MISP

INTELLIGENCE SHARING

MISP 2.5 administration

Control access, review operations and recover confidently

CIRCL / Team MISP Project

https://www.misp-project.org/

Reference: 3 November 2026

What you will practise

- Delegate access without confusing account and organisation scope.
- Define an audience and verify it with ordinary accounts.
- Review knowledge bases, connections and instance defaults.
- Distinguish jobs, workers and scheduled tasks.
- Plan evidence, recovery and a controlled update.

Prepare a reversible lab

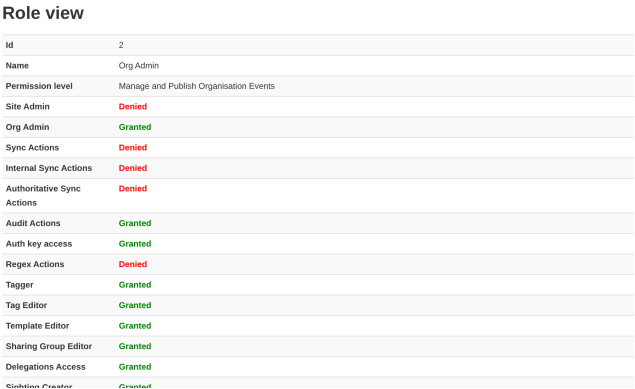
- Use a disposable instance and operator-provided accounts.
- Keep all example records synthetic and unpublished.
- Define the expected change, owner and rollback before editing.
- Use disabled peer/feed records with documentation-only URLs.

Separate the responsibility scopes

Site administrator	Organisation admin	Platform operator
Instance-wide MISP policy Organisations and roles Sharing and diagnostics	Own organisation User management Account lifecycle No site settings	Services and deployment Database, files and secrets Backups and recovery

MISP role permissions and host access are separate.
Review the actual role flags and deployment policy.

Inspect actual role flags

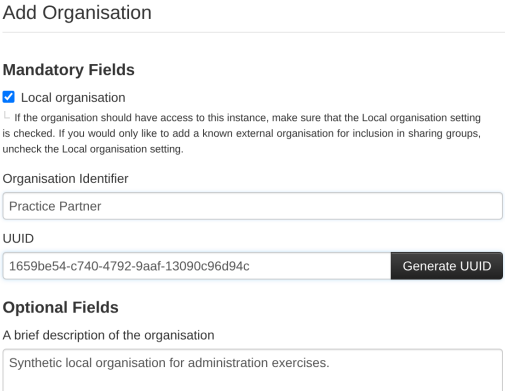


Role view

Id	2
Name	Org Admin
Permission level	Manage and Publish Organisation Events
Site Admin	Denied
Org Admin	Granted
Sync Actions	Denied
Internal Sync Actions	Denied
Authoritative Sync Actions	Denied
Audit Actions	Granted
Auth key access	Granted
Regex Actions	Denied
Tagger	Granted
Tag Editor	Granted
Template Editor	Granted
Sharing Group Editor	Granted
Delegations Access	Granted
Sighting Creator	Granted

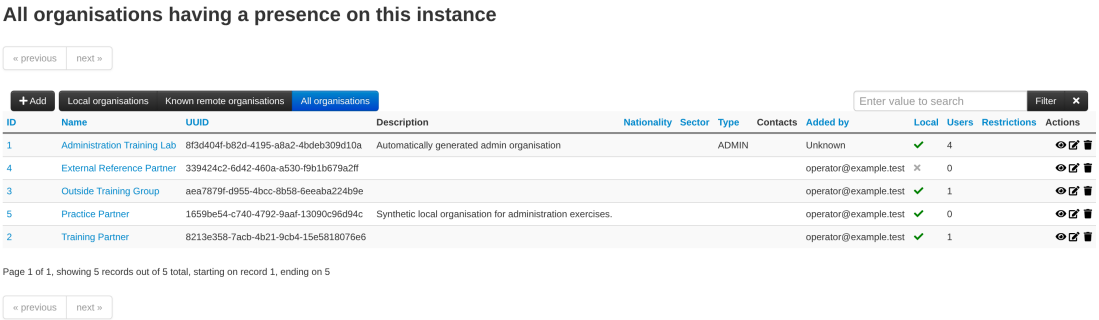
Read the permission level and individual flags. A role name alone is not an access policy.

Create a local organisation deliberately



For a new local organisation, choose Local organisation and a stable UUID; reuse known partner UUIDs.

Review organisation identity after saving

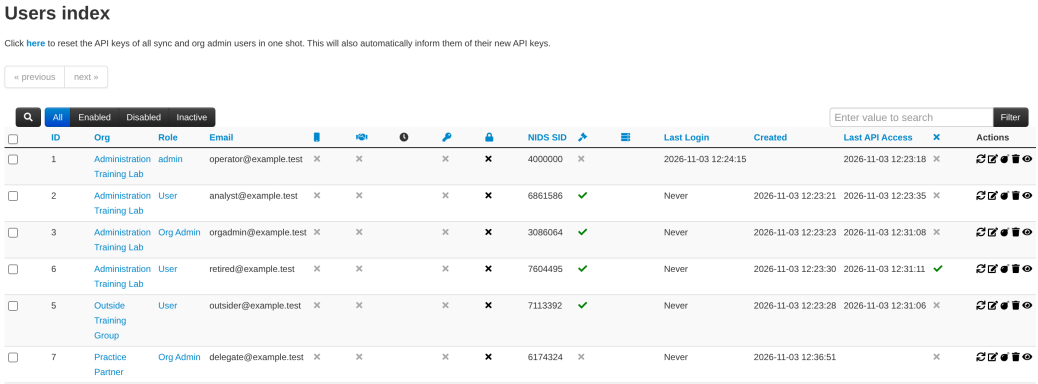


Check local/external status and UUIDs before adding users or sharing-group membership.

Provision a user with the intended scope

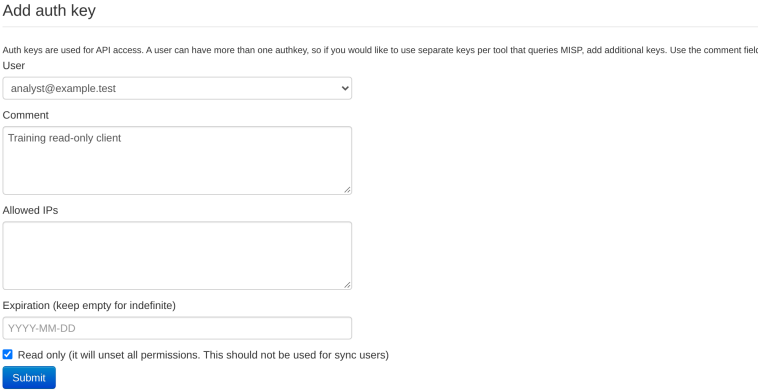
Select the correct organisation and role. Deliver access through your approved onboarding process.

Review lifecycle and delegated administration



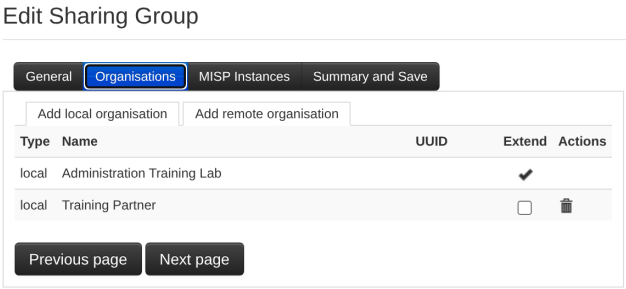
Verify the saved organisation, role and account status; disable retired access under the offboarding plan.

Issue a key for a defined client



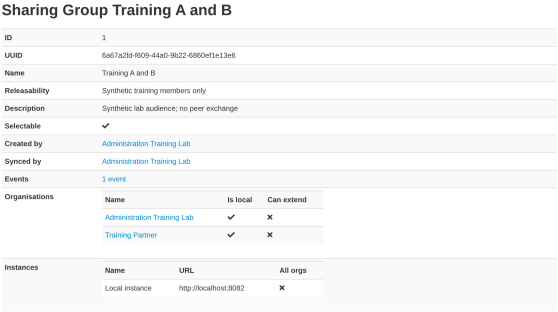
Use a purpose, expiry, allowed sources and Read only where appropriate. Never capture the generated secret.

Define membership before topology



Choose explicit member organisations and review Extend rights. Membership does not require a peer connection.

Inspect the saved sharing group



Sharing Group Training A and B

ID	1
UUID	6a67a2fd-f609-44a0-9b22-6860ef1e13e6
Name	Training A and B
Releasability	Synthetic training members only
Description	Synthetic lab audience; no peer exchange
Selectable	✔
Created by	Administration Training Lab
Synced by	Administration Training Lab
Events	1 event

Organisations

Name	Is local	Can extend
Administration Training Lab	✔	✖
Training Partner	✔	✖

Instances

Name	URL	All orgs
Local instance	http://localhost:8082	✖

Review organisations, instance constraints, Active and Roaming together before using the group.

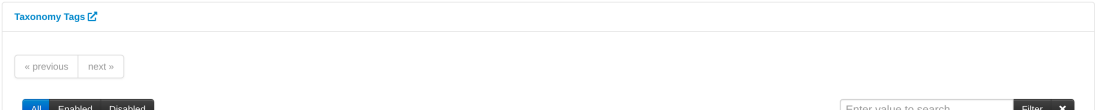
Verify visibility with ordinary identities

Reference check	Observed result
Host analyst	Reads the private and group events.
Partner ordinary user	Reads the group event; private event denied.
Outside ordinary user	Group event denied.
Org Admin	Site settings denied.

Prepare taxonomies and tags before class

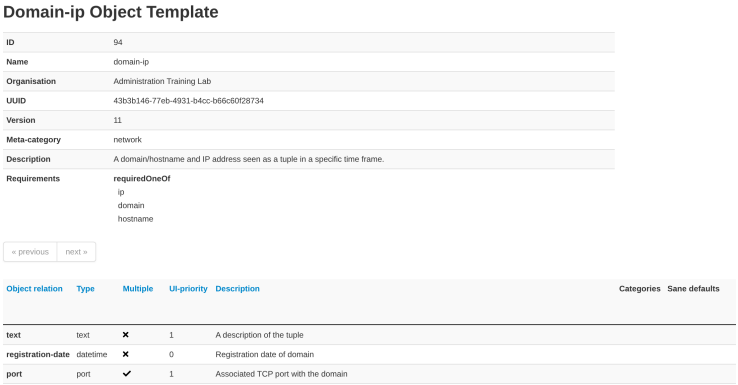
TLP Taxonomy Library

ID	171
Namespace	tlp
Description	The Traffic Light Protocol (TLP) (v2.0) was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information sharing happens from an information source, towards one or more recipients. TLP is a set of four standard labels (a fifth label is included in amber to limit the diffusion) used to indicate the sharing boundaries to be applied by the recipients. Only labels listed in this standard are considered valid by FIRST. This taxonomy includes additional labels for backward compatibility which are no more validated by FIRST SIG.
Version	10
Enabled	✔
Highlighted	✖
Action	Disable taxonomy



Update the bundled catalogue through the deployment workflow, then enable the taxonomy and required tags.

Review object templates and versions



Domain-ip Object Template

ID	94
Name	domain-ip
Organisation	Administration Training Lab
UUID	43b3b146-77eb-4931-b4cc-b66c60f28734
Version	11
Meta-category	network
Description	A domain/hostname and IP address seen as a tuple in a specific time frame.
Requirements	**requiredOneOf** ip domain hostname

« previous next »

Object relation	Type	Multiple	UI-priority	Description	Categories	Sane defaults
text	text	✖	1	A description of the tuple		
registration-date	datetime	✖	0	Registration date of domain		
port	port	✔	1	Associated TCP port with the domain		

Inspect template UUID, version, requirements and active state before users create structured records.

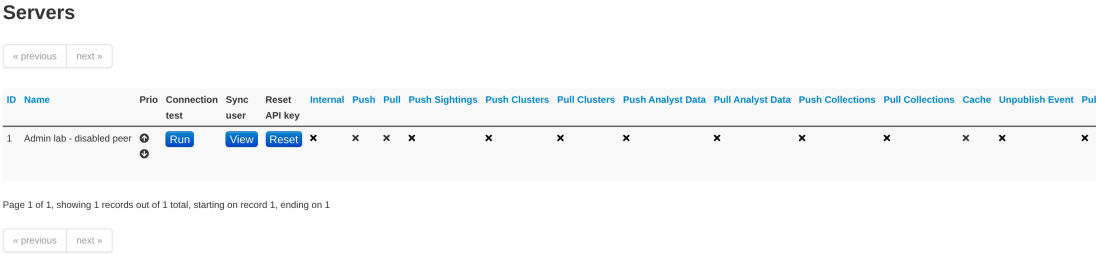
Treat a warninglist hit as a review signal

The enabled bundled list matches 192.0.2.25. A match does not itself block ingestion, export or an action.

Distinguish review aids from input/output controls

- Warninglists flag values for review.
- Allowlist/export filters can change selected outputs.
- Regex rules can reject or modify supported input paths.
- Test scope and side effects with a small fixture first.

Stage a peer without transferring data

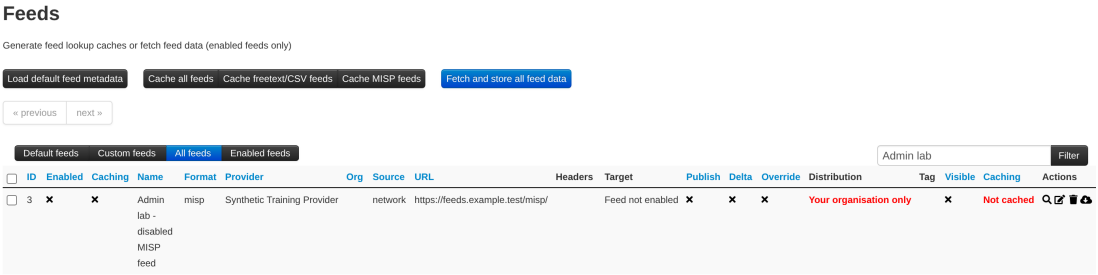


The reference peer uses a reserved .test URL and has transfer directions disabled. No connection test is run.

Validate sync policy in a controlled window

- Agree direction, scope, filters and responsibility with the peer.
- Validate TLS and the remote identity; avoid bypassing verification.
- Use a small authorised test record and inspect both ends.
- Check changes, deletions, feedback and failure behaviour.

Stage a feed before enabling it



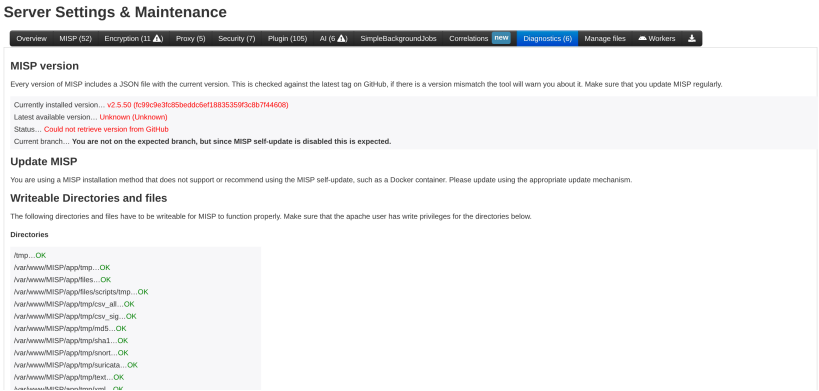
Inspect provider, format and destination policy while Enabled and caching remain off.

Make defaults explicit and verify their scope

Critical	MISP.showorg	true	Setting this setting to "false" will hide all organisation names / logos.
Critical	MISP.osuser	www-data	The Unix user MISP (php) is running as
Critical	MISP.email	operator@example.test	The e-mail address that MISP should use for all notifications
Critical	MISP.disable_emailing	false	You can disable all e-mailing using this setting. When enabled, no outgoing e-mails will be sent by MISP.
Critical	MISP.default_event_distribution	Your organisation only	The default distribution setting for events (0-4).
Critical	MISP.default_attribute_distribution	Inherit from event	The default distribution setting for attributes, set it to 'event' if you would like the attributes to default to the event distribution level. (0-3 or "event")
Critical	MISP.default_event_tag_collection	None	The tag collection to be applied to all events created manually.
Critical	MISP.default_publish_alert	true	The default setting for publish alerts when creating users.

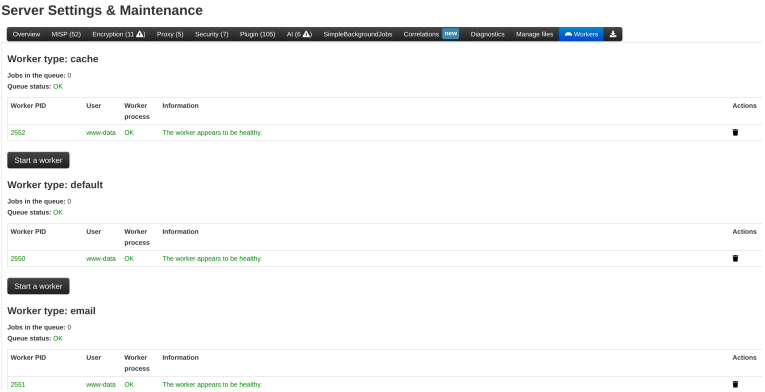
The lab sets `MISP.default_event_distribution` to organisation-only. Existing records retain their saved scopes.

Read diagnostics as evidence



Review the reported version, dependencies and deployment-specific warnings; investigate the cause of each relevant issue.

Workers execute jobs; queues hold pending work



Check queue, process, owner and status. A healthy process and an empty queue are different observations.

Follow a job through to completion

Jobs

Purge job entries: Completed All

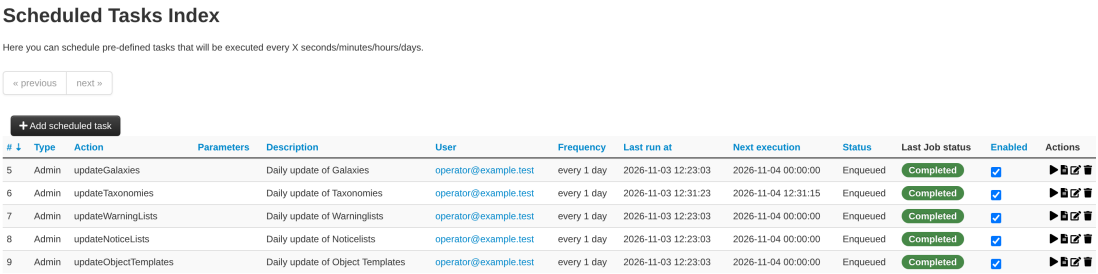
« previous next »

All Default Prio Email Cache

ID ↑	Date created	Date modified	Process ID	Worker	Job type	Input	Message	Organisation name	Status	Progress
10	2026-11-03 12:31:23	2026-11-03 12:31:24	69119d44-00fc-4d1e-b816-b3d1f35d0501	default	admin_action	updateTaxonomies	All taxonomies are up to date already.	Administration Training Lab	Completed	Completed
9	2026-11-03 12:23:03	2026-11-03 12:23:08	fa5e386f-b827-43ba-8a1b-9d3f61412e38	default	admin_action	updateObjectTemplates	All object templates are up to date already.	Administration Training Lab	Completed	Completed
8	2026-11-03 12:23:03	2026-11-03 12:23:08	586d0d48-9a0d-4621-b76c-661245d270a4	default	admin_action	updateNoticeLists	Notice lists	Administration Training Lab	Completed	Completed

Inspect job type, progress, live status and message; keep enough evidence to diagnose failures.

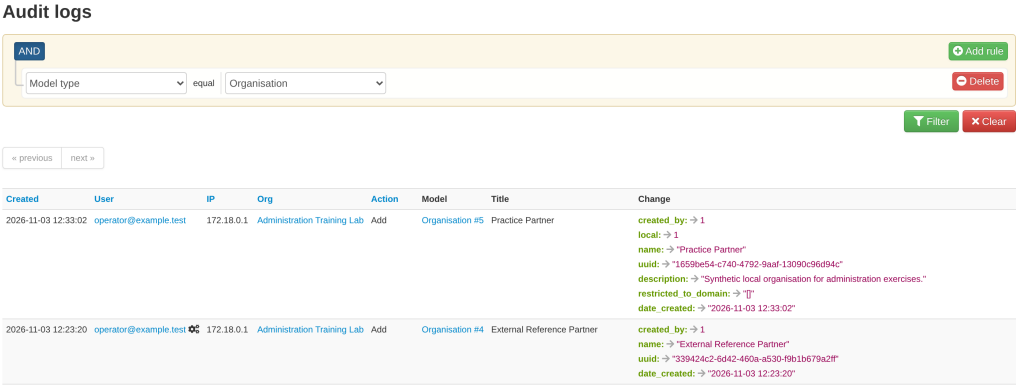
A schedule is a request for future work



# ↓	Type	Action	Parameters	Description	User	Frequency	Last run at	Next execution	Status	Last Job status	Enabled	Actions
5	Admin	updateGalaxies		Daily update of Galaxies	operator@example.test	every 1 day	2026-11-03 12:23:03	2026-11-04 00:00:00	Enqueued	Completed	☑	
6	Admin	updateTaxonomies		Daily update of Taxonomies	operator@example.test	every 1 day	2026-11-03 12:31:23	2026-11-04 12:31:15	Enqueued	Completed	☑	
7	Admin	updateWarningLists		Daily update of Warninglists	operator@example.test	every 1 day	2026-11-03 12:23:03	2026-11-04 00:00:00	Enqueued	Completed	☑	
8	Admin	updateNoticeLists		Daily update of Noticelists	operator@example.test	every 1 day	2026-11-03 12:23:03	2026-11-04 00:00:00	Enqueued	Completed	☑	
9	Admin	updateObjectTemplates		Daily update of Object Templates	operator@example.test	every 1 day	2026-11-03 12:23:03	2026-11-04 00:00:00	Enqueued	Completed	☑	

Review action, execution identity, interval, next run and last job before enabling or forcing a task.

Use a narrow audit question

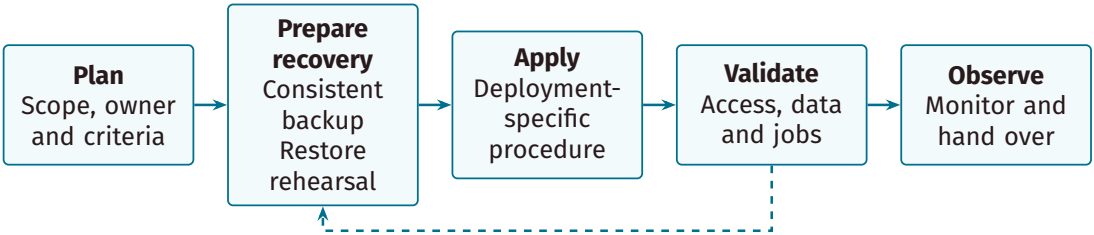


Filter the audit log to Organisation changes in this synthetic lab, then inspect actor, time and action.

Trace the failing layer before changing it

- Start with user-visible symptom, time and affected record/job.
- Check MISP audit/application logs and the relevant worker error.
- Then inspect web/PHP, database, Redis and service logs.
- Share a reviewed diagnostic excerpt through the appropriate channel.

Prepare recovery before the change



Use the update path for the deployment

- Read release notes and migration/dependency requirements.
- Rehearse with a representative copy and recovery plan.
- Use the supported package, container or source procedure.
- Validate access, schema, data, background work and integrations.
- Monitor, document and apply the rehearsed recovery criteria.

Triage a failed refresh

Observation	Next useful check
Task due, no job	Scheduler health, execution identity and task state.
Job queued, not running	Correct queue, worker process and permissions.
Job failed	Relevant error, input/source and dependency health.
Job completed, wrong result	Saved data, scope, version and consumer expectations.

Checkpoint: delegate and verify an audience

- Create a synthetic organisation and delegated account.
- Review a client key with a defined purpose and expiry.
- Limit a sharing group to the intended two organisations.
- Verify group/private access with member and outside users.

Checkpoint: explain the operational handover

- Locate a relevant setting, diagnostic, worker, task and audit entry.
- Explain how to verify a disabled connection before enabling it.
- Describe a restore rehearsal and update acceptance criteria.
- Record owner, evidence, monitoring and the next review date.