OCF “Gaborone-1” – List of Auditable Events – Security WG CR 3150

13.20 List of Auditable Events

Whenever a Device detects an occurrence of any of the Auditable Events in Table XX, then the Device shall log an AEE using the corresponding "category", "priority" and "auxiliaryinfo" Properties defined in Table XX. The "auxiliaryinfo" Property shall contain the entries in the "auxiliaryinfo" column of Table XX in the order specified in the table with each bullet contained in a separate array entry. The "auxiliaryinfo" Property may contain additional entries for further information following the entries for mandatory information. The "aeid" Property shall include the corresponding Auditable Event Identifier from Table XX.

Table XX List of mandatory Auditable Events and corresponding Property values

Auditable Event Identifier ("aeid")	Auditable Event Description	Example "message"	"category"	"priority"	"auxiliaryinfo"
AC-1	A Device received a request from an authenticated Client with valid URI path, valid interface and valid operation for that resource, but for which access was denied.	"Access Denied"	0x01 (Access Control)	2 (WARN)	• Client IP address & port in format [xxxx:..:xxxx]:xxxx • Client UUID in UUID format (e.g. "00000000-0000-0000-0000-000000000000") • Resource URI (e.g. "/oic/sec/ael") • Requested CRUDN operation (e.g. "CREATE") • Server security state (e.g. "RFNOP") • Asserted roles by Client (e.g. "oic.role.owner"), or "No roles asserted" if there are none
AUTH-1	The Device encountered an error during a DTLS handshaking procedure due to a credential validation failure.	"DTLS handshake failed due to a credential validation failure"	0x08 (Authentication)	1 (ERR)	• Client IP address & port in format [xxxx:..:xxxx]:xxxx •
COMM-1	The Device received a CoAP request which contained unexpected /unsupported CoAP header parameters or unexpected/unsupported CoAP options.	"Unexpected CoAP Command"	0x40 (COMM)	2 (WARN)	• Client IP address & port in format [xxxx:..:xxxx]:xxxx • Hex-encoded CoAP header in format [xx:xx:xx:xx] • Hex-encoded CoAP options except payload (empty if not present)

Whenever a Device detects an occurrence of any of the Auditable Events in Table YY, then the Device should log an AEE using the corresponding "category", "priority" and "auxiliaryinfo" Properties defined in Table YY. The "auxiliaryinfo" Property shall contain the entries in the "auxiliaryinfo" column of Table YY in the order specified in the table with each bullet contained in a separate array entry. The "auxiliaryinfo" Property may contain additional entries for further information following the entries for mandatory information. The "aeid" Property shall include the corresponding Auditable Event Identifier from Table YY.

Table YY List of recommended Auditable Events and corresponding Property values

Auditable Event	Auditable Event Description	Example "message"	"category"	"priority"	"auxiliaryinfo"

Identifier					
SVR-1	The Device's attempted to use one of its credentials, and detected that the credential is expired	“My credential is expired”	0x10 (SVR Modification)	2 (WARN)	• credid • Credential expiration value
SVR-2	The Device could not validate the role certificate being asserted	"Role assertion failed"	0x10 (SVR Modification)	2 (WARN)	• Client IP address & port in format [xxxx:...:xxxx]:xxxx