



PUBLIC

SAP HANA Platform 2.0 SPS 06

Document Version: 1.0 – 2021-12-03

SAP HANA Security Checklists and Recommendations

Content

1	SAP HANA Security Checklists and Recommendations.	3
1.1	General Recommendations.	3
1.2	Checklist for Secure Handover.	4
2	SAP HANA Database Checklists and Recommendations.	6
2.1	Recommendations for Database Users, Roles, and Privileges.	6
2.2	Recommendations for Network Configuration.	14
2.3	Recommendations for Data Encryption.	17
2.4	Recommendations for File System and Operating System.	20
2.5	Recommendations for Auditing Configuration.	22
2.6	Recommendations for Trace and Dump Files.	24
2.7	Recommendations for Tenant Database Management.	26
3	SAP HANA XS, Advanced Model.	28
3.1	Recommendations for XS Advanced Administration User.	28
3.2	Recommendations for Organizations and Spaces.	30
3.3	Recommendations for Network Configuration.	31

1 SAP HANA Security Checklists and Recommendations

SAP HANA has many configuration settings that allow you to customize your system. Some of these settings are important for the security of your system, and misconfiguration could leave your system vulnerable.

The checklists offer recommendations and information about optimizing your security configuration to help you run your SAP HANA securely. However, please note the following:

- The checklists and recommendations offered here are not exhaustive.
In addition, depending on your specific implementation scenario and technical environment, some of the recommendations may not apply or be different.
- Do not use the checks as instructions on how to configure individual settings.
If a particular check result indicates an insecure setting, refer to the indicated documentation and follow the instructions there to change the configuration setting.
- This document does not replace the *SAP HANA Security Guide*, the central document for all information relating to the secure operation and configuration of SAP HANA.

[General Recommendations \[page 3\]](#)

General recommendations for keeping SAP HANA secure.

[Checklist for Secure Handover \[page 4\]](#)

If you received your SAP HANA system pre-installed from a hardware or hosting partner, there are several things we strongly recommend you do immediately after handover.

Related Information

[SAP HANA Security Guide](#)

1.1 General Recommendations

General recommendations for keeping SAP HANA secure.

- Create a security concept for the SAP HANA scenario that you want to implement as early as possible in your implementation project.
- Install SAP HANA revisions that are marked as security-relevant as soon as possible. Do this by checking SAP HANA security notes either directly, or using services provided by SAP Support.
For more information, see *SAP HANA Security Patches* in the *SAP HANA Security Guide*.

Related Information

[SAP HANA Security Patches](#)

1.2 Checklist for Secure Handover

If you received your SAP HANA system pre-installed from a hardware or hosting partner, there are several things we strongly recommend you do immediately after handover.

- Change the password of all operating system users, in particular the following:
 - `<sid>adm`
 - `<sid>crypt` (if the local secure store has been installed)
 - `root`
 - `sapadm`

For more information, see your operating system documentation.

- In all databases, review all database users created by the installing party, and delete or deactivate those that are not needed in your scenario.

→ Remember

If you received a system with tenant databases, make sure to do this in all tenant databases and in the system database.

For more information about database users that are created in the SAP HANA database by default, see the *SAP HANA Security Guide*.

- In all databases, change the password of all predefined database users, in particular the password of the database user `SYSTEM`. In addition, deactivate the `SYSTEM` user. For more information, see the *SAP HANA Security Guide*.

→ Remember

If you received a system with tenant databases, make sure to do this in all tenant databases and in the system database.

i Note

Predefined internal technical users (`SYS, _SYS_*` users) are permanently deactivated and cannot be used to log on. It is not possible to change the password of these users.

- Change the following encryption master keys:
 - Instance secure store in the file system (SSFS)
 - System public key infrastructure (PKI) SSFS

For more information about how to change the encryption master keys, see *SAP Note 2183624 (Potential information leakage using default SSFS master key in HANA)* and the *SAP HANA Administration Guide*.

- Re-create the system public key infrastructure (PKI) used to protect internal communication in order to create new certificates and private keys. You can trigger this by deleting the system PKI SSFS.

Alternatively, you can use SAPControl to reset the system PKI with the methods

`UpdateSystemPKI [<force>]` and `UpdateInstancePSE [<force>]`.

i Note

In a system replication landscape, you must copy the system PKI SSFS data file and key file from the primary system to the same location on the secondary system(s). For more information, see the section on secure internal communication in the *SAP HANA Security Guide*.

Related Information

[Deactivate the SYSTEM User](#)

[Change a Database User](#)

[Change the SSFS Master Keys](#)

[SAP Control WebService](#) 

[Secure Internal Communication Between Sites in System Replication Scenarios](#)

[SAP Note 2183624](#) 

2 SAP HANA Database Checklists and Recommendations

Checklists and recommendations to help you operate and configure the SAP HANA database securely

→ Tip

SAP Note [1969700](#) contains collections of useful SQL statements for monitoring and analyzing the SAP HANA database. The statements contained in the file `HANA_Security_MiniChecks.txt` perform all of the SQL-based checks listed in this documentation.

2.1 Recommendations for Database Users, Roles, and Privileges

Recommendations for securing access to SAP HANA.

SYSTEM User

Default	The database user <code>SYSTEM</code> is the most powerful database user with irrevocable system privileges. The <code>SYSTEM</code> user is active after database creation.
Recommendation	<p>Use <code>SYSTEM</code> to create database users with the minimum privilege set required for their duties (for example, user administration, system administration). Then deactivate <code>SYSTEM</code>. You may however temporarily reactivate the <code>SYSTEM</code> user for emergency or bootstrapping tasks. See <i>Deactivate the SYSTEM User</i> in the <i>SAP HANA Security Guide</i>.</p> <div><p>i Note</p><p>The <code>SYSTEM</code> user is not required to update the SAP HANA database system; a lesser-privileged user can be created for this purpose. However, to upgrade SAP support package stacks, SAP enhancement packages and SAP systems using the Software Update Manager (SUM) and to install, migrate, and provision SAP systems using the Software Provisioning Manager (SWPM), the <code>SYSTEM</code> user is required and needs to be temporarily reactivated for the duration of the upgrade, installation, migration or provisioning.</p></div>
How to Verify	In the system view <code>USERS</code> , check the values in columns <code>USER_DEACTIVATED</code> , <code>DEACTIVATION_TIME</code> , and <code>LAST_SUCCESSFUL_CONNECT</code> for the user <code>SYSTEM</code> .
Related Alert	No

More Information	See the sections on predefined users and deactivating the SYSTEM user in the <i>SAP HANA Security Guide</i> .
-------------------------	---

Password Lifetime of Database Users

Default	With the exception of internal technical users (<code>_SYS_*</code> users), the default password policy limits the lifetime of user passwords to 182 days (6 months).
Recommendation	<p>Do not disable the password lifetime check for database users that correspond to real people.</p> <p>In 3-tier scenarios with an application server, only technical user accounts for the database connection of the application server should have a password with an unlimited lifetime (for example, <code>SAP<sid></code> or <code>DBACOCKPIT</code>).</p> <div> <p>Note</p> <p>Such technical users should have a clearly identified purpose and the minimum authorization required in SAP HANA.</p> </div>
How to Verify	<p>In the <code>USERS</code> system view, check the value in the column <code>IS_PASSWORD_LIFETIME_CHECK_ENABLED</code>. If it is <code>FALSE</code>, the password lifetime check is disabled.</p> <p>The time of the last password change is indicated in the column <code>LAST_PASSWORD_CHANGE_TIME</code>.</p>
Related Alert	No
More Information	See the section on the password policy in the <i>SAP HANA Security Guide</i> .

System Privileges

Default	System privileges authorize database-wide administration commands. The users <code>SYSTEM</code> and <code>_SYS_REPO</code> have all these privileges by default.
----------------	---

Recommendation

System privileges should only ever be granted to users that actually need them.

In addition, several system privileges grant powerful permissions, for example, the ability to delete data and to view data unfiltered and should be granted with extra care as follows:

Only administrative or support users should have the following system privileges in a production database:

- CATALOG READ
- TRACE ADMIN

In a database of any usage type, the following system privileges should be granted only to administrative users who actually need them:

- ADAPTER ADMIN
- AGENT ADMIN
- AUDIT ADMIN
- AUDIT OPERATOR
- BACKUP ADMIN
- BACKUP OPERATOR
- CERTIFICATE ADMIN
- CREATE REMOTE SOURCE
- CREDENTIAL ADMIN
- ENCRYPTION ROOT KEY ADMIN
- EXTENDED STORAGE ADMIN
- INIFILE ADMIN
- LDAP ADMIN
- LICENSE ADMIN
- LOG ADMIN
- MONITOR ADMIN
- OPTIMIZER ADMIN
- RESOURCE ADMIN
- SAVEPOINT ADMIN
- SERVICE ADMIN
- SESSION ADMIN
- SSL ADMIN
- TABLE ADMIN
- TRUST ADMIN
- VERSION ADMIN
- WORKLOAD ADMIN
- WORKLOAD * ADMIN

How to Verify

To check which user has a particular system privilege, query the `EFFECTIVE_PRIVILEGE_GRANTEES` system view, for example:

```
SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE  
= 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'SSL ADMIN' AND GRANTEE  
NOT IN ('SYSTEM', '_SYS_REPO');
```

Related Alert

No

More Information

See the section on system privileges in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*.

System Privileges: Critical Combinations

Default	The users <code>SYSTEM</code> and <code>_SYS_REPO</code> have all system privileges by default.
Recommendation	Critical combinations of system privileges should not be granted together, for example: <ul style="list-style-type: none">• <code>USER ADMIN</code> and <code>ROLE ADMIN</code>• <code>CREATE SCENARIO</code> and <code>SCENARIO ADMIN</code>• <code>AUDIT ADMIN</code> and <code>AUDIT OPERATOR</code>• <code>CREATE STRUCTURED PRIVILEGE</code> and <code>STRUCTUREDPRIVILEGE ADMIN</code>
How to Verify	To check a user's privileges, query the <code>EFFECTIVE_PRIVILEGES</code> system view, for example: <pre>SELECT * FROM "PUBLIC"."EFFECTIVE_PRIVILEGES" WHERE USER_NAME = '<USER_NAME>';</pre>
Related Alert	No
More Information	See the section on system privileges in the <i>SAP HANA Security Guide</i> and the section on system views for verifying user authorization in the <i>SAP HANA Administration Guide</i> .

System Privilege: DATA ADMIN

Default	The system privilege <code>DATA ADMIN</code> is a powerful privilege. It authorizes a user to execute all data definition language (DDL) commands in the SAP HANA database. Only the users <code>SYSTEM</code> and <code>_SYS_REPO</code> have this privilege by default.
Recommendation	No user or role in a production database should have this privilege.
How to Verify	You can verify whether a user or role has the <code>DATA ADMIN</code> privilege by executing the statement: <pre>SELECT * FROM EFFECTIVE_PRIVILEGE GRANTEEES WHERE OBJECT_TYPE = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'DATA ADMIN' AND GRANTEE NOT IN ('SYSTEM', '_SYS_REPO');</pre>
Related Alert	No
More Information	See the section on system privileges in the <i>SAP HANA Security Guide</i> and the section on system views for verifying user authorization in the <i>SAP HANA Administration Guide</i> . See also SAP Note 2950209.

System Privilege: DEVELOPMENT

Default	The system privilege <code>DEVELOPMENT</code> authorizes some internal <code>ALTER SYSTEM</code> commands. By default, only the users <code>SYSTEM</code> and <code>_SYS_REPO</code> have this privilege.
Recommendation	No user or role in a production database should have this privilege.

How to Verify	<p>You can verify whether a user or role has the <code>DEVELOPMENT</code> privilege by executing the statement:</p> <pre>SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'DEVELOPMENT' AND GRANTEE NOT IN ('SYSTEM', '_SYS_REPO');</pre>
Related Alert	No
More Information	<p>If requested by SAP HANA support, this privilege can be granted using SQL. It is not included in the privilege handling overview in the SAP HANA Security Guide.</p> <p>See the section <i>System Views for Verifying Users' Authorization</i> in the <i>SAP HANA Administration Guide</i>.</p>

Analytic Privilege: `_SYS_BI_CP_ALL`

Default	<p>The predefined analytic privilege <code>_SYS_BI_CP_ALL</code> potentially allows a user to access all the data in activated views that are protected by XML-based analytic privileges, regardless of any other XML-based analytic privileges that apply.</p> <p>Only the predefined roles <code>CONTENT_ADMIN</code> and <code>MODELING</code> have the analytic privilege <code>_SYS_BI_CP_ALL</code> by default. By default, only the user <code>SYSTEM</code> has these roles.</p>
Recommendation	Do not grant this privilege to any user or role in a production database.
How to Verify	<p>You can verify whether a user or role has the <code>_SYS_BI_CP_ALL</code> privilege by executing the statement:</p> <pre>SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE = 'ANALYTICALPRIVILEGE' AND OBJECT_NAME = '_SYS_BI_CP_ALL' AND PRIVILEGE = 'EXECUTE' AND GRANTEE NOT IN ('SYSTEM', 'MODELING', 'CONTENT_ADMIN');</pre>
Related Alert	No
More Information	See the sections on privileges and predefined database roles in the <i>SAP HANA Security Guide</i> and the section on system views for verifying user authorization in the <i>SAP HANA Administration Guide</i> .

Debug Privileges

Default	No user has debug privileges
Recommendation	The privileges <code>DEBUG</code> and <code>ATTACH_DEBUGGER</code> should not be assigned to any user for any object in production systems.

How to Verify	<p>You can verify whether a user or role has debug privileges by executing the statements:</p> <pre>SELECT * FROM GRANTED_PRIVILEGES WHERE PRIVILEGE='DEBUG' OR PRIVILEGE='ATTACH DEBUGGER';</pre>
Related Alert	No
More Information	See the section on privileges in the <i>SAP HANA Security Guide</i> and the section on system views for verifying user authorization in the <i>SAP HANA Administration Guide</i> .

Predefined Catalog Role CONTENT_ADMIN

Default	<p>The role <code>CONTENT_ADMIN</code> contains all privileges required for working with information models in the repository of the SAP HANA database.</p> <p>The user <code>SYSTEM</code> has the role <code>CONTENT_ADMIN</code> by default.</p>
Recommendation	Only the database user used to perform system updates should have the role <code>CONTENT_ADMIN</code> . Otherwise do not grant this role to users, particularly in production databases. It should be used as a role template only.
How to Verify	<p>You can verify whether a user or role has the <code>CONTENT_ADMIN</code> role by executing the statement:</p> <pre>SELECT * FROM GRANTED_ROLES WHERE ROLE_NAME = 'CONTENT_ADMIN' AND GRANTEE NOT IN ('SYSTEM');</pre>
Related Alert	No
More Information	See the section on predefined database roles in the <i>SAP HANA Security Guide</i> and the section on system views for verifying user authorization in the <i>SAP HANA Administration Guide</i> .

Predefined Catalog Role MODELING

Default	<p>The role <code>MODELING</code> contains the predefined analytic privilege <code>_SYS_BI_CP_ALL</code>, which potentially allows a user to access all the data in activated views that are protected by XML-based analytic privileges, regardless of any other XML-based analytic privileges that apply.</p> <p>The user <code>SYSTEM</code> has the role <code>MODELING</code> by default.</p>
Recommendation	Do not grant this role to users, particularly in production databases. It should be used as a role template only.
How to Verify	<p>You can verify whether a user or role has the <code>MODELING</code> role by executing the statement:</p> <pre>SELECT * FROM GRANTED_ROLES WHERE ROLE_NAME = 'MODELING' AND GRANTEE NOT IN ('SYSTEM');</pre>
Related Alert	No
More Information	See the section on predefined database roles in the <i>SAP HANA Security Guide</i> and the section on system views for verifying user authorization in the <i>SAP HANA Administration Guide</i> .

Predefined Catalog Role SAP_INTERNAL_HANA_SUPPORT

Default	<p>The role <code>SAP_INTERNAL_HANA_SUPPORT</code> contains system privileges and object privileges that allow access to certain low-level internal system views needed by SAP HANA development support in support situations.</p> <p>No user has the role <code>SAP_INTERNAL_HANA_SUPPORT</code> by default.</p>
Recommendation	<p>This role should only be granted to SAP HANA development support users for their support activities.</p>
How to Verify	<p>You can verify whether a user or role has the <code>SAP_INTERNAL_HANA_SUPPORT</code> role by executing the statement:</p> <pre>SELECT * FROM EFFECTIVE_ROLE_GRANTED WHERE ROLE_NAME = 'SAP_INTERNAL_HANA_SUPPORT';</pre>
Related Alert	<p>ID 63 (Granting of <code>SAP_INTERNAL_HANA_SUPPORT</code> role)</p>
More Information	<p>See the section on predefined database roles in the <i>SAP HANA Security Guide</i> and the section on system views for verifying user authorization in the <i>SAP HANA Administration Guide</i>.</p>

Predefined Repository Roles

Default	<p>SAP HANA is delivered with a set of preinstalled software components implemented as SAP HANA Web applications, libraries, and configuration data. The privileges required to use these components are contained within repository roles delivered with the component itself.</p> <p>The standard user <code>_SYS_REPO</code> automatically has all of these roles. Some may also be granted automatically to the standard user <code>SYSTEM</code> to enable tools such as the SAP HANA cockpit to be used immediately after installation.</p>
Recommendation	<p>As repository roles can change when a new version of the package is deployed, either do not use them directly but instead as a template for creating your own roles, or have a regular review process in place to verify that they still contain only privileges that are in line with your organization's security policy.</p> <p>Furthermore, if repository package privileges are granted by a role, we recommend that these privileges be restricted to your organization's packages rather than the complete repository. Therefore, for each package privilege (<code>REPO.*</code>) that occurs in a role template and is granted on <code>.REPO_PACKAGE_ROOT</code>, check whether the privilege can and should be granted to a single package or a small number of specific packages rather than the full repository.</p>
How to Verify	<p>To verify whether a user or role has a particular role, execute the following statement, for example:</p> <pre>SELECT * FROM EFFECTIVE_ROLE_GRANTED WHERE ROLE_NAME ='sap.hana.xs.admin.roles::HTTPDestAdministrator';</pre>
Related Alert	<p>No</p>

More Information

For a list of all roles delivered with each component, see [SAP HANA Security Reference Information](#) [Components Delivered as SAP HANA Content](#) in the *SAP HANA Security Guide*.

User Parameter CLIENT

Default

The CLIENT user parameter can be used to authorize named users in SAP HANA. Only a user with the USER ADMIN system privilege can change the value of the CLIENT parameter already assigned to other users. However, at runtime, any user can assign an arbitrary value to the CLIENT parameter either by setting the corresponding session variable or passing the parameter via placeholder in a query. While this is the desired behavior for technical users that work with multiple clients such as SAP Business Warehouse, S/4 HANA, or SAP Business Suite, it is problematic in named user scenarios if the CLIENT parameter is used to authorize access to data and not only to perform data filtering.

Recommendation

Prevent named users from changing the CLIENT user parameter themselves but allow technical users to do so in their sessions and/or queries.

How to Verify

To verify that users are generally not permitted to change the CLIENT user parameter, ensure that the parameter [authorization] secure_client_parameter in the global.ini file is set to true:

```
SELECT * FROM "M_INIFILE_CONTENTS" WHERE  
KEY='SECURE_CLIENT_PARAMETER';
```

To verify that only permitted roles or users can change the CLIENT user parameter, execute the following statement:

```
SELECT * FROM EFFECTIVE_PRIVILEGE_GRANTEES WHERE OBJECT_TYPE  
= 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'CLIENT_PARAMETER_ADMIN';
```

Related Alert

No

More Information

See *SAP Note 2582162 (How to Restrict Use of the CLIENT Parameter)* and the section on authorization in the *SAP HANA Administration Guide*.

Related Information

[Predefined Users](#)

[Deactivate the SYSTEM User](#)

[Password Policy](#)

[System Privileges](#)

[System Views for Verifying Users' Authorization](#)

[Predefined Database \(Catalog\) Roles](#)

[Predefined Repository Roles](#)

[Components Delivered as SAP HANA Content](#)

[Restrict Use of the CLIENT User Parameter](#)

[SAP Note 2582162](#)

[System Views for Verifying Users' Authorization](#)

[SAP Note 2950209](#)

2.2 Recommendations for Network Configuration

Recommendations for integrating SAP HANA securely into your network environment.

General Recommendations

For general recommendations, please read the section on network security in the *SAP HANA Security Guide*.

Open Ports

Default	During installation, ports such as SQL 3<instance_no>15 and HTTP 80<instance_no> are opened by default.
Recommendation	Only ports that are needed for running your SAP HANA scenario should be open. For a list of required ports, see the <i>SAP HANA Administration Guide</i> .
How to Verify	Verify opened ports at operating system level using Linux commands such as <code>netcat</code> or <code>netstat</code> .
Related Alert	No
More Information	See the section on communication channel security in the <i>SAP HANA Security Guide</i> and the section on ports and connections in the <i>SAP HANA Administration Guide</i> .

Internal Host Name Resolution in Single-Host System

Default	<p>SAP HANA services use IP addresses to communicate with each other. Host names are mapped to these IP addresses through internal host name resolution, a technique by which the use of specific and/or fast networks can be enforced and communication restricted to a specific network. In single-host systems, SAP HANA services listen on the loopback interface only (IP address 127.0.0.1).</p> <p>In <code>global.ini</code> files, the <code>[communication] listeninterface</code> is set to <code>.local</code>.</p>
Recommendation	Do not change the default setting.

How to Verify	<p>Using SAP HANA cockpit, check which ports are listening.</p> <p>This information is available in the Network Security Information app in the SAP HANA Security Overview catalog. The value of the <i>Listening On</i> field should be <i>Local Network</i>.</p> <p>Alternatively, execute the following SQL statement:</p> <pre>SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION = 'communication' AND KEY = 'listeninterface';</pre>
Related Alert	No
More Information	See the section about ports and connections in the <i>SAP HANA Administration Guide</i> .

Internal Host Name Resolution in Multiple-Host System

Default	In a distributed scenario with multiple hosts, the network needs to be configured so that inter-service communication is operational throughout the entire landscape. The default configuration depends on how you installed your system.
Recommendation	<p>Multiple-host systems can run with or without a separate network definition for inter-service communication. The recommended setting depends accordingly:</p> <ul style="list-style-type: none"> If a separate network is configured for internal communication, the parameter [communication] listeninterface should be set to .internal. In addition, you should add key-value pairs for the IP addresses of the network adapters used for SAP HANA internal communication in the [communication] internal_hostname_resolution section. If a separate network is not configured for internal communication, the parameter [communication] listeninterface should be set to .global. This setting exposes internal SAP HANA service ports, so it is strongly recommended that you secure internal SAP HANA ports with an additional firewall.

i Note

Communication properties are in the default configuration change blocklist (multidb.ini). This means that they cannot initially be changed in tenant databases. They must be changed from the system database. If appropriate for your scenario, you can remove these properties from the change blocklist. SAP HANA deployment scenarios are described in the *SAP HANA Master Guide*. For more information about how to edit the change blocklist, see the *SAP HANA Administration Guide*.

How to Verify

Check which ports are listening using the SAP HANA cockpit.

This information is available in the [Network Security Information](#) app in the [SAP HANA Security Overview](#) catalog. The value of the *Listening On* field should be *Global Network* or *Internal Network*.

Alternatively, execute the following SQL statements:

```
SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION =  
'communication' AND KEY = 'listeninterface';
```

```
SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION =  
'internal_hostname_resolution';
```

Related Alert	86 (Internal communication is configured too openly)
More Information	See the section on internal hostname resolution in the <i>SAP HANA Administration Guide</i> .

Host Name Resolution in System Replication

Default

The parameter `[system_replication_communication] listeninterface` parameter is set to **.global**.

Recommendation

The recommended setting depends on whether or not a separate network is defined for internal communication:

- If a separate internal network channel **is configured** for system replication, the parameter `[system_replication_communication] listeninterface` parameter should be **.internal**. You also need to add key-value pairs for the IP addresses of the network adapters for the system replication in the `[system_replication_hostname_resolution]` section.
- If a separate network **is not configured** for system replication, the parameter `[system_replication_communication] listeninterface` should be set to **.global**. However, in this case, it is important to secure communication using TLS/SSL and/or to protect the SAP HANA landscape with a firewall. In the `[system_replication_hostname_resolution]` section, add entries for all hosts of neighboring sites (at a minimum) or all hosts of own site as well as for all hosts of neighboring sites. In addition, set the parameter `[system_replication_communication] allowed_sender` to restrict possible communication to specific hosts. The parameter value must contain a list of the foreign hosts that are part of the SAP HANA system replication landscape.

i Note

Communication properties are in the default configuration change blocklist (`multidb.ini`). This means that they cannot initially be changed in tenant databases. They must be changed from the system database. If appropriate for your scenario, you can remove these properties from the change blocklist. SAP HANA deployment scenarios are described in the *SAP HANA Master Guide*. For more information about how to edit the change blocklist, see the *SAP HANA Administration Guide*.

How to Verify

To check the value of the above parameters, execute the following statements:

```
SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION =  
'system_replication_communication' AND KEY =  
'listeninterface';  
  
SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION =  
'system_replication_communication' AND KEY =  
'internal_hostname_resolution';  
  
SELECT * FROM "PUBLIC". "M_INIFILE_CONTENTS"WHERE SECTION =  
'system_replication_communication' AND KEY =  
'allowed_sender';
```

Related Alert	No
More Information	See the section on hostname resolution for system replication in the <i>SAP HANA Administration Guide</i> .

Related Information

[Communication Channels](#)

[Network Security](#)

[Ports and Connections](#)

[Internal Host Name Resolution](#)

[Host Name Resolution for System Replication](#)

2.3 Recommendations for Data Encryption

Recommendations for data encryption and encryption key management

Instance SSFS Master Key

Default	The instance secure store in the file system (SSFS) protects internal root keys in the file system. A unique master key is generated for the instance SSFS in every installation.
Recommendation	If you received your system pre-installed from a hardware or hosting partner, we recommend that you change the master key of the instance SSFS immediately after handover to ensure that it is not known outside of your organization.
How to Verify	Using the SAP HANA cockpit, check the change date of the master key. This information is available in SAP HANA cockpit on the resource overview page.

Related Alert	84 (Insecure instance SSF encryption configuration)
More Information	See the section on server-side data encryption in the <i>SAP HANA Security Guide</i> and the section on changing the SSFS master keys in the <i>SAP HANA Administration Guide</i> .

System PKI SSFS Master Key

Default	The system public key infrastructure (PKI) SSFS protects the X.509 certificate infrastructure that is used to secure internal TLS/SSL-based communication. A unique master key is generated for the system PKI SSFS in every installation.
Recommendation	If you received your system pre-installed from a hardware or hosting partner, we recommend that you change the master key of the instance SSFS immediately after handover to ensure that it is not known outside of your organization.
How to Verify	Check the change date of the master key in the SAP HANA cockpit. This information is available in the SAP HANA cockpit on the resource overview page.
Related Alert	84 (Insecure instance SSF encryption configuration)
More Information	See the section on server-side data encryption in the <i>SAP HANA Security Guide</i> and the section on changing the SSFS master keys in the <i>SAP HANA Administration Guide</i> .

Root Encryption Keys

Default	<p>SAP HANA features the following data encryption services:</p> <ul style="list-style-type: none"> • Data volume encryption • Redo log encryption • Data and log backup encryption • An internal encryption service available to applications requiring data encryption <p>Unique root keys are generated for all services in every database.</p>
Recommendation	If you received your system pre-installed from a hardware or hosting partner, we recommend that you change all root keys immediately after handover to ensure that they are not known outside of your organization.
How to Verify	Query system view <code>ENCRYPTION_ROOT_KEYS</code> .
Related Alert	No
More Information	See the sections on server-side data encryption in the <i>SAP HANA Security Guide</i> and the <i>SAP HANA Administration Guide</i> .

Encryption Key of the SAP HANA Secure User Store (hdbuserstore)

Default	<p>The secure user store (hdbuserstore) is a tool installed with the SAP HANA client. It is used to store SAP HANA connection information, including user passwords, securely on clients.</p> <p>Information contained in the SAP HANA secure user store is encrypted using a unique encryption key.</p>
Recommendation	<p>If you are using the current version of the SAP HANA client, there is no need to change the encryption key of the secure user store. However, if you are using an older version of the SAP HANA client, we recommend changing the encryption key after installation of the SAP HANA client.</p>
How to Verify	<p>You know the encryption has been changed if the file <code>SSFS_HDB.KEY</code> exists in the directory where the SAP HANA client is installed.</p>
Related Alert	<p>No</p>
More Information	<p>See the section on hdbuserstore in the <i>SAP HANA Client Interface Programming Reference</i> and SAP Note 2210637.</p>

Data and Log Volume Encryption

Default	<p>Data and log volume encryption are not enabled</p>
Recommendation	<p>We recommend that you enable data and log volume encryption immediately after installation or handover from your hardware or hosting partner, and after you have changed the root encryption keys for both services.</p>
How to Verify	<p>Execute the following statement:</p> <pre>SELECT * FROM M_ENCRYPTION_OVERVIEW WHERE SCOPE='LOG' OR SCOPE = 'PERSISTENCE'</pre>
Related Alert	<p>No</p>
More Information	<p>See the section on data and log volume encryption in the <i>SAP HANA Security Guide</i> and the section on enabling encryption of data and log volumes in the <i>SAP HANA Administration Guide</i>.</p>

Related Information

[Server-Side Data Encryption Services](#)
[Change the SSFS Master Keys](#)
[Changing Encryption Root Keys](#)
[SAP HANA User Store \(hdbuserstore\)](#)
[Change the User Store Encryption Key](#)
[SAP Note 2210637](#)
[Data and Log Volume Encryption](#)

2.4 Recommendations for File System and Operating System

Recommendations for secure operating system access and data storage in the file system

General Recommendation

Stay up to date on security recommendations available for your operating system and consider them in the context of your implementation scenario and security policy.

See also the following SAP Notes:

- SAP Note 1944799 (SUSE Linux Enterprise Server 11.x for SAP Applications)
- SAP Note 2009879 (Red Hat Enterprise Linux (RHEL) 6.x)

Operating System Users

Default	<p>Only operating system (OS) users that are needed for operating SAP HANA exist on the SAP HANA system, that is:</p> <ul style="list-style-type: none">• <code>sapadm</code> (required to authenticate to SAP Host Agent)• <code><sid>adm</code> (required by the SAP HANA database)• <code><sid>crypt</code> (if the local secure store has been installed)• Dedicated OS users for every tenant database if the system is configured for high isolation
---------	---

i Note

There may be additional OS users that were installed by the hardware vendor. Check with your vendor.

Recommendation	Ensure that no additional unnecessary users exist.
How to Verify	Refer to your operating system documentation
Related Alert	No
More Information	See the section on predefined users in the <i>SAP HANA Security Guide</i> .

OS File System Permissions

Default	The access permission of files exported to the SAP HANA server can be configured using the <code>[import_export] file_security</code> parameter in the <code>indexserver.ini</code> configuration file. The default permission set is 640 (<code>[import_export] file_security=medium</code>).
Recommendation	Do not change default access permission of exported files. In addition, ensure that only a limited number of database users have the system privilege <code>IMPORT</code> and <code>EXPORT</code> .
How to Verify	<ul style="list-style-type: none">You can verify the parameter setting by executing the command: <pre>SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION = 'import_export' AND KEY = 'file_security';</pre>You can verify which users or roles have the <code>IMPORT</code> or <code>EXPORT</code> privilege by executing the statement: <pre>SELECT * FROM EFFECTIVE_PRIVILEGE GRANTEEES WHERE (OBJECT_TYPE = 'SYSTEMPRIVILEGE') AND (PRIVILEGE = 'EXPORT' OR PRIVILEGE='IMPORT');</pre>You can verify the permissions of directories in the file system using the SAP HANA database lifecycle manager (HDBLCM) resident program with installation parameter <code>check_installation</code>.
Related Alert	No
More Information	See the section on checking the installation of an SAP HANA system using the SAP HANA database lifecycle manager (HDBLCM) in the SAP HANA Administration Guide, as well as SAP Note 2252941.

OS Security Patches

Default	OS security patches are not installed by default
Recommendation	Install OS security patches for your operating system as soon as they become available. If a security patch impacts SAP HANA operation, SAP will publish an SAP Note where this fact is stated. It is up to you to decide whether to install such patches.
How to Verify	Refer to your operating system documentation
Related Alert	No
More Information	<ul style="list-style-type: none">SAP Note 1944799 (SUSE Linux Enterprise Server 11.x for SAP Applications)SAP Note 2009879 (Red Hat Enterprise Linux (RHEL) 6.x)

OS sudo Configuration

Default	Users have to either specify the root password or be part of a dedicated user group to be able to run arbitrary commands as root.
----------------	---

Recommendation	Do not change your sudo configuration to allow users such as <code><sid>adm</code> to use sudo to run arbitrary commands as root without specifying the root password.
How to Verify	<p>Check the <code>/etc/sudoers</code> file. The specific configuration may vary with your Linux distribution, but configuration options to look for are:</p> <ul style="list-style-type: none"> • <code>Defaults targetpw</code> This setting requires the root password to be provided when running sudo in general. • <code>ALL ALL=(ALL) ALL</code> This should only be used if <code>Defaults targetpw</code> is also set. <p>If you use the storage connector option to mount SAP HANA volumes, during SAP HANA installation your sudo configuration is modified to allow <code><sid>adm</code> to run a dedicated set of commands as root, such as:</p> <pre><sid></pre> <p>This is intentional and does not pose a security risk. However, <code><sid>adm</code> should not be able to run arbitrary commands as root without proper authentication. <code>adm ALL=NOPASSWD: /sbin/multipath,/sbin/multipathd,/etc/init.d/multipathd,/usr/bin/sg_persist,/bin/mount [...]</code></p>
Related Alert	No
More Information	See the sudo and sudoers documentation (man 8 sudo, man 5 sudoers)

Related Information

[Predefined Users](#)

[Check the Installation Using the Command-Line Interface](#)

[SAP Note 2252941](#) 

[SAP Note 1944799](#) 

[SAP Note 2009879](#) 

2.5 Recommendations for Auditing Configuration

Recommendations for audit configuration

Auditing

Default	Auditing is disabled by default.
----------------	----------------------------------

Recommendation	Verify whether auditing is required by your security concept, for example to fulfill specific compliance and regulatory requirements.
How to Verify	<p>Check the status of auditing in the SAP HANA cockpit</p> <p>This information is available on the Auditing card of the Database Overview page.</p> <p>Alternatively, you can execute the following statement:</p> <pre>SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION = 'auditing configuration' AND KEY = 'global_auditing_state';</pre>
Related Alert	No
More Information	See the sections on auditing in the <i>SAP HANA Security Guide</i> and the <i>SAP HANA Administration Guide</i> .

Audit Trail Target: syslog

Default	The default audit trail target is syslog (SYSLOGPROTOCOL) for the system database
Recommendation	If you are using syslog, ensure that it is installed and configured according to your requirements (for example, for writing the audit trail to a remote server).
How to Verify	Refer to your operating system documentation
Related Alert	No
More Information	See the section on audit trails in the <i>SAP HANA Security Guide</i> and your operating system documentation.

Audit Trail Target: CSV Text File

Default	The audit trail target CSV text file (CSVTEXTFILE) is not configured by default
Recommendation	Do not configure CSV text file (CSVTEXTFILE) as an audit trail target in a production system as it has severe restrictions.
How to Verify	<p>Check the configured audit trail targets in the Auditing of the SAP HANA cockpit</p> <p>Alternatively, execute the following statements:</p> <ul style="list-style-type: none"> SELECT * FROM "PUBLIC" . "M_INIFILE_CONTENTS" WHERE SECTION = 'auditing configuration' AND VALUE = 'CSVTEXTFILE'; SELECT * FROM "PUBLIC"."AUDIT_POLICIES" WHERE TRAIL_TYPE='CSV';
Related Alert	No
More Information	See the section on audit trails in the <i>SAP HANA Security Guide</i> .

Related Information

[Auditing Activity in SAP HANA](#)

[Audit Trails](#)

[Auditing Activity in the SAP HANA Database](#)

[CREATE AUDIT POLICY Statement \(Access Control\)](#)

[Best Practices and Recommendations for Creating Audit Policies](#)

2.6 Recommendations for Trace and Dump Files

Recommendations for handling trace and dump files

Trace Files

Default

Basic tracing of activity in database components is enabled by default, with each database service writing to its own trace file. Other traces (for example, SQL trace, expensive statements trace, performance trace) must be explicitly enabled.

Users with the system privilege `CATALOG READ` can read the contents of trace files in the SAP HANA database explorer. At operating system level, any user in the `SAPSYS` group can access the trace directory: `/usr/sap/<SID>/HDB<instance>/<host>/trace/<db_name>`

Recommendation

- Enable tracing to troubleshoot specific problems only and then disable.
- Exercise caution when setting or changing the trace level. A high trace level may expose certain security-relevant data (for example, database trace level `DEBUG` or SQL trace level `ALL_WITH_RESULTS`).
- Delete trace files that are no longer needed.

How to Verify

You can check which traces are enabled and how they are configured, as well as view trace files in the SAP HANA database explorer.

Related Alert

No

More Information

See the section on security risks of trace and dump files in the *SAP HANA Security Guide* and the section on traces in the *SAP HANA Administration Guide*.

Dump Files

Default

The system generates core dump files (for example, crash dump files) automatically. Runtime (RTE) dump files can be triggered explicitly, for example by using the SAP HANA database management console (`hdbcons`) or as part of a full system information dump (`fullSystemInfoDump.py`) using the SAP HANA cockpit.

RTE dump files must be generated by the `<sid>adm` user.

⚠ Caution

Technical expertise is required to use `hdbcons`. To avoid incorrect usage, use `hdbcons` only with the guidance of SAP HANA development support.

To create RTE dump files in a running system as part of a full system information dump in the SAP HANA cockpit, a user requires the `EXECUTE` privilege on procedure

`SYS.FULL_SYSTEM_INFO_DUMP_CREATE`.

Dump files are stored in the trace directory and have the same access permissions as other trace files (see above).

Runtime dump files created as part of a full system information dump can be retrieved by users with the `EXECUTE` privilege on the procedure

`SYS.FULL_SYSTEM_INFO_DUMP_RETRIEVE` using the SAP HANA cockpit. At operating system level, any user in the `SAPSYS` group can access their storage location: `/usr/sap/SID/SYS/global/sapcontrol/snapshots`

Recommendation	<ul style="list-style-type: none">• Generate runtime dump files to analyze specific error situations only, typically at the request of SAP support.• Delete dump files that are no longer needed.
How to Verify	<ul style="list-style-type: none">• You can view core dump files in the SAP HANA database explorer• You can download the file collections generated by a full system information dump in the SAP HANA cockpit.
Related Alert	No
More Information	See the section on security risks of trace and dump files in the <i>SAP HANA Security Guide</i> and the section on collecting diagnosis information for SAP Support in the <i>SAP HANA Administration Guide</i> .

Related Information

[Security Risks of Trace, Dump, and Captured Workload Files](#)

[Collecting Diagnosis Information for SAP Support](#)

2.7 Recommendations for Tenant Database Management

Recommendations for securely configuring tenant databases

SAML-Based User Authentication

Default	All tenant databases use the same trust store as the system database for SAML-based user authentication
Recommendation	<p>To prevent users of one tenant database being able to log on to other databases in the system (including the system database) using SAML, create individual certificate collections with the purpose SAML and SSL in every tenant database.</p> <p>In addition, specify a non-existent trust store for every tenant database using the <code>[communication] sslTrustStore</code> property in the <code>global.ini</code> file.</p>
How to Verify	<p>Execute the following statements:</p> <ul style="list-style-type: none">• In the tenant database: <code>SELECT * FROM PSES WHERE PURPOSE = 'SAML' OR PURPOSE = 'SSL';</code>• In the system database: <code>SELECT * FROM SYS_DATABASES.M_INIFILE_CONTENTS WHERE DATABASE_NAME='<TENANT_DB_NAME>' AND SECTION='communication' AND KEY = 'ssltruststore';</code>
Related Alert	No
More Information	See the sections on SSL configuration on the SAP HANA server and certificate collections in the <i>SAP HANA Security Guide</i> .

Configuration Blocklist

Default	A configuration change blocklist (<code>multidb.ini</code>) is delivered with a default configuration. The parameters contained in the blocklist can only be changed by a system administrator in the system database, not by the administrators of individual tenant databases.
Recommendation	Verify that the parameters included in the <code>multidb.ini</code> file meet your requirements and customize if necessary.
How to Verify	<p>To see which parameters are blocklisted, execute the statement:</p> <pre>SELECT * FROM "PUBLIC"."M_INIFILE_CONTENTS" WHERE FILE_NAME = 'multidb.ini';</pre>
Related Alert	No
More Information	See the section on default blocklisted system properties in tenant databases in the <i>SAP HANA Security Guide</i> and the section on how to prevent changes to system properties in tenant databases in the <i>SAP HANA Administration Guide</i> .

Restricted Features

Default	<p>To safeguard and/or customize your system, it is possible to disable certain database features that provide direct access to the file system, the network, or other resources, for example import and export operations and backup functions.</p> <p>No features are disabled by default.</p>
Recommendation	<p>Review the list of features that can be disabled and disable those that are not required in your implementation scenario.</p>
How to Verify	<p>To see the status of features, query the system view <code>M_CUSTOMIZABLE_FUNCTIONALITIES</code>:</p> <pre>SELECT * FROM "PUBLIC". "M_CUSTOMIZABLE_FUNCTIONALITIES";</pre>
Related Alert	<p>No</p>
More Information	<p>See the section on restricted features in tenant databases in the <i>SAP HANA Security Guide</i> and the section on how to disable features on tenant databases in the <i>SAP HANA Administration Guide</i>.</p>

Related Information

[TLS/SSL Configuration on the SAP HANA Server](#)
[Certificate Collections](#)
[Default Blocklisted System Properties in Tenant Databases](#)
[Prevent Changes to System Properties in Tenant Databases](#)
[Restricted Features in Tenant Databases](#)
[Disable Features on a Tenant Database](#)

3 SAP HANA XS, Advanced Model

Checklists and recommendations to help you operate and configure the SAP HANA XS Advanced Model runtime securely

3.1 Recommendations for XS Advanced Administration User

Recommendations for XS advanced administration user

XSA_ADMIN User

Default	XSA_ADMIN is a first-level administrator user with irrevocable privileges. This user has unlimited access to the Controller and therefore needs to be handled carefully.
Recommendations	<ul style="list-style-type: none">• Change the XSA_ADMIN password at regular intervals.• Avoid creating other powerful users with privileges similar to XSA_ADMIN.• Keep the number of people with XSA_ADMIN credentials as small as possible. Delegate specific tasks like space management to lesser-privileged users instead. <p>Alternatively, set up lesser-privileged XS advanced users to run the server without the administrative user. Then deactivate the XSA_ADMIN user. See the next section.</p>
How to Verify	<pre>SELECT DISTINCT USER_NAME FROM USER_PARAMETERS WHERE PARAMETER = 'XS_RC_XS_CONTROLLER_ADMIN'</pre> <div>i Note This statement can only be executed by a user administrator.</div>
Related Alert	No
More Information	See the section on predefined XS advanced users in the <i>SAP HANA Security Guide</i> .

Initial Setup with XSA_ADMIN

Default	The XSA_ADMIN user can use the Controller without any restrictions and is the only user in a position to do the initial setup of the model. This includes appointing at least one Org Manager who is able to set up spaces, and managing global resources such as buildpacks and external brokers.
---------	--

Recommendations

Set up your system so that `XSA_ADMIN` is not needed for normal system operation. You can do this as follows:

1. Perform the basic settings that require the administrative access rights of `XSA_ADMIN` as required:
 - Install custom SSL certificates (`xs trust-certificate` and `xs set-certificate` commands)
 - Appoint at least one XS advanced user to be OrgManager of each organization (strongly recommended)
 - Register all required service brokers (optional)
 - Create all required shared domains (optional)
 - Create all required custom buildpacks (optional)
 - Create all required runtimes (optional)
 - Configure logical databases (optional)
 - Set up global environment variables (`xs set_running|staging_environment_variable_groups` command) (optional)
2. Grant one or more XS advanced users the following role collections:
 - `XS_AUTHORIZATION_ADMIN` (managing roles, role-collections, and so on)
 - `XS_USER_ADMIN` (assigning role-collections to XS advanced users)
3. Deactivate the `XSA_ADMIN` with the following SQL statement:
`ALTER USER XSA_ADMIN DEACTIVATE USER NOW`

Note

In an emergency, a user with system privilege `USER ADMIN` can reactivate this user with the SQL statement: `ALTER USER XSA_ADMIN ACTIVATE USER NOW`

How to Verify	In the system view <code>USERS</code> , check the values in columns <code>USER_DEACTIVATED</code> , <code>DEACTIVATION_TIME</code> , and <code>LAST_SUCCESSFUL_CONNECT</code> for the user <code>XSA_ADMIN</code> .
Related Alert	No
More Information	See the section on scopes, attributes, and role collections in the <i>SAP HANA Security Guide</i> .

Related Information

[Predefined XS Advanced Users](#)
[Scopes, Attributes, and Role Collections](#)

3.2 Recommendations for Organizations and Spaces

Recommendations for setting up organizations and spaces

Space Isolation

Default	The instances of applications in the same space run with the same operating system (OS) user. Each space can have a different OS user.
Recommendations	For space isolation, each space should use an own dedicated OS user only for this space.
How to Verify	Current space user mapping can be viewed with the <code>xs spaces</code> command. The user column shows the used OS user for each listed space.
Related Alert	No
More Information	See the section on organizations and spaces in the <i>SAP HANA Security Guide</i> .

Privileges of Space Operating System (OS) User

Default	Spaces are mapped to operating system (OS) users that are used to stage and run applications.
Recommendations	<ul style="list-style-type: none">• Don't use <code><sid>adm</code> or any other high privileged OS user as a space OS user.• Restrict the privileges of the space OS user as much as possible.
How to Verify	Current space user mapping can be viewed with the <code>xs spaces</code> command. Verify the OS privileges of each OS users listed.
Related Alert	No
More Information	See the section on organizations and spaces in the <i>SAP HANA Security Guide</i> .

SAP Space

Default	System applications are deployed to the SAP space by default.
Recommendations	Use the PROD space to deploy your applications, or create new spaces for the applications as required. To ensure isolation, do not deploy your applications to the SAP space. In addition, do not assign the <code>SpaceDeveloper</code> role to platform users in the SAP space, unless it is absolutely necessary.
How to Verify	Log on to the SAP space and use the <code>xs apps</code> command to confirm that the list of applications running in the target space (SAP) includes only system applications, for example, the deployer, the product-installer, etc.

Related Alert	No
More Information	See the section on organizations and spaces in the <i>SAP HANA Security Guide</i> .

Logon with xs CLI

Default	XS advanced session is stored in the file system of the current OS user
Recommendations	We recommend logging on to XS advanced (<code>xs login</code> command) only with a personal OS user with a home directory that is not readable to other OS users.
How to Verify	-
Related Alert	No

Related Information

[Organizations and Spaces](#)

3.3 Recommendations for Network Configuration

Recommendations for integrating SAP HANA XS advanced securely into your network environment.

Network and Communication Security

Default	The XS advanced platform router, which is realized by an SAP Web Dispatcher instance, exposes the public end point for the whole system. The router is configured in a way that all application and public server end points are represented by an external URL. External requests are routed to the appropriate back-end instance according to the internal routing table.
Recommendations	Limit network access to your system in a way that only the platform router's end points are accessible from outside the system. This can be accomplished by means of network zones and firewalls.
How to Verify	Get in touch with your network administrators.
Related Alert	No
More Information	See the sections on XS advanced application server components and public end points in the <i>SAP HANA Security Guide</i> .

Default	The XS advanced platform router, which is realized by an SAP Web Dispatcher instance, accepts cipher suites TLS 1.0, TLS 1.1 and TLS 1.2 for external requests, by default. The weaker suite TLS 1.0 is allowed due to the fact that a lot of clients do not support higher protocol versions.
Recommendations	If the limitation for some non-compatible clients is accepted, it is recommended to disable all TLS versions below TLS 1.2 as described in the <i>SAP HANA Administration Guide</i> .
Related Alert	No
More Information	See the following section of the <i>SAP HANA Administration Guide</i> : ► Application Run-Time Services ► Maintaining the SAP HANA XS Advanced Model Run Time ► Configuring the XS Advanced Platform Router ► Configuring the Platform Router with INI Parameters ►

Security Areas

Default	The JDBC connection to the SAP HANA database is not encrypted by default.
Recommendations	Activate JDBC TLS/SSL between application server and the SAP HANA database in all scenarios. Configure custom SSL certificates as described in the <i>SAP HANA Security Guide</i> .
How to Verify	Get in touch with your network administrators.
Related Alert	No
More Information	See the section on XS advanced certificate management in the <i>SAP HANA Security Guide</i> .

Certificate Management

Default	By default, the XS advanced server runs with self-signed certificate for all domains.
Recommendations	Configure the XS advanced server to accept a custom certificate for all your domains, especially the shared domain (used for XS CLI communication). Custom certificates can be upload by using the <code>xs set-certificate</code> command for each domain.
How to Verify	Check the certificate in your Web browser when loading from a specific domain.
Related Alert	No
More Information	See the section on XS advanced certificate management in the <i>SAP HANA Security Guide</i> , as well as SAP Note 2243019 in <i>Related Information</i> below.

Related Information

[Application Server Components](#)
[Public Endpoints](#)
[XS Advanced Certificate Management](#)
[Configuring the XS Advanced Platform Router](#)

SAP Note 2243019 

Important Disclaimer for Features in SAP HANA



For information about the capabilities available for your license and installation scenario, refer to the [Feature Scope Description for SAP HANA](#).

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.