Securaa Installation and Deployment Guide

Contact Information
support@securaa.io

432,6th Main, Vijay Nagar, Mysore, 1st Stage KA 570017 IN

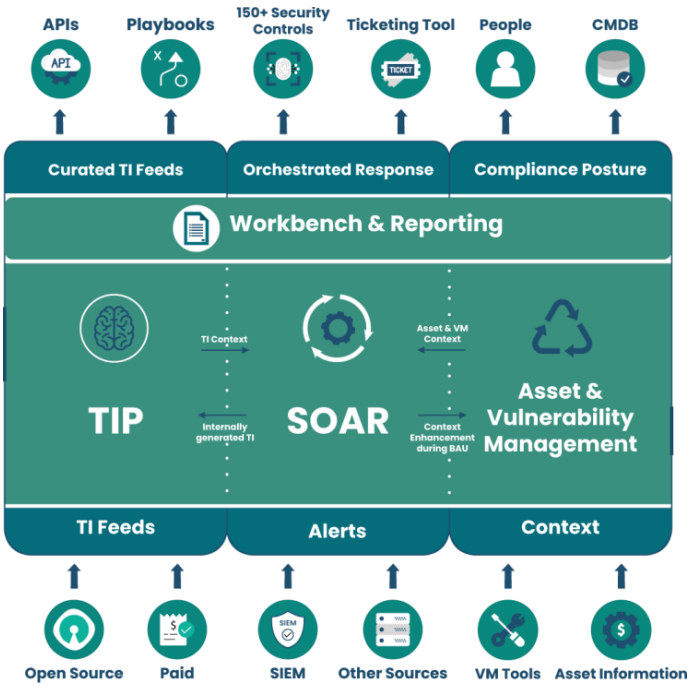
Last Revised: 01 July 2023

Contents

Securaa Platform Overview

Securaa brings together the benefits of a mature threat intelligence platform (TIP), proactive asset and vulnerability management (AVM), and reliable security orchestration, automation, and response (SOAR) under a single umbrella.

- Threat Intelligence feeds for SOC teams to be predictive while enabling effective management of protective and detective security controls
- Unified compliance posture across assets to proactively manage the organization's vulnerability posture and security controls coverage gaps.
- Out of box API integrations and pre-configured playbooks to improve SOC's ability to shrink the triage and response time.

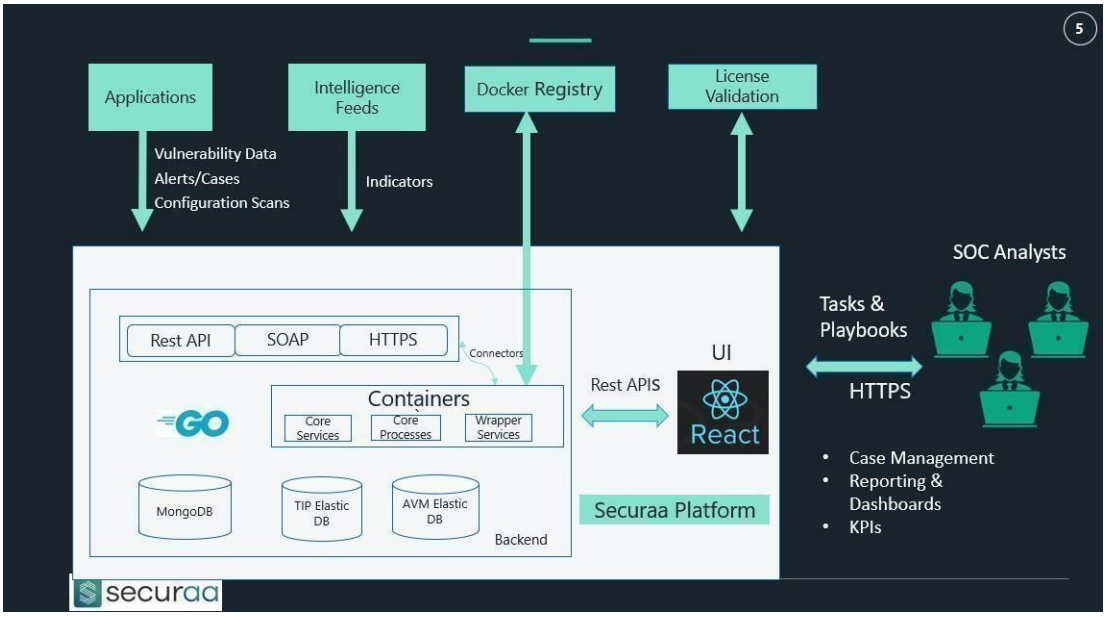


Product Components

Securaa comprises of the following components as shown in the architecture diagram below:

- Application Server (Developed in react)
- Databases (Mongo dB and Elastic)
- Intelligence feeds (Only with a TIP License) to use the Threat Intelligence Platform.
- Docker Registry: To pull the latest images from Securaa servers for installation.
- Licensing Server: To validate the license

The product is accessible through a web interface for analysts and other users.



Installation Process

Prerequisites for Deployment

Securaa needs the following for a successful deployment:

- Internet connectivity to Securaa Servers to download the latest software versions and Docker images
- Administrative privileges on the operations system platform
- SSH Connectivity tools like Putty to connect with Securaa platforms
- Browser software like Chrome to access Securaa's web interface.

Operating system requirements

Securaa can be deployed on the following operating systems and must meet the minimum hardware requirements.

Operating System	Supported Version
RHEL	9.x, 8.x
Rocky Linux	8.x
Alma Linux	8.x
Centos 9 Stream	9.x

Centos 9 Stream ISO Link: **http://mirror.stream.centos.org/9-stream/BaseOS/x86_64/iso/CentOS-Stream-9-latest-x86_64-boot.iso**

AMI'S Supported on AWS Market Place:

Operating System with Version	AMI ID
RED HAT#9	ami-0d03b1ad793d7ac93
RED HAT#8	ami-05a4c0ca40388112e
ALMA LINUX 8.6	ami-0fc548f4049251034
ROCKY Linux	ami-0246556fe022e6505

Hardware Requirements Enterprise/Standalone Setup (Proof of concept):

COMPONENT	SINGLE VM MINIMUM	MULTI VM (2 servers MINIMUM	MULTI VM (3 servers) MINIMUM
CPU	8 CPU cores	6 CPU cores	8 CPU cores
Memory	16 GB RAM	8 GB RAM	16 GB RAM
Storage	500 GB SSD	250 GB SSD	250 GB SSD

Hardware Requirements Enterprise/Standalone Setup (PRODUCTION):

COMPONENT	SINGLE VM MINIMUM	MULTI VM (2 servers MINIMUM	MULTI VM (3 servers) MINIMUM	REMOTE INTEGRATION SERVER
CPU	16 CPU cores	8 CPU cores	8 CPU cores	8 CPU
Memory	32 GB RAM	16 GB RAM	16 GB RAM	4 GB RAM
Storage	500 GB SSD	250 GB SSD	250 GB SSD	100 GB SSD

Hardware Requirements MSSP (Proof of concept):

COMPONENT	SINGLE VM MINIMUM	MULTI VM (2 servers) MINIMUM	MUTI VM (3 servers) MINIMUM	REMOTE INTEGRATION SERVER
CPU	8 CPU	4 CPU	4 CPU	8 CPU
Memory	16 GB RAM	8 GB RAM	4 GB RAM	4 GB RAM
Storage	250 GB SSD	150 GB SSD	100 GB SSD	100 GB SSD

Hardware Requirements MSSP (PRODUCTION):

COMPONENT	SINGLE VM MINIMUM	MULTI VM (2 servers) MINIMUM	MUTI VM (3 servers) MINIMUM	REMOTE INTEGRATION SERVER
CPU	16 CPU	4 CPU	4 CPU	8 CPU
Memory	32 GB RAM	8 GB RAM	4 GB RAM	16 GB RAM
Storage	500 GB SDD	150 GB SSD	150 GB SSD	150 GB SSD

Network Connectivity Requirements

The following URLs need to be whitelisted before installation. Securaa downloads the latest software version, Dockerimages, and other dependencies from these URLs:

- https://s3.us-east-2.amazonaws.com/
- https://665853670667.dkr.ecr.us-east-2.amazonaws.com/
- https://release.securaa.io:9002
- https://repo.securaa.io/
- https://production.cloudflare.docker.com
- https:// registry-1.docker.io
- https:// auth.docker.io
- https:// ecr.us-east-2.amazonaws.com
- prod-us-east-2-starport-layer-bucket.s3.us-east-2.amazonaws.com

The following ports need to be whitelisted.

1. 443 – Web access
2. 8000 – Web socket

Prerequisites Before Installation

Append "sslverify=false" in yum.conf file, present in /etc/ directory. By default, Securaa uses a self-signed certificate for the HTTPS configuration of the repository server. SSL verification needs to be disable in the yum configuration file before executing installer RPM.

wget should be pre-installed.

Note: Internet Access is mandatory for Securaa Installation only.

Securaa Installation

Below steps can be used to set up Securaa on a single virtual machine:

1. Take server SSH access download the installer rpm with the helpof URL “share by Securaa” & command.

```
ec2-user@ip-172-31-31-253:~
[ec2-user@ip-172-31-31-253 ~]$ wget --no-check-certificate https://s3.us-east-2.amazonaws.com/securaa.releases/Release+5.2/mssp/securaa_mssp_complete-5.2.0-22.x86_64.rpm
```

2. Give Read/Write permission to the installer with the help of mentioned command.
   Command: sudo chmod 777 rpm.
   Command: rpm -ivh rpm_name.rpm --force --nodeps
   The installation will start.

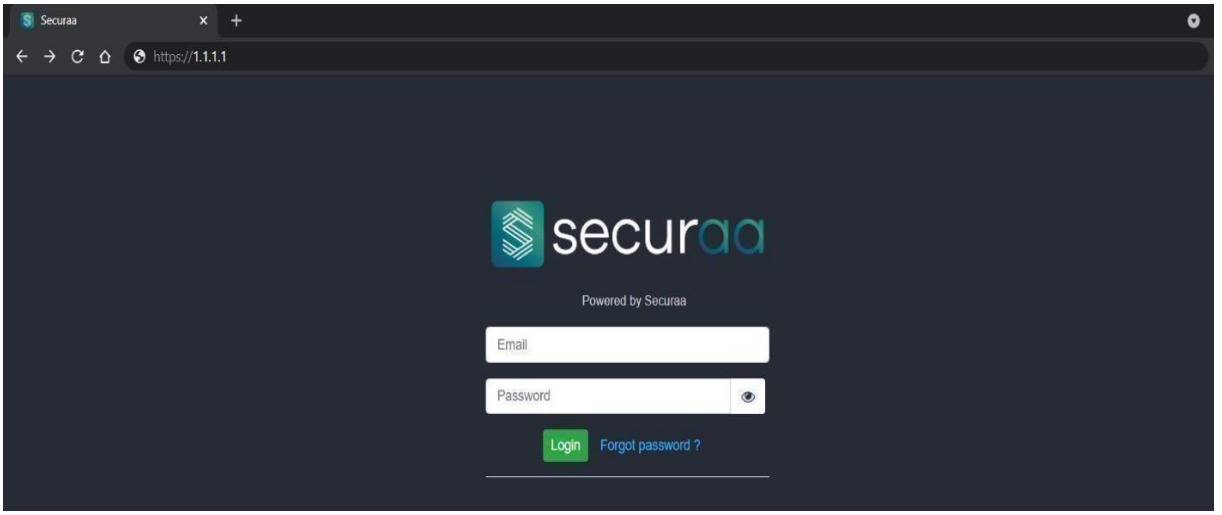
```
[root@ip-172-31-4-62 ec2-user]# ls
securaa_mssp_complete-5.2.0-22.x86_64.rpm
[root@ip-172-31-4-62 ec2-user]# rpm -ivh securaa_mssp_complete-5.2.0-22.x86_64.rpm --force --nodeps
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:securaa_mssp_complete-5.2.0-22   ################################# [100%]
Begin Installation !!
Installing zip and unzip for software unpackage...
package installed.
Installing yum utils...
package installed.
Installing python and pip packages...
package installed.
Installing flask package...
package installed.
Installing wget package...
package installed.
Installing git packages...
package installed.
```

3. After installation, Reboot the server.

```
========================================== SECURAA is Installed, Please Reboot the Machine ==============================

Created symlink /etc/systemd/system/default.target.wants/zona_manager.service → /etc/systemd/system/zona_manager.service.
Created symlink /etc/systemd/system/default.target.wants/sbot.service → /etc/systemd/system/sbot.service.
uavc:  op=setenforce lsm=selinux enforcing=0 res=1[root@ip-172-31-4-62 ec2-user]#
[root@ip-172-31-4-62 ec2-user]#
```

4. Access the Securaa Web interface through VM host IP.
   URL -> https://{server_IP}



Post Installation Configuration

***NOTE**: Please configure the following settings before you start using Securaa:*

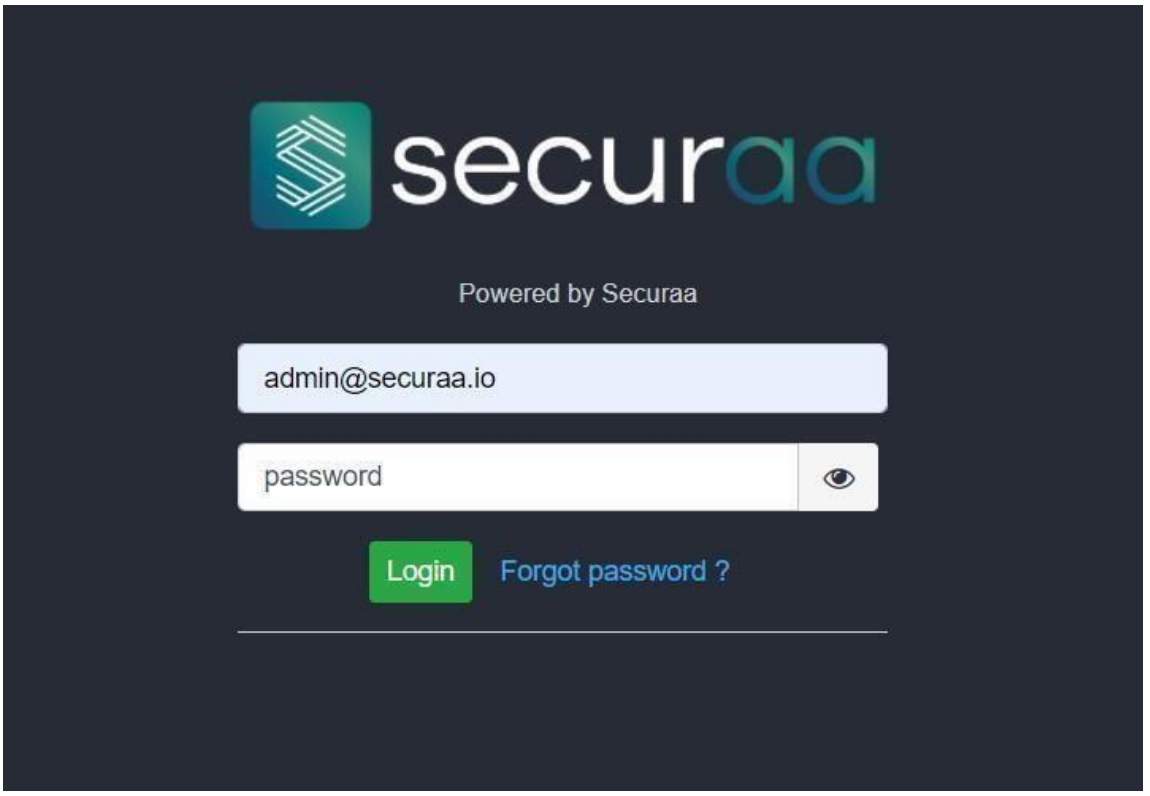
1. Reset admin password. Default credentials are [admin@securaa.io/password]
2. Adding at least 1 tenant is mandatory.
3. Setup SMTP settings. SMTP setting present under Configuration-> Platform-> General-> System. This is used for email notifications.
4. Setup SIEM batch timing.
   Use to configure the fetch interval for SIEM and other alerting sources

Accessing Securaa

Login with default credentials:

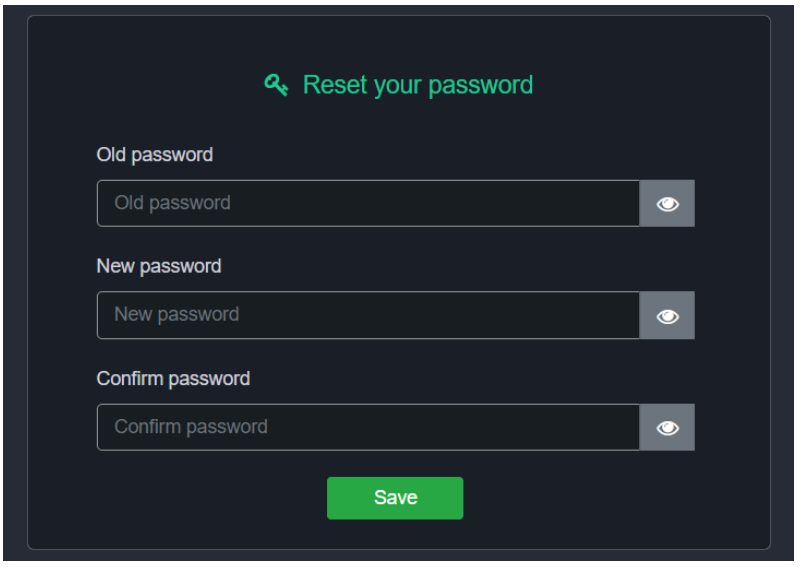
Username: **admin@securaa.io**

Password: **password**


securaa
Powered by Securaa
admin@securaa.io
password
Login
Forgot password ?

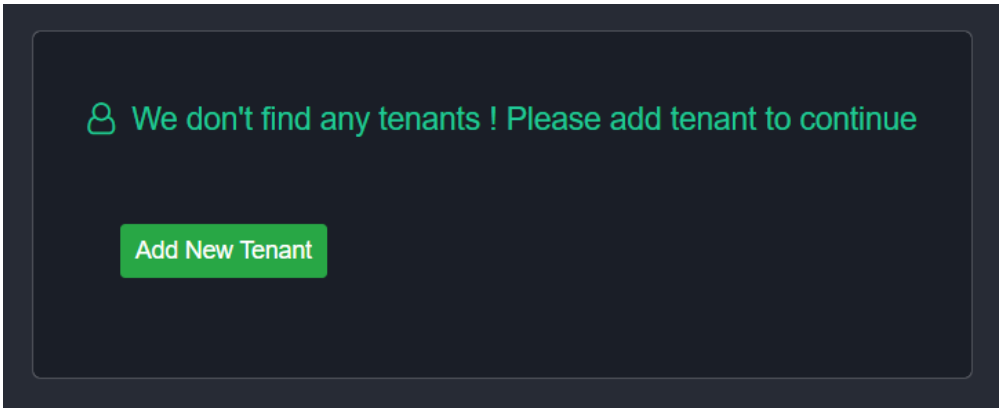
After Login, reset the "***admin***" user password.

NOTE: Admin password can only be reset ***once***.



Configuring Tenant

NOTE: MSSP version support multiple tenants. More tenants can be added from the CONFIGURATION -> PLATFORM tab.



Insert tenant details & click on the save button.

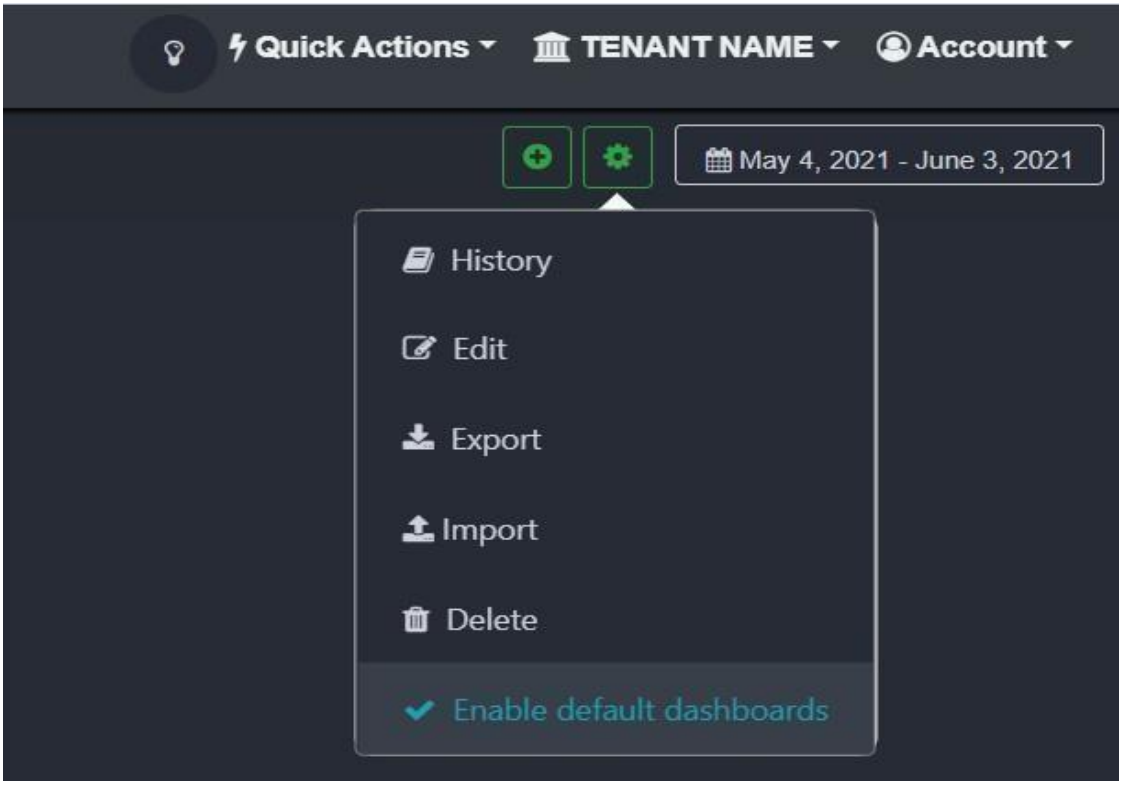
Local Host Type: A tenant database will be created in Securaa core database.

Remote Host Type: Tenant databases will be created on different remote server. For this type of tenant, 1 separate server is required.

NOTE: Multiple Remote tenants cannot be installed on the same server.

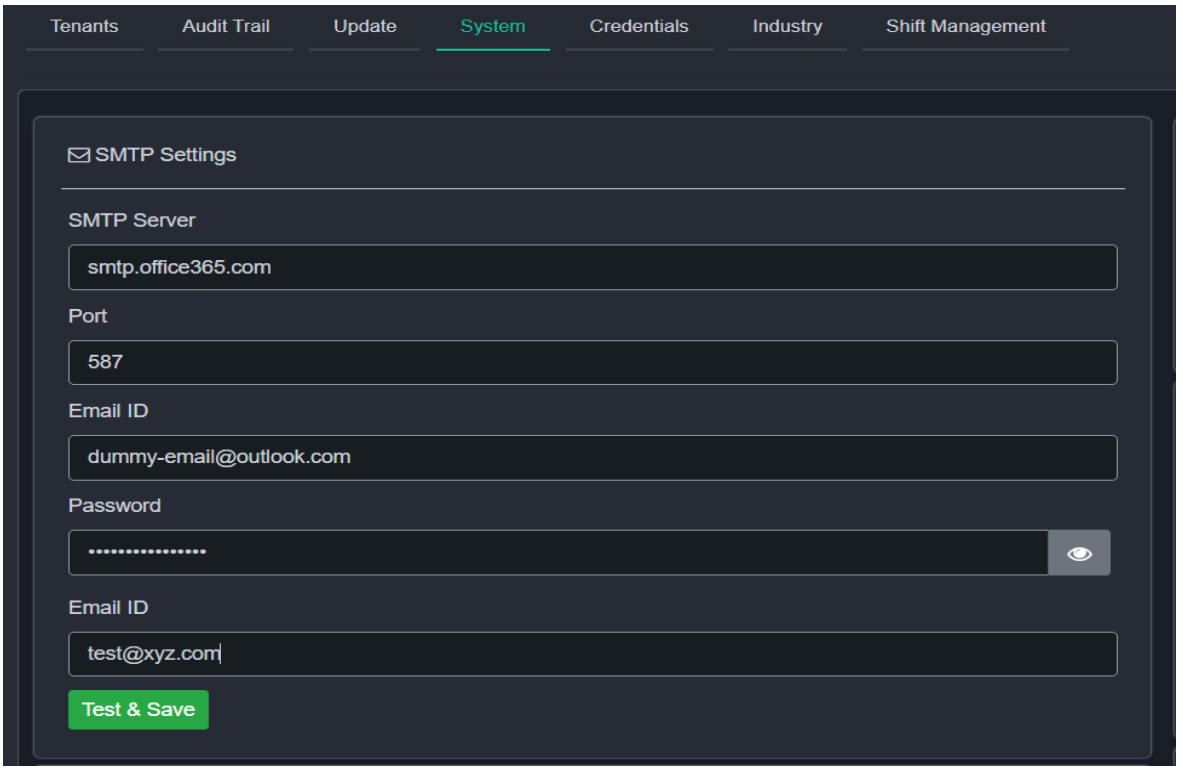
After successful tenant creation, the Dashboard page will open.

By default, Securaa does not show default dashboards. To enable the default dashboard, click on the *Setting* button, and click on "*Enable default dashboard*".



Setup SMTP server configuration

SMTP configuration present under the platform. Click on CONFIGURATION -> PLATFORM -> GENERAL -> SYSTEM



SIEM batch setting

SIEM batch setting is present on the same System page. SIEM batch is a Securaa service that fetches the offense from the SIEM application based on a defined time. 1 min can be configured for live offense ingestion.