Platform & Access

FortiAnalyzer 7.4 Administrator

KNOWLEDGE CHEATSHEET

ADMINISTRATIVE ACCESS

Identity Authenticate → **Profile** Allowed actions → **ADOM** Data scope → **Trusted hosts** Source

01 Platform operation and administrator access

Analyzer and collector roles

- **Analyzer mode** is the default. It receives logs, maintains the SQL analytics database, and provides event management and reporting.
- **Collector mode** receives and stores logs, then forwards them to an analyzer. This separates log collection from analytics processing; prioritize archive storage on collectors.
- **Operating mode** selects the appliance's role. **ADOM device mode** controls whether FortiGate VDOMs can be split across administrative domains.
- Size for **logs per second**, daily volume, analytics retention and archive retention. SQL indexing needs additional storage and processing beyond compressed log files.

Administrative scope and authentication

- An **administrator profile** determines permitted actions; assigned **ADOMs** determine the data and devices in scope. Successful authentication does not grant unrestricted administration.
- **Super_User** has full administrative privileges. **Standard_User** supports routine log and device administration but lacks full system configuration rights, including system mail-server configuration.
- **Trusted hosts** restrict the source addresses allowed to access an administrator account. Combine these restrictions with the required management protocols and least-privilege profiles.
- For **SAML**, an **identity provider (IdP)** authenticates users and issues assertions; a **service provider (SP)** consumes them. FortiAnalyzer can be configured for either role.

LDAP and wildcard administrators

- Configure a **remote LDAP server** with reachable address, directory search settings and appropriate bind credentials. Directory lookup and administrator authorization are separate steps.
- **Match all users on remote server** creates a wildcard administrator mapping. Matching users sign in with their own remote credentials and receive the mapping's profile and ADOM access.
- To admit a particular **LDAP group**, constrain the remote authentication mapping to that group. A wildcard mapping should not unintentionally grant access to the entire directory.
- Check directory connectivity, group matching and assigned permissions independently. Keep a tested **local recovery administrator** available if remote authentication fails.

ADOMs & Devices

FortiAnalyzer 7.4 Administrator

KNOWLEDGE CHEATSHEET

DEVICE ONBOARDING

Device Register → **Identity** Authorize → **ADOM** Assign → **Logs** Analyze

02 ADOMs and device management

Administrative domains and VDOMs

- **ADOMs** partition devices, logs, reports and administrative access. Enabling ADOMs creates default domains for supported device families.
- Choose an **ADOM type** compatible with the logging device. A **Security Fabric ADOM** combines supported Fabric device types for log correlation and reporting.
- **Normal mode**, the default ADOM device mode, keeps a FortiGate in one ADOM. **Advanced mode** permits VDOMs from one FortiGate to reside in different ADOMs.
- ADOM device mode can be changed through the **GUI or CLI**. Disk quotas are a separate setting; Normal mode does not make an ADOM's quota permanently fixed.

Moving devices and rebuilding analytics

- Before deleting an ADOM, remove its **registered devices**. Built-in **default ADOMs** cannot be deleted.
- When moving a device to another ADOM, its **archive logs** move with it. Existing SQL analytics need rebuilding before the destination can analyze the retained history.
- **execute sql-local rebuild-adom** rebuilds an ADOM's SQL analytics from available archive logs. Plan for processing time and temporary effects on queries and reports.
- A rebuild can recover only the **history still retained in archives**. Select the destination ADOM when checking reports, datasets and log visibility after a move.

Registration and authorization

- **Unauthorized** means the device's registration has not yet been accepted. Confirm its identity and authorize it before relying on normal log management.
- Pre-registration by **serial number** or **pre-shared key** can associate a new device with its intended ADOM. A device-initiated request still requires the applicable authorization workflow.
- For **Fabric Authorization**, verify the FortiAnalyzer authorization address and port, server settings, and browser reachability from the management computer.
- A **FortiGate HA cluster** contains distinct member serial numbers. Devices registered before cluster formation can be grouped manually; a shared transport IP alone does not identify the original log producer.

Logs & Storage

FortiAnalyzer 7.4 Administrator

KNOWLEDGE CHEATSHEET

FROM COLLECTION TO ANALYTICS

FortiGate Generate → **Transfer** Receive → **Archive** Retain → **SQL** Analyze

03 Log collection, analytics and storage

Real-time, archive and analytics logs

- **Real-time logs** have arrived but are not yet indexed in SQL. FortiAnalyzer first writes incoming entries to log files.
- **Archive logs**, also called **offline logs**, are retained log files. Completed files are rolled and compressed; they preserve material for later database rebuilds.
- **Analytics logs** are indexed in the SQL database and available to FortiView, normal Log View, events and reports. A retained archive does not itself guarantee queryable analytics history.
- A **data policy** sets analytics and archive retention separately. Archive browsing or rebuilding serves a different purpose from querying the online analytics database.

Collection path and missing logs

- Check the **FortiGate source settings** first: firewall-policy logging, enabled log types, filters and FortiAnalyzer destination. Registration alone does not enable every expected log.
- **OFTP** handles Fortinet log-transfer communication. Reliable, encrypted FortiGate-to-FortiAnalyzer logging uses **TCP 514**; verify reachability and compatible TLS settings.
- When FortiAnalyzer is unreachable, the FortiGate logging process **buffers logs locally** and uploads retained entries after reconnection. Capacity is finite; prolonged outages can cause loss.
- **miglogd** is the older FortiGate logging-process name; newer FortiOS releases use **fgtlogd** for FortiAnalyzer logging. Select diagnostics for the sending FortiGate's software.
- In a **Security Fabric**, a root FortiGate can relay downstream logs. Read device identifiers inside the log to identify origin; the packet source may be the relay. An upstream FortiGate performing **NAT** can also generate its own traffic logs for those sessions.

Processes, connections and integrity

- **diagnose system print netstat** displays network connections, protocol information, addresses and socket states. Use it to distinguish connection failure from a log-processing problem.
- On FortiAnalyzer, **oftpd** handles device log-transfer connections, **logfiled** manages log files and size-based rolling, and **sqlplugind** participates in SQL log insertion.
- **set log-checksum** under **config system global** controls file integrity records: **md5** records a hash, **md5-auth** adds an authentication code, and **none** disables recording.
- **Checksums** help detect changes to log files. **TLS** protects data in transit. Configure these controls separately; an integrity record does not encrypt a connection or stop a file from being changed.

Logs & Storage / Resilience & Fabric

FortiAnalyzer 7.4 Administrator

KNOWLEDGE CHEATSHEET

FROM COLLECTION TO ANALYTICS

FortiGate Generate → **Transfer** Receive → **Archive** Retain → **SQL** Analyze

Forwarding and scheduled aggregation

- **Forwarding mode** sends received logs in real time to supported FortiAnalyzer, syslog or **CEF** destinations. Match the output format to the receiver.
- **Aggregation mode** stores log and content files, then uploads them on a schedule to another FortiAnalyzer. It requires a sending and receiving FortiAnalyzer.
- For FortiAnalyzer-to-FortiAnalyzer transfers, both forwarding and aggregation support **encrypted transfer**. Check receiver configuration, authorization and network reachability.
- A delayed scheduled upload, an unreachable receiver and a SQL indexing backlog affect different stages. Compare **receive, forward and insert status** before changing retention settings.

Disk quotas and retention planning

- **Total Quota = total system storage - reserved space**. Available quota for new allocation differs from current free disk space and from the amount already allocated to ADOMs.
- **Reserved space** supports system operation. Account for disk size, RAID layout and usable capacity when planning storage; raw installed capacity is not all available for ADOM quotas.
- An ADOM divides storage between **analytics** and **archive** needs. Retention days express the desired history; allocated capacity must also sustain the actual incoming volume.
- Track **used**, **allocated** and **available** values separately. Increasing retention without enough quota cannot guarantee that the requested history will remain available.

04 Resilience, recovery and FortiAnalyzer Fabric

RAID capacity and disk failures

- **RAID 0** stripes data and has no disk-failure tolerance. **RAID 1** mirrors data. **RAID 5** uses distributed parity; a supported **RAID 6+0** layout stripes across double-parity groups.
- **RAID 10** stripes across mirrored pairs. Four equal 2 TB drives provide about **4 TB usable** before filesystem and system reservations; there is no parity component.
- **Degraded** means the array has lost redundancy because a member drive is missing or failed. **Rebuilding** means data is being reconstructed onto a replacement drive.
- Use a supported **hot swap** to replace a failed drive on hardware designed for it, then monitor the rebuild. **execute format disk** is destructive disk reinitialization; it is not routine failed-drive recovery.

Resilience & Fabric

FortiAnalyzer 7.4 Administrator

KNOWLEDGE CHEATSHEET

RECOVERY LAYERS

- **RAID** — Disk resilience
- **HA** — Service continuity
- **Backup** — Restore history
- **Fabric** — Central view

HA operation and primary election

- **FortiAnalyzer HA** synchronizes logs and selected configuration settings. Members must use the same **operation mode**; plan compatible firmware, models and sufficient storage.
- Separate **peer heartbeat**, log synchronization and client log delivery when troubleshooting. Routed peer communication requires appropriate addresses and routing; a heartbeat timeout does not describe SQL status.
- After primary failure, the eligible unit with the **highest configured priority** becomes primary. If priorities tie, the **highest primary IP address** breaks the tie.
- For a controlled HA firmware upgrade, upgrade **secondary units before the primary** following the supported upgrade path. Preserve backups and verify cluster and log synchronization afterward.

Initial and real-time log synchronization

- **Initial Logs Sync** transfers existing logs from the primary to a newly added unit. After initial synchronization, the secondary reboots and rebuilds its log database.
- **Log Data Sync** maintains real-time log synchronization after the initial transfer. The primary forwards new logs to secondary units.
- Log Data Sync is **enabled by default** for HA units, including secondaries, so a promoted secondary can continue synchronizing the remaining units.
- Check both **initial synchronization completion** and **ongoing log synchronization**. A unit that is reachable but lacks synchronized logs does not provide the same recovery readiness.

Fabric supervision and recoverable backups

- A **FortiAnalyzer Fabric supervisor** provides a central view across member FortiAnalyzers. Logging devices register to **members**, which collect their logs; the supervisor is not a direct logging-device registration target.
- Fabric membership requires **compatible releases and connectivity**. HA support differs between members and supervisors; the supervisor does not support HA. Incident access on the supervisor is **read-only**.
- A **system configuration backup** preserves system and report configuration. Protect it with encryption and retain the restore password. Device log archives require a separate backup plan.
- **RAID**, **HA synchronization** and **backups** address different failures. Keep recoverable copies outside the appliance and verify restoration before relying on them.