evaluated Risk – Information

Recommendation: The table shows the additional data sources maintained in your J2EE Engine. Unauthorized access to these databases may be possible.
Check whether you really need them.

2.4.4 Restriction of HTTP PUT Method (JE032)

Purpose:
To check whether file uploads are enabled and whether restrictions are in place to limit the user community allowed to perform such activities.
The HTTP PUT method belongs to a standard supported by many Web servers. It allows any kind of file to be uploaded to the server via HTTP request. The SAP NetWeaver AS Java also supports this standard in general. There is a risk that the HTTP PUT method may be misused to upload unwanted files or malware. The purpose of this check is to find out whether file uploads are enabled and whether restrictions are in place to limit the user community allowed to perform such activities.

Procedure:

Command Line: IF "YSAP-SERVERCORE" < 710
1. Log on to SAP NetWeaver Administrator as an administrator.
4. Click the global-web.xml entry and choose "Show details" to display the file content or choose download.
5. Check the parameter “Upload Enabled” and “DenyList”, and enter the values into the check table.

Command Line: ENDIF.

Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA as administrator.
2. Navigate to Configuration => Infrastructure => Java Config Browser:
3. Navigate to /Local System >cluster_config >system >instances> ID<node-ID> >
   cfg >services> servlet_jsp> persistent.
5. Check the parameter “Upload Enabled” and “DenyList”, and enter the values into the check
   table.

   Command Line: ENDIF.

   Sample file entries:

   

   

   <servlet>
   ...<init-param>
   ,,<param-name>Upload Enabled</param-name>
   ,,<param-value>true</param-value>
   ,,</init-param>
   ,,<init-param>
   ,,<param-name>DenyList</param-name>
   ,,<param-value>*.jsp;*.jspx;*.tag;*.tagx</param-value>
   ,,</init-param>
   

   <servlet>

   Risk Rating:
   GREEN: If the parameter Upload Enabled is set to “false”.
   YELLOW: If the parameter Upload Enabled is set to “true”.

   YELLOW:

   Evaluated Risk - Medium
   Description: To check whether file uploads are enabled and whether restrictions are in place
to limit the user community allowed to perform such activities.

   Result: The table below shows the parameter settings of the HTTP PUT method.

   Recommendation: The upload via the PUT method is currently enabled. Limit the upload
operations defining a list of resources that cannot be uploaded using the PutServlet. To do
this, you can use the DenyList initialization parameter of the PutServlet in the global-web.xml.
If you do not use the HTTP PUT method you may disable it for security reasons. Please see
SAP Note 1975430.
   Background: The Web Container provides protection of the default PUT implementation
provided by the PutServlet. The protection is implemented in a filter class that is mapped to
the PutServlet.

   By default, files with .jsp extension cannot be uploaded. If you need to protect other files from
being uploaded, you must add the corresponding file extensions to the value of the DenyList
initialization parameter.

   Recommendation: The upload via the HTTP PUT method is currently disabled. This is
considered a secure option however it may impact on your business processes if no upload is
possible.

   See also SAP Note 1975430.
   Background: The Web Container provides protection of the default PUT implementation
provided by the PutServlet. The protection is implemented in a filter class that is mapped to
the PutServlet.

   By default, files with .jsp extension cannot be uploaded. If you need to protect other files from
being uploaded, you must add the corresponding file extensions to the value of the DenyList
initialization parameter.
2.4.5 Restriction of Download Functions (JE144)

**Purpose:**
Every authorized user can download files from the Java engine by adding the alias @download@ to the URL of the system. The alias for the download function can only be accessed by an authenticated user with appropriate authorizations. The alias is just an additional option for accessing the download via URL. If you deactivate the alias, the known URL will not be accessible, making it more difficult for an attacker to access it.

**Procedure:**

```
Command Line: IF "YSAP-SERVERCORE" < 710
1. In NWA => System Management=> Configuration =>Virtual Hosts,
2. Under the Details pane, go to "Application Aliases".
3. Look for the application alias named @download@.
4. If this alias is activated, you can access the download function of the system by adding the alias @download@ to the URL of the system.
Command Line: ENDIF.
```

```
Command Line: IF "YSAP-SERVERCORE" >= 710
1. In NWA, navigate to Configuration => Infrastructure => Java HTTP Provider Configuration=> Virtual Hosts Tab => Application Aliases.
2. Look for the application alias named @download@.
3. If this alias is activated, you can access the download function of the system by adding the alias @download@ to the URL of the system.
Command Line: ENDIF.
```

**Risk Rating:**
GREEN if the download alias is deactivated
YELLOW if the download alias is activated (default)

**Evaluated Risk - Medium**

**Description:** We checked whether the URL download alias is deactivated.

**Result:** We found a lack of restriction of download functions.

**Recommendation:** Deactivate download alias (@download@).

```
Command Line: IF "YSAP-SERVERCORE" >= 710
Implementation:
1. In the NetWeaver Administrator, navigate to Configuration => Infrastructure.
2. There, you will find the @download@ application alias.
Command Line: ENDIF.
```

**Background:** The alias for the download function can only be accessed by an authenticated user with appropriate authorizations. The alias is just an additional option for accessing the download via URL. If you deactivate the alias, the known URL will not be accessible, which will make it more difficult for an attacker to access it. Please also take a look at the other aliases and deactivate them if not needed.

2.4.6 HTTP Based Browsing (JE033)

**Purpose:**
To ensure that system information is not disclosed as a result of HTTP-based browsing.

**Procedure:**

```
Command Line: IF "YSAP-SERVERCORE" < 710
1. Log on to NetWeaver Administrator as an administrator.
2. Go to 'System Management' -> 'Configuration' -> Virtual Hosts.
3. Choose "Default" and check that the "Directory List" option is not selected.
Command Line: ENDIF
```

```
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to NetWeaver Administrator as an administrator.
```

<Service Name>,  <Customer Name>  <date of session>
2. Go to 'Configuration Management' - 'Infrastructure' - 'Java HTTP Provider Configuration'.  
3. On the 'general' tab page, check that the "Directory List" option is not selected.  

Command Line: ENDIF  

Risk Rating:  
Check is rated automatically when you save:  
GREEN if "Directory List" is not selected.  
YELLOW if "Directory List" is selected (enabled).  

YELLOW:  
Evaluated Risk - Medium  
Description: To ensure that system information is not disclosed as a result of HTTP-based browsing.  

Result: We found that the Directory List setting is enabled.  

Command Line: IF "YSAP-SERVERCORE" < 710  
Recommendation: Turn off HTTP-based file browsing in the Visual Administrator under Cluster --> Server --> Services --> Choose the HTTP provider and deselect the "Directory List" option.  
Command Line: ENDIF.  

Command Line: IF "YSAP-SERVERCORE" >=710 Recommendation: Turn off HTTP-based file browsing in SAP NetWeaver Administrator under 'Configuration Management' - 'Infrastructure' - 'Java HTTP Provider Configuration'. On the 'general' tab page, deselect the "Directory List" option.  
Command Line: ENDIF.

2.4.7 Security of SAP Logon tickets (JE137)  
Purpose:  
To check if SAP Logon Tickets are unique.  

Procedure:  
Command Line: IF "YSAP-SERVERCORE" < 710  
1. Log on to the NWA as administrator.  
2. Navigate to Authentication and Single Sign-On: Authentication for EvaluateTicketLoginModule  
3. On the Authentication tab page, select "SAP-J2EE-Enince" in the Components table.  
4. In the "Authentication Stack", find and select "EvaluateTicketLoginModule".  
5. In the table beneath the options of login module "EvaluateTicketLoginModule", find the value of ume.configuration.active.  
For CreateTicketLoginModule  
6. On the Authentication tab page, select the "ticket" in the Components table.  
In the "Authentication Stack", find and select "com.sap.security.core.server.jaas.CreateTicketLoginModule".  
7. In the table beneath the options of login module "com.sap.security.core.server.jaas.CreateTicketLoginModule", find the parameter and value of ume.configuration.active  
Command Line: ENDIF  
Command Line: IF "YSAP-SERVERCORE" >= 710  
1. Log on to the NWA as administrator.  
3. For EvaluateTicketLoginModule  
a. On the Authentication tab page, select "SAP-J2EE-Enince" in the Components table.  
b. In the "Authentication Stack", find and select "EvaluateTicketLoginModule".  
c. In the table beneath the options of login module "EvaluateTicketLoginModule", find the value of ume.configuration.active.  
4. For CreateTicketLoginModule  
a. On the Authentication tab page, select the "ticket" in the Components table.  

<Service Name>,  <Customer Name>  <date of session>
b. In the "Authentication Stack", find and select "com.sap.security.core.server.jaas.CreateTicketLoginModule".
c. In the table beneath the options of login module "com.sap.security.core.server.jaas.CreateTicketLoginModule", find the the parameter and value of ume.configuration.active.

Command Line: ENDIF

Risk Rating:
The check is rated automatically when you choose SAVE:
GREEN: "ume.configuration.active = true" in the login modules that apply to tickets (CreateTicketLoginModule and EvaluateTicketLoginModule)
YELLOW: "ume.configuration.active" is not set in the login modules that apply to tickets (CreateTicketLoginModule and EvaluateTicketLoginModule)

Note: The recommended value need to be chosen from the pull-down list manually. If the Login Module is not available in the system, please choose "N/A" in the current value and recommended value. Otherwise the recommended value should be “True”.

Description: We checked whether the SAP logon tickets are unique.

Result: We found that the following parameter(s) are not set as recommended.

Evaluated Risk - Medium
Recommendation: Set the "ume.configuration.active = True" parameter in the login modules that apply to tickets (CreateTicketLoginModule and EvaluateTicketLoginModule).

Background: When issuing logon tickets, it is necessary to make sure that the user ID of the user for which the logon ticket has been issued is unique. For SAP Web Application Server, this includes determining the system ID and the client where the user exists. These attributes are necessary when maintaining the access control list in accepting systems and are therefore included in the user’s logon ticket.

2.4.8 HTTPONLY Setting for SAP Logon Tickets (JE138)

Purpose:
To check that the security settings of the SAP Logon Ticket are appropriate.

Procedure:
Check the UME property for the HTTPONLY setting for SAP Logon Tickets.

Command Line: IF "YSAP-SERVERCORE" < 710
1. Log on to the NWA with administrative rights.
2. Navigate to Analysis -> Configuration -> J2EE Configuration browser.
3. Drill down to cluster_data -> server -> cfg -> services -> com.sap.security.core.ume.service -> Pane: Properties
4. In the properties, filter or look for ume.logon.httponlycookie and enter it in the check table.

Command Line: ENDIF.

Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the Configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for ume.logon.httponlycookie and enter it in the check table.

Command Line: ENDIF.

Risk Rating:
The check is rated automatically when you choose SAVE:
GREEN if "ume.logon.httponlycookie" is set to "true"
YELLOW if "ume.logon.httponlycookie" is not set to "true"

Evaluated Risk - Medium
**Description:** We checked whether the security settings of the SAP logon ticket are appropriate.

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:** Set the "Ume.Logon.HTTPonlycookie" parameter to the recommended value since the "HTTPonly" setting for the logon ticket protects the SAP SSO logon ticket from being read by JavaScripts in the client browser. This reduces the risk of cross-site scripting attacks initiated by the unintentional installation of malicious JavaScripts in the client browser.

**Background:** The SAP SSO logon ticket cookie is particularly sensitive since it authenticates the user against backend systems. Whoever obtains this cookie can access the backend system with the ID of the user for whom the ticket was originally issued. Therefore, the SAP logon ticket cookie must be specially protected against theft. We also recommend using SSL encryption to secure the SAP logon tickets while they are being transferred over the network.

### 2.4.9 Enforce SSL encryption for Transfer of SAP Logon Tickets (JE139)

**Purpose:**
To check that SSL-encrypted transfer is enforced for SAP Logon Tickets

**Procedure:**
*Command Line: IF "YSAP-SERVERCORE" < 710*
1. Log on to the NWA with administrative rights.
2. Navigate to Analysis -> Configuration -> J2EE Configuration browser.
4. In the properties, filter or look for ume.logon.security.enforce_secure_cookie and enter it in the check table.
*Command Line: ENDIF.*

*Command Line: IF "YSAP-SERVERCORE" >= 710*
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for ume.logon.security.enforce_secure_cookie and enter it in the check table.
*Command Line: ENDIF.*

**Risk Rating:**
The check is rated automatically when you save:
GREEN, SSL is enforced for transfer of SAP Logon Tickets
RED, SSL is not enforced for transfer of SAP Logon Tickets

**Evaluated Risk - High**

**Description:** We checked whether SSL-encrypted transfer is enforced for SAP logon tickets.

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:** Use SSL at least between the client and the first load balancer or reverse proxy. See SAP Note 1527879 (Switching to HTTPS Transport Layer Security) and SAP Note 1531399 (SSL tips for preventing session hijacking).
Use DNS aliases in a separate subdomain for accessing the portal and the integrated systems. (See other issue for details.) After you have implemented SSL (at least between the browsers and the load balancers of the portal and all directly accessible integrated systems), set
"ume.logon.security.enforce_secure_cookie" to "True", so that the SAP Logon Ticket can only be sent via HTTPS connections.

**Background:** Setting parameter "Ume.Logon.Security.Enforce_Secure_Cookie" to "True" makes sense if HTTPS is used for accessing the portal and all integrated systems. Then, the parameter can ensure that the SAP Logon Ticket is only transferred via SSL connections. This parameter enables an indicator that has an effect in the browser. It can be activated if the connection between the browser and the first load balancer or reverse proxy uses SSL.

**Note:** It is not a prerequisite that SSL is used on the complete connections between browser and portal server, but all systems that are to receive the SAP Logon Ticket must also be accessed via HTTPS.

### 2.4.10 Control Lifetime of SAP Logon Tickets (JE140)

**Purpose:**
To check the lifetime of the SAP Logon Ticket

**Procedure:**

- **Command Line:** IF "YSAP-SERVERCORE" < 710
  1. Log on to the NWA with administrative rights.
  2. Navigate to Analysis -> Configuration -> J2EE Configuration browser.
  3. Drill down to cluster_config -> system/instances/<instance> >cfg> service> /com.sap.security.core.ume.service properties.
  4. Check the value of the LOGIN.TICKET_LIFETIME parameter.
- **Command Line:** ENDIF.

- **Command Line:** IF "YSAP-SERVERCORE" >= 710
  1. Log on to the NWA with administrative rights.
  2. On the configuration tab, choose "Infrastructure".
  3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
  4. Check the value of the LOGIN.TICKET_LIFETIME parameter.
- **Command Line:** ENDIF.

**Risk Rating:**
GREEN if LOGIN.TICKET_LIFETIME parameter is 8 or less
YELLOW if LOGIN.TICKET_LIFETIME parameter is more than 8

**Evaluated Risk - Medium**
**Description:** We checked the lifetime of the SAP logon ticket.

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:**
If integrated authentication is not used:
The recommended setting for the SAP logon ticket lifetime is the default setting of 8 hours, which corresponds to a working day. Although reducing the lifetime further may decrease the risk of someone misusing a stolen logon ticket, having to re/authenticate during work may be inconvenient for end users. Therefore, to balance usability with functionality, we usually recommend that you do not reduce the parameter value below the recommended value.

If integrated authentication is used (for example, KERBEROS/SPNego):
Since an integrated authentication via Kerberos is implemented and re-authentication is fully automatic, it is worth considering reducing the validity period of the SAP logon ticket to enforce a re-authentication via Kerberos sooner than after 8 hours.
2.4.11 Verify Setting for Domain Relaxing (JE141)

**Purpose:**
Verification of setting for domain relaxing

**Procedure:**
To check that the value of "ume.logon.security.relax_domain.level" is higher than 1:

*Command Line: IF "YSAP-SERVERCORE" < 710*
1. Log on to the NWA with administrative rights.
2. Navigate to Analysis -> Configuration -> J2EE Configuration browser.
3. Drill down to cluster_config -> system/instances/<instance> >cfg> service> /com.sap.security.core.ume.service properties.
4. In the properties, filter or look for ume.logon.security.relax_domain.level and enter it in the check table.

*Command Line: ENDF*

*Command Line: IF "YSAP-SERVERCORE" >= 710*
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for ume.logon.security.relax_domain.level and enter it in the check table.

*Command Line: ENDF*

**Risk Rating:**
The check is rated automatically as "SHOW" when you save.

Note: This check should always be included in the report.

**Description:** We verified the setting for domain relaxing.

**Result:** The table below shows the setting for domain relaxing.

**Background:** The browser sends the logon ticket only to the hosts that belong to the subdomain for which the cookie is issued by the server. The "ume.logon.security.relax_domain.level" parameter controls for which subdomains the cookie will be issued by the Java server, thus allowing the Java server to control the browser behavior.

The recommended value "1" for domain relaxing means that the SAP logon ticket is issued for all hosts that belong to exactly the same subdomain as the Java system (for example, if the Java system host name is Myhost.wdf.sap.com with domain relaxing = 1, the cookie is issued for *.wdf.sap.com). A setting higher than 2 means that even the host from the next higher domain level will receive the logon ticket (for example, if the Java system host name is Myhost.wdf.sap.com with domain relaxing = 2, the cookie is issued for *.sap.com). In most cases, the recommended setting of "1" is adequate.

See also SAP Note 791765.

2.4.12 HTTPONLY Setting for Session and Load Balancing Cookies (JE145)

**Purpose:**
To check the HTTP setting for session and load balancing cookies

**Help:**
http://help.sap.com/saphelp_nw73ehp1/helpdata/en/49/c9fa1002c8087be10000000a42189d/frameset.htm

**Procedure:**
*Command Line: IF "YSAP-SERVERCORE" < 710*
1. Log on to the NWA with administrative rights.
2. Navigate to Analysis -> Configuration -> cluster_data -> server -> cfg -> services -> http ->
Pane: properties.
3. Check the value for SystemCookiesDataProtection.

Command Line: ENDIF.

Command Line: IF "YSAP-SERVERCORE" >= 710
1. NWA: => Configuration => Infrastructure =>Java System properties:
2. Select the "Services" tab and search for the HTTP provider service.
3. Check the value of SystemCookiesDataProtection

Command Line: ENDIF.

Risk Rating:
The check is rated automatically when you save:
GREEN if value is TRUE
YELLOW if value is FALSE

YELLOW:

Evaluated Risk - Medium

Description: We checked the HTTP setting for session and load balancing cookies.

Result: The settings for session and load balancing cookies are not configured correctly.

Recommendation: The HTTP service property SystemCookiesDataProtection enables the HttpOnly attribute to be used for system cookies by configuring the property value to true. The "httponly" setting described in SAP Note 943336 protects both the JSESSIONID and the load balancing cookie SAPLB_* from being read by JavaScripts in the client browser. This reduces the risk of cross-site scripting attacks initiated by the unintentional installation of malicious JavaScripts in the client browser.

Note: You may need to keep this value set to false if your application relies on parsing one of the system cookies mentioned above via Java scripts. This is especially relevant for the JSESSIONID cookie, which reflects the J2EE servlet specification mechanism for session tracking.

Do not set the "SystemCookiesDataProtection" property to true if the ICM property "disable_url_session_tracking" is also set to true. If both properties are set to true, AS Java cannot handle HTTP sessions correctly.

2.4.13 Session Fixation Protection (JE146)

Purpose:
To check that session fixation protection is enabled.

Procedure:

Command Line: IF "YSAP-SERVERCORE" >= 710
1. NWA: => Configuration => Infrastructure =>Java System properties:
2. Select the "Services" tab.
3. Search for the Web Container (servlet_jsp) service:
4. Goto to => View => Expert Mode to show all parameters.
5. Check the following parameters:
   SessionIPProtectionEnabled
   SessionIdRegenerationEnabled

Note that in Release 7.0, the parameters are not set by default (= false). In Release 7.30, SessionIdRegenerationEnabled is set to true by default, but IP protection is deactivated.

Additional Information: When SessionIdRegenerationEnabled = true, the new session cookie JSESSIONMARKID is created in addition to JSESSIONID and is used as a secured session identifier. This session identifier will be regenerated on every new authentication.

Command Line: ENDIF.

Risk Rating:
The check is rated automatically when you save:
GREEN if both parameters are set to true
YELLOW if both parameters are not set to true
**YELLOW:**  
**Evaluated Risk - Medium**  
**Description:** We checked whether session fixation protection is enabled.

**Result:** We found that the following parameter(s) are not set as recommended.

**Recommendation:** There are two main parameters for protecting sessions against replay attacks. To minimize the risk of a session replay attack, both parameters should be set to "True".

**Additional Information:** When SessionIdRegenerationEnabled = True, the new session cookie JSESSIONMARKID is created in addition to JSESSIONID and is used as a secured session identifier. This session identifier will be regenerated on every new authentication.

SessionIPProtectionEnabled: Specifies whether the session IP protection is enabled. When this property is set to "True", the HTTP session cannot be accessed from different IPs. Only requests from the IP that started the session are processed.

See also SAP Note 1720505 – InvalidSessionException when IP protection is enabled – for possible side-effects and fixes when the parameter is enabled.

If you are using a reverse proxy server, any type of a load balancer, or SAP Web dispatcher in front of the J2EE Engine, you must configure the ClientIpHeaderName property of the HTTP Provider Service as described at http://help.sap.com/saphelp_erp60_sp/helpdata/en/ac/2bc55a78e54d60b561140048eea80cframeset.htm

SessionIDRegenerationEnabled: Specifies whether session regeneration is enabled. When this property is set to "True", the Web container regenerates the session ID on every login. The SessionIDRegenerationEnabled parameter can have rare side-effects in special scenarios. Check the description of the potential side-effects of the parameter and possible countermeasures in SAP Note 1417679.

Note that you may also need to tune the "SecuritySessionIdGracePeriod" parameter if your application allows the client to issue many HTTP requests in parallel within a short time period. For more details, see SAP Note 1464914, SAP Note 1417679, and SAP Library: http://help.sap.com/saphelp_nw73ehp1/helpdata/en/44/691ccdce2a3675e10000000a114a6b/content.htm and http://help.sap.com/saphelp_nw73ehp1/helpdata/en/a9/22118e3a3249a49f977d54fe7dac97/content.htm

### 2.4.14 Invoker Servlet (JE165)

**Procedure:**
1. NWA: => Configuration => Infrastructure => Java System properties.
2. Select the "Services" tab.
4. Find the parameter EnableInvokerServletGlobally.

**Risk Rating:**
- The check is rated automatically when you save:
- GREEN if value is FALSE
- RED if value is TRUE

**Evaluated Risk - High**  
**Description:** The invoker servlet is intended only to be used for rapid prototyping and allows HTTP clients to invoke servlets that have not been declared in the application's WEB-INF/web.xml file.

A specially crafted URL using the invoker servlet feature can allow unauthenticated access to arbitrary servlets. In addition, there is no authentication needed in order to invoke these servlets.

**Result:** The settings for Logon ticket is not configured correctly.
Recommendation: The invoker servlet feature should be disabled to close the security gap described above.

2.5 J2EE - User Store - General Checks <;GENERAL;SID>

Purpose: To enter a chapter header in the report
Procedure: Perform the subchecks if the section is applicable to the analyzed system.
Rating: Set the rating to NOT PEFORMED if the section is not applicable. Otherwise, do not set a rating or set TOOL RATING.

2.5.1 Users of Standard User Group "Administrators" (JE045)

Purpose:
To check whether any users other than system administrators belong to the standard "Administrators" group (for single stack installations) or "SAP_J2EE_ADMIN" (for dual stack installations).

Procedure:
1. Open the UME Web Administration (via NetWeaver Administration > User Management).
2. Find and select the "Administrators" group.
3. Select the "Assigned Users" tab page and choose "Go".
4. In the "Assigned Users" table, select the users that belong to the UME group "Administrators".

Risk Rating:
Check is rated automatically when you save: GREEN if no additional administrators are found. RED if additional administrators are found.

Evaluated Risk - High
Description: To check users of the standard "Administrators" (for single stack installations) or "SAP_J2EE_ADMIN" (for dual stack installations) group. This group is assigned significant and powerful authorizations and should only be assigned where absolutely necessary.

Result: The table below displays users that belong to the standard "Administrators" group. Please note that only up to 50 users are displayed in the table below.

Recommendation: Check whether all users that were identified in the "Administrators" user group need to belong to this group and remove the authorization if necessary.

2.5.2 Security of User Mapping Data (JE147)

Purpose:
To check whether user mapping information is protected using strong encryption.

Procedure:
Check ume.usermapping.unsecure.
(This parameter must not be changed. It only indicates the current status.)
Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_data -> server -> cfg -> services -> com.sap.security.core.ume.service -> properties pane.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the "ume.usermapping.unsecure" parameter.
Command Line: ENDIF.
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrator rights
2. On the configuration tab page, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or search for "User Management Engine".
4. In the properties, filter or look for the ume.usermapping.unsecure property and enter it in the check table.

Command Line: ENDIF.

Or

For all versions:
Download the configuration file.
-In the UME console, go to "Configuration", support tab "Download Configuration file".
-Open Overview properties and search for the ume.usermapping.unsecure property.

Risk Rating:
The check is rated automatically when you choose SAVE:
GREEN: ume.usermapping.unsecure is set to "false"
RED: ume.usermapping.unsecure is set to "true"

Evaluating Risk - High

Description: We checked whether user mapping information is protected using strong encryption.

Result: We found that user mapping information is not protected.

Recommendation: Install the fully featured version of the SAP Java Cryptographic Toolkit and encrypt the user mapping data in the system according to SAP Note 823286.

Background: System administrators, or anyone who manages to obtain access at administrative level, could obtain users' passwords.

2.5.3 Users of Standard User Group "Guests" (JE046)

Purpose:
To check whether users other than the 'GUEST' user belong to the standard 'Guests' group.

Procedure:
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Find and select the "Guests" group on a single stack system or 'SAP_J2EE_GUEST' group on a dual stack system.
3. Select the "Assigned Users" tab page and choose "Go".
4. Copy users except 'Guest' and 'SAP_GUEST' to the check table.

Risk Rating:
The check is rated automatically when you save:
GREEN: No users other than the 'Guest' or 'SAP_GUEST' user belong to the standard 'Guests'/'SAP_J2EE_GUEST' group.
RED: Users other than the standard guest user belong to the standard guests group.

Evaluating Risk - High

Description: To check whether users other than the 'GUEST' user belong to the standard 'Guests' group (for single stack installations) or "SAP_J2EE_GUEST" group (on dual stack installations).

Result: The table below displays users that belong to the standard "Guests" group. Please note that only up to 50 users are displayed in the table below.

Recommendation: Check whether all users in the standard GUEST user group are necessary.
2.5.4 Guest User "GUEST" should be Locked (JE148)

**Purpose:**
To check whether the guest user 'Guest' or SAP_GUEST is locked.

**Procedure:**
Check whether the guest user 'Guest'/SAP_GUEST' is locked (only one of the two users exists).
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Search for the "Guest" or "SAP_GUEST" or "J2EE_GUEST" user in a dual stack system.
3. Under the Details pane on the Account tab, check whether the user account is locked.

**Risk Rating:**
GREEN if the guest user is locked.
RED if the guest user is not locked.

**Evaluated Risk - High**
**Description:** To check whether the guest user account is locked.

**Result:** We found that the guest user account is not locked.

**Recommendation:** Lock the guest user account "Guest" (for single stack systems) or "SAP_J2EE_GUEST" (on a dual stack system).

2.5.5 Critical UME Actions of Role "Everyone" (JE149)

**Purpose:**
The "Everyone" role is a special role. A list of user permissions for "Everyone" and the actions associated with the role should be checked.

**Procedure:**
Check the actions of the "Everyone" role using the UME.
As of 7.1, you will find uncritical actions such as logon help and self registration but should not find critical actions.
1. Open the UME Web Administration (via NetWeaver Administration > User Management).
2. Find and select the "Everyone" role.
3. Select the "Assigned Action" tab page and choose "Go".
4. Find critical actions, for example, jndi_all_operations, manage_all, AclSuperUser, "UME. Manage_All", "UME.Manage_Users", "UME.Manage_Groups", "UME.Manage_Roles", "UME.Manage_Role_Assignments", "UME.Manage_All_Companies", "UME.System_Admin", "UME.Sync_Admin", "UME.Batch_Admin", "UME.Manage_My_Profile", "UME.AclSuperUser".

**Risk Rating:**
GREEN: Only non-critical permissions and actions are part of the "Everyone" role.
RED: There are critical permissions and actions within the "Everyone" role.

**Evaluated Risk - High**
**Description:** We checked the actions of the "Everyone" role, which may include critical permissions.

**Result:** We found that there were critical actions within the "Everyone" role.

**Recommendation:** Review the actions assigned to the special "Everyone" role and remove any unwanted actions from this role.

2.6 J2EE - UME User Store <;GENERAL;SID>

**Purpose:** To enter a chapter header in the report

**Procedure:** Perform the subchecks if the section is applicable to the analyzed system.
Rating: Set the rating to NOT PEFORMED if the section is not applicable. Otherwise, do not set a rating or set TOOL RATING.

2.6.1 Disabling of SAP* as User Administrator (JE064)

Purpose:
To check whether SAP* is disabled as the super administrator for user management. (If SAP* is active, you cannot log on with any other user.)

Procedure:
Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_data -> server -> cfg -> services -> com.sap.security.core.ume.service -> properties pane.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the parameter "ume.superadmin.activated".
Command Line: ENDIF
Command Line: IF "YSAP-SERVERCORE" >= 710
1. In the NWA, choose Configuration -> Infrastructure -> Java Configuration Browser.
3. Check the value of the ume.superadmin.activated parameter.
Command Line: ENDIF
All releases:
Download the configuration file.
-In the UME console, go to "Configuration", support tab "Download Configuration file".
-Open overview properties and search for "ume.superadmin.activated".

Risk Rating:
GREEN: Parameter is "false".
RED: Parameter is "true".
RED:
Evaluated Risk - High
Description: To check whether the SAP* user is disabled as the super administrator for user management.

Result: We found that the SAP* user is activated.

Recommendation: To avoid misuse of the SAP* user for UME user administration, this user should be enabled only temporarily in emergency situations (for example, if you configured user management incorrectly and can no longer log on to any applications, or all administrator users are locked). To deactivate the SAP* user, set the "ume.superadmin.activated" parameter to "False".

2.6.2 Password Authentication Allowed (JE070)

Purpose:
To check whether password logon or only certificate logon is allowed for logging on to the UME user store.

Procedure:
Command Line: IF "YSAP-SERVERCORE" < 700
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system/instances/<instance>/cfg/services/com.sap.security.core.ume.service/properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the value of the ume.logon.security_policy.cert_logon_required parameter.
Command Line: ENDIF.
Command Line: IF "YSAP-SERVERCORE" >= 700 AND "YSAP-SERVERCORE" < 730
1. Download the configuration file.
2. In the UME console, go to "Configuration", Support tab “Download Configuration file”.
3. Open overview properties and search for "ume.logon.security_policy.cert_logon_required".
Command Line: ENDIF.
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for "ume.logon.security_policy.cert_logon_required" and enter it in the check table.
Command Line: ENDIF.
Risk Rating:
Check is rated automatically when you save:
GREEN: Only certificate logon is allowed (ume.logon.security_policy.cert_logon_required =true)
YELLOW: Password logon is allowed (ume.logon.security_policy.cert_logon_required =false)
YELLOW:
Evaluated Risk - Medium
Description: To check whether password logon or only certificate logon is allowed for logging on to the UME user store.
Result: We found that password logon is allowed for logging on to the UME user store.
Recommendation: For the UME user store, you should only allow certificate logon (and not password logon) if you are using SSL. To change the logon option, change the value of the "ume.logon.security_policy.cert_logon_required" parameter.
The value "TRUE" means that only certificate logon is allowed.
The value "FALSE" means that password logon is allowed.

2.6.3 Lock Time After Failed Logon Attempts (JE048)
Purpose:
To check how many minutes a user ID is locked after a series of failed logon attempts.
Procedure:
Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services ->
com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the value of the auto_unlock_time parameter.
Command Line: ENDIF.
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for auto_unlock_time and enter it in the check table.
Command Line: ENDIF.
For all versions:
Download the configuration file.
- In the UME console, go to “Configuration”, support tab “Download Configuration file”
- Open overview properties and search for auto_unlock_time.
For all versions:
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Select "Configuration" > "Security Policy".
3. Check the value of the "Auto Unlock Time (Minutes)" property.

**Risk Rating:**
Check is rated automatically when you save:
GREEN: More than or equal to 60 minutes.
RED: Less than 60 minutes.

**Evaluated Risk - High**

**Description:** To check how many minutes a user ID is locked after a series of failed logon attempts.

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:** Set the lock time for a user ID with a series of failed logon attempts to a value greater than 60 minutes. You can do so by setting the value of the "ume.logon.security_policy.auto_unlock_time" parameter.

### 2.6.4 Number of Allowed Failed Logon Attempts (JE049)

**Purpose:**
To check how many failed logon attempts are allowed before a user ID is locked.

**Procedure:**

**Command Line:** IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system > instance > <instance> -> cfg -> services -> com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the value of the ume.logon.security_policy.lock_after_invalid_attempts parameter.

**Command Line:** ENDIF.

**Command Line:** IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for ume.logon.security_policy.lock_after_invalid_attempts and enter it in the check table.

**Command Line:** ENDIF.

**For all versions:**
Download the configuration file.

- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for ume.logon.security_policy.lock_after_invalid_attempts.

**For all versions:**
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Select "Configuration" > "Security Policy".
3. Check the value of the "Maximum Number of Failed Logon Attempts" property.

**Risk Rating:**
GREEN: Less than 6 attempts.
RED: More than 6 attempts.

**Evaluated Risk - High**

<Service Name>, <Customer Name> <date of session>
**Description**: To check how many failed logon attempts are allowed before a user ID is locked.

**Result**: We found that the number of failed logon attempts that are allowed before a user ID is locked is too high.

**Recommendation**: Set the number of permitted logon attempts to a value <= 6. You can do so by setting the "ume.logon.security_policy.lock_after_invalid_attempts" value.

### 2.6.5 New Password Includes Old Password (JE050)

**Purpose**: To check whether a new password can contain the old one.

**Procedure**:

Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration => J2EE Configuration browser,
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services -> com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check parameter "ume.logon.security_policy.oldpass_in_newpass_allowed".

Command Line: ENDIF.

Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for ume.logon.security_policy.oldpass_in_newpass_allowed and enter it in the check table.

Command Line: ENDIF.

For all versions:

- Download the configuration file.
- In the UME console, go to “Configuration”, support tab “Download Configuration file”
- Open overview properties and search for ume.logon.security_policy.oldpass_in_newpass_allowed.

For all versions:

1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Select “Configuration” > “Security Policy”.
3. Check whether the indicator “Allow Old Password as Part of New Password” is selected.

**Risk Rating**:

Check is rated automatically when you save:
GREEN, Not allowed
YELLOW, Allowed

YELLOW:

**Evaluated Risk - Medium**

**Description**: To check whether a new password can contain the old one.

**Result**: We found that the following parameter is not set as recommended.

**Recommendation**: Do not allow a new password to contain the old one. These are weak passwords that can be guessed easily by an attacker. You can change this parameter setting in "ume.logon.security_policy.oldpass_in_newpass_allowed".
2.6.6 Password Contains Alphabetic and Numeric Characters  

**Purpose:**  
To check whether the password has to include a certain number of letters and numeric characters.

**Procedure:**  
*Command Line:* IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services -> com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check parameter "ume.logon.security_policy.password_alpha_numeric_required".
*Command Line:* ENDIF.

*Command Line:* IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the "ume.logon.security_policy.password_alpha_numeric_required" parameter.
*Command Line:* ENDIF.

For all versions:
- Download the configuration file.  
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for ume.logon.security_policy.password_alpha_numeric_required.

For all versions:
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Select "Configuration" > "Security Policy".
3. Check the value of the "Minimum Number of Alphanumeric Characters in Password" property.

**Risk Rating:**  
The check is rated automatically when you save:  
GREEN if the value is > 0.  
YELLOW if the value is 0.

**Evaluated Risk - Medium**

**Description:** To check whether the password has to include a certain number of letters and numeric characters.

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:** Force a minimum number of alphabetical and numeric characters in passwords by changing the value for the "ume.logon.security_policy.password_alpha_numeric_required" parameter. For example, if the property is set to 3, passwords must contain at least 3 letters and at least 3 numbers (default value is 0).

2.6.7 Regular Password Change  

**Purpose:**  
To check whether users have to change their password on a regular basis.

**Procedure:**  
*Command Line:* IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services ->
com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the "ume.logon.security_policy.password_expire_days" parameter.

Command Line: ENDIF
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
Check the "ume.logon.security_policy.password_expire_days" parameter.
Command Line: ENDIF
For all versions:
Download the configuration file.
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for ume.logon.security_policy.password_expire_days.
For all versions:
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Select "Configuration" > "Security Policy".
3. Check the value of the "Password Validity Period (Days)" property.

Risk Rating:
The check is rated automatically when you save:
GREEN:, Password authentication is disabled or the value is <= 60.
YELLOW:, The value is between 60 and 120.
RED:, The value is > 120.
RED:
Evaluated Risk - High
YELLOW:
Evaluated Risk - Medium
Description: We checked whether users have to change their password on a regular basis.

Result: We found that the following parameter is not set as recommended.

Recommendation: Disable the password logon or force a password change at least every 60 days by changing the value for "ume.logon.security_policy.password_expire_days".

2.6.8 Minimum Password Length (JE053)

Purpose:
To check the password minimum length.

Procedure:
Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services ->
com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. In the Property pane, search for the "ume.logon.security_policy.password_min_length" parameter.
Command Line: ENDIF
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the `ume.logon.security_policy.password_min_length` parameter.

**Command Line:** `ENDIF`

For all versions:

- Download the configuration file.
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for `ume.logon.security_policy.password_min_length`.

For all versions:

1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Select "Configuration" > "Security Policy".
3. Check the value of the "Minimum Length of Password" property.

**Risk Rating:**

The check is rated automatically when you save:
- **GREEN:** Password length >= 8.
- **YELLOW:** Password length is 6 or 7.
- **RED:** Password length < 6.

**Evaluated Risk - High**

**Evaluated Risk - Medium**

**Description:** We checked the password minimum length parameter. Accounts with a low password length are easier to guess and misuse.

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:** Specify an appropriate minimum length for passwords of at least 8 characters. Change the value for "ume.logon.security_policy.password_min_length" to at least the recommended value.

### 2.6.9 Password Contains Upper and Lower Case Letters (JE054)

**Purpose:** To check whether the password has to include a certain number of upper and lower-case letters.

**Procedure:**

**Command Line:** `IF "YSAP-SERVERCORE" < 710`

1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to `cluster_config/system >instances -> <instance> -> cfg > services -> com.sap.security.core.ume.service` -> properties.
3. Turn on the filter in the Property pane.
4. Search for the "ume.logon.security_policy.password_mix_case_required" parameter.

**Command Line:** `ENDIF`

**Command Line:** `IF "YSAP-SERVERCORE" >= 710`

1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the "ume.logon.security_policy.password_mix_case_required" parameter.

**Command Line:** `ENDIF`.

For all versions:
- Download the configuration file.
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for "ume.logon.security_policy.password_mix_case_required".

For all versions:

1. Open UME Web Administration (by choosing NetWeaver Administration > User Management)
2. Select "Configuration" > "Security Policy".
3. Check the value of the "Minimum Number of Mixed Case Letters in Password" property.

**Risk Rating:**
The check is rated automatically when you save:
GREEN:,, The value is > 0.
YELLOW:,, The value is 0.

**Evaluated Risk - Medium**

**Description:** To check whether the password has to include a certain number of upper and lower-case letters. Passwords are case sensitive and using both lower and upper case increases the pool of character combinations and strengthens your password protection.

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:** Force a minimum number of uppercase and lowercase letters in passwords by changing the value for
"ume.logon.security_policy.password_mix_case_required" to at least the recommended value. For example, if the property is set to 3, passwords must contain at least 3 lowercase letters and 3 uppercase letters (default value = 0).

#### 2.6.10 Password Contains Special Characters (JE055)

**Purpose:**
To check whether the password has to include a certain number of special characters (for example, ?, !, /, ( ), #, and so on).

**Procedure:**

**Command Line:** IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system > instances -> <instance> -> cfg -> services -> com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Check the "ume.logon.security_policy.password_special_char_required" parameter.

**Command Line:** ENDIF

**Command Line:** IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the "ume.logon.security_policy.password_special_char_required" parameter.

**Command Line:** ENDIF

For all versions:

- Download the configuration file.
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for
"ume.logon.security_policy.password_special_char_required".

For all versions:
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management).
2. Select "Configuration" > "Security Policy".
3. Check the value of the "Minimum Number of Special Characters in Password" property.

**Risk Rating**
The check is rated automatically when you save:
GREEN,, The value is > 0.
YELLOW,, The value is 0.,,
Evaluated Risk - Medium

Description: To check whether the password has to include a certain number of special characters (for example, ?, !, /, (, ), #, and so on). Incorporating such characters into password constructs significantly strengthens password protection, makes passwords harder to guess, and reduces the risk of dictionary attacks.

Result: We found that the following parameter is not set as recommended.

Recommendation: Your passwords should include a certain number of special characters (such as ?, !, /, (, ), #, and so on). This can be forced by changing the value for the "ume.logon.security_policy.password_special_char_required" parameter.

2.6.11 Password Includes the User-ID (JE056)

Purpose:
To check whether the password can include the user ID.

Procedure:

Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services -> com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Check the "ume.logon.security_policy.userid_in_password_allowed" parameter.

Command Line: ENDIF.

Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the "ume.logon.security_policy.userid_in_password_allowed" parameter.

Command Line: ENDIF.

All versions:
Download the configuration file.
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for "ume.logon.security_policy.userid_in_password_allowed".

Risk Rating:
The check is rated automatically when you save:
GREEN: Value is FALSE.
RED: Value is TRUE.

Evaluated Risk - High

Description: To check whether the password can include the user ID. Allowing a user to use their user ID in the password makes the password easier to guess.

Result: We found that you currently allow your password to include the logon ID.

Recommendation: Do not allow passwords that contain the user ID.
You can do this by setting the value for "ume.logon.security_policy.userid_in_password_allowed" to "False."
2.6.12 Trivial Passwords are Not Sufficiently Prohibited (JE150)

**Purpose:**
To check how many minutes a user ID is locked after a series of failed logon attempts.

**Procedure:**
Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services -> 
   com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Check the "UME.LOGON_SECURITY_POLICY.PASSWORD_IMPERMISSIBLE" parameter.
   Command Line: ENDIF
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the UME.LOGON_SECURITY_POLICY.PASSWORD_IMPERMISSIBLE parameter.
   Command Line: ENDIF.

For all versions:
- Download the configuration file.
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for "UME.LOGON_SECURITY_POLICY.PASSWORD_IMPERMISSIBLE".

**Risk Rating:**
The check is rated automatically when you save:
GREEN if more than or equal to 100 entries
RED if less than 100 entries

**Evaluated Risk - High**
**Description:** To check whether trivial and obvious passwords are prohibited.

**Result:** We found that there were not enough entries in the "impermissible passwords" property.

**Recommendation:** Maintain at least 100 values in the "impermissible passwords" property.
You can do so by adding entries under the "ume.logon.security_policy.password_impermissible" value. Enter a comma-separated list of terms or character combinations that are rejected by the UME when users set their passwords. Use the asterisk (*) and question mark (?) as variables. An asterisk (*) stands for any sequence of characters, and a question mark (?) stands for a single character.

**Background:** This property is used to prevent passwords from being guessed easily. In this property, you can exclude your company name, town, products, and so on. You can use the wildcard ("**") for generic entries.

2.6.13 Self-Registration (JE158)

**Purpose:**
To check whether self-registration is disabled

**Procedure:**
Check whether ume.logon.selfreg is false
**Command Line: IF "YSAP-SERVERCORE" < 710**
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_data/system >instances -> <instance> -> cfg -> services ->
   com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the "ume.logon.selfreg parameter" parameter.
Or
Download the configuration file.
- In the UME console, go to "Configuration", support tab "Download Configuration file".
- Open overview properties and search for ume.logon.selfreg property.
**Command Line: ENDIF**

**Command Line: IF "YSAP-SERVERCORE" >= 710**
1. Log on to user identity management.
2. Display all roles.
3. Search for roles that have the action UME.Selfregister_User.
4. Check whether end users are assigned to the role.
**Command Line: ENDIF**

**Risk Rating:**
The check is rated automatically when you save:
GREEN if ume.logon.selfreg is set to false or end users with self-registration actions were not found.
RED if ume.logon.selfreg is set to true or enabled and end-users with self-registration actions were not found.

**RED:**
**Evaluated Risk - High**
**Description:** We checked whether self-registration is disabled.

**Result:** Self-registration for users is possible.

**Command Line: IF "YSAP-SERVERCORE" < 710**
**Recommendation:** Disable self-registration. Set the "ume.logon.selfreg" parameter to False to ensure that end users are not assigned roles that have the action "ume.selfregister_user".
**Command Line: ENDIF**

**Command Line: IF "YSAP-SERVERCORE" >= 710**
**Recommendation:** Ensure that end users are not assigned roles that have the action "ume.selfregister_user".
**Command Line: ENDIF**

**Background:** Even though a role is not assigned and content is not displayed after login, the user is able to access some components, for example, if a portal is deployed, all portal applications that are in the "low_safety" security zone.
Additionally, the user is issued an SAP Logon Ticket, which means that the user can authenticate to SSO-enabled back-end systems via Single Sign-On. This, of course, only applies if a user that already exists in the back end is created on the portal.

**2.6.14 Self-Registration of Guest User is Enabled (JE151)**

**Purpose:**
To check whether self-registration of a guest user is enabled if self-registration is enabled.

**SAP Help:**
- 7.01: UME Properties for the Security Policy

**Procedure:**
**Command Line: IF "YSAP-SERVERCORE" < 710**
If self-registration is enabled, check whether self-registration of a guest user is enabled.
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_data/system >instances -> <instance> -> cfg -> services -> com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the parameter in the Property pane.
5. Check the "ume.admin.selfreg_guest" parameter.

**Command Line:** ENDIF.

**Command Line:** IF "YSAP-SERVERCORE" >= 710

1. Log on to the NWA as administrator.
2. Choose Configuration -> Infrastructure > Java System Properties.
3. Choose the instance under the template.
4. Go to the Services tab.
5. Search for "User Management Engine".
6. In the Property pane, search for the "ume.admin.selfreg_guest" parameter.

**Command Line:** ENDIF.

**Risk Rating:**
Check is rated automatically when you save:
GREEN: Parameter is set to FALSE
YELLOW/MEDIUM: Parameter is set to TRUE
YELLOW:

**Evaluated Risk - Medium**

**Description:** Check whether self-registration of a "Guest" user is enabled.

**Result:** We found that the self-registration of a guest user is not set up as recommended.

**Recommendation:** Disable self-registration of the "Guest" user in the UME Web administration if not explicitly required.

**Procedure:** Disable self-registration for guests by setting the UME parameter "ume.admin.selfreg_guest" to "False".

### 2.6.15 Self-Management (JE152)

**Purpose:**
To check whether the end users modify their own account details.

**Procedure:**
Check whether the ume.admin.allow_selfmanagement property is false.

**Command Line:** IF "YSAP-SERVERCORE" >= 710

1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system -> instances -> <instance> -> cfg -> services -> com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. Search for the property in the Property pane.
5. Check the "ume.admin.allow_selfmanagement property" parameter.

**Command Line:** ENDIF

**Command Line:** IF "YSAP-SERVERCORE" >= 710

1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. In the properties, filter or look for ume.admin.allow_selfmanagement property and enter it in the check tab.

**Command Line:** ENDIF

Or for all versions:
Download the configuration file.
-In the UME console, go to "Configuration", support tab "Download Configuration file".
-Open overview properties and search for ume.admin.allow_selfmanagement property.

<Service Name>,  <Customer Name>  <date of session>
**Risk Rating:**
Check is rated automatically when you save:
GREEN if ume.admin.allow_selfmanagement is set to false
RED if ume.admin.allow_selfmanagement is set to true

**RED:**

**Evaluated Risk - High**
**Description:** We checked whether end users are able to modify their own account details.

**Result:** We found that end users are able to modify their own account details.

**Recommendation:** We do not recommend self-management for end users.

**Background:** If self-management is enabled, end users can modify their user account details (for example, their name and contact details) in identity management. However, this function does not allow roles to be assigned or authorizations to be enhanced.

### 2.6.16 SPML check of HTTP Header *(JE169)*

**Procedure:**

```
Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services ->
   com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. In the Property pane, search for the "UME.SPML.HTTP_HEADER_CHECK_ACTIVE" parameter.
   Command Line: ENDIF.
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the "UME.SPML.HTTP_HEADER_CHECK_ACTIVE" parameter.
   Command Line: ENDIF.
```

**Risk Rating:**
Check is rated automatically when you save:
GREEN: if value is TRUE
YELLOW: if value is FALSE

**YELLOW:**

**Evaluated Risk - Medium**
**Description:** When set to true all incoming HTTP requests are checked by the SPML service whether they contain the HTTP header "X-Requested-With" with value "XMLHttpRequest".

**Result:** We found that the following parameter is not set as recommended.

**Recommendation:** Specify the parameter appropriately. Change the value for "UME.SPML.HTTP_HEADER_CHECK_ACTIVE" to at least the recommended value.

### 2.6.17 Disabling of URL logon *(JE170)*

**Procedure:**

```
Command Line: IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
2. Drill down to cluster_config/system >instances -> <instance> -> cfg -> services ->
   com.sap.security.core.ume.service -> properties.
3. Turn on the filter in the Property pane.
4. In the Property pane, search for the "UME.LOGON.USERPWD_AUTOMATIC_LOGON" parameter.
   Command Line: ENDIF.
```

**<Service Name>, <Customer Name>, <date of session>**
parameter.
Command Line: ENDIF.
Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA with administrative rights.
2. On the configuration tab, choose "Infrastructure".
3. In the Java system properties, click the Service tab and filter or look for "User Management Engine".
4. Check the "UME.LOGON.USERPWD_AUTOMATIC_LOGON" parameter.
Command Line: ENDIF.

Risk Rating:
Check is rated automatically when you save:
GREEN: if value is FALSE
YELLOW: if value is TRUE
YELLOW:
Evaluated Risk - Medium
Description: To improve protection against login-XSRF attacks, we recommend that you disable or set to false the authentication property "Enable Automatic Logon with User ID and Password" which disables logon via URL parameters.

Result: We found that the following parameter is not set as recommended.

Recommendation: Disable the logon via URL. Change the value for "UME.LOGON.USERPWD_AUTOMATIC_LOGON" to at least the recommended value.

2.7 J2EE - Change Management <;GENERAL;SID>
Purpose: To enter a chapter header in the report
Procedure: Perform the subchecks if the section is applicable to the analyzed system.
Rating: Set the rating to NOT PEFORMED if the section is not applicable. Otherwise, do not set a rating or set TOOL RATING.

2.7.1 Password DTR Emergency User (JE084)

Purpose:
Applicable only for NWDI systems!
To check whether the password for the DTR emergency user is maintained in the property file.
Procedure:
1. Start the DTR Admin Plug-In in the NetWeaver Developer Studio.
2. Check whether an emergency user is maintained in file host:[port]/dtr/ws/system/config/active/registry/repository.properties.
3. If so, check whether the password of the emergency user is maintained.
Risk Rating:
GREEN: Emergency user password is maintained in the property file.
RED: Either no emergency user is maintained or the password is not maintained in the property file.

RED:
Evaluated Risk - High
Description: To check whether the password for the DTR emergency user is maintained in the property file. The Design Time Repository (DTR) is a repository that provides file versioning and the DTR client is part of the SAP NetWeaver Developer Studio.

Result: We determined that either no password for the DTR emergency user or no emergency user is maintained in the property file.
**Recommendation**: Create a DTR emergency user and maintain the password in the property file.

### 2.7.2 Users Authorized to Administer the SLD (JE085)

**Purpose**:  
To check whether system administrators are the only persons authorized to perform administration tasks in the System Landscape Directory (SLD).  

**Procedure**:  

*Command Line: IF "YSAP-SERVERCORE" < 700*  
1. Log on to Visual Administrator as an administrator.  
2. In the left pane, expand Cluster > Server > Services > Security Provider.  
3. In the right pane, choose Runtime > Policy Configurations and select the component sap.com/com.sap.lcr*sld.  
5. Choose the Security Roles tab page and check whether only system administrators have the J2EE security role "LcrAdministrator" or "LcrInstanceWriterAll".  
List all relevant users in the table.  
*Command Line: ENDIF.*  

*Command Line: IF "YSAP-SERVERCORE" >= 700*  
Log on to User Management as an administrator.  
In Identity Management, search for the groups "SAP_SLD_ADMINISTRATOR " and "SAP_SLD_ORGANIZER ".  
List all relevant users in the table.  
*Command Line: ENDIF.*  

**Risk Rating**:  
Check is rated automatically when you save:  
GREEN if no additional administrators found.  
YELLOW if additional administrators found.  

**Evaluated Risk - Medium**  
**Description**: To check whether system administrators are the only persons authorized to perform administration tasks in the System Landscape Directory (SLD).  

**Result**: We found additional administrators who are authorized to perform administrative tasks in the System Landscape Directory (SLD). Please note that only up to 50 users are displayed in the table below.  

**Recommendation**: Review whether all users found in the groups "SAP_SLD_ADMINISTRATOR" and "SAP_SLD_ORGANIZER" are appointed system administrators.  

### 2.7.3 Users Authorized to Activate Software in the CBS (JE086)

**Purpose**:  
To check whether developers and system administrators are the only persons authorized to activate software components in the Component Build Service (CBS).  

**Background information**:  
- SAP Note 840523: describes authorizations settings that are configured by default as of NW 7.00 SP 13 and that need to be created manually beforehand.  

**Procedure**:  
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management) and open "Identity Management".  
2. Identify UME roles that include the UME actions CBS.Developer or CBS.XDeveloper (as of Release 7.00 SP13, the UME role NWDI.Developer is available and assigned to these actions automatically when the J2EE usage type DI is initialized). Do so by selecting each role and opening the "Assigned Actions" tab page.
3. Check that only system administrators and developers are assigned to the identified role(s). List the relevant groups and users in the table.

**Risk Rating:**
Check is rated automatically when you save:
GREEN if no additional users found.
YELLOW if additional users found.

**Evaluated Risk - Medium**
**Description:** To check whether developers and system administrators are the only persons authorized to activate software components in the Component Build Service (CBS).

**Result:** We found persons other than developers and system administrators who are authorized to activate software components in the Component Build Service (CBS).

**Recommendation:** Check whether all users found with a UME role that includes the UME action "CBS.Developer" or "CBS.XDeveloper" are developers and system administrators and authorized to activate software components in the Component Build Service (CBS).

### 2.7.4 Users Authorized to Administer the CBS (JE087)

**Purpose**
To check whether the system administrators are the only persons authorized to perform administration tasks in the Component Build Service (CBS).

**Background information:**
- SAP Note 840523: describes authorizations settings that are configured by default as of NW 7.00 SP 13 and that must be created manually beforehand.

**SAP Help:**
- 7.00: Roles in the Component Build Service
- 7.00: Configuring the NWDI User Management

**Procedure**
1. Open the UME Web Administration (by choosing NetWeaver Administration > User Management) and open "Identity Management".
2. Identify UME roles that include the UME action CBS.Administrator (as of Release 7.00 SP13, the UME role NWDI.Administrator is available and assigned to this action automatically when the J2EE usage type DI is initialized). Do so by selecting each role and opening the "Assigned Actions" tab page.
3. Check that only system administrators are assigned to the identified role(s). List the relevant groups and users in the table.

**Risk Rating**
Check is rated automatically when you save:
GREEN: No additional administrators found.
YELLOW: Additional administrators found.

**Evaluated Risk - Medium**
**Description:** To check whether the system administrators are the only users authorized to perform administration tasks in the Component Build Service (CBS).

**Result:** We found users (other than system administrators) who are authorized to perform administration tasks in the Component Build Service (CBS).

**Recommendation:** Check whether all users found with a UME role that includes the UME action "CBS.Administrator" are appointed administrators.
2.8 SAP Enterprise Portal <;GENERAL;SID>

**Purpose:** To enter a chapter header in the report
**Procedure:** Perform the subchecks if the section is applicable to the analyzed system.
**Rating:** Set the rating to NOT PERFORMED if the section is not applicable. Otherwise, do not set a rating or set TOOL RATING.

2.8.1 EP - General

2.8.1.1 Use of SSL for Communication with the Portal (EP103)

**Purpose:** To check whether communication with the portal over the Internet is encrypted, especially if passwords are transmitted.

**Procedure:**
Try to access the portal over the Internet and check whether HTTP is possible. For example, type the portal address http://<host:port>/irj/portal in your browser without being connected to the SAProuter.

**Risk Rating:**
GREEN: The portal cannot be accessed from the Internet.
RED: HTTP access over the Internet is possible.

**Evaluated Risk - High**
**Description:** To check whether communication with the portal over the Internet is encrypted, especially if passwords are transmitted.

**Result:** We found that the portal communicates unencrypted over the Internet.

**Recommendation:** Implement SSL.

**Background:** Non-encrypted data could be compromised.

2.8.1.2 Use of Multiple Authentication Schemes (EP108)

**Purpose**
To check the priority of multiple authentication schemes. If two or more authentication schemes use the same login module stack (= authentication template), all these authentication schemes should have the same priority.

**Procedure**

*Command Line:* IF "YSAP-SERVERCORE" < 710
1. Choose Analysis -> Configuration -> J2EE Configuration browser.
3. Right-click the authschemes.xml entry to display its context menu. Choose 'Show details' to see the entire file content.
4. Continue with step 5 below.

*For all versions:*
The authschemes.xml file is contained in the ZIP file that can be downloaded from UME Web Administration > Configuration > Support > Download Configuration ZIP File and open it in a text editor. Open directory 'global' > open file authschemes.xml.

Continue with step 5 below.
5. Check the file for identical login modules (= authentication-templates) and their priority.
   - <authscheme name="Authscheme Name"><authentication-template>Template Name</authentication-template><priority>21</priority><frontendtype>2</frontendtype><frontendtarget>com.sap.portal.runtime.logon.certlogon</frontendtarget>
<authscheme>
Command Line: ENDISF

Command Line: IF "YSAP-SERVERCORE" >= 710
1. Log on to the NWA as administrator.
2. Choose Configuration -> Infrastructure => Config Browser.
4. In the Configurations tree, open the node cluster_data > server > persistent >
com.sap.security.core.ume.service.
5. Right-click the authschemes.xml entry to display its context menu. Choose 'Show details' to see the entire file content.
For all versions:
The authschemes.xml file is contained in the ZIP file that can be downloaded from UME Web
Administration > Configuration > Support > Download Configuration ZIP File and open it >
Open directory 'global' > open file authschemes.xml.
Continue with step 6 below.
6. Check the file for identical login modules (= authentication-templates) and their priority.
   - <authscheme name="Authscheme Name">
   <authentication-template>Template Name</authentication-template>
   <priority>21</priority>
   <frontendtype>2</frontendtype>
   <frontendtarget>com.sap.portal.runtime.logon.certlogon</frontendtarget>
 </authscheme>

Command Line: ENDISF
Risk Rating:
GREEN: If identical priorities are used or there is only one authentication scheme.
YELLOW: If different priorities are used.
YELLOW:
Evaluated Risk - Medium
Description: To check the priority level of multiple authentication schemes. If two or more
authentication schemes use the same login module stack (= authentication template), all
these authentication schemes should have the same priority level.

Result: We found that some authentication schemes have a different priority.

Recommendation: If one logon module stack (authentication template) is used in different
authentication schemes, it should have the same priority. Otherwise, users already
sufficiently authenticated may be forced to authenticate themselves a second time.
For more information, see the "Portal Platform Security Guide".

2.8.1.3 Security Mode for production systems (EP171)

Purpose:
To ensure that the productive mode is set.

Procedure:
1. NWA: => Configuration => Infrastructure =>Java System properties.
2. Select the "Services" tab and search for the Portal Runtime Container Extension
   (tc~epbc~prtc~core) service.
3. Check the value of portal.runtime.security.mode.

Risk Rating:
The check is rated automatically when you save:
GREEN if value is production
RED if value is development

RED:
Evaluated Risk - High
Description: If the Portal Runtime Security Mode is not set to “production”, then the Security Zone ACLs are not or only partially enforced. This can be used in development and test systems to simplify the development and testing processes.

Result: The settings for the security mode are not set as recommended.

Recommendation: In a productive system this parameter should be set to “production.”

2.8.2 EP - User Administration
SAP NW Application Server Java enables you to create user administrators with separate role creation and role assignment capabilities. Not only is this important for compliance reasons, but also to ensure the security of your system. An all-powerful administrator can create and assign roles as he or she pleases, leaving your system exposed to abuse by a single individual. By separating role creation and role assignment, two administrators must cooperate to abuse their powers. Therefore, instead of having a super administrator, it is recommended to create user administrator, content administrator, etc.

2.8.2.1 Portal Super Administrators Found (EP153)

Purpose
To check whether users have access to portal administration functions.

Procedure
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management) and navigate to "Identity Management".
2. Search for administrator roles (select the object type "portal role" and enter pcd:portal_content/administrator/super_admin/super_admin_role * as the search criterion, for instance).
3. For each relevant role found, open the details and check the assigned users (directly or indirectly through group assignments). Add all users found in the check table.

Risk Rating
Check is rated automatically when you save:
GREEN if no user was found.
RED if users were found.

RED:
Evaluated Risk - High
Description: To check whether users have access to super administration functions in the portal.

Result: Users have been found who have access to super administration functions in the portal. Please note that only up to 50 users are displayed in the table below.

Recommendation: The users specified in the table have authorization for super administration functions. Review these users and remove these authorizations if the users do not really need them. In order to ensure segregation of duties, it is recommended to create dedicated users for content or user administration instead of having a super administrator.

2.8.2.2 Nested Roles are Used (2019)

Purpose
To check whether a user role is included in another user role.

Procedure
1. Open the portal as an administrator and navigate to Content Administration > Portal Content.
2. Open the search form, select the ‘role’ object type, and use an empty search string to display all existing portal roles.
3. Check each role found to determine whether it contains nested roles.

**Risk Rating**
GREEN: No nested roles found.
YELLOW: Nested roles found.

**Evaluated Risk - Medium**
Recommendation: Although technically possible, it is preferable not to nest roles. First, only the end-user authorization for the top level role will be checked. Second, we generally recommend that you use a flat structure in terms of nesting groups and roles, as this increases both the transparency of the overall authorization concept and the performance of the portal.

### 2.8.2.3 Additional Portal Administrators Found (EP115)

**Purpose**
To check whether additional users have access to portal administration functions.

**Procedure**
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management) and navigate to "Identity Management".
2. Search for administrator roles (select the object type "role" and enter `pcd:portal_content/com.sap.pct/administrator/system_admin/com.sap.portal.system_admin_role` as the search criterion, for instance).
3. For each relevant role found, open the details and check the assigned users (directly or indirectly through group assignments). Add any users not stated in the questionnaire to the check table.

**Risk Rating**
Check is rated automatically when you save:
GREEN: Only those users stated in the questionnaire have authorization for administration functions.
RED: Additional users were found.

**Evaluated Risk - High**
**Description**: To check whether additional users have access to portal administration functions.

**Result**: Users have been found who have access to portal administration functions. Please note that only up to 50 users are displayed in the table below.

**Recommendation**: The users specified in the table have authorization for administration functions. Review these users and remove these authorizations if the users do not really need them.

### 2.8.2.4 Additional Portal User Administrators Found (EP117)

**Purpose**
To check whether additional users have access to portal user administration functions.

**Procedure**
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management) and navigate to "Identity Management".
2. Search for user administrator roles (select the object type 'role' and enter "pcd:portal_content/com.sap.pct/administrator/user_admin/com.sap.portal.user_admin_role" as the search criterion, for instance).
3. For each relevant role found, open the details and check the assigned users (directly or indirectly through group assignments). Add any users not stated in the questionnaire to the check table.
Risk Rating
Check is rated automatically when you save:
GREEN if only those users stated in the questionnaire have authorization for administration functions.
RED if additional users were found.
RED:

Evaluated Risk - High
Description: To check whether additional users have access to portal user administration functions.

Result: Users have been found who have access to user administration functions in the portal. Please note that only up to 50 users are displayed in the table below.

Recommendation: The users specified in the table have authorization for administration functions. Review these users and remove these authorizations if the users do not really need them.

2.8.2.5 Additional Portal Content Administrators Found (EP116)

Purpose
To check whether additional users have access to portal content administration functions.

Procedure
1. Open UME Web Administration (by choosing NetWeaver Administration > User Management) and navigate to "Identity Management".
2. Search for content administrator roles (select the object type 'role' and enter "pcd:portal_content/com.sap.pct/administrator/content_admin/com.sap.portal.content_admin_role" as the search criterion, for instance).
3. For each relevant role found, open the details and check the assigned users (directly or indirectly through group assignments). Add any users not stated in the questionnaire to the check table.

Risk Rating
Check is rated automatically when you save:
GREEN if only those users stated in the questionnaire have authorization for administration functions.
RED if additional users were found.
RED:

Evaluated Risk - High
Description: To check whether additional users have access to portal content administration functions.

Result: Users have been found who have access to content administration functions in the portal. Please note that only up to 50 users are displayed in the table below.

Recommendation: The users specified in the table have authorization for content administration functions. Review these users and remove these authorizations if the users do not really need them.

2.8.2.6 Anonymous Logon (EP113)

Purpose
To check if anonymous logon is possible.

Procedure
No action is necessary.

Risk Rating
Rating is set automatically according to the authentication schemes.
GREEN if anonymous logon is not possible.
YELLOW if write authorizations were found.
YELLOW:
Evaluated Risk - Medium
Description: To check if anonymous logon is possible.

Result: We determined that anonymous logon exists in the authentication schemes.
Recommendation: Please make sure that the users with anonymous logon only have necessary authorizations.

Background: The authorizations assigned to users with anonymous logon should not have administration functions or other sensitive content. These users should have read authorization only because the changes these users make cannot be traced.

2.8.3 Knowledge Management <;GENERAL;SID>
Purpose: To enter a chapter header in the report
Procedure: Perform the subchecks if the section is applicable to the analyzed system.
Rating: Set the rating to NOT PEFORMED if the section is not applicable. Otherwise, do not set a rating or set TOOL RATING.

2.8.3.1 Use of HTML Text Editor (KM109)
Purpose
To check whether an HTML editor is allowed for collaboration services or (as of SAP NetWeaver 7.00 SPS 8) whether the secure HTML editor is activated.

Procedure
Log on to the Enterprise Portal as an administrator.
Version 7.00 (< SPS 8): System Administration --> System Configuration --> Knowledge Management (--> Configuration) --> Content Management --> Repository Services --> Discussion Service. Check whether "Secure discussion" is selected.
Version 7.00 (> SPS 7): As of NetWeaver 7.00 SPS 8, a secure HTML editor is available. Check whether it is enabled in the portal administration by choosing System Administration > System Configuration > Knowledge Management > Content Management > Utilities > Editing > HTML Editing.

Risk Rating
GREEN if only the text editor is allowed or the Secure HTML editor is activated.
RED if the HTML editor can be used or the Secure HTML editor is deactivated.
RED:
Evaluated Risk - High
Description: To check whether an HTML editor is allowed for collaboration services or whether the secure HTML editor is activated (as of SAP NetWeaver 7.00 SPS 8).

Result: We found that the HTML editor is allowed for collaboration services or the secure HTML editor is not activated.

Recommendation: Replace the HTML editor for collaboration services with a text editor. To configure discussion services, choose the following path in the portal:
System Administration --> System Configuration --> Knowledge Management (--> Configuration) --> Content Management --> Repository Services --> Discussion Service. Select "Secure discussion".

Background: With HTML, it is possible to create malicious code such as JavaScript (for example, a popup which asks for a user name and password). This code can be executed by clicking this file.
2.8.3.2 Assignments of System Principal Privileges (KM155)

**Purpose:**
To check which users, groups, or roles have system principal privileges

**Procedure:**
1) Log on to the Portal as administrator.
2) Choose System Administration -> System Configuration -> Knowledge Management.
3) In Content Management, choose Utilities -> System Principals.
4) Check the system role.
5) By default, only the standard system users and the roles "super_admin_role", "system_admin_role", and "content_admin_role" have system principal privileges assigned.
6) Check the system user.
7) By default, only service users (cmadmin_service, ice_service, index_service, notificator_service, subscription_service, timebasedpublish_service, collaboration_service, action_inbox_service, uwl_service) should be assigned.

**Risk Rating**
GREEN if standard system users and the roles "super_admin_role", "system_admin_role", and "content_admin_role" have system principal privileges assigned
RED if non-standard system users and the roles "super_admin_role", "system_admin_role", and "content_admin_role" have system principal privileges assigned

**Evaluated Risk - High**
**Description:** We checked which users, groups, or roles have system principal privileges.

**Result:** We found users, groups, or roles that have system principal privileges.

**Recommendation:** Assign the “super_admin_role”, “system_admin_role”, and “content_admin_role” roles carefully and only if needed.

**Background:** System principal privileges give major authorizations to a user, group, or role in Content Management regardless of the ACL on the CM folders or objects.

2.8.3.3 Security of KM Repositories (KM159)

**Purpose**
To check whether KM repositories have default permissions.

**Procedure**
1. Log on to the portal as an administrator.
2. In the top-level navigation bar, choose Content Administration -> KM Content -> Toolbox -> Permissions.
3. Choose "Details" for each repository and check the permission in the new browser window that opens.
4. Check whether the permission is "Everyone", "Full Control" and enter the repository in the check table.

**SAP Notes:**
1499993 - Insecure default configuration of ACLs in KM
1648138 - Insecure default configuration of ACLs in KM repositories

How to change permissions:

**Risk Rating:**
GREEN if repositories do not contain the “Everyone”, “Full Control” authorizations.
RED if repositories contain the “Everyone”, “Full Control” authorizations.

**Evaluated Risk - High**
**Description:** To check whether the Knowledge Management (KM) repositories have default permissions.
Result: We found that the “Everyone” group of the following KM repositories has “Full control”.

Recommendation: We recommend that you remove the “Everyone”, “Full Control” authorization from the repositories listed in the table above.

Background: By default, all KM repositories and their subfolders have the default permission “Everyone: Full Control”. Since all users belong to the “Everyone” user group by default, it may allow newly registered users to access and compromise the repositories and documents.

2.8.3.4 Security of KM Reports (KM156)

Purpose
To check who is allowed to execute and view KM reports.

Procedure
No action is required. The check is processed in the "Security of KM Repositories (KM159)" check and the rating also depends on that check.

Risk Rating
GREEN if the “Reporting” repository does not contain the "Everyone", "Full Control" authorizations.
RED if the "Reporting" repository contains the "Everyone", "Full Control" authorizations.
RED:
Evaluated Risk - High
Description: To check who is allowed to execute and view Knowledge Management (KM) reports.

Result: We found that “Everyone” is allowed to start and execute KM reports.

Recommendation: We recommend that you remove the “Full Control” permission for the “Everyone” user from the "Reporting" repository and its subfolders.

Background: KM reports are used to perform evaluations across the system. Some reports also allow you to carry out certain operations. With “read” authorization, you can view reports in the “Reporting” repository; with “write” permission, you can also run these reports. The reports themselves are executed with a service user that has all permissions by default.

2.8.3.5 Use of HTML Text Editor

Purpose
To make sure that the secure HTML editing is activated.

Procedure
No action required.

Rating
This check will be rated GREEN automatically.
GREEN:
With HTML, it is possible to create malicious code such as JavaScript (for example, a popup which asks for a user name and password). This code can be executed by clicking this file. Therefore, the most secure way to use the HTML editor is enabling the secure HTML editor and activating only the basic formatting.

Recommendation: Follow the Portal path System Administration > System Configuration > Knowledge Management > Content Management > Utilities > Editing > HTML Editing, and make sure that the two options in the table are activated.
2.8.3.6 Assignments of System Principal Privileges

**Purpose**
To make sure that only standard system roles and users have principal privileges.

**Procedure**
No action required.

**Rating**
This check will be rated GREEN automatically.

**GREEN:**
System principal privileges give major authorizations to a user, group, or role in Content Management regardless of the ACL on the CM folders or objects. Therefore, only standard system users and system roles should have system principal privileges assigned.

Recommendation:
Follow the Portal path System Administration > System Configuration > Knowledge Management > Content Management > Utilities >System Principals, and make sure that for both System roles and system users only standard system roles and users in the table below are assigned.

2.8.3.7 Security of KM Repositories

**Purpose**
To make sure that appropriate permissions for KM repositories are assigned.

**Procedure**
No action required.

**Rating**
This check will be rated GREEN automatically.

**GREEN:**
After installation, all KM repositories and their subfolders have the default permission “Everyone-Full Control”. Since all users belong to the Everyone-user-group by default, it may allow newly registered users to access and compromise the repositories and documents. To restrict access to KM repositories and to secure content and configurations, appropriate permissions have to be assigned. Please refer to SAP Notes 1499993 and 1648138.

Recommendation:
We strongly recommend that you change some of the initial permissions to meet your requirements.
Make sure you are logged on as user with the Super Administrator role.
In the top-level navigation bar, click Content Administration → KM Content → Toolbox → Permissions.
Navigate to a folder where you need to adapt permissions and choose Details. The permissions page with all the functions you need to adapt permissions opens.
Change the permissions to meet your requirements and as recommended in SAP Note 599425.

We also recommend that you remove the “Full Control” permission for the “Everyone” user from the "Reporting" repository and its subfolders. KM reports are used to perform evaluations across the system. Some reports also allow you to carry out certain operations. With “read” authorization, you can view reports in the “Reporting” repository; with “write” permission, you can also run these reports. The reports themselves are executed with a service user that has all permissions by default.
2.9 System Recommendations (JAVA) (SY124)

Purpose
To check whether the System Recommendations tool is being used. This is a mandatory prerequisite for setting up a strong security patch process.
For further recommendations, refer to http://support.sap.com/sysrec.

Procedure
This check is analyzed and rated automatically. No further action is necessary.

Rating
The rating is set automatically.
GREEN: The System Recommendations tool is used and shows results that are up to 31 days old.
YELLOW:
- The System Recommendations tool is used but the results are older than 31 days.
- The System Recommendations tool is not used for this system.
- The System Recommendations tool is not used at all.
RED:
Comment Line: DO NOT DELETE OR CHANGE!
Comment Line: Text is being created during runtime.
YELLOW:
Comment Line: DO NOT DELETE OR CHANGE!
Comment Line: Text is being created during runtime.
GREEN:
Comment Line: DO NOT DELETE OR CHANGE!
Comment Line: Text is being created during runtime.

Recommendation: SAP strongly recommends applying important security fixes as soon as possible.
The 'System Recommendations' application provides a detailed recommendation regarding which SAP security notes (ABAP and non-ABAP) should be implemented based on the actual status of the system and the notes already implemented. This is a mandatory prerequisite for setting up a strong security patch process. For more information, refer to http://support.sap.com/sysrec.