MTN Ghana Charging Security Baseline - Compliance Checklist Final

ERICSSON

MTN Ghana CS Security Baseline Implementation & Rollout - Compliance Checklist

Sr. NO	Baseline REQ tag	Security Control	Control Objectives - Details of Compliance Issue	Appl APP
MBSSv3 (MoP)				
Security Module 1: Accounts & Password Management				
1	OS_ACC_007	Restrict root access on Linux	Disable direct access to root ID and then require the system administrators to obtain root privileges by using the su - command. Root privileges can be delegated out to other user accounts as required. As a best practice you do not want to provide the root password to multiple users as it makes auditing and tracking who is doing what with the account more difficult. To provide root access to other users, the user account can be added to the sudoers file which will grant them root privileges.	NA
2	OS_ACC_009, APP_HARD_003	Disallow root access via FTP	Direct root access via ftp is disabled	NA

3	OS_ACC_001, OS_ACC_006, OS_ACC_007, OS_ACC_008, DB_ACC_001, DB_ACC_002, DB_ACC_003, DB_ACC_004, APP_ACC_001, APP_ACC_002	Prevent sharing of privileged accounts	Direct access to root or other suoeruser is disabled. Approprite privilege to the same has been given to a limited set of users.	APPL
4	OS_ACC_005, DB_ACC_011, APP_ACC_003, DB_ACC_017	Set account lockout threshold for invalid logon attempts	User account gets locked out automatically after 5 invalid or failed logon attempts	APPL

5	OS_ACC_013, OS_ACC_014, APP_HARD_003	Restrict mounting of NFS shares	NFS must be configured so that only authorized hosts can mount the remote shares. If all hosts on the network can mount remote shares, then the data residing on the file systems would be accessible to even the unauthorized hosts.	NA
6	OS_ACC_026	Restrict concurrent unauthenticated user access from different terminals	Maximum number of concurrent ssh connection is restricted	NA
7	OS_ACC_010, OS_ACC_011	Use of SSH key based authentication	Ssh login should be carried forward via password/keybased authentication.	NA

8	OS_ACC_004, DB_ACC_008 , APP_ACC_006	Remove or disable inactive users	Inactive users will be deleted as per userlist shared by MTN. MTN will take care of this	APPL
9	DB_ACC_001, DB_ACC_002	Prevent direct login to the database	TimesTen database run in embeded mode. it uses OS layer authentication. And direct connecting to DB over network is not possible	NA
10	DB_ACC_019, DB_ACC_023, DB_ACC_020	Enable database authentication	Direct login to TimesTen database is not allowed. Only users with privilege to sdpuser can switch to the same at the unix layer and login to the database	NA

11	OS_ACC_024, DB_ACC_019, DB_ACC_023	Assign or change password to default system account	Default system account password has been changed	APPL
12	OS_ACC_024, DB_ACC_019, DB_ACC_020, DB_ACC_023, APP_ACC_016	Change default passwords after node installation/upgrade	Default system account password has been changed after node installation/upgrade	APPL

13	APP_ACC_007, DB_ACC_016, OS_ACC_022, DB_ACC_018	Set Password Restriction	Password restriction has been enabled for user account	APPL
14	OS_ACC_016, OS_ACC_017, OS_ACC_018, OS_ACC_025, OS_ACC_021, OS_ACC_023, APP_ACC_009, APP_ACC_014, DB_ACC_014, DB_ACC_024, DB_ACC_012	Set Password Complexity	Password complexity has been enabled for user account	APPL

15	OS_ACC_019, OS_ACC_020, DB_ACC_013, APP_ACC_008, APP_ACC_015, DB_ACC_015	Set password expiry	Password expiry has been enabled for user account	APPL
16	DB_ACC_020, DB_ACC_024	Set password complexity verification function	Setting the password complexity verification functions to enforce the password complexity configured for the different layers.	NA
17		SDP dump tool configuration and file transfer permission	SDP dump tool configuration and file transfer permission is not allowed for all users. Only users with privilege to sdpuser and root can switch to the same at the unix layer and use SDP dump tool.	NA

Security Module 2: Hardening				
18	OS_HARD_006, OS_HARD_003, APP_HARD_006	Disable unsecured services	Unsecured services are disabled	NA
19	OS_ACC_027	Configure the SSH Session Timeout	When logging in through a remote connection with SSH, it may be effective to set the timeout value directly through the concerned service. SSH allows administrators to set an idle timeout interval. After this interval has passed, the idle user will be automatically logged out	NA
20	APP_HARD_003	Disable Anonymous FTP Login	Doing ftp as anonymous user is disabled	NA
21	OS_ACC_028	Setting X11 Protocol Forwarding	X11 forwarding is a mechanism that allows graphical interfaces of X11 programs running on a remote Linux/Unix server to be displayed on a local client machine. Behind the scene, the X11 output of a remotely running program is authorized to be sent to localhost via an X11 connection between client and a remote server. Hence the X11 forwarding sessions should be encrypted and encapsulated.	NA

22	OS_HARD_002, APP_HARD_001, APP_VUL&PAT_001	Disable unused services	Unused services are disabled	NA
23	OS_HARD_009	Linux, enable stack protection against buffer overflows	Enabling stack protection prevents certain classes of buffer overflow attack and is a significant security enhancement	NA
24	OS_HARD_010	Configure TCP Wrappers	TCP Wrappers is a host-based access control system that allows administrators to control who has access to various network services based on the IP address of the remote end of the connection	NA
25	APP_HARD_004	Disable/Remove CGI Test script	Certain conditions in the test-cgi file, shipped with older NCSA and Apache HTTP server packages, could allow a remote attacker to submit a query to view the contents of the cgi-bin directory or other directories on the Web server. This information could be useful to an attacker in performing future attacks on the system.	NA

26	OS_HARD_007	Create and enable Warning Banners	Warning banner is enabled	APPL
27	OS_HARD_004	Disable/configure weak SNMP community string	SNMP community string is configured to provide strong access control	NA
28	OS_HARD_012	Disable Trace/Track in Apache HTTPD	The HTTP1.1 protocol requires support for the TRACE request method which reflects the request back as a response and is intended for diagnostics purposes. The TRACE method is not needed and is easily subjected to abuse and is disabled	NA

29	OS_HARD_013	Disable SSL Weak Cipher (using RC4) in Apache	SSL Cipher is an encryption algorithm, which is used as a key for data transfer between two computers over the Internet. The SSL/TLS protocols support many encryption ciphers including many weak ciphers that are subject to man-in-the-middle attacks and information disclosure. Therefore, it is critical to ensure the configuration only allows strong ciphers greater than or equal to 128 bit to be negotiated with the client	NA
30	OS_HARD_014	Disable SSLv3 and TLSv1 Protocol Weak CBC Mode	To secure data that is being transferred, TLS/SSL makes use of one or more cipher suites. A cipher suite is a combination of authentication, encryption and message authentication code (MAC) algorithms. All of which are used during the negotiation of security settings for a TLS/SSL connection as well as for the secure transfer of data.	NA
31	OS_HARD_015	Upgrade a Supported Version of Apache HTTP Server	Running of old version of Apache HTTP server is always a security vulnerability. So the apache server has to be upgraded to support the latest version	NA
32	OS_HARD_016	Disable SSH Weak CBC Mode Ciphers	The symmetric portion of the SSH Transport Protocol has security weaknesses that allows recovery of up to 32 bits of plaintext from a block of cipher text that is encrypted with the Cipher Block Chaining (CBC) method. It may allow a remote unprivileged user who can intercept SSH network traffic to gain access to a portion of plain text information from intercepted traffic which would otherwise be encrypted. It is possible to work around this issue by disabling the use of those CBC Mode Ciphers in SSH for operational analytics. The directive SSH Ciphers are used to limit the types of ciphers that SSH uses during communication.	NA

33	OS_ACC_031	Reset/Recover Root Password	root password is recovered using CD/DVD or without using CD/DVD	NA
Security Module 3: Audit Logging				
34	OS_LOG_001, OS_LOG_002, DB_LOG_001, DB_LOG_002, DB_LOG_004, APP_LOG_001	Enable Audit Logging	Audit logging is enabled to track user activities, and to monitor logins and logouts to identify unauthorized access	APPL

35	OS_LOG_003	Logging of user activities on OS level	OS level logging is enabled to capture unsuccessful login attempts	NA
36	DB_LOG_007, OS_LOG_005, APP_LOG_004	Restrict access of audit logs	Read and write permission of Audit logs should be provided to super user only	NA

37	APP_LOG_002, DB_LOG_006, OS_LOG_004, APP_LOG_003	Configuring remote syslog from LINUX server (Optional)	Log file integrity can be achieved by enabling remote logging. Logs and audit files can be transferred to a remote server using protected protocols. In case of security incidence, for example tampered log files, the remote files can be used for verification of the local log files.	NA
Security Module 4: 3pp Software and Patching				
38	OS_VUL&PAT_005	Prevent SMTP information disclosure	The remote SMTP server answers to the EXPN and VRFY commands. The EXPN command can be used to find the delivery address of mail aliases and the VRFY command may be used to check the validity of an account. SMTP information disclosure should be disabled	NA
39	OS_VUL&PAT_006	SMTP and web server version shall not be disclosed	It has been identified that SMTP and the Web services discloses the version information. This could be a potential attack vector which reveals the vulnerabilities associated with the respective platforms. SMTP and webserver version disclosure should be disabled	NA
40	DB_VUL&PAT_001, DB_VUL&PAT_003	Upgrade database to the latest patch version	The node should be upgraded to the latest available ICP (Intermediate Correction Package).	NA

41	OS_VUL&PAT_001, OS_VUL&PAT_002, OS_VUL&PAT_003, DB_VUL&PAT_002	Upgrade operating system to the latest patch version	The node should be upgraded to the latest available ICP (Intermediate Correction Package).	NA
Security Module 5: Enhancement Security Feature - Optional				
42	MR-036-NW002	Configure the host based firewall – Optional	IP filter provides port and IP based access control	NA
Security Module 6: Additional Specific Requirement				
43	OS_VUL&PAT_ADD_001, DB_VUL&PAT_ADD_001, APP_VUL&PAT_ADD_001	Provide screenshot for security control validation	Post implementation of MBSSv3, screenshot and evidences on the following security areas could be provided, whether are applicable and possible: • SU Logging • Review of audit logs • Direct root login • Cron tabs • Legal warning • Account ownership and authorization	NA
44	OS_VUL&PAT_ADD_002	Provide consistent information regarding security control configuration	Screenshot on /etc/passwd and /etc/shadow files could be taken after MBSSv3 implementation and be provided to the auditor team on time	NA
Security Module 7: Security Policy				
45	OS_VUL&PAT_ADD_003, DB_VUL&PAT_ADD_002	Perform regular reviews of audit logs	Usage of Security Information and Event Management (SIEM) solution e.g. Ericsson Centralized Audit Logging (ECAL), Arcsight, Imperva, etc., will help MTN Ghanal management to capture, analyze and subsequently act on log and alert information collected from a wide array of systems across the operational network including charging and mediation.	APPL
46	OS_VUL&PAT_004 DB_VUL&PAT_004	Initiate a vulnerability scan by the Qualys scanner after implementation	After MBSSv3 implementation MTN Ghanal should run a vulnerability scanning to check their charging system security compliance status to MTN Group CS baseline.	APPL

47	OS_COMPL_XXX DB_COMPL_XXX APP_COMPL_XXX	Security Compliance Checklist Automation	Ericsson Security Manager (ESM) Product which provides a Security Compliance and Monitoring tool to help automate checklist serial of tasks intended to be performed regularly.	APPL

MTN Ghana Charging Security Baseline - Compliance Checklist Final

licability Level		Implementation Status	Recommendations for action		Comments (What to Check)
DB	OS		Status	Readiness Date	
NA	APPL	Fully Compliant	No action		MoP Work Package tag: WP002_v3 **OS:** To prevent direct login via any console device(tty), the /etc/securetty file must be edited and the tty device removed. An empty /etc/securetty file prevents driect root from login from any device. To prevent direct login via ssh, edit (vi) the /etc/ssh/sshd_config file and set the parameter: PermitRootLogin no Then restart sshd service through /etc/init.d/sshd restart
NA	APPL				MoP Work Package tag: WP003_v3 **OS:** To disallow root access via FTP the following parameters should be set in the /etc/vsftpd/vsftpd.conf file: userlist_enable=YES userlist_deny=YES In the /etc/pam.d/vsftpd file "deny file" shall be set to deny file=/etc/vsftpd/ftpusers. root (if not already present) should be added to files /etc/vsftpd/ftpuser /etc/vsftpd/user_list. If any changes are made vsftpd service should be restarted

APPL	APPL				MoP Work Package tag: WP004_v3 **OS:** Verify that only a limited set of users have been granted superuser privileges in the /etc/sudoers file: cat /etc/sudoers To assign superuser privileges to a user, as root, in /etc/sudoers file add: <username> ALL=(ALL) ALL Alternatively add user to group with: useradd -g <groupname> <username> and then in /etc/sudoers add: %<groupname> ALL=(ALL) ALL To grant specific superuser privilege to a user or group, set: <username> ALL=(<superuser>) ALL %<groupname> ALL=(<superuser>) ALL **Database:** No individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application. If required, user can be assigned sdpuser priviledge through /etc/sudoers file: <username> ALL=(sdpuser) ALL **Application:** Select Authority in the Sys admin menu, then select the Users tab to assign appropriate roles to a user.
NA	APPL				MoP Work Package tag: WP005_v3 **OS:** To set account lockout threshold, in the /etc/pam.d/system-auth and /etc/pam.d/password-auth files, set the parameter deny=<value>, unlock_time=<value>. Note: The <value> should correspond to the MTN Security Baseline values. **Application:** Select Authority in the Sys admin menu, then select the General tab. Set Max failed logins parameter to <value>. Note: The <value> should correspond to the MTN Security Baseline values

NA	APPL					MoP Work Package tag: WP006_v3 **OS:** If NFS service is running on node, check that NFS shares are properly configured: cat /etc/exports To export In /etc/exports file, define NFS shares as: <directory to export> <client IP> (permissions/options) Then restart NFS service. On client run: mount <NFS_Server_IP>:/<NFS Share> <mountpoint>
NA	APPL					MoP Work Package tag: WP007_v3 **OS:** To restrict concurrent unauthenticated user access the following parameters should be set in the /etc/ssh/sshd_config file: MaxSessions <value> MaxStartups <value> MaxAuthTries <value> If any changes are made, the sshd service should be restarted: service sshd restart Note: The <value> should correspond to the MTN Security Baseline values
NA	APPL					MoP Work Package tag: WP008_v3 **OS:** A Pre-rquisite to implement this WP is the follwing: There needs to be a Central Unix Server from where user needs to login to the related IN Node (e.g SDP , AIR etc). Individual user account would be created on the Central Server and SSH keys for that User would be created (generated) as per Procedure, for this user and transferred to the same user home dir in the corresponding node e.g SDP , AIR etc Verify that SSH encryption keys have been generated for UNIX/Linux user, and used to login for user authentication: cat /home/<user>/.ssh/authorized_keys Refer to instructions in MoP for details on how to set up SSH key based authentication.

NA	APPL					MoP Work Package tag: WP009_v3 **OS:** Verify that default inacivity period is set in /etc/default/useradd : INACTIVE=<value> For existing users verify inactivity settings with: `chage -l <username>` To check the last login time for each user: last | grep <username> To disable user after <value> days: `chage -I` <value> <user> To delete user: userdel --remove <user_name> To lock inactive user: `passwd -l` <username> Note: The <value> should correspond to the MTN Security Baseline values. **Application:** To remove inactive user, select Authority in the Sys admin menu, select a user
APPL	NA					MoP Work Package tag: WP010_v3 **Database:** TimesTen is running in embedded mode and connecting directly to DB over network is not possible. Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions . However, TimesTen support human interaction using system account i.e. sdpuser or root, internal/external identified individual users. Only root and sdpuser are to have, and must have, access to the database application.
APPL	NA					MoP Work Package tag: WP011_v3 **Database:** Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions . However, TimesTen support human interaction using system account i.e. sdpuser or root, internal/external identified individual users. Only root and sdpuser are to have, and must have, access to the database application.

NA	APPL					MoP Work Package tag: WP012_v3 **OS:** To display password status information of a user, use "-S" option in passwd command. passwd -S <username> If required, password can be changed using the below command passwd <user_name> **Database:** Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions . However, TimesTen support human interaction using system account i.e. sdpuser or root, internal/external identified individual users. Only root and sdpuser are to have, and must have, access to the database application. **Application:** To change password, select Authority in the Sys admin menu, select a user from the Users tab, then enter a strong password in the password fields.
NA	APPL					MoP Work Package tag: WP013_v3 **OS:** To display password status information of a user, use "-S" option in passwd command. passwd -S <username> If required, password can be changed using the below command passwd <user_name> **Database:** TimesTen uses OS Layer authentication. **Application:** To change password, select Authority in the Sys admin menu, select a user from the Users tab, then enter a strong password in the password fields.

NA	APPL					MoP Work Package tag: WP016_v3 **OS:** To set password restriction the following parameters should be set in the /etc/login.defs file: PASS_MAX_DAYS <value> PASS_MIN_DAYS <value> PASS_WARN_AGE <value> To set password restriction the following parameters should be set in the /etc/pam.d/system-auth and /etc/pam.d/password-auth files: password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=<value> Note: The <value> should correspond to the MTN Security Baseline values. Application: Select Authority in the Sys admin menu, then select the General tab. Set Password valid to <value>. Note: The <value> should correspond to the MTN Security Baseline values.
NA	APPL					MoP Work Package tag: WP017_v3 **OS:** To set password complexity the following parameter should be set in the /etc/pam.d/system-auth and /etc/pam.d/password-auth files: password requisite pam_cracklib.so try_first_pass retry=<value> difok=<value> ocredit=<value> dcredit=<value> ucredit=<value> lcredit=<value> minlen=<value> Note: The <value> should correspond to the MTN Security Baseline values. **Application:** Select Authority in the Sys admin menu, then select the General tab. Enable and set Strict password Configuration

NA	APPL					MoP Work Package tag: WP018_v3 **OS:** To set password expiry the following parameters should be set in the /etc/login.defs file: PASS_MAX_DAYS <value> PASS_MIN_DAYS <value> PASS_WARN_AGE <value> To set password expiry the following parameters should be set in the /etc/pam.d/system-auth and /etc/pam.d/password-auth files: password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=<value> To set password expiry period for existing non-system user chage --maxdays <value> <username> Note: The <value> should correspond to the MTN Security Baseline values. **Application:** Select Authority in the Sys admin menu, then select the General tab. Set Password valid to <value>.
NA	APPL					MoP Work Package tag: WP019_v3 **OS:** To set password complexity the following parameter should be set in the /etc/pam.d/system-auth and /etc/pam.d/password-auth files: password requisite pam_cracklib.so try_first_pass retry=<value> difok=<value> ocredit=<value> dcredit=<value> ucredit=<value> lcredit=<value> minlen=<value> Note: The <value> should correspond to the MTN Security Baseline values. **Application:** Select Authority in the Sys admin menu, then select the General tab. Enable and set Strict password Configuration.
NA	APPL					MoP Work Package tag: WP045_v3 **OS:** Snapshot and Subscriber Dump Tools tools are executed only by sdpuser or root. So, the appropriate roles of sdpuser or root should only be provided to pre-defined users. Roles can be assigned in the /etc/sudoers file (see WP004_v3)

NA	APPL				MoP Work Package tag: WP21_v3 **OS:** To check which services are running: chkconfig --list To disable the service use: chkconfig <service_name> off Furthermore OS Services running in this node and their status are conform with corresponding version of CIS Red Hat Enterprise Linux 6.X / 7.X Benchmark (Chapter 2 Services). Meaning, unsecured and unused services are disabled by default, except for those which are used by the application (business need), like "echo" service for FDS application
NA	APPL				MoP Work Package tag: WP21bis_v3 **OS:** To set SSH Session Timeout the following parameters should be set in the /etc/ssh/sshd_config file: ClientAliveInterval <value> ClientAliveCountMax <value> If any changes are made, the sshd service should be restarted: service sshd restart Note: The <value> should correspond to the MTN Security Baseline values.
NA	APPL				MoP Work Package tag: WP22_v3 **OS:** To disable Anonymous FTP Login the following parameter should be set in the /etc/vsftpd/vsftpd.conf file: anonymous_enable=NO If any changes are made, the vsftpd service should be restarted: service vsftpd restart
NA	APPL				MoP Work Package tag: WP22bis_v3 **OS:** To set X11 Protocol Forwarding the following parameter should be set in the /etc/ssh/sshd_config file: X11Forwarding yes If any changes are made, the sshd service should be restarted: service sshd restart

NA	APPL				MoP Work Package tag: WP23_v3 OS: To check which services are running: chkconfig --list To disable the service use: chkconfig <service_name> off Furthermore OS Services running in this node and their status are conform with corresponding version of CIS Red Hat Enterprise Linux 6.X / 7.X Benchmark (Chapter 2 Services). Meaning, unsecured and unused services are disabled by default, except for those which are used by the application (business need), like "echo" service for FDS application
NA	APPL				MoP Work Package tag: WP25_v3 **OS:** To enable stack protection the following parameter should be set in the /etc/sysctl.conf file: kernel.exec-shield = 1 If any changes are made, a restart of the server is required.
NA	APPL				MoP Work Package tag: WP26_v3 **OS:** Note: Customer is expected to provide the list of the Network segments which must connect to the system/IN Node via which Network Service. To configure TCP Wrappers add the IP addresses* of allowed hosts in the file /etc/hosts.allow and set ALL:ALL in /etc/hosts.deny. *Format: ALL: <net>/<mask>, <net>/<mask>, …
NA	APPL				MoP Work Package tag: WP28_v3 OS: To fix this remove the files as below if they exist: rm /var/apache/cgi-bin/printenv rm /var/apache/cgi-bin/test-cgi

NA	APPL					MoP Work Package tag: WP029_v3 **OS:** Verify that the banner provided by the customer is included in the following files: /etc/issue /etc/motd Verify that /etc/ssh/sshd_config file includes following entry: banner /etc/issue if FTP is used, verify that /etc/vsftpd.conf includes the following entry: ftpd_banner=<banner_text> or alternatively that /etc/vsftpd.conf includes: banner_file=<path/to/banner/file> and that the specified banner_file above contains the banner provided by the customer.
NA	APPL					MoP Work Package tag: WP030_v3 **OS:** update the /etc/sma/snmp/snmpd.conf file as below: rocommunity <strong strings> rwcommunity <strong strings> Restart the snmpd daemon using following command: /etc/init.d/init.sma start If ESA is selected change community strings in /opt/esa/conf/communityCfg.xml file To disable SNMP v1 and v2 comment or delete following lines in /etc/sma/snmp/snmpd.conf file: com2sec local default [<read-write_community>] com2sec network default [<read-only_community>] NOTE: Community strings in the OSS and in the ESA must be identical
NA	APPL					MoP Work Package tag: WP046_v3 **OS:** To disable TRACE HTTP verb in Apache the following parameter should be set in the /etc/httpd/conf/httpd.conf file: TraceEnable off

NA	APPL				MoP Work Package tag: WP047_v3 **OS:** To set cipher suite the following parameters should be set in the /etc/httpd/conf.d/ssl.conf file: SSLHonorCipherOrder On SSLCipherSuite HIGH:!MEDIUM:!NULL:!MD5 If any changes are made, the httpd service should be restarted: service httpd restart
NA	APPL				MoP Work Package tag: WP048_v3 **OS:** To disable SSLv2, SSLv3 and TLSv1, the following parameters should be set in the /etc/httpd/conf.d/ssl.conf file: SSLProtocol all -SSLv2 -SSLv3 -TLSV1 If any changes are made, the httpd service should be restarted: service httpd restart Note: Make sure to check that TLSv1.1 and/or TLSv1.2 are available for node before before disabling TLSv1.
NA	APPL				MoP Work Package tag: WP49_v3 **OS:** Taken care during ICP Upgrade
NA	APPL				MoP Work Package tag: WP050_v3 **OS:** To disable SSH Weak CBC Mode Ciphers the following parameters should be set in the /etc/ssh/sshd_config file: Ciphers aes128-ctr,aes192-ctr,aes256-ctr MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160 If any changes are made, the sshd service should be restarted: service sshd restart

NA	APPL				MoP Work Package tag: WP051_v3 **OS:** IMPORTANT! This WP is informational and requires NO action unless root password has been lost. For instructions on how to recover/reset the root password refer to instructions in Common Linux MOP.
APPL	APPL				MoP Work Package tag: WP35_v3 **OS:** Verify that system auditing is enabled: auditctl -s List all loaded audit rules auditctl –l Verify that the rules from /usr/share/doc/audit-2.2/stig.rules as well as the following rules are loaded: -w /var/log/audit -w /etc/audit/auditd.conf -w /etc/audit/audit.rules If reconfiguration is required, refer to instruction in MoP for further detail. Database: Audit logging for SDP TimesTen database is active by default, audit logfile stored under the path /var/log/ttlog. Application: 1. Go to the Authority Window, Audit Schema Tab. 2. Click on Create button to create a new schema if not created. 3. Select the schema name from the drop down menu and right click on the schema name and create a MO. To view the generated audit log, select Authority in the Sys admin menu, then select the Audit Log tab

NA	APPL					MoP Work Package tag: WP38_v3 **OS:** Update the /etc/login.defs file with the following entry: FAILLOG_ENAB yes The file /etc/audit/audit.rules should have the following entries. -w /var/log/faillog -p wa -k logins -w /var/log/lastlog -p wa -k logins -w /var/log/tallylog -p wa -k logins -w /var/run/faillock -p wa -k logins To verify that the rules have been loaded, run: auditctl -l | egrep -i "faillock|lastlog|tallylog|sudoers" If reconfiguration is required, refer to instructions in MoP for further detail
NA	APPL					MoP Work Package tag: WP39_v3 **OS:** The following files should have read and write permission only for the superuser: ls -ld /var/log/audit/audit.log ls -ld /var/log/faillog ls -ld /var/log/ttlog ls -ld /var/opt/fds/logs/audit If not, refer to instructions in MoP for further detail

NA	APPL				MoP Work Package tag: WP40_v3 To set up remote logging, the following configuration should be set in the /etc/rsyslog.conf file: *.* @<remote>:514 where <remote> is the remote server IP. To enable remote audit logging, the following parameters in the /etc/audisp/plugins.d/syslog.conf file should be set: active = yes direction = out path = builtin_syslog type = builtin args = LOG_INFO format = string If reconfiguration is required, refer to MoP for detailed instructions. Note: Make sure remote server is properly configured
NA	APPL				MoP Work Package tag: WP41_v3 To fix this edit(VI) the file /etc/mail/sendmail.cf and set the parameter PrivacyOptions as below: O PrivacyOptions=authwarnings,goaway,restrictmailq,restrictqrun
NA	APPL				MoP Work Package tag: WP42_v3 **For Apache:** Verify that the following parameters are set in the /etc/apache/httpd.conf file: ServerSignature Off ServerTokens Prod **For SMTP** To prevent SMTP version disclosure the following parameter should be set in the /etc/mail/sendmail.cf file: SmtpGreetingMessage=$j If any changes are made, the SMTP service should be restarted: service sendmail restart
APPL	NA				MoP Work Package tag: WP43_v3 Taken care during ICP Upgrade

NA	APPL				MoP Work Package tag: WP44_v3 Taken care during ICP Upgrade
NA	APPL				MoP Work Package tag: WP34_v3 To check status of iptables: service iptables status If reconfiguration is required, refer to MOP for detailed instructions.
NA	APPL				MoP Work Package tag: WP52v3 **OS:** Take screenshots of ls -l /var/log/secure ls -l /var/log/audit/audit.log ls -l /var/run/faillock ls -l /var/log/messages ls -l /var/log/lastlog ls -l /var/log | grep -i ttlog cat /etc/ssh/sshd_config| grep -i PermitRootLogin crontab -l more /etc/issue more /etc/motd more /etc/ftpd/banner.msg cat /etc/sudoers cat /etc/group cat /etc/passwd
NA	APPL				MoP Work Package tag: WP53_v3 **OS:** Take screenshots of /etc/passwd /etc/shadow
APPL	APPL				MoP Work Package tag: WP54_v3 SIEM tool needs to be implemented
APPL	APPL				MoP Work Package tag: WP55_v3 Vulnerability Scanner has to be run .

MTN Ghana Charging Security Baseline - Compliance Checklist Final

APPL	APPL					MoP Work Package tag: WPAddCompl_v3 Ericsson Security Manager (ESM) Product which provides a Security Compliance and Monitoring tool to help automate checklist serial of tasks intended to be performed regularly.