Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.
Abstract

Software security remains a critical topic of interest to all companies and to the information technology industry. The security of a specific system thereby also significantly depends on the secure configuration of this system.

With Configuration Validation within SAP Solution Manager, SAP offers a tool to validate various kinds of software configuration items. This helps to standardize and harmonize configuration items within the ABAP and Java world cross system, using a single configuration item repository within SAP Solution Manager.

In this hands-on session participants learn to use configuration validation templates with typical use cases in the space of Security Validation. The basic set-up of Configuration Validation is explained step by step and described for typical reporting scenarios. As the use case, a typical software level and parameter validation scenario will be implemented. We’ll use the latest options of SAP Solution Manager 7.1 to define a target system which exactly matches the strong requirements of many corporate security policies.
Agenda

- **Best Practices-based Services**

  **Security Tools and Services**

  - EarlyWatch Alert (EWA) – Security Chapter
  - Security Notes Report (RSECNOTE)
  - System Recommendations
  - Security Optimization Service (SOS)
  - Configuration Validation

- Run SAP Standard for Security

Appendix

- SAP Enterprise Support Report
Establishing Security in a Structured Approach

ANALYZE – the vulnerable points of the SAP solution in order to

- Decrease the risk of a system intrusion
- Ensure the confidentiality of business data
- Ensure the authenticity of users
- Substantially reduce the risk of costly downtime due to wrong user interaction

CHECK – and implement Application Lifecycle Security

- Security Patch Management / System Recommendation
- Security Configuration Monitoring e.g. EarlyWatch Alert, Security Optimization Service and Configuration Validation

SAFEGUARD – implementation of security functionality

- Secure configuration e.g. SAP Gateway Security and SAP Message Server Security
- SAP BusinessObjects Governance, Risk, and Compliance Solutions
- SAP NetWeaver Identity Management
Security Management – Continuous Process Along a Quality Circle

- Establish the objectives and processes necessary to deliver results in accordance with the expected output.
- Implement the new processes and procedures.
- Analyze the differences and determine their root cause. Determine where to apply changes that will lead to improvements and the expected results.
- Measure the new processes and compare the results via indicators (KPIs) against the expected results in order to identify possible differences.

The security plans (Plan) are implemented (Do) and the implementation is then evaluated (Check). After the evaluation both plans and implementation of the plan are carried out (Act).
IT Security Lifecycle Based on the SAP Solution Manager

- Configuration Validation
- + EGI Empowerment

- GRC Solutions
- + Safeguarding
- SAP NW IdM
- + Safeguarding
- Single Sign On Solutions
- + Safeguarding
- SOS EoD Services

- SOS Remote Service
- SOS Onsite Service

For each IT organization

- Value Proposition
- RunSAP Security Standard
- Security Workshop
- Security On-boarding

- Security in EWA
- Security in TSM
- Security in ESR
- SOS Self Service
- + EGI Empowerment

Security Notes Recommendations
- Security Notes Tool RSECNOTE
- System Recommendations

EGI  Expert Guided Implementation
ESR  Enterprise Support Report
EWA  EarlyWatch Alert
SOS  Security Optimization Service
SSO  Single Sign-On
GRC  Governance, Risk & Compliance
Agenda

➡️ **Best Practices-based Services**

**Security Tools and Services**

➡️ *EarlyWatch Alert (EWA) – Security Chapter*

➡️ *Security Notes Report (RSECNOTE)*

➡️ *System Recommendations*

➡️ *Security Optimization Service (SOS)*

➡️ *Configuration Validation*

➡️ **Run SAP Standard for Security**

**Appendix**

➡️ *SAP Enterprise Support Report*
The Role of EarlyWatch Alert (EWA) for Security

SAP EarlyWatch Alert (EWA) (see http://service.sap.com/ewa)

SAP EarlyWatch Alert is an important part of making sure that your core business processes work. It is a tool that monitors the essential administrative areas of SAP components and keeps you up to date on their performance and stability. SAP EarlyWatch Alert runs automatically to keep you informed, so you can react to issues proactively, before they become critical.

Security in the EarlyWatch Alert:

- The EWA Report includes selected information on critical security observations
  - SAP Security Notes: ABAP and Kernel Software Corrections
  - Default Passwords of Standard Users
  - Password Policy
  - Gateway and Message Server Security
  - Users with Critical Authorizations
- More detailed and additional information can be found with the help of the security self-services
EarlyWatch Alert in the “SAP Engagement and Service Delivery” Work Center

Filter sessions by your solution
System name is shown in column “Context”
Alerts are visible on tab “Details”
Access Word report on tab “Attachments”
EarlyWatch Alert in the “System Monitoring” Work Center

Filter sessions by your solution
Generate HTML report
During this EarlyWatch Alert Session, we detected issues that could potentially affect your system. We recommend that you take corrective action as soon as possible.

**Alert Overview**

- [-] Standard users including SAP or DDI have default passwords.
- [-] Security-related SAP HotNews have not been applied in the system.
- [-] Security weaknesses identified in the Gateway or the Message Server configuration

**Check Overview**

<table>
<thead>
<tr>
<th>Topic Rating</th>
<th>Topic</th>
<th>Subtopic Rating</th>
<th>Subtopic</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Security</td>
<td>[ ]</td>
<td>SAP Security Notes: AGAP and Kernel Software Corrections</td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td>[ ]</td>
<td>Default Passwords of Standard Users</td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td>[ ]</td>
<td>Password Policy</td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td>[ ]</td>
<td>Gateway and Message Server Security</td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td>[ ]</td>
<td>Users with Critical Authorizations</td>
</tr>
</tbody>
</table>
EarlyWatch Alert Chapter “Security”
Overview

7 Security

Critical security issues were found in your system.
See the information in the following sections.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>Security-related SAP Notes</td>
</tr>
<tr>
<td>🔴</td>
<td>Default Passwords of Standard Users</td>
</tr>
<tr>
<td>✔</td>
<td>Password Policy</td>
</tr>
<tr>
<td>🚫</td>
<td>Gateway and Message Server Security</td>
</tr>
<tr>
<td>🚫</td>
<td>Users with Critical Authorizations</td>
</tr>
</tbody>
</table>
7.1 SAP Security Notes: ABAP and Kernel Software Corrections

Software corrections from SAP Security HotNews have been identified as missing on this system. Most probably, your system is exposed to corresponding security threats.

**Recommendation:** Apply SAP Security Notes, which are relevant to your system!


The tool RSECNTE in transaction ST13 provides you with a list of those SAP Security Notes that have been identified as missing in this EWA check. RSECNTE covers SAP's Security HotNews with software-related corrections for ABAP or Kernel and an additional selection of SAP Security Notes.

For more information, refer to SAP Note [888889](https://service.sap.com/securitynotes).

In the Security Notes list on the SAP Service Marketplace referenced above, the flag “Automatic check in EWA” (last column) identifies those SAP Security Notes, for which the implementation is completely checked in the EWA.

In tool RSECNTE, 7 SAP Security Notes have manually been marked as not to be considered.
7.2 Default Passwords of Standard Users

Standard users including SAP® or DDIC have default passwords.

**Recommendation:**
Use report **RSUSR003** to check the usage of default passwords by standard users.

Ensure that
- user SAP® exists in all clients
- users SAP®, DDIC, SAPCPIC and EARLYWATCH have non-default passwords in all clients
- profile parameter login/no_automatic_user_sapstar is set to 1.

For more information, see section "Protecting Standard Users" and section "Profile Parameters for Logon and Password (Login Parameters)" either in the SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

Make sure that the standard password for user TMSADM is changed in client 000 and delete this user in any other client. The SAP note **1414256** describes a support tool for changing the password of user TMSADM in all systems of the transport domain.
7.3.1 Password Complexity

PARAMETER: LOGIN/MIN_PASSWORD_LNG

<table>
<thead>
<tr>
<th>Rating</th>
<th>Instance</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>All instances</td>
<td>3</td>
<td>8</td>
</tr>
</tbody>
</table>

The current system settings allow a minimum password length less than 6 characters. This allows weak passwords. Attackers may successfully recover such passwords and exploit this to gain unauthorized access to the system.

**Recommendation:** Use a minimum value of 8 for the profile parameter `login/min_password_lng`.

In addition, SAP provides options to enforce complex passwords. Find the current settings of the corresponding profile parameters in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Instance</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/min_password_letters</td>
<td>All instances</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_uppercase</td>
<td>All instances</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_lowercase</td>
<td>Instance dependent</td>
<td>3; 5; 0</td>
</tr>
<tr>
<td>login/min_password_digits</td>
<td>All instances</td>
<td>2</td>
</tr>
<tr>
<td>login/min_password_specials</td>
<td>Instance dependent</td>
<td>1; 3; 5</td>
</tr>
</tbody>
</table>
7.3.2 Validity of Initial Passwords

**PARAMETER:** login/password_max_idle_initial

<table>
<thead>
<tr>
<th>Rating</th>
<th>Parameter</th>
<th>Instance</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚫</td>
<td>login/password_max_idle_initial</td>
<td>All instances</td>
<td>0</td>
</tr>
</tbody>
</table>

Initial passwords are valid for an unrestricted time.

**Recommendation:**
Restrict the password validity to 14 days or less. More information can be found in SAP Note [862989](https://support.sap.com) and in section "Profile Parameters for Logon and Password (Login Parameters)" either in the SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.
7.4 Gateway and Message Server Security

7.4.1 Kernel Patch Level

<table>
<thead>
<tr>
<th>Rating</th>
<th>Kernel Release</th>
<th>Current Kernel Patch Level</th>
<th>Minimal Required Kernel Patch Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>701</td>
<td>89</td>
<td>98</td>
</tr>
</tbody>
</table>

To enable certain Gateway and Message Server security functionality, a minimum patch level of the kernel is required. Your system currently misses this requirement.

**Recommendation:**

Update the kernel of your system to the newest kernel patch level available. At least update to a kernel patch level equal or higher than the minimal required kernel patch level given above. Additional information can be found in SAP Note 1298433.
7.4.2 Gateway Security

Gateway Security Properties

The parameter gw/reg_no_conn_info controls the activation of certain security properties of the SAP Gateway. It is defined as a bit mask with one bit per property.

On your system the following properties were identified:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Value Name</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bypassing security in reg_info &amp; sec_info</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>✔️</td>
<td>Bypassing sec_info without reg_info</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>CANCEL registered programs</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Uppercase/lowercase in the files reg_info and sec_info</td>
<td>0</td>
<td>8</td>
</tr>
</tbody>
</table>

**Recommendation:**
Enable the missing properties by adding the respective recommended values to the current value of gw/reg_no_conn_info.

More information regarding gw/reg_no_conn_info can be found in SAP Note [1444282](http://support.sap.com/1444282).
Enabling an Initial Security Environment

**PARAMETER: gw/acl_mode**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>★</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**Recommendation:**
Parameter gw/acl_mode can be set to 1 to activate a more secure default behavior in case that either of the access control lists defined by gw/sec_info and gw/reg_info does not exist.
SAP recommends to set gw/acl_mode=1 to establish an additional line of defense in case any of the mentioned access control lists is missing.
More information can be found in SAP Note 1480644.

Gateway Access Control Lists

**PARAMETERS: gw/sec_info gw/reg_info**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Instance</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>★</td>
<td>All instances</td>
<td>gw/sec_info is not defined or empty</td>
</tr>
</tbody>
</table>

**Recommendation:**
The profile parameters gw/sec_info and gw/reg_info provide the file names of the corresponding access control lists. These access control lists are critical to control the RFC access to your system including connections to RFC servers. You should create and maintain both access control lists, which can be done via transaction SMGW. More information can be found in SAP Note 1425765.
7.4.3 Message Server Security

Separation of Internal and External Message Server Communication

<table>
<thead>
<tr>
<th>Parameters: rdisp/msserv rdisp/msserv_internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rating</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>![ ]</td>
</tr>
<tr>
<td>![ ]</td>
</tr>
</tbody>
</table>

**Recommendation:**
Communication with the message server should be separated into SAP system internal communication (TCP/IP port defined by rdisp/msserv_internal) and communication e.g. from user SAPGUIs to the system (TCP/IP port defined by rdisp/msserv). Network firewalls should block access to the port given in rdisp/msserv_internal from outside the SAP system. Set parameter rdisp/msserv_internal to a TCP/IP port number different to the port number given in rdisp/msserv and additionally protect access to the internal message server port by appropriate firewalls. More information can be found in SAP Note 821875.
Message Server Administration Allowed for External Clients

**PARAMETER: MS/MONITOR MS/ADMIN_PORT**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Parameter</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>![High Risk Icon]</td>
<td>ms/monitor</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>![High Risk Icon]</td>
<td>ms/admin_port</td>
<td>12345</td>
<td>0</td>
</tr>
</tbody>
</table>

**Recommendation:**
SAP recommends to block external administration of the message server by setting the profile parameters ms/monitor and ms/admin_port both to the value 0. More information can be found in SAP Note 821875.

The profile parameter ms/admin_port can be set dynamically via transaction SMMS -> Goto -> Security Settings.

Message Server Access Control List

**PARAMETER: MS/ACL_INFO**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>![High Risk Icon]</td>
<td>ms/ACL_INFO is not defined or empty</td>
</tr>
</tbody>
</table>

**Recommendation:**
The profile parameter ms/ACL_INFO provides the file name of the message server’s access control list. This list controls, which application servers are allowed to log on to the message server. SAP recommends to define and properly maintain this list to prohibit rogue application servers to join the system. More information can be found in SAP Note 821875.
7.5 Users with Critical Authorizations

For more information about the following check results, please refer to SAP Note [863362].

[...]

7.5.1 Users Authorized to Display all Tables

Unauthorized access to sensitive data is possible if too many users are granted this authorization. The number of users with this authorization is stated for each client.

<table>
<thead>
<tr>
<th>Client</th>
<th>No. of Users Having This Authorization</th>
<th>No. of Valid Users</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>600</td>
<td>222</td>
<td>249</td>
<td></td>
</tr>
<tr>
<td>800</td>
<td>4110</td>
<td>4292</td>
<td></td>
</tr>
</tbody>
</table>

**Authorization objects:**

Object 1: S_TCODE with TCD=SE16, TCD=SE16N, TCD=SE17, TCD=SM30, or TCD=SM31
Object 2: S_TABU_DIS with ACTVT = 03 or 02 and DICBERCLS = *

7.5.2 Users Authorized to start all Reports

7.5.3 Users Authorized to Debug / Replace

7.5.4 Users Authorized to Display Other Users Spool Request
Exercises

EarlyWatch Alert report
Agenda

- Best Practices-based Services

Security Tools and Services
- EarlyWatch Alert (EWA) – Security Chapter
- Security Notes Report (RSECNOTE)
- System Recommendations
- Security Optimization Service (SOS)
- Configuration Validation

Run SAP Standard for Security

Appendix
- SAP Enterprise Support Report
Value Proposition

The SAP Security Optimization Service is designed to verify and improve the security of the SAP systems of customers by identifying potential security issues and giving recommendations on how to improve the security of the system.

Keeping the security and availability of customer SAP solutions high is a tremendous value to customers’ businesses - a value delivered by the SAP Security Optimization Service. Analysis is the key to this value, which is necessary to:

- Decrease the risk of a system intrusion
- Ensure the confidentiality of business data
- Ensure the authenticity of users
- Substantially reduce the risk of costly downtime due to wrong user interaction

More information can be found under the alias SOS in the SAP Service Marketplace:

http://www.service.sap.com/sos
SAP Security Optimization Service – Overview

- The SAP Solution Manager offers the possibility to locally execute the SAP Security Optimization Service
  - All completely automated checks in ABAP systems
  - No additional costs for this service

SAP Security Optimization

- Broad range of security checks extending the Self-Service checks
- Performed by experienced service engineers
- Part of CQC service offering

SAP Security Optimization Remote Service

- Individual range of security checks, e.g. for the SAP Enterprise Portal
- Performed by specialists
- Additional costs for this service

SAP Security Optimization Onsite Service
Security Optimization Service
Scope of Remote Service and Self Service

**SAP NetWeaver Application Server ABAP**
- Basis administration check
- User management check
- Super users check
- Password check
- Spool and printer authorization check
- Background authorization check
- Batch input authorization check
- Transport control authorization check
- Role management authorization check
- Profile parameter check
- SAP GUI Single Sign-On (SSO) check
- Certificate Single Sign-On (SSO) check
- External authentication check

**SAP NetWeaver Application Server Java**
- Landscape check
- Configuration check
- SSL check
- Administration check

**SAProuter**
- SAProuttab check
- OS access check
- SNC check

**SAP Enterprise Portal**
- Landscape check
- Configuration check
- Administration check
- SSL check
- Authorization check for portal content, user management and administration

Scope of the SOS Self Service
Scope of the Security Optimization Self Service for the SAP NetWeaver Application Server ABAP

- Basis administration check
- User management check
- Super users check
- Password check
- Spool and printer authorization check
- Background authorization check
- Batch input authorization check
- Transport control authorization check
- Role management authorization check
- Profile parameter check
- SAP GUI Single Sign-On (SSO) check
- Certificate Single Sign-On (SSO) check
- External authentication check
In order to determine the actual risk, the vulnerabilities are ranked using a rating logic. The rating is based on the severity and probability of each vulnerability.

A report is created containing the identified vulnerabilities of the analyzed SAP system. The report contains recommendations to eliminate or reduce the vulnerabilities found during the Security Optimization Service.

The implementation of the recommended security measures can be done:
- By the customer
- By SAP security consulting
- By certified SAP partners

Managed System

Solution Manager
Questionnaire

The questionnaire is filled out by the customer to prepare the service.
The questionnaire contains about 25 questions.
Specification of known users with critical authorizations in the questionnaire skips them from the report.
This helps to keep the report readable and to do a correct risk analysis.
Customize the look of the report.
Selection of the tested clients.

2.1 Print the User Data (All Checks)
Procedure
If you want user data (first name, last name and department of the user) printed in the User Data*.
If you do not select, the field only the user name is printed.
When creating the ST14 data the sending of the user data to SAP(first and last name) parameter.

Print User Data?
Flag
Activate if user data wanted

2.2 Download and Check for Very Weak Passwords (0145)
Procedure
If you want your user passwords checked, select the field "Download Encrypted Passwords".
In this case we download the encrypted passwords of your users and try a very simple dictionary attack on them.

Download passwords?
Flag
Activate if pwd check wanted

2.3 User for Remote Access from SAP (0531)
Procedure
Enter the name of the user (or one of the users) that you hand over to SAP for logging on to your SAP system.

Client

User ID

2.4 User Segregation (0004)
Procedure
If you have segregated your users in different user groups, select the field "User Segregation" in the table.

Segregation in Usergroups
Flag
Activate checkbox if used

2.5 Super Users (0021)
Procedure
List for each client the known super users.
These are the users having the profile SAP_ALL.
- Please mention the users with user type "dialog", "service", "system" or "communication".
- If a super user exists in all clients, you can also insert "ALL" in the field "Client" instead of listing all clients.

Client

User

© 2012 SAP AG. All rights reserved.
### Customer Report: Action Items

The action items list on top of the report gives a good overview about the complete system status. The action items are created automatically of all checks rated with high risk. The list can be individually adapted.

We use the red traffic light as “high risk” and the yellow traffic light as “medium risk.” “Green” results are normally skipped in order to reduce the size of the report.

All checks have a four-digit identifier which allows to find the detailed description in the report easily.

<table>
<thead>
<tr>
<th>Issue Description</th>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Optimization, Sample Customer</td>
<td><strong>3 Detected Issues</strong></td>
</tr>
<tr>
<td><strong>Action Items</strong></td>
<td></td>
</tr>
<tr>
<td>1 Users - Other Than the System Administrators - Are Authorized to Call ST14 7. (0168)</td>
<td></td>
</tr>
<tr>
<td>6 Users - Other Than the System Administrators - Are Authorized to Maintain Users (0002)</td>
<td></td>
</tr>
<tr>
<td>1 Users - Other Than System Administrators - Are Authorized to Maintain System Profiles (0152)</td>
<td></td>
</tr>
<tr>
<td>6 Users Are Authorized to Execute All Function Modules</td>
<td></td>
</tr>
<tr>
<td>8 Users Are Authorized to Access Tables with User Data (0013)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Maintain Authorizations Directly in the Production System (0074)</td>
<td></td>
</tr>
<tr>
<td>1 Unexpected Users Are Authorized to Change a Super User Accounts (0026)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Delete an Authorization Check Before Transaction Start (0111)</td>
<td></td>
</tr>
<tr>
<td>5 Users Are Authorized to Delete a Client (0306)</td>
<td></td>
</tr>
<tr>
<td>7 Users Are Authorized to Create New Clients (0305)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Maintain Authorizations Directly in the Production System (0074)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Maintain Authorization Group of Tables (0515)</td>
<td></td>
</tr>
<tr>
<td>6 Users Are Authorized to Start/Stop Application Servers (0154)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Maintain System Profiles (0152)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Maintain Trusted Systems (0240)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Maintain Trusting Systems (0268)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for User Maintenance (0511)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Role Maintenance (0512)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Authorization Maintenance (0513)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Role Maintenance (0512)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Authorization Maintenance (0513)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Role Maintenance (0512)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Authorization Maintenance (0513)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Role Maintenance (0512)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Authorization Maintenance (0513)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Role Maintenance (0512)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Authorization Maintenance (0513)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Role Maintenance (0512)</td>
<td></td>
</tr>
<tr>
<td>1 Users Are Authorized to Call Function Modules for Authorization Maintenance (0513)</td>
<td></td>
</tr>
</tbody>
</table>
Customer Report: 
Example of an Authorization Check

Information in the checks:

Explanation of the vulnerability
Some “Unexpected” users having this authorization
The number of unexpected users
A recommendation how to handle this situation
All checked authorization objects

6.3.7 Users - Other Than the Spool Administrators - Are Authorized to Print on all Devices (0197)

Output of sensitive data can be sent accidentally to a wrong printer and could be accessed by an unauthorized employee.

<table>
<thead>
<tr>
<th>Client</th>
<th>User</th>
<th>Type</th>
<th>Last Name</th>
<th>First Name</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>AARONF</td>
<td>A</td>
<td>Aaron</td>
<td>Frank</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>ANTONOV</td>
<td>A</td>
<td>Antonov</td>
<td>Igor</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>AUTUMW</td>
<td>A</td>
<td>Autumn</td>
<td>Wallis</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BARCANI</td>
<td>A</td>
<td>Barcan</td>
<td>Ivory</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BLACKBEARDC</td>
<td>A</td>
<td>Blackbeard</td>
<td>Christ</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BLUEBERRYA</td>
<td>A</td>
<td>Blueberry</td>
<td>Agneta</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BLUMBERGH</td>
<td>A</td>
<td>Blumberg</td>
<td>Harald</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BRAUERM</td>
<td>A</td>
<td>Brauer</td>
<td>Michael</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BUSHH</td>
<td>A</td>
<td>Bush</td>
<td></td>
<td>OFFICE</td>
</tr>
<tr>
<td>300</td>
<td>FERRYG</td>
<td>A</td>
<td>Ferry</td>
<td>Greg</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>HENSGNERJ</td>
<td>A</td>
<td>Hensgner</td>
<td>Joan</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>KINGD</td>
<td>A</td>
<td>King</td>
<td>David</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>KINGF</td>
<td>A</td>
<td>King</td>
<td>Frank</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>LANDISG</td>
<td>A</td>
<td>Landis</td>
<td>George</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>ROBERTA</td>
<td>A</td>
<td>Robert</td>
<td>Alexander</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>VOLKOVIC</td>
<td>A</td>
<td>Volkov</td>
<td>Chris</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>WINTERH</td>
<td>A</td>
<td>Winter</td>
<td>Natascha</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>XERTAMY</td>
<td>A</td>
<td>Xertam</td>
<td>Yanis</td>
<td></td>
</tr>
</tbody>
</table>

Count: 220

Evaluated result:
More than 20% of your users, of at least one client, can print on all devices.

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

Authorization object:
Object: S_SPO_DEV with SPODEVICE = *.
Sample Questionnaire and Report
How to Identify „Top Issues“
Candidate „Missing Security Notes“

Candidate: „**Missing Security Notes**“

Threat: Missing security Notes – especially missing Security HotNews – point to security weaknesses which are identified as present in your system. These weaknesses may have the potential to be exploited by anyone to anonymously execute code, access data or change your system bypassing system settings and authorization checks.

In the SOS report look for section „**Basis Authorization“ – „Basis Administration“ – „Security-related SAP Notes““

Action: Identify, which Security Notes are missing and implement them on the system
How to Identify „Top Issues“
Candidate „Standard Users with Default Password“

- Candidate: „Standard Users with Default Password“
- Threat: Standard users with default passwords allow anyone, who is able to establish a network connection to your system, to anonymously enter it and execute code under potentially high authorizations.
- In the SOS report look for section „User Authorization“ – „Standard Users“
  Check-ID 0041
- Action: Change the password
- Remark: Look for the other checks in this SOS section as well. They also contain valuable recommendations to protect your system from this threat!
How to Identify „Top Issues“
Candidate „Insufficient Password Policy“

Candidate: „Insufficient Password Policy“
Threat: Weak passwords may give unauthorized people access to potentially powerful accounts. This risks the confidentiality, integrity and availability of your data.

In the SOS report look for section „Authentication“ – „Passwords“ Check-ID 0123

Action: Carefully review the whole „Password“ section of the SOS. Decide on an appropriate password policy (if not already defined) and implement it with recommended settings as given suggested in the SOS report.
4 Special Focus Checks

4.1 Additional Super User Accounts Found (0022)
In this system, the following super user accounts were found that were not mentioned in the questionnaire. (These are the users having the profile SAP_ALL). All superuser accounts that were found in your system are REMOVED from all the following checks. This means that checks that report 5 authorized users, for example, actually have 5 users and ALL superuser accounts authorized for your system. Keep this in mind when you look at all other checks below.

<table>
<thead>
<tr>
<th>Client</th>
<th>User</th>
<th>Type</th>
<th>Last Name</th>
<th>First Name</th>
<th>Department</th>
<th>User Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>BASIS01</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>BASIS02</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>BASIS03</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>COURT</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Candidate: „Users with SAP_ALL“
- Threat: Users with „SAP_ALL“ can completely compromise your system – intentionally or unintentionally. Moreover they can not only circumvent any authorization checks but any auditing as well.
- In the SOS report look for section „Special Focus Checks“ – „Additional Super User Accounts Found“ - Check-ID 0022
- Action: Avoid „SAP_ALL“ as far as possible and try to restrict it to relevant emergency accounts which are only used in emergency situations under tight control. Add accepted SAP_ALL accounts to the questionnaire and closely monitor this section in future SOS runs.
How to Identify „Top Issues“
Candidate „Users with full authorization for S_RFC“

- Candidate: „Users with full authorizations for S_RFC“
- Threat: These users can be used to call any RFC function from outside the system.
- In the SOS report look for section „Basis Authorization“ – „Incoming RFC“ Check-ID 0241
- Action: Limit users with authorization S_RFC with RFC_NAME=* to the minimum. Limit the RFC functions, for which a specific user is authorized to the required set – or remove the authorization completely where possible.
How to Identify „Top Issues“
Candidate „Users authorized to debug / replace“

- **Candidate:** „**Users authorized to debug / replace**“
- **Threat:** These users can run all programs with debug / replace, e.g. replace an data value or bypass any authorization check.
- **In the SOS report look for section „**Change Management“ – „**Change Control“** Check-ID 0308
- **Action:** Limit users with this authorization to the unavoidable minimum. Authorization for „Debug / Replace“ should not be present at all in production systems.
How to Identify „Top Issues“
Candidate „Users authorized to start all reports“

Candidate: „Users authorized to start all reports“
Threat: These users can start all reports, potentially also bypassing certain S_TCODE checks.
In the SOS report look for section „Change Management“ – „Data & Program Access“ Check-ID 0512
Action: Limit users with this authorization to the unavoidable minimum
How to Identify „Top Issues“
Candidate „Users authorized to display all tables“

- Candidate: „Users authorized to display all tables“
- Threat: These users can view all tables, including technical information as well as any business or personal data
- In the SOS report look for section „Change Management“ – „Data & Program Access“
  Check-ID 0513
- Action: Limit users with this authorization to the unavoidable minimum
How to Identify „Top Issues“
Candidate „Users authorized to execute all function modules“

- **Candidate**: „Users authorized to execute all function modules“
- **Threat**: These users can execute any function modules, where several critical function modules do not contain any further authorization checks.
- **In the SOS report look for section „Change Management“ – „Data & Program Access“ Check-ID 0520**
- **Action**: Limit users with this authorization to the unavoidable minimum
How to Identify „Top Issues“
Candidate „Users with extensive authorizations“

- Candidate: „Users with extensive authorizations“
- Threat: These users have so many authorizations that they are close to a super user.
- In the SOS report look for section „User Authorization“ – „Super Users“
  Check-ID 0023
Beyond this have an additional general look over the SOS authorization checks whether there users that are listed unexpectedly often or in unexpected places. Especially look in SOS checks with „Evaluated Risk – High“
- Action: Limit the authorization for these users to the required minimum
Candidate: "RFC destinations with login information"

Threat: These RFC destinations allow access to remote systems with stored login information. Unauthorized usage will compromise the security of the remote system.

In the SOS report look for section "Basis Authorization" – "Outgoing RFC" Check-ID 0254

Action: For each RFC connection with login information find a responsible persons, who knows about the need and purpose for this entry. Check the other entries whether they can be removed and remove all entries, that are not needed any longer.
How to Identify „Top Issues“
Candidate „Security Audit Log Deactivated“

- **Candidate: „Security Audit Log Deactivated“**
- **Threat:** If the Security Audit Log is deactivated, security critical events are not recorded and are neither available for monitoring nor for the follow-up of any security incident.
- **In the SOS report look for section „Authentication“ – „General Authentication“**
  **Check-ID 0136**
- **Action:** Switch on the Security Audit Log in all clients. The Security Audit Log is optimized for performance. So if logging is restricted to critical security violations only, activation of the Security Audit log should be possible on all systems including production systems.
Deriving an Action Plan

Deriving an Action Plan is easy ... in theory.

The SOS report is designed to already contain everything you need for it:
- a general introduction
- the findings and explanations
- risk ratings
- recommendations
- technical background information

So just go ahead!
Deriving an Action Plan

... is not that easy when the report is huge

When the SOS report is huge

- working on it as described on the slide before takes a lot of time and resources
- ... and may even cause that nothing happens at all.

The goal of the SOS however is not to produce a nice report but to have impact and improve the security of the respective system!

Recommended solution:

- Identify „Systematic Issues“ (e.g. issues with the authorization concept) and trigger a solution
- Identify „Top Issues“ and solve them first!
- Identify „Quick Wins“ and implement them
- Determine the remaining risk and
  - either address the next set of „Top Issues“
  - or get agreement, that the achieved level of security looks acceptable until the next scheduled run of the SOS
**Action Definition Template**

<table>
<thead>
<tr>
<th>Name / Identification of the Action</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Short summary of the issue</td>
<td></td>
</tr>
<tr>
<td>Required Actions</td>
<td></td>
</tr>
<tr>
<td>Who</td>
<td>By When</td>
</tr>
<tr>
<td>tbd</td>
<td>tbd</td>
</tr>
</tbody>
</table>

*Use the standard procedure that works best in your environment for defining, assigning and tracking actions. This can be issues / top issues in the Solution Manager, some ticketing system or a manual process based on Word, PowerPoint, Outlook or something else.*
Further Information and Contact

Contact address
SecurityCheck@sap.com

Public information
SAP Service Marketplace, using alias /SOS
http://service.sap.com/sos

SAP Notes:
• Note 696478 - SAP Security Optimization: Preparation & Additional Info
• Note 837490 - Execution of the Security Optimization Self-Service
• Note 863362 - Security Checks in the SAP EarlyWatch Alert

Related SAP education training opportunities
• http://www.sap.com/education
  Search for ADM960: Security in SAP system environments
Security Optimization Service: EGI session

Get in-depth knowledge of the Security Optimization Service functionality with the Expert Guided Implementation (EGI) service.

The EGI gives the participants the opportunity to set up ready-to-use Security Optimization Reports in their own SAP Solution Manager.

Training, practical experience, remote consulting

**Empowering**, Web session, 1-2 h. each morning
SAP expert explains step-by-step configuration using training materials

**Execution**, 2-3 h. on the same day
Participants execute demonstrated steps within their own project, on their own SAP environment

Expertise on demand, during execution
Participants have direct access to an SAP expert who directly supports them remotely, if necessary, during the execution

More information on available EGI topics and booking information can be found here:

https://service.sap.com/esacademy

⇒ EGI Registration

EGI for Security Optimization
Exercises

Security Optimization Service report
Agenda

➤ Best Practices-based Services

Security Tools and Services

➤ EarlyWatch Alert (EWA) – Security Chapter
➤ Security Notes Report (RSECNOTE)
➤ System Recommendations
➤ Security Optimization Service (SOS)
➤ Configuration Validation

➤ Run SAP Standard for Security

Appendix
➤ SAP Enterprise Support Report
Consider Customers Situation of Today …

**Challenges**

- A large number of systems… Complex SAP Landscape …
- … Need to perform comparison of current configuration status against a defined target or standard configuration baselines
- … with minimum efforts and ASAP
End-to-End Diagnostics and SAP Solution Manager

End-to-End Reporting
Prove value to business

End-to-End Monitoring and Alerting
Automate operations

End-to-End Root Cause Analysis
Lower mean time to resolution

Component specific Root Cause Analysis

SAP SOLUTION MANAGER

- SAP EarlyWatch Alert
- Service Level Reporting
- Customer BI Reporting

System Monitoring
End-user Monitoring
Interface Monitoring
Job Monitoring
Business Process Monitoring

Unified Alert Inbox
Alert correlation and propagation
Open data provider and alert consumer

End-to-End Change Analysis
- End-to-End Workload Analysis
- End-to-End Exception Analysis
- End-to-End Trace Analysis

E2E Change Analysis is the main prerequisite for Configuration Validation

MANAGED SYSTEMS

ABAP
Java
.NET
C(++)

© 2012 SAP AG. All rights reserved.
Configuration Validation
Architecture Overview

Solution Manager EHP1

Configuration Validation

- Virtual InfoProvider OSMD_VCA1
- Function Module
- Configuration and Change Database (CCDB)
- DB Table
- Target System Maintenance
- Configuration Validation Reporting
- Change Reporting
- Interactive BI based Reporting
- Manual maintenance of copied configuration data
- Copy
- Customer defined system configurations / baselines
- Existing system configurations

JAVA based installations
- Diagnostics Agents

ABAP based installations
- Solution Tool Plugins
- Extractor Framework (EFWK) Once a day
- Solution Tool Plugins

Configuration Compliance Report - Security Overview

© 2012 SAP AG. All rights reserved.
## Content Deliverables – Configuration Items Overview

<table>
<thead>
<tr>
<th>Application</th>
<th>Software Release Validation</th>
<th>Parameter Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Support Package Stack</td>
<td>• SAP Product specific settings</td>
</tr>
<tr>
<td></td>
<td>• Software Component Versions</td>
<td>- PI/XI specific configuration</td>
</tr>
<tr>
<td></td>
<td>• Implemented SAP Notes</td>
<td>- BI specific configuration</td>
</tr>
<tr>
<td></td>
<td>• Imported ABAP Transports</td>
<td>- BIA specific configuration</td>
</tr>
<tr>
<td>Kernel</td>
<td>• Web AS ABAP Kernel Release</td>
<td>• ABAP Instance Parameters</td>
</tr>
<tr>
<td></td>
<td>• Java VM version</td>
<td>- Java VM parameters for J2EE</td>
</tr>
<tr>
<td></td>
<td>• Web AS Java Release</td>
<td>Database Parameters</td>
</tr>
<tr>
<td>Database</td>
<td>• Database Release</td>
<td>Operating System Parameters</td>
</tr>
<tr>
<td>Operating System</td>
<td>• Operation System Release</td>
<td>Operating System Environment Settings</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td>Standard Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gateway Secinfo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gateway Reginfo</td>
</tr>
</tbody>
</table>
Possible Reference Systems / Configuration Baselines

1. Reference is an Existing System
   - Data stored in Configuration and Change Database (CCDB)
   - Latest available snapshot used for comparison
   - No changes of configuration items are allowed

2. Reference is a Target System
   - Content of existing configuration is copied into a separate database table
   - Copied configuration items can be edited to match a specific audit task
   - Reference system should contain a restricted number of configuration items
Configuration Validation
Target System Maintenance
## Configuration Validation

### Drilldown Reporting

### Configuration Compliance - Selected Items of one ConfigStore

<table>
<thead>
<tr>
<th>Reference System</th>
<th>SMX 0020253585</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison Systems</td>
<td>B35 0020144209, B70 0020261098, C50 0020108503, C50 0020182324, C70 SAP-INTERN, ESU 0120021077</td>
</tr>
<tr>
<td>Config Store</td>
<td>ΔBAP_INSTANCE_PAHI</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>login/fails_to_user_lock, login/min_password_ing, login/no_automatic_user_sapstar</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System</th>
<th>Instance Name</th>
<th>Configuration Item</th>
<th>Config. Item Value</th>
<th>Target Value</th>
<th>Last Check [UTC]</th>
<th>Compliant (1=yes, 0=no)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMX 0020253585</td>
<td>D00</td>
<td>login/fails_to_user_lock</td>
<td>5</td>
<td>#</td>
<td>20100909200301</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/min_password_ing</td>
<td>6</td>
<td>#</td>
<td>20100909200301</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/no_automatic_user_sapstar</td>
<td>1</td>
<td>#</td>
<td>20100909200301</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>DVEBMGS00</td>
<td>login/fails_to_user_lock</td>
<td>5</td>
<td>#</td>
<td>20100909200300</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/min_password_ing</td>
<td>6</td>
<td>#</td>
<td>20100909200300</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/no_automatic_user_sapstar</td>
<td>1</td>
<td>#</td>
<td>20100909200300</td>
<td>1</td>
</tr>
<tr>
<td>B35 0020144209</td>
<td>DVEBMGS00</td>
<td>login/fails_to_user_lock</td>
<td>12</td>
<td>5</td>
<td>20100323200608</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/min_password_ing</td>
<td>3</td>
<td>6</td>
<td>20100323200608</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/no_automatic_user_sapstar</td>
<td>0</td>
<td>1</td>
<td>20100323200608</td>
<td>0</td>
</tr>
<tr>
<td>B70 0020261098</td>
<td>DVEBMGS21</td>
<td>login/fails_to_user_lock</td>
<td>5</td>
<td>5</td>
<td>20100909200302</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/min_password_ing</td>
<td>6</td>
<td>6</td>
<td>20100909200302</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/no_automatic_user_sapstar</td>
<td>0</td>
<td>1</td>
<td>20100909200302</td>
<td>0</td>
</tr>
<tr>
<td>C50 0020108503</td>
<td>DVEBMGS00</td>
<td>login/fails_to_user_lock</td>
<td>10</td>
<td>5</td>
<td>20081019105001</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/min_password_ing</td>
<td>6</td>
<td>6</td>
<td>20081019105001</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>login/no_automatic_user_sapstar</td>
<td>0</td>
<td>1</td>
<td>20081019105001</td>
<td>0</td>
</tr>
<tr>
<td>C60 0020182324</td>
<td>DVEBMGS00</td>
<td>login/fails_to_user_lock</td>
<td>5</td>
<td>5</td>
<td>20100909193657</td>
<td>1</td>
</tr>
</tbody>
</table>
Configuration Validation
Predefined Security Report in Solution Manager 7.0 (discontinued)
Introducing operators offers a greater flexibility to define a fitting target system.
New with Solution Manager 7.1
Operators and Target Systems

In Solution Manager 7.1 all rules are transparent and no rules are hardcoded

Operators available for all types of Config Stores: property, table, text, and xml
Operators comprise the rule used for validation for a Config Item
New with Solution Manager 7.1
SAP Notes: based on RSENCNOTE / System Recommendations

Option b) all notes based on System Recommendations

ABAP_NOTES and JAVA_NOTES of a Target System can be filled with:

- System recommendations which are the SAP Notes relevant for the source system
- Online recommendations which are the SAP Notes from SAP Security List

Option a) ABAP security notes based on RSENCNOTE
New with Solution Manager 7.1
ABAP Notes – based on recommendations from RSECNOTE

Option a) ABAP security notes based on RSECNOTE

The SAP Notes from the SAP Security List
- Software and Kernel dependency of a Note is provided
- Only relevant SAP Notes for the source system can be inserted (the SAP Notes matching Components and Kernel Release from the source system)
New with Solution Manager 7.1
ABAP/Java Notes – based on System Recommendations

Option b) all notes based on System Recommendations

The SAP Notes relevant for the source system can be restricted via

• Data Range
• Note Group – for example only Security and Hotnews SAP Notes can be inserted
New with Solution Manager 7.1 SP 2
Use Case – Predefined Report about Security Notes from RSECNOTE
New with Solution Manager 7.1 SP 2
Use Case – Predefined Report about Security Notes from RSECNOTE

**Selected ConfigStores and Items**
- Only Non compliant Items with Value and Target Value

```
Selection: Reference and Comparison System, Config Store and Item(s)
DGRT001VIRTUAL, SD7 0020270862, S17 0020270862, SQ7 0020230702, ST7 0020270862, SW7 0020270862, SD7, S17, SQ7, ST7
```

### Configuration Items

<table>
<thead>
<tr>
<th>Config Item</th>
<th>System</th>
<th>Compliance</th>
<th>Last Check [UTC]</th>
<th>Compliant (1=Yes, 0=No, '-'=Not valued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001490437</td>
<td>SQ7 0020230702</td>
<td>No</td>
<td>20110609180215</td>
<td>0</td>
</tr>
<tr>
<td>0001556749</td>
<td>SD7 0020270862</td>
<td>No</td>
<td>20110609181329</td>
<td>0</td>
</tr>
<tr>
<td>0001556649</td>
<td>S17 0020270862</td>
<td>No</td>
<td>20110609181407</td>
<td>0</td>
</tr>
<tr>
<td>0001556649</td>
<td>SQ7 0020230702</td>
<td>No</td>
<td>20110609180215</td>
<td>0</td>
</tr>
<tr>
<td>0001556649</td>
<td>ST7 0020270862</td>
<td>No</td>
<td>20110609180158</td>
<td>0</td>
</tr>
<tr>
<td>0001556649</td>
<td>SD7 0020270862</td>
<td>No</td>
<td>20110609181329</td>
<td>0</td>
</tr>
<tr>
<td>0001556649</td>
<td>S17 0020270862</td>
<td>No</td>
<td>20110609181407</td>
<td>0</td>
</tr>
<tr>
<td>0001556649</td>
<td>SQ7 0020230702</td>
<td>No</td>
<td>20110609180215</td>
<td>0</td>
</tr>
<tr>
<td>0001556649</td>
<td>ST7 0020270862</td>
<td>No</td>
<td>20110609180158</td>
<td>0</td>
</tr>
</tbody>
</table>

BUCHHOLZF, 10.06.2011 08:51:46
New with Solution Manager 7.1
Critical User Authorizations: Config Stores in CCDB

- **AUTH_CHECK_USER**
  User authority check store

- **AUTH_PROFILE_USER**
  User profile check store

- **AUTH_TRANSACTION_USER**
  User transaction check store

**Example:** Store Content of AUTH_PROFILE_USER

<table>
<thead>
<tr>
<th>History</th>
<th>PROFILE</th>
<th>USER</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_ALL</td>
<td></td>
<td>ADSUSER</td>
<td>USER IS AUTHORIZED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AGRAM/WALKA</td>
<td>USER IS AUTHORIZED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALEREMOTE</td>
<td>USER IS AUTHORIZED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AMRAM</td>
<td>USER IS AUTHORIZED</td>
</tr>
</tbody>
</table>
New with Solution Manager 7.1
Critical User Authorizations: Customizing Store Content

CCDB Administration tool allows to customize those store contents

- Call transaction **CCDB** to start CCDB Administration tool
- Navigate to tab “**Technical Systems**”
- Select system and display stores relevant for user critical authorizations

- Navigate to tab “**Customizing**”
- Create new customizing variant and adjust it accordingly (by default only users with SAP_ALL role are tracked)
New with Solution Manager 7.1

Critical User Authorizations: Analysis of user profiles

**AUTH_PROFILE_USER**: User profile check store in the Target System (reference) defines that no user is allowed to have SAP_ALL profile

**Validation Output**: The Users which have critical authorizations in the system SI7 (compared system)
New with Solution Manager 7.1
Critical User Authorizations: Analysis of user authorizations

**AUTH_CHECK_USER**: User authorizations check store in the Target System (reference) defines that only certain admin users are allowed to have debug authorizations

**Validation Output**: Users which have the critical debug authorizations in the system SD7 (compared system) can be easily found
New with Solution Manager 7.1
Critical User Authorizations: Analysis of user transactions

**AUTH_TRANSACTION_USER:** User transaction check store in the Target System (reference) defines that only admin users are allowed to have authorizations for the transaction SM59

**Validation Output:** The Users which are not allowed to have the authorizations for Configuration RFC in the system SD7 (compared system) can be easily found.
New with Solution Manager 7.1
RFC Hopping: Overview

Risk of RFC Hopping with RFC Destinations
Privilege Escalation
User impersonation
Bypass Network Firewalls
Hop through the whole system landscape (e.g. jump to a central system like the SolMan)

Countermeasure
Identify critical RFC Destinations across systems
Identify RFC Destinations to critical systems

User Authorizations
User ABC with restricted permissions
User XYZ with SAP_ALL permissions
User EWA with restricted permissions
User AWE with SAP_ALL permissions
New with Solution Manager 7.1
RFC Hopping: Store RFCDES_TYPE_3_CHECK

**RFCDES_TYPE_3_CHECK**: For each RFC Destinations it is checked if the user provided in this RFC Destination has critical authorizations and/or can be used for login.

**CV_USER_PROFILE_RESULT**
- **CRITICAL_USER_PROFILE** – User provided exists in destination System and has critical authorizations
- **OK_USER_NOT_IN_PROFILE_STORE** - User provided exists in destination System but does not have critical authorizations
- **OK_NO_USER_OR_PW_IN_RFCDEST** - No user and/or no pw is stored in the destination
RFC Hopping: Target System to find all critical RFC Destinations

RFCDES>Type_3_CHECK: This Store has been reduced up to one record and defines the pattern to search all RFC Destinations with critical status.
New with Solution Manager 7.1
RFC Hopping: Output with critical RFC Destinations

**0TPL_0SMD_VCA2_NCOMPL_CI_REF**: This report shows all the RFC Destinations with critical status. The critical user authorizations could be customized via the `AUTH_PROFILE_USER` Store (by default the users with the profile “SAP_ALL” is checked).

### Validation Details:
In the column “Comparison Value” you can find all the details on the critical RFC Destination. In our example for the RFC Destination “PMIB4X001” which is created in the system B4X the user “PIRWBUSER” and the password saved in the logon data. This user has the profile “SAP_ALL” assigned in the system B4X.
RFCDES_TYPE_3_CHECK: This Store has been reduced up to one record and defines the pattern to search all RFC Destinations pointing to the System SI7.
New with Solution Manager 7.1
RFC Hopping: Output with the RFC Destinations pointing to a critical System

**0TPL_0SMD_VCA2_CITEMS_REF:** This Report displays validation results for all RFC Destinations.

**Filter:** Select filter value “Yes” for column “Compliance” to display only the RFC Destinations pointing to the critical system.
New with Solution Manager 7.1
UI: Security Template

The new Security Template:

- Supports customer to have a head start when starting with configuration validation towards security. It contains suggestion for rules and values for a number of Config Stores and can be used to create a target system.
- It’s possible to add or remove Config Stores and to change rules and values.
New with Solution Manager 7.1
Security Template: Examples of Store Definition

**MS_SECINFO**

<table>
<thead>
<tr>
<th>Line Content</th>
<th>Operator</th>
<th>Operator Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line OK</td>
<td>Regex</td>
<td>HOST=[&quot;]*</td>
</tr>
<tr>
<td>Line not OK</td>
<td>Not regex</td>
<td>HOST=[&quot;</td>
</tr>
</tbody>
</table>

The definition means that the entry HOST=* which is the default entry used in a system in case no message server ACL is defined is validated as NON compliant.

**GW_SECINFO**

<table>
<thead>
<tr>
<th>Line Content</th>
<th>Operator</th>
<th>Operator Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER OK</td>
<td>Regex</td>
<td>&quot;USER=[&quot;]*</td>
</tr>
<tr>
<td>USER-HOST OK</td>
<td>Regex</td>
<td>&quot;USER-HOST=[&quot;]*</td>
</tr>
<tr>
<td>HOST OK</td>
<td>Regex</td>
<td>&quot;HOST=[&quot;]*</td>
</tr>
<tr>
<td>TP OK</td>
<td>Regex</td>
<td>&quot;TP=[&quot;]*</td>
</tr>
<tr>
<td>Line not OK</td>
<td>Not(Regex</td>
<td>&quot;USER=[&quot;]* USER-HOST=[&quot;]* HOST=[&quot;]* TP=[&quot;]*</td>
</tr>
</tbody>
</table>

This definition is to validate all lines that use only parameters with the * as non compliant which would be the same result as the validation of EhP1, see SAP note 1234799.

**SICF_SERVICES**

In a SAP system only the really needed services for the SAP Internet Communication Framework (ICF) should be active.
New with Solution Manager 7.1
Security Template: Examples of Store Definition

**STANDARD_USERS**

<table>
<thead>
<tr>
<th>CLIENT</th>
<th>USER</th>
<th>PASSWORD_STATUS</th>
<th>EXISTS</th>
<th>LOCKED</th>
</tr>
</thead>
<tbody>
<tr>
<td>( Contains ) *</td>
<td>( = ) DDC</td>
<td>( Not equal ) DEFAULT</td>
<td>( Ignore ) X</td>
<td>( Ignore )</td>
</tr>
<tr>
<td>( Contains ) *</td>
<td>( = ) EARLYWATCH</td>
<td>( Not equal ) DEFAULT</td>
<td>( Ignore ) X</td>
<td>( Ignore )</td>
</tr>
<tr>
<td>( Contains ) *</td>
<td>( = ) SAP*</td>
<td>( Not equal ) DEFAULT</td>
<td>( = ) X</td>
<td>( Ignore )</td>
</tr>
<tr>
<td>( Contains ) *</td>
<td>( = ) SAPCPC</td>
<td>( Not equal ) DEFAULT</td>
<td>( Ignore ) X</td>
<td>( Ignore )</td>
</tr>
<tr>
<td>( Contains ) *</td>
<td>( = ) TMSADM</td>
<td>( Not equal ) DEFAULT</td>
<td>( Ignore ) X</td>
<td>( Ignore )</td>
</tr>
</tbody>
</table>

The Password status should not be DEFAULT. The user SAP* must exist in all clients and its password must be changed. For the other users there is no need to be existent in all clients.

**ABAP_INSTANCE_PAHI**

The definition covers parameters that are validated also by the security optimization services (SOS). The Regex for login/ticket_expiration_time means less than 12 hours would be compliant.
New with Solution Manager 7.1
E2E Alerting

It’s possible to add a target system to E2E Alerting. Non-compliant items could then cause an alert within the alert inbox (System alert: configuration validation)
New with Solution Manager 7.1 SP 3
Management Dashboard

WebDynpro ABAP Application **MY_DASHBOARD**
The dashboard apps show the validation results of the comparison of selected systems with a target system.
Further Information and Contact
Configuration Validation

Configuration Validation @ Service Market Place
https://service.sap.com/diagnostics

→ END-TO-END ROOT CAUSE ANALYSIS
  Demos
  Presentations
  Configuration Guide (goon in folder ‘media library’)

Configuration Validation @ SDN
http://wiki.sdn.sap.com/wiki/display/TechOps/ConfVal_Overview
http://wiki.sdn.sap.com/wiki/display/TechOps/ConfVal_Home
  Best Practice
Configuration Validation: EGI session

Get in-depth knowledge of the Configuration Validation functionality with the Expert Guided Implementation (EGI) service.

The EGI gives the participants the opportunity to set up ready-to-use Configuration Validation Reports in their own SAP Solution Manager.

Training, practical experience, remote consulting

**Empowering**, Web session, 1-2 h. each morning
SAP expert explains step-by-step configuration using training materials

**Execution**, 2-3 h. on the same day
Participants execute demonstrated steps within their own project, on their own SAP environment

**Expertise on demand**, during execution
Participants have direct access to an SAP expert who directly supports them remotely, if necessary, during the execution

More information on available EGI topics and booking information can be found here:

https://service.sap.com/esacademy ➔ EGI Registration
Demo

Configuration Validation
Configuration Validation
SAP Solution Manager Workcenter – Change Management

Quicklink for Easy Access Menu:
WebDynpro ABAP DIAGCPL_VIRT_SYS
Configuration Validation
Maintain Target System – Create with Template

![Configuration Validation Screen](image)

- **Source System**
  - **System ID**: [Blank]
  - **System Type**: [Blank]
  - **Store Name**: [Blank]
  - **Store Type**: [Blank]
  - **Search String**: [Blank]

- **Select Source Systems**
  - [Create with Template]

- **Select Config Stores**
  - **Name**: sapscu
  - **Group**: HARDWARE
  - **Category**: CONFIG
  - **Type**: XML
  - **Host**: wdflbrmt0698
  - **Component Version**: 000000000010
  - **Landscape ID**: wdflbrmt0698

- **Additional Config Stores**
  - AUTH PROFILE USER
  - AUTH_CHECK_USER
  - AUTH_TRANSACTION_USER
  - ADAP_INSTANCE_PAI
  - GW_REGINFO
  - GW_SECINFO
  - PSE_CERT
  - ABAP_START_PROFILE
  - ABAP_INSTANCE_PROFILE
  - ENV VARIABLES
Configuration Validation
Maintain Target System – Create with Template

Create Target System from a Template

- System ID: SEC_00
- Description: Security Validation Target for customer #00

Select Template / Target System

- Display SAP Templates
- Display mnr Target Systems

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Created by</th>
</tr>
</thead>
<tbody>
<tr>
<td>0DI</td>
<td>Template for UTPL_0SMO_COMPL_SLS...</td>
<td></td>
</tr>
<tr>
<td>0CB</td>
<td>Template for UTPL_0SMO_COMPL_OB...</td>
<td></td>
</tr>
<tr>
<td>OREF_COM</td>
<td>Reference Template for Communication...</td>
<td></td>
</tr>
<tr>
<td>OREF_VEM</td>
<td>Reference Template for Memory Config...</td>
<td></td>
</tr>
<tr>
<td>0SEC</td>
<td>Template for UTPL_0SMO_COMPL_SEC...</td>
<td></td>
</tr>
<tr>
<td>0SEC_NEW</td>
<td>New Definition for 0SEC</td>
<td>SAP</td>
</tr>
<tr>
<td>0SW</td>
<td>Template for UTPL_0SMO_COMPL_SW...</td>
<td></td>
</tr>
</tbody>
</table>

Read the store list from Template and copy the same stores from source system. Leave the content of copied stores unchanged!

Create
### Configuration Validation

#### Maintain Target System – Edit Target Values

**Target System Maintenance**
- Create
- Edit

**Target System**
- **Long SID:**
- **Description:**
- **Store Type:**
- **Owner:**
- **Customer Target Systems**
- **SAP Target Systems**

**Select Target System**
- **SID**
- **Description**
- **ConfStores of Target System: SEC_00**
  - **Store Name**
  - **Type**
  - **Group**
  - **Instance Type**
  - **STANDARD_USERS**
  - **TABLE**
  - **ABAP-SECURITY**
  - **AUTH_PROFILE_USER**
  - **TABLE**
  - **USER-AUTH...**
  - **SICF_SERVICES**
  - **TABLE**
  - **ABAP-SECURITY**
  - **MS_5EINFO**
  - **TABLE**
  - **ABAP-SECURITY**
  - **ABAP_NOTES**
  - **TABLE**
  - **ABAP-SOFTWARE**
  - **GW_REGINFO**
  - **TEXT**
  - **INSTANCE**
  - **DIALOG**
  - **GW_SECINFO**
  - **TEXT**
  - **INSTANCE**
  - **DIALOG**
  - **ABAP_INSTANCE_PAHI**
  - **PROPERTY**
  - **INSTANCE**
  - **CENTRAL**
  - **SAP_KERNEL**
  - **PROPERTY**
  - **INSTANCE**
  - **CENTRAL**
  - **GLOBAL**
  - **PROPERTY**
  - **SYSTEM-CHAN...**

© 2012 SAP AG. All rights reserved.
Configuration Validation
Show result – Predefined Cross-System Security Notes report
Configuration Validation
Show result – Maintain Views

Selected ConfigStores and Items - Only Non compliant Items with Value and Target Value

Configuration Items

Config Item | System | Compliant (1=Yes, 0=No, "="Not valued)
------------|--------|-----------------
0001557197  | M14 0120003411 | 0
0001560538  | M14 0120003411 | 0
0001560649  | M14 0120003411 | 0
0001565444  | M14 0120003411 | 0
0001567630  | M14 0120003411 | 0
0001567882  | M14 0120003411 | 0

Exercises

Configuration Validation
Exercises

Configuration Validation

Create Target System
Exercises

Configuration Validation

Edit target System
Exercises

Configuration Validation

Create Comparison List
Exercises

Configuration Validation

Reporting
Further Information

SAP Public Web:

SAP Solution Manager Configuration Validation:
http://wiki.sdn.sap.com/wiki/display/TechOps/ConfVal_Home

SDN Security and Identity Management:
http://www.sdn.sap.com/irj/sdn/security

SDN NetWeaver Security Forum:

SAP Help SAP NetWeaver Security Guides:

SAP Help SAP ERP Security Guides:
http://help.sap.com/erp2005_ehp_05/helpdata/en/4a/686e42f50b0d53e100000000a155106/frameset.htm

Security Patch Process FAQ
http://scn.sap.com/community/security/blog/2012/03/27/security-patch-process-faq
Further Information

**SAP Public Web:**

SDN ABAP Development General Forum:

SAP Help Secure Programming ABAP and JAVA:
http://help.sap.com/saphelp_nw70ehp2/helpdata/en/44/6ad7dbe5254ddee10000000a1553f7/frameset.htm

SDN Blog “How to get RFC call traces to build authorizations for S_RFC for free!”:
Further Information

SAP Service Marketplace:

RunSAP End-to-End Solution Operations:  
https://service.sap.com/runsap

SAP Security Notes  
https://service.sap.com/securitynotes

SAP Security White Papers:  
https://service.sap.com/securitynotes -> White Papers

SAP Notification Services, Support Portal Newsletter:  
https://service.sap.com/notifications

SAP Security @ SMP:  
https://service.sap.com/security

SAP Security Guides:  
https://service.sap.com/securityguide

SAP Security Optimization Services:  
https://service.sap.com/sos

SAP EarlyWatch Alert:  
https://service.sap.com/ewa
Further Information

Related SAP Education and Certification Opportunities

http://www.sap.com/education/
ADM940  –  Authorization Concept AS ABAP
ADM950  –  Secure SAP System Management
ADM960  –  Security in SAP System Environment
P_ADM_SEC_70  –  SAP Certified Technology Professional - Security with SAP NetWeaver 7.0

Expert Guided Implementation Trainings

https://service.sap.com/esacademy
SOS  -  EGI for Security Optimization Service
ConfigVal  -  EGI for Configuration Validation