SAP Solutions

Security Recommendations: A Practical Guide for Securing SAP® Solutions

Table of Contents

The Best-Run Businesses Run SAP®

Prioritizing Security

Information security is a top priority for your business. With cyberattackers becoming more sophisticated and relentless in their approach, we at SAP are committed to continuously innovating our software to help ensure that your information is always safe – both on premise and in the cloud. We prioritize security so that you can stay focused on running your business and managing your customer relationships effectively using SAP® solutions, safe in the knowledge that your data is fully protected.

WHY SAP SOFTWARE MUST BE SECURED

SAP software stores and processes a wide range of sensitive and valuable information, such as personal data, prices, and product procedures. To protect this data and to help ensure that this information is not intercepted or falsified, we recommend that you follow our security requirements. This guide provides an overview of the measures and methods you should implement to correctly and securely operate, maintain, and configure your SAP solutions.

ABOUT OUR SECURITY RECOMMENDATIONS

Figure 1 shows the secure operations map that forms the basis for the structure of our security recommendations. It consists of 16 security-relevant topics for our software systems across five areas:

- Security compliance
- Secure operation
- Secure setup
- Secure code
- Infrastructure security

Figure 1: The Secure Operations Map

Security compliance	Security governance	Audit	Cloud security	Emergency concept
Secure operation	Users and authorizations	Authentication and single sign-on	Support security	Security review and monitoring
Secure setup	Secure configuration	Communication security	Data security	
Secure code	Security maintenance of SAP® software code	Custom code security		
Infrastructure security	Network security	Operating system and database security	Front-end security	

Not all of these 16 topics are regarded as equally important. That is why some individual topics are not covered or are summarized together with others in this document.

Common Security Issues

The most common issues you are likely to encounter when implementing our security recommendations are:

- Lack of an established patch process
- Unencrypted communication between your SAP solutions
- Inadequately secured interfaces
- No established data backup process and no emergency processes in place
- Missing or incorrect security configuration of the system

INFRASTRUCTURE SECURITY

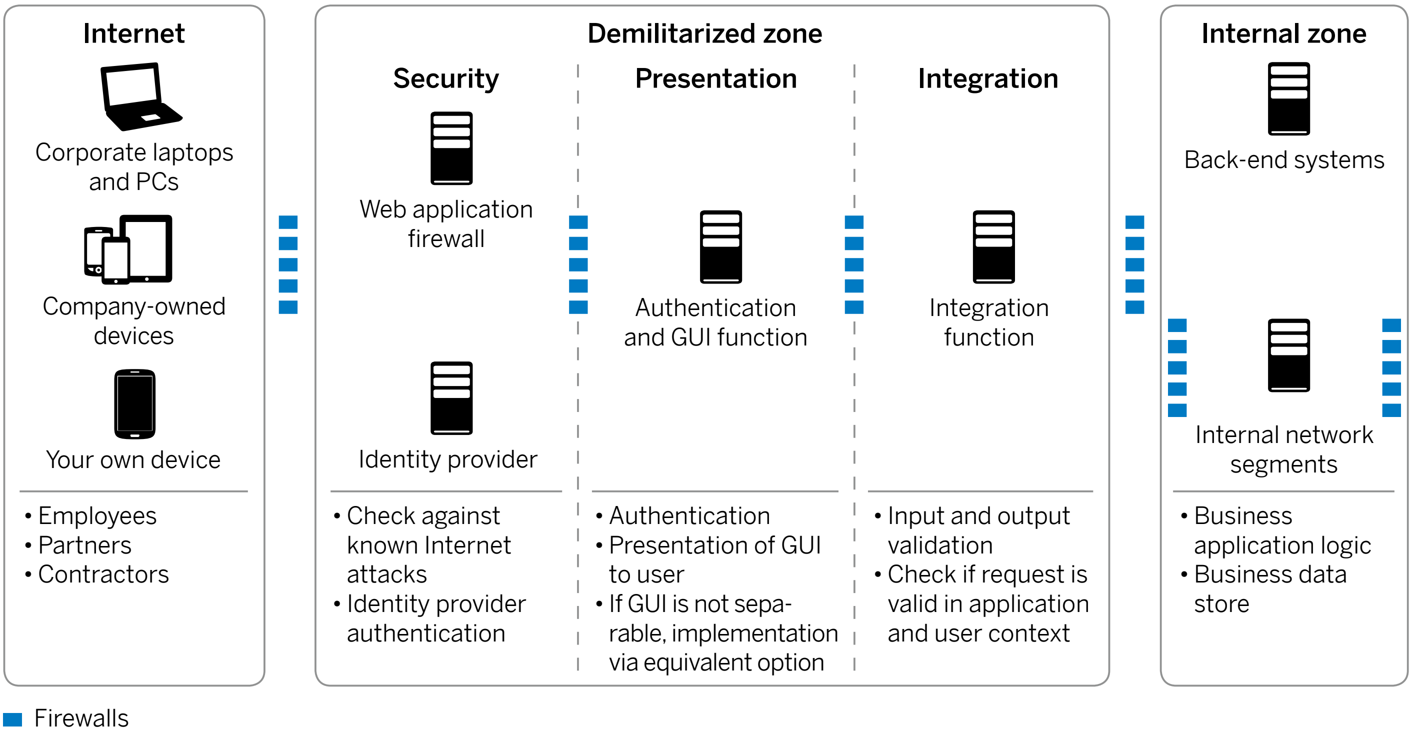
You should begin by securing your network, database, and front-end settings. These are the most critical components to protect when you begin implementing security measures across your systems.

Network Security

Network security includes the administration of network topology, isolation of the network, restriction of network services and protocols, and the development of a domain concept. Your network security should comply with our security requirements. To do this, you may need to develop processes and configure your system settings.

Given the ever-increasing number of mobile devices and the Internet accessibility that they enable, we recommend setting up a network infrastructure comparable to the scheme outlined in Figure 2.

Figure 2: Recommended Network Infrastructure Settings


Internet
Corporate laptops and PCs
Company-owned devices
Your own device
• Employees
• Partners
• Contractors
Demilitarized zone
Security
Web application firewall
Identity provider
• Check against known Internet attacks
• Identity provider authentication
Presentation
Authentication and GUI function
• Authentication
• Presentation of GUI to user
• If GUI is not separable, implementation via equivalent option
Integration
Integration function
• Input and output validation
• Check if request is valid in application and user context
Internal zone
Back-end systems
Internal network segments
• Business application logic
• Business data store
🟦 Firewalls

The internal network segments within the internal zone require very different levels of authorization, reflecting the different levels of access security between administration networks, server networks, and office networks. More details can be found in our white paper titled "Secure Configuration of SAP NetWeaver® Application Server Using ABAP®."

You must set up your back-end systems and in-house network segments separately from the upstream demilitarized zone (DMZ) and the Internet in the "internal zone." You should also set up firewalls in all of the following locations:

- Within the internal zone
- Between the three layers of the DMZ: security, presentation, and integration
- Between the Internet, DMZ, and the internal zone

Only essential connections should be able to pass through these firewalls. You should block attempts to access databases and the SAP HANA® studio. In exceptional circumstances, you may access the SAP HANA database using a terminal server. In addition, you should authenticate and verify all access through the Internet within the DMZ before it is forwarded to internal parts of the network by using Web application firewalls and authentication of identity providers. Configure the firewalls between the network segments accordingly. You should also restrict administrator access and ensure it is only facilitated using authenticated and encrypted connections. In general, we recommend encrypting internal communications using a Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Network Communication (SNC).

Database Security

You should implement our database security requirements across all of your SAP solutions and in accordance with your system provider's recommendations. This includes updating and testing your software, performing antivirus scans, and checking the integrity of critical system files and configurations.

In general, you should be able to track all administrator access to the operating system. Use only personalized accounts. When switching to administrative accounts, you should do so transparently by logging the activities performed. By restricting use of the database, proprietary database applications, and database-specific functions, as well as managing authorization controls, you can help ensure optimum database security. This includes:

- Ensuring that data in the database can be accessed using only SAP tools or by implementing special security measures
- Setting up encryption for authentication and communication at the level of the database drivers or by means of suitable mechanisms at operating-system or application level
- Installing separately secured network segments for database and application servers
- Establishing dedicated security mechanisms that depend on the specifics of the different databases and database providers, such as SAP HANA, or the SAP MaxDB® database

Front-End Security

The security settings on the front end must be made for client workstations as well as for mobile devices. Because of the ever-increasing use of personal mobile devices, it is important to clearly define a security strategy that differentiates between company-owned devices and personal mobile devices. Bring your own device, or BYOD, is becoming increasingly important for your company.

Front-end security for mobile devices should include:

- Security settings for company-owned mobile devices
- The definition of a process for secure software distribution, management, and configuration of these end points
- Implementation of secure communication between end points and back-end systems
- Encryption of company data on the devices
- Rules for password complexity on mobile devices equivalent to those for workplace computers
- The option to centrally delete sensitive data on mobile devices using mobile device management solutions

SECURE CODE

Once you have successfully implemented security measures across your network, databases, and front end, you should begin the ongoing process of ensuring that your code is always fully secure and up to date.

Code in SAP Software

Our solutions must be checked and updated at regular intervals. We recommend installing the latest support package regularly, at least once a year.

On the second Tuesday of every month, we publish the latest security corrections and security recommendations as security notes in the context of the “SAP Security Patch Day,” which you should take care to assess and implement in a timely manner. Not only should you implement the actual program correction or replace the respective code, but you should also activate or implement the configuration recommendations provided with our security notes. We recommend establishing a dedicated process for implementing these updates.

In addition, we recommend securely setting up, and continuously maintaining, parts of your custom-defined SAP solution landscape by using SAP Solution Manager and the “system recommendations” and “configuration validation” functions.

You should begin by securing your network, database, and front-end settings. These are the most critical components to protect when you begin implementing security measures across your systems.

Custom Code

You must ensure that custom code is secure during the entire code development process by defining a custom code lifecycle management process. This process should do the following:

- Ensure that software developers receive ongoing training in secure programming, current vulnerabilities and ways they can be avoided, and software development security
- Define, sign off on, and implement guidelines for secure programming
- Introduce a staged development and release process in software development with fixed, defined acceptance milestones
- Avoid or replace custom code that is not being used or can be replaced with our standard code
- Use security source-code scan tools regularly to identify the most common vulnerabilities in the source code, such as the SAP NetWeaver Application Server component, add-on for code vulnerability analysis, for the ABAP programming language, and the SAP Fortify software by HPE for many other programming languages and for static application security testing of custom-built code based on SAP HANA as well as on SAP Cloud Platform
- Ensure that developers analyze and assess the in-house developments in their systems in accordance with data protection regulations and compliance guidelines and under aspects of malicious code avoidance

To achieve this, we recommend installing custom code lifecycle management functionality from SAP Solution Manager.

SECURE SETUP

Encryption is crucial when it comes to securely configuring our solutions.

Securing Your Configuration

Our recommended security settings enable you to configure your system securely. You can find our guidelines outlined in our security baseline template and in our white papers that focus on secure configuration.

The definition of general security policies and measures for improving password security marks another important pillar of secure configuration. This includes activating certain parameters for password security and setting profile parameters to define minimum requirements for passwords. The same rules apply to authentication and encryption. It is worth mentioning that physically stored data, also known as “data at rest,” can also be secured – through the encryption of hard disks, for example.

In addition, our virus-scan interface secures file uploads. You can use this interface to check files that are uploaded to the SAP software from an external location for viruses and malware. The SAP E-Recruiting application is a good example of software in which this might occur, as it allows you to upload applicant files using the Internet. This is done by rerouting such files through an externally connected third-party virus scanner before loading them into the SAP software system.

Securing Interfaces

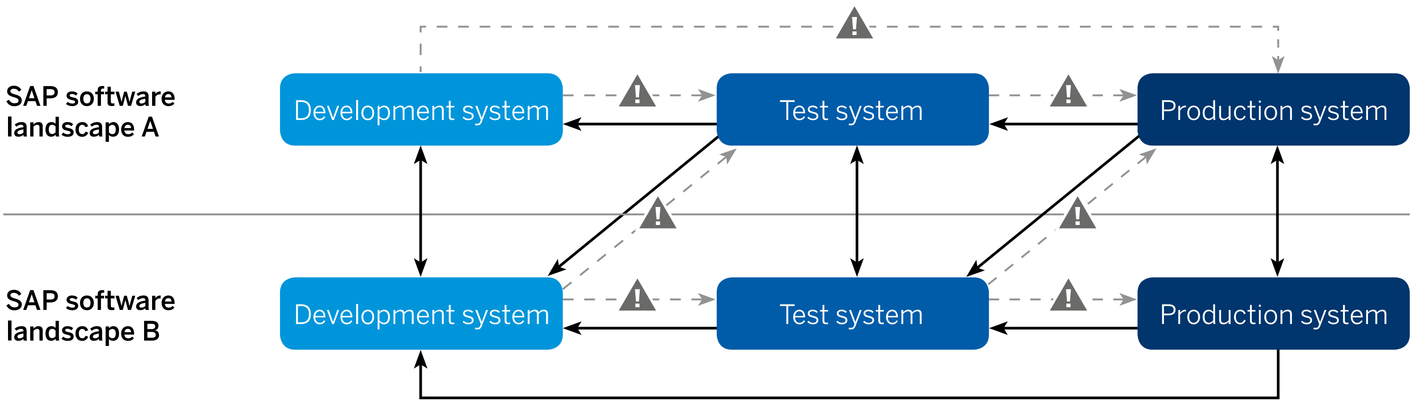
Every piece of information that is classified as confidential, such as passwords, must be transferred in encrypted form. This takes place using the most updated technology.

All connections must be defined, documented, and, if they are no longer used, removed. In general, connections are allowed between systems of the same security classification, and from systems with a higher security classification to systems with a lower security classification. Connections from systems with a lower security classification to systems with a higher security classification are allowed only for storing configuration about technical connections.

In-House Development and Test Landscapes

When it comes to internal development and test landscapes, the same rules apply as for production systems. Connections from systems with a higher security classification to systems with a lower security classification are allowed, for example, from a test system to a development system. (See Figure 3)

Figure 3: Connections Between Systems of Higher and Lower Security Classifications



→ **OK:** Remote function call (RFC) destinations between systems of same security classification

⚠ → **CHECK:** RFC destinations from a system with a low security classification to a system with a high security classification (trust relationship and stored credentials)
RFC destinations from a system with a high security classification to a system with a low security classification (callback)

Inspecting your security performance and planning for the unexpected are crucial to the overall success of the security measures you install.

SECURE OPERATION

Best practices for secure operation include carefully monitoring user access and authorization as well as logging any attempts to violate security.

User and Authorization Management

The main prerequisite for secure user and authorization management is defining, implementing, and monitoring an authorization process. In particular, you must monitor and document the assignment of critical authorizations. Best practices include:

- Enabling the user administrator to create, change, and delete users; reset and unblock passwords; and assign roles and profiles
- Avoiding creating users with extensive rights
- Granting administrators the rights required only for their respective area of work, and avoiding granting authorizations that are not explicitly required
- Ensuring that, immediately after installation of standard user profiles, all initial passwords are changed
- Establishing that standard user profiles are not being used for remote function call, or RFC, connections and background jobs

Security Incident Monitoring and Using Audit Logs

In addition to the secure setup of these systems, secure operation includes continuous monitoring to detect break-in attempts, violations of requirements, or security policies. This allows you to initiate corrective measures. For effective and analyzable logging, always activate and properly configure native logging mechanisms.

You should restrict access to the log files and logging settings. You can also secure log files by storing them on other systems, ensuring that you analyze them regularly using the applicable tools. Further active security measures should be scheduled and performed frequently in the form of white box analyses (security system assessments), black box analyses (penetration tests), or technical scanning for security vulnerabilities (vulnerability scanning). We recommend using the following tools for security monitoring and reporting:

- The SAP EarlyWatch® Alert service, which monitors the essential administrative areas of SAP components and keeps you up to date on performance and stability
- The SAP Security Optimization service, which is designed to verify and improve the security of SAP solutions by identifying potential security issues and providing key recommendations

SECURITY COMPLIANCE

Inspecting your security performance and planning for the unexpected are crucial to the overall success of the security measures you install.

Security Auditing

You should check and assess the security of your system by regularly conducting in-house and external audits. Audits generally serve these purposes:

- Detecting irregularities and attacks so that you can respond appropriately
- Deciphering what happened after the fact, in the sense of forensic analysis

In general, you should be able to track all administrator access to the operating system.

Ideally, you should integrate these measures into a corporate audit plan, which you should create in line with risk management strategies and update at least once a year. When planning specific audit objectives, you should consider the company's risk-management, regulatory, and statutory requirements. Audit execution requires the inclusion of various pieces of technical information. Depending on their technical specifications, our solutions offer various options for monitoring and recording security-related events.

Emergency and Backup Processes

You must prepare your emergency and data-backup process in such a way that you can deploy it immediately in an emergency. It should address the following emergency scenarios:

- Failure of an individual server
- Failure of an individual database
- Compromise of an SAP solution
- Failure of the transport system (ABAP) or the software distribution (Java)
- Outage of network connections
- Outage of an entire data center

When planning your emergency procedure, you must be careful to:

- Define the processes and people responsible
- Conduct regular emergency drills and adjust the processes accordingly
- Create and modify emergency users
- Collect required logs and data
- Define the rules and triggers for identification and classification of incidents
- Define "incident response" processes – that is, the occurrence of a vulnerability in the respective system environment – including the implementation of corrections and recovery measures
- Prepare technical and nontechnical (for example, legal) follow-on activities and improvements

A material aspect of emergency planning is the data backup of the SAP software systems. Clear responsibilities and process flows for end-to-end data backup and recovery must be defined in a data backup strategy. When creating this strategy, consider the following:

- Time of backup of components and data
- Authorizations required for this purpose
- Authorizations required for data recovery
- Access authorizations for archived backup data
- Physical storage of backup data, which should be separated from production data

When conducting your risk assessment, remember to also check whether the availability requirements for individual application areas, business processes, or organizational areas are high enough to warrant making a backup system available.

Every piece of information that is classified as confidential, such as passwords, must be transferred in encrypted form. This takes place using the most updated technology.

Keeping on Top of Your Security

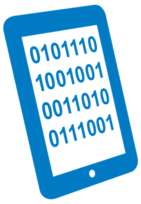
Once you have followed these steps, you can feel confident that your security is functioning at optimum levels. There are additional measures you can take too. We're here to help you take those extra measures and get peace of mind. Our resources and tools are available to answer your questions, offer expert advice, and provide support. A good starting point would be to familiarize yourself with the various white papers that we've published on security and compare these to actual situations that you are encountering in your own company. It's also a good idea to refer to our security guides and security baseline template for further information and support. And take advantage of our tools, which include SAP EarlyWatch Alert, SAP Security Optimization, our system recommendations, and our configuration validation. These tools are available to you as part of your maintenance contract, although additional charges may apply. From here, you'll be in a strong position to devise your own company action plan and create a security road map. We also recommend making use of existing **external offers**, which include the guides, working groups, and special interest groups developed by our regional user groups. Finally, we invite you to **actively raise open security questions** with us by sending us a message any time. After all, your security is our priority.

ADDITIONAL INFORMATION
Further details are available at the following locations (some of these resources require user/password authentication):

- SAP Security Optimization Services Media Library
- Security Baseline Template
- Secure Operations Map
- Security White Papers
- SAP Security Optimization
- Security guides for SAP Solutions
- SAP HANA Security Checklists and Recommendations
- SAP EarlyWatch Alert
- Recommendations for SAP solutions

Our Compliance and Security Solutions
For more information on the solutions that we offer in the area of compliance and security, please refer to the following sources:

- Security Software
- Governance, Risk, and Compliance Management



Once you have followed these steps, you can feel confident that your security is functioning at optimum levels.

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.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

The Best-Run Businesses Run SAP®