LAYER SEVEN SECURITY

SECURING THE JOURNEY TO SAP S/4HANA®

A SECURITY FRAMEWORK FOR S/4HANA MIGRATIONS

WHITE PAPER

Layer Seven Security offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Layer Seven Security makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

SECURING THE JOURNEY TO SAP S/4HANA

A SECURITY FRAMEWORK FOR S/4HANA MIGRATIONS

CONTENTS

INTRODUCTION

SAP Business Suite 4 SAP HANA (S/4HANA) is the successor to SAP Enterprise Resource Planning (ERP), optimized for the in-memory database SAP HANA and providing an enhanced user experience based on the SAP Fiori interface. S/4HANA is the core of SAP's strategy for digital transformation to support high volume and real-time information processing and analytics.

Mainstream maintenance for SAP ERP is scheduled to end in December 2027. Extended maintenance will be offered by SAP at a premium for a limited period after the end of mainstream maintenance. Support for ERP will terminate in 2030. Therefore, SAP customers must migrate to S/4HANA before 2028 if they do not wish to pay for extended maintenance, or 2030 for continued support from SAP.

29% of SAP customers had migrated to S/4HANA by 2022. 19% were in process of migrating. 10% were in pilot phase. 26% were evaluating the business case. 16% had yet to plan for the migration. Overall, more than two thirds of organizations had not fully migrated to S/4HANA as of 2022. [1]

52% of organizations migrating to S/4HANA select a greenfield strategy that involves removing and replacing legacy ERP systems, as opposed to a brownfield approach that maintains customizations while upgrading to S/4HANA.[2]

68% of organizations are deciding to host S/4HANA on the cloud. This includes both public and private cloud infrastructure.[2]

For most organizations, migrating to S/4HANA is a complex and drawn-out process,requiring extensive planning, funding and resourcing. 81% of digital transformation projects experience delays and failures, costing organizations an average of $4.12 million.[3] Security concerns are the most significant roadblock to successful migrations. The path to S/4HANA involves redesigning security models to address significant differences between the system architectures of ERP and S/4HANA. Authentication and authorization models differ significantly between the solutions. There are also significant differences in data structures, communication protocols, cross-system interfaces, and other areas.

The security challenges are intensified by concerns related to deploying SAP in the cloud and the need to secure customizations implemented through custom code migrated from ERP to S/4HANA. The concerns are justified. Insecure SAP applications in cloud environments can be discovered and compromised in less than three hours.[4] SAP customers have an average of 2500 vulnerabilities within their custom programs and two-thirds of organizations do not perform automated vulnerability scanning for custom SAP code.[5]

[1] SAP S/4 Migration, SAPinsider, May 2022

[2] The Journey to SAP S/4HANA, PwC, 2019

[3] Digital Transformation Projects, Couchbase, 2022

[4] Active Cyberattacks on Business-Critical SAP Applications, Onapsis, 2021

[5] SAP Security Survey Report, Turnkey Consulting, 2021

S/4HANA SECURITY FRAMEWORK

This whitepaper presents a comprehensive framework for securely migrating from SAP ERP to S/4HANA. The recommendations are aligned, but are not limited to, SAP requirements in the Security Guide for SAP S/4HANA.[6]

The detailed recommendations in this guide will enable SAP customers to protect S/4HANA installations in the cloud and on-premise, and secure custom ABAP and Fiori developments migrated from ERP systems or deployed directly in S/4HANA. The implementation of the recommendations in the guide will also prevent misconfigurations in the ABAP and HANA constituents of S/4HANA and control access to critical administrative and functional areas.

The whitepaper includes recommendations for automating pre and post go-live security checks for S/4HANA using SAP Solution Manager. SAP recommends the installation of Solution Manager in S/4HANA landscapes. Solution Manager provides diagnostic and monitoring applications that support vulnerability management, patch management, and system monitoring for securing S/4HANA.

USER ADMINISTRATION AND AUTHENTICATION

S/4HANA supports multiple authentication methods. The standard method for both ABAP and HANA is user ID and password. Form-based authentication for the standard method is preferred over basic authentication. For HTTP connections, basic authentication passes user credentials in a header variable as a base-64 encoded string. Form-based authentication transmits credentials as a URL parameter. For SAP ABAP protocols such as dialog and RFC, credentials are passed from clients to servers using SAP routines. However, in common with HTTP connections, credentials are only encoded, not encrypted. Therefore, Secure Sockets Layer (SSL) for HTTP, and Secure Network Communications (SNC) for SAP protocols is recommended when using the standard authentication method. Furthermore, robust password policies should be defined and enforced using login/password* parameters in ABAP and the password policy section of the indexserver.ini file in HANA. This includes minimum requirements for password length, complexity, and expiration. Security policies should not exempt specific users or groups from the baseline standards of the global password policy. Support for insecure password hash mechanisms should blocked to prevent the storage of vulnerable password hashes in SAP user tables.

Client certificates based on the X.509 standard provide a more secure authentication mechanism than the standard method. However, X.509 certificates remain valid for a relatively long time. Therefore, S/4HANA should be configured to revoke the certificates after a defined period to minimize the security risk.

S/4HANA also supports Single Sign-On (SSO) mechanisms for authentication using logon tickets. Kerberos, X.509, and SAML 2.0 are preferred over proprietary logon tickets for greater flexibility and security. SSL is recommended to safeguard logon tickets used for web-based authentication. The tickets are vulnerable to compromise since they are stored as non-persistent cookies in web browsers.

[6] Security Guide for SAP S/4HANA, SAP, 2022

External authentication mechanisms such as SAML and Kerberos are also supported by S/4HANA. Note that Kerberos typically authenticates users through active directory systems. Since these systems are usually internal, Kerberos is not suitable for authenticating external access unless using VPN.

For SAP HANA, the default value of parameter authentication_methods should be updated to support only approved authentication methods.

Technical users required for background jobs and interfaces in S/4HANA should be configured as system user types. The use of communication, service and reference user types should be minimized due to risks associated with these user types. Service users, for example, provide anonymous dialog access to S/4HANA.

Standard users delivered with S/4HANA should be secured. This includes the SAP* in all ABAP clients and the SYSTEM user in the system and tenant databases of SAP HANA. Such users should not be used for scheduled jobs and background operations. Administrative authorizations, roles, profiles and transactions should be restricted to required users only based on the principal of least privilege. System privileges for HANA users should also be controlled. Technical users should not be granted administrative profiles such as SAP_ALL in productive systems. This risk is especially high for technical users supporting RFC destinations with stored credentials.

SYSTEM HARDENING WITH SAP SECURITY NOTES

SAP recommends the implementation of the security notes listed in Figure 4.1 during the setup of S/4HANA. The notes include manual steps and therefore cannot be automatically applied using SNOTE. The status of the security notes should be managed in System Recommendations (SysRec). SysRec is an application in SAP Solution Manager that connects directly to SAP Support to automatically discover and calculate required notes for SAP systems including S/4HANA. Other notes reported by SysRec that are not included in Figure 4.1 should also be reviewed and implemented, particularly hot news and high priority security notes.

SECURITY NOTE	DESCRIPTION
1322944	ABAP: HTTP security session management
1531399	Enabling SSL for Session Protection
1585767	Enabling Virus Scanning in SAP Content Server
1616535	Secure configuration of ICM for the ABAP application server
1693981	Unauthorized modification of displayed content
1853140	Managing SAProuter from external host
1973081	XSRF vulnerability: External start of transactions with OK-Code
2086818	Fixing POODLE SSLv3.0 (CVE-2014-3566) Vulnerability
2107562	Fixing POODLE SSLv3.0 (CVE-2014-3566) Vulnerability in Money Mobiliser Platform
2142551	Clickjacking Framing Protection in AS ABAP
2185122	Switchable authorization checks for RFC in data extraction within CA-MDG-APP-FIN
2245332	Clickjacking Framing Protection in SAPUI5 Apps
2260344	OS command injection vulnerability in SCTC_* Function modules
2319172	Clickjacking Framing Protection in SAP GUI for HTML
2319192	Clickjacking Framing Protection in BSP
2333957	Clickjacking Framing Protection in SAP Fiori Launchpad for NW AS ABAP
2349128	Clickjacking Framing Protection in UI theme designer on ABAP
2421287	Front-end printing with SAP GUI 750

Figure 4.1: Security Notes for S/4HANA

SAP S/4HANA SYSTEM LANDSCAPE

S/4HANA includes S4CORE powered by the NetWeaver Application Server ABAP and SAP HANA. SAP ERP in existing SAP Business Suite landscapes can be converted to S/4HANA. The embedded Fiori front end server is recommended for S/4HANA, whereas the hub deployment is recommended for SAP Business Suite and S/4HANA deployments on SAP Cloud Platform.

SAP recommends the deployment of the application lifecycle management platform SAP Solution Manager for both S/4HANA and Business Suite landscapes. The migration to S/4HANA should be managed using Focused Build in Solution Manager. Focused Build provides standardized processes and tools to support the transition to S/4HANA based on SAP best practices and lessons learned from 600 digital transformation projects worldwide[7]. Solution Manager also supports health, performance and security monitoring for S/4HANA systems post go-live using preconfigured KPIs, metrics and templates.

NETWORK AND COMMUNICATION SECURITY

S/4HANA is a software ecosystem comprised of application and database layers, tightly integrated with an operating system at the host level. S/4HANA requires a Linux host and currently supports Red Hat Enterprise Linux and SUSE Linux Enterprise Sever. The operating systems should be hardened in accordance with Red Hat/ SUSE recommendations and/ or security benchmarks provided by organizations such as the Center for Internet Security (CIS).

The active services in the host should be limited to the TCP/IP ports required for Application Server ABAP, SAP HANA Platform, SAP Central Services, and NetWeaver Services[8]. Ports for other areas should only be activated if required. External access to the ports should be restricted using network firewall rules. Internal firewall rules are also recommended to segment S/4HANA from other groups. This will minimize the attack surface and restrict network access to S/4HANA.

The SAProuter and Web Dispatcher should be configured to securely filter external access to S/4HANA. The application gateways should be patched to the latest available versions and releases. Route connection strings in the SAProuter should block native and unencrypted connections and deny connections requests not explicitly permitted by the access control list. The Web Dispatcher should block public monitoring and the disclosure of system information in error messages. Administration of the Web Dispatcher should be restricted to required hosts. URL filters should be defined in access control lists to control access to sensitive applications and services accessed through the Web Dispatcher.

Access controls lists for the registration and starting of external programs should be maintained for the gateway server using the reginfo and secinfo files. Known bypasses of the ACLs should be blocked. Whitelists should be enabled for RFC callbacks and the use of RFC destinations with stored credentials should be minimized to manage the risk of RFC hopping. Trusted RFC connections should be secured against misuse by maintaining the S_RFCACL authorization for relevant technical users.

[7] Manage your Conversion to SAP S/4HANA with SAP Solution Manager and Focused Build, SAP, 2022

[8] TCP/IP Ports of All SAP Products, SAP Help Portal, 2022

ICF AND SESSION SECURITY

Specific ABAP programs in S/4HANA can be accessed using web-based protocols through ICF services. Therefore, only the required ICF services should be activated in the system. Services with known vulnerabilities such as FORMTORFC, IDOC_XML, SOAP RFC and WEB RFC should be deactivated. Conversely, services that support security mechanisms should be activated. This includes the services UICS and WHITELIST for protection against clickjacking attacks.

Session security protection should be enabled to protect session cookies. This can be performed using transaction SICF_SESSIONS and setting the HttpOnly flag to deny client-side scripts access to session cookies.

FILE SYSTEM ACCESS SECURITY

Data files in S/4HANA should be secured against directory traversal attacks by mapping logical paths and file names to physical paths and file names. This will validate requested directories against stored directories before granting access to files. The file paths accessed in S/4HANA can be identified using event IDs CUQ, CUR, CUS, CUT, DU5 and EU4 in the Security Audit Log. Physical paths should be entered in transaction SFILE and SF01 for client-independent and client-dependent paths, respectively. Path validation should be activated with the setting ON for setting REJECT_EMPTY_PATH in table FILECMCUST. This can be performed using transaction SM30.

VIRUS SCANNING

The SAP Virus Scan Interface (VSI) should be enabled to secure against potential malware in files uploaded to S/4HANA. VSI requires an external scanning engine. The interface will protect against files with known virus signatures, untrusted file types, and files with active content such as JavaScript. VSI rejects documents uploads that do not comply with rules in scan profiles. The SAP-delivered scan profiles should be enabled. The following scan profiles can be deactivated if you do not want to scan files downloads from S/4HANA: /SCET/GUI_DOWNLOAD, /SIHTTP/HTTP_DOWNLOAD and /SOAP_CORE/WS_SEND. The VSI allowlist for approved MIME types should be as restrictive as possible.

ADDITIONAL SYSTEM HARDENING ACTIVITIES

HTTP whitelists should be configured using Unified Connectivity (UCON) to define domains or hosts permitted to frame applications in S/4HANA. This will provide further safeguards against clickjacking attacks. UCON should also be used to activate communication assemblies that control external access to remote-enabled function modules in S/4HANA.

SAP recommends activating available switchable authorization checks for S/4HANA. This can be performed using transaction SACF and SACF_COMPARE and will secure access to critical function modules by introducing additional checks to supplement the standard check for authorization object S_RFC.

Authorization checks for transactions called by ABAP programs should enforced using profile parameter auth/check/calltransaction. The recommended setting is 3 for new installations of S/4HANA and 2 for installations migrated from SAP ERP.

DATA PROTECTION AND PRIVACY

SAP provides Read Access Logging (RAL) configurations for S/4HANA. RAL is used to log and monitor access to sensitive data including Personally Identifiable Information (PII). RAL should be activated in each client before activating the configurations.

The Security Audit Log should also be activated for all clients and filters maintained to log critical and severe events at a minimum for all users and groups.

The HANA audit log should be activated and the audit trail should set to table and/or syslog. Audit policies should be configured for SAP HANA to log critical system and user events.

Change logging should be activated for specific tables including property and user tables.

The default settings for gateway server logging should be updated to include actions such as security changes, monitor commands, the launching of external programs, and the registration of servers.

CROSS APPLICATION INFRASTRUCTURE

S/4HANA supports the storage of payment card data. The options Masked Display and Encrypted When Saved should be selected to mask payment card displayed in the UI and encrypt data stored in tables.   The SAP Cryptographic Library (SAPCRYPTOLIB) should be installed to support cryptographic functions. Encryption should be activated for supported credit card types.

ENTERPRISE BUSINESS APPLICATIONS

Usage information provided by Custom Code Management (CCM) in SAP Solution Manager should be analyzed for SAP ERP prior to migrating customizations from ERP to S/4HANA. This will identify unused, redundant code and programs cloned from standard SAP-delivered code. Redundant and cloned custom code can be removed to reduce the scope of the effort for brownfield migrations.

S/4HANA Readiness Checks should be executed using the ABAP Test Cockpit (ATC) to identify usage of simplified SAP standard objects in custom code that must be adapted before migration to S/4HANA. The results of the ATC analysis can be uploaded to the SAP Readiness Check for S/4HANA Conversion.[9]

Custom ABAP, UI5 and SQLScript programs migrated from ERP or developed directly in S/4HANA should be subject to static and dynamic code vulnerability analysis during the build phase. This will detect code security vulnerabilities including ABAP, SQL, OS command and other forms of injection attacks, missing or broken authorization checks, hardcoded users and passwords, directory traversal, cross-site scripting

[9] Custom Code Migration for SAP S/4HANA, SAP, 2022

and calls to critical function modules, reports, tables, and authorizations. Security notes provided by SAP address programming flaws in SAP-delivered code. Customers are responsible for securing custom developments.

Access to sensitive transactions and authorization objects for S/4HANA modules should be restricted using the principal of least privilege. This includes profiles and roles for functions in Finance, Human Capital Management, and other areas. User permissions should also be segregated to ensure conflicting functions are not assigned to end users.

SECURITY COMPLIANCE

Automated compliance gap assessments for S/4HANA can be performed using the Cybersecurity Extension for SAP (CES). This includes the detection of vulnerabilities in custom code and access to functional areas in S/4HANA. CES is an SAP-certified addon for SAP Solution Manager. The checks can be performed during and after migration by selecting the S/4HANA Security Compliance tile in the Fiori launchpad for SAP Solution Manager.

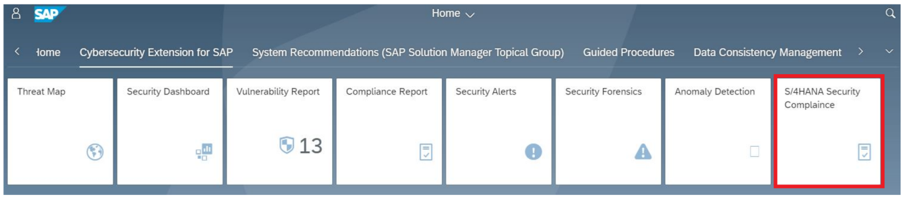
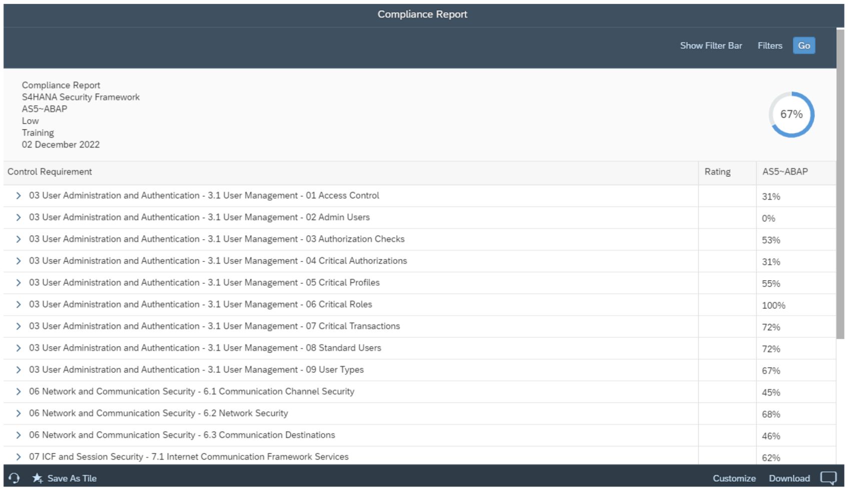


Figure 14.1: SAP Solution Manager

The gap assessment provides an overall compliance score for S/4HANA and each requirement.



Compliance Report

Compliance Report
S4HANA Security Framework
AS5~ABAP
Low
Training
02 December 2022

67%

Control Requirement	Rating	AS5~ABAP
03 User Administration and Authentication - 3.1 User Management - 01 Access Control		31%
03 User Administration and Authentication - 3.1 User Management - 02 Admin Users		0%
03 User Administration and Authentication - 3.1 User Management - 03 Authorization Checks		53%
03 User Administration and Authentication - 3.1 User Management - 04 Critical Authorizations		31%
03 User Administration and Authentication - 3.1 User Management - 05 Critical Profiles		55%
03 User Administration and Authentication - 3.1 User Management - 06 Critical Roles		100%
03 User Administration and Authentication - 3.1 User Management - 07 Critical Transactions		72%
03 User Administration and Authentication - 3.1 User Management - 08 Standard Users		72%
03 User Administration and Authentication - 3.1 User Management - 09 User Types		67%
06 Network and Communication Security - 6.1 Communication Channel Security		45%
06 Network and Communication Security - 6.2 Network Security		68%
06 Network and Communication Security - 6.3 Communication Destinations		46%
07 ICF and Session Security - 7.1 Internet Communication Framework Services		62%

Figure 14.2: S/4HANA Security Compliance

Users can drilldown from each requirement to review the detailed findings. Results can be filtered to focus on specific requirements and findings. The S/4HANA security compliance report can also exported to CSV or PDF for distribution within an enterprise. You can learn more at https://layersevensecurity.com/cybersecurity-extension-for-sap/

LAYER SEVEN SECURITY

Layer Seven Security is an SAP Partner and an industry leader in the provision of security solutions and services for SAP platforms. The company is recognized as one of the Top Ten SAP Solution Providers of 2018 and Top 25 Cybersecurity Companies of 2020.

Layer Seven Security's industry-leading Cybersecurity Extension for SAP delivers advanced vulnerability management, threat detection and incident response to secure SAP systems from cyber attack.

CONTACT US

www.layersevensecurity.com
info@layersevensecurity.com

SAP Partner