Self Hosted SSO Identity Server with Authentik by Optick

Customer Launch and Administration Guide

AWS Marketplace AMI Publisher Optick

What this server provides
A ready to launch private SSO and identity access server powered by Authentik on Ubuntu 24.04 with Docker Compose, PostgreSQL, Redis, Nginx reverse proxy, first boot automation, generated akadmin credentials, backup and restore helpers, and optional SSL setup.

Item	Value
Operating system	Ubuntu 24.04
Application	Authentik 2026.2.3
Runtime	Docker Compose with PostgreSQL and Redis
Default access model	Public IP first with optional domain and HTTPS later
Default OS user	ubuntu

Important first launch note

Please wait and refresh if needed
On a fresh AWS launch, the first boot service generates secrets, creates the akadmin password, writes the help page, and starts the Authentik containers. If http://PUBLIC_IP/ does not show the login page immediately, wait about one minute and refresh the page. This is normal during first boot.

Quick Start

Step	Action	Success looks like
1	Launch the AMI with a public IP and open the required security group ports.	The instance is reachable by SSH and browser.
2	Connect by SSH using the ubuntu user and your Amazon private key.	You can read FIRST_LOGIN.txt.
3	Open the Authentik login URL in a browser.	The Authentik login page appears.
4	Sign in as akadmin using the generated password from FIRST_LOGIN.txt.	You reach the Authentik admin interface.
5	Change the generated akadmin password and configure MFA.	The administrator account is secured.

Before You Begin

- Use an AWS account that can launch EC2 instances from AWS Marketplace AMIs.
- Assign a public IPv4 address to the instance during launch.
- Open inbound TCP port 80 for browser access and TCP port 22 for SSH administration.
- Open TCP port 443 only if you plan to configure optional HTTPS with a domain name.
- Have your Amazon private key available for SSH access as the ubuntu user.

Recommended Instance Sizes

Use case	Recommended instance	Notes
Small evaluation	t3.medium	Good for basic testing and light SSO evaluation.
Recommended default	t3.large or m6i.large	Safer choice for steadier use and multiple integrations.
Heavier production use	m6i.xlarge or larger	Use for more users, more providers, and heavier authentication activity.

Required Security Group Ports

Port	Protocol	Source	Purpose
22	TCP	Your administrator IP range	SSH access to the Ubuntu server.
80	TCP	0.0.0.0/0 or trusted web ranges	HTTP access to Authentik and Optick help page.
443	TCP	0.0.0.0/0 or trusted web ranges	Optional HTTPS after domain and SSL setup.
389	TCP	Trusted network ranges only	Optional LDAP outpost use if configured later.
636	TCP	Trusted network ranges only	Optional LDAPS outpost use if configured later.

Launch the Instance

1. Launch the AWS Marketplace AMI from AWS Marketplace or the EC2 console.
2. Choose an instance type that matches your expected workload.
3. Assign a public IPv4 address.
4. Allow inbound TCP port 80 and TCP port 22 in the security group.
5. Wait for the instance status checks to pass.

Connect to the instance using your Amazon private key and the **ubuntu** user:

```
ssh -i /path/to/your-key.pem ubuntu@PUBLIC_IP
```

After you connect by SSH, read the first login notes:

```
cat /home/ubuntu/FIRST_LOGIN.txt
```

First boot timing note
If the browser page is not ready immediately after launch, wait about one minute and refresh http://PUBLIC_IP/. First boot is generating credentials and starting the Authentik containers.

First Login to Authentik

Open the Authentik login page in your browser:

http://PUBLIC_IP/

Use the generated credentials shown in /home/ubuntu/FIRST_LOGIN.txt:

Credential	Value
Username	akadmin
Password	Generated uniquely on first boot and stored in /home/ubuntu/FIRST_LOGIN.txt

Security recommendation
After your first successful login, change the akadmin password immediately and store the new password securely. Also configure MFA for administrator users.

Optick Help Page

The AMI includes a local help page with the main access paths and useful commands:

http://PUBLIC_IP/optick.html

The help page is generated on first boot using the new instance public IP address.

Useful Administration Commands

Command	Purpose
optick-authentik-url	Show the current public URLs and first login reminder.
optick-authentik-status	Show Docker, Nginx, local Authentik checks, and disk usage.
optick-authentik-logs	Show recent Authentik stack logs.
optick-authentik-logs -f	Follow live Authentik logs.
optick-authentik-restart	Restart the Authentik Docker Compose stack.
optick-authentik-backup	Create a local backup of the database and application files.
optick-authentik-restore /path/to/backup.tar.gz	Restore from a local backup archive.
optick-authentik-ssl	Configure optional domain based HTTPS with Certbot.

Common validation commands:

optick-authentik-url

optick-authentik-status

optick-authentik-backup

ls -lh /opt/optick-authentik/backups

Backup and Restore

Run a backup after important setup or configuration changes:

optick-authentik-backup

Backups are written to:

/opt/optick-authentik/backups

To restore a backup, provide the backup file path and confirm the restore prompt:

optick-authentik-restore /opt/optick-authentik/backups/BACKUP_FILE.tar.gz

Backup handling
Store backups securely. The local backup command is intended for convenience. For production use, copy important backups to secure storage outside the instance.

Optional Domain and HTTPS Setup

The AMI works from the public IP by default. If you have a domain name, create a DNS A record pointing to the instance public IP, make sure ports 80 and 443 are open, then run:

optick-authentik-ssl

The helper will ask for your domain name and email address for certificate renewal notices.

Common File Locations

Path	Purpose
/opt/optick-authentik	Main application directory.
/opt/optick-authentik/docker-compose.yml	Docker Compose stack definition.
/opt/optick-authentik/.env	Runtime secrets generated on first boot. Protect this file.
/home/ubuntu/FIRST_LOGIN.txt	Generated first login notes and akadmin password.
/var/www/html/optick.html	Public help page generated on first boot.
/usr/local/sbin/optick-authentik-firstboot	First boot initialization script.
/etc/systemd/system/optick-authentik-firstboot.service	Systemd first boot service.

Troubleshooting

Issue	Recommended action
The browser does not show the Authentik login page immediately.	Wait about one minute and refresh http://PUBLIC_IP/. First boot may still be starting containers.
The page does not load at all.	Confirm the instance has a public IP and the security group allows inbound TCP port 80.
SSH does not work.	Confirm inbound TCP port 22 is open to your IP and use the ubuntu user with your Amazon private key.
Login fails with akadmin.	Run cat /home/ubuntu/FIRST_LOGIN.txt and carefully copy the generated password.
Containers are not healthy.	Run optick-authentik-status and optick-authentik-logs to review service state and logs.
Disk usage grows over time.	Review backups and logs, then move old backups off the instance if needed.

Security Notes

- Change the generated akadmin password after first login.
- Enable MFA for administrator users.
- Restrict SSH access to trusted administrator IP ranges where possible.
- Use HTTPS with a domain name for production deployments.
- Protect /opt/optick-authentik/.env because it contains runtime secrets.
- Run backups before major configuration changes and store important backups outside the instance.

Reference Links

- Authentik documentation: https://docs.goauthentik.io/
- Authentik Docker Compose installation: https://docs.goauthentik.io/install-config/install/docker-compose/
- Authentik GitHub releases: https://github.com/goauthentik/authentik/releases
- Authentik proxy provider documentation: https://docs.goauthentik.io/add-secure-apps/providers/proxy/