INTRODUCTION

SAP® solutions make customer businesses best-run businesses by providing software solutions to optimize and innovate core businesses processes. The SAP technology platform with ABAP™ is used to store and process business-critical data (e.g. financial data, human resources data, and customer relationship data). Therefore, it is crucial that customers secure the SAP technology platform. SAP systems must fulfill compliance regulations, such as the Sarbanes-Oxley Act (SOX). More generally, conformance to data protection and privacy laws as well as compliance to industry-specific regulations is required. Since SAP systems run business-critical processes, protecting them from attacks is a vital need.

To protect ABAP systems against unauthorized access and manipulation, security configuration must be applied on different levels (e.g. landscape architecture, operating system, database, SAP Basis, SAP applications, SAP authorizations). SAP and third parties provide comprehensive documentation on how ABAP systems can be secured, e.g. SAP Security Guides, SAP Security Notes, SAP Community Network, and materials in many books. Please refer to the Appendix of this document for further references.

The purpose of this document is to provide recommendations for the most important security configuration activities that should be performed for ABAP systems on an SAP Basis level. It does not cover topics that are mainly related to corporate policies or business processes, which differ largely from customer to customer. Examples of these exclusions are system administration and operation (e.g. operating system security, database security), SAP authorization concepts (e.g. segregation of duties on business and system operations levels), secure development, logging, and tracing.

The general scope of this document is a set of security measures for ABAP systems against unauthorized access within the corporate network. For Internet scenarios, additional security measures must be considered and implemented. More details can be found in the documentation provided by SAP. The topics listed in the following are covered in this document.

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>CONTENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Filtering</td>
<td>Network filtering is a fundamental requirement for secure ABAP systems. It reduces the attack surface to the least number of services required to be accessed by end users. Security measures for these services required in typical customer installations are covered in the remaining sections of the document.</td>
</tr>
<tr>
<td>SAP GUI for Windows</td>
<td>Customers can increase the security of their client workstations using the latest SAP GUI for Windows with security rules. It restricts SAP systems in the ability to perform security-relevant operations on client workstations (e.g. execute commands, upload files, etc.).</td>
</tr>
<tr>
<td>Password Management</td>
<td>Default passwords, weak password policies, and old password hashes can lead to insecure systems and need to be configured in a secure way.</td>
</tr>
<tr>
<td>Secure HTTP (HTTPS) &amp; Secure Network Communication</td>
<td>Cryptographically secured network communication is recommended to mitigate risks of interception of communication containing business data and user credentials (e.g. passwords, SAP logon tickets, etc.). Furthermore, protection of cryptographic keys is required.</td>
</tr>
<tr>
<td>Limit Web-Enabled Content</td>
<td>Only web content that is needed for business scenarios should be accessible to end users.</td>
</tr>
<tr>
<td>ABAP RFC (Remote Function Call) Connectivity</td>
<td>Security of SAP systems relies on separation of systems of different security classifications (e.g. development, test, and production). Interconnectivity between systems of different security classification might be required, but should be done considering guidelines to ensure security of systems with higher classification.</td>
</tr>
<tr>
<td>SAP Gateway Security &amp; SAP Message Server Security</td>
<td>Secure configuration of SAP gateways and SAP message servers is required to mitigate the risk of unauthorized access to SAP systems.</td>
</tr>
<tr>
<td>Security Patch Management for ABAP</td>
<td>Security Notes need to be implemented to ensure that identified security vulnerabilities are closed and cannot be misused by attackers.</td>
</tr>
<tr>
<td>Security Configuration Monitoring</td>
<td>As system configuration may change, monitoring of security configuration is essential to ensure systems remain in a secure state.</td>
</tr>
</tbody>
</table>

If you require support during implementation of SAP Security Notes referenced in this document please create an SAP customer support ticket for the primary component of the corresponding SAP Note (e.g. primary component BC-CST-GW for SAP Note 1408081 [39]).
NETWORK FILTERING

Secure network architecture is a fundamental requirement for secure ABAP systems. Network filtering must be used to reduce the attack surface. Implementation of network filtering between end user networks and ABAP systems [1] is required and documented in the SAP NetWeaver® Security Guide [2].

Figure 1: Attack Surface Reduction through Network Filtering

The network services listed in the following table are required to be accessible from end-user networks in most real-world ABAP installations. All other network services are typically not required and should be blocked between the end-user network and ABAP systems. Network services listed below refer to the standard installation of ABAP systems [3]. NN is used as a place holder for the instance number of the SAP system.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>REQUIRED FOR</th>
<th>PORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Dispatcher</td>
<td>SAP Dispatcher is used by SAP GUI. The communication protocol used is SAP DIAG.</td>
<td>32NN</td>
</tr>
<tr>
<td>SAP Gateway</td>
<td>SAP Gateway manages SAP Remote Function Call (RFC) communication.</td>
<td>33NN</td>
</tr>
<tr>
<td>SAP Message Server</td>
<td>SAP Message Server manages load balancing information and SAP internal communication.</td>
<td>36NN</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Secure HTTP</td>
<td>443NN</td>
</tr>
</tbody>
</table>
The network architecture depends on infrastructure components (e.g. SAProuter, SAP WebDispatcher, Load Balancer), which need to be taken into account for architecture planning. These infrastructure components do not change the fact that access to SAP DIAG, SAP RFC, SAP Message Server and HTTPS is necessary, but have impact on network filtering implementation.

This document acts on the assumption that only the network services listed above are available to end-user networks. Only security configurations for these services are covered by this document. If additional network services are made available to end-user networks, additional security measures need to be taken to secure these services.

![Diagram of SAP Architecture with Network Filtering](image)

**SAP GUI FOR WINDOWS**

ABAP systems can access security-critical functionality on SAP GUI end-user workstations under the permission of the end user (e.g. upload / download files, change Windows registry, execute programs).

SAP GUI 7.10 introduced the possibility of alerting end users in case of such access from ABAP systems. The option of alerting on security events can be enabled [4] but end users need to confirm access requests. This can lead to many security pop-ups.

SAP GUI 7.20 improves granularity and flexibility of security event handling. This is done using configurable security rules. SAP GUI 7.20 offers a default set of security rules that can be extended by customers [5]. This mitigates the risk of malicious attacks on SAP GUI workstations from ABAP systems that have been compromised.

It is strongly recommended to implement the following security measures:

- The latest available SAP GUI version should be deployed on all end user workstations [6].
- It should be ensured that SAP GUI security rules are activated [7] using at least the security rule setting “Customized” and default action “Ask”. 

Administrative access to the ABAP systems needs to be done from an administration network. This network is allowed to access the ABAP systems with administrative protocols (e.g. SSH, RDP, database administration, etc.). Access to the administrative network must be properly secured by common security concepts (e.g. allow administrative access to the ABAP systems only from dedicated subnets or admin workstations).
PASSWORD MANAGEMENT

SAP systems need to store password information in some representation like all systems using password-based logon. SAP systems do not store passwords as such but use one-way functions to calculate so-called password hashes. These are stored in the database. The system verifies user passwords using the one-way function to calculate the hash and compare it against the stored value. Since it is a one-way function, the password itself cannot be calculated from the stored password hashes.

All systems using this method are subject to password dictionary attacks or password brute-force attacks if the password hashes can be retrieved from the system [8]. The following security measures should therefore be taken to significantly reduce the probability of successful password cracking attacks.

Password Policy
- Set strong password policies according to your corporate policy [9]. The following profile parameters are relevant to configure password policies.
  - login/min_password_Ing
  - login/min_password_letters
  - login/min_password_digits
  - login/min_password_lowercase
  - login/min_password_uppercase
  - login/min_password_specials
  - login/password_max_idle_initial
  - login/password_max_idle_productive
  - login/password_max_idle_initial

- Enforce password policy for existing passwords during logon (login/password_compliance_to_current_policy = 1)

Password Hashes
- Restrict access to tables (USR02, USH02 and in later releases USRPWDHISTORY) containing password hashes [10] by changing the table authorization group of these tables. Non-administrative users must not have access to this new table authorization group.
- Activate the latest password hashing mechanism (code version) available for your release by setting the profile parameters below. Downward-compatible password hashes should not be stored on releases 7.0 onward. If you use SAP Central User Administration (CUA) you need to ensure that the CUA system has at least the same or a higher release than all attached systems [11] and that additional relevant SAP Notes are implemented, e.g. [12] [13].

<table>
<thead>
<tr>
<th>RELEASES</th>
<th>RECOMMENDED PROFILE PARAMETERS</th>
<th>CODE VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 4.5</td>
<td>No special profile parameter needed</td>
<td>B</td>
</tr>
<tr>
<td>4.6 to 6.40</td>
<td>login/password_charset=2</td>
<td>E</td>
</tr>
<tr>
<td>7.00 – 7.01</td>
<td>login/password_downwards_compatibility=0</td>
<td>F</td>
</tr>
<tr>
<td>7.02 onwards</td>
<td>login/password_downwards_compatibility=0</td>
<td>H</td>
</tr>
</tbody>
</table>

- After activation of the latest password-hashing mechanism, redundant password hashes need to be deleted from the relevant tables [14].

Users with ABAP Default Password
- Changing default passwords is crucial for secure system operation [15]. The default users that are created in different clients in every ABAP system are SAP*, DDIC, EARLYWATCH, SAPCPIC and TMSADM. Ensure to change the passwords of default users in all clients including unused clients. The report RSUSR003 [16] [17] or the Early Watch Alert can be used to verify that default passwords have been changed.
- Password change for the default user TMSADM needs to be done for all systems in an SAP transport management domain at the same time [18] [19]. A tool is provided to assist changing the TMSADM password in a transport landscape [20]. Systems with releases older than 4.6C should lock the user TMSADM [21].

SECURE NETWORK COMMUNICATION

The SAP proprietary protocols SAP DIAG (used for SAP GUI) and SAP RFC do not cryptographically authenticate client and server, neither do they encrypt network communication. Passwords transmitted over the network can be eavesdropped. Additionally, due to missing mutual authentication, rogue systems could intercept network traffic, manipulate content, and forward it to legitimate servers ("Man in the Middle" attacks).

Secure Network Communication (SNC) provides cryptographically strong mutual authentication, integrity protection of transmitted data, and encryption of network traffic. Its use is highly recommended to mitigate aforementioned risks.
SNC can be used without additional partner software for all RFC communication between SAP servers as well as for SAP GUI communication if SAP server and SAP GUI clients run Windows [22] [23]. An SNC partner product is required to secure SAP GUI connections in heterogeneous system landscapes (e.g. servers run AIX and clients run Windows).

The profile parameters snc/data_protection/min, snc/data_protection/max, snc/data_protection/use set the SNC level to be used: (1) secure authentication, (2) data integrity protection, and (3) confidentiality. Not all partner solutions provide all three SNC properties.

![CORPORATE NETWORK](image)

Figure 3: Recommended Scenarios for Secure Network Communication (SNC)

Although detailed requirements for SNC implementations are customer-specific, at least the following security measures should be taken:
- Implement SNC between SAP GUI and ABAP systems since end user traffic may pass networks susceptible to network sniffing (snc/enable=1). The use of SNC is documented in the SNC User’s Guide [24].
- For production systems it is highly recommended to deactivate non-SNC access for most SAP GUI users (snc/accept_insecure_gui=U). Only a small number of emergency accounts should be able to access the system with password login.
- For RFC communication, SNC should be implemented if the network traffic is susceptible to sniffing by end users.

**SECURE HTTP (HTTPS)**

Besides SAP DIAG, ABAP systems offer web-based access over HTTP. With HTTP all communication, including user credentials like passwords or SAP Logon Tickets, is unencrypted and can be sniffed in the network. Therefore web-based access should be secured using HTTPS (HTTP over SSL/TLS).

**Usage of HTTPS**
- Usage of HTTPS is strongly recommended at least for all browser access from end users to ABAP systems. End users should not use HTTP to access ABAP systems.
- For communication between ABAP systems, HTTPS should be implemented if the network traffic is susceptible to sniffing by end users.
- HTTPS should be implemented to terminate on infrastructure components (e.g. load balancers, reverse proxies) in the server network or ABAP systems should be configured to directly support HTTPS / SSL server. Information about SSL server configuration is provided in SAP Notes and the SAP Help Portal [25], [26], [27].

SSL server configuration requires cryptographic keys. Other cryptographic keys are used for creation of SAP Logon Tickets, Secure Network Communication, or Web Service security. These keys are stored in PSE files on the server file system in the directory <instance directory>/sec and in the database table SSF_PSE_D. Access to these keys must be protected. The system security of ABAP systems is highly endangered if unauthorized access to cryptographic keys is possible. The following security measures should be taken to restrict the access.

**Protection of Cryptographic Keys**
- Restrict access to the table SSF_PSE_D by assigning the table to a dedicated table authorization group [28]. End users should not have access to this new table authorization group.
- Restrict file system access to PSE files from ABAP programs [29].
LIMIT WEB-ENABLED CONTENT

ABAP systems offer web-enabled content that can be accessed using web browsers. This content is managed by the SAP Internet Communication Framework (ICF) and maintained via transaction SICF. Some of the ICF services could potentially be misused, and unauthorized access to system functionality might be possible.

Figure 4: Attack Surface Reduction by limiting ICF services

The following recommendations apply for the handling of web-enabled content in the SAP Internet Communication Framework:

- Only ICF services that are required for business scenarios should be enabled. Particularly on productive SAP systems, not all ICF services should be enabled.
- If it is suspected that more ICF services than necessary are activated, actual usage of ICF services can be analyzed and services can be mass maintained with releases 7.0 onwards.
- Short term: Review at least all ICF services that do not require user authentication. This includes all services in /sap/public as well as services with stored logon data.
- Short term: It is recommended to deactivate at least the ICF services listed in the table below if they are not used in your business scenarios.

<table>
<thead>
<tr>
<th>SICF SERVICE</th>
<th>SAP NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>/sap/bc/soap/rfc</td>
<td>SAP Note 1394100 [31]</td>
</tr>
<tr>
<td>/sap/bc/echo</td>
<td>SAP Note 626073 [32]</td>
</tr>
<tr>
<td>/sap/bc/FormToRfc</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/report</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/xrfc</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/xrfc_test</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/error</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/webrfc</td>
<td>SAP Note 865853 [33]</td>
</tr>
<tr>
<td>/sap/bc/bsp/sap/certreq</td>
<td>SAP Note 1417568 [34]</td>
</tr>
<tr>
<td>/sap/bc/bsp/sap/certmap</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/gui/sap/its/CERTREQ</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/gui/sap/its/CERTMAP</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/bsp/sap/bsp_veri</td>
<td>SAP Note 1422273 [35]</td>
</tr>
<tr>
<td>/sap/bc/iDoc_XML</td>
<td>SAP Note 1487606 [36]</td>
</tr>
<tr>
<td>/sap/bc/srt/iDoc</td>
<td></td>
</tr>
</tbody>
</table>

ABAP RFC CONNECTIVITY

SAP Remote Function Call (RFC) is an SAP proprietary protocol. It is the main integration technology between SAP systems and is also heavily used in integrations with non-SAP systems. Other integration technologies like web services are increasingly complementing RFC.

RFC connections between systems are maintained in so-called RFC destinations. RFC destinations are maintained in destination source systems pointing to destination target systems. Improper management of RFC destinations can lead to privilege escalation. SAP ALL access in production systems could potentially be gained using improperly configured RFC destinations in development systems. These risks can be mitigated by following the guidelines below to maintain ABAP connections (type 3) and logical connections (type L) in transaction SM59. The following recommendations focus on these two destination types.
To securely manage ABAP and logical RFC destinations, three different categories are distinguished.

- 1) Destinations storing technical connectivity configuration without stored credentials and without trust relationships between the systems. They require user authentication for each access.
- 2) Destinations with technical connectivity configuration using stored credentials (i.e. client, user, and password).
- 3) Destinations with technical connectivity configuration using trusted system logon (Trusted / Trusting RFC).

All three categories of RFC destinations are allowed to be used between systems of the same security classification (e.g. from a production system to another production system). They are also allowed from systems of higher security classification to systems of lower security classification (e.g. from a production system to a development system).

As a general guideline, destinations from systems of lower security classification to systems of higher security classification are not allowed to store user credentials or to use trusted system logon (e.g. from a development system to a production system). These destinations are only allowed to store technical connectivity configuration and authenticate the user for each access. One exception to this general guideline is TMS destinations. If these destinations are required nevertheless, they must be considered security risks and must only be used after thorough risk analysis.

Additionally, it should be generally forbidden from systems of higher security classification to trust systems of lower security classification. Otherwise, the security level of the trusting system is reduced to the security level of the trusted system.

Particularly in production environments, users stored in RFC destinations should only have the minimum authorization in the destination target that is required for the business scenario executed over that destination [37] [38]. We recommend using dedicated accounts per scenario wherever possible. Inspect the SAP Security Guide of an application to get information about required authorizations. It is a common misunderstanding to assume that assigning SAP_ALL privileges to users in destinations with stored credentials is secure as long as the user is not of type “DIALOG.”

Figure 5 ABAP RFC Connectivity
The following security measures should be taken to mitigate the risk of unauthorized access via RFC destinations:

- Analyze all system trust relationships between ABAP systems using transactions SMT1 and SMT2. Identify the trust relationships in which systems of higher security classification trust systems of lower security classification (e.g. test to production, or development to production). Remove this system trust wherever possible.
- Identify RFC destinations with stored user credentials from systems of lower security classification to systems of higher security classification (using report RSRFCCHK). The stored credentials should be removed wherever possible. This way, user authentication is enforced for every access.
- Create a list of RFC destinations with stored credentials and ensure that user accounts have minimum authorizations (especially not SAP_ALL) assigned in the destination target and that the user type is set to "SYSTEM."

**SAP GATEWAY SECURITY**

The SAP gateway is the technical component of the application server that manages the communication for all SAP Remote Function Call (RFC) based functionality. RFC communication can be categorized in three different scenarios as shown in the figure below.

1) **ABAP RFC**: The most frequently used RFC functionality in customer installations is provided by ABAP remote-enabled function modules. For instance, technologies like Business Application Programming Interface (BAPI), Application Link Enabling (ALE), or Intermediate Document (IDoc) are provided by ABAP and use RFC as the underlying communication protocol. Securing these ABAP connections is covered in the section on ABAP RFC connectivity. The mechanisms used to secure this communication are based on end user authentication and authorization checks in the ABAP system (e.g. authorization object S/rfc in the called system and S_ICF in the calling system). The SAP gateway does not perform additional security checks.

2) **Registered RFC Server Program**: The second-most used RFC functionality is the so-called registered RFC server programs. These use the SAP RFC library and integrate ABAP systems with non-ABAP systems that provide RFC functions. The external RFC server programs register at the SAP gateway and can later be accessed by RFC clients via the same SAP gateway. Very often this RFC client is actually the ABAP system where the external RFC server program is registered. This is configured in transaction SM59 in RFC destinations of type T with technical setting “Registered Server Program”. One example for this use case is the SAP NetWeaver Search and Classification TREX.

Registered RFC server programs are a very common integration technology and are being developed by SAP and partner companies. Typically, registered RFC servers do not perform user authentication or authorization checks. Registration of RFC server programs and RFC client access to these servers is controlled via SAP gateway access control lists (secinfo for releases up to 4.6 and reginfo in higher releases).

3) **Started RFC Server Program**: Finally there are so-called started RFC server programs. They are also built with the SAP RFC library but instead of registering at the SAP gateway they reside on the host of the application server. The SAP gateway launches these RFC server programs triggered by RFC client requests. One example is the start of the RFC server program SAPXPG, which is used via transaction SM49 to execute operating system commands on application servers. SAP default configurations only start these RFC server programs locally. This is configured in transaction SM59 in RFC destinations of type T with technical setting “Start on Explicit Host” and gateway options explicitly pointing to the local SAP gateway or just being blank. Again in most cases started RFC servers do not perform user authentication or authorization checks. As in the case of registered RFC servers, access to these started RFC servers is controlled via SAP gateway access control lists (secinfo for all releases).
For system security it is of utmost importance that the SAP gateway access control lists (ACL) are created and maintained properly. The ACL files do not exist in default installations. Hence no restrictions exist regarding RFC server registration, access to registered RFC servers, or starting of RFC server programs in default installations. This can lead to system compromise.

SAP provides guidelines on how to set up the ACLs [39] [40], and minimum SAP kernel patch levels and configuration switches need to be implemented [41] [42]. SAP provides a tool [43] to create SAP gateway ACLs that cover typical usage scenarios for registered and started RFC server programs.

SAP gateway logging should be activated in order to support ongoing maintenance and provide monitoring [44].

Additionally, SAP gateway monitoring should only allow local access (gw/monitor = 1) [45]. This is the default configuration setting since release 6.40.

The following security measures should be taken to protect the SAP gateway:
- Verify the minimum SAP kernel patch levels [41]
- Set profile parameters gw/sec_info, gw/reg_info and gw/reg_no Conn_info
- Create secinfo and reginfo ACL files manually [39] or with the tool [43]
- Reload ACL files dynamically on each application server to activate changes
- If necessary, missing configurations can be identified by
  - Activation of SAP gateway logging and log file review
  - Analysis of the error messages shown on the RFC client

SAP MESSAGE SERVER SECURITY

The SAP message server is a system component that provides two services. On the one hand, it manages SAP communication between the application servers of one SAP system. On the other hand, it provides load-balancing information to clients like the SAP GUI. In standard installations before release 7.0, both clients and application servers use the same message server port for communication. Since release 7.0, default installations automatically split the message server port in an internal port (used for application server connections) and an external port (used for end user connections). This is defined via profile parameters rdisp/mshost, rdisp/msserv, and rdisp/msserv_internal.

Without appropriate security measures, malicious programs on client machines could potentially access the message server to spoof application server communication. This could potentially lead to privilege escalation. It is therefore strongly recommended to implement the following security measures to mitigate the risks of unauthorized SAP message server access [46] [47].

<table>
<thead>
<tr>
<th>RELEASES</th>
<th>RECOMMENDED CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 4.5</td>
<td>The SAP message server port (rdisp/mshost, rdisp/msserv) should be firewalled. Only network segments with SAP servers should be granted access to this port. Client networks should be blocked from accessing the SAP message server. Please be aware that this has an impact on the ability to provide load balancing functionality to SAP GUI clients.</td>
</tr>
<tr>
<td>4.6</td>
<td>The SAP message server services should be separated in two ports [46]. One port is used for SAP GUI client access (rdisp/msserv) and the other is used for access to internal server communication (rdisp/msserv_internal). Internal system communication (rdisp/msserv_internal) needs to be firewalled. Only network segments with SAP servers should be granted access to internal server communication. Additional information is provided in the SAP NetWeaver Security Guide [47].</td>
</tr>
<tr>
<td>6.40 onwards</td>
<td>In addition to the measures recommended for release 4.6, a message server ACL should be activated that lists all relevant network interfaces (e.g. including failover interfaces) of all application servers (ms/acl_info).</td>
</tr>
</tbody>
</table>

In addition to the access restrictions for the SAP message server, it is recommended to restrict the access to remote message server monitoring (ms/monitor = 0) [48].
SECURITY PATCH MANAGEMENT FOR ABAP

As with all software and despite thorough testing, ABAP systems may have software bugs that can cause functionality issues but may also be security critical. The common method to deliver small software fixes are SAP Notes. For security critical issues, SAP releases SAP Security Notes. A comprehensive list of all released SAP Security Notes is available in the SAP Service Market Place [49].

To ensure that required SAP Security Notes are installed on ABAP systems, the following security measures are recommended:
- As a minimum, regularly (at least once a month in the week after an SAP Security Patch Day) review the SAP EarlyWatch Alert report which allows you to check if relevant SAP Security Notes are missing. Due to technical restrictions, the report can currently not check all SAP Security Notes automatically [50]. Those notes which are checked automatically are flagged in the list of SAP Security Notes on the SAP Service Marketplace [49]. Implement SAP Security Notes which have not yet been implemented.
- In addition, regularly review the released SAP Security Notes [49] to identify security notes where implementation cannot be checked automatically via SAP EarlyWatch Alert (e.g. SAP Notes with general configuration guidelines).

SECURITY CONFIGURATION MONITORING

ABAP systems can become insecure again if previously applied security configurations are reverted or disabled. Security configuration monitoring is therefore recommended to regularly verify applied security configurations (recommended at least once a month). Identified deviations need to be realigned. SAP offers different granularity for security configuration monitoring.

- SAP Early Watch Alert (EWA) is a tool that monitors the essential administrative areas of SAP components and keeps customers up to date on their performance and stability. As part of EWA, SAP also provides selected checks on security-relevant configuration (including aforementioned implementation status of relevant SAP Security Notes) [51][52].
- SAP Security Optimization Service (SOS) is designed to check the security of your SAP system. This service comprises a system analysis and the resulting recommendations for system settings. It addresses system and customizing settings that impact system security. It focuses on internal and external system security. To improve the internal security, many critical authorization combinations are checked. External security is improved by checking the access possibilities to your system and checking the authentication methods used. This service checks the configuration of an ABAP system on pre-defined security topics [53].
- SAP Computing Center Management System (CCMS) is a general framework to monitor an ABAP system and alert on events. CCMS can be customized to monitor security-critical settings and alert you in case of changes [54].
- SAP Solution Manager Diagnostics (SMD) Configuration Validation Reporting delivers a generic framework to verify configurations of connected managed SAP systems. This framework can be used to define expected system configurations according to policies and guidelines and compare them against the actual configuration of managed SAP systems [55].

To ensure that ABAP systems are in a secure state, the following security measures are recommended:
- Define which security configurations must be monitored
- Implement a solution to monitor relevant security configurations and alert in case of deviations
This document is focused on a selection of very important security-related configurations in ABAP systems. Due to its compact nature it is not complete. In-depth resources on SAP security can be found in the, SAP Service Marketplace, the SAP Help Portal and in the SAP Developer Network.

**SAP Service Marketplace**
- SAP Security @ SMP (https://service.sap.com/security)

**SAP Help Portal**
- SAP Library including online version of SAP NetWeaver Security Guides (http://help.sap.com)

**SAP Developer Network**
- Security and Identity Management (https://www.sdn.sap.com/irj/sdn/security)

---

1. Architecture of the SAP NetWeaver Application Server
3. TCP/IP Ports Used by SAP Applications
4. SAP Note 1038799 - Security: Controlling backend operations
5. SAP Note 1483525 - New security center in SAP GUI for Windows 7.20
6. SAP Note 147519 - Maintenance strategy / deadlines 'SAP GUI'
7. SAP GUI for Windows 7.20 Security Guide
8. SAP Note 1237762 - ABAP systems: Protection against password hash attacks
9. SAP NetWeaver Application Server ABAP Security Guide, Profile Parameters for Logon and Password (Login Parameters)
10. SAP Note 1484692 - Protect read access to password hash value tables
11. SAP Note 1300104 - CUA: new password hash procedures: Background information
12. SAP Note 1306019 - CUA: Downward-compatible passwords in old child systems
13. SAP Note 1022812 - CUA: Initial passwords not possible for child systems
14. SAP Note 1458262 - ABAP: recommended settings for password hash algorithms
15. SAP NetWeaver Application Server ABAP Security Guide, Section Protecting Standard Users
16. SAP Note 40689 - New reports for the User Information System
17. SAP Note 1488159 - SJMUSART003 incorrect results for CODVN = 'F'
18. SAP Note 1488406 - Handling the generated user TMSADM
19. SAP Note 761637 - Logon restrictions prevent TMSADM logon
20. SAP Note 1414256 - Help tool for changing TMSADM password
21. SAP Note 1486759 - Blocking unauthorized access to system using TMSADM to 4.6B
22. SAP Note 352295 - Microsoft Windows Single Sign-On options
23. Unleash the Power of Single Sign-On with Microsoft and SAP

---

**APPENDIX**

Due to its compact nature it is not complete. In-depth resources on SAP security can be found in the, SAP Service Marketplace, the SAP Help Portal and in the SAP Developer Network.

**SAP Service Marketplace**
- SAP Security @ SMP
- SAP Security Guides
- SAP Security Notes
- SAP Security Optimization Services
- RunSAP End-to-End Solution Operations

**SAP Help Portal**
- SAP Library including online version of SAP NetWeaver Security Guides

**SAP Developer Network**
- Security and Identity Management
- SAP Community Network Forums: Security

---

1. Architecture of the SAP NetWeaver Application Server
3. TCP/IP Ports Used by SAP Applications
4. SAP Note 1038799 - Security: Controlling backend operations
5. SAP Note 1483525 - New security center in SAP GUI for Windows 7.20
6. SAP Note 147519 - Maintenance strategy / deadlines 'SAP GUI'
7. SAP GUI for Windows 7.20 Security Guide
8. SAP Note 1237762 - ABAP systems: Protection against password hash attacks
9. SAP NetWeaver Application Server ABAP Security Guide, Profile Parameters for Logon and Password (Login Parameters)
10. SAP Note 1484692 - Protect read access to password hash value tables
11. SAP Note 1300104 - CUA: new password hash procedures: Background information
12. SAP Note 1306019 - CUA: Downward-compatible passwords in old child systems
13. SAP Note 1022812 - CUA: Initial passwords not possible for child systems
14. SAP Note 1458262 - ABAP: recommended settings for password hash algorithms
15. SAP NetWeaver Application Server ABAP Security Guide, Section Protecting Standard Users
16. SAP Note 40689 - New reports for the User Information System
17. SAP Note 1488159 - SJMUSART003 incorrect results for CODVN = 'F'
18. SAP Note 1488406 - Handling the generated user TMSADM
19. SAP Note 761637 - Logon restrictions prevent TMSADM logon
20. SAP Note 1414256 - Help tool for changing TMSADM password
21. SAP Note 1486759 - Blocking unauthorized access to system using TMSADM to 4.6B
22. SAP Note 352295 - Microsoft Windows Single Sign-On options
23. Unleash the Power of Single Sign-On with Microsoft and SAP