



SIEM EVENT CATALOG

SIEM EVENT ID MAPPING REFERENCE

1. HOW TO READ THIS CATALOG

Smart Squad writes one JSON document per security event to the `ss_Security` channel on each application server. On hosted / shared servers, the same JSON document is also sent to the owning agency's HTTPS endpoint (section 7). The Windows Event Log entry and the JSON payload map as follows:

EVENT LOG PROPERTY	VALUE
Log (channel)	<code>ss_Security</code>
Source	<code>ss_Security</code>
Event ID	The catalog event ID (<code>event.id</code> in the JSON)
Level	Derived from <code>event.severity</code> (section 2)
Message	The JSON document

- **event.id is the wire-stable key.** Build parsers and detection rules on the ID; `event.name` is the human-readable label and may be extended in future releases.
- **New events are always added under new IDs.** Existing IDs never change meaning.
- Every event carries `@timestamp` (UTC, millisecond precision), `event`, `actor`, `action` and `source`. `subject`, `details`, `session_id` and `correlation_id` appear where the event has them.
- **Every event carries `event.uid` (2.9.5)**, a GUID unique to that occurrence. `event.id` says what kind of event it is; `event.uid` says which one. HTTPS push is delivered at least once, so remove duplicates on `event.uid`. The same occurrence has the same `event.uid` in the Event Log and in HTTPS push.
- Events emitted by the Processor service have no `actor.ip` or `actor.user_agent` because they are not tied to an HTTP request.

EVENT ID RANGES

RANGE	CATEGORY	EVENT.CATEGORY	STATUS
1000-1999	Authentication	<code>authentication</code>	In use
2000-2999	Authorization decisions	-	Reserved
3000-3999	Data read	<code>data_read</code>	In use
4000-4999	Data modification	<code>data_modification</code>	In use
5000-5999	Administration	<code>admin</code>	In use
6000-6999	System / health	-	Reserved
7000-7999	Files / attachments	-	Reserved
8000-8999	External integrations	-	Reserved
9000-9999	Unallocated	-	Reserved

2. SEVERITY LEVELS

`event.severity` is the authoritative severity. The Windows Event Log Level is derived from it so channel-level filtering works, but SIEM rules should key off the JSON value.

EVENT.SEVERITY	WINDOWS EVENT LOG LEVEL	USED FOR
info	Information (4)	Routine activity: successful sign-in, record viewed or saved, MFA challenge
low	Warning (2)	Sensitive reads and notable changes: person, vehicle and face queries, search audit, scan hand-off collected, ticket cancelled, configuration changed, forced logoff
medium	Warning (2)	Failed authentication attempts, refused scan hand-offs, and administrative changes to accounts, roles and Smart Draft prompts
high	Error (1)	Account lockout
critical	Error (1)	Reserved; no event uses this level in this release

3. OUTCOMES AND REASON CODES

EVENT.OUTCOME	MEANING
success	The action completed. Used by every non-failure event.
failure	The action was attempted and rejected. Carries event.reason. Used by 1002 and 1012.
denied	The action was refused by policy. Carries event.reason. Used by 1003 (lockout) and 3009 (scan hand-off refused).
unknown	Reserved; not used in this release.

`event.reason` is a structured code so rules can threshold without parsing free text:

EVENT.REASON	EVENT	MEANING
invalid_credentials	1002	Login ID or credential rejected (all credential types), or a rejected one-time password counted as a failed login.
invalid_otp	1012	One-time password did not match.
max_failed_attempts	1003	Consecutive failures reached the lockout threshold.
USER	1004	User signed out.
forced:ADMIN	1004	Administrator forced the session off.
forced:TIMEOUT	1004	Idle-session sweep ended the session (Processor).
forced:DISABLED	1004	The account was disabled (administrator, bulk import archive, or the inactivity sweep) and its open sessions were ended.
inactivity	5004	The Processor inactivity sweep disabled an account not used within the agency threshold.

EVENT.REASON	EVENT	MEANING
not_found, agency_mismatch, user_mismatch, device_mismatch, expired	3009	Scan hand-off refused: no such transfer; it belongs to another agency, user or device; or it has expired.

4. EMITTING COMPONENTS

COMPONENT	PROCESS	SOURCE.APP	EVENTS
Smart Squad web application	SmartSquad.Service (IIS worker process)	SmartSquad.Service	All authentication, data read, data modification and administration events. With HTTPS push, it also queues each agency's events.
Smart Squad Processor	SmartSquad.Processor (Windows service)	SmartSquad.Processor	1004 with reason forced:TIMEOUT (idle-session sweep); 5004 with reason inactivity, preceded by 1004 forced:DISABLED (inactivity sweep); 4002 for note entries committed by autosave. These events have no ip or user_agent because there is no HTTP request. With HTTPS push, the Processor also sends every agency's queued events.
CPIC / PIP / MPI query gateways	SmartSquad.CPIC, SmartSquad.PIP, SmartSquad.MPI (IIS)	per_gateway	Optional. Queries are always written to the database Search Audit; emitting 3008 to SS_Security from these hosts is enabled by adding the same Siem.* settings to each gateway configuration and registering the channel on that host.
RMS / CAD / DEMS connector hosts	Niche, Axon, Hexagon, IRS, ReportExec (Windows services)	-	Do not write to SS_Security. They log application exceptions to their own operational channels only.
Smart Squad Deployer (Faction Four tool)	SmartSquad.Deployer, run by Faction Four operators	SmartSquad.Deployer	5090 siem.test only, queued for one agency's HTTPS push during onboarding and sent by the Processor. Never written to SS_Security.

Each event carries `source.host` and `source.app`, so one channel subscription covers every server. In multi-server deployments, collect `ss_security` from every web server and from the Processor server. With HTTPS push, the web application and the Processor queue each agency's events, and the Processor sends them.

5. EVENT CATALOG

45 events are emitted in Smart Squad 2.9.5; 12 IDs are defined and reserved for future use. "Web" = Smart Squad web application, "Processor" = Smart Squad Processor service, "Deployer" = the Faction Four Deployer tool (5090 only).

AUTHENTICATION (1000-1999)

Mapping

EVENT ID	EVENT NAME	SEVERITY	EVENT LOG LEVEL	OUTCOME	REASON CODES	EMITTED BY	STATUS
1001	auth.login.success	info	Information	success	-	Web	EMITTED
1002	auth.login.failure	medium	Warning	failure	invalid_credentials	Web	EMITTED
1003	auth.login.lockout	high	Error	denied	max_failed_attempts	Web	EMITTED
1004	auth.logout	info (USER), low (forced)	Information / Warning	success	USER forced:ADMIN forced:TIMEOUT forced:DISABLED	Web, Processor	EMITTED
1005	auth.session.expired	-	-	-	-	-	RESERVED
1010	auth.mfa.challenge.issued	info	Information	success	-	Web	EMITTED
1011	auth.mfa.success	info	Information	success	-	Web	EMITTED
1012	auth.mfa.failure	medium	Warning	failure	invalid_otp	Web	EMITTED
1020	auth.password.change	-	-	-	-	-	RESERVED
1021	auth.password.reset.requested	info	Information	success	-	Web	EMITTED
1022	auth.password.reset.completed	info	Information	success	-	Web	EMITTED
1030	auth.token.issued	-	-	-	-	-	RESERVED
1031	auth.token.revoked	-	-	-	-	-	RESERVED
1040	auth.cert.issued	-	-	-	-	-	RESERVED
1041	auth.cert.revoked	-	-	-	-	-	RESERVED
1050	auth.sso.success	-	-	-	-	-	RESERVED
1051	auth.sso.failure	-	-	-	-	-	RESERVED

Detail

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
1001	Successful sign-in on any credential type (Smart Squad local, Active Directory, Microsoft Entra ID, device certificate). The actor carries user_id, username, agency_id, device_id, ip and user_agent.	login	(none; actor only)	-

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
1002	Failed sign-in attempt on any credential type, including a disabled account on password sign-in, an unregistered device, and a failed device, OTP, NFC, biometric or wearable verification. Also raised after a rejected one-time password (following 1012), because a rejected OTP counts as a failed login. actor.user_id is present when the login ID matches an account. Not reported: expired passwords, unknown login IDs and licence failures. A device-certificate sign-in with user credentials can emit 1002 immediately before its 1001.	login	(none; actor only)	-
1003	Sign-in attempt refused because consecutive failures reached the agency lockout threshold. Emitted on every refused attempt while the account stays locked, not once. The account stays locked until an administrator resets it, and an alert email goes to the agency security contact. actor.username carries the login ID (the internal user ID for device-certificate sign-ins).	login	(none; actor only)	-
1004	Session ended. USER = the user signed out, or an earlier session on the same device was closed at sign-in (web application). forced:ADMIN = an administrator forced the session off from the Current Users screen (web application). forced:TIMEOUT = the idle-session sweep ended the session (Processor). forced:DISABLED = the account was disabled and each open session was ended: by an administrator or a bulk user import that archives the account (web application), or by the inactivity sweep (Processor). actor.username carries the internal user ID, not the login ID.	logout	(none; session_id set)	-
1005	Not emitted in this release. Idle expiry is reported as 1004 with reason forced:TIMEOUT.	-	-	-
1010	One-time password generated and sent for a device or session that requires multi-factor authentication. actor.device_id identifies the device.	mfa_challenge	(none; actor only)	method (user OTP delivery: CELL, EMAIL or ALL)
1011	One-time password accepted.	mfa_verify	(none; actor only)	method = OTP
1012	One-time password rejected. Followed by 1002 for the same login ID.	mfa_verify	(none; actor only)	method = OTP attempts
1020	Not emitted in this release. Password changes completed through the reset flow are reported as 1022.	-	-	-
1021	Password reset (forgot password) request created; a reset link is emailed to the user.	password_reset_request	user	-
1022	Password changed through a reset link.	password_reset_complete	user	-
1030	Not emitted in this release.	-	-	-

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
1031	Not emitted in this release.	-	-	-
1040	Not emitted in this release. Device-certificate sign-ins are reported through 1001 / 1002.	-	-	-
1041	Not emitted in this release.	-	-	-
1050	Not emitted in this release. Entra ID and Active Directory sign-ins are reported through 1001 / 1002.	-	-	-
1051	Not emitted in this release. See 1050.	-	-	-

DATA READ (3000-3999)

Mapping

EVENT ID	EVENT NAME	SEVERITY	EVENT LOG LEVEL	OUTCOME	REASON CODES	EMITTED BY	STATUS
3001	data.note.viewed	info	Information	success	-	Web	EMITTED
3002	data.report.viewed	info	Information	success	-	Web	EMITTED
3003	data.ticket.viewed	info	Information	success	-	Web	EMITTED
3004	data.person.queried	low	Warning	success	-	Web	EMITTED
3005	data.vehicle.queried	low	Warning	success	-	Web	EMITTED
3006	data.intel.viewed	info	Information	success	-	Web	EMITTED
3007	data.face.searched	low	Warning	success	-	Web	EMITTED
3008	DataSearchAudited *	low	Warning	success	-	Web (CPIC/PIP/MPI gateways optional)	EMITTED
3009	data.scan.retrieved	low (success), medium (denied)	Warning	success, denied	not_found agency_mismatch user_mismatch device_mismatch expired	Web	EMITTED

* 3008: This event reports its name as DataSearchAudited rather than in the dotted convention used by the other events. Filter on the event ID.

Detail

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
3001	Note opened for viewing (mirrors the note access audit).	view	note	-

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
3002	Report loaded for viewing, from Smart Squad or from the RMS.	view	report	format (HTM, PDF)
3003	Ticket viewed or printed.	view print	ticket	-
3004	Person query sent to the RMS: criteria search, single-record retrieval, or batch retrieval by candidate IDs (for example after a face match). Search criteria are not logged.	search get search_by_ids	person (id set for get only)	id_count (search_by_ids)
3005	Vehicle or plate query sent to the RMS. Search criteria are not logged.	search get	vehicle (id set for get only)	-
3006	Intel posting viewed. Also the default classification for intel activity that is not a create or update (posting archived, RMS link removed, attachment added); the raw verb is preserved in action.	raw intel audit verb, e.g. View Posting - {officer}	intel_posting	-
3007	Facial recognition search executed. The probe image and candidate records are never logged.	search	face_search (face search record id)	source confidence_level candidate_count
3008	Every Smart Squad-originated search captured by the Search Audit: person, vehicle, business, location, occurrence, geographic area, note, ticket, form, transcription, virtual interview and face searches, plus CPIC, PIP and MPI queries when gateway emission is enabled, and every scan hand-off collection (search_type SCAN_RETRIEVAL, after each 3009). correlation_id links the event to the Search Audit record.	search	search_audit (Search Audit record id)	search_type destination
3009	Scan hand-off collected (2.9.5): a licence or other scan taken on the officer's mobile device is held on the server and collected by the officer's in-car device over its own session (Alert.asmx getScanResult). Emitted on every attempt: success when the row is returned and deleted; denied when the transfer does not exist, belongs to another agency or user, was requested by a different device, or has expired. The scan content is never logged. Each 3009 is followed by a 3008 (search_type SCAN_RETRIEVAL).	retrieve	scan_transfer (transfer id)	scan_transfer_id scan_type created_by_user_id created_utc device_id

DATA MODIFICATION (4000-4999)

Mapping

EVENT ID	EVENT NAME	SEVERITY	EVENT LOG LEVEL	OUTCOME	REASON CODES	EMITTED BY	STATUS
4001	data.note.created	info	Information	success	-	Web	EMITTED
4002	data.note.modified	info	Information	success	-	Web, Processor	EMITTED
4003	data.note.deleted	info	Information	success	-	Web	EMITTED

EVENT ID	EVENT NAME	SEVERITY	EVENT LOG LEVEL	OUTCOME	REASON CODES	EMITTED BY	STATUS
4004	data.note.locked	-	-	-	-	-	RESERVED
4005	data.note.unlocked	-	-	-	-	-	RESERVED
4010	data.report.submitted	info	Information	success	-	Web	EMITTED
4011	data.report.ai_activity	info	Information	success	-	Web	EMITTED
4012	data.report.exported	info	Information	success	-	Web	EMITTED
4020	data.ticket.created	info	Information	success	-	Web	EMITTED
4021	data.ticket.modified	-	-	-	-	-	RESERVED
4022	data.ticket.voided	low	Warning	success	-	Web	EMITTED
4030	data.intel.created	info	Information	success	-	Web	EMITTED
4031	data.intel.modified	info	Information	success	-	Web	EMITTED
4040	data.form.submitted	info	Information	success	-	Web	EMITTED
4041	data.form.modified	info	Information	success	-	Web	EMITTED

Detail

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
4001	New note created.	Create Note	note	activity link_id location
4002	Any audited change to a note that is not a create, delete, lock or unlock. Note exports and RMS/CAD linking are reported here with the verb in action. Entries committed by the autosave process are emitted by the Processor.	raw note audit verb: Add Note Entry Add Note Entry (from autosave) Update Note Title / Flag / Weather Add Attachment Update Attachment Link Note to RMS Record Link Note to CAD Call Export Note to Email / RMS / Folder / DEMS Note Reviewed Moved Attachment	note	activity link_id (entry or attachment id) location
4003	Deletion inside a note (attachment removed). Notes themselves are retained, never deleted.	Delete Attachment	note	activity link_id location
4004	Defined and mapped; no note activity in this release produces a lock verb.	-	-	-
4005	Defined and mapped; no note activity in this release produces an unlock verb.	-	-	-

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
4010	Report created or saved in Smart Squad and, when configured, in the RMS.	create update	report	rms_report_id (RMS-managed reports)
4011	AI-assisted action on a report (Smart Draft generation or Smart Review). Prompts, outputs and model parameters stay in the database.	SMART_DRAFT SMART_REVIEW	report	ai_activity_id occurrence_id entry_id activity_type
4012	Report PDF exported to the RMS, or a note change-history export produced.	export note_change_history. export	report (export) or note (change history)	occurrence_id (export) request_id, note_ owner_user_id (change history)
4020	Ticket created.	create	ticket	-
4021	Not emitted in this release. Ticket updates are recorded in the database ticket audit only.	-	-	-
4022	Ticket cancelled, or a cancellation reversed.	cancel uncancel	ticket	-
4030	Intel posting created, or an RMS record linked to a posting.	raw intel audit verb: Create Posting - {officer} create RMS link - {officer}	intel_posting	-
4031	Intel posting updated, or an RMS link changed.	raw intel audit verb: Update Posting - {officer} update RMS link - {officer}	intel_posting	-
4040	Form submission created, printed or exported. Viewing and record-linking are recorded in the database audit only.	submit print export_email export_rms export_folder	form_ submission	-
4041	Existing form submission saved.	save	form_ submission	-

ADMINISTRATION (5000-5999)

Mapping

EVENT ID	EVENT NAME	SEVERITY	EVENT LOG LEVEL	OUTCOME	REASON CODES	EMITTED BY	STATUS
5001	admin.user.created	medium	Warning	success	-	Web	EMITTED
5002	admin.user.modified	medium	Warning	success	-	Web	EMITTED
5003	admin.user.enabled	medium	Warning	success	-	Web	EMITTED

EVENT ID	EVENT NAME	SEVERITY	EVENT LOG LEVEL	OUTCOME	REASON CODES	EMITTED BY	STATUS
5004	admin.user.disabled	medium	Warning	success	inactivity	Web, Processor	EMITTED
5010	admin.config.changed	low	Warning	success	-	Web	EMITTED
5020	admin.agency.modified	-	-	-	-	-	RESERVED
5030	admin.smartdraft.prompt_ changed	medium	Warning	success	-	Web	EMITTED
5040	admin.role.created	medium	Warning	success	-	Web	EMITTED
5041	admin.role.modified	medium	Warning	success	-	Web	EMITTED
5042	admin.role.disabled	medium	Warning	success	-	Web	EMITTED
5043	admin.role.enabled	medium	Warning	success	-	Web	EMITTED
5044	admin.role.capability_ granted	medium	Warning	success	-	Web	EMITTED
5045	admin.role.capability_ revoked	medium	Warning	success	-	Web	EMITTED
5046	admin.user.role_assigned	medium	Warning	success	-	Web	EMITTED
5047	admin.user.role_removed	medium	Warning	success	-	Web	EMITTED
5090	siem.test	info	- (not written to the Event Log)	success	-	Deployer (sent by the Processor)	EMITTED

Detail

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
5001	User account created by an administrator, manually or through bulk import. The actor is the administrator; the subject is the new account.	create	user (target account)	target_login_id
5002	User profile refreshed from the RMS or Microsoft Entra ID (when Admin.SyncRMSUserInfo / Admin.SyncAADUserInfo is on), at sign-in or when an administrator opens the account. Edits made in the admin portal user editor, and bulk user updates, are recorded in the database only in this release.	update	user (target account)	target_login_id
5003	User account enabled by an administrator.	enable	user (target account)	target_login_id

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
5004	User account disabled. By an administrator (departure, suspension, transfer): no reason, actor = the administrator. By the Processor inactivity sweep (Security.InactiveAccountDisableDays): reason inactivity, actor.username SYSTEM, details.trigger inactivity_sweep; accounts that never signed in and exempt login IDs are skipped. In both cases the account's open sessions are ended first (1004 forced:DISABLED). A bulk user import that archives an account emits only the 1004.	disable	user (target account)	target_login_id last_login_date, inactive_days_ threshold, trigger (inactivity sweep)
5010	System configuration value changed in the admin portal. Values are replaced by [REDACTED] when the key matches a sensitive pattern (password, token, secret, apikey, authtoken, privatekey, clientsecret, connectionstring).	update	config (configuration key)	config_name old_value new_value sensitive
5020	Not emitted in this release.	-	-	-
5030	Smart Draft AI prompt catalogue change: prompt version created, activated, superseded or rolled back. Previews (dry runs) and tuning-recommendation decisions are recorded in the database prompt audit only.	CREATE_VERSION ACTIVATE SUPERSEDE ROLLBACK	smartdraft_ prompt (occurrence type)	occurrence_type version_id
5040	Role created in the admin portal (2.9.5). Every role event is also written to the database role audit.	create	role	role_id role_name detail (description)
5041	Role name or description changed.	update	role	role_id role_name detail (old -> new name and description)
5042	Role disabled.	disable	role	role_id role_name
5043	Role re-enabled.	enable	role	role_id role_name
5044	Capability granted to a role. One event per capability added.	grant	role	role_id role_name capability_key
5045	Capability removed from a role. One event per capability removed.	revoke	role	role_id role_name capability_key
5046	Role assigned to a user in the admin portal, or through a bulk user import that sets a role. The subject is the user; details name the role.	assign	user (target account)	role_id role_name
5047	Role removed from a user. The subject is the user; details name the role.	remove	user (target account)	role_id role_name

EVENT ID	TRIGGER	ACTION VALUES	SUBJECT.TYPE	DETAILS KEYS
5090	HTTPS push test event (2.9.5). Queued by a Faction Four operator from the Deployer to confirm an agency's HTTPS push end to end, and delivered to that agency's endpoint only; never written to SS_Security. actor.username identifies the operator (DEPLOYER:<account>); actor.agency_id is the agency under test. Not a user action; safe to exclude from detection rules.	siem_remote_test	(none)	note

6. SAMPLE EVENT

Failed login as written to the `Message` field:

```
{
  "@timestamp": "2026-09-02T14:32:11.482Z",
  "event": {
    "id": 1002,
    "uid": "3f9c2d4e-8a1b-4c7d-9e2f-5a6b7c8d9e0f",
    "name": "auth.login.failure",
    "category": "authentication",
    "severity": "medium",
    "outcome": "failure",
    "reason": "invalid_credentials"
  },
  "actor": {
    "user_id": "1024",
    "username": "jsmith",
    "agency_id": "7",
    "ip": "10.4.12.88",
    "user_agent": "Mozilla/5.0 ..."
  },
  "action": "login",
  "source": {
    "host": "SS-WEB-01",
    "app": "SmartSquad.Service",
    "app_version": "2.9.5.0"
  },
  "error": {}
}
```

7. COLLECTION

On-premise. Subscribe to the `ss_security` channel only, with a local agent on each Smart Squad server or a Windows Event Collector subscription:

```
<QueryList>
  <Query Id="0" Path="SS_Security">
    <Select Path="SS_Security">*</Select>
  </Query>
</QueryList>
```

Hosted / shared servers: HTTPS push (2.9.5).

- Each agency's own events are POSTed in batches to an HTTPS endpoint the agency provides.
- Body format: `ndjson` (one event JSON per line, `application/x-ndjson`) or `splunk-hec` (one `{"time", "sourcetype": "smartsquad:security", "event"} envelope` per line).
- Every request carries `X-SmartSquad-Agency`, `X-SmartSquad-Batch-Id` and `X-SmartSquad-Event-Count`. With HMAC authentication it also carries `X-SmartSquad-Timestamp` and `X-SmartSquad-Signature`.
- Delivery is at least once and in order. `@timestamp` is the event time, not the delivery time.
- Setup, authentication options and response handling are in the Customer Overview.

Recommended indexed fields: `event.id`, `event.uid`, `event.name`, `event.category`, `event.severity`, `event.outcome`, `event.reason`, `actor.user_id`, `actor.username`, `actor.agency_id`, `actor.ip`, `subject.type`, `subject.id`, `source.host`, `source.app`, `correlation_id`.

8. WHAT IS NOT IN THIS FEED

- **Database audit records.** Login history, note, ticket, intel posting and form submission audit trails, the Search Audit, the face search log and the AI activity log are kept in the Smart Squad database and reviewed through the admin portal. They hold content-level detail and are not mirrored to the Event Log.
- **Operational logs.** The `SS_WebSvc`, `SS_Processor` and per-connector Event Log channels contain unstructured application exception text for troubleshooting. They carry no security semantics and are not recommended for the security pipeline.
- **Credentials, personal-information values and record content** never appear in the feed. Events carry identifiers, not data.