Test ID	Test	Test Description
SAP Security Information		
SEC.01-00	SAP Gateway Security Configuration (secinfo)	
SEC.01-01	SAP Message Server Configuration	
SEC.01-02	SAProuter Permission Table	
SEC.01-03	SAP Gateway Security Configuration (reginfo)	
SEC.01-04	Security Audit Log	
SEC.01-05	CPIC-Destinations	
SEC.01-06	Missing SAP Security Patches	
SEC.01-07	Security Audit Configuration	
SEC.01-08	Web Dispatcher Permission Table	
SEC.01-09	RFC Destinations	
SEC.01-10	Active SAP Services	
General Tests		
GEN.01-00	Users with default authorization profiles	
GEN.01-01	Forbidden passwords	
GEN.01-02	Locked Transaction Codes	
GEN.01-03	Deactivated Authorization Objects	
GEN.01-04	Passwords of Standard Users in all Clients	
GEN.01-05	List of Users According to Logon Date and Password Change	
GEN.01-06	List of users having assigned a developer key	
Sensitive System Access		
UA.03-01	User Maintenance: Assign authorization roles to users (ASSIGN_ROLE_AUTH=ASSIGN, CHECK_S_USER_SAS = NO)	
UA.03-02	User Maintenance: Create user accounts	
UA.03-03	Database Administration: Execute DB commands directly from SAP	
UA.03-04	User Maintenance: Change user accounts	
UA.03-05	User Maintenance: Assign authorization roles to user accounts (ASSIGN_ROLE_AUTH=CHANGE, CHECK_S_USER_SAS = NO)	
UA.03-06	User Maintenance: Unlock user accounts (password reset)	
UA.04-01	TREX Administration: Administrate Search and Classification	
UA.05-01	Authorization Management: Deactivate Authorization Checks for Authorization Objects	
UA.06-01	User Maintenance: Assign authorization roles/profiles to user accounts (CHECK_S_USER_SAS = YES)	
UA.06-02	User Maintenance: Assign authorization profiles to user accounts (S_USER_PRO)	
UA.07-01	System Profile Parameters: System Security Configuration	
	abap/ext_debugging_possible	You can use this profile parameter to restrict external/HTTP debugging for external sessions
	auth/object_disabling_active	You can deactivate authorization objects globally in transaction AUTH_SWITCH_OBJECTS if this parameter has the value “Y” or is not set. If the parameter has the value “N”, deactivation is not allowed.
	auth/rfc_authority_check	Execution of the RFC authorization check against authorization object S_RFC
	gw/reg_info	File reginfo controls the registration of external programs in the gateway.

Test ID	Test	Test Description
	gw/reg_no_conn_info	Set this parameter to restrict gateway connections of hosts, which are not listed in the GW ACL file.
	gw/sec_info	The secinfo security file is used to prevent unauthorized launching of external programs.
	icm/HTTPS/verify_client	This parameter specifies whether or not a client must produce a certificate. There are three verification levels (0-2): 0: No certificate is required and the server does not ask for one. 1: The server requests a certificate from the client. If the client
	icm/server_port_0	ICM server specification
	icm/server_port_1	ICM server specification
	icm/server_port_2	ICM server specification
	icm/server_port_3	ICM server specification
	icm/server_port_4	ICM server specification
	login/disable_password_logon	Deactivation of password-based logon
	login/failed_user_auto_unlock	Controls the unlocking of users locked by logging on incorrectly. If the parameter is set to 1, locks that were set due to failed password logon attempts only apply on the same day (as the locking). If the parameter is set to 0, the locks remain in effect
	login/fails_to_user_lock	Every time an incorrect logon password is entered, the failed logon counter for the relevant user master record is increased. The logon attempts can be logged in the Security Audit Log. If the limit specified by this parameter is exceeded, the relevant us
	login/min_password_diff	The administrator can use this parameter to specify by how many characters a new password must differ from the old password when the user changes it. This parameter is ignored when new users are created or when passwords are reset to the initial password.
	login/min_password_digits	Defines the minimum number of digits (0-9) in passwords. Default value: 0; permissible values: 0 – 40. Available as of SAP Web AS 6.10 (Until SAP NetWeaver 6.40 (inclusive), up to 8 characters.)
	login/min_password_letters	Defines the minimum number of letters (A-Z) in passwords. Default value: 0; permissible values: 0 – 40. Available as of SAP Web AS 6.10 (Until SAP NetWeaver 6.40 (inclusive), up to 8 characters.)
	login/min_password_lng	Defines the minimum length of the password. Default value: 6; permissible values: 3 – 40. Until SAP NetWeaver 6.40 (inclusive), up to 8 characters.
	login/min_password_lowercase	Specifies how many characters in lower-case letters a password must contain. Permissible values: 0 – 40; default value 0. Available after SAP NetWeaver 6.40"
	login/min_password_specials	Defines the minimum number of special characters in the password Permissible special characters are, in particular, !"@ $%&/()=?'`+~#-_.,;:{[]}\<>| and space and the grave accent. After SAP NetWeaver 6.40, all characters that are not letters or digits are
	login/min_password_uppercase	Specifies how many characters in upper-case letters a password must contain. Permissible values: 0 – 40; default value 0. Available after SAP NetWeaver 6.40
	login/no_automatic_user_sapstar	If the user master record of the user SAP is deleted, it is possible to log on with SAP* and the initial password PASS.
	login/password_change_for_SSO	With password-based logon, the system checks whether the user's password needs to be changed (for example, because the password is initial or has expired). If non-password-based logon variants are used (SSO: SNC, X.509, PAS, logon ticket), no check is cur
	login/password_compliance_to_current_policy	You can use this parameter to control whether the system checks whether the password used for a password-based logon fulfills the current password rules and, if necessary, prompts the user to change his or her password.
	login/password_downwards_compatibility	As of SAP NetWeaver (SAP_BASIS) 7.0, the system supports logon with passwords that can consist of up to 40 characters (previously: 8), and which are case-sensitive (previously, the system automatically converted from lowercase to uppercase letters). It is
	login/password_expiration_time	The value 0 indicates that no users are forced to change their passwords. Values greater than 0 specify the number of days after which users need to change their passwords. (Exception: Users of the types SERVICE and SYSTEM).
	login/password_hash_algorithm	Defines the format and hash algorithm for new passwords
	login/password_history_size	This parameter specifies the size of the password history. The password history is consulted whenever a user choose a new password. The system rejects any passwords that are saved in the password history
	login/password_max_idle_initial	You can use this parameter to define the maximum period of time between the time of the password being (re)set and the next logon with the initial password. After this period expires, the system displays the message "Initial password has expired" and the
	login/password_max_idle_productive	You can use this parameter to define the maximum period of time between the time of the last password change and the next logon with this password. After this period expires, the system displays the message "Initial password has expired" and the logon is
	rec/client	This parameter can be used to activate or deactivate table auditing specific to the client. The setting of this parameter determines whether write operations on certain tables (flagged appropriately in their technical settings in ABAP Dictionary) are logg
	rfc/reject_expired_passwd	Set this parameter to avoid users logging on with initial or expired user accounts.
	rsau/enable	Enable Security Audit

Test ID	Test	Test Description
	snc/accept_insecure_cpic	Accept insecure incoming CPIC connections on an SNC-enabled application server
	snc/accept_insecure_gui	Accept logins from unprotected (non-SNC-secured) SAP GUIs into an SNC-enabled application server
	snc/accept_insecure_rfc	Accept insecure incoming RFC connections on an SNC-enabled application server
	snc/enable	If this parameter is set to “1”, the work processes try to activate/initialize the module SNC (Secure Network Communications) when starting up.
	ssl/ciphersuites	Default SSL/TLS server cipher suites (and flags)
	ssl/client_ciphersuites	Default SSL/TLS client cipher suites (and flags)
UA.08-03	Program change and execution: Execute a function module	
UA.08-04	Program change and execution: Execute a function in the SAP module pool	
UA.09-01	Security Audit Logging: Delete Security Audit Logs	
UA.09-02	Security Audit Logging: Modify Security Audit Logging	
UA.10-01	RFC Connections: Logon remotely via RFC	
UA.10-02	Batch Job Administration: Execute batch jobs using any other user ID	
UA.10-03	Batch Job Administration: Batch Administration	
UA.10-04	Batch Job Administration: Batch Scheduling	
UA.10-05	Batch Job Administration: Batch Processing	
UA.20-01	Authorization Bypass: Write Debugging	
UA.32-01	OS Administration: Write and execute OS commands out of SAP	
System Change Authorizations		
CM.00-01	Transport Management System: System change option	
CM.00-02	Client Administration: Client protection settings	
CM.00-03	Transport Management System: System change option change log	
CM.00-04	Client Administration: Client protection settings change log	
CM.01-01	Transport Management System: Configure the SAP Transport Management System	
CM.01-02	Transport Management System: Import SAP Transports	
CM.02-01	System Profile Parameters: Maintain profile parameters	
CM.02-02	Transport Management System: Maintain system change option	
CM.02-04	Client Administration: Modify client protection settings	
CM.02-05	SAP Customizing: Maintain SAP IMG customizing	
CM.03-01	Transport Management System: Maintain any client independent table (e.g. client settings)	
CM.03-03	Transport Management System: Maintain table assigned to the authorization group SS (SAP control)	
CM.10-01	Transport Management System: Modify Data Dictionary Objects	
CM.10-02	Program change and execution: Directly execute an SAP program	
CM.10-03	Program change and execution: Modify function modules	
CM.10-04	Program change and execution: Modify SAP Enhancements	
CM.10-05	ABAP queries: Write code in query infosets	
CM.10-06	ABAP queries: Maintain SAP queries	
CM.11-01	Authorization Maintenance: Create authorization role	
CM.11-02	Authorization Maintenance: Change authorization role	

Test ID	Test	Test Description
CM.11-03	Authorization Maintenance: Create authorization profile	
CM.11-04	Authorization Maintenance: Change authorization profile	
CM.11-05	Authorization Maintenance: Modify SAP authorizations	
CM.11-06	Authorization Maintenance: Create SAP authorizations	