



VENTEX CONNECT

EVALUATION PLAYBOOK / PUBLIC METHOD / 2026

19 PAGES

SECURE COMMUNICATION EVALUATION PLAYBOOK 2026

A verifiable method for adoption, operation and decision-making

STATUS / PUBLIC WORKING DOCUMENT

Working method, not an audit, certification or legal advice.

VERSION 1.0 / 13 AUGUST 2026 / ventex-connect.com

01

Why a evaluation needs evidence

A secure messenger is not an isolated interface. Security emerges from identities, devices, roles, behaviour, operations and a tested fallback route.

OBJECTIVE

Translate technical and organisational assumptions into 30 days of observable work.

NOT AN OBJECTIVE

This does not replace privacy review, an ISMS, penetration testing or a cryptography audit.

Decision model

The evaluation asks whether a named workflow works acceptably under named conditions, not whether a product is abstractly 'secure'.

GO

Criteria met, risks accepted, conditions and owners recorded.

ITERATE

Benefit is visible but named gaps require another bounded experiment.

STOP

Protection boundary, operation or benefit is insufficient.

03

Draw the protection boundary

Before the first login, record what is inside and outside evaluation responsibility.

INSIDE

Named accounts and devices; approved data; scoped functions; support and incident process; retention and deletion.

OUTSIDE

Fully compromised endpoints; coerced authorised users; unapproved integrations; unknown platform flaws; out-of-charter workflows.

04

Threats as hypotheses

A threat model remains practical when each assumption becomes an exercise or verifiable record.

EXAMPLES

Stolen password -> verify MFA and session view. Lost device -> measure targeted revocation. Broken connection -> inspect reconnect and duplicates. Untrusted primary channel -> activate contact tree.

RULE

Never stage a scenario secretly in production. Approve time, test data and abort condition first.

05

Identity and devices

Identity is a lifecycle, not a one-time login.

CHECKS

Registration; invitation; device label; distinct session; passkey or second factor; new device; key change; loss; revocation; recovery; leaver access.

MEASURE

Detection time, revocation time, failed retries and remaining sessions after close-out.

06

Workflow before feature list

Start with one workflow, not a tour of every control.

WORKFLOW MAP

Trigger; decision; required information; accountable role; permitted channel; record; fallback route.

EXAMPLE

Alarm confirmed -> operator opens Mission Room -> pins situation format -> dispatcher assigns task -> closing decision is recorded.

07

Mission Room protocol

A room needs a stable situation format so current facts and decisions remain distinguishable.

SITUATION UPDATE

Time; author; role; confirmed facts; assumptions; decision; task and owner; next update time.

AVOID

Unmarked assumptions; competing decision messages; files without context; screenshots as the only system of record.

08

Incident communication

During a cyber incident the primary identity or messaging system may itself be part of the problem.

ACTIVATION

Trust-switch criteria; independent contact tree; primary and fallback channels; verified roles; fixed update cadence.

RETURN

Return only after identities, devices, sessions, integrations, open invitations and tokens have been reassessed.

30-day plan

Four deliberate phases produce more insight than one long unstructured test.

WEEK 1 - BASELINE

Onboarding, core workflow, permitted data and baseline measures.

WEEK 2 - FRICTION

Device change, weak connection, files, search and role transfer.

WEEK 3 - RESILIENCE

Revocation, fallback and redacted incident exercise.

WEEK 4 - DECISION

Interviews, Evidence Matrix, risks and final report.

Measurement dictionary

A metric is useful only when start, end, unit, source and owner are defined.

CORE MEASURES

Onboarding completion; median time to first valid message; task completion without workaround; median device revocation time; reconnect duplicates; operator confidence with reason.

NO VANITY METRICS

Message or login counts alone prove neither security nor operational benefit.

11

Friction register

A workaround is evidence, not user failure.

ENTRY

Time; role; intended job; observed obstacle; workaround; risk; frequency; owner; next test.

PRIORITY

Address high frequency plus high protection impact first. Keep cosmetic requests separate.

Controlled exercises

Exercises test the protection boundary without provoking real harm.

A - LOST DEVICE

Revoke a test device and retry the previous session.

B - RECONNECT

Disconnect, prepare messages, reconnect and inspect order and duplicates.

C - TRUST SWITCH

Declare the primary channel untrusted and activate the contact tree.

ABORT

Stop on unexpected production data, a real security event or unclear ownership.

Evidence Matrix and Claim Ledger

The Evidence Matrix records what was observed. The Claim Ledger governs what may be said publicly.

EVIDENCE

Requirement; test; result; artefact; owner; date; status.

CLAIM

Wording; audience; supporting evidence IDs; boundary; approver; expiry.

Privacy and observation

Evaluation measurement should improve product decisions, not create hidden personal profiles.

MINIMISE

Only necessary events; aggregate measures where possible; short retention; role-based access; redaction before export.

TRANSPARENCY

Participants know what is collected, why, who can access it and when it is deleted.

15

Security event during the evaluation

A genuine suspicion interrupts the exercise. Operational incident handling takes priority.

IMMEDIATE

Notify Evaluation Owner and Security Contact; stop the affected workflow; preserve evidence; revoke only with approval; use fallback.

AFTERWARDS

Record timeline and decisions; assess notification duties separately; explicitly approve restart.

Final decision

Tie the decision to criteria, not general enthusiasm.

DECISION RECORD

Criteria met; partial or unmet criteria; residual risks and acceptor; conditions for next stage; data and access to close.

SIGN-OFF

Sponsor: _____ Evaluation Owner: _____ Security: _____ VENTEX: _____ Date: _____

Transfer to operations

A successful evaluation is not production. Transition requires separate acceptance.

BEFORE PRODUCTION

Operating and support model; restore drill; independent monitoring; roles and access; data processing; external review proportionate to risk.

CHANGE CONTROL

Version, compare and separately approve evaluation and production configurations.

Sources and review

Primary sources inform authentication, incident response, communications, privacy and group communication.

SOURCES

NIST SP 800-61r3; NIST SP 800-63B-4; CISA Emergency Communications Guidance; Regulation (EU) 2016/679; RFC 9420; ENISA Secure Group Communications.

REVIEW

Owner: VENTEX Connect Product & Security
Version: 1.0
As of: 13 August 2026
Next review: material product change or 13 February 2027

PUBLIC METHOD / NOT AN AUDIT OR CERTIFICATION