



Service Report

EarlyWatch®Alert

Confidential

SAP System ID

XXX

Product

SAP S/4HANA 1709

Status

DB System

SAP HANA Database 2.00.034.00

Customer

Analysis from 27.04.2020

Until 03.05.2020

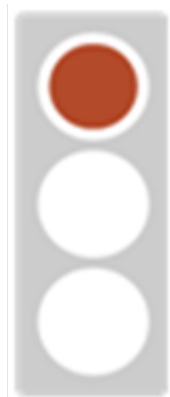
Processed by SAP

Session No. 0000000000000

Installation No. 0000000000

Customer No. 0000

1 Service Summary



The EarlyWatch Alert service has detected severe problems that may cause you to lose business.
Take corrective action immediately.

[...]

ALERT OVERVIEW

[...]	[...]
	The connection to SAP Support Backbone using RFC must urgently be updated to HTTPS.
	SAP HANA database: User SYSTEM is active and valid.
	Standard users have default password.
	Secure password policy is not sufficiently enforced.
	A high number of users has critical authorizations

[...]

CHECK OVERVIEW

Topic Rating	Topic	Subtopic Rating	Subtopic
[...]			
	Security		
			Maintenance Status of current SAP HANA Database Revision
			SAP HANA System Privilege DATA ADMIN
			SAP HANA Password Policy
			SAP HANA Audit Trail
			SAP HANA SQL Trace Level
			SAP HANA Network Settings for Internal Services
			SAP HANA Network Settings for System Replication Communication (listeninterface)
			SAP HANA SSFS Master Encryption Key
			Activation Status and Validity of User SYSTEM
			Age of Support Packages
			Default Passwords of Standard Users

2 Security



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

Rating	Check	System ID
	Maintenance Status of current SAP HANA Database Revision	XXX
	SAP HANA System Privilege DATA ADMIN	XXX
	SAP HANA Password Policy	XXX
	SAP HANA Audit Trail	XXX
	SAP HANA SQL Trace Level	XXX
	SAP HANA Network Settings for Internal Services	XXX
	SAP HANA Network Settings for System Replication Communication (listeninterface)	XXX
	SAP HANA SSFS Master Encryption Key	XXX
	Activation Status and Validity of User SYSTEM	XXX
	Age of Support Packages	XXX
	Default Passwords of Standard Users	XXX
	Control of the Automatic Login User SAP*	XXX
	Protection of Passwords in Database Connections	XXX
	ABAP Password Policy	XXX
	RFC Gateway and Message Server Security	XXX
	Users with Critical Authorizations	XXX

2.1 SAP HANA Database XXX

2.1.1 Maintenance Status of current SAP HANA Database Revision

The following table shows your current SAP HANA database revision.

Rating	Product Version	HANA Revision	Release Date	Age of Revision in Months	Deployment Date	Age of Deployment Date in Months
	2.00 SP 03	2.00.034.00	19.10.2018	19	12.11.2018	18

The Support Package Level of your SAP HANA database will run out of security maintenance within the next 6 months. Due to the age of your SAP HANA revision your database software is likely already missing published and unpublished security fixes. Furthermore, if critical vulnerabilities are detected that require a code correction from SAP, SAP may soon no longer analyze whether your current revision is affected. To ensure the security of your system, you will then need to upgrade to a new Support Package.

Recommendation: Implement a clear SAP HANA maintenance strategy ensuring that the HANA software is kept up to date.

As a general recommendation, an upgrade to the latest HANA revision of an SAP HANA major release should be performed at least once per year.

For more information about the SAP HANA revision and maintenance strategy, see SAP Notes

[2021789](#) - SAP HANA 1.0 Revision and Maintenance Strategy

[2378962](#) - SAP HANA 2.0 Revision and Maintenance Strategy

[1948334](#) - SAP HANA Database Update Paths for Maintenance Revisions for possible update paths.

Note: As of SAP HANA 2.0 SPS 1, Multi Tenancy is mandatory. Systems running as SINGLEDB will be converted. Consequently, several manual security measures will be required in your system to protect the newly created SYSTEMDB.

For additional general information, refer to SAP Note [2115815](#) - FAQ: SAP HANA Database Patches and Upgrades

2.1.2 SAP HANA Audit Trail

Sources of information for the SAP HANA audit trail:

- [SAP HANA Security Guide](#)
- [SAP HANA Administration Guide](#)
- [SAP HANA Audit Trail Best Practice](#) in the SCN

2.1.2.1 Auditing Status

Auditing is disabled in the security settings of your SAP HANA database.

Recommendation: Activate the SAP HANA audit trail and define appropriate audit policies.


2.1.2.2 Audit Policies

No customer-defined audit policies are enabled.

Recommendation: Define audit policies according to your needs.

2.1.3 Activation Status and Validity of User SYSTEM

The activation status and validity dates (VALID FROM and VALID TO) of user SYSTEM have been checked in system table USERS.

Rating	Check
	User SYSTEM is currently active and valid.

Active standard users are an easy and widely used target for hacking attacks since they are available in every system. Furthermore, the user SYSTEM is like a super user with very powerful user authorizations that cannot be revoked.

Recommendation: Review the current usage of user SYSTEM and set up and test a user and role concept, so that the use of user SYSTEM becomes obsolete.

Deactivate the user account with the SQL statement:





```
ALTER USER SYSTEM DEACTIVATE USER NOW.
```

To prevent misuse of user SYSTEM, activate related audit policies in your SAP HANA system as described in the SAP HANA Administration Guide.

2.2 ABAP Stack of XXX

2.2.1 Age of Support Packages

The following table shows the current status, the final assembly date at SAP, and the implementation date of selected key software components that are installed in the system.

Software Component	Release	Support Package	Final assembly date	Age of final assembly date in months	Support Package import date	Age of SP import date in months	Rating
S4CORE	102	2	15.04.2018	25	05.06.2018	23	
SAP_ABA	75C	2	26.03.2018	26	05.06.2018	23	
SAP_BASIS	752	2	15.05.2018	24	05.06.2018	23	
SAP_GWFND	752	2	26.03.2018	26	05.06.2018	23	

SAP provides SAP Security Notes with high or very high priority for Support Packages shipped within the last 24 months. We identified key software components on your system that are outside of this timeframe.

For more information as well as exceptions, see <https://support.sap.com/securitynotes> --> "SAP Security Patch Day".

Recommendation: Run support package updates at least once a year. In addition, evaluate SAP Security Notes once a month at the time of the monthly SAP Security Patch Day. SAP strongly recommends always performing support package updates for the complete support package stack and not just for the software components listed above. See <https://support.sap.com/en/my-support/software-downloads/support-package-stacks.html> for further information.

2.2.2 Default Passwords of Standard Users

Standard users have default passwords.

Recommendation:

Run report **RSUSR003** to check the usage of default passwords by standard users.

Ensure that users **SAP*** (must exist in all clients), **SAPCPIC**, and **EARLYWATCH** have non-default passwords in all clients. For more information, see ["Protecting Standard Users"](#) either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

Make sure that the standard password for user **TMSADM** has been changed. SAP Note [1414256](#) describes a support tool to change the password of user TMSADM in all systems of the transport domain.

SAP Note [1552894](#) shows how to update the report RSUSR003 to show the status of user TMSADM.

2.2.3 ABAP Password Policy

If password login is allowed for specific instances only, the password policy is checked only for these instances.

2.2.3.1 Validity of Initial Passwords

Rating	Parameter	Instance	Current Value(s)
	login/password_max_idle_initial	All instances	30

Initial passwords are valid for more than 14 days.

Recommendation: Proceed as follows:

-- Handle users of type C (Communication) with initial passwords because they will be locked if the above profile parameter is set.

Use transaction SUIM/report RSUSR200 in each client to find users of type C (Communication).

If these users are active and in use, switch the user type to B (System). This has no negative effect.

– Restrict the password validity to 14 days or less. Note that the value 0 grants unlimited validity.


- For more information, see SAP Note [862989](#) and the [Profile Parameters for Logon and Password \(Login Parameters\)](#) section, either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

2.2.4 RFC Gateway and Message Server Security

2.2.4.1 Message Server Security

Message Server Access Control List

PARAMETER: MS/ACL_INFO

Rating	Instance	Error Condition
	All instances	ms/acl_info is defined

MESSAGE SERVER ACCESS CONTROL LIST

Rating	Error Condition
	HOST=*

At least one of the following critical conditions is true:

Profile parameter ms/acl_info is not set

File ms_acl_info does not exist

File ms_acl_info contains at least one trivial entry

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.

The file ms_acl_info referenced by this profile parameter should exist and should not contain trivial entries.

SAP recommends defining and properly maintaining this list to prevent rogue application servers from accessing the system. For more information, see SAP Note [821875](#).

2.2.5 Users with Critical Authorizations




For more information about the following check results, see SAP Note [863362](#).

Recommendation: Depending on your environment, review your authorization concept and use the Profile Generator (transaction PFCG) to correct roles and authorizations. You can use the User Information System (transaction SUIM) to

check the results. For each check, you can review the roles or profiles that include the authorization objects listed in the corresponding section.

2.2.5.1 Super User Accounts

Users with authorization profile SAP_ALL have full access to the system. There should be a minimum of such users. The number of users with this authorization profile is stated for each client.



Client	No. of Users Having This Authorization	No. of Valid Users	Rating
000	3	8	
800	28	141	
900	1	163	

Authorization profile:

SAP_ALL

2.2.5.2 Users Authorized to Change or Display all Tables

Unauthorized access to sensitive data is possible if too many users have this authorization. The specified number of users for each client have the checked authorization.

Client	No. of Users Having This Authorization	No. of Valid Users	Rating
800	29	141	
900	62	163	



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 = *

2.2.5.3 Users Authorized to Start all Reports

This authorization allows critical functions and reports that do not contain their own authorization checks to be executed. The specified number of users for each client have the checked authorization.

Client	No. of Users Having This Authorization	No. of Valid Users	Rating
800	29	141	
900	62	163	



Authorization objects:

Object 1: S_TCODE with TCD=SE38 or TCD=SA38 or TCD=SC38

Object 2: S_PROGRAM with P_ACTION=SUBMIT P_GROUP=*

2.2.5.4 Users Authorized to Debug / Replace

This authorization provides access to data and functions, since any authorization check that is built in ABAP can be bypassed. In addition, you can change data during processing, which may lead to inconsistent results. The specified number of users for each client have the checked authorization.

Client	No. of Users Having This Authorization	No. of Valid Users	Rating
800	32	141	
900	162	163	

Authorization objects:

Object 1: S_DEVELOP with ACTVT=02 (change) and OBJTYPE=DEBUG



Note: If you do not want to disable development in your system, you have to exclude the OBJTYPE=DEBUG with ACTVT=02 from the profile and allow any other object type for S_DEVELOP. This means that development and debugging with visualization is still possible.

You can achieve this by linking two authorizations to the object S_DEVELOP: one with all object types (except for "DEBUG") and all activities, and another for the object type DEBUG only and all activities (except for 02).

2.2.5.5 Users Authorized to Display Other Users Spool Request

This authorization allows unauthorized access to sensitive data contained in spool requests. The specified number of users for each client have the checked authorization.

Client	No. of Users Having This Authorization	No. of Valid Users	Rating
--------	--	--------------------	--------

Client	No. of Users Having This Authorization	No. of Valid Users	Rating
800	29	141	
900	41	163	

Authorization objects:

Object 1: S_TCODE with TCD = SP01 or SP01O

Object 2: S_ADMI_FCD with S_ADMI_FCD = SP01 or SP0R



Object 3: S_SPO_ACT with SPOACTION = BASE and DISP and SPOAUTH = * or __USER__

2.2.5.6 Users Authorized to Administer RFC Connections

If too many users have this authorization, two problems can occur:

- Unauthorized access to other systems
- Malfunction of interfaces if invalid connection data is entered

The specified number of users for each client have the checked authorization.

Client	No. of Users Having This Authorization	No. of Valid Users	Rating
800	29	141	
900	41	163	



Authorization objects:

Object 1: S_TCODE with TCD=SM59

Object 2: S_RFC_ADM with ACTVT NE 03, 39

2.2.5.7 Users Authorized to Reset/Change User Passwords

The following users are allowed to change and reset the passwords of users. This is very risky because any of these users could change the password and log on themselves with another user. The only consequence is that the "real user" would no longer be able to log on because the password would have been changed. However, this normally results in the password being reset, because there is a chance that the "real user" might have forgotten the correct password.

Client	No. of Users Having This Authorization	No. of Valid Users	Rating
800	29	141	
900	62	163	

Authorization objects:

Object 1: S_TCODE with TCD=SU01 or TCD=OIBB or TCD=OOUS or TCD=OPF0 or TCD=OPJ0 or TCD=OVZ5

Object 2: S_USER_GRP with ACTVT=05