Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

Goal & Vision:

> **"Secure. Auditable. Role-Based. Cloud-Ready."**

This project is a real-world, **enterprise-grade IAM and Access Control demo** designed to simulate how a modern cloud company — **Henry Enterprise LLC** — would implement:

- Zero Trust principles
- Role-based portals
- Multi-Factor Authentication (MFA)
- Centralized Identity with LDAP/SSO
- Auditable access logging (Cloudwatch)
- Visualization (Grafana/Prometheus)

All built step-by-step in an RHEL 9 EC2 instance on AWS Free Tier.

> **Target Use Case**: An internal **Employee Portal for HR, IT Support, Sales,** and **Admins,** each with its own dashboard. Unauthorized users can’t access or even view protected routes. All login and access activities are logged, monitored, and visualized with CloudWatch, Prometheus, and Grafana.

Core Technologies

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

Component	**Purpose**	**Key Features**
FreeIPA	LDAP + Kerberos Backend	Centralized directory, role-based groups
Keycloak	OIDC Identity Provider	LDAP federation, MFA(TOTP), Realm roles
Flask + Apache (httpd)	Employee Portal	Secure reverse proxy, RBAC enforcement
Podman / Docker	Container runtime	Isolated Keycloak & supporting service
Prometheus + Grafana	Monitoring stack	Visual metrics dashboards, audit insights
AWS Cloudwatch	Centralized logging	Real-time log metrics & dashboards
RHEL 9 EC2	Secure host	SELinux, chronyd sync, systemd service

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

Phase 1: system prerequisite check.

[scripts/00-prereqs-check.sh]

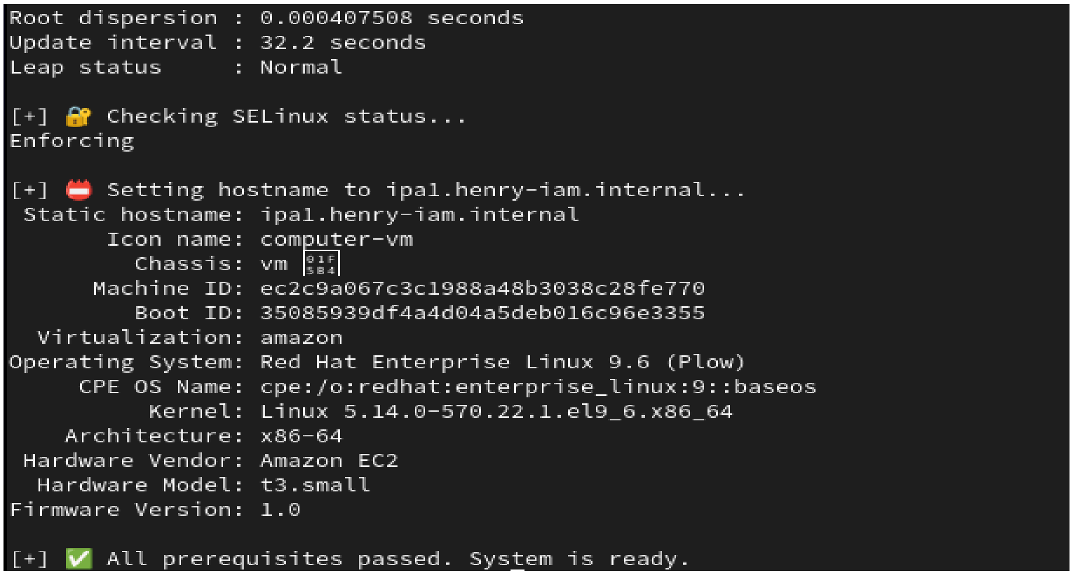
System Prerequisite check (scripts/00-prereqs-check.sh). Ensures that the environment is ready for automation.

- OS: RHEL 9 verified
- User: ec2-user (sudo-capable)
- Tools: sudo, curl, ping
- Network: outbound connectivity confirmed
- Hostname: Valid and persistent
- Time sync: chronyd running (Kerberos critical)
- SELinux: enforcing or permissive
- DNS resolution working

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

# In this step, we automated everything with a script. In our project directory on GitHub, it will be located under scripts/ as 00-prereqs-check.sh. If successful, the outcome will resemble the image below.



```
Root dispersion : 0.000407508 seconds
Update interval : 32.2 seconds
Leap status     : Normal

[+] 🔐 Checking SELinux status...
Enforcing

[+] 📛 Setting hostname to ipa1.henry-iam.internal...
 Static hostname: ipa1.henry-iam.internal
       Icon name: computer-vm
         Chassis: vm 🖴
      Machine ID: ec2c9a067c3c1988a48b3038c28fe770
         Boot ID: 35085939df4a4d04a5deb016c96e3355
  Virtualization: amazon
Operating System: Red Hat Enterprise Linux 9.6 (Plow)
     CPE OS Name: cpe:/o:redhat:enterprise_linux:9::baseos
          Kernel: Linux 5.14.0-570.22.1.el9_6.x86_64
    Architecture: x86-64
 Hardware Vendor: Amazon EC2
  Hardware Model: t3.small
Firmware Version: 1.0

[+] ✅ All prerequisites passed. System is ready.
```

Phase 2 — FreeIPA Bootstrap (With Auto Password Generation) [*scripts/20-freeipa.sh*]

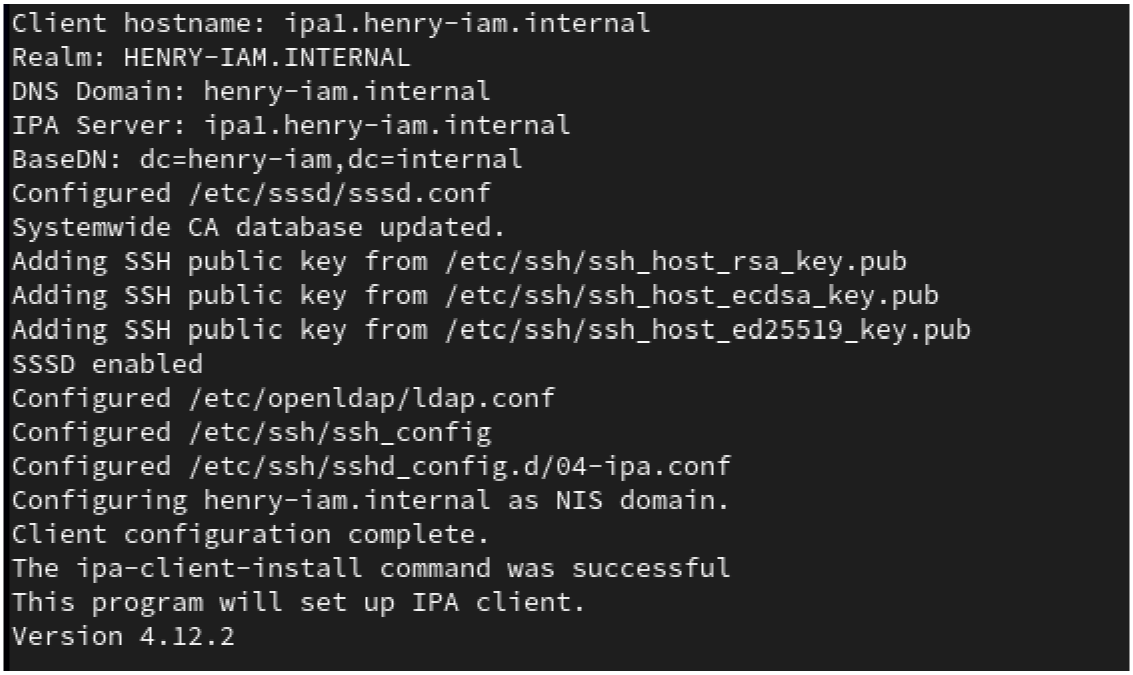
Tasks:

- Auto-install FreeIPA in integrated mode
- Domain: henry-iam.internal
- Create groups: hr, it_support, sales, admins
- Create demo users with auto-generated secure passwords
- Save credentials to /etc/henry-portal/freeipa-users.txt

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

#verify: script name, 20-freeipa.sh



```
Client hostname: ipa1.henry-iam.internal
Realm: HENRY-IAM.INTERNAL
DNS Domain: henry-iam.internal
IPA Server: ipa1.henry-iam.internal
BaseDN: dc=henry-iam,dc=internal
Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring henry-iam.internal as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
This program will set up IPA client.
Version 4.12.2
```

Phase 3 — Keycloak Setup (OIDC + LDAP + TOTP)

[scripts/30-keycloak.sh]

Tasks:

- Pull Keycloak image (v23+)
- Auto-generate admin credentials

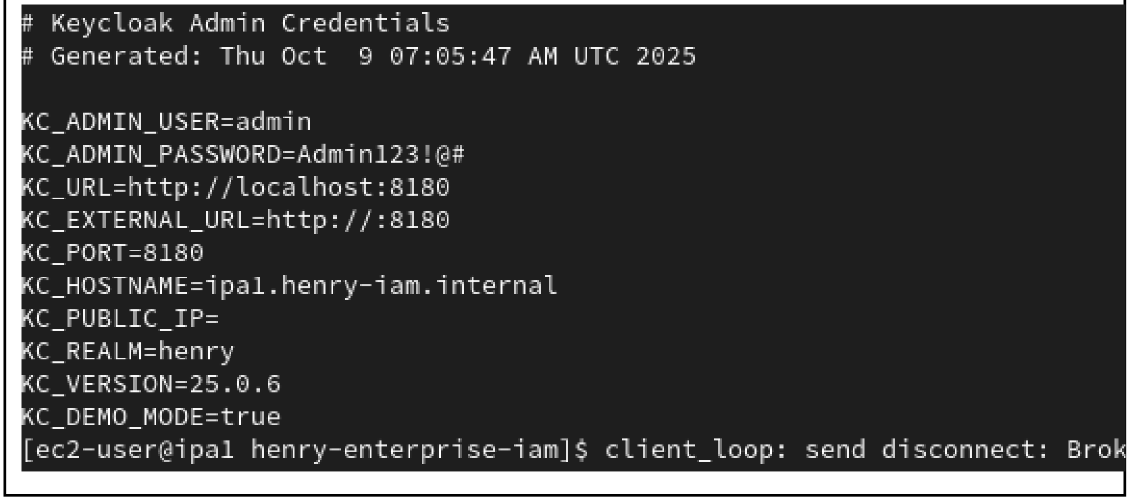
Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

- Configure LDAP bind to FreeIPA
- Enable TOTP (MFA)
- Create realm: security-project-1
- Create OIDC client: employee-portal

Outcome: Keycloak admin console available on http://<host>:8180/ and LDAP users can now authenticate with MFA

#Verify. In the image, we will see the details of our configured Keycloak. When we log in with the admin details, we will get the second image.

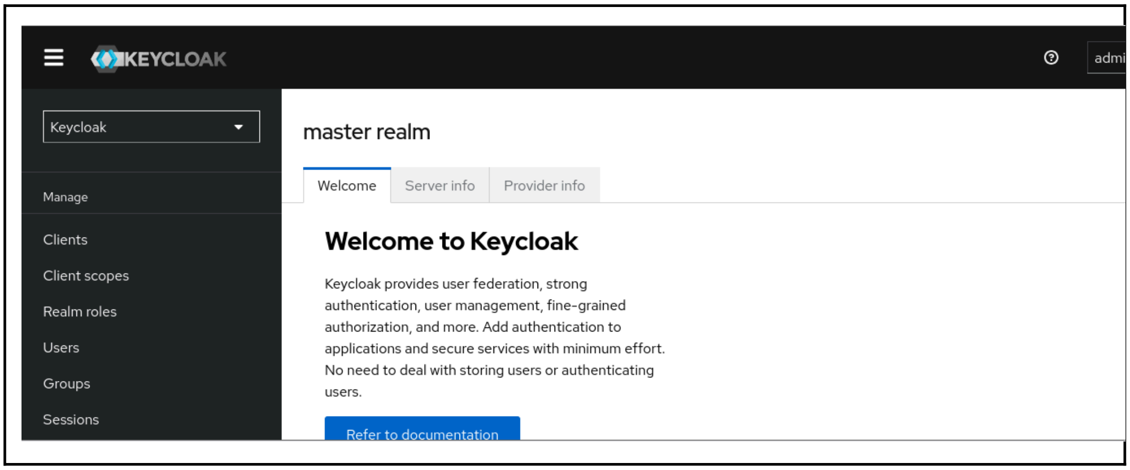


```
# Keycloak Admin Credentials
# Generated: Thu Oct  9 07:05:47 AM UTC 2025

KC_ADMIN_USER=admin
KC_ADMIN_PASSWORD=Admin123!@#
KC_URL=http://localhost:8180
KC_EXTERNAL_URL=http://:8180
KC_PORT=8180
KC_HOSTNAME=ipa1.henry-iam.internal
KC_PUBLIC_IP=
KC_REALM=henry
KC_VERSION=25.0.6
KC_DEMO_MODE=true
[ec2-user@ipa1 henry-enterprise-iam]$ client_loop: send disconnect: Brok
```

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe



master realm

Welcome to Keycloak

Keycloak provides user federation, strong authentication, user management, fine-grained authorization, and more. Add authentication to applications and secure services with minimum effort. No need to deal with storing users or authenticating users.

Phase 4 – Automated Realm + Roles + Clients Setup

[scripts/40-keycloak-init.sh]

Uses kcadm.sh for fully automated realm provisioning.

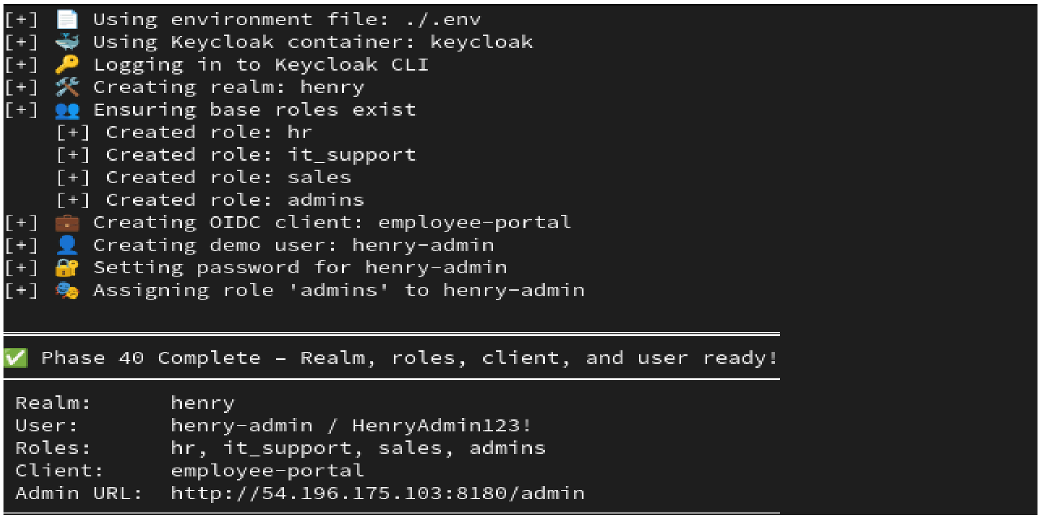
Tasks:

- Create realm: henry-enterprise
- Create roles: HR, IT Support, Sales, Admin
- Create OIDC clients: employee-portal, hr-portal
- Configure:
    1. Token lifespan
    2. Secure redirects URLS
    3. Role mappings to JWT claims

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

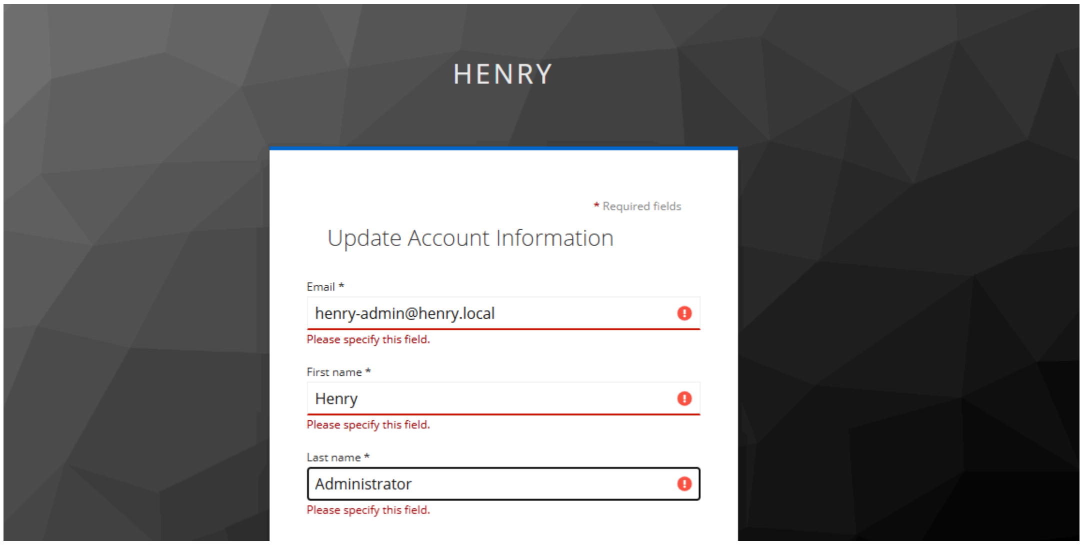
#verify



```
[+] 📄 Using environment file: ./.env
[+] 🐳 Using Keycloak container: keycloak
[+] 🔑 Logging in to Keycloak CLI
[+] 🛠 Creating realm: henry
[+] 👥 Ensuring base roles exist
    [+] Created role: hr
    [+] Created role: it_support
    [+] Created role: sales
    [+] Created role: admins
[+] 💼 Creating OIDC client: employee-portal
[+] 👤 Creating demo user: henry-admin
[+] 🔐 Setting password for henry-admin
[+] 🎭 Assigning role 'admins' to henry-admin

✅ Phase 40 Complete – Realm, roles, client, and user ready!

 Realm:        henry
 User:         henry-admin / HenryAdmin123!
 Roles:        hr, it_support, sales, admins
 Client:       employee-portal
 Admin URL:    http://54.196.175.103:8180/admin
```



* Required fields

Update Account Information

Email *

henry-admin@henry.local

Please specify this field.

First name *

Henry

Please specify this field.

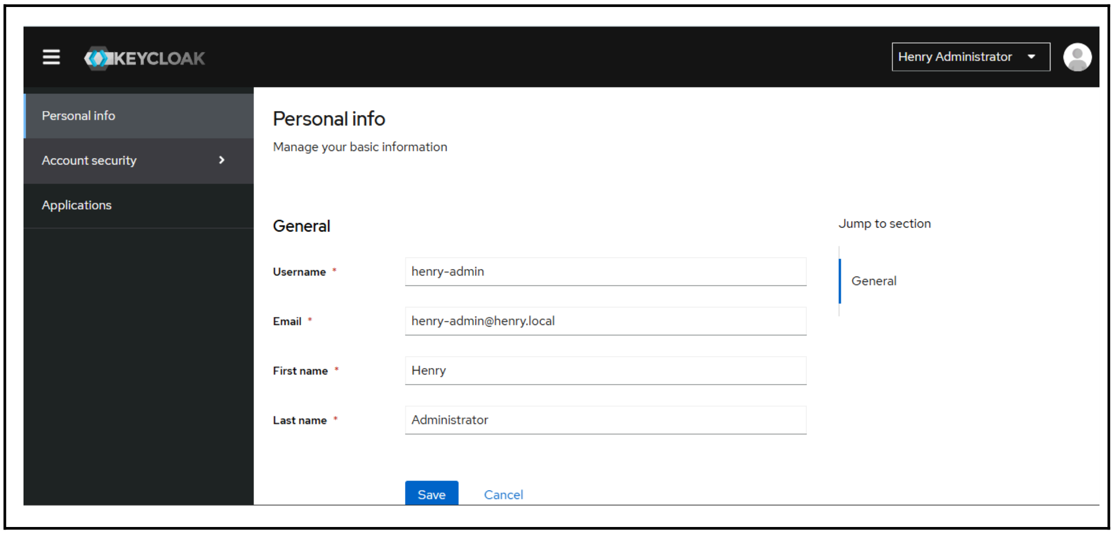
Last name *

Administrator

Please specify this field.

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe



Personal info

Manage your basic information

General

Username * henry-admin

Email * henry-admin@henry.local

First name * Henry

Last name * Administrator

Phase 5 – Direct LDAP Auth Portal (Apache + Flask)

[scripts/50-portal.sh]

Tasks:

- Deploy Flask web app under /employee/
- Configure Apache reverse proxy + systemd service
- Implement role-based views
    1. /hr
    2. /it
    3. /sales
    4. /admins

Log all authentication attempts to /var/log/henry-portal/access.log

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

Phase 6 — OIDC-Protected Employee Portal (/portal)

(scripts/60-portal-oidc.sh)

The goal in this phase is to build a secure, role-based **Employee Portal** served under **https://<host>/portal/** and protected by Keycloak (OIDC).

The main business website landing page will represent **Henry Enterprise LLC,** with a clearly labeled link to the employee portal. Once the user clicks “Portal,” they are prompted to log in with their Keycloak credentials, and upon authentication, are redirected to a role-specific custom page:

- “**HR = HR dashboard”**
- **“IT Support = IT dashboard”**
- **“Sales = CRM/leads dashboard”**
- **“Admin = Full access dashboard”**

Role Mapping (Realm Roles → portal Views”

Realm Roles	**Portal Views**
hr	HR dashboard: employee table
it_support	IT tools: logs/tickets summary
sales	Sales: Leads/CRm sample
admins	Admin: user counts + full access

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

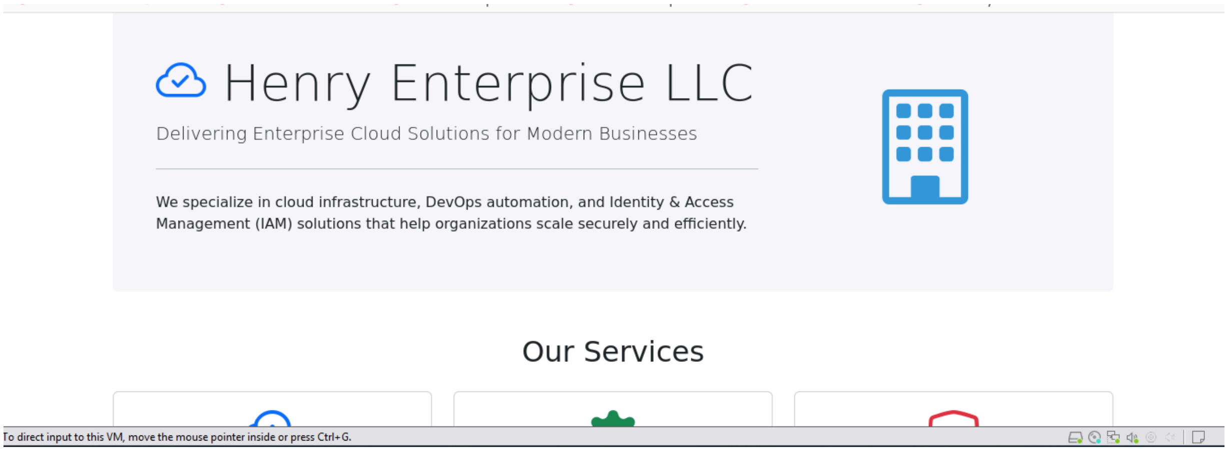
Author: Henry Ibe

Each role has a distinct, visually separate web page representing its domain, not just conditional components on the same page. After login, users are redirected to their custom section immediately based on their realm role.

- MFA enforced during Keycloak login

#verify

1. **Landing page for our business**



Henry Enterprise LLC

Delivering Enterprise Cloud Solutions for Modern Businesses

We specialize in cloud infrastructure, DevOps automation, and Identity & Access Management (IAM) solutions that help organizations scale securely and efficiently.

Our Services

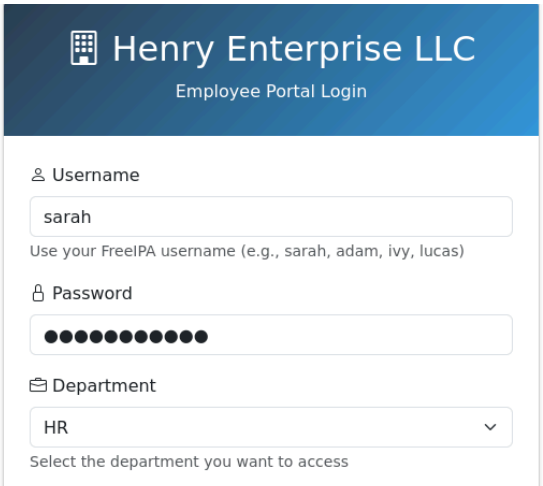
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

#verify: Logging in as the user Sarah in the HR dept.

2.

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe



Henry Enterprise LLC

Employee Portal Login

Username

sarah

Use your FreeIPA username (e.g., sarah, adam, ivy, lucas)

Password

●●●●●●●●●●●

Department

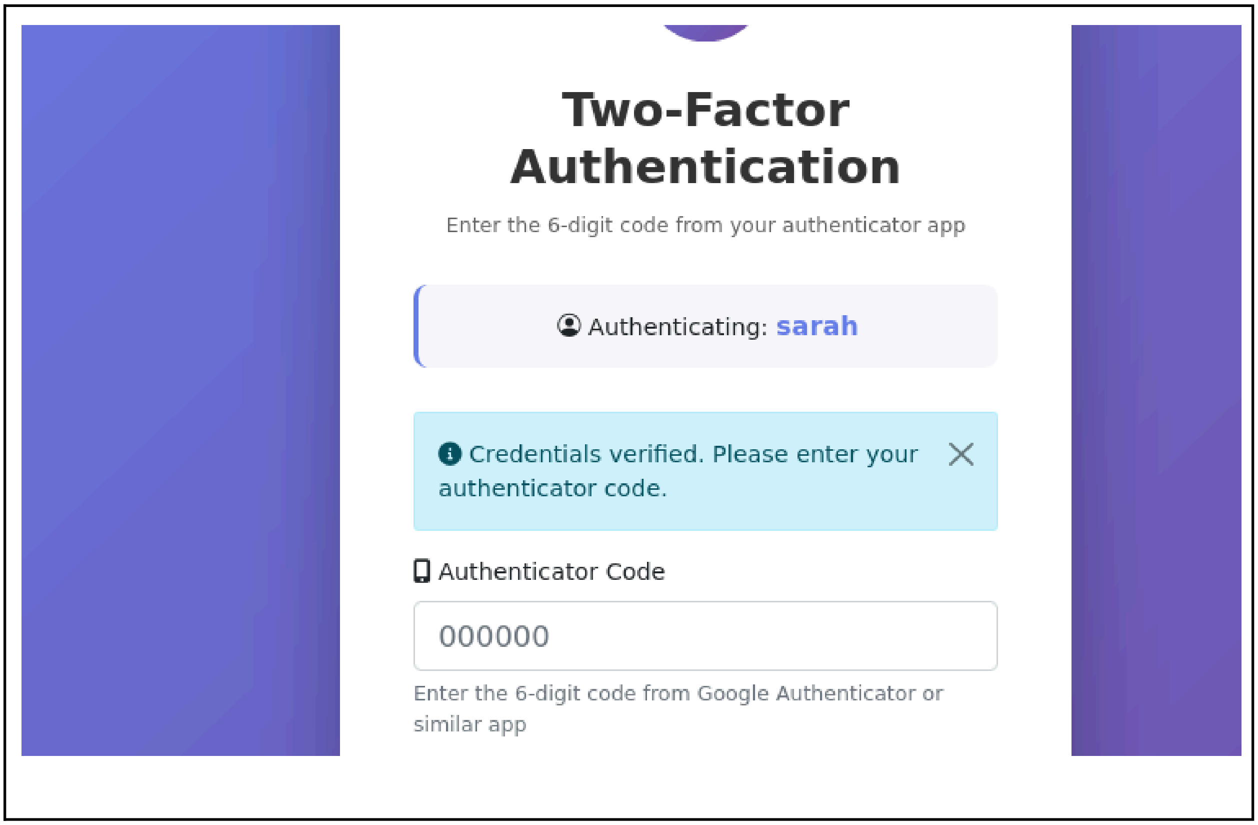
HR

Select the department you want to access

#verify: I will be prompted for a TOTP code from my Google Authenticator.
3.

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe



Two-Factor Authentication

Enter the 6-digit code from your authenticator app

Authenticating: **sarah**

Credentials verified. Please enter your authenticator code.

Authenticator Code

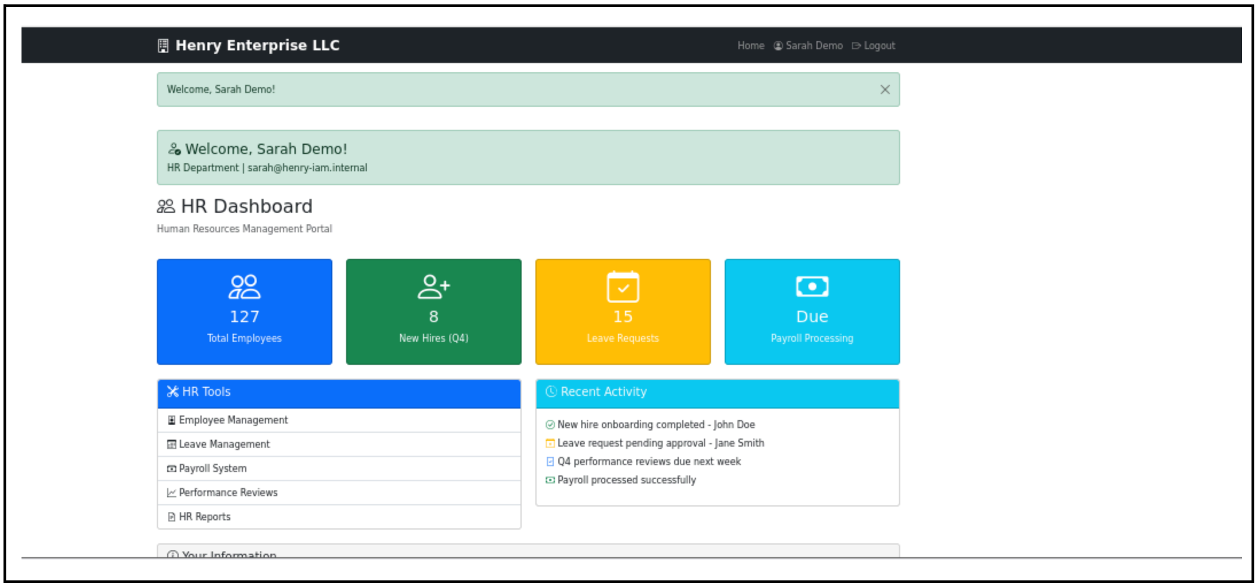
000000

Enter the 6-digit code from Google Authenticator or similar app

#verify: A custom dashboard for user Sarah in the HR department will show when successfully authenticated.
4.

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe



Welcome, Sarah Demo!

Welcome, Sarah Demo!
HR Department | sarah@henry-iam.internal

HR Dashboard
Human Resources Management Portal

127
Total Employees

8
New Hires (Q4)

15
Leave Requests

Due
Payroll Processing

HR Tools
- Employee Management
- Leave Management
- Payroll System
- Performance Reviews
- HR Reports

Recent Activity
- New hire onboarding completed - John Doe
- Leave request pending approval - Jane Smith
- Q4 performance reviews due next week
- Payroll processed successfully

Your Information

Phase 7 - Observability with Grafana & Prometheus [*scripts/70-monitoring.sh*]

Adds monitoring and audit visualization.

Metrics Tracked

- Failed logins
- Invalid TOTP attempts
- Unauthorized role access
- Login latency

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

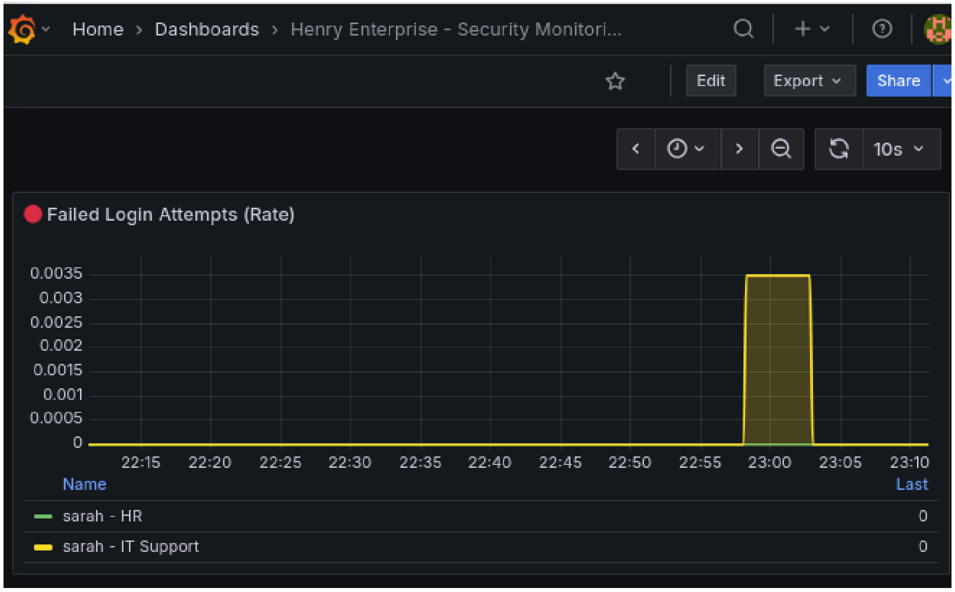
- Login count by department
- Successful authentications

Tools

- Prometheus scrapes Flask and Apache logs
- Grafana dashboards visualize metrics

Outcome: Security dashboards display real-time authentication and access metrics.

#verify: Built out Grafana dashboard

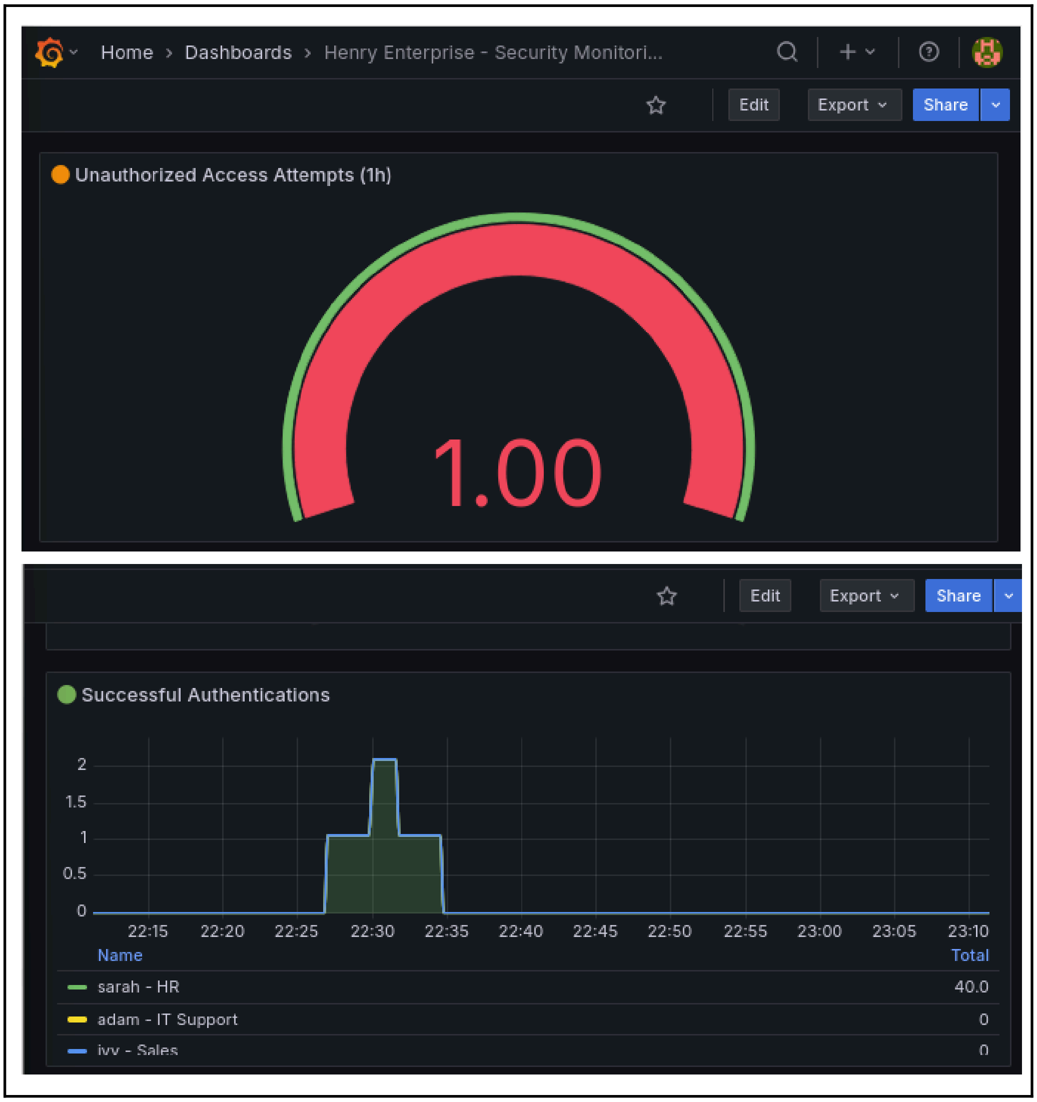


● Failed Login Attempts (Rate)

Name	Last
🟩 sarah - HR	0
🟨 sarah - IT Support	0

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

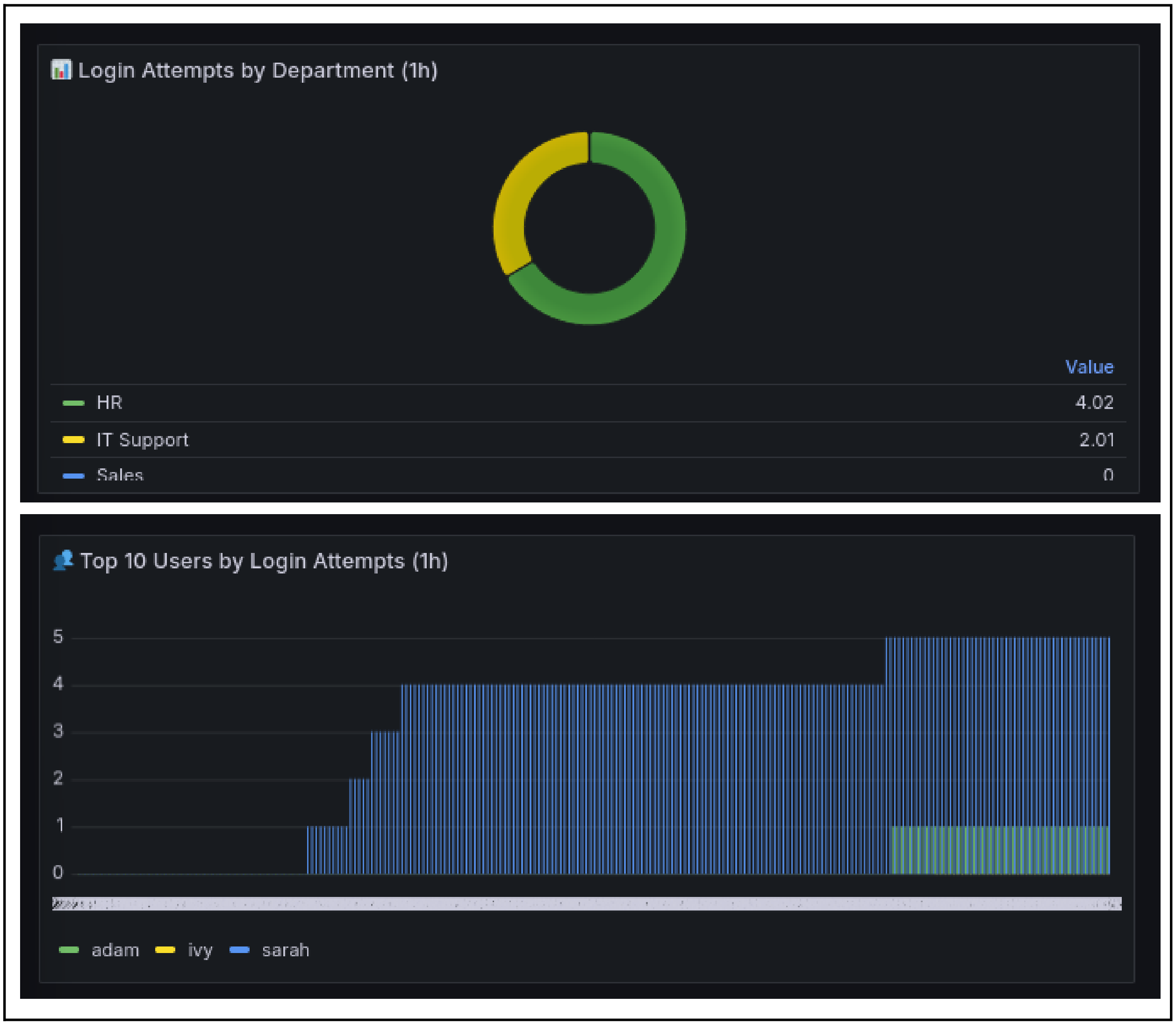
Author: Henry Ibe


Home › Dashboards › Henry Enterprise - Security Monitori...
Edit
Export
Share
Unauthorized Access Attempts (1h)
1.00
Edit
Export
Share
Successful Authentications
2
1.5
1
0.5
0
22:15
22:20
22:25
22:30
22:35
22:40
22:45
22:50
22:55
23:00
23:05
23:10

Name	Total
sarah - HR	40.0
adam - IT Support	0
ivy - Sales	0

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe



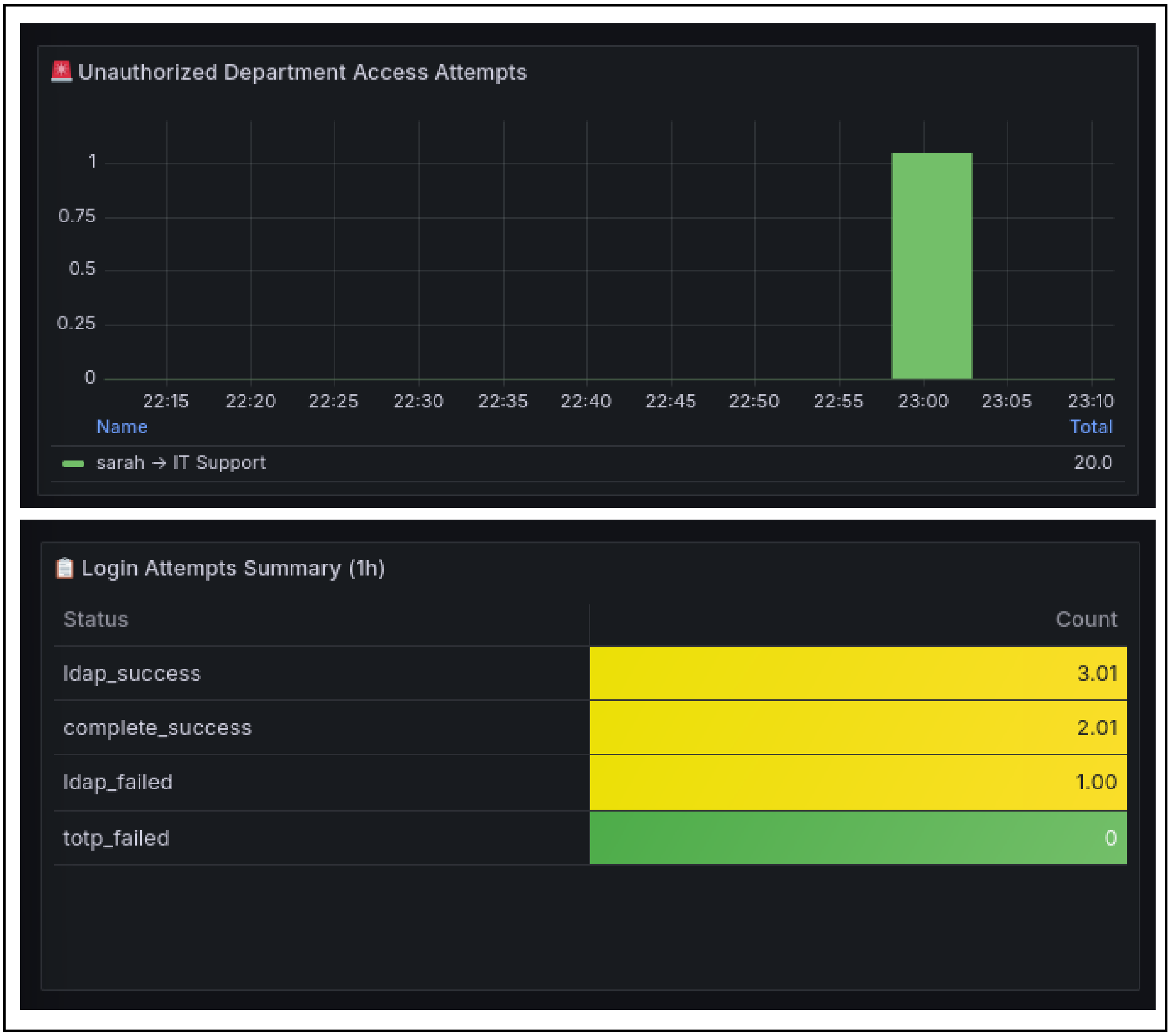
📊 Login Attempts by Department (1h)

	Value
🟩 HR	4.02
🟨 IT Support	2.01
🟦 Sales	0

👤 Top 10 Users by Login Attempts (1h)

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

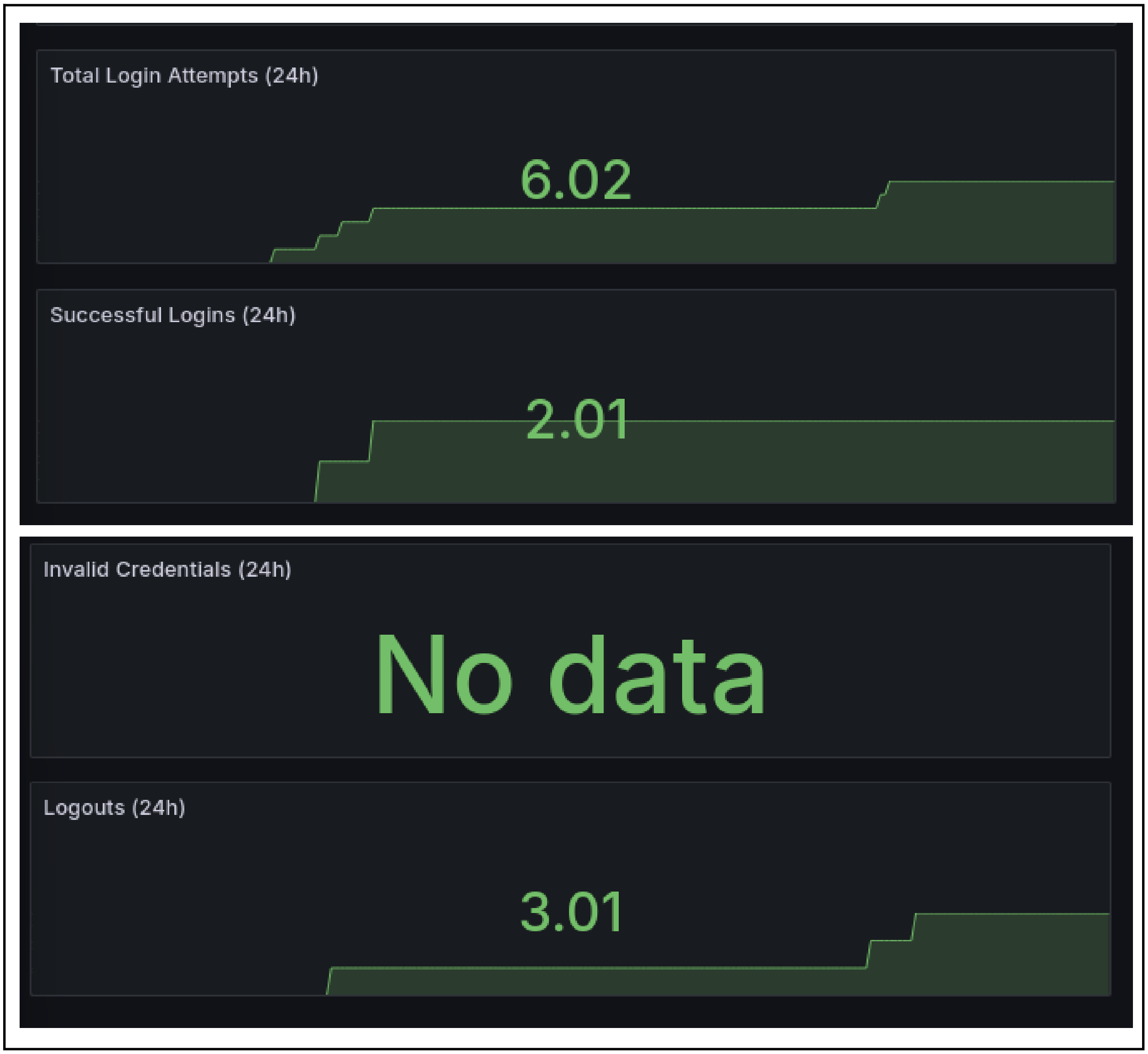


📋 Login Attempts Summary (1h)

Status	Count
ldap_success	3.01
complete_success	2.01
ldap_failed	1.00
totp_failed	0

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe



Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe

Core Security Principles Demonstrated

Security Control	**Implementation**
Zero Trust	Every request is authenticated; no implicit trust
Least Privilege	Role-based route enforcement
MFA	Keycloak TOTP via Google Authenticator
Auditable Access	Cloudwatch + Prometheus + Grafana
Centralized Identity	FreeIPA (LDAP/Kerberos) + Keycloak (OIDC)
Defense in Depth	Apache reverse proxy, SELinux, SSL/TLS readiness

Henry Enterprise Secure Portal - MFA-Enabled Role-Based Access System”

Author: Henry Ibe