

Security Optimization Self Service – A Real-life Example



Applies to:

SAP Solution Manager 4.0 EhP1 SP2 - Security Optimization Self Service.

For more information, visit the [Security homepage](#).

Summary

This article will describe a real-life example of how to prepare a system for the Security Optimization Self Service (SOSS) and how to generate a security report in Solution Manager.

Author: Dagwin Stox

Company: Atos Origin

Created on: 28 May 2009

Author Bio



Dagwin Stox is working for the Atos Origin SAP Competence Center (sapCC), which provides a training and demo environment to all Atos Origin SAP consultants. The mission of the sapCC is to promote and increase understanding of the SAP solutions within the Atos Origin SAP community and to provide a collaborative environment for its Customers and Partners. Dagwin's areas of expertise are SAP NetWeaver, Solution Manager, DUET and SAP Security.

Table of Contents

Security Optimization (Self) Service	3
Pre-requisites	3
Preparing W70	4
Execution of the Security Optimization Self Service on SM3	8
Related Content	16
Disclaimer and Liability Notice	17

Security Optimization (Self) Service

SAP offers a slew of services to its customers, see here:

<https://service.sap.com/supportofferings>

One of the services SAP offers is the SAP Security Optimization Service (SOS).

This is how SAP describes this service:

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.

See this link for a complete description of the service:

<https://service.sap.com/sos>

In short, the customer will have to fill in a questionnaire, after which SAP will gather and analyze data on the system through a remote service connection. A report is produced that will be discussed with the customer.

This is a valuable tool to help customers secure their systems, but unfortunately it is only available via a premium maintenance engagement.

SAP Solution Manager however delivers the Security Optimization Self Service (SOSS).

This allows you to perform the service for your (customer) system.

The systems mentioned in this article are SM3 (Solution Manager) and W70 (NetWeaver – ABAP).

Pre-requisites

- The target system (W70) exists in the System Landscape on Solution Manager (SM3).
- All RFC's for communication between W70 and SM3 have been generated and are working.
- For a complete report, EarlyWatch alerts must have been generated for W70 (see later).
- The connection to the SAP OSS on W70 and SM3 must work.

This document contains three sections:

- This introduction to the SOSS
- Preparing the target system for the service (W70)
- Running the service on the Solution Manager (SM3)

Preparing W70

First of all, make sure your systems have the latest version of the ST-A/PI tool installed. For Solution Manager this currently is release 01L_CRM570, for NetWeaver it is release 01L_BCO700.

Before you continue, you have to make sure that the system you want to perform the Security Optimization Self Service for is registered in the system landscape on the solution manager and that RFC destinations have been created between solution manager and this system.

The system also needs to be assigned to a logical solution.

These actions fall outside of the scope of this article and have been completed for W70.

On W70 (the NetWeaver system), you can use transaction ST14 to view the data determined for the SAP Security Optimization locally, if you have the appropriate authorizations.

Use transaction PFCG to create a new role and name it Z_SECURITY_CHECK.

Go to the Authorizations tab and click on Edit Authorizations.

Go to Edit -> Insert authorization(s) -> Manual input and select object S_PTCH_ADM.

Enter "02" for the Activity, "SECURITY-CHECK" for the component and "*" for the Table.

Add authorization object S_TCODE and enter "ST14" for the Transaction Code.

Add authorization object S_ADMI_FCD. Click on the field System administration function and select "AUDD" and "STOR". Click on Save to transfer the values.

This is what the profile should look like:

The screenshot displays the SAP Security Optimization Self Service (SOSS) interface for the role Z_SECURITY_CHECK. The interface shows a tree view of authorization objects and their associated data. The following table summarizes the key authorizations shown in the screenshot:

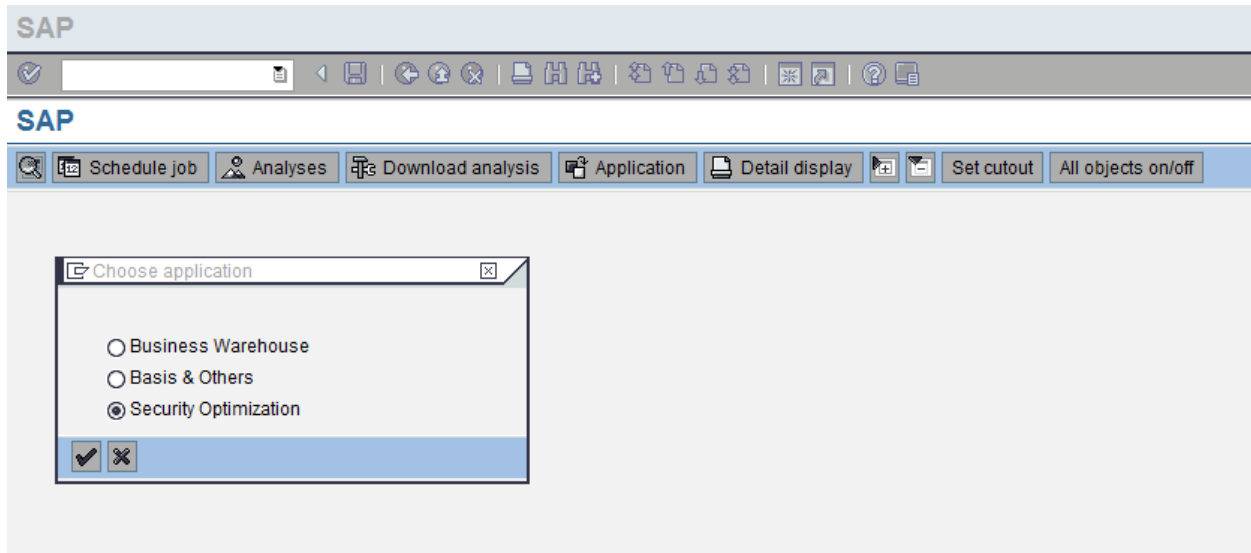
Authorization Object	Transaction Code	Activity	Component	Table Name
Cross-application Authorization Objects	AAAB			
Transaction Code Check at Transaction Start	S_TCODE			
Transaction Code Check at Transaction Start	T-SEC_CHK00			
Transaction Code	ST14			TCD
Basis: Administration	BC_A			
System Authorizations	S_ADMI_FCD			
System Authorizations	T-SEC_CHK00			
System administration function	AUDD, STOR			S_ADMI_FCD
Administrating Component-Specific Patches (Configuration)	S_PTCH_ADM			
Administrating Component-Specific Patches (Configuration)	T-SEC_CHK00			
Activity	02			ACTVT
Component	SECURITY-CHECK			COMPONENT
Table Name	*			TABLE

Save and generate the profile, then assign this role to the userID that you want to use for the SOSS.

I will assume this will be your user profile for this article.

Save the role and perform a user comparison.

Now run transaction ST14 and select the application Security Optimization:



Since this is the first time we run this application, no data is available. Click on “Schedule job” to create a job to collect the data for the SOSS. First assign a name and then select a client. Data will however be collected for all existing clients. In the Analysis scope section, select “Checks for SAP WebAS (R/3) Basis System”.

In the Data area section, you can enter parameters for the SOSS. For a complete description, see SAP note 696478. Click on the + sign to have 8 instead of 2 lines for input.

We will use these parameters:

- BS List personal data (N/Y)		Y
- BS List profiles (N/Y)		Y
- BS User for SAPNet R/3 Frontend		<SAP_UserID>

Replace <SAP_UserID> with your userID, you need to supply a user here who can open the connection to SAPNet.

You can check this in transaction SM59.

We will schedule the job to start immediately.

When all settings are done (see screenshot below), click on “Schedule job” to start the data collection.

Via the menu Utilities -> Jobs overview you can check the status of the job.

When the job is finished, go back to transaction ST14.

Application analysis

Client: Total clients: Production:

Analysis title:

Data area

Document(s)	Choose doc/obj type	Document no./object
	BS List personal data (N/Y)	Y
	BS List profiles (N/Y)	Y
	BS User for SAPNet R/3 F	UserID

or al Pos. 1-8 of 8

Timeframe from to

Analysis scope

- Security Optimization
 - Checks for SAP WebAS (R/3) Basis System
 - Checks for ITS Backend System
 - Checks for ITS Monitoring System
 - Checks for J2EE Backend System

Job start

Immed. start
 Start at
 No start

Multiple jobs in parallel

Check Schedule job Application

Choose Utilities -> Analysis browser from the menu. From here we can send the collected data to solution manager for processing. You can also explore the data collected from here if you want to.

Change the Remote System to Solution Manager (see screenshot) and note the Guid of the analysis. In this case, the Guid is D5L0UWASS8DHO0KMS3K81FBCF. You will need the guid later when performing the self service in your Solution Manager system.

Service Software Framework: Analysis browser & Download

Search analyses Download analysis View data

Search criteria

Search locally

Analyses in local system

Se.	Date	No#	User	Title
▶	29.04.2009	01	BE03155D	Security Optimization Self S

Remote system

Conf (SA-Net 00)
 Solution Manager

Search remotely

Analyses in Solution Manager

Se.	Date	No#	User	Title
-----	------	-----	------	-------

Send

Download analysis

Analysis

Guid: **D5L0UWASS8DH00KMS3K81FBCF** User: UserID

Date: 29.04.2009 No#: 01 Type: ST14

Title: Security Optimization Self Service Status: COMPLETED

Instnr: 0020104863 SID: W70 Size[b]: 780.317

Send to: Solution Manager

Send Send in background

Selected analysis in local system

Guid	D5L0UWASS8DH00KMS3K81FBCF	User	UserID	Type	ST14
Date	29.04.2009	No#	1	Instnr.	0020104863 SID W70
Title	Security Optimization Self Service	Session		Status	COMPLETED
				Size[b]	780.317
				Time	11:57:00

Click on the “Send” button. Click on Send again to confirm.

You will get a confirmation message that sending the data was successful and the analysis will appear in the section “Analyses in Solution Manager”.

This concludes our actions on W70.

Execution of the Security Optimization Self Service on SM3

We prepared the NetWeaver system W70 for use of the SOSS.

We will now logon to the Solution Manager system SM3.

First thing to check is if the system is present in the system landscape.

Start transaction SMSY, this opens the Systems Landscape.

Use the Find button (goggles) to search for "W70" (without the quotes).

The first result returned will be the database W70. Click on "Find next".

The next result will be the system with SystemID W70 under SAP Web AS.

Click on W70. You will see that it is used in logical component Z_SAP_WAS_700.

The screenshot shows the SAP Solution Manager interface. The main window displays the 'Where-Used List for System W70' dialog. The dialog has a 'System' field set to 'W70' and a 'Product Version' of 'SAP WEB AS 7.00'. The 'Use in Logical Components' table is as follows:

Log. Comp.	Activation Status	Product Version	Main Instance	Name	System Role
Z_SAP_WAS_70	Active	SAP WEB AS 7.00	SAP WEB AS ABAP	SAP_WAS_70	Development System; Training System; Production System

The 'Use in System Groups/Landscapes' table is also visible:

Group Type	System Group	Inactive	Description
Project Landscapes	ZGNE99	<input type="checkbox"/>	Gudrun's Project
Solution Landscapes - Operation	Dagwin Stox	<input type="checkbox"/>	Dagwin Stox
Solution Landscapes - Operation	Dummy	<input type="checkbox"/>	Dummy
Solution Landscapes - Operation	SAP Solution	<input type="checkbox"/>	SAP Solution

In the left-hand tree view, the system 'W70' is highlighted with a red circle. The 'Where Used' button (goggles icon) is also highlighted with a red circle.

Click on Z_SAP_WAS_700.

If you look at the logical component, you will see that client 100 of system W70 has been assigned as a demo system in this solution. Other assignments can be made (as you can see for W70).

This is important to know, as we will now create a solution that will contain this logical component.

Logical Component

Product/Main Instance

Name

Delivered by SAP

Component Group

Last Changed On/By

Current System Assignments

System Assignments

Product Version	Development System	Demo System	Training System	Evaluation System	Production System	SAP Referenc System
SAP WEB AS 7.00	W70:100	W70:100	W70:100		W70:100	

When you create a solution, it will get the leading role “Production” by default. If you later add logical components to the solution and the system assignment doesn’t match the leading role, the Maintenance Optimizer e.g. will not be able to download patches. You need to make sure the leading role of the solution and the assignments of the systems you add to the solution match (see later).

Now, start transaction SOLUTION_MANAGER.

If you’re not in the Solution Overview but went directly into a solution you created, click on “Solution Overview” in the left menu.

I will create a new solution called “Security Optimization Self Service Demo”.

This will start a wizard.

The wizard asks a name and the default language for the solution and creates the solution.

Note that your solution has a solution ID, which is 000001755510000 for this solution.

You can use this ID to assign permissions to this solution.

Next thing to do is to go into the Solution Settings.

Solution Edit Goto Settings System Help

Solution: Security Optimization Self Service Demo

Refresh

Solution Landscape Solution Monitoring Best Practices

System Landscape Maintenance
You define and manage, for example, systems, servers, databases and RFC connections which are relevant for your solution.

Project Scoping
You receive an overview of projects that are assigned to your solution, create new projects, or manage projects that have already been assigned.

Solution Settings
Edit your solution settings.

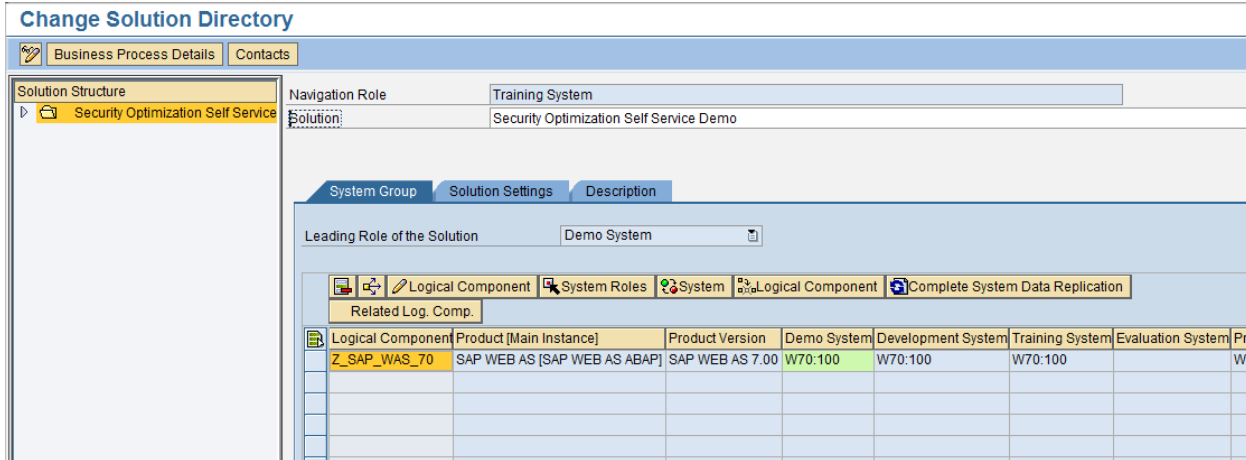
Solution Landscape Maintenance
You specify the business processes, interfaces and systems in your solution. You can make settings for the graphical display of the systems and servers.

Service Connections
Create service connections for the systems in your solution. Open a temporary service connection, so that a member of SAP Support can logon to your system.

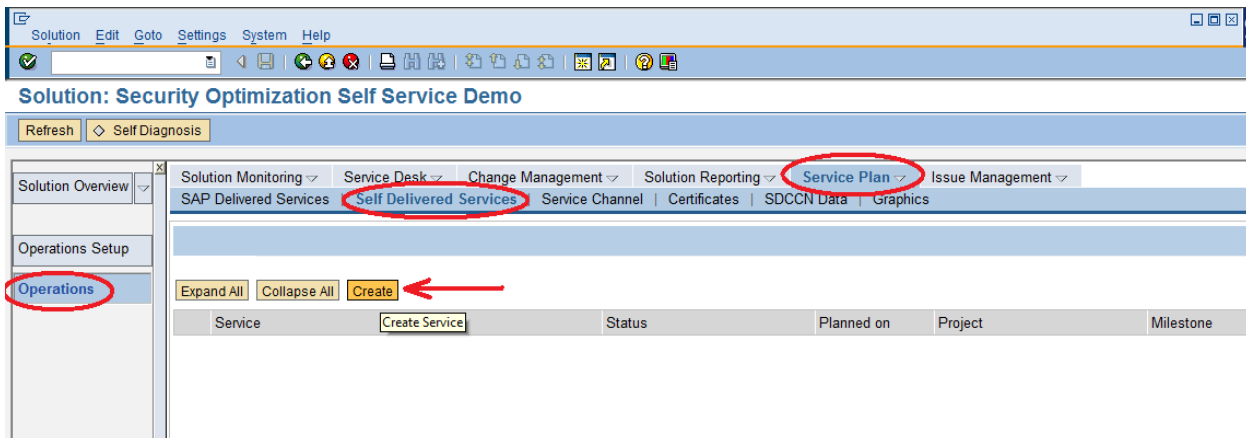
In the Solution Settings window, click on the pencil icon to switch to change mode.

Change the leading role of the solution to “Demo System”. You will be prompted to save the changes immediately, click “Yes” to agree.

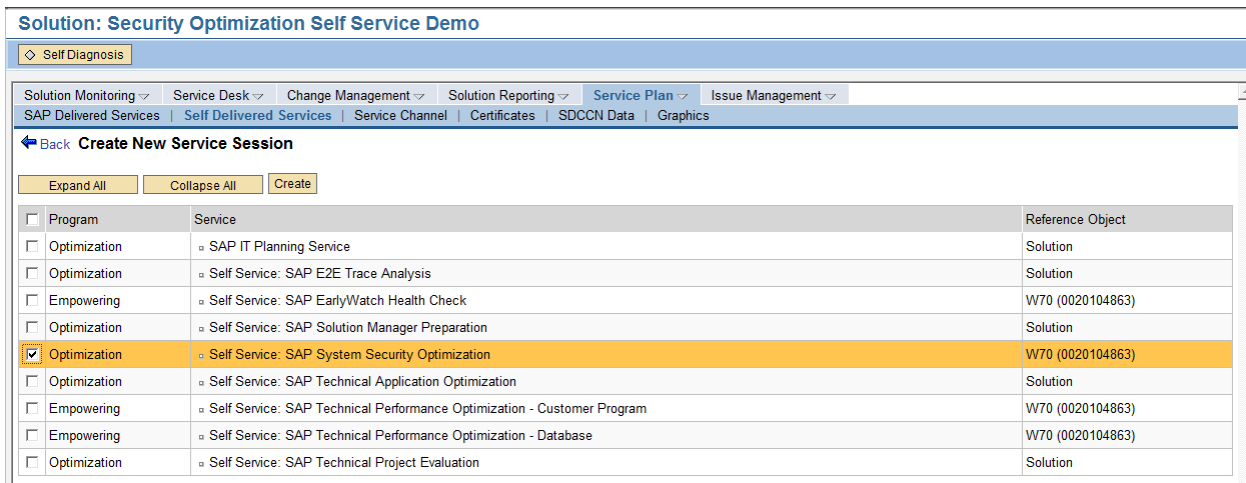
Now click in the “Logical Component” column and use the search function to find logical component Z_SAP_WAS_700. Select it and confirm. Save your solution, which now looks like this:



Use the Back button to get back into the solutions main screen. Click on “Operations” in the left menu. Select “Service Plan” from the top menu and chose subsection “Self Delivered Services”. Click on the “Create” button to create a new service.



You will be presented with a number of options. Choose the optimization service for "Self Service: SAP Security Optimization" for system W70 and click on Create.



In the next step, confirm the date for the service.

The service will now appear in the “Self Delivered Services” section:

Solution: Security Optimization Self Service Demo

The screenshot shows the SAP Self Service Demo interface. The top navigation bar includes 'Refresh' and 'Self Diagnosis'. The main menu has 'Solution Overview', 'Operations Setup', and 'Operations'. The 'Operations' section is active, showing a table of services. The table has columns for Service, Status, Planned on, Project, and Milestone. One service, 'SAP System Security Optimization', is listed with a status of 'in Process' and a planned date of '29.04.2009'. Below this, a 'Sessions' table is visible, with columns for Session, Workbench Status, Planned on, and Session Context. The 'System Security Optimization' session is highlighted with a red circle.

Service	Status	Planned on	Project	Milestone
SAP System Security Optimization	in Process	29.04.2009		

Session	Workbench Status	Planned on	Session Context
System Security Optimization	Initial	29.04.2009	W70 (0020104863)

Expand it and click on “System Security Optimization”.

You can change the comment for this service session if you want to.

The first thing to do is to fill out the questionnaire. The answers you provide here will have an influence on the content and look of the end report.

Solution: Security Optimization Self Service Demo

The screenshot shows the 'Service Session Details' page for 'System Security Optimization'. The session details include: Session: SAP System Security Optimization - System Security Optimization, Planned on: 29.04.2009, Workbench Status: In process, and Workbench Rating: a dropdown menu. The 'Scope/Comment' tab is active, showing a text area with the comment 'sapCC demo of the SAP Security Self Optimization Service' circled in red. At the bottom, there are several buttons: 'Save & Back', 'Save', 'Cancel', 'Open Session Workbench', 'Reset Session Workbench', 'Display HTML Report', and 'Create Questionnaire', which is circled in red.

Click on the button “Create Questionnaire. You will get a confirmation message that the questionnaire has been created. The button now changes into “Edit Questionnaire”. Click on it.

You are now taken to the questionnaire. Initially, you will only see a few items in the left menu.

Once you checked the first item (“Configuration of session and questionnaire), click on the button “Save + next open check”. The rest of the questionnaire will appear.

Change "Security Optimization Self Service Questionnaire - Security Op

HTML document Word document Attachments Action List

Introduction to the Questionnaire
 Configuration of Session and Questionnaire
 Import Data from Word Document
 General Company Data
 Cover Page for Security Optimization
 R/3 Basis and WebAS ABAP Stack
 Clientlist (0000)
 Print the User Data (All Checks)
 User for Remote Access from SAP (0531)
 User Segregation (0004)
 Super Users (0021)
 System Administrators (0151)
 User Administrators (0001)
 Super User Administrators (0025)
 Background Administrators (0217)
 Spool Administrators (0191)
 Batch Input Administrators (0224)
 Key Users (0511)
 Transport Administrators (0351)
 Query Administrators (0516)
 Query Users (0518)
 Role & Auth Administrators (0071)
 Trusting Systems (Outgoing) (0271)
 Trusted Systems (Incoming) (0246)
 RFC Connections with Complete Logon Data
 Systems Allowed to Issue Trusted SSO Ticket
 Trusted Certification Authorities (CAs) (0629)
 Scan of Transports (0348)
 Scan of Source Code (0335)
 Use of the J2EE Engine (0771)

Print the User Data (All Checks)

Procedure
 If you want user data (first name, last name, and department of the user) to be printed in the report, select the "Print User Data" field.
 If you do not select this field, only the user name is printed.
 When ST14 data is created, a parameter can be used to prevent user data (first and last name) from being sent to SAP.

Automatic rating (Green) Green Yellow Red

+ next open check Security Optimization Self Service Quest

Print User Data Instruction (Print user data)

Print User Data?	Flag
Activate if user data wanted	<input checked="" type="checkbox"/>

The second item, "Import data from Word document" can be skipped in this case. You can import the data here from a questionnaire that was sent to and filled in by a customer e.g.

Check each item in the questionnaire. You can use the button "Security Optimization Self Service Quest" for more info regarding each item.

Complete all questions and use the Save button in the top menu to save your answers.

It is important to fill in the questionnaire as accurate as possible!

Your answers will be reflected in the results of the security check, will the impact the length and usability of the report and will determine the recommendations made in the report.

If you don't provide e.g. the list of known Super Users, all users with the corresponding authorizations will be listed in the report, including those users that are supposed to have these authorizations.

If you supplied the known Super Users, you would only get a list of users to review for which you did not know they had Super User privileges.

Use the Back button to return to the self service session.

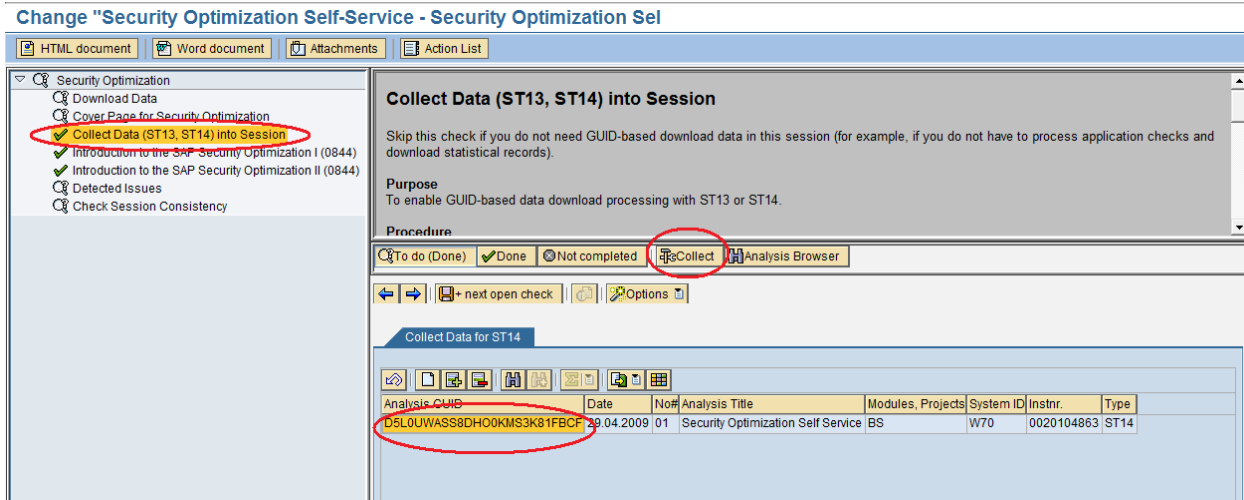
Switch to the tab "Documents & SDCCN Data" (see screenshot).

Click on the "Display" button underneath "SDCCN Data".

If an Earlywatch session has been performed, the system W70 will appear. If no Earlywatch session has been performed, the system will not appear. The Session Workbench will use the Earlywatch session data if it's available, giving you an extensive report. If no session data is available, the Session Workbench will only contain a few items as shown in this screenshot below, which is only presented here for your information.

For this real-life example, I created and performed an Earlywatch session. The creation of Earlywatch alerts falls outside the scope of this article.

This means session data is available and the Session Workbench will contain a lot more items than the screenshot below (see later).

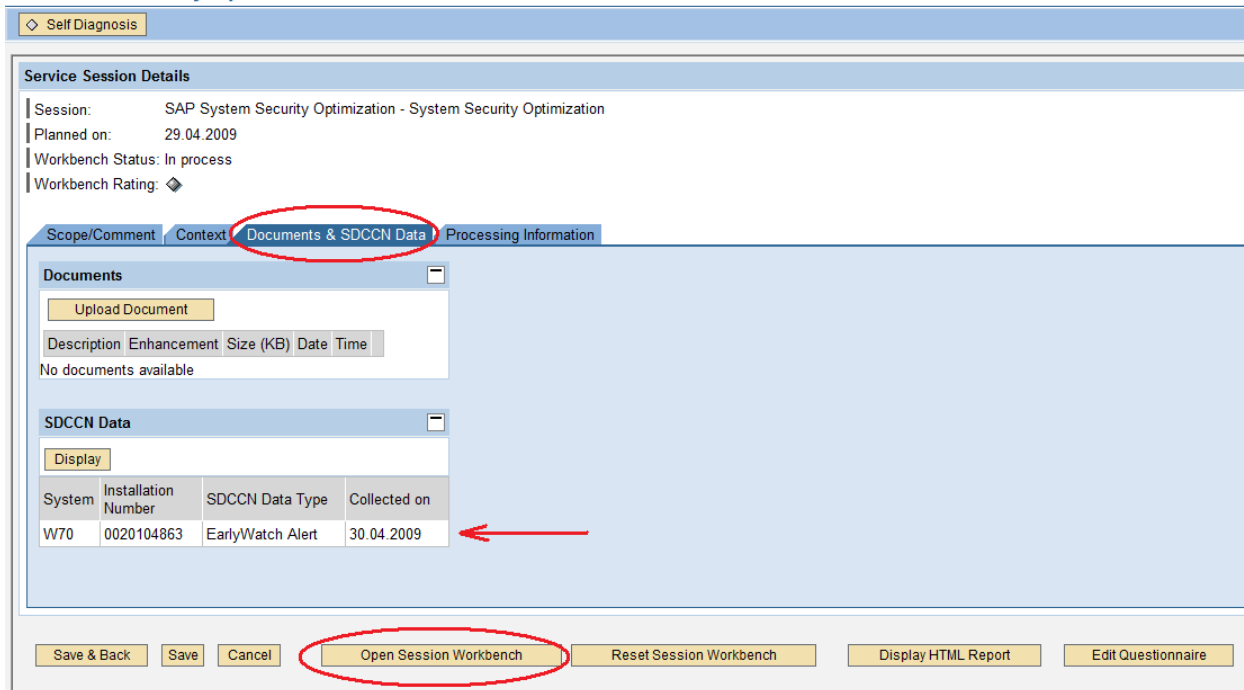


(example of Session Workbench without session data available)

So, we do have the session data available.

Click on “Open Session Workbench”. When prompted that no SDCCN connection has been created yet, click “Yes” to confirm.

Solution: Security Optimization Self Service Demo



You will enter into the session workbench.

If an Earlywatch session was performed, the entries in section “Download data” will be filled in. If not, you can fill in the entries manually.

This is how the Session Workbench looks with session data available:

Change "Security Optimization Self-Service - Security Optimization Sel"

HTML document Word document Attachments Action List

Security Optimization

- Download Data
- Product Components for W70
- Users and Applications
- Cover Page for Security Optimization**
- Collect Data (ST13, ST14) into Session
- Read ST14 Download
- Compare Clients From Download to Questionnaire Data
- Introduction to the SAP Security Optimization I (0844)
- Introduction to the SAP Security Optimization II (0844)
- Special Focus Checks
- Authentication
- Basis Authorization
- Change Management
- User Authorization
- Web Application Server
- Customer Specific Authorization Checks
- Detected Issues
- Check Session Consistency

Cover Page for Security Optimization

Enter the information for the cover page in the check tables below.

Some data should already be filled in automatically. Check if these entries are correct.

Automatic Rating Done Not completed

next open check Security Optimization Self Service Report

System Customer

SAP System ID	SAP Product	Release	Modules	DB System
W70	SAP NetWeaver	7.0		ORACLE 10.2.0.2.0

Remark: in this screenshot, all items have already been processed.

First, check/edit the cover, mark the item as done and click on "Save + next open check".

Select item "Collect data (ST13/ST14) into session". Here you can import the data collected on system W70 that was sent to Solution Manager.

In the right pane, enter the guid you noted for the analysis performed on W70. Hit the "Collect button".

Change "Security Optimization Self-Service - Security Optimization Sel"

HTML document Word document Attachments Action List

Security Optimization

- Download Data
- Product Components for W70
- Users and Applications
- Cover Page for Security Optimization
- Collect Data (ST13, ST14) into Session**
- Read ST14 Download
- Compare Clients From Download to Questionnaire Data
- Introduction to the SAP Security Optimization I (0844)
- Introduction to the SAP Security Optimization II (0844)
- Special Focus Checks
- Authentication
- Basis Authorization
- Change Management
- User Authorization
- Web Application Server
- Customer Specific Authorization Checks
- Detected Issues
- Check Session Consistency

Collect Data (ST13, ST14) into Session

Skip this check if you do not need GUID-based download data in this session (for example, if you do not have to process application checks and download statistical records).

Purpose
To enable GUID-based data download processing with ST13 or ST14.

Procedure

To do (Done) Done Not completed Collect Analysis Browser

next open check Options

Collect Data for ST14

Analysis GUID	Date	No#	Analysis Title	Modules, Projects	System ID	Instrn.	Type
D5L0UWASS8DH00KMS3K81FBCF	09.04.2009	01	Security Optimization Self Service	BS	W70	0020104863	ST14

When done, click on "Save + next open check".

The rest of the items on the left will be executed automatically. If not, check and complete each one of them.

You can check the results from within the Session Workbench by expanding the items on the left with the results (see red square in screenshot above).

If you click on the "Word Document" button, a Word document is generated.

Note: If you get an error message in Word when you try to generate the report saying that programmatic access is not allowed, you need to change the macro security settings in Word.

Check Microsoft Knowledgebase Article 282830 for instructions to prevent the error:

<http://support.microsoft.com/kb/282830>

On my system, it took about 10 minutes to generate the report, it is 65 pages long and it's about 1,5 MB in size.

Save the Session Workbench and use the Back button to get back to the service session details. Here you can see that the Word document appears in the “Documents” section.

Solution: Security Optimization Self Service Demo

◇ Self Diagnosis



Service Session Details

Session: SAP System Security Optimization - System Security Optimization
 Planned on: 29.04.2009
 Workbench Status: In process
 Workbench Rating: ◇

Scope/Comment | Context | Documents & SDCCN Data | Processing Information

Documents

Upload Document

Description	Enhancement	Size (KB)	Date	Time	
Word Report	DOC	1.586	30.04.2009	18:37:34	
Word Logfile	LOG	7	30.04.2009	18:14:06	

SDCCN Data

Display

System	Installation Number	SDCCN Data Type	Collected on
W70	0020104863	EarlyWatch Alert	30.04.2009

Save & Back | Save | Cancel | Open Session Workbench | Reset Session Workbench | **Display HTML Report** | Edit Questionnaire

Use the “Display HTML Report” button to view the report in HTML form in your SAPGUI session. You now have your Security Optimization Self Service report!

Related Content

[Security Optimization Service : workshop presentation \(PDF\)](#)

[SAP Insider article about Security Optimization Self Service](#)

[SAP Note 696478 - SAP Security Optimization: Preparation & additional info](#)

[SAP Note 837490 – Execution of the security optimization self-service](#)

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.