



Optimized

SAP Security Information SEC.01-00 SAP detawy Security Configuration SEC.01-01 SAP Message Server Configuration SEC.01-02 SAP message Server Configuration SEC.01-03 SAP detawy Security Configuration SEC.01-03 SAP detawy Security Configuration (reginfo) SEC.01-04 Security Audit Log SEC.01-05 CPIC-Destinations SEC.01-06 Security Audit Configuration SEC.01-07 Security Audit Configuration SEC.01-08 SEC.01-09 SEC.01-0		Uptimized			
SEC.01-00 SAP Pateway Security Configuration (secinfo) SEC.01-01 SAP Message Server Configuration SEC.01-02 SAP Outer Permission Table SEC.01-03 SAP Outer Permission Table SEC.01-04 SEC.01-05 SEC.01-05 SEC.01-06 SEC.01-06 SEC.01-06 SEC.01-07 SEC.01-06 SEC.01-07 SEC.01-06 SEC.01-07 SEC.01-08 Web Dispatcher Permission Table SEC.01-09 SEC.01-	Test ID	Test		Test Description	
SEC.01-01 SAP Nessage Server Configuration SEC.01-02 SAP Outbre Permission Table SEC.01-03 SAP Gateway Security Configuration (reginfo) SEC.01-04 Security Audit Log SEC.01-05 SAP Gateway Security Patches SEC.01-06 Missing SAP Security Patches SEC.01-07 Security Audit Configuration SEC.01-07 Security Audit Configuration SEC.01-08 Security Patches SEC.01-09 RFC Destinations SEC.01-10 Active SAP Services SEC.01-10 Active S		SAP Security Information			
SEC.01-02 SAProuter Permission Table SEC.01-03 SAP Gateway Security Configuration (reginfo) SEC.01-04 Security Audit Log SEC.01-05 (PIC-Destinations SEC.01-06 Web Dispatcher Permission Table SEC.01-07 Security Audit Configuration SEC.01-08 Web Dispatcher Permission Table SEC.01-10 Active SAP Services SEC.01-10 Active SAP Services SEC.01-10 Analysis of OS permissions on the SAP profile parameter directory SEC.02-00 Configuration changes for SAP gateway intrusion detection SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP profile parameter directory SEC.04-01 Objects in transports without an HTTP whitelist check SEC.04-02 WebDynpro applications without domain relaxing SEC.04-01 Objects in transports with automatic code execution after import General Tests General Tests General Code GEN.01-01 Forbidden passwords GEN.01-03 Deactivated Authorization profiles GEN.01-04 Deactivated Authorization Dipicts GEN.01-05 Deactivated Authorization Dipicts GEN.01-06 List of users having assigned a developer key Sensitive System Access Sensitive Sustaina Access Sensitive System Access Sensitive Sustaina Access Sensitive	SEC.01-00		0		
SEC.01-03 SAP Gateway Security Configuration (reginfo) SEC.01-04 Security Audit Log SEC.01-05 (Pic-Destinations) SEC.01-05 (Pic-Destinations) SEC.01-06 Missing SAP Security Patches SEC.01-07 Security Audit Configuration SEC.01-07 Security Audit Configuration SEC.01-08 Web Dispatcher Permission Table SEC.01-09 RFC Destinations SEC.01-09 RFC Destinations SEC.01-09 RFC Destinations SEC.01-10 Active SAP Services SEC.01-11 Dialog users in RFC connections SEC.01-10 Active SAP Services SEC.01-11 Dialog users in RFC connections SEC.02-00 Configuration changes for SAP gateway logging SEC.02-00 Configuration changes for SAP gateway logging SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP printip parameter directory SEC.03-02 Analysis of OS permissions on the SAP printip parameter directory SEC.03-04 Analysis of OS permissions on the SAP instance directory SEC.03-05 Analysis of OS permissions on the SAP instance directory SEC.03-06 WebDynpro applications without an HTTP whitelist check SEC.04-07 WebDynpro applications without an HTTP whitelist check SEC.04-08 WebDynpro applications without an HTTP whitelist check SEC.04-09 WebDynpro applications without an HTTP whitelist check SEC.03-01 Objects in transports with automatic code execution after import SEC.03-01 Objects in transports with automatic code execution after import SEC.03-02 Objects in transports with automatic code execution after import SEC.03-03 Objects in transports with automatic code execution after import SEC.03-04 Objects in transports with automatic code execution after import SEC.03-04 Objects in transports with automatic code execution after import SEC.03-04 Objects in transports with automatic code execution after import SEC.03-04 Objects in all Clients SEC.03-05 Objects in all Clients SEC.03-06 Objects in all Clients SEC.03-06 Objects in all Clients SEC.03-06 Objects in all Clients SEC.03-07 Objects in all Clients SEC.03-09 Objects in all Clients SEC.03-09 Objects in all Clients SEC.					
SEC.01-04 Security Audit Log SEC.01-05 CPIC-Destinations SEC.01-07 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 SEC.01-10 Ipliagusers in RFC connections SEC.01-10 Active SAP Services SEC.01-10 Ipliagusers in RFC connections SEC.01-10 Analysis of OS permissions on the SAP profile parameter directory SEC.02-01 Analysis of OS permissions on the SAP profile parameter directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.04-04 Active dwebDynpro development services SEC.04-05 WebDynpro applications without an HTTP whitelist check SEC.04-05 WebDynpro applications without an HTTP whitelist check SEC.04-06 Nebrophy applications without domain relaxing SEC.05-07 Objects in transports in transports without domain relaxing SEC.05-07 Objects to transports development services SEC.05-09 Objects to transports development services SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-01 Objects to transports of the SAP instance directory SEC.05-05 Objects to transports on the SAP instance directory SEC.05-06 Objects to transports on the SAP instance directory SEC.05-07 Objects to transports on the SAP instance directory SEC.05-07 Objects to transports on the SAP instance directory SEC.05-07 Objects to transports on the SAP instance directory SEC.05-07 Objects to transports on the SAP instance directory SEC.05-07 Obje			0		
SEC.01-06 Missing SAP Security Patches SEC.01-07 Security Audit Configuration SEC.01-08 Web Dispatcher Permission Table SEC.01-08 Net Destinations SEC.01-09 RFC Destinations SEC.01-10 RFC Destinations SEC.01-10 I Dalog users in RFC connections SEC.01-10 I Dalog users in RFC connections SEC.02-01 SAP Gateway Intrusion detection SEC.03-02 Configuration changes for SAP gateway logging SEC.03-03 Analysis of OS permissions on the SAP transport directory SEC.03-01 Analysis of OS permissions on the SAP profile parameter directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.03-04 OF SEC.03-05 Analysis of OS permissions on the SAP instance directory SEC.03-06 I Diplects in transports with automatic code execution after import SEC.04-00 WebDynpro applications without domain relaxing SEC.04-00 Users with default authorization profiles GEN.01-00 Users with default authorization profiles GEN.01-00 Users with default authorization objects GEN.01-00 Deactive Active Active SAP secording to Logon Date and Password Change GEN.01-00 Users having assigned a developer key Sessitive System Access UA.03-01 User Maintenance Assign authorization roles to users	SEC.01-03	SAP Gateway Security Configuration (reginfo)	0		
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 SEC.01-10 Ioliaguaser in RFC connections SEC.01-10 Active SAP Services SEC.01-10 Active SAP Services SEC.01-11 Analysis of Services SEC.01-10 Analysis of Sermissions on the SAP grateway logging SEC.02-01 SAP Gateway intrusion detection SEC.03-01 Analysis of Sermissions on the SAP transport directory SEC.03-02 Analysis of Sermissions on the SAP profile parameter directory SEC.03-03 Analysis of Sermissions on the SAP instance directory SEC.03-04 Analysis of Sermissions on the SAP instance directory SEC.03-07 MebDynpro applications without an HTTP whitelist check SEC.04-08 WebDynpro applications without domain relaxing SEC.05-09 Ioligets in transports with automatic code execution after import GEN.01-00 Users with default authorization profiles GEN.01-01 Forbidden passwords GEN.01-02 Locked Transaction Codes GEN.01-03 Passwords of Standard Users in all Clients 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 According to Logon Date and Password Change GEN.01-06 User Walning and Active Services UA.03-01 User Maintenance: Assign authorization roles to users	SEC.01-04	Security Audit Log			
SEC.01-07 Security Audit Configuration SEC.01-08 Web Dispatcher Permission Table SEC.01-10 RCD Destinations SEC.01-10 Active SAP Services SEC.01-11 Dialog users in RFC connections SEC.02-00 Configuration changes for SAP gateway logging SEC.02-01 SAP Gateway intrusion detection SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP profile parameter directory SEC.03-04 Analysis of OS permissions on the SAP intranse directory SEC.03-05 Analysis of OS permissions on the SAP intranse directory SEC.03-06 Analysis of OS permissions on the SAP intranse directory SEC.03-07 Analysis of OS permissions on the SAP intranse directory SEC.03-08 Analysis of OS permissions on the SAP intranse directory SEC.03-09 Analysis of OS permissions on the SAP intranse directory SEC.03-00 Analysis of OS permissions on the SAP intranse directory SEC.03-00 Analysis of OS permissions on the SAP intranse directory SEC.03-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HITTP whitelist check SEC.04-02 WebDynpro applications without an HITTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.03-04 Objects in transports with automatic code execution after import SEC.04-05 Objects in transports with automatic code execution after import SEC.04-06 Objects in transports with automatic code execution after import SEC.04-07 Objects in transports with automatic code execution after import SEC.04-08 Objects in transports with automatic code execution after import SEC.04-09 Objects in transports with automatic code execution after import SEC.04-09 Objects in transports with automatic code execution after import SEC.04-00 Objects in transports with automatic code execution after import SEC.04-01 Objects in transport with automatic code execution after import SEC.04-02 Objects in transports with automatic code execution after import SEC.04-03 Objects in tr	SEC.01-05	CPIC-Destinations			
SEC.01-08 Web Dispatcher Permission Table SEC.01-09 RFC Destinations SEC.01-10 Joing users in RFC connections SEC.01-11 Dialog users in RFC connections SEC.02-00 Configuration changes for SAP gateway logging SEC.02-01 SAP Gateway Intrusion detection SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP profile parameter directory SEC.03-04 Analysis of OS permissions on the SAP profile parameter directory SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HITP whitelist check SEC.04-03 WebDynpro applications without an HITP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.04-01 Users with default authorization profiles GEN.01-00 Users with default authorization profiles GEN.01-01 Secretary Secretar	SEC.01-06				
SEC.01-09 RFC Destinations SEC.01-10 Active SAP Services SEC.02-11 Dialog users in RFC connections SEC.02-01 SEC.02-01 SAP Gateway intrusion detection SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-01 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-02 SEC.05-01 Objects in transports with automatic code execution after import General Tests GEN.01-00 GEN.01-00 Users with default authorization profiles GEN.01-01 Forbidden passwords GEN.01-03 Deactivated Authorization Objects GEN.01-03 Deactivated Authorization Objects GEN.01-04 Deactivated Authorization Dipects GEN.01-05 Disc of Standard Users in all Clients GEN.01-06 Dist of Users According to Logon Date and Password Change GEN.01-06 Ust of Users According to Logon Date and Password Change GEN.01-06 Ust of Users According to Logon Date and Password Change GEN.01-06 Ust of Users According to Logon Date and Password Change GEN.01-06 Ust of Users According to Logon Date and Password Change GEN.01-06 Ust of Users According to Logon Date and Password Change GEN.01-06 Ust of Users According to Logon Date and Password Change Ust.01-03-01 User Maintenance: Assign authorization roles to users	SEC.01-07	Security Audit Configuration			
SEC.01-10 Active SAP Services SEC.02-10 Configuration changes for SAP gateway logging SEC.02-01 SAP Gateway intrusion detection SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP profile parameter directory SEC.03-04 Activated WebDynpro development services SEC.04-01 Activated WebDynpro applications without an HTTP whitelist check SEC.04-02 WebDynpro applications without domain relaxing SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import 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	SEC.01-08	Web Dispatcher Permission Table			
SEC.02-00 Configuration changes for SAP gateway logging SEC.02-01 SAP Gateway intrusion detaction SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.03-04 Analysis of OS permissions on the SAP instance directory SEC.03-05 Analysis of OS permissions on the SAP instance directory SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import General Test 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 devoloper key Sensitive System Access UA.03-01 User Maintenance: Assign authorization roles to users	SEC.01-09	RFC Destinations			
SEC.02-00 Configuration changes for SAP gateway logging SEC.02-01 SAP Gateway intrusion detection SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import GEN.01-00 Users with default authorization profiles GEN.01-00 Users with default authorization profiles GEN.01-01 Forbidden passwords 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					
SEC.03-01 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP profile parameter directory SEC.03-04 Analysis of OS permissions on the SAP profile parameter directory SEC.03-05 Analysis of OS permissions on the SAP profile parameter directory SEC.03-06 Analysis of OS permissions on the SAP profile parameter directory SEC.03-07 Analysis of OS permissions on the SAP profile parameter directory SEC.03-08 Analysis of OS permissions on the SAP profile parameter directory SEC.03-09 Analysis of OS permissions on the SAP profile parameter directory SEC.03-01 Activated WebDynpro development services SEC.03-02 WebDynpro applications without an HTTP whitelist check SEC.03-03 WebDynpro applications without domain relaxing SEC.03-04 Users with default authorization services SEC.03-05 Users with default authorization profiles GEN.01-01 Users with default authorization profiles 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			典		
SEC.03-02 Analysis of OS permissions on the SAP transport directory SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import 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	SEC.02-00	Configuration changes for SAP gateway logging	東		
SEC.03-02 Analysis of OS permissions on the SAP profile parameter directory SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import 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.01-05 List of Users According to Logon Date and Password Change GEN.01-05 User Maintenance: Assign authorization roles to users		•			
SEC.03-03 Analysis of OS permissions on the SAP instance directory SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import 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.01-05 List of Users having assigned a developer key Sensitive System Access UA.03-01 User Maintenance: Assign authorization roles to users		Analysis of OS permissions on the SAP transport directory	NEW		
SEC.04-01 Activated WebDynpro development services SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import 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	SEC.03-02	Analysis of OS permissions on the SAP profile parameter directory	*		
SEC.04-02 WebDynpro applications without an HTTP whitelist check SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import 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	SEC.03-03	Analysis of OS permissions on the SAP instance directory			
SEC.04-03 WebDynpro applications without domain relaxing SEC.05-01 Objects in transports with automatic code execution after import 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	SEC.04-01				
SEC.05-01 Objects in transports with automatic code execution after import 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					
SEC.05-01 Objects in transports with automatic code execution after import 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	SEC.04-03	WebDynpro applications without domain relaxing	*		
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	SEC.05-01	Objects in transports with automatic code execution after import			
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	General Tes	ts			
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	GEN.01-00	Users with default authorization profiles			
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	GEN.01-01	· · · · · · · · · · · · · · · · · · ·			
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	GEN.01-02	Locked Transaction Codes			
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	GEN.01-03	Deactivated Authorization Objects			
GEN.01-06 List of users having assigned a developer key Sensitive System Access UA.03-01 User Maintenance: Assign authorization roles to users	GEN.01-04				
Sensitive System Access UA.03-01 User Maintenance: Assign authorization roles to users	GEN.01-05	List of Users According to Logon Date and Password Change			
UA.03-01 User Maintenance: Assign authorization roles to users	GEN.01-06	List of users having assigned a developer key			
	Sensitive System Access				
UA.03-02 User Maintenance: Create user accounts	UA.03-01				
	UA.03-02	User Maintenance: Create user accounts			



Test ID	Test	Test Description
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 roles to user accounts	
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	
UA.06-01	User Maintenance: Assign roles/profiles to user accounts	
UA.06-02	User Maintenance: Assign profiles to user accounts (S_USER_PR0)	
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.
	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.
	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):
	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
	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
	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
	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
	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
	login/min_password_Ing	Defines the minimum length of the password. Default value: 6; permissible values: 3 – 40. Until SAP NetWeaver 6.40 (inclusive), up to 8
	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
	login/min_password_specials	Defines the minimum number of special characters in the password Permissible special characters are, in particular, !"@ \$%&/()=?'`+~#-
	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
	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
	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
	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),



Test ID	Test	Test Description
	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
	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.
	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
	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
	rec/client	This parameter can be used to activate or deactivate table auditing specific to the client. The setting of this parameter determines
	rfc/reject_expired_passwd	Set this parameter to avoid users logging on with initial or expired user accounts.
	rsau/enable	Enable Security Audit
	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
	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.09-03	Security Audit Logging: Delete Security Audit Logs (after OSS note 2191612)	
UA.09-04	Security Audit Logging: Modify Security Audit Logging (after OSS note	
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 Cha	ange 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	
CM.01-02	Transport Management System: Import SAP Transports	
CM.02-01	System Profile Parameters: Maintain profile parameters	



Test ID	Test	Test Description
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	
CM.03-03	Transport Management System: Maintain table assigned to the	
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	
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	