

LDAP Manager

Captive Portal and Identity-Based Network Access for Campus and Enterprise Networks

LDAP Manager puts a captive portal in front of your network and ties every session to a named account in your existing directory. It gives your team one place to create users, manage groups, upload accounts in bulk, issue time-bound guest logins and control how many devices each person may use — and it keeps users connected as they move around the campus.

PROVEN IN PRODUCTION

Measured on a live deployment at a 10,000-user higher-education campus — actual figures, not projections.

10,000+	668,000	0.00%	43 ms	60+ days
CONCURRENT SESSIONS	REQUESTS PER DAY	SERVICE ERROR RATE	AVERAGE RESPONSE TIME	CONTINUOUS UPTIME

AT A GLANCE

Captive portal with directory login

Users sign in with the credentials they already have. No agent, no certificate, no shared password.

Complete user and group management

Create, edit, disable and expire accounts; manage group membership; upload thousands of users from a single file.

Users stay connected while they move

Devices moving between network segments or access points are recognised and resumed automatically — no second login.

Delegated administration

Hand specific tasks to specific teams without giving anyone more access than the task requires.

Overview

Most networks still identify users by IP address. That breaks the moment someone moves, a lease expires, or a device is shared — and it leaves the security team reading logs full of addresses instead of names. LDAP Manager closes that gap. A user opens a browser, is presented with a captive portal, signs in with their directory account, and from that point the network knows exactly who they are for the life of the session.

For the people who run the network, it is a single console for the whole user lifecycle: create and import accounts, organise them into groups, apply policy by group, issue guest logins that expire on their own, and see who is online right now. It works alongside the directory, DHCP and perimeter security you already operate rather than replacing them.

Core Capabilities

Captive Portal

Unauthenticated devices are presented with a branded sign-in page automatically. Works on every major platform and with the built-in captive-network assistants on phones and laptops — nothing to install.

User and Group Management

Create, edit, disable, expire and delete accounts from one console. Manage group membership directly, and let group membership drive the policy each user receives.

Guest and Visitor Accounts

Issue logins that carry a mandatory expiry date and switch themselves off when it passes. Reception or guest-house staff can be given a role that manages visitors and nothing else.

Seamless Roaming

A device that moves between network segments, buildings or access points is recognised and its session resumed automatically. Users are not returned to the login page and connections are not dropped.

Directory Authentication

Users sign in with the credentials they already hold. Accounts are authenticated against your LDAP directory over an encrypted connection; there is no second password database to keep in step.

Bulk Upload and Bulk Update

Import thousands of accounts from a single file at the start of a term or intake, then update, enable, disable or expire a selected set in one action instead of one at a time.

Device Limit Control

Set how many devices an account may use at once — by group as a default, and per user where someone needs more. A shared teaching credential can cover a whole laboratory while ordinary accounts stay capped.

Identity for Network Policy

Verified user-to-address information is published to your network enforcement point, so access rules and reporting refer to named users and groups rather than to IP addresses.

Why It Matters

Accountability	Every session is attributable to a named account, with sign-in time, address, device identifier where available and sign-out time retained for audit and incident response.
Less Administrative Load	Bulk import, group-driven policy and self-service password reset remove most of the repetitive account work from the network team.
Fewer Helpdesk Calls	Automatic roaming resumption and self-service password reset address the two most common reasons users call.
No Client Software	Any device with a browser works. Nothing to install on endpoints, nothing to update, nothing to support.

Feature Set

Captive Portal and Authentication

FEATURE	DESCRIPTION
Automatic redirection	Devices that have not yet signed in are sent to the portal without the user having to type an address.
Directory sign-in	Credentials are verified against your LDAP directory over an encrypted connection.
Branded login page	The portal carries your institution's identity rather than a generic page.
Universal device support	Windows, macOS, Linux, Android and iOS, including the captive-network assistants built into each.
Session lifetime control	Sessions carry a configurable duration and are closed automatically when it expires.
Already-connected handling	A user returning to the portal while still signed in is told so, and may end the session or continue.

User, Group and Guest Management

FEATURE	DESCRIPTION
Account lifecycle	Create, view, edit, disable, set an expiry date, reset a password and delete — each a separately grantable action.
Group management	Create and maintain directory groups and move users between them; group membership drives the policy a user receives.
Bulk upload	Import a large batch of accounts from a single prepared file, with per-row validation and a result report.
Bulk update	Apply a change across a prepared list of existing accounts in one operation.
Bulk actions on selection	Enable, disable, edit or remove a set of users picked from the console in a single step.
Guest accounts	Time-bound logins with a mandatory expiry date, issued by staff who hold only the guest-management role.
Per-user restrictions	Override the group default for an individual account — for example a higher device allowance.

Self-Service for End Users

FEATURE	DESCRIPTION
Password reset	Users reset their own password using a one-time code sent by e-mail, without contacting the helpdesk.
Device list	Users can see which of their devices are currently signed in.
Sign out a device	Users may end any one of their own sessions to free a device slot, without re-entering credentials.

Administration and Security

Network teams are rarely the only people who need to create accounts. A guest house needs to issue visitor logins; a department may manage its own students. LDAP Manager is built around delegation, so those tasks can be handed out without handing out full administrative rights.

Role-Based Administration

Administrator accounts are assigned a role assembled from twenty discrete permissions. A role grants exactly the actions it needs and nothing more — a guest-house operator can create and expire visitor accounts while remaining unable to delete users, alter groups, view the session monitor or reach system settings.

PERMISSION GROUP	INCLUDED CAPABILITIES
User management	View, create, edit and delete; reset password; disable or set an expiry date; change group membership.
Bulk operations	Bulk upload, bulk update, and bulk edit, enable, disable or delete on a selected set — each grantable separately.
Visibility scoping	A role can be restricted to a single user group, so that administrator sees and acts on only those accounts.
Oversight	Live session monitor, usage reports, scheduled summary reports and a system health dashboard.
System	Administrator account management, system settings and published user documentation.

Security Controls

- **Restricted management access.** The administration console is reachable only from an approved list of management addresses; requests from anywhere else are refused before any credential is accepted.
- **Audit trail.** Administrative actions are recorded with the acting account, the affected user and a timestamp.
- **Encrypted transport.** All user and administrative traffic is carried over TLS; directory traffic is encrypted end to end.
- **Separation of duties.** Destructive permissions — delete, bulk delete, group management and system settings — are independently grantable and are off by default in delegated roles.
- **Session accountability.** Each session records the account, address, device identifier where available and sign-in and sign-out times.

Monitoring and Reporting

CAPABILITY	WHAT IT SHOWS
Live session monitor	Who is online now, on which addresses, since when.
Usage reports	Authentication and session activity over a chosen period.
Scheduled summaries	Periodic reports generated and circulated automatically.
System health	Continuous sampling of processor, memory and storage utilisation, retained as a rolling trend so an overnight event is still visible the next morning.

Deployment and High Availability

LDAP Manager is installed alongside your existing network services. Users, administrators and your enforcement point all reach it through a single service address; the arrangement behind that address is invisible to them.

How a User Connects

1. Redirect	A device that has not yet signed in is sent to the captive portal automatically.
2. Recognise	If the device already holds an active session — for example because it has simply moved to another part of the network — that session is resumed and no login page is shown.
3. Authenticate	Otherwise the user signs in and the credentials are verified against the directory.
4. Apply policy	Group membership and any per-user restriction determine the device allowance and session duration; the session is recorded.
5. Admit	Verified identity is published to the enforcement point, which applies identity-based access rules for the life of the session.

High Availability

LDAP Manager is supplied as a redundant pair. Both units are fully configured and ready to serve; one carries the live traffic while the other stands by. The pair monitors itself continuously and verifies that the serving unit is genuinely answering users — not merely that it is powered on.

AVAILABILITY FEATURE	WHAT IT MEANS FOR YOU
Automatic failover	If the serving unit stops answering, the standby takes over by itself. No operator action and no helpdesk call are required.
Sessions preserved	Signed-in users are not logged out by a failover. Live session state is kept current on the standby unit, so users continue working through the event.
Maintenance without downtime	Updates and maintenance can be carried out on one unit while the other serves users, so routine work does not need an outage window.
Automatic recovery	A unit returning to service rejoins and brings itself up to date on its own.
No single point of failure	Neither unit is special; either can carry the full user load alone.

In the reference deployment the system recorded zero unplanned failovers across the most recent seven-day observation window, with the serving unit holding continuous uptime in excess of sixty days.

Measured Production Performance

The figures below were taken from a live deployment serving a 10,000-user higher-education campus — a mixed environment of wired laboratory networks, campus Wi-Fi, hostels and administrative offices. They are measurements taken under ordinary production load, not benchmarks run under favourable conditions.

Scale and Throughput

METRIC	MEASURED VALUE
Concurrent active sessions	10,200
Users served	6,800+ on a single day; 10,000+ accounts provisioned
New sessions established	approximately 30,000 per day
Requests handled	668,166 in a single day

Responsiveness and Reliability

METRIC	MEASURED VALUE
Average response time	43 ms across all request types
Requests exceeding 2 seconds	283 of 668,166 — 0.04%
Service error rate	0.00% — no server errors in the measured day
Unplanned failovers	none across a seven-day window
Continuous uptime	60+ days

Roaming Effectiveness

Roaming resumption depends on recognising a device as it reappears on a new part of the network. Where the integration is in place, recognition succeeded for 98–99% of sessions, sustained day after day. Devices outside that scope simply sign in as normal — the feature degrades cleanly rather than failing.

98–99%	9,568	1.50	0
DEVICE RECOGNITION WHERE INTEGRATED	SESSIONS RESUMED AUTOMATICALLY PER DAY	AVERAGE ACTIVE SESSIONS PER USER	EXTRA LOGINS REQUIRED WHEN ROAMING

Before roaming resumption was introduced, users crossing between network segments were returned to the login page and accumulated duplicate sessions. After deployment, the proportion of users holding more than two simultaneous sessions fell by roughly two-thirds.

Specifications

Integration

Directory	LDAP directory services over an encrypted connection.
Network enforcement	Verified identity is published to the customer's firewall or access-control point for identity-based policy. Supported platforms are confirmed during design.
Device recognition	Integration with the customer's DHCP service enables automatic roaming resumption. Optional — the portal operates without it.
Notifications	Standard e-mail for welcome messages, account notices and one-time password-reset codes.
Client platforms	Any device with a standards-compliant browser, including the captive-network assistants built into Android, iOS, Windows and macOS. No client software or agent is required.

Deployment

Form	Supplied as a redundant pair, as physical appliances or virtual machines.
Service address	Users and administrators reach the system through a single address; failover is transparent to them.
Transport security	TLS for all user and administrative traffic; encrypted directory connections.
Sizing	Runs on standard server hardware or virtual infrastructure. The deployment described in this document carries its full production load with substantial headroom in both processing and memory. Sizing for a specific site is determined during design.

Data Retention

Session records — account, address, device identifier, sign-in and sign-out time — are retained for audit and reporting, for a period configurable to your institution's policy. System utilisation samples are retained on a separate, shorter cycle.

Talk to us

Next steps for your deployment

NEXT STEP	WHAT IT INVOLVES
Technical walkthrough	A working session with your network team covering the features that matter to your environment, and how they map onto what you run today.
Pilot deployment	A limited rollout on a part of your network, so the product is evaluated against your own users and traffic rather than a demonstration.
Proposal	Licensing, support and professional services quoted against your user count, number of sites and availability requirements.

Commercial Information

Licensing, pricing, support terms, warranty and professional-services scope are quoted per deployment. Please contact Optimus Secure for a proposal sized to your user count, site topology and availability requirements.

Optimus Secure

Network Access Management

To arrange a technical walkthrough or a pilot deployment, contact your Optimus Secure representative.

All performance figures in this document were measured on a live production deployment and are reproduced without alteration. Actual results depend on site topology, hardware and traffic profile. Specifications are subject to change.