



Security Guide | PUBLIC
2022-06-21

SAP Security Guide: SAP Applications on SAP Adaptive Server Enterprise

Content

- 1 User Administration and Authentication. 3**
- 1.1 Operating System Users. 4
- 1.2 Database Logins. 5
- 1.3 SAP System Users. 6

- 2 Network and Communication Security. 8**

- 3 File System Permissions. 9**

- 4 Maintenance Actions in the DBA Cockpit. 10**

- 5 Additional Information. 13**

1 User Administration and Authentication

SAP applications running on the database SAP Adaptive Server Enterprise (SAP ASE) use the authentication mechanisms provided with the SAP NetWeaver Application Server platform. Therefore, the security recommendations and guidelines for user administration and authentication as described in the following guides also apply to SAP Business Suite on SAP ASE:

- **ABAP:**
<http://help.sap.com/nw>
▶ *SAP NetWeaver Platform* ▶ *SAP NetWeaver <Release>* ▶ *Security* ▶ *SAP NetWeaver Security Guide* ▶ *Security Guides for SAP NetWeaver Functional Units* ▶ *Security Guides for the AS ABAP* ▶
- **Java:**
<http://help.sap.com/nw>
▶ *SAP NetWeaver Platform* ▶ *SAP NetWeaver <Release>* ▶ *Security* ▶ *SAP NetWeaver Security Guide* ▶ *Security Guides for the AS Java* ▶

In addition to these guidelines, we include information about user administration and authentication that specifically applies to the use of SAP applications on the database SAP Adaptive Server Enterprise.

You need to ensure the security of the users that the installer created during installation. The table below lists these users:

- Operating system users
- Database logins
- SAP system users

The installer will, by default, have assigned the master password to all users that were created, unless you specified other passwords.

If you change user passwords, be aware that SAP system users might exist in multiple SAP system clients (for example, if a user was copied as part of the client copy). Therefore, you need to change the passwords in all the relevant SAP system clients.

The installer has applied the master password to users **SAP*** and **DDIC** only for SAP system clients 000 and 001, not to users **SAP***, **DDIC**, and **EARLYWATCH** in client 066.

Instead, the installer always assigns the following passwords to these users in client 066:

SAP*: 06071992

EARLYWATCH: support

i Note

Client 066 is no longer available in newly installed SAP systems based on SAP NetWeaver 7.5. For more information, see SAP Note [1749142](#).

1.1 Operating System Users

During the installation, the installer checks all required accounts (users, groups) and services on the local machine. The installer checks whether the required users and groups already exist. If not, the installer creates the following new users and groups:

Operating System Users - UNIX

User	Primary Group
UNIX superuser <code>root</code>	No primary group assigned by the installer (group <code>sapinst</code> is assigned as secondary group)
SAP system administrator <code><sapsid>adm</code>	<code>sapsys</code> (<code>sapinst</code> as secondary group)
<code>syb<dbsid></code>	<code>sapsys</code>

Operating System Users - Windows

User	Comment
SAP system administrator <code><sapsid>adm</code>	SAP system administrator
<code>syb<dbsid></code>	Database administrator
<code>SAPService<sapsid></code>	SAP service user

Users and Groups of the SAP Host Agent:

User:	Primary Group:	Additional Group:	Comment:
<code>sapadm</code>	<code>sapsys</code>	<code>sapinst</code>	Host Agent administrator

i Note

We recommend changing the user IDs and passwords for users that are automatically created during installation.

The table below shows the tools to use for user management and user administration:

Tool:	Detailed Description:
Transactions SU01, PFCG (user and role maintenance with SAP NetWeaver AS ABAP)	For more information, see http://help.sap.com/nw ▶ SAP NetWeaver Platform ▶ SAP NetWeaver <Release> ▶ Security ▶ SAP NetWeaver Security Guide ▶ User Administration and Authentication ▶

Tool:	Detailed Description:
User Management Engine with SAP NetWeaver AS Java	<p>For more information, see http://help.sap.com/nw</p> <p>▶ SAP NetWeaver Platform ▶ SAP NetWeaver <Release> ▶ Security ▶ SAP NetWeaver Security Guide ▶ User Administration and Authentication ▶</p>

1.2 Database Logins

During installation, the installer creates the following database users:

Login:	Roles:	Comment:
sapsa	sap_adm, sybase_ts_role	Database Administrator
sapssso	sso_role	Database Security Officer
SAPSR3	sap_mon	ABAP connect / database login
SAPSR3DB	sap_mon	Java connect / database login

i Note

For security reasons, the Adaptive Server default login `sa` is locked by the installer after installation has been completed.

Proceed as described in SAP Note [1796540](#) to change the password for users SAPSR3, SAPSR3DB, sapsa, sapssso, and sa on the database server.

1.3 SAP System Users

After installation, ABAP and Java system users are available. The following table shows these users, together with recommendations on how you can ensure the security of these users:

User:	User Name:	Comment:
SAP system user	SAP*	This user exists in at least clients 000, 001, and 066* of the ABAP system. We recommend that you use strong password and auditing policies for this user.
	DDIC	This user exists in at least clients 000, 001, and 066* of the ABAP system. We recommend that you use strong password and auditing policies for this user.
	EARLYWATCH	This user exists in at least client 066* of the ABAP system.
	SAPCPIC	This user exists in at least client 000 and 001 of the ABAP system.
Administrator	The name that you gave this user during installation or the default name J2EE_ADMIN	This user exists in at least clients 000 and 001 of the ABAP system and in the User Management Engine (UME) of the Java system. It has administrative permissions for user management. We recommend that you use strong password and auditing policies for this user.
Guest	The name that you gave this user during installation or the default name J2EE_GUEST	This user exists in at least clients 000 and 001 of the ABAP system and in the User Management Engine (UME) of the Java system. It is used for anonymous access.
Communication user for the J2EE engine	The name that you gave this user during installation or the default name SAPJSF	This user exists in at least clients 000 and 001 of the ABAP system and in the User Management Engine (UME) of the Java system. It is used for remote function calls (RFC) between the ABAP system and the Java.
SDM	SDM	This user is used to access the Software Deployment Manager (SDM) in the Java system.

User:	User Name:	Comment:
User for Adobe Document Services (ADS)	ADSUser	This user exists in at least clients 000 and 001 of the ABAP system and in the User Management Engine (UME) of the Java system. It is used for basic authentication.
User for Adobe Document Services (ADS)	ADS_AGENT	This user exists in at least clients 000 and 001 of the ABAP system and in the User Management Engine (UME) of the Java system. It is used for processing forms between an ABAP and a Java environment.
Data supplier user for System Landscape Directory (SLD) (optional)	The name that you gave this user during installation. The recommended name is SLDDSUSER.	This user exists in at least clients 000 and 001 of the ABAP system and in the User Management Engine (UME) of the Java system. The installer created this user automatically if you chose <i>Configure local SLD</i> during the installation.

i Note

* Client 066 is no longer available in newly installed SAP systems based on SAP NetWeaver 7.5. For more information, see SAP Note [1749142](#).

i Note

We recommend changing the user IDs and passwords for users that are automatically created during installation.

The table below shows the tools for user management and administration:

Tool:	Detailed Description:
Transactions SU01, PFCG (user and role maintenance with SAP NetWeaver AS ABAP)	For more information, see http://help.sap.com/nw <ul style="list-style-type: none"> ▶ SAP NetWeaver Platform ▶ SAP NetWeaver <Release> ▶ Security ▶ SAP NetWeaver Security Guide ▶ User Administration and Authentication ▶
User Management Engine with SAP NetWeaver AS Java	For more information, see http://help.sap.com/nw <ul style="list-style-type: none"> ▶ SAP NetWeaver Platform ▶ SAP NetWeaver <Release> ▶ Security ▶ SAP NetWeaver Security Guide ▶ User Administration and Authentication ▶

2 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs, without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, there is no way that intruders can compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN, they cannot exploit well-known bugs and security holes in network services on the server machines. The network topology for SAP on ASE is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply.

UserID and password are encoded only when transported across the network. Therefore, we recommend using encryption at the network layer, either by using the Secure Sockets Layer (SSL) protocol for HTTP connections or Secure Network Communications (SNC) for the SAP protocols dialog and RFC.

For more information, see:

- Network and Transport Layer Security
<http://help.sap.com/nw>
▶ *SAP NetWeaver Platform* ▶ *SAP NetWeaver <Release>* ▶ *Security* ▶ *SAP NetWeaver Security Guide* ▶
Network and Communication Security ▶
- Security Guides for Connectivity and Interoperability Technologies
<http://help.sap.com/nw>
▶ *SAP NetWeaver Platform* ▶ *SAP NetWeaver <Release>* ▶ *Security* ▶ *SAP NetWeaver Security Guide* ▶
Security Guides for Connectivity and Interoperability Technologies ▶

3 File System Permissions

The file systems and logical volumes must have the permissions and owners shown in the following table. The installer sets the required permissions and owners.

i Note

You can create the owners and groups manually if they do not exist. Otherwise, the installer creates them automatically.

File System Permissions - UNIX

File System / Logical Volume	Permissions	Owner	Group
/sybase/<DBSID>	750	syb<dbsid>	sapsys
/sybase/<DBSID>/sybsystem	750	syb<dbsid>	sapsys
/sybase/<DBSID>/sybtemp	750	syb<dbsid>	sapsys
/sybase/<DBSID>/sapdiag	750	syb<dbsid>	sapsys
/sybase/<DBSID>/sapdata_<n>	750	syb<dbsid>	sapsys
/sybase/<DBSID>/saplog_<n>	750	syb<dbsid>	sapsys

File System Permissions - Windows

File System /Logical Volume	Access Privilege Full Control for User/Group
<drive>:\sybase\<DBSID>	syb<dbsid>, Administrators, SYSTEM, SAPLocalAdmin
<drive>:\sybase\<DBSID>\sybsystem	syb<dbsid>, Administrators, SYSTEM, SAPLocalAdmin
<drive>:\sybase\<DBSID>\sybtemp	syb<dbsid>, Administrators, SYSTEM, SAPLocalAdmin
<drive>:\sybase\<DBSID>\sapdiag	syb<dbsid>, Administrators, SYSTEM, SAPLocalAdmin
<drive>:\sybase\<DBSID>\sybdata_<n>	syb<dbsid>, Administrators, SYSTEM, SAPLocalAdmin
<drive>:\sybase\<DBSID>\saplog_<n>	syb<dbsid>, Administrators, SYSTEM, SAPLocalAdmin

After installation, you also need to copy the installation directory to a separate, secure location and then delete the installation directory.

4 Maintenance Actions in the DBA Cockpit

The DBA Cockpit provides a set of actions to monitor and to maintain the database. To be able to perform these actions, the SAP user requires some additional authorizations. A user must first have the global authorization and then additionally the appropriate system-specific permission. For example, to administrate a system, the user must have `S_RZL_ADM` authorization for maintenance and the system-specific authorization for maintenance. The following sections provide information about how global and system-specific authorizations are checked and what you need to do to gain the required authorizations.

The maintenance actions provided in the DBA Cockpit set locks to prevent parallel processing. All changes to the database are recorded in an audit log.

Global Authorization Check

When you start the DBA Cockpit or change to another system in the DBA Cockpit, an authorization check is performed.

You can enable or disable the database maintenance in general using the profile parameter `db/s/dba/ccms_maintenance`. If this profile parameter is not set in the instance profile, the default value `1` is used.

Depending on the setting of profile parameter `db/s/dba/ccms_maintenance`, the following authorization checks exist:

- If the profile parameter is set to `0`, SAP users cannot perform any maintenance actions, regardless of their personal permissions.
- If the profile parameter is set to `1`, SAP users can perform maintenance actions depending on their personal permission for the authorization object `S_RZL_ADM`. The attribute `ACTVT` of this authorization object defines whether a user may maintain or only monitor objects.

System-specific Authorization Check

In addition to the permissions that are globally granted, you can restrict access to specific systems that were configured in the DBA Cockpit. You enable or disable the system-specific permission checks using the profile parameter `db/s/dba/ccms_security_level`.

If this profile parameter is **not** set in the instance profile, the default value `0` is used. Depending on the setting of profile parameter `db/s/dba/ccms_security_level`, the following authorization checks are performed when you select a system in the DBA Cockpit:

- If parameter `db/s/dba/ccms_security_level` is set to `0`, no additional system-specific check is performed.
- If parameter `db/s/dba/ccms_security_level` is set to `1`, SAP system users can perform actions depending on their personal permission for the authorization object `S_DBCON`.

The attributes `DBA_DBHOST`, `DBA_DBSID`, and `DBA_DBUSER` must match the corresponding attributes for the database connection that was assigned to the selected system. The special value `<LOCAL SYSTEM>` for the attribute `DBA_DBSID` is used to identify the local system itself.

The attribute `ACTVT` of this `S_DBCON` authorization object defines the level of permitted actions and can have the following values:

Value:	Description:
03 Display	Enables read access to all screens of the DBA Cockpit except to those that only have a maintenance mode and no read-only mode.
23 Maintain	Enables read and maintenance access to all screens of the DBA Cockpit except those that require extended maintenance permissions.
36 Extended maintenance	Enables read and maintenance access to all screens of the DBA Cockpit including special maintenance screens.

i Note

The only screen for which extended maintenance permission is required is the `SQL Command Line` screen that you can access in the `Favorites` list of the DBA Cockpit.

You can grant authorizations for using the DBA Cockpit with the following roles:

- `SAP_BC_S_DBCON_USER`
Read-only role that allows monitoring access to all systems configured within the DBA Cockpit.
- `SAP_BC_S_DBCON_ADMIN`
Additionally grants administration rights to the user for all systems. This role does *not* include the value *Extended Maintenance*.

i Note

Make sure that you have maintained the authorizations for your DBA user and for all batch users that either run jobs of the DBA Planning Calendar or the SAP standard jobs `SAP_COLLECTOR_FOR_PERFMONITOR` and `SAP_CCMS_MONI_BATCH_DP`.

Granting Database Permissions

To access the database, the database user that is used for monitoring must at least have sufficient authorizations as follows:

- If you want to connect to remote systems running on SAP ASE, you can freely select a user for monitoring. Nevertheless, we recommend that you use the `sapsa` login when adding remote systems because only `sapsa` has sufficient authorizations to execute administrative tasks.
- If you want to connect to remote systems running on any other database platform, see the appropriate DBA Cockpit documentation for the database platform.

- Local systems use a special administration connection. This connection is called `+++SYBADM` and is automatically generated. When you start the DBA Cockpit and the administration connection does not have yet a user assigned, you are asked for the password of the `sapsa` login.
If you do not supply the correct user credentials, a standard connection with the SAP connect user is used instead of the administration connection. In this case all administrative actions of the DBA Cockpit are disabled. You can change the user and password for the administrative connection as described in *Configuring Database Connections* in the Database Administration Guide. This is mandatory for background tasks that require administrative permissions.

Locking of Actions






For each maintenance action that you have selected using the DBA Cockpit, a lock is set for the system that is being monitored. All locks are released when you exit the DBA Cockpit or when you change to another system.

Auditing of Maintenance Actions

When you make changes that affect database objects such as Adaptive Server configuration parameters, an audit log is written. You can display this audit log in the DBA Cockpit.

5 Additional Information

For more information about specific topics, see the Quick Links as shown in the table below.



Content	Quick Links
Security	Security Community 
Security Guides	http://help.sap.com/nw ▶ SAP NetWeaver <product> ▶ Security ▶
Related SAP Notes	http://support.sap.com/notes  Use http://support.sap.com/securitynotes  to stay informed about the latest critical SAP Notes (updated monthly).
Released Platforms	http://support.sap.com/pam 
Network Security	http://help.sap.com/nw ▶ SAP NetWeaver <product> ▶ Security ▶
SAP Solution Manager	http://help.sap.com/solutionmanager https://support.sap.com/en/solution-manager.html 
SAP ASE - Security Administration Guide	https://help.sap.com/viewer/p/SAP_ASE ▶ <Release> ▶ Security ▶ Security Administration Guide ▶

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.

© 2022 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.