

i14 SSIEM Project User Manual

Table of Contents

1. Introduction
2. Getting Started
3. Dashboard Overview
4. Log Queries
5. Alert Management
6. Reporting
7. User Administration
8. Troubleshooting

Introduction

Welcome to the SIEM (Security Information and Event Management) system. This manual will guide you through the features and functionalities of our SIEM solution.

Getting Started

1. Access the SIEM web interface at: <https://i14-ssiem.com>

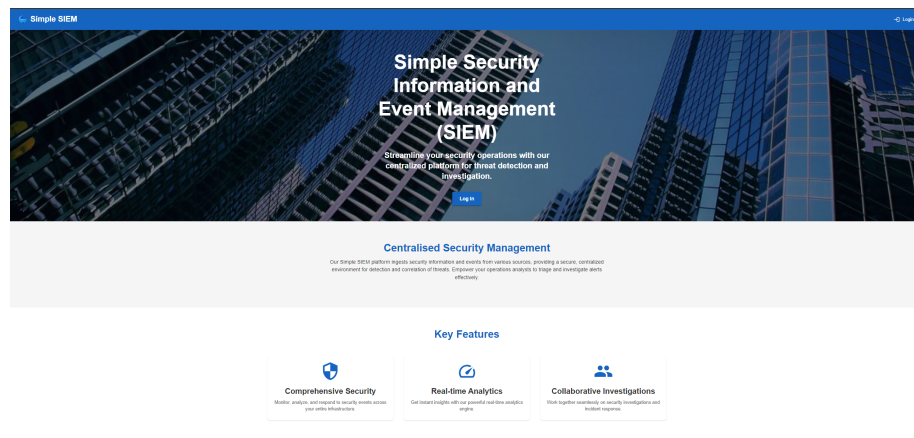


Figure 1: Landing Page

2. Log in using your provided credentials.
3. Upon first login, you'll be greeted with the dashboard.

Dashboard Overview

The dashboard provides a high-level overview of your security posture:

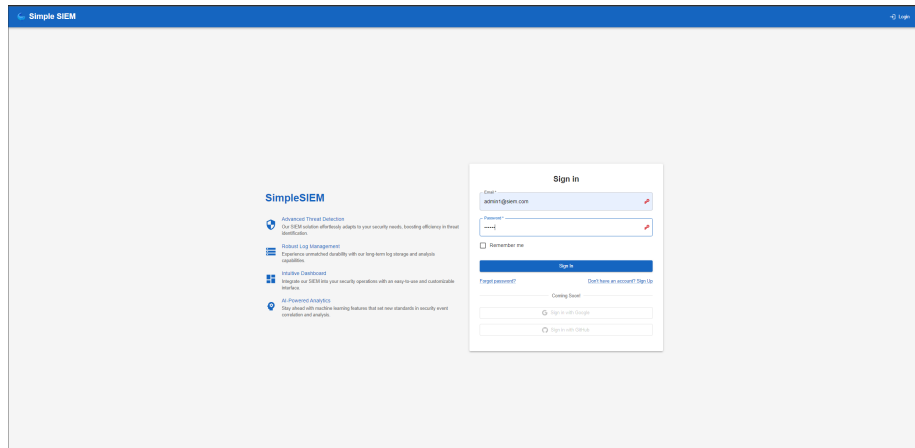


Figure 2: Login Page

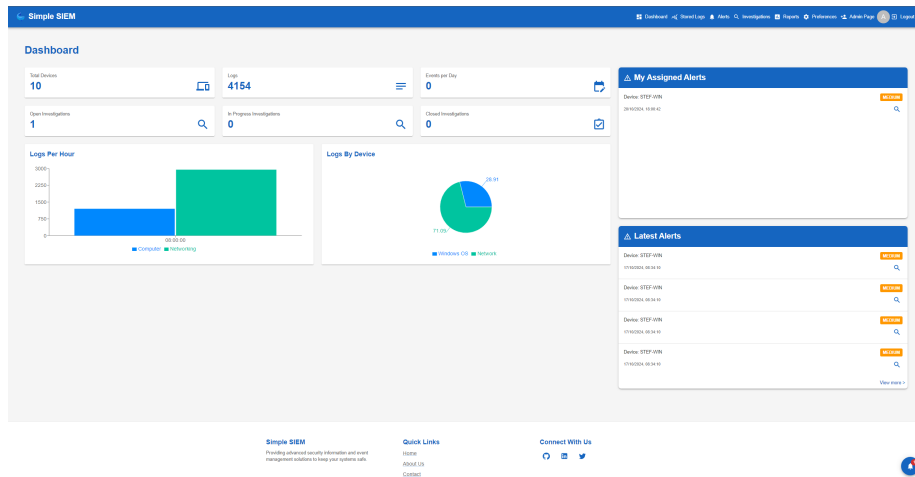


Figure 3: Dashboard Page

Dashboard Cards

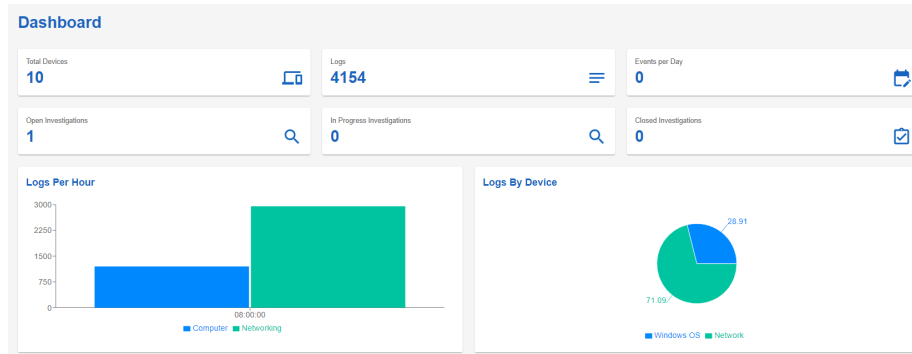


Figure 4: Dashboard Cards

- **Total Devices:** shows how many different devices have generated logs.
- **Logs:** Card shows how many logs are currently stored within the SIEM. Clickable to navigate to the stored logs page.
- **Events per Day:** Shows the number of alerts that have been generated in the past 24 hours. Clickable to navigate to the alerts page.
- **Open Investigations:** Shows the number of currently open investigations. Clickable to navigate to the Investigations page.
- **In Progress Investigations:** Shows the number of currently in progress investigations. Clickable to navigate to the Investigations page.
- **Closed Investigations:** shows the number of closed investigations. Clickable to navigate to the Investigations page.
- **Logs Per Hour:** Shows the number of alerts that have been generated per hour in a 24 hour timeline.
- **Logs by Device:** Demonstrates the portion of logs generated by device.

Alert Lists

- **My Assigned Alerts:** Shows the currently logged in user the alerts that they have been assigned. Clicking on the alert will open a pop-up window to show more details.
- **Latest Alerts:** Shows the latest alerts that have been generated by the application they have not been assigned to a user.

Log Queries

1. Navigate to the "Stored Logs" section via the Navigation bar
2. Use filters to narrow down log entries:
 - **Time range**
 - **Log source:** Computer and Router logs are stored in two different sections to allow for simpler searching.

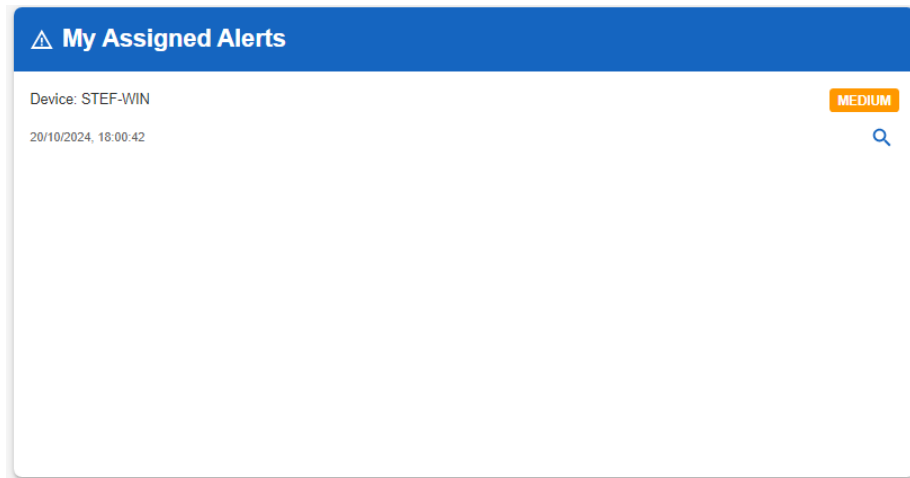


Figure 5: Assigned Alerts

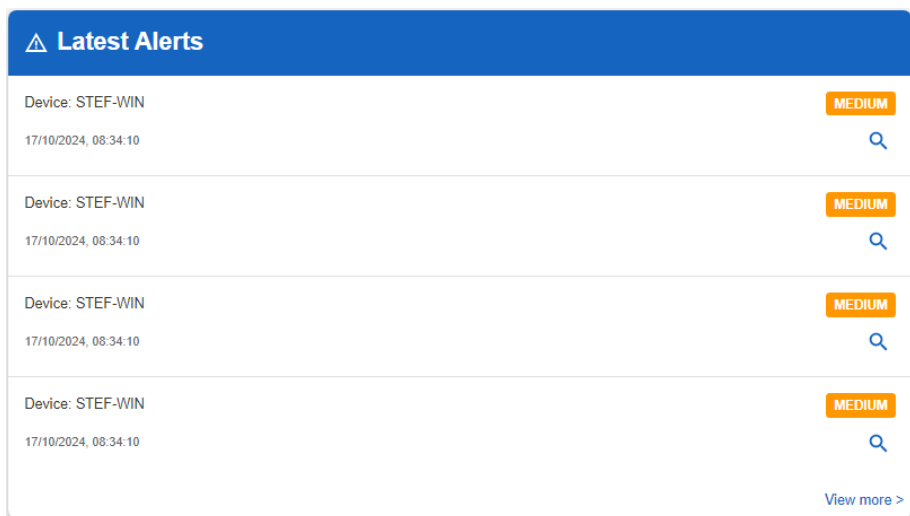


Figure 6: Latest Alerts

Alerts

Q Search alerts...

Severity

Medium

AllInfoLowMediumHighCritical

ID	Time	Hostname	Severity	Rule	
34	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	Remote Desktop Connection	
33	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	After-hours Login	
32	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	Remote Desktop Connection	
31	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	After-hours Login	
30	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	Remote Desktop Connection	
29	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	After-hours Login	
28	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	Remote Desktop Connection	
27	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	After-hours Login	
26	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	Remote Desktop Connection	
25	17/10/2024, 08:34:10	STEF-WIN	MEDIUM	After-hours Login	

Rows per page: 101-10 of 28

Figure 8: Alerts Page

Alert Details

Alert ID34

Created At17/10/2024, 08:34:10

SeverityMEDIUM

RuleRemote Desktop Connection

HostnameSTEF-WIN

Event ID4624

User IDN/A

Assignment

Assign To

Comments

Add a comment...

Close

Save Changes

Figure 9: Alert Details



Investigations						
ID	Device	Alert Type	Status	Timestamp	Assigned To	Action
1	STEF-WIN	Remote Desktop Connection	Open	17/10/2024, 08:34:10	admin1@siem.com	 

Figure 10: Investigation

Investigate Alert

Alert ID

34

Created At

17/10/2024, 08:34:10

Severity

MEDIUM

Hostname

STEF-WIN

Rule

Remote Desktop Connection

Related Logs

No related logs found.

Assigned Analyst: admin1@siem.com

Change Status

In Progress

Notes

Add investigation notes here

Cancel

Update

Figure 11: Investigation Details

Generate Report for Investigation

Generate New Report

Report Title *

Report of Investigation with Alert ID 34 at 10/17/2024, 8:34:10 AM with MEDIUM Severity

Enter a concise and descriptive title for your report

Report Type *

Security Incident

Status *

Draft

Rules

10: Remote Desktop Connection

Select rules

Select all applicable rules for this report

Description *

Author

admin1@siem.com

Cancel

Generate and Download Report

Figure 12: Generate Report

Reports Management

+ New Report

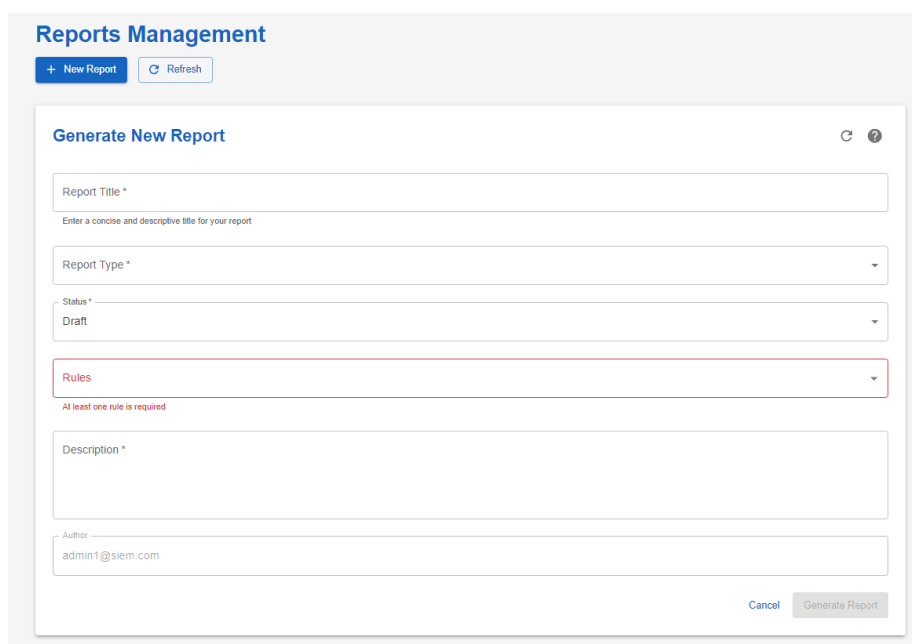
Refresh

Available Reports		▼ Show Filters	
Sample Incident Report 20	<div>System Performance</div> <div>Open</div>		
Last updated: October 21st, 2024			
Sample Incident Report 19	<div>Compliance Audit</div> <div>Open</div>		
Last updated: October 21st, 2024			
Sample Incident Report 18	<div>Network Traffic Analysis</div> <div>Archived</div>		
Last updated: October 21st, 2024			
Sample Incident Report 17	<div>Network Traffic Analysis</div> <div>Archived</div>		
Last updated: October 21st, 2024			
Sample Incident Report 16	<div>System Performance</div> <div>Pending</div>		
Last updated: October 21st, 2024			
Sample Incident Report 15	<div>User Activity</div> <div>Approved</div>		
Last updated: October 21st, 2024			
Sample Incident Report 14	<div>Compliance Audit</div> <div>Draft</div>		
Last updated: October 21st, 2024			
Sample Incident Report 13	<div>Network Traffic Analysis</div> <div>Open</div>		

Figure 13: Report Management

Reporting

1. Go to the “Reports” section
2. Choose from pre-defined report templates or create a custom report



The screenshot shows a web interface for 'Reports Management'. At the top, there's a header with the title 'Reports Management' and two buttons: '+ New Report' and 'Refresh'. Below this is a form titled 'Generate New Report'. The form contains several fields: 'Report Title *' with a placeholder 'Enter a concise and descriptive title for your report', 'Report Type *' as a dropdown menu, 'Status *' with 'Draft' selected, 'Rules' as a dropdown menu with a red border and a message 'At least one rule is required', 'Description *' as a text area, and 'Author' with the email 'admin1@siem.com'. At the bottom right of the form are 'Cancel' and 'Generate Report' buttons.

Figure 14: Generate Report

3. Set parameters (time range, data sources, etc.)
4. Generate report in various formats (PDF, CSV, HTML)
5. View Generated reports

Preferences

1. Go to Preferences page via the navigation bar.
2. View the details of the user logged in.

User Administration

For users with administrative privileges:

1. Access “Admin” section
2. Manage user accounts:
 - Create new users
 - Delete User accounts

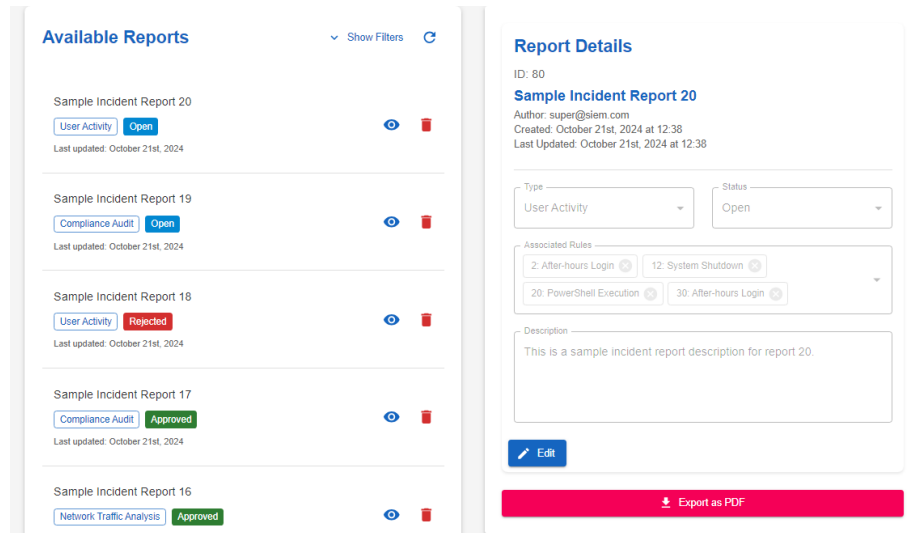


Figure 15: Report Details

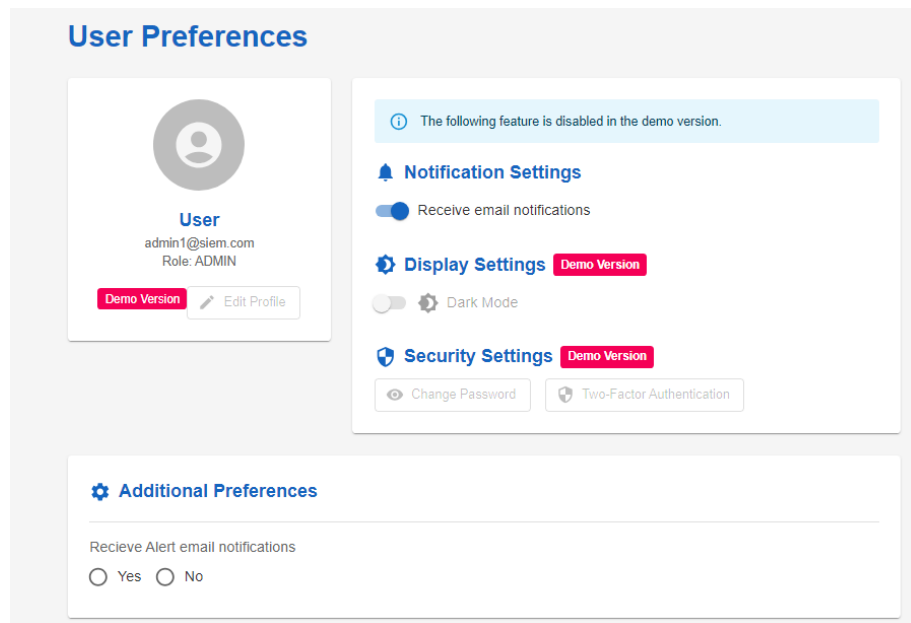


Figure 16: Preferences

The image displays a web interface for user management, divided into two main panels. The left panel, titled 'Add New User', contains a form for 'Employee User Registration'. This form includes input fields for 'First Name *', 'Last Name *', 'Email *', and 'Password *', each with a red eye icon for toggling visibility. Below these fields are radio buttons for 'Employee Role' with options 'ADMIN' and 'ANALYST'. A blue 'Submit' button is at the bottom of the form. The right panel, titled 'Existing Users', lists five users with their email addresses and roles. Each user entry has a trash icon to its right for deletion. The users listed are: admin1@siem.com (ADMIN), super@siem.com (ADMIN), user1@siem.com (ANALYST), user2@siem.com (ANALYST), and admin2@siem.com (ADMIN).

Employee User Registration	
First Name *	Last Name *
Email *	
Password *	
Employee Role	
<input type="radio"/> ADMIN	
<input type="radio"/> ANALYST	
Submit	

Existing Users	
admin1@siem.com Role: ADMIN	
super@siem.com Role: ADMIN	
user1@siem.com Role: ANALYST	
user2@siem.com Role: ANALYST	
admin2@siem.com Role: ADMIN	

Figure 17: Admin Page

- Modify user roles and permissions
 - Reset passwords
3. Configure system settings:
- Log retention policies
 - Alert rules
 - Integration with external systems

Troubleshooting

Common issues and solutions:

- No data in dashboard: Check log source connections
- Slow performance: Try narrowing time ranges for queries
- Login issues: Verify network connectivity and user account status