# Table of Contents

4  Introduction  
6  Network Filtering  
8  SAP GUI for Microsoft Windows  
9  Password Management  
9.1 Password Policy  
9.2 Password Hashes  
9.3 Users with ABAP Default Password  
10 Secure Network Communication  
11 Secure HTTP (HTTPS)  
11.1 Usage of HTTPS  
11.2 Protection of Cryptographic Keys  
11.3 Protection of Session Identifiers  
12 Limit Web-Enabled Content  
13 ABAP RFC Connectivity  
15 Gateway Security  
15.1 ABAP RFC  
15.2 Registered RFC Server Program  
15.3 Started RFC Server Program  
17 Message Server Security  
18 Security Patch Management for ABAP  
19 Security Configuration Monitoring  
20 Appendix  
21 Endnotes
Introduction

SAP helps our customers become best-run businesses by providing software solutions to optimize and innovate core businesses processes. The SAP NetWeaver® technology platform with the ABAP™ programming language is used to store and process business-critical data (such as financial, human resources, and customer relationship data). Therefore, it is crucial that customers secure their SAP® software platform. SAP software systems must fulfill compliance requirements and follow regulations such as the Sarbanes-Oxley Act. More generally, they must conform to data protection and privacy laws as well as comply with industry-specific regulations. Since SAP software systems run business-critical processes, protecting them from attacks is vital.

To protect systems based on ABAP against unauthorized access and manipulation, security configuration must be applied on different levels (landscape architecture, operating system, database, SAP technology, SAP applications, and SAP authorizations, for example). SAP and third parties provide comprehensive documentation on how ABAP systems can be secured, including SAP security guides, SAP security notes, SAP Community Network, and materials in many books. Additionally a document was released on how to protect Java- and ABAP-based SAP applications against common attacks. 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 the level of SAP technology. 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 (such as operating system security and database security), SAP authorization concepts (including segregation of duties on business and system operations levels), secure development, logging, and tracing.

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

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 (for example, primary component BC-CST-GW for SAP Note 140808141) in the SAP Notes tool.
<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 systems based on the SAP NetWeaver® Application Server component. 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 Microsoft Windows</td>
<td>Customers can increase the security of their client workstations using the latest SAP GUI for Microsoft Windows with security rules. It restricts SAP software systems in the ability to perform security-relevant operations on client workstations (execute commands, upload files, and so on).</td>
</tr>
<tr>
<td>Password Management</td>
<td>Default passwords, weak password policies, and old password hashes can lead to insecure systems and must be configured in a secure way.</td>
</tr>
<tr>
<td>Secure HTTP (HTTPS) and Secure Network Communication</td>
<td>Cryptographically secured network communication is recommended to mitigate risks of interception of communication containing business data and user credentials (passwords, SAP logon tickets, and so on). Protection of cryptographic keys is also 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>Remote Function Call (RFC) Connectivity with ABAP® Programming Language</td>
<td>Security of SAP software systems relies on separation of systems of different security classifications (such as development, test, and production). If interconnectivity between systems of different security classification is required, it should be done considering guidelines to ensure the security of systems with higher classification.</td>
</tr>
<tr>
<td>Gateway Security and Message Server Security</td>
<td>Secure configuration of gateways and message servers is required to mitigate the risk of unauthorized access to SAP software systems.</td>
</tr>
<tr>
<td>Security Patch Management for ABAP</td>
<td>Security notes must 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>
Secure network architecture is a fundamental requirement for secure ABAP systems. Network filtering must be used to reduce the attack surface (see Figure 1). Implementation of network filtering between end-user networks and ABAP systems\(^2\) is required and documented in the SAP NetWeaver Security Guide.\(^3\)

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.\(^4\) NN is used as a placeholder for the instance number of the SAP software system.

<table>
<thead>
<tr>
<th>Service</th>
<th>Required For</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatcher</td>
<td>The dispatcher is used by SAP(^a) GUI. The communication protocol used is DIAG.</td>
<td>32NN</td>
</tr>
<tr>
<td>Gateway</td>
<td>The gateway manages remote function call (RFC) communication.</td>
<td>33NN</td>
</tr>
<tr>
<td>Message Server</td>
<td>The 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>

RFC = Remote function call
DIAG = Dynamic information and action gateway

Figure 1: Attack Surface Reduction Through Network Filtering

With network filtering

SAP servers with database

Database
Operating system

End user

Firewall

RFC
DIAG

With network filtering

SAP servers with database

Database
Operating system

End user

Firewall

RFC
DIAG

Default attack surface: all services

Reduced attack surface: accessible services

RFC = Remote function call
DIAG = Dynamic information and action gateway
The network architecture depends on SAP infrastructure components (such as the SAP router, Web dispatcher, and load balancer), which must be taken into account for architecture planning (see Figure 2). These infrastructure components do not change the fact that access to DIAG, RFC, message server, and HTTPS is necessary, but they have impact on network filtering implementation.

This document assumes 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 must be taken to secure these services.

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 (SSH, RDP, database administration, and so on). Access to the administration network must be properly secured by common security concepts (for example, to allow administrative access to the ABAP systems only from dedicated subnets or admin workstations).

Figure 2: Example of SAP® Architecture with Network Filtering

RFC = Remote function call
DIAG = Dynamic information and action gateway

Corporate network

End-user network
Message server
RFC
DIAG
HTTPS

Firewall

SAP® software systems
Application server
Database

Firewall

SAP

Administrative network
Administrative protocols: SSH, RDP, database administration and so on

Other systems

Server
Database

RDF = Remote function call
DIAG = Dynamic information and action gateway
SAP GUI for Microsoft Windows

ABAP systems can access security-critical functionality on SAP GUI end-user workstations under the permission of the end user (such as uploading and downloading files, changing the Microsoft Windows registry, and executing 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, but end users must 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. This mitigates the risk of malicious attacks on SAP GUI workstations from ABAP systems that have been compromised.

We strongly recommend implementing the following security measures:
- Deploy the latest available SAP GUI version on all end-user workstations.
- Ensure that SAP GUI security rules are activated using at least the security rule setting “Customized” and default action “Ask.”
Password Management

SAP software systems must store password information in some representation like all systems using password-based logon. SAP software 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. 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. The following profile parameters are relevant to configure password policies.

- login/min_password_lng
- login/min_password_letters
- login/min_password_digits
- login/min_password_lowercase
- login/min_password_uppercase
- login/min_password_specials
- login/password_max_idle_productive
- login/password_max_idle_initial
- login/password_history_size
- login/password_expiration_time

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 by changing the table authorization group of these tables. Users that are not administrators 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 central user administration (CUA), you must ensure that the CUA system has at least the same or a higher release than all attached systems and that additional relevant SAP Notes are implemented.

<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>4.6–6.40</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 onward</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.

USERS WITH ABAP DEFAULT PASSWORD

Changing default passwords is crucial for secure system operation. The default users that are created in different clients in every ABAP system are SAP*, DDIC, EARLYWATCH, SAPCPIC, and TMSADM. Be sure to change the passwords of default users in all clients including client 066 and unused clients. The report RSUSR003 or the SAP EarlyWatch Alert services can be used to verify that default passwords have been changed.

Password change for the default user TMSADM must be done for all systems in an SAP transport management domain at the same time. A tool is provided to assist changing the TMSADM password in a transport landscape. Systems with releases older than 4.6C should lock the user TMSADM.
Secure Network Communication

The SAP proprietary protocols DIAG (used for SAP GUI) and RFC do not cryptographically authenticate client and server, nor do they encrypt network communication. Passwords transmitted over the network can be eavesdropped on. 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 (see Figure 3 for examples of recommended uses).

SNC without single sign-on capability is available to all SAP NetWeaver customers for SAP GUI using SNC client encryption and for all RFC communication between SAP servers. Basic single sign-on capabilities are available in environments where SAP servers and SAP GUI clients run Microsoft Windows. For comprehensive SNC capabilities and advanced management of credentials and single sign-on in Microsoft Windows and heterogeneous environments, we recommend using the SAP NetWeaver Single Sign-On application or a certified SNC partner product.

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.”
- For RFC communication, SNC should be implemented if the network traffic is susceptible to sniffing by end users.
- We recommend using strong cryptographic authentication and we recommend deactivating password-based access for most SAP GUI users. Delete formerly used password hashes of those users from the database. Only a small number of emergency accounts should be able to access the system with password login.

![Figure 3: Recommended Scenarios for Secure Network Communication (SNC)](image)

**Corporate network**

- **End-user network**
  - SAP® GUI (using DIAG)
  - Firewall
  - SNC recommended

- **Server network**
  - ABAP™
  - Firewall
  - SNC recommended

- **Other server network**
  - ABAP
  - Firewall
  - SNC recommended

**Corporate network**

- **End-user network**
  - SAP® GUI (using DIAG)
  - Firewall
  - SNC recommended

- **Server network**
  - ABAP™
  - Firewall
  - SNC recommended

- **Other server network**
  - ABAP
  - Firewall
  - SNC recommended

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

**Legend**

- DIAG = Dynamic information and action gateway
- SNC = Secure network communication
- DB = Database
Secure HTTP (HTTPS)

Besides 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 (for example, load balancers or reverse proxies) in the server network, or ABAP systems should be configured to directly support HTTPS/SSL servers. Information about SSL server configuration is provided in SAP Notes and the SAP help portal.\(^{62, 63, 64}\)

SSL server configuration requires cryptographic keys. Other cryptographic keys are used for creation of SAP logon tickets, SNC, or Web service security. These keys are stored in personal security environment (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.\(^{29}\) End users should not have access to this new table authorization group.

Restrict file system access to PSE files from ABAP programs.\(^{30}\)

**PROTECTION OF SESSION IDENTIFIERS**

Web applications use security session identifiers created after logon to authenticate subsequent access. The identifiers are destroyed after logoff. Session handling must be securely configured in order to prevent misuse of security session identifiers.\(^{1}\)

---

Figure 4: Recommended Scenarios for Secure HTTP (HTTPS)

---

DB = Database

Secure Configuration of SAP NetWeaver Application Server Using ABAP
Limit Web-Enabled Content

ABAP systems offer Web-enabled content that can be accessed using web browsers. This content is managed by the 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.

The following recommendations apply for the handling of Web-enabled content in the ICF:

- Only ICF services that are required for business scenarios should be enabled. Particularly on productive SAP software systems, not all ICF services should be enabled (see Figure 5).
- 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 onward.31
- 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.31
- Short term: We recommend deactivating at least the ICF services listed in the table below if they exist in your release and are not used in your business scenarios.

<table>
<thead>
<tr>
<th>ICF Service</th>
<th>SAP Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>/sap/bc/soap/rfc</td>
<td>SAP Note 1394100</td>
</tr>
<tr>
<td>/sap/bc/echo</td>
<td>SAP Note 626073</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</td>
</tr>
<tr>
<td>/sap/bc/bsp/sap/certreq</td>
<td>SAP Note 1417568</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</td>
</tr>
<tr>
<td>/sap/bc/bsp/sap/icf</td>
<td></td>
</tr>
<tr>
<td>/sap/bc/IDoc_XML</td>
<td>SAP Note 1487606</td>
</tr>
<tr>
<td>/sap/bc/srt/IDoc</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: Attack Surface Reduction by Limiting ICF Services

![Figure 5: Attack Surface Reduction by Limiting ICF Services](image-url)

Default attack surface: all ICF services active

Reduced attack surface: limited ICF services active
ABAP RFC Connectivity

RFC is an SAP proprietary protocol. It is the main integration technology between SAP software systems and is also heavily used in integrations with non-SAP software 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 (such as 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 (that is, from a production system to another production system). They are also allowed from systems of higher security classification to systems of lower security classification (such as from a test 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 (for example, 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 (see Figure 6). One exception to this general guideline is transport management system (TMS) destinations. If these destinations are required, they must be considered security risks and must only be used after thorough risk analysis.

Figure 6: Remote Function Call (RFC) Connectivity for SAP NetWeaver® Application Server

---

OK: RFC destinations from systems of higher security classifications to lower or same security classification

CHECK: RFC destinations category 2 and 3 are a security risk and must only be used after thorough risk analysis.
Additionally, systems of higher security classification should be generally forbidden 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.

Access to trusting systems is further controlled by the authorization object S_RFCACL. This object must be strictly controlled, and full wildcard authorizations should not be granted. Also, the default configuration to leave the authorization object out of the authorization profile SAP_ALL should not be changed (ADD_S_RFCACL=NO in customizing table PRGN_CUST).

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. We recommend using dedicated accounts per scenario wherever possible. 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.”

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

- Ensure that RFC authority checks are enabled by setting profile parameter auth/rfc_authority_check.
- 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 (development to test, 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. 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.” Within its SAP Solution Manager 7.1 application management solution, SAP implemented diagnostics functionality (configuration validation reporting) to ease this activity for managed SAP software systems.
Gateway Security

The gateway is the technical component of the application server that manages the communication for all RFC-based functionality. RFC communication can be categorized in three different scenarios, as shown in Figure 7.

**ABAP RFC**

The most frequently used RFC functionality in customer installations is provided by ABAP remote-enabled function modules. For instance, technologies like the BAPI® programming interface, 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 (authorization object S_RFC). The gateway does not perform additional security checks.

**REGISTERED RFC SERVER PROGRAM**

The second-most used RFC functionality is the so-called registered RFC server program. These use the RFC library and integrate ABAP systems with non-ABAP systems that provide RFC functions. The external RFC server programs register at the gateway and can later be accessed by RFC clients via the same 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 engine 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 gateway access control lists (secinfo for releases up to 4.6 and reginfo in higher releases).

**STARTED RFC SERVER PROGRAM**

Finally, there are so-called started RFC server programs. They are also built with the RFC library, but instead of registering at the gateway, they reside on the host of the application server. The 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 that explicitly point to the local gateway or are just 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 gateway access control lists (secinfo for all releases).
For system security, it is of utmost importance that the 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,\textsuperscript{41, 42} and minimum SAP kernel patch levels and configuration switches must be implemented.\textsuperscript{43, 44} SAP provides a tool to create gateway ACLs that cover typical usage scenarios for registered and started RFC server programs.\textsuperscript{45}

Gateway logging should be activated in order to support ongoing maintenance and provide monitoring.\textsuperscript{46} Additionally, gateway monitoring should only allow local access ($\text{gw/monitor} = 1$).\textsuperscript{47} This is the default configuration setting since release 6.40.

The following security measures should be taken to protect the gateway:
- Verify the minimum kernel patch levels\textsuperscript{43}
- Set profile parameters $\text{gw/sec\_info}$, $\text{gw/reg\_info}$ and $\text{gw/reg\_no\_conn\_info}$
- Create secinfo and reginfo ACL files manually\textsuperscript{41} or with the tool\textsuperscript{45}
- Reload ACL files dynamically on each application server to activate changes
- If necessary, missing configurations can be identified by:
  - Activation of gateway logging and log file review
  - Analysis of the error messages shown on the RFC client
## Message Server Security

The message server is a system component that provides two services. On the one hand, it manages communication between the application servers of one SAP software 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. We therefore strongly recommend implementing the following security measures to mitigate the risks of unauthorized message-server access.\(^{48,49}\)

In addition to the access restrictions for the message server, we recommend restricting the access to remote message server monitoring \((\text{ms/monitor} = 0)\).\(^{50}\)

### Releases

<table>
<thead>
<tr>
<th>Releases</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 4.5</td>
<td>The message server port ((\text{rdisp/mshost}, \text{rdisp/msserv})) should be firewalled. Only network segments with SAP(^{\circ}) servers should be granted access to this port. Client networks should be blocked from accessing the 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 message server services should be separated in two ports.(^{46}) One port is used for SAP GUI client access ((\text{rdisp/msserv})), and the other is used for access to internal server communication ((\text{rdisp/msserv_internal})). Internal system communication ((\text{rdisp/msserv_internal})) must be firewalled. Only network segments with SAP servers should be granted access to internal server communication. Additional information is provided in the SAP NetWeaver(^{\circ}) Security Guide.(^{49})</td>
</tr>
<tr>
<td>6.40 onward</td>
<td>As an alternative to the firewall approach for the internal system communication as recommended for release 4.6, security can be applied on the message server service itself. A message server access control list (ACL) can be activated that lists all relevant network interfaces (including failover interfaces) of all application servers ((\text{ms/acl_info})).</td>
</tr>
</tbody>
</table>
As with all software and despite thorough testing, SAP software 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 security notes. A comprehensive list of all released SAP security notes is available on the SAP Service Marketplace extranet.

To ensure that SAP security notes are installed on SAP software systems, the following security measures are recommended:

- Implement comprehensive security patch management using SAP Solution Manager system recommendations. It allows you to manage all missing security notes for SAP systems that are registered in SAP Solution Manager. It takes the current software configuration, according to installed software components, release, and service pack level, and the implemented notes into account to calculate recommendations. It supports the complete change process.

- In addition, regularly review the released SAP security notes on the SAP Service Marketplace to identify those notes that are not covered by SAP Solution Manager system recommendations. Usually these are notes for system components that are actually not registered in the SAP Solution Manager.

- Alternatively, as a minimum, check the SAP EarlyWatch Alert report and its corresponding report RSECNOTE at least monthly, which allows you to check whether selected critical SAP security notes are implemented. Due to technical restrictions, the report can only check for SAP Notes with ABAP correction instructions or that refer to SAP kernel patches.

Security Patch Management for ABAP
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:

- The SAP EarlyWatch Alert services 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 this service, SAP also provides selected checks on security-relevant configuration (such as the aforementioned implementation status of relevant SAP security notes with correction instructions).

- The SAP Security Optimization service is designed to check the security of your SAP software 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 predefined security topics.

- The computing center management system (CCMS) is a general framework to monitor an ABAP system and issue alerts on events. CCMS can be customized to monitor security-critical settings and alert you in case of changes.

- Diagnostics configuration validation reporting through the SAP Solution Manager delivers a generic framework to verify configurations of connected managed SAP software 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 software systems.

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 issue alerts in case of deviations
Appendix

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 on SAP Service Marketplace, the SAP help portal, and the SAP Developer Network site.

**SAP Service Marketplace**
- Run SAP Methodology ([https://service.sap.com/runsap](https://service.sap.com/runsap))

**SAP Help Portal**
SAP Library, including the online version of the *SAP NetWeaver Security Guide* ([http://help.sap.com](http://help.sap.com))

**SAP Developer Network**
Endnotes

1. Protecting Java- and ABAP-Based SAP Applications Against Common Attacks
   http://service.sap.com/~form/sapnet?_SHORTKEY =01100035870000073716&_SCENARIO =01100035870000000208&_OBJECT=011000358700001376952010E
2. Architecture of the SAP NetWeaver Application Server
   http://help.sap.com/saphelp_nw70/helpdata/en/fe/a7b5386f64b555e100000009b38f8cf/frameset.htm
4. TCP/IP Ports Used by SAP Applications
   http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/4e515a43-0e01-0010-2da1-9bce452c280b
5. SAP Note 1483525 – New security center in SAP GUI for Windows 7.20
   https://service.sap.com/sap/support/notes/1483525
6. SAP Note 147519 – Maintenance strategy/deadlines for SAP GUI
   https://service.sap.com/sap/support/notes/147519
7. SAP GUI for Windows 7.20 Security Guide
   http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/002444be-7018-2d10-e18e-a8c537198ef6
8. SAP Note 1237762 – ABAP systems: Protection against password hash attacks
   https://service.sap.com/sap/support/notes/1237762
9. SAP NetWeaver Application Server ABAP Security Guide, Profile Parameters for Logon and Password (Login Parameters)
   http://help.sap.com/saphelp nw70/helpdata/en/22/41c43ac23c3f2te10000000a114084/frameset.htm
10. SAP Note 1484692 – Protect read access to password hash value tables
    https://service.sap.com/sap/support/notes/1484692
11. SAP Note 1300104 – CUA: New password hash procedures: Background information
    https://service.sap.com/sap/support/notes/1300104
12. SAP Note 1306019 – CUA: Downward-compatible passwords in old child systems
    https://service.sap.com/sap/support/notes/1306019
13. SAP Note 1022812 – CUA: Initial passwords not possible for child systems
    https://service.sap.com/sap/support/notes/1022812
14. SAP Note 1458262 – ABAP: recommended settings for password hash algorithms
    https://service.sap.com/sap/support/notes/1458262
15. SAP NetWeaver Application Server ABAP Security Guide, Section Protecting Standard Users
    http://help.sap.com/saphelp nw70/helpdata/en/3e/cdaccbedc411d3a6510000e835363f/frameset.htm
16. SAP Note 40689 – New reports for the User Information System
    https://service.sap.com/sap/support/notes/40689
17. SAP Note 1488159 – SUIM RSUSR003 incorrect results for CODVN = ‘F’
    https://service.sap.com/sap/support/notes/1488159
18. SAP Note 1488406 – Handling the generated user TMSADM logon
    https://service.sap.com/sap/support/notes/1488406
19. SAP Note 761637 – Logon restrictions prevent TMSADM logon
    https://service.sap.com/sap/support/notes/761637
20. SAP Note 1552894 – RSUSR003: Checking the standard password for user TMSADM
    https://service.sap.com/sap/support/notes/1552894
21. SAP Note 1414256 – Changing TMSADM password is too complex
    https://service.sap.com/sap/support/notes/1414256
22. SAP Note 1515926 – Update #1 to Security Note 1414256
    https://service.sap.com/sap/support/notes/1515926
23. SAP Note 1486759 – Blocking unauthorized access to system using TMSADM to 4.6B
    https://service.sap.com/sap/support/notes/1486759
24. SAP Note 1643878 – Release Notes for SNC Client Encryption
    https://service.sap.com/sap/support/notes/1643878
    https://service.sap.com/~sapdownload/011000358700001270931999E/SNCHBEN.PDF
26. SAP Note 352295 – Microsoft Windows Single Sign-On options
    https://service.sap.com/sap/support/notes/352295
27. Unleash the Power of Single Sign-On with Microsoft and SAP
    http://download.microsoft.com/download/c/6/c/c6c42b9f-66f4-47b3-99be-8e5afa1ddc9a/SSO%20with%20MS%20and%20SAP.pdf
28. SAP NetWeaver Single Sign-On
29. SAP Note 1485029 – Protect read access to key tables
    https://service.sap.com/sap/support/notes/1485029
30. SAP Note 1497104 – Protect access to PSE files by additional AUTHORITY-CHECK  
https://service.sap.com/sap/support/notes/1497104
31. SAP Note 1498575 – Mass Maintenance of ICF Services  
https://service.sap.com/sap/support/notes/1498575
32. SAP Note 1394100 – Security note: Access to RFC-enabled modules via SOAP  
https://service.sap.com/sap/support/notes/1394100
33. SAP Note 626073 – Unreleased Internet Communication Framework services  
https://service.sap.com/sap/support/notes/626073
34. SAP Note 865853 – WebReporting/WebRFC obsolete as of NW2004s  
https://service.sap.com/sap/support/notes/865853
35. SAP Note 1417568 – Unauthorized change of contents in CERTREQ and CERTMAP  
https://service.sap.com/sap/support/notes/1417568
36. SAP Note 1422273 – Unauthorized modification of displayed content in BSP  
https://service.sap.com/sap/support/notes/1422273
37. SAP Note 1487606 – Security note: IDoc inbound processing via HTTP/SOAP  
https://service.sap.com/sap/support/notes/1487606
38. SAP Library, Trusted/Trusting Relationships Between SAP Systems  
39. SAP Note 93254 – RFC short dump RFC_NO_AUTHORITY  
https://service.sap.com/sap/support/notes/93254
40. SAP Solution Manager – SAP Technical Operations – Section “RFC Hopping”  
41. SAP Note 1408081 – Basic settings for reg_info and sec_info  
https://service.sap.com/sap/support/notes/1408081
42. SAP Library, Security Settings in the SAP Gateway  
http://help.sap.com/saphelp_nw70/helpdata/en/bb/9f135a4b9b1d189750000e8322d00/frameset.htm
43. SAP Note 1298433 – Bypassing security in reginfo & secinfo  
https://service.sap.com/sap/support/notes/1298433
44. SAP Note 1444282 – gw/reg_no_conn_info settings  
https://service.sap.com/sap/support/notes/1444282
45. SAP Note 1425765 – Generation of sec_info reg_info proxy_info  
https://service.sap.com/sap/support/notes/1425765
46. SAP Note 910919 – Setting up Gateway logging  
https://service.sap.com/sap/support/notes/910919
47. SAP Note 64016 – Using the SAP Gateway monitor GWMON  
https://service.sap.com/sap/support/notes/64016
48. SAP Note 1421005 – Secure configuration of the message server  
https://service.sap.com/sap/support/notes/1421005
49. SAP NetWeaver Application Server ABAP Security Guide, Security Settings for the SAP Message Server  
http://help.sap.com/saphelp_nw70/helpdata/en/4e/cffdb69d10424e97eb1d993b1e2cfd/frameset.htm
50. SAP Note 821875 – Security settings in the message server  
https://service.sap.com/sap/support/notes/821875
51. SAP Note 888889 – Automatic checks for security notes using RSENCOTE  
https://service.sap.com/sap/support/notes/888889
52. SAP Service Marketplace – SAP Security Notes  
https://service.sap.com/securitynotes
53. SAP Service Marketplace, SAP Solution Manager – System Recommendations  
https://service.sap.com/SysRec
54. SAP Library, SAP Solution Manager – System Recommendations  
https://service.sap.com/saphelp_sm71_sp01/helpdata/EN/83/68fad4952d42a192469fa02586aeff/frameset.htm
55. SAP Note 863362 – Security checks in the SAP EarlyWatch Alert  
https://service.sap.com/sap/support/notes/863362
56. SAP Service Marketplace – SAP EarlyWatch Alert and SAP EarlyWatch Alert for Solutions  
https://service.sap.com/ewa
57. SAP Service Marketplace – SAP Security Optimization Service  
https://service.sap.com/sos
58. Monitoring in the CCMS  
http://help.sap.com/saphelp_nw70/helpdata/en/49/6272376d3bfa2be10000009b38f8cf/frameset.htm
59. SAP Service Marketplace – End-to-End Change Control Management  
https://service.sap.com/changecontrol
60. SAP Solution Manager – SAP Technical Operations – Configuration Validation
   http://wiki.sdn.sap.com/wiki/display/TechOps/ConfVal_Home

61. SAP Note 1560878 - White list for SOAP Processor & IDoc SOAP Application

62. SAP Note 510007 - Setting up SSL on Web Application Server ABAP

63. How to Configure SSL for SAP NetWeaver Mobile 7.1 (For pure SSL configuration, skip step 4.4 and 4.5)
   http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f0ea4e25-6ecf-2c10-c4a8-a3742844915d

64. Configuring SAP Web AS for Supporting SSL
   http://help.sap.com/saphelp_nw70/helpdata/en/65/6a563c6f658a06e04d05a000000a1a405a00000/frameset.htm