Actions Taken	SafeConsole Audit Output	Splunk Log Output
Device Password Reset Email	{"serial":"000FFEC697CDB260800060B9","cn":"domain.local/SC_SPLUNK\\\\admin","hwid":"230A154F","key":"Gg6fFikeWQHiAZ2j1Q6/RQ==","email":"kLastname@Domain.com","status":"IN_USE"}	{"severity":"DEBUG","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-1","message":"log: ADMIN {admin=[kLastname+helpdesk@Domain.com], action[password_reset_success], ip_address[x.x.x.x91], data=[{\"name\":\"kLastname+helpdesk@Domain.com\",\"email\":\"kLastname+helpdesk@Domain.com\"}]}"}
Device Changed Owner	{"serial":"000FFEC697CDB260800060B9","new_user_cn":"domain.local/Test","old_user_cn":"domain.local/SC_SPLUNK\\\\admin"}	{"severity":"DEBUG","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-3","message":"log: ADMIN {admin=[admin], action[change_safestick_owner], ip_address[x.x.x.x91], data=[{\"serial\":\"78E7D1C280DDB260800056BE\",\"new_user_cn\":\"test/TESTSPLUNK\",\"old_user_cn\":\"domain.local/SC_SPLUNK\\\\admin\"}]}"}
Device Status Change : Lost	{"safestick_list":[{"safeStickStatus":"LOST","serial":"78E7D1C280DDB260800056BE"}]}	{"severity":"TRACE","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-4","message":"log: ADMIN getPreparedStatement: org.hsqldb.jdbc.JDBCPreparedStatement@142f0be[sql=[insert into admin_logentry(action, data, time, user_name, last_ip) values(?, ?, now(), ?, ?)], parameters=[[set_safestick_status], [{\"safestick_list\":[{\"safeStickStatus\":\"LOST\",\"serial\":\"78E7D1C280DDB260800056BE\"}]}], [admin], [xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx]]]"}
Device Status Change: Denied	{"safestick_list":[{"safeStickStatus":"DENIED_ACCESS","serial":"78E7D1C280DDB260800056BE"}]}	{"severity":"TRACE","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-3","message":"log: ADMIN getPreparedStatement: org.hsqldb.jdbc.JDBCPreparedStatement@12ef5e2[sql=[insert into admin_logentry(action, data, time, user_name, last_ip) values(?, ?, now(), ?, ?)], parameters=[[set_safestick_status], [{\"safestick_list\":[{\"safeStickStatus\":\"DENIED_ACCESS\",\"serial\":\"78E7D1C280DDB260800056BE\"}]}], [admin], [xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx]]]"}
Device Status Change: Waiting to be reset	{"safestick_list":[{"safeStickStatus":"RESET_PENDING","serial":"000FFEC697CDB260800060B9"}]}	{"severity":"DEBUG","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-3","message":"log: ADMIN {admin=[admin], action[set_safestick_status], ip_address[xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx], data=[{\"safestick_list\":[{\"safeStickStatus\":\"RESET_PENDING\",\"serial\":\"000FFEC697CDB260800060B9\"}]}]}"}
Device Status Change: Deleted	{"endpoint":{"owner":"domain.local/SC_SPLUNK\\\\admin","safeStickStatus":"RESET_PENDING","lastUsed":"2019-11-21T11:53:07-06:00","serialBarcode":"78E7D1C280DDB260800056BE","hasRecoveryCode":true,"serial":"78E7D1C280DDB260800056BE","hardwareID":"230A154F","lastIP":"x.x.x.x163","isUpdated":true,"isOnline":false,"version":"6.2.0","geolocation":{}}}	{"severity":"DEBUG","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-3","message":"log: ADMIN {admin=[admin], action[device_delete], ip_address[xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx], data=[{\"endpoint\":{\"owner\":\"domain.local/SC_SPLUNK\\\\admin\",\"safeStickStatus\":\"RESET_PENDING\",\"lastUsed\":\"2019-11-21T11:53:07-06:00\",\"serialBarcode\":\"78E7D1C280DDB260800056BE\",\"hasRecoveryCode\":true,\"serial\":\"78E7D1C280DDB260800056BE\",\"hardwareID\":\"230A154F\",\"lastIP\":\"x.x.x.x163\",\"isUpdated\":true,\"isOnline\":false,\"version\":\"6.2.0\",\"geolocation\":{}}}]}"}
Admin login success	{"last_ip":"xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx","realm":"UserDatabaseRealm"}	{"severity":"TRACE","logger":"com.blockmaster.safeconsole.rest.resources.RESTDevice","thread":"http-443-5","message":"recordLog: Received log line: {\"type\":\"login\",\"time\":\"2019-11-21T19:46:11+00:00\",\"user\":\"domain.local/SC_SPLUNK\\admin\",\"login\":\"Domain.loc/Tech/test-Testing/USERPATH\",\"computer\":\"Computername\",\"data\":{\"space_total\":\"4194304\", \"space_used\":\"1024\", \"computerOS\":\"Windows 10 Ent | Windows Admin\"}}"}
Admin login fail	{"last_ip":"xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx","realm":"JDBCRealm"}	
Admin Password Recovery	{"name":"kLastname+helpdesk@Domain.com","email":"kLastname+helpdesk@Domain.com"}	{"severity":"TRACE","logger":"com.blockmaster.console.entities.module.MpwdModule","thread":"http-443-5","message":"moduleJSON [{\"recoverySubject\":\"SafeConsole Password reset for {owner.name} ({device.serial})\",\"isDefault\":false,\"restricted\":false,\"certificate\":\"34ed04fce4bc605b603af3128dcfab359ca46d4f905e0db2d7b35e93c6e919ff\",\"certificateName\":\"password recovery certificate\",\"supportTelephone\":\"\",\"id\":49,\"supportEMail\":\"johnb@Domain.com\",\"queryEMail\":true,\"enabled\":true}]"}
Admin Saved Server settings	{"data":{"country":"CA","city":"Division No. 19","latitude":XXXXXXX,"action":"add","ip_address":"0.0.0.0","region":"Manitoba","longitude":xxxxxxxxx},"key":"geolocation"}	{"severity":"DEBUG","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-2","message":"log: ADMIN {admin=[admin], action[save_server_setting], ip_address[xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx], data=[{\"data\":{\"location\":\"ini\",\"value\":\"[\\\"admin\\\"]\",\"enabled\":false},\"key\":\"dismiss_releasenotes_users_5500\"}]}"}
Admin Saved Policy Config	{"policy":[{"policy":18},{"autorun":19},{"gui":20},{"aboutme":21},{"fblocker":22},{"logger":23},{"mpwd":24},{"timer":25},{"wprotect":26},{"lost":27},{"flogger":28},{"menu":29},{"console":30},{"zone":31},{"geofence":32},{"antivirus":33},{"portblocker":34},{"standalone":35},{"cpanel":36},{"login":37},{"trustzone":38}]}	{"severity":"DEBUG","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-6","message":"log: ADMIN {admin=[admin], action[save_configuration], ip_address[xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx], data=[{\"ou\":-1,\"policy\":[{\"policy\":1},{\"autorun\":2},{\"gui\":3},{\"aboutme\":4},{\"fblocker\":5},{\"logger\":6},{\"mpwd\":7},{\"timer\":8},{\"wprotect\":9},{\"lost\":10},{\"flogger\":11},{\"menu\":12},{\"console\":13},{\"zone\":14},{\"geofence\":15},{\"antivirus\":16},{\"portblocker\":39},{\"standalone\":40},{\"cpanel\":41},{\"login\":42},{\"trustzone\":17}]}]}"}
Admin Add New Admin	{"oupath":"domain.local","email":"kLastname+test@gmail.com","username":"Test"}	{"severity":"DEBUG","logger":"com.blockmaster.console.handlers.LogHandler","thread":"http-443-6","message":"log: ADMIN {admin=[admin], action[add_user], ip_address[xxxx:x:x:x:xxxx:xxxx:xxxx:xxxx], data=[{\"oupath\":\"domain.local\",\"email\":\"kLastname+test@gmail.com\",\"username\":\"Test\"}]}"}