



SCADAfence

OT Security. At Scale.

SCADAfence Multi-Site Portal

User's Manual

Version 2.6.3

SCADAfence Ltd.**Headquarters: +972-3-7630785****Email: info@scadafence.com****Web: <https://www.scadafence.com>**

The information contained in this document, or any addendum or revision thereof is proprietary of SCADAfence Ltd. and is subject to all relevant copyright, patent and other laws and treaties protecting intellectual property, as well as any specific agreement protecting SCADAfence Ltd. rights in the aforesaid information. Any use of this document or the information contained herein for any purposes other than those for which it was disclosed is strictly forbidden.

SCADAfence Ltd. reserves the right, without prior notice or liability, to make changes in product design or specifications.

SCADAfence Ltd. assumes no responsibility for the use thereof nor for the rights of third parties, which may be affected in any way by the use thereof.

This document may contain flaws, omissions or typesetting errors; no warranty is granted nor liability assumed in relation thereto unless specifically undertaken in SCADAfence Ltd.'s sales contract or order confirmation.

Information contained herein is periodically updated and changes will be incorporated into subsequent editions. If you have encountered an error, please notify SCADAfence Ltd.

All specifications are subject to change without prior notice.

© Copyright by SCADAfence Ltd., 2022. All rights reserved worldwide.

Document Information

Document Number	SFDC-005
Product	SCADAfence Multi-Site
Document Title	SCADAfence Multi-Site Portal User's Manual
Release	Version 2.6.3
Release Date	January 2022

Table of Contents

- CHAPTER 1 ABOUT THIS MANUAL..... 9**
 - 1.1. Related Materials 9
 - 1.2. Additional Support 9
 - 1.3. Glossary 10
- CHAPTER 2 INTRODUCTION 11**
 - 2.1. SCADAfence Multi-Site Overview..... 11
 - 2.2. System Architecture 11
 - 2.3. Browser Requirements..... 12
 - 2.4. Display Requirements 12
- CHAPTER 3 GETTING STARTED 13**
 - 3.1. Login 13
 - 3.2. Menu Sidebar 14
 - 3.3. Additional Options 15
 - 3.3.1. Sorting Table Data 16
 - 3.3.2. Filtering Records 16
 - 3.4. Selecting Columns 18
 - 3.5. Header Icons 18
 - 3.6. Paging Mechanism 19
 - 3.7. Hyperlinks..... 19
 - 3.8. Alert Severity..... 19
- CHAPTER 4 DASHBOARD 20**
 - 4.1. Current Status 21
 - 4.2. Alerts per Site 21
 - 4.3. Assets per Site 23
 - 4.4. Total Alerts by Severity 24
 - 4.5. Sites Status 24
- CHAPTER 5 ALERT MANAGER 25**
 - 5.1. Alert Tabs 26
 - 5.2. Alert List 27
 - 5.3. Alert Filters..... 28
 - 5.4. Alert Resolution 28
 - 5.5. Activity Logs 28
- CHAPTER 6 ASSETS MANAGER 29**
 - 6.1. Assets List..... 30
- CHAPTER 7 SITES STATUS 33**
 - 7.1. Sites Map..... 35
- CHAPTER 8 SYSTEM SETTINGS..... 37**
 - 8.1. Settings..... 38

8.1.1.	Sites Configuration	38
8.1.2.	Sites Health Status.....	45
8.1.3.	Configuration Profile Management.....	46
8.1.4.	Account API Keys Management	57
8.1.5.	License Management	58
8.1.6.	Syslog Configuration.....	59
8.1.7.	Alerts Sources.....	61
8.2.	User Management and Security Settings.....	62
8.2.2.	Account Security Settings	65
8.3.	User Settings	66
8.3.1.	Multi-Factor Authentication	66
8.4.	System Language Settings.....	67
8.5.	Admin Settings	67
8.5.1.	Change Password	68
8.5.2.	Logout.....	68

List of Figures

Figure 1: System Architecture..... 11

Figure 2: Login Page 13

Figure 3: SCADAfence Multi-Site Dashboard Page 14

Figure 4: Menu Sidebar, in Closed and Opened States..... 14

Figure 5: Additional Options 15

Figure 6: Click on a Field Header to Change the Sorting Order 16

Figure 7: Filtering Records 16

Figure 8: Filtered Records 17

Figure 9: Clear Filters Icon..... 17

Figure 10: Selecting Columns 18

Figure 11: Header Icons 18

Figure 12: Paging Mechanism 19

Figure 13: Accessing On-Screen Help..... 19

Figure 14: Dashboard Entry in Sidebar Menu 20

Figure 15: Dashboard Page 20

Figure 16: Current Status 21

Figure 17: Choose Vertical or Horizontal Bar Charts 21

Figure 18: Alerts per Site – Vertical Bar Charts..... 22

Figure 19: Alerts per Site – Horizontal Bar Charts 22

Figure 20: Choose Vertical or Horizontal Bar Charts 23

Figure 21: Asset Distribution by Device Type – Vertical Bar Charts 23

Figure 22: Asset Distribution by Device Type – Horizontal Bar Charts 23

Figure 23: Top IPs at Risk 24

Figure 24: Traffic Volume per Protocol..... 24

Figure 25: Alert Manager Entry in Sidebar Menu 25

Figure 26: Alert Manager Page 25

Figure 27: Alerts Tabs..... 26

Figure 28: Alert List 27

Figure 29: Alert Filters..... 28

Figure 30: Asset Manager Entry in Sidebar Menu 29

Figure 31: Assets List..... 30

Figure 32: Quick Asset Summary 31

Figure 33: Asset Detailed Information 32

Figure 34: Sites Status Page 34

Figure 35: Sites Map Page 35

Figure 36: Hover to Display Site Alert Summary 36

Figure 37: Setting Entry in Sidebar Menu 37

Figure 38: General Settings Page 37

Figure 39: Settings Page 38

Figure 40: Site Configuration Page 38

Figure 41: Add New Site 40

Figure 42: Site Info Page 41

Figure 43: Exporting the Site Configuration Information 42

Figure 44: Delete Site Data 42

Figure 45: Software Update 43

Figure 46: Configuration Update Window 44

Figure 47: Sites Health Check Status 45

Figure 48: Configuration Profiles Management Page 46

Figure 49: Add New Configuration Profile 48

Figure 50: Editing a Configuration Profile 49

Figure 51: Alert Configuration Window 51

Figure 52: Confirmation for Explicit Definition of Internal IP addresses 52

Figure 53: Confirmation for Automatic Definition of Internal IP addresses 52

Figure 54: IP Group Configuration Window 53

Figure 55: Email Configuration Window 54

Figure 56: Email Scheduler Configuration Window 55

Figure 57: Active Directory Configuration Window 56

Figure 58: Site Distribution Page 57

Figure 59: Account API Keys Management Settings 58

Figure 60: License Management Page 59

Figure 61: Syslog Configuration Settings 60

Figure 62: Alert Sources Settings 61

Figure 63: Adding a New Alert Source 62

Figure 64: User Management and Security Settings Menu 62

Figure 65: User Management Settings	63
Figure 66: Add User.....	64
Figure 67: Enabling the MFA.....	65
Figure 68: White List Options.....	65
Figure 69: Adding the Additional Password.....	66
Figure 70: Google Authentication Entry	67
Figure 71: User Interface Language Setting.....	67
Figure 72: Admin Settings Menu.....	68
Figure 73: Changing the Password.....	68
Figure 74: Logout Confirmation	69

List of Tables

Table 1: Contact Us	9
Table 2: Definitions	10
Table 3: Alert Severity	19
Table 4: Current Status Fields	21
Table 5: Alert List Fields	27
Table 6: Assets List Fields.....	30
Table 7: Alert List Fields	34
Table 8: Sites Map Fields.....	35
Table 9: Sites Configuration Fields.....	39
Table 10: Add New Site Window Fields	40
Table 11: Add New Site Window Fields	43
Table 12: Configuration Update Window Fields	44
Table 13: Sites Health Status Fields	45
Table 14: Sites Health Status Detailed Information.....	46
Table 15: Configuration Profiles Management Fields.....	47
Table 16: Distribution History Fields.....	47
Table 17: Add New Profile Configuration Window Fields.....	48
Table 18: Alert Configuration Fields	51
Table 19: Email Configuration Fields.....	54
Table 20: Email Scheduler Fields.....	55
Table 21: Active Directory Fields	56
Table 22: Profile's Distribution History Fields.....	57
Table 23: Account API Keys Management Fields	58
Table 24: Syslog Configuration Fields	60
Table 25: Alert Sources Fields	61
Table 26: User Management Fields	63
Table 27: User's Fields.....	64

Chapter 1

About this Manual

This user's manual describes the operation of **SCADAfence Multi-Site**, the SCADAfence cybersecurity management portal for industrial networks. Multi-Site provides high-level monitoring capabilities for distributed networks that span multiple geographic locations and organizational units.

The manual introduces network coordinators to SCADAfence Multi-Site's user interface and its powerful, at-a-glance network monitoring tools, helping them to track cyber threats and compliance requirements, and immediately handle security and operational risks as they appear.

Release Information

- SCADAfence Multi-Site– Version 2.6.3

1.1. Related Materials

Refer to the following documents for additional information:

- *SCADAfence Multi-Site & Governance Portal Deployment Guide*
- *SCADAfence Governance Portal User's Manual*
- *SCADAfence Platform User's Manual*

1.2. Additional Support

You can contact us for more information and assistance as follows:

Table 1: Contact Us

Telephone	Email
Headquarters: +972-3-7630785	Support: support@scadafence.com

1.3. Glossary

Table 2: Definitions

Term	Definition
Asset	Any computing device in the SCADA network – including servers, endpoints, PLCs, HMIs – that has a traceable IP or MAC address.
ARP	Address Resolution Protocol. ARP is a protocol used to IP network addresses to the hardware (MAC) addresses used by a data link protocol (Ethernet).
CSV	Comma-Separated Values. Exported files containing CSV data can be viewed and processed using spreadsheet software, such as Excel.
DNS	Domain Name Server. DNS is a naming system used to translate domain names into numerical IP addresses that are used to locate and identify computer services.
HMI	Human-Machine Interface
IP	Internet Protocol. An IP address is a numerical identifier assigned to a computing device or node in a TCP/IP network. The address is used to locate and identify the node in communications with other nodes on the network.
IT	Information Technology
MAC	Media Access Control. A MAC address is a unique identifier assigned to network interfaces that supports communications at the data link layer (Ethernet) of a network segment (LAN).
OT	Operational Technology
PLC	Programmable Logic Controller. A computing device typically used to automate industrial, electromechanical processes.
SIEM	Security Information and Event Management. SIEM software provides real-time collection and analysis of security alerts generated by applications and networking hardware.
SMB	Server Message Block. A network file sharing protocol.
TCP	Transmission Control Protocol. TCP is a transport-layer protocol used to establish a network connection for the exchange of data between two applications.
UDP	User Datagram Protocol. UDP is a connectionless, transport-layer protocol that supports the exchange of datagrams between two applications.

Chapter 2 Introduction

2.1. SCADAfence Multi-Site Overview

The SCADAfence Multi-Site Portal provides an organization-wide view of ICS/SCADA operational networks and their cyber-security status, offering a unified view of geographically and operationally distinct networks. Multi-Site connects to site-specific SCADAfence Platform servers, providing administrators with enhanced visibility of their entire operational network, presenting an overview of security alerts, while allowing them to drill down and view the status on a per-site and per-asset level. The system also enables network administrators to gauge the level of network security compliance with an array of standards and requirements.

2.2. System Architecture

The SCADAfence Multi-Site Portal server receives periodic updates from the SCADAfence Platforms that are distributed throughout the organization. A PC with a Web browser is used to access the Multi-Site Portal.

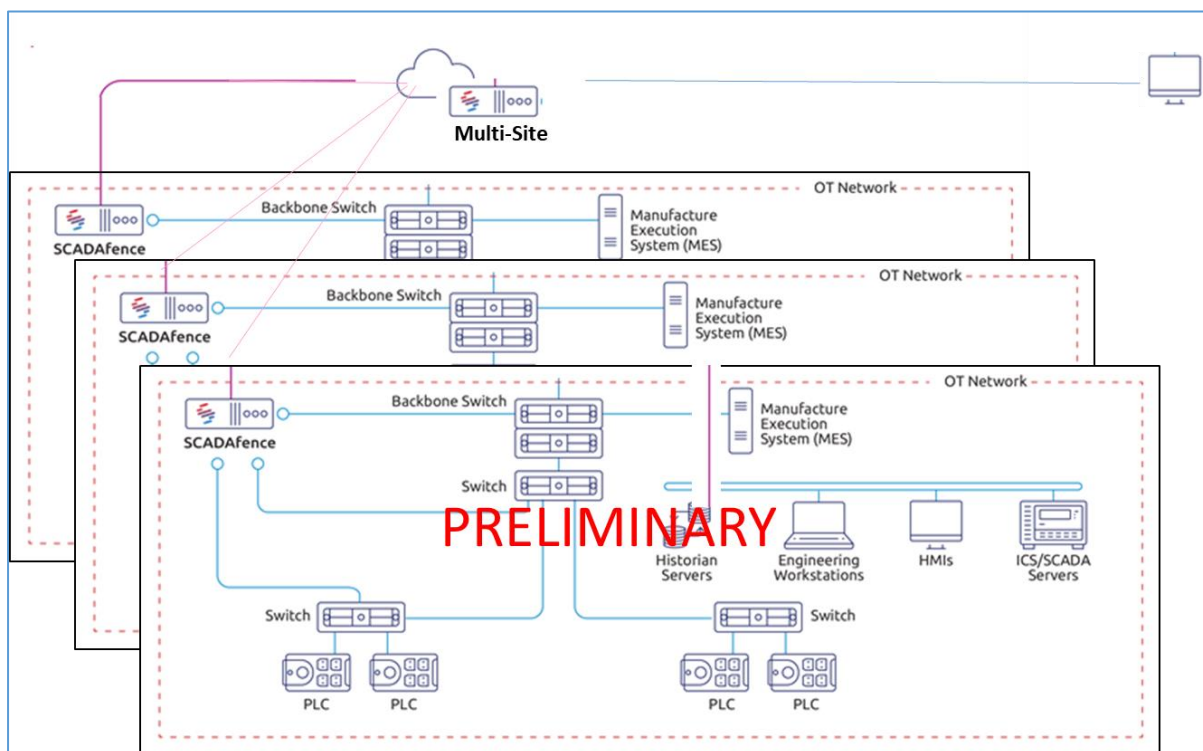


Figure 1: System Architecture

2.3. Browser Requirements

SCADAfence requires use of one of the following browsers for accessing the SCADAfence Multi-Site server:

- Google Chrome
- Mozilla Firefox

NOTE

The browser should be kept up-to-date with a version released during the last 6 months.

2.4. Display Requirements

The recommended display resolution for optimal use of the SCADAfence Multi-Site user interface is 1920 horizontal * 1080 vertical or higher. Other supported resolutions:

- 1680 x 1050
- 1440 x 900
- 1280 x 800

Chapter 3

Getting Started

This chapter is intended to help you with your first use of the system, and introduces the features of the SCADAfence Multi-Site user interface.

3.1. Login

In order to log in to the SCADAfence Multi-Site system, you will need to know the URL of the system server, as well as the username and password.

NOTE

Contact SCADAfence support if you do not know the URL of the system server.

➔ **To log in to SCADAfence Multi-Site:**

1. Enter the URL of the system server in your browser. The login page appears as shown in Figure 2 below.

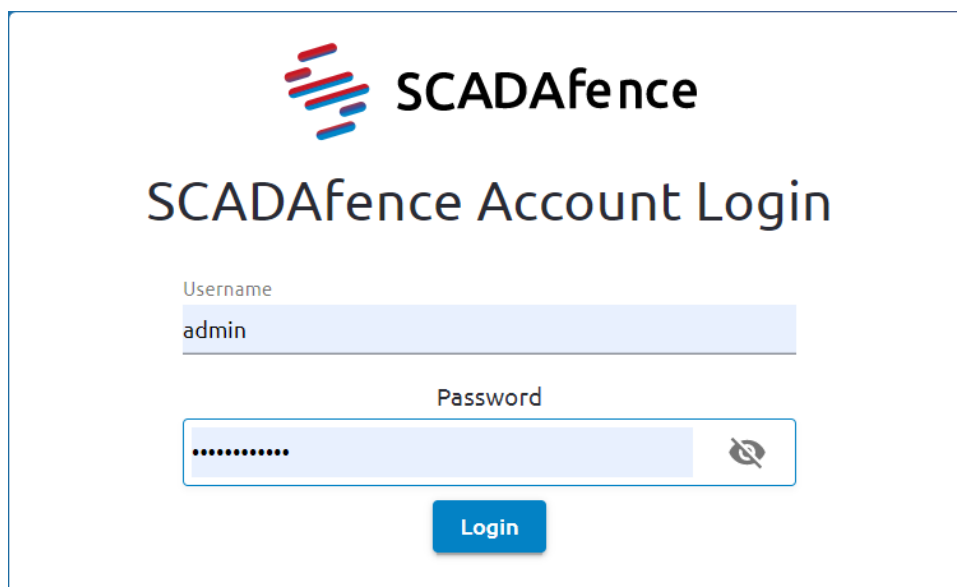


Figure 2: Login Page

2. Fill in the Username and Password fields, and click **Login**. The following are usernames and passwords for your initial login.
 - **Username:** admin
 - **Password:** 123456

NOTE

You will be required to modify the password following your initial login and then to log back in again.

The Dashboard page appears as shown in Figure 3 below.



Figure 3: SCADAfence Multi-Site Dashboard Page

3.2. Menu Sidebar

The SCADAfence Multi-Site uses a menu-driven user interface to provide access to a rich set of monitoring functions. The menu sidebar is depicted in Figure 4 below.

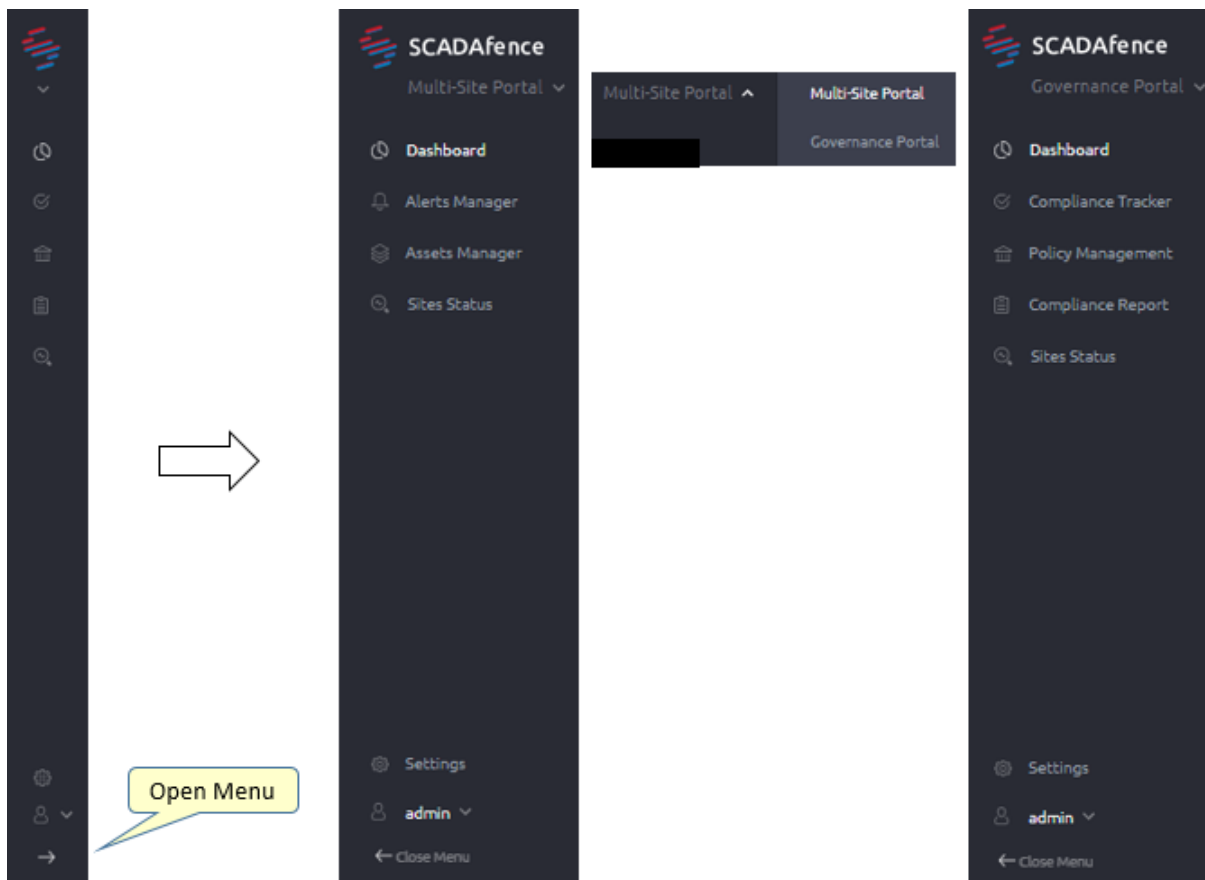



Figure 4: Menu Sidebar, in Closed and Opened States

The menu sidebar, which appears on the left side of the page, appears in iconized form, as shown on the left side of figure. Click on the **Open Menu** icon  to shown the menu in its expanded state, in which the names of the menu entries appear alongside the icons. Click on the **Close Menu** icon to return the menu to its iconized state.

The entries at the top of the menu sidebar provide access to the following SCADAfence Multi-Site functions:

Multi-Site Portal

- [Dashboard](#)
- [Alert Manager](#)
- [Asset Manager](#)
- [Sites Status](#)

Governance Portal. Please Refer to *SCADAfence Governance Portal User's Manual*

In addition, the entries on the bottom of the menu sidebar provide access to [administrative functions](#):

- [System Settings](#)
- [Admin Settings](#)

3.3. Additional Options

You can access sorting and filtering functions by clicking on the **Additional Options** icon in the relevant column, as shown in the figure below.

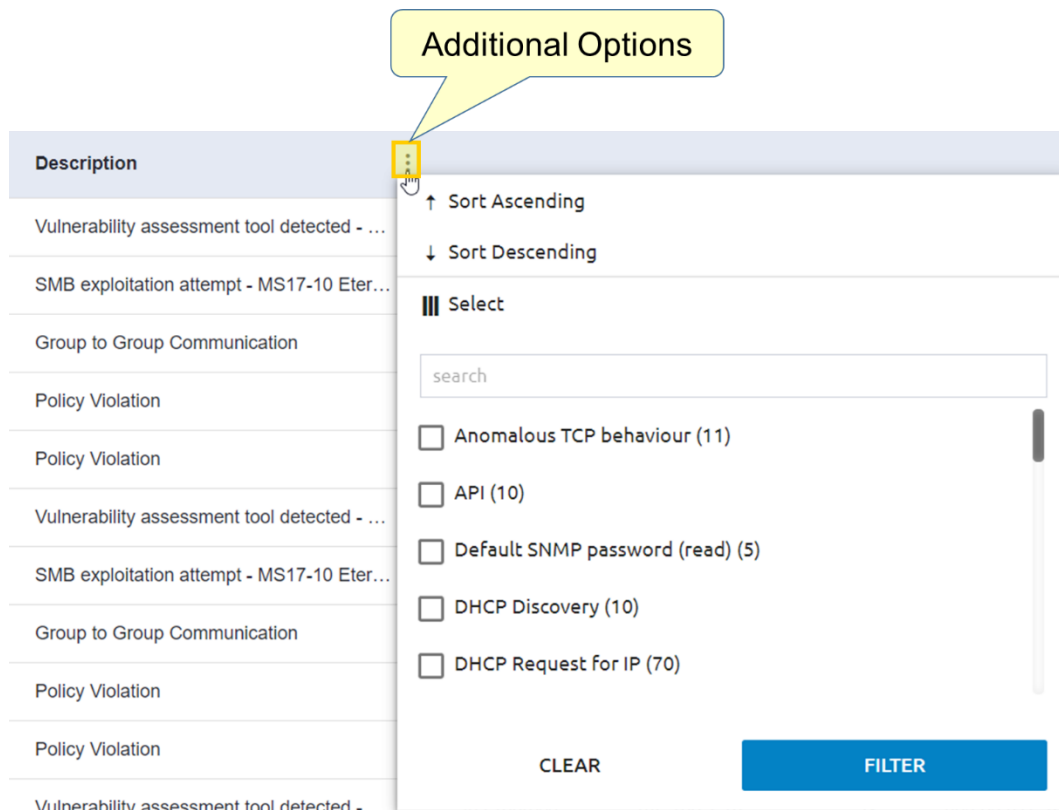


Figure 5: Additional Options

The sorting and filtering features are described in the following sections.

3.3.1. Sorting Table Data

You can change the order in which data is displayed in the tables by selecting the **Sort Ascending** or **Sort Descending** entry in the **Additional Options** menu (see Figure 5 above). In addition, you can change the sorting order of the table by clicking on a field name in the header. An up/down arrow (see Figure 6 below) appears to indicate the field used to sort data, and whether the information is displayed in ascending or descending order.

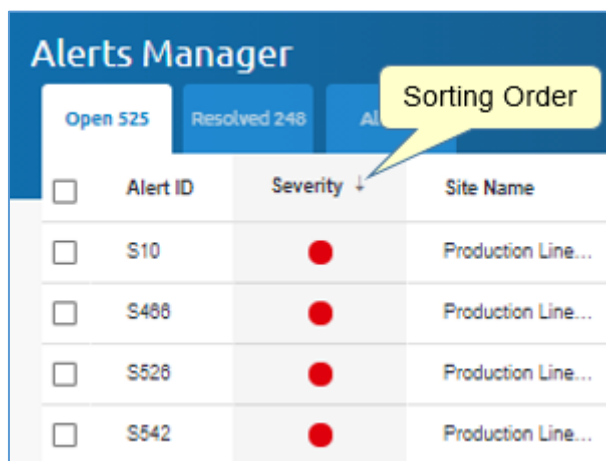


Figure 6: Click on a Field Header to Change the Sorting Order

3.3.2. Filtering Records

You can use the SCADAfence Multi-Site filtering mechanism to focus on a specific record or records (see Figure 5 above). To filter records, click on the **Additional Options** icon in the relevant column, select **Filter**, choose one or more filtering values, and click on the **Filter** button, as shown in the figure below.

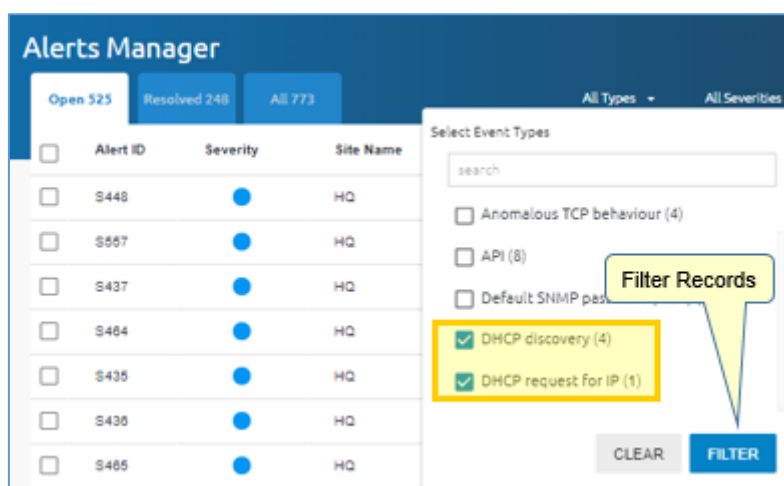
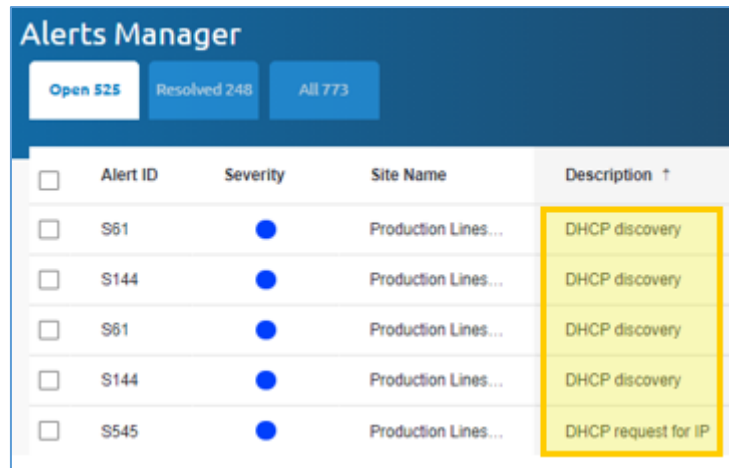


Figure 7: Filtering Records

NOTE

The type of filter used is dependent on the column being filtered and the type of value that appears in the column.

The filtered records appear as shown in Figure 8 below.



<input type="checkbox"/>	Alert ID	Severity	Site Name	Description ↑
<input type="checkbox"/>	S61	●	Production Lines...	DHCP discovery
<input type="checkbox"/>	S144	●	Production Lines...	DHCP discovery
<input type="checkbox"/>	S61	●	Production Lines...	DHCP discovery
<input type="checkbox"/>	S144	●	Production Lines...	DHCP discovery
<input type="checkbox"/>	S545	●	Production Lines...	DHCP request for IP

Figure 8: Filtered Records

You can apply filtering to multiple columns in the table.

- When you select multiple filters in a column, all records that meet *any* of the selected criteria appear, in “binary OR” fashion.
- When you apply filters in multiple columns, only those records that meet the criteria in *all* of the filtered columns appear, in “binary AND” fashion.

To clear all filters in a single operation, click on the **Clear Filters** icon at the top of the page.

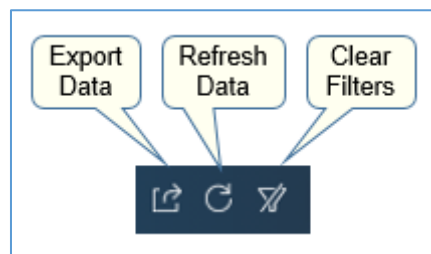


Figure 9: Clear Filters Icon

3.4. Selecting Columns

Some of the tables in the system allow you to add or remove columns from the display. To add or remove columns, click on the **Select Columns** dropdown, check or uncheck the column check boxes as required, and click on the **Save** button. Click **Reset** to restore the original default columns.

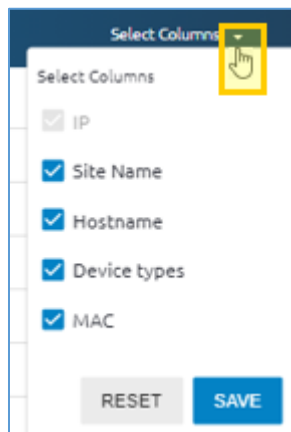


Figure 10: Selecting Columns

3.5. Header Icons

Header icons, shown in the figure below, appear on many of the pages in the SCADAfence Multi-Site user interface:

- **Export Data.** Click on this icon to download an Excel worksheet containing the data that is currently displayed on the page.
- **Refresh Data.** Click on this icon to reload the data as it currently appears in the system database.
- **Clear Filters.** Click on this icon to clear all filters that are currently applied to the table.

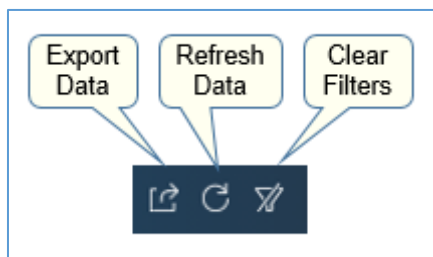


Figure 11: Header Icons

3.6. Paging Mechanism

Tables with numerous records are accompanied by a paging mechanism at the bottom of the page, as shown in the figure below.

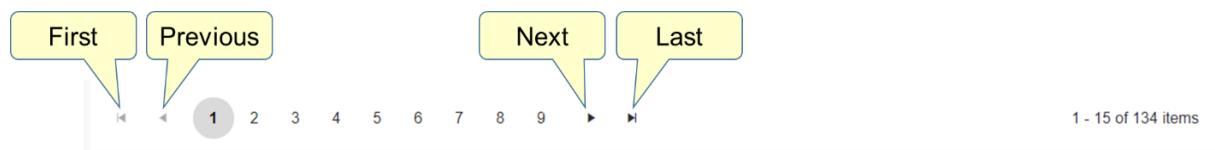


Figure 12: Paging Mechanism

The mechanism displays the number of records in the list, and allows you to select pages using the following options:

- **First** page
- **Previous** page
- **Next** page
- **Last** page
- Clicking on one of the page numbers displayed on the paging mechanism

3.7. Hyperlinks

Many of the column headers in the displayed tables are accompanied by a question icon.



Figure 13: Accessing On-Screen Help

3.8. Alert Severity

Each alert in the system is assigned a color-based severity, as described in the table below:

Table 3: Alert Severity

Color	Severity
Red	Critical
Orange	Severe
Purple	Threat
Blue	Warning
Light Blue	Information

Chapter 4

Dashboard

The Dashboard page provides an overall view of alerts, network assets, and site health. To access the Dashboard page, click on the **Dashboard** entry in the sidebar menu.

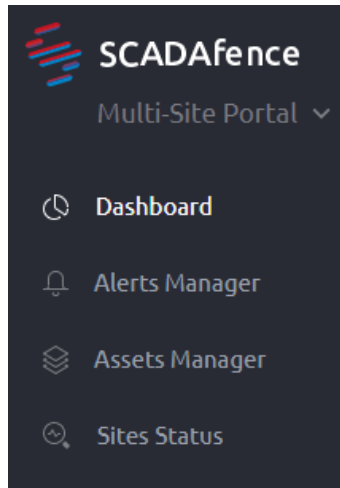


Figure 14: Dashboard Entry in Sidebar Menu

The Dashboard page appears as shown in the figure below.



Figure 15: Dashboard Page

The page is divided into the following sections:

- [Current Status](#). Information on current alert levels, as well as site and asset summaries.
- [Alerts per Site](#). A graphic representation of the number of alerts at each site, distributed by severity.

- [Assets per Site](#). A graphic representation of the number of assets at each site, distributed by asset type.
- [Total Alerts by Severity](#). An organization-wide graphical summary of open alerts, distributed by severity.
- [Sites Status](#). A proportional representation of the active and inactive sites in the organizational network.

4.1. Current Status

The Current Status panel, depicted in Figure 16 below, provides at-a-glance insights into network activity across the organization.

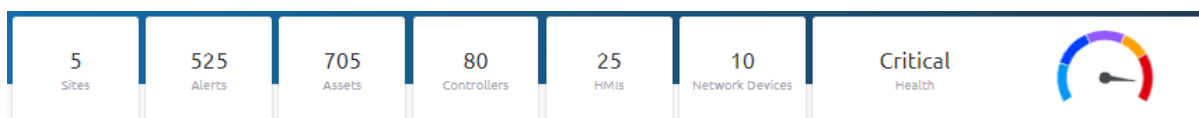


Figure 16: Current Status

The information provided in the panel is described in the table below:

Table 4: Current Status Fields

Field	Description
Sites	The number of sites tracked by SCADAfence Multi-Site
Alerts	The number of currently open alerts.
Devices	The total number of assets monitored by the system.
Controllers	The total number of programmable logic controllers monitored by the system.
HMIs	The number of monitored stations deploying a Human-Machine Interface.
Network Devices	The number of network devices (switches, routers, etc.) monitored by the system.

4.2. Alerts per Site

The Alerts per Site panel, depicted in Figure 18 below, presents bar charts representing the number of open alerts in each site, distributed according to their [severity](#).

The bar charts can be distributed either horizontally or vertically. Click on the desired selector (shown in the figure below) to modify the presentation.



Figure 17: Choose Vertical or Horizontal Bar Charts

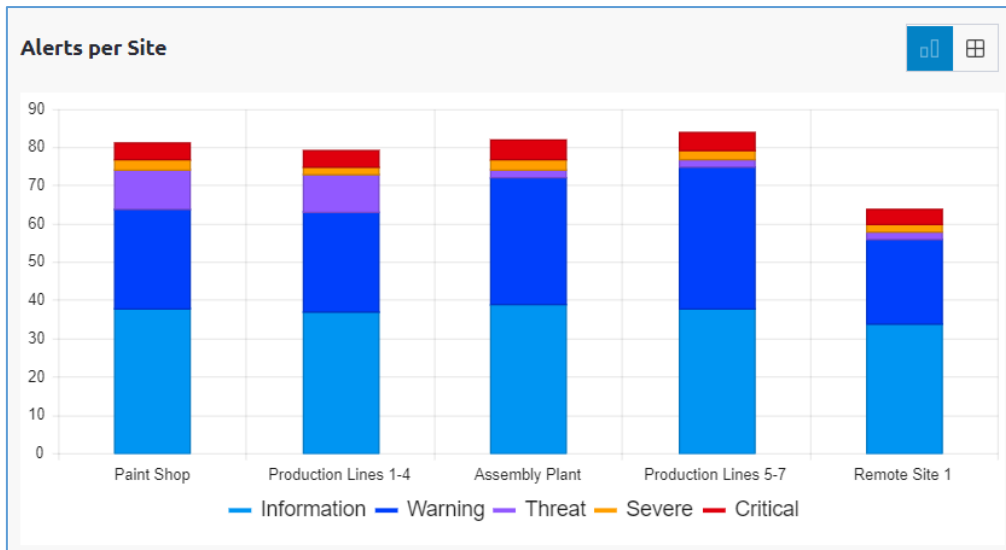


Figure 18: Alerts per Site – Vertical Bar Charts

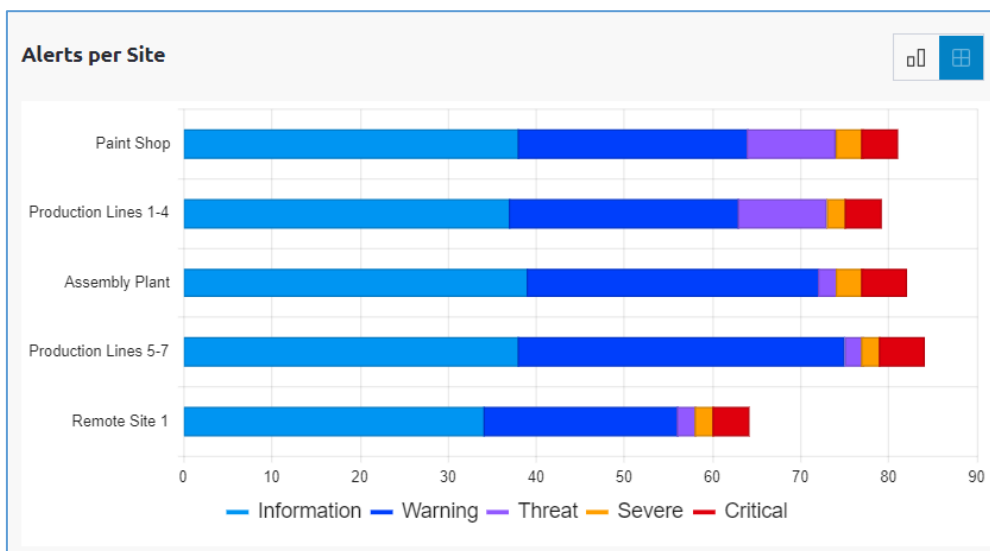


Figure 19: Alerts per Site – Horizontal Bar Charts

4.3. Assets per Site

The Assets per Site panel, depicted in Figure 21 and Figure 22 below, presents bar charts representing the number of devices in each site, distributed according to their type.

The bar charts can be distributed either horizontally or vertically. Click on the desired selector (shown in the figure below) to modify the presentation.



Figure 20: Choose Vertical or Horizontal Bar Charts

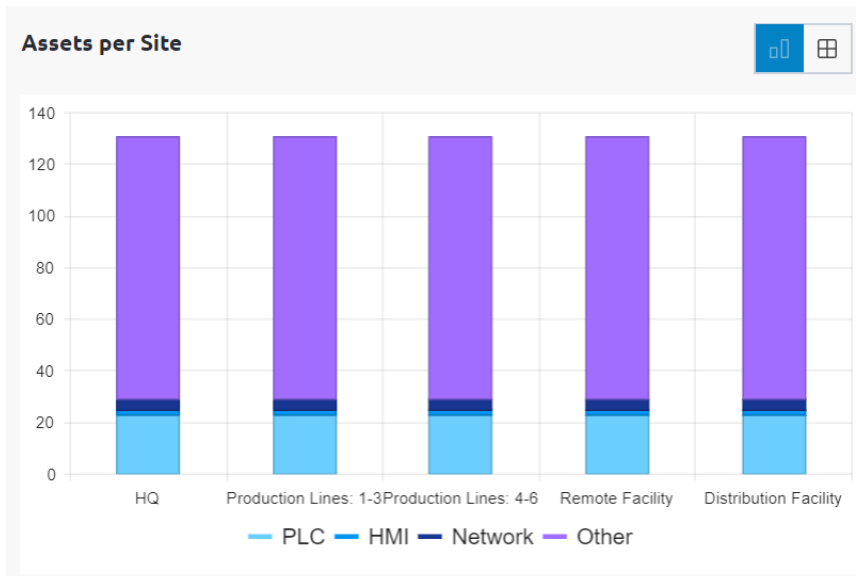


Figure 21: Asset Distribution by Device Type – Vertical Bar Charts

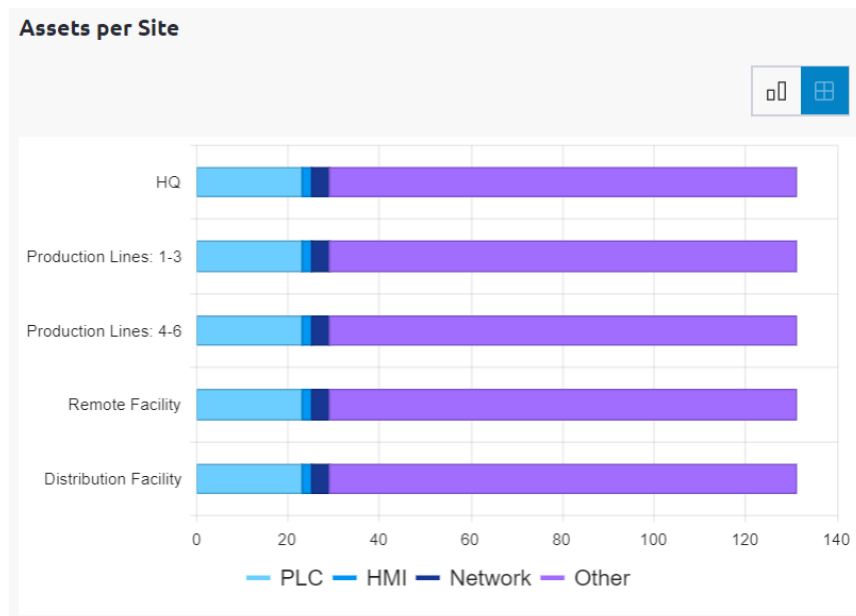


Figure 22: Asset Distribution by Device Type – Horizontal Bar Charts

4.4. Total Alerts by Severity

The Total Alerts by Severity panel, depicted in the figure below, provides a view of open alerts across the organization, distributed according to their [severity](#).

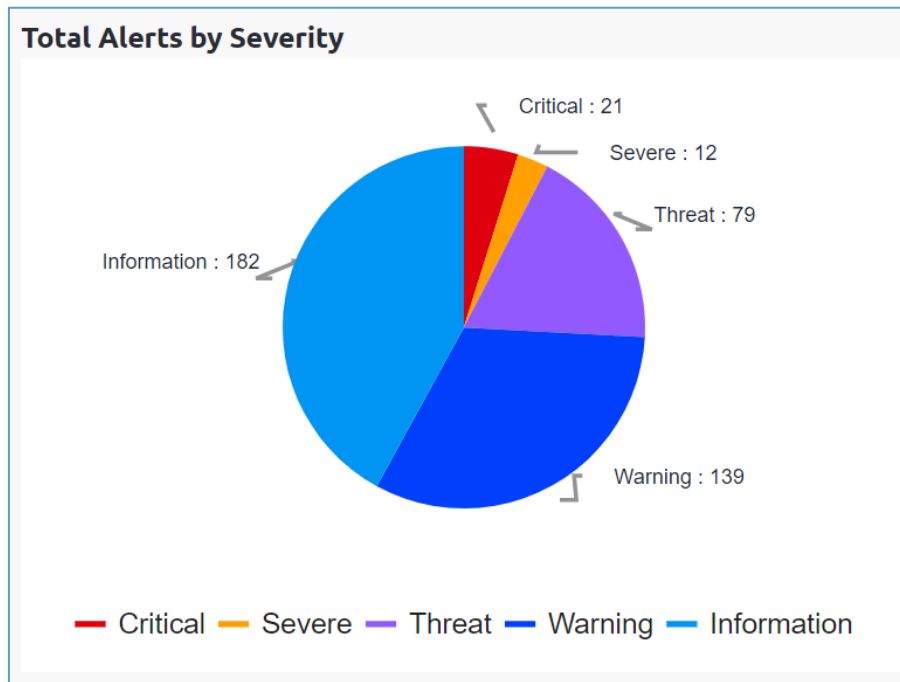


Figure 23: Top IPs at Risk

4.5. Sites Status

The Sites Status panel, shown in the figure below, displays a proportional representation of the active and inactive sites in the organizational network.

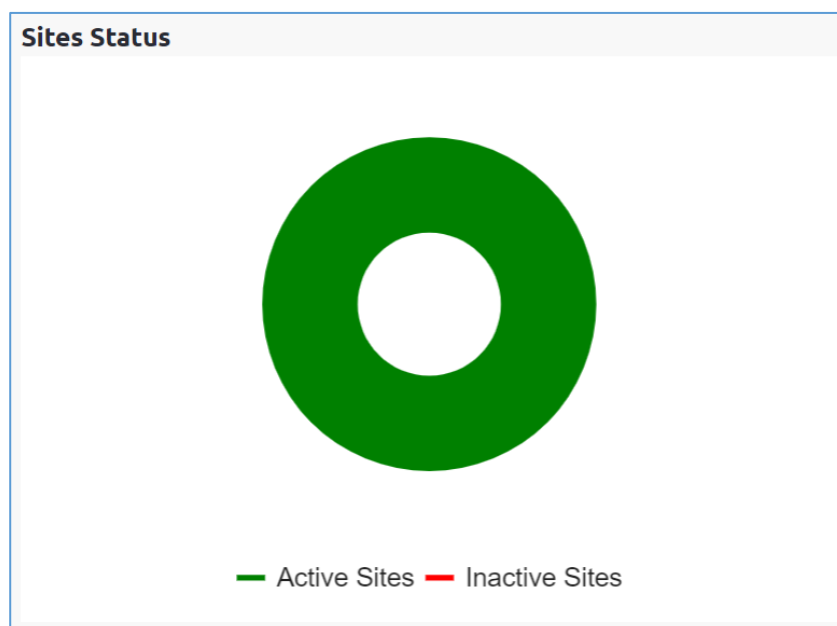


Figure 24: Traffic Volume per Protocol

Chapter 5

Alert Manager

The Alert Manager allowing you to track alerts in specific sites and across the organizational network.

To access the Alert Manager page, click on the **Alert Manager** entry in the sidebar menu.

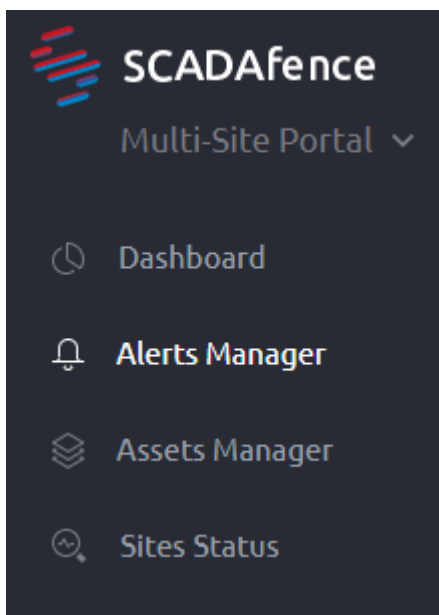


Figure 25: Alert Manager Entry in Sidebar Menu

The Alerts Manager page appears as shown in Figure 26 below.

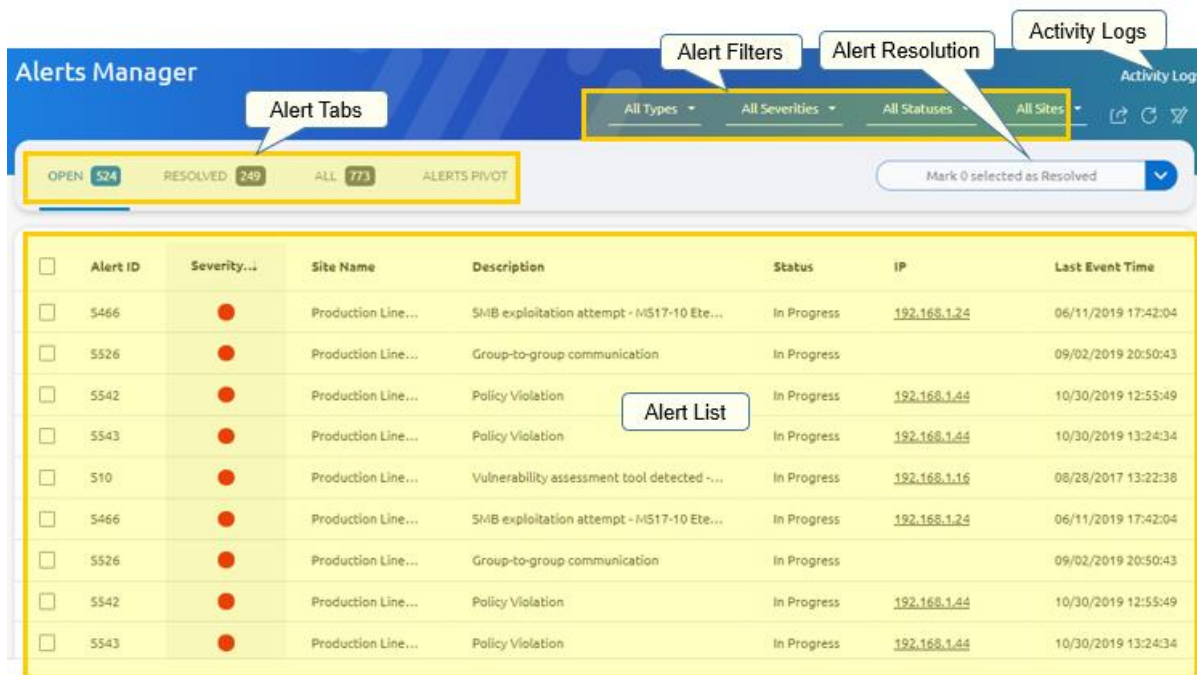


Figure 26: Alert Manager Page

The page is divided into the following sections:

- [Alert Tabs](#). The alert tables allow you *all alerts*, or according to their *status* – open, or resolved.
- [Alert List](#). A list of alerts, their severity, and description.
- [Alert Filters](#). Alert filters allow you to select alerts for display according to their location, type, severity, and/or status.
- [Alert Resolution](#). The alert resolution control allows you to resolve an alert or a group of alerts.
- [Activity Logs](#). The activity logs tab displays the applied activities on the alerts.

5.1. Alert Tabs

The Alert Tabs appear at the top of the tab list, as shown in the figure below.

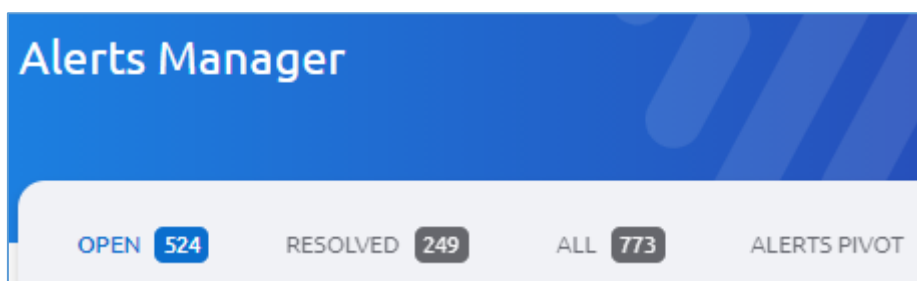


Figure 27: Alerts Tabs

The tabs provide a summary of alerts by category, each tab displaying the number of alerts that fit into the category:

- **Open Alerts.** Unresolved alerts awaiting handling.
- **Resolved Alerts.** Archive of resolved alerts.
- **All Alerts.** A compilation of alerts from all the above alert types.
- **Alerts Pivot.** Alert information, grouped by Alert Type. To see the full list of the alerts for a specific alert type, click on the + icon of the selected row.

5.2. Alert List

The alert list provides up-to-date information on alerts corresponding to your Alert Tab selection.

Alert ID	Severity..i	Site Name	Description	Status	IP	D...	Last Event Time	Total Events	SF...
5466	●	Production Line...	SMB exploitation attempt - MS17-10 Ete...	In Progress	192.168.1.24	S...	06/11/2019 17:42:04	1	
5526	●	Production Line...	Group-to-group communication	In Progress		U...	09/02/2019 20:50:43	1	
5542	●	Production Line...	Policy Violation	In Progress	192.168.1.44	C...	10/30/2019 12:55:49	1	
5543	●	Production Line...	Policy Violation	In Progress	192.168.1.44	C...	10/30/2019 13:24:34	1	
510	●	Production Line...	Vulnerability assessment tool detected -...	In Progress	192.168.1.16	N...	08/28/2017 13:22:38	1	
5466	●	Production Line...	SMB exploitation attempt - MS17-10 Ete...	In Progress	192.168.1.24	S...	06/11/2019 17:42:04	1	
5526	●	Production Line...	Group-to-group communication	In Progress		U...	09/02/2019 20:50:43	1	
5542	●	Production Line...	Policy Violation	In Progress	192.168.1.44	C...	10/30/2019 12:55:49	1	
5543	●	Production Line...	Policy Violation	In Progress	192.168.1.44	C...	10/30/2019 13:24:34	1	
510	●	Remote Security	Vulnerability assessment tool detected -...	In Progress	192.168.1.16	N...	08/28/2017 13:22:38	1	
5526	●	Remote Security	Group-to-group communication	In Progress		U...	09/02/2019 20:50:43	1	

Figure 28: Alert List

The information provided in the fields in the list is described in the table below:

Table 5: Alert List Fields

Field	Description
Alert ID	A unique ID number representing the alert that was raised.
Severity	Indicates the severity of the alert.
Site Name	The name of the site in which the alert event occurred.
Description	A brief description, or “headline”, of the alert
Status	Indicates the status of the alert: <ul style="list-style-type: none"> ● Created. The alert is open and awaiting handling. ● In progress. The alert has been reviewed. ● Resolved. The alert was handled and has been closed.
IP	IP address of the asset on which the alert was raised
Details	A complete description of the alert.
Last Event Time	The date and time of the occurrence of the last alert. A complete description of the alert, including linked references to the assets involved.
Total Events	
SF Platform	Enables access to the SCADAfence Platform to view the alert.

5.3. Alert Filters

The Alert Filters, shown in the figure below, help you to zero in on specific alerts. The filters allow you select one or more alert descriptions, severities, and statuses for display. See Table 5 above for a description of each filter.

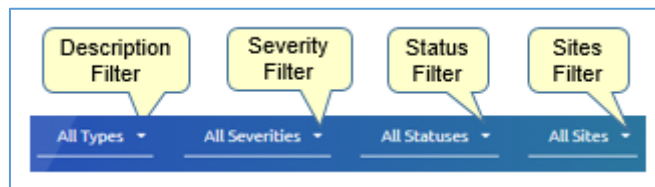


Figure 29: Alert Filters

To select filters, click on the downward arrow to open one of the dropdown list boxes, check one or more boxes, and click on the **Filter** button to save the selection.

When selecting alerts using multiple selections in multiple filters, note the following:

- When you select multiple entries in a filter, all records that meet *any* of the selected criteria appear, in “binary OR” fashion.
- When you select entries in multiple filters, only those records that meet the criteria in *all* of the filters columns appear, in “binary AND” fashion.

5.4. Alert Resolution

The Alert Resolution control allows you to designate alerts as resolved or as not resolved, using the drop-down menu. To resolve one or more alerts, click the relevant check boxes to select the alerts. A confirmation message appears in the Alert Resolution control box.

5.5. Activity Logs

The Activity Logs Tab allows you to display all the activities applied on the alerts. The information can be filtered by sites and alert types.

Chapter 6

Assets Manager

The Asset Manager page provides details on all computing devices connected to the network, including PLCs, HMIs, servers, and endpoints. SCADAfence *automatically generates asset inventory* without prior knowledge or user configuration.

To access the Asset Manager page, click on the **Assets Manager** entry in the sidebar menu.

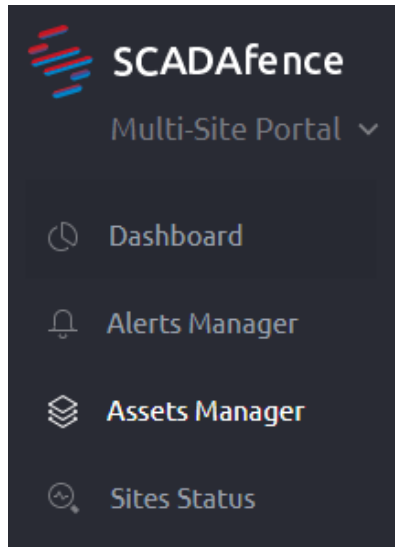


Figure 30: Asset Manager Entry in Sidebar Menu

The Asset Manager page displays a list of network assets, including details on each asset.

6.1. Assets List

The Assets List tab appears as shown in Figure 31 below.



Figure 31: Assets List

The information provided in the fields in the list is described in the table below. Optional fields can be selected using the **Select Columns** dropdown list box.

Table 6: Assets List Fields

Field	Description
Default Fields	
IP	The IP address of the asset.
Site Name	The facility or location name.
Hostname	The asset's hostname.
Device Type	The type of asset.
MAC	The MAC address of the asset.
Vendor	The asset vendor.
OS	The operating system installed in the asset, if known.
Total Traffic	The asset's total traffic volume (transmitted and received).
Optional	
Total Sent	Total traffic sent by the asset – in bytes.
OU	Organizational unit (user-entered data).
Owner	Asset owner (user-entered data).
Physical Location	The physical location of the asset (user-entered data).
Comment	A free text field containing additional information on the asset (user-entered data).

Criticality	The level of criticality of the asset (user-entered data).
Firmware Version	The firmware version of the asset.
Module Name	Asset module name.
Hardware Version	The hardware version of the asset.
Serial Number	The serial number of the asset.
PLC	Additional details on the device, including the PLC vendor name.

+ Click on the **Open Quick Summary** symbol expand the row to display additional information on the asset, as shown in the figure below.

	IP ↑	Site Name	Hostname	Device types	MAC
-	10.146.29.253	HQ	scadafence-pc	Workstation	08:00:27:7C:15:A0
Connections: 1 internal					
Device types:	Workstation		MAC:	08:00:27:7C:15:A0	
OS:	Windows 7		First seen:	March 17th 2019, 12:27:58	
Hostname:	scadafence-pc		Last Seen:	March 17th 2019, 15:16:48	
Vendor:	PCS Computer Systems GmbH		NIC Type:	Ethernet	

Figure 32: Quick Asset Summary

You can use the asset filtering mechanism to focus on a specific asset record or records. For further information on filtering, see section 3.3.2.

Double click on the selected asset's IP address to display detailed information on the asset, as shown in the figure below:

Assets Network > 10.10.4.201

10.10.4.201 Site: Site_144 [Go to Asset](#)

Device type: Communications Adapter

Vendor: Rockwell Automation

MAC: 00:10:9C:BE:4B:41

First seen: January 09, 2022, 15:23:43

Last Seen: January 09, 2022, 15:23:43

NIC Type: Ethernet

Additional Details

Asset name: 1756-ENBTSrx2FA

Serial number: SDA103

Firmware version: 06.04

Vendor: Rockwell Automation(Rx2F)Allen-Bradley

Device Type: Communications Adapter

Connections

Industrial traffic

Activity and alerts log

Open Ports

CVE

CVE ID	Published	Score	Vendor	Description	Info
CVE-2018-17024	12/01/2018 16:29:00	8.6	rockwell automation	Rockwell Automation MicroLogix 1400 Controllers and 1754 ControlLogix Communications Modules An unauthenticated, remote threat actor o	Info
CVE-2013-6435	01/04/2013 23:55:00	7.8	rockwell automation	Rockwell Automation Ethernet/IP products: 1756-ENBT, 1756-ENB, 1756-ENBT, and 1756-ENB communication modules; CompactLogix L32E	Info
CVE-2013-6436	01/04/2013 23:55:00	7.8	rockwell automation	Buffer overflow in Rockwell Automation Ethernet/IP products: 1756-ENBT, 1756-ENB, 1756-ENBT, and 1756-ENB communication modules; C	Info
CVE-2013-6437	01/04/2013 23:55:00	10	rockwell automation	Rockwell Automation Ethernet/IP products: 1756-ENBT, 1756-ENB, 1756-ENBT, and 1756-ENB communication modules; CompactLogix L32E	Info
CVE-2013-6438	01/04/2013 23:55:00	7.8	rockwell automation	Buffer overflow in Rockwell Automation Ethernet/IP products: 1756-ENBT, 1756-ENB, 1756-ENBT, and 1756-ENB communication modules; C	Info

1 - 5 of 10 items

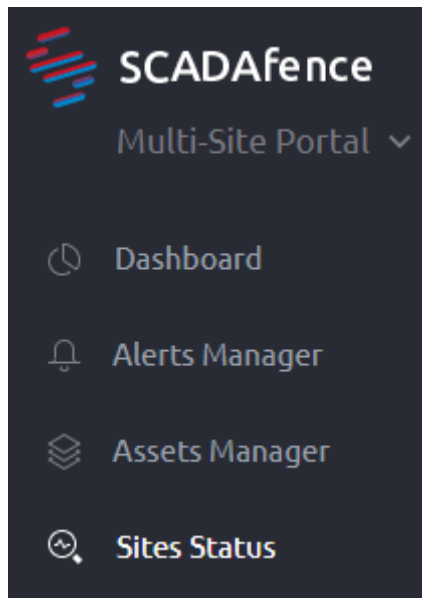
Figure 33: Asset Detailed Information

Chapter 7

Sites Status

The Sites Status page provides a high-level view of each site, providing a summary of assets and open alerts.

To access the Sites Status page, click on the **Sites Status** entry in the sidebar menu.



The Sites Status page appears as shown in the figure below.

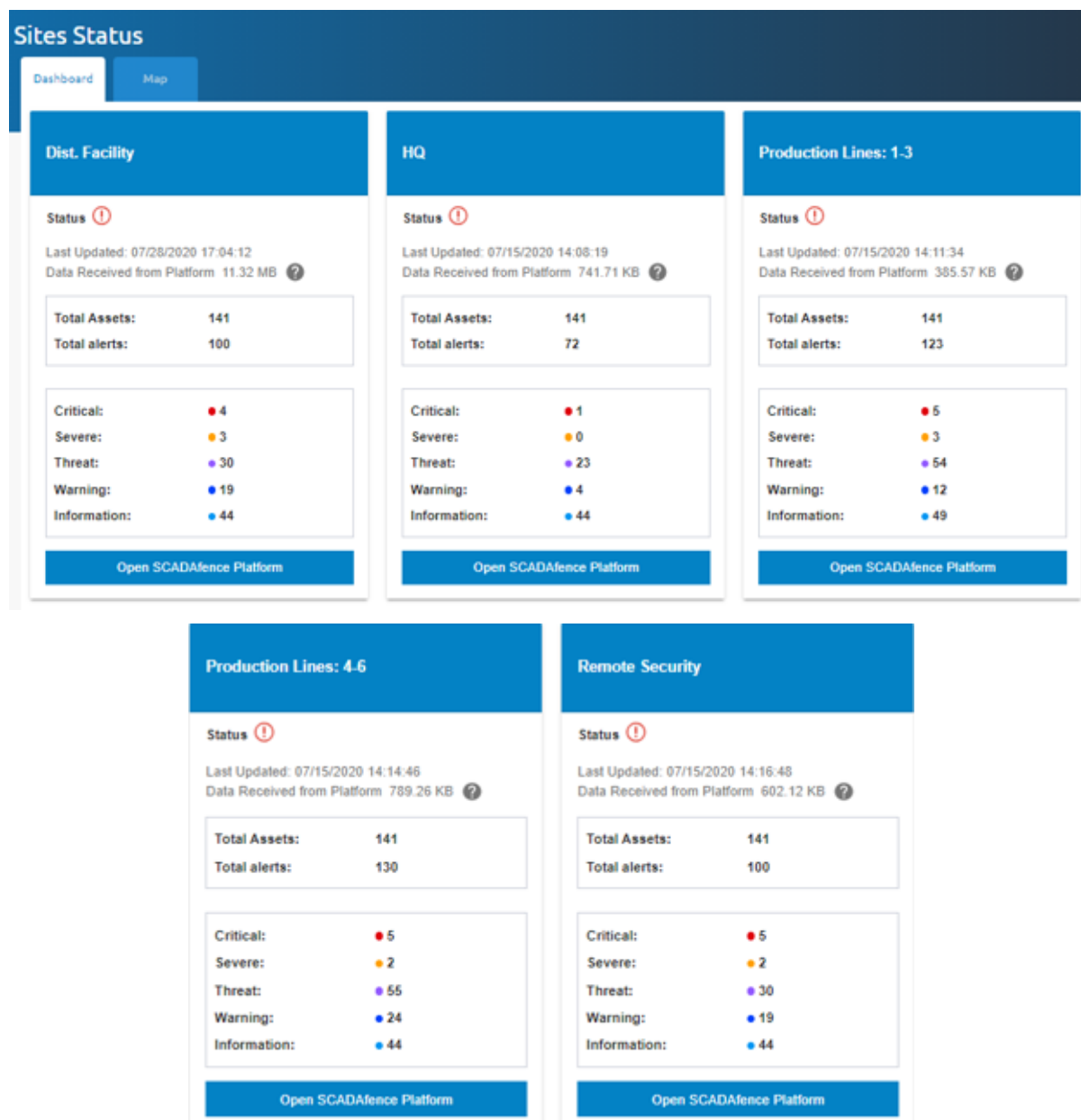


Figure 34: Sites Status Page

The information provided for each site on the page is described in the table below:

Table 7: Alert List Fields

Field	Description
Site Name	The name of the site.
Status	Indicates the connectivity status of the site:
	<div style="display: flex; align-items: center;"> Online. Data was received from the site during the last hour. </div> <div style="display: flex; align-items: center;"> Offline. Data has not been received from the site during the last hour. </div>
Last Updated	The timestamp of the last update received from the SCADAfence Platform installed at the site.
Total Assets	The number of monitored assets at the site.
Total Alerts	The number of open alerts associated with assets at the site.

Severity	The distribution of severities of the open alerts.
----------	----------------------------------------------------

7.1. Sites Map

The Sites Map page provides a high-level, map-based summary of monitored sites in the organization.

To access the Sites Maps page, click on the **Map** tab in the **Sites Status** section.

The Sites Map page appears as shown in the figure below:

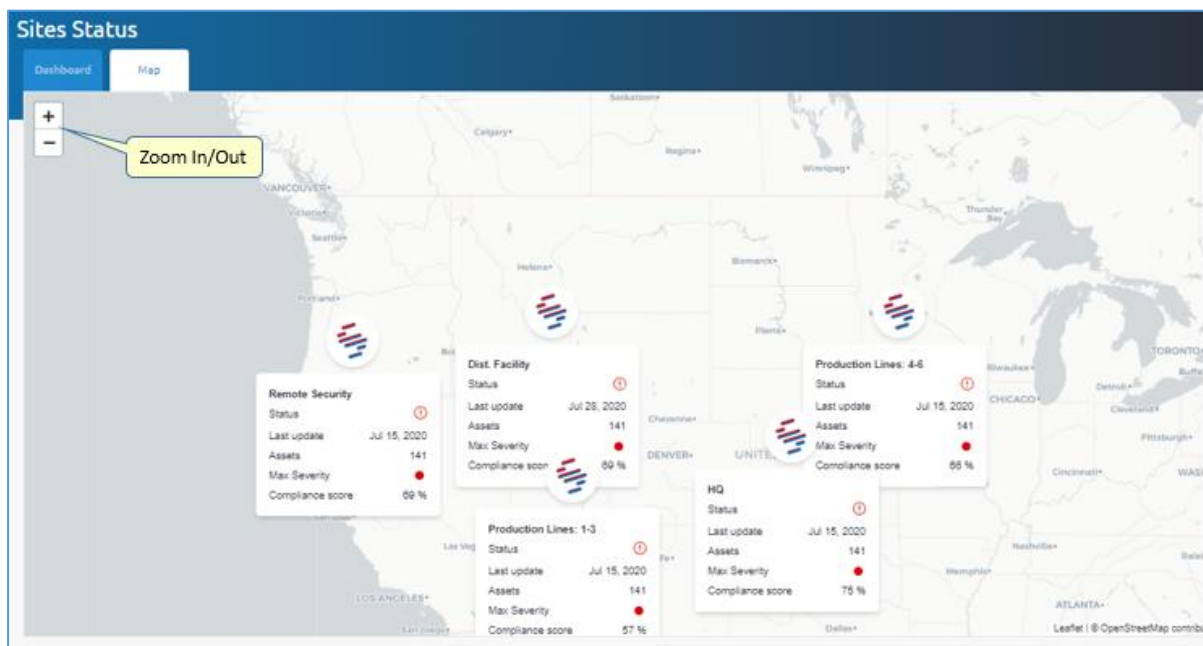


Figure 35: Sites Map Page

For each site on the Sites Map, the following information is provided.

Table 8: Sites Map Fields

Field	Description			
Site Name	The name of the site.			
Status	Indicates the connectivity status of the site:			
	<table border="1"> <tr> <td></td> <td>Online. Data was received from the site during the last hour.</td> </tr> <tr> <td></td> <td>Offline. Data has not been received from the site during the last hour.</td> </tr> </table>		Online. Data was received from the site during the last hour.	
	Online. Data was received from the site during the last hour.			
	Offline. Data has not been received from the site during the last hour.			
Last Update	The timestamp of the last update received from the SCADAfence Platform installed at the site.			
Assets	The number of monitored assets at the site.			
Max. Severity	The highest severity among the open alerts at the site.			
Compliance Score	The percentage of standard requirements complied with at the site.			

Use the **Zoom In** and **Zoom Out** controls to control the map resolution.

Hover over a site summary to display a summary of open alerts, as shown in the figure below.

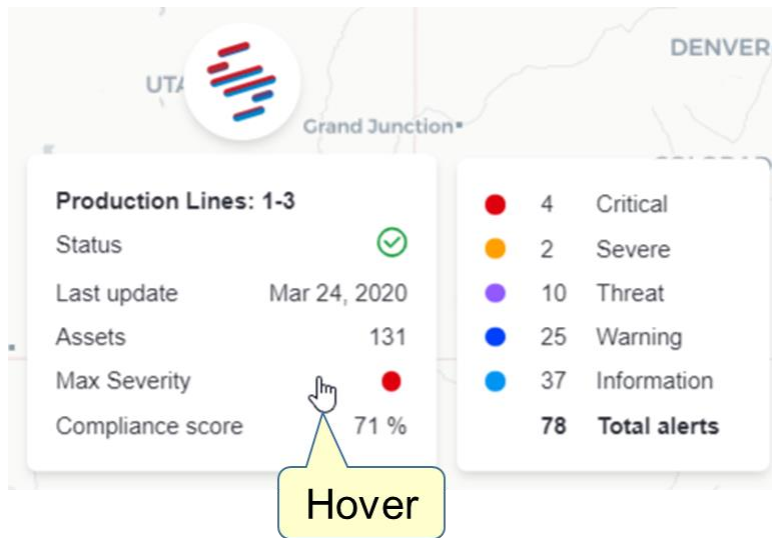


Figure 36: Hover to Display Site Alert Summary

Chapter 8

System Settings

The Setting sub-menu allows you to configure a variety of system functions.

➔ **To access the Setting page:**

1. Click on the Setting entry in the sidebar menu.

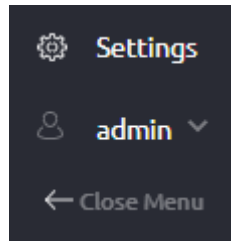


Figure 37: Setting Entry in Sidebar Menu

2. The Settings page appears as shown in the figure below:

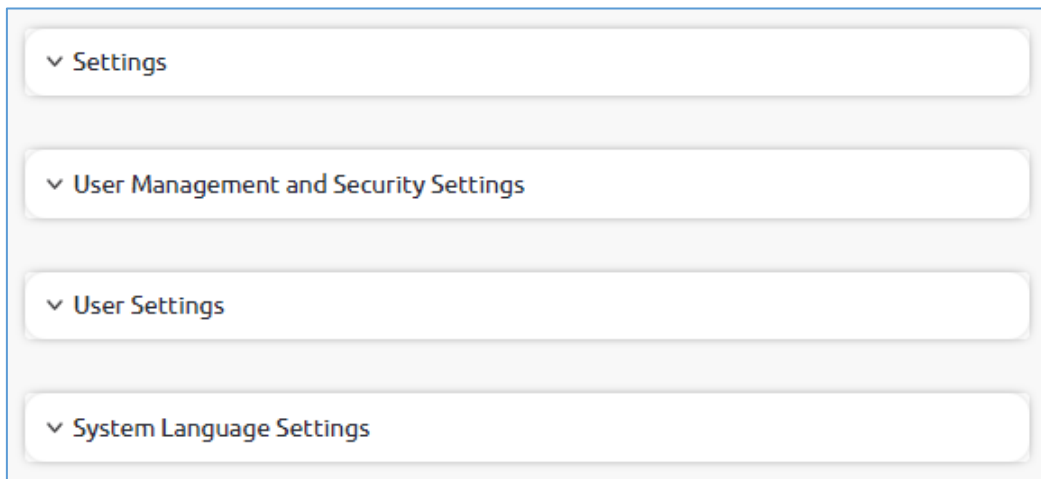


Figure 38: General Settings Page

- [Settings](#)
- [User Management and Security Settings](#)
- [User Settings](#)
- [System Language Settings](#)

8.1. Settings

Using the Settings menu, you can manage the following settings:

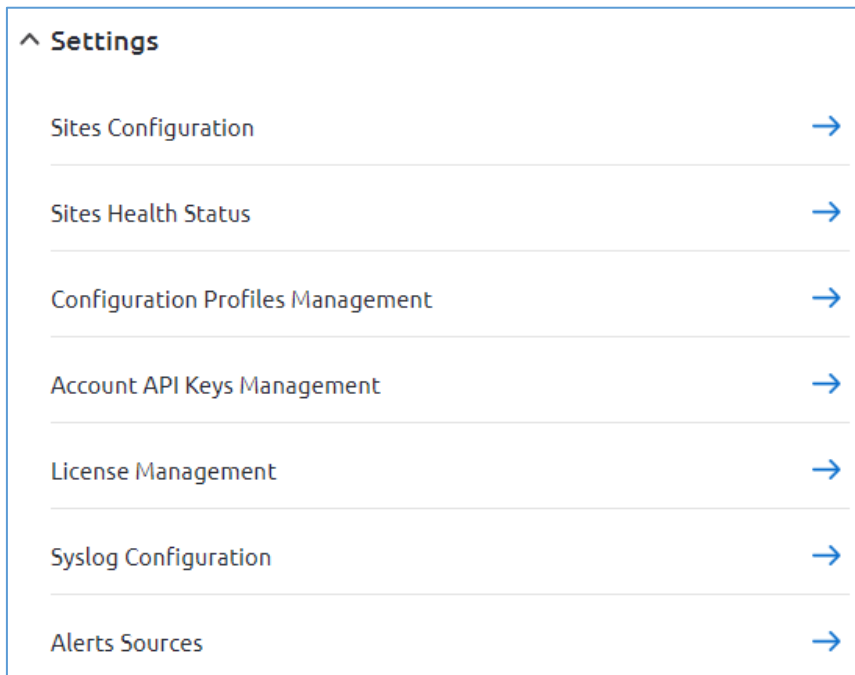


Figure 39: Settings Page

- [Sites Configuration](#)
- [Sites Health Status](#)
- [Configuration Profiles and Management](#)
- [Account API Keys Management](#)
- [License Management](#)
- [Syslog Configuration](#)
- [Alert Sources](#)

8.1.1. Sites Configuration

To perform sites configuration, click on the **Sites Configuration** arrow (see Figure 39). The Sites Configuration page appears as shown in the figure below.

The screenshot shows the 'Sites Configuration' page with a table of site data. The table has the following columns: Site No., Site Name, IP, SW Version, Last SW Update, SW Update Status, Site update Readin..., and Connection Status. There are five rows of data, each with a checkbox on the left and 'Cancel' and 'trash' icons on the right.

Site No...	Site Name	IP	SW Version ↑	Last SW Update	SW Update Status	Site update Readin...	Connection Status
<input type="checkbox"/>	46	HQ	52.58.169.13		Remote update not supported	Version not supported	●
<input type="checkbox"/>	47	Production Lines: 1-3	192.168.3.22		Remote update not supported	Version not supported	●
<input type="checkbox"/>	48	Production Lines: 4-6	192.168.4.221		Remote update not supported	Version not supported	●
<input type="checkbox"/>	49	Remote Security	172.1.33.25		Remote update not supported	Version not supported	●
<input type="checkbox"/>	83	Dist. Facility	172.4.11.4		Remote update not supported	Version not supported	●

Figure 40: Site Configuration Page

The Sites Configuration page displays the sites status and enables updating the SCADAfence version installed in the sites. It contains the following fields:

Table 9: Sites Configuration Fields

Field	Description
Site Number	A unique ID number representing the site.
Site Name	The name of the site.
IP	The IP address of the SCADAfence Platform located at the site.
SW Version	The SCADAfence version that is installed in the site
Last SW Update	Time of the last software update in the site.
SW Update Status	Details the site's readiness for software update
Site Update Readiness	Upgrade is not supported in legacy software versions, This field indicates whether the upgrade is possible from the site's current software version.
Connection status	Site monitoring status: <ul style="list-style-type: none"> • Active. The site is currently being monitored by the SCADAfence Platform. • Inactive. The site is <i>not</i> currently being monitored by the SCADAfence Platform.

The buttons on the top right of the page enable initiating a software version update to selected sites, and canceling it if necessary.

The **Cancel** button in each row allows you to cancel a site's upgrade operation.

8.1.1.1. Adding a New Site

➔ **To add a new site:**

1. Click on the **+Add New** button.
2. The Add New Site Page is displayed as shown in the figure below:

Figure 41: Add New Site

3. Enter the site information as described in the table below:


Table 10: Add New Site Window Fields

Field	Description
Site Name	The name of the site.
Site Address	The IP address of the SCADAfence Platform located at the site.
Latitude	The latitude of the site location. This determines the position of the site on the geographic Sites Map.
Longitude	The longitude of the site location. This determines the position of the site on the geographic Sites Map.
Description	A short site description.
Active	Site monitoring status: <ul style="list-style-type: none"> • Yes. The site is set to "Active" and will be monitored by the SCADAfence Platform. • No. The site is set to "Inactive" and will <i>not</i> be monitored by the SCADAfence Platform.

4. Click **Save**.

8.1.1.2. Editing an Existing Site

➔ To edit a site's information:

1. In the Site Configuration page, click on the **Edit** icon  of the selected site.

1. The Edit Site page allows you to set various parameters of the selected site, using the following tabs:
 - [Site Info](#). Used to modify of the site's information.
 - [Software Update](#). Used to update/rollback the site's software version.
 - [Configuration Update](#). Used to modify the configuration of the site.

8.1.1.3. Site Info

The Site Info page allows you to modify the selected site information and to delete the site's data/traffic, as shown in the below figure:

Delete Site Data	
Delete All Data	Delete Traffic Data
Total Assets:	141
Total L2 Assets:	0
Total Alerts:	155
Total Activity Logs:	0
Total Conversations:	0
Total Industrial Conversations:	0

Figure 42: Site Info Page

Edit the site information for the selected site, as described in Table 10 above.

- ➔ **To export the site's configuration information:**
1. In the **API Keys** section, enter the **API Owner Name**.

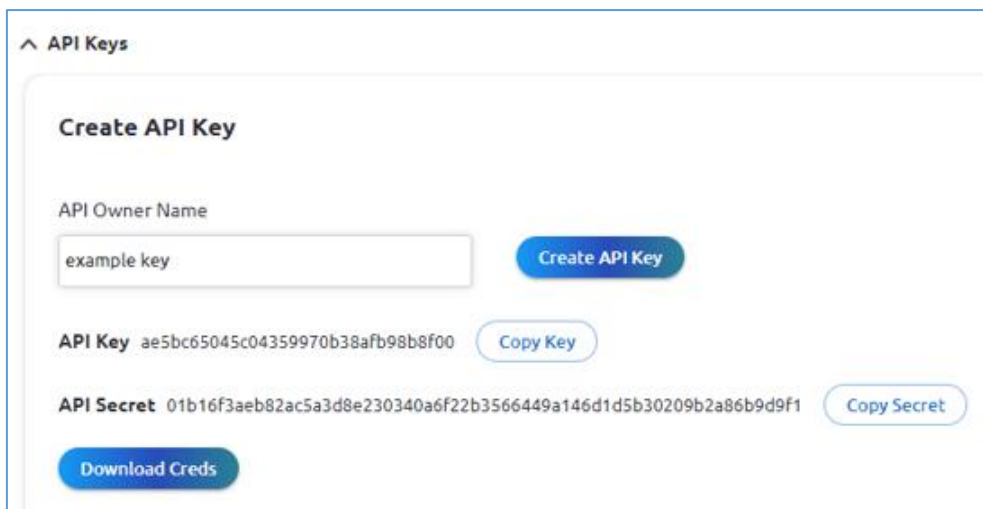


Figure 43: Exporting the Site Configuration Information

2. Click on the **Create API Key** button to create the credentials information.
3. Click on the **Download Creds** button to export the credentials file.
4. Keep the downloaded site-configuration file and upload it in the SCADAfence Platform (see the note below).

NOTE

In SCADAfence Platform **Setting >> SCADAfence Cloud and Multi-Site Portal Configuration**, enter the site name associated with the configuration file that you exported, and click **Upload Connection Info** button to import the site's configured values.

You can delete all the data for the selected site, including logs and alerts, by clicking on the **Delete All Data** button.

NOTE

After the **Delete All Data** operation, you will have a site with no data. Platform will update the Multi-Site and sync the data.

You can delete the traffic data by clicking on the **Delete Traffic Data** button, as shown in the below figure:

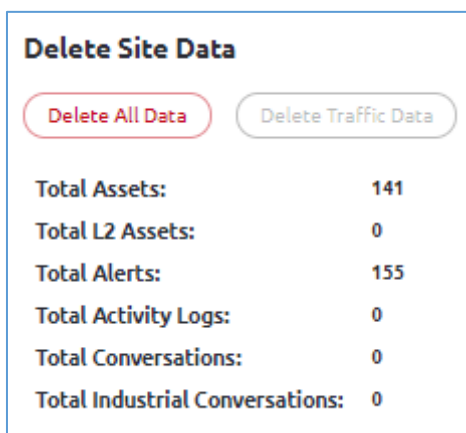


Figure 44: Delete Site Data

8.1.1.4. Software Update

The Software Update page allows you to perform a software update or a rollback for the selected site:

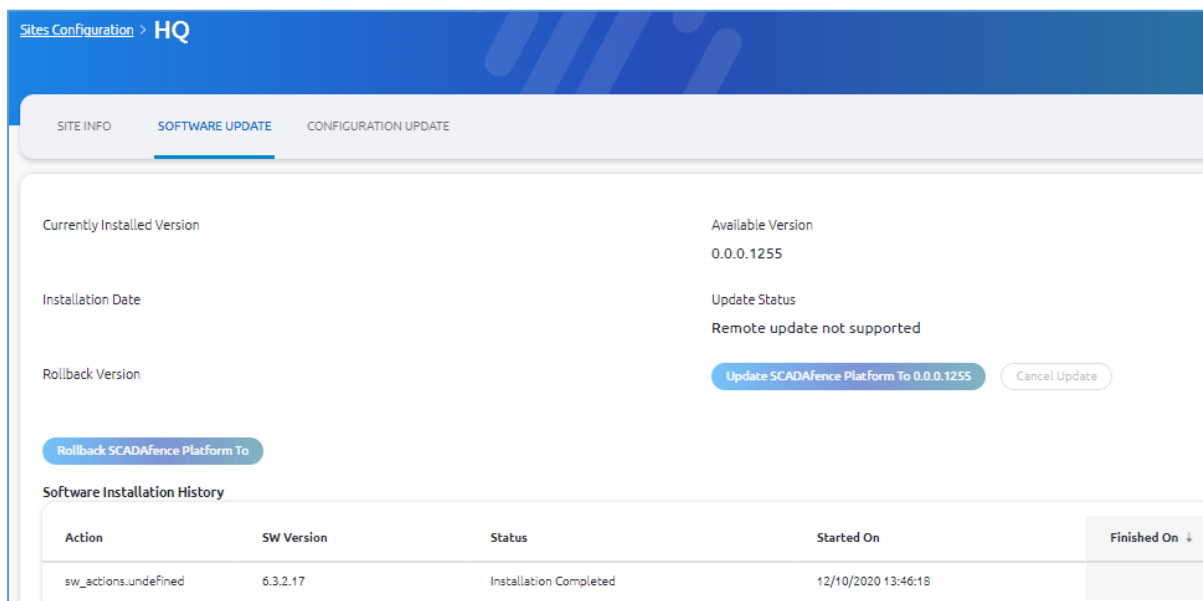


Figure 45: Software Update

- **Currently Installed Version.** The current software version of the site.
- **Installation Date.** The latest installation date.
- **Rollback version.** The software version that is available for rollback. Click on the **Rollback SCADAfence Platform To** button, to apply the rollback.
- **Software Installation History,** displays the following information on the installations, applied in the selected site:

Table 11: Add New Site Window Fields

Field	Description
Action	The action applied on the site.
SW Version	The software version of the site.
Status	The status of the installation.
Started On	The beginning time of the installation.
Finished On	The completion time of the installation.

- **Available Version.** The software version, available for update. Click on the **Update SCADAfence Platform To** button, to apply the update.
- **Update Status.** Presents the readiness of the update process. The "Remote Update not Supported" message indicates that the current software version of the selected site does not support a remote update.

8.1.1.5. Configuration Update

The Configuration Update Page displays information on the site's configuration, as described below:

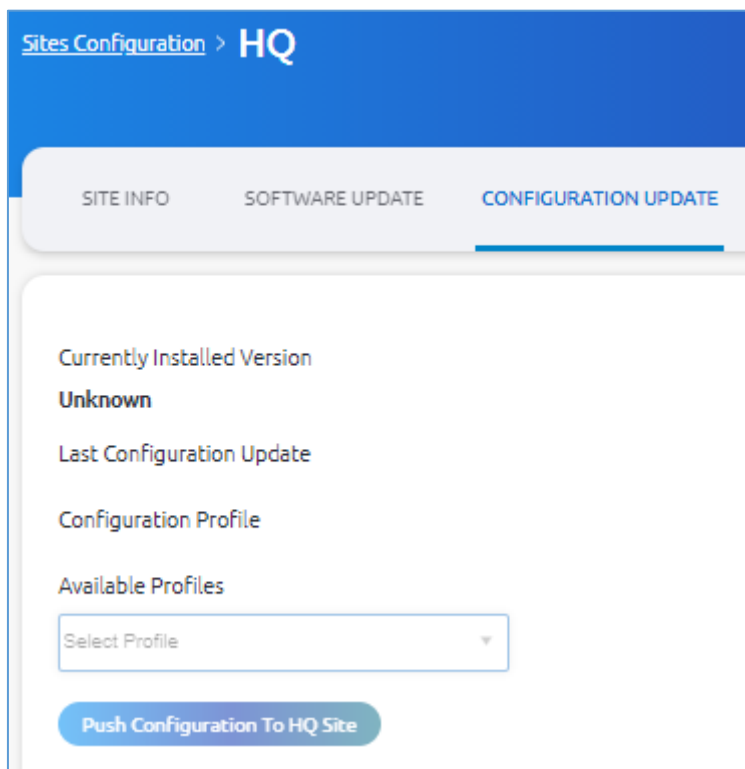


Figure 46: Configuration Update Window

The fields appearing in the figure above are described in the table below:

Table 12: Configuration Update Window Fields

Field	Description
Currently Installed Version	The current SCADAfence Platform software version of the site.
Last Configuration Update	The last configuration update time.
Configuration Profile	Enter the name of the configuration profile (see 8.1.2, for Profile Management Configuration).
Available Profiles	The list of the pre-defined profiles.

➔ To update the site's configuration parameters:

1. Enter the name of the configuration profile.
2. Click on the **Push Configuration** button.

8.1.2. Sites Health Status

The Sites Health Status page allows you to check the health status of each site. The Sites Health Status page appears as shown in the figure below:

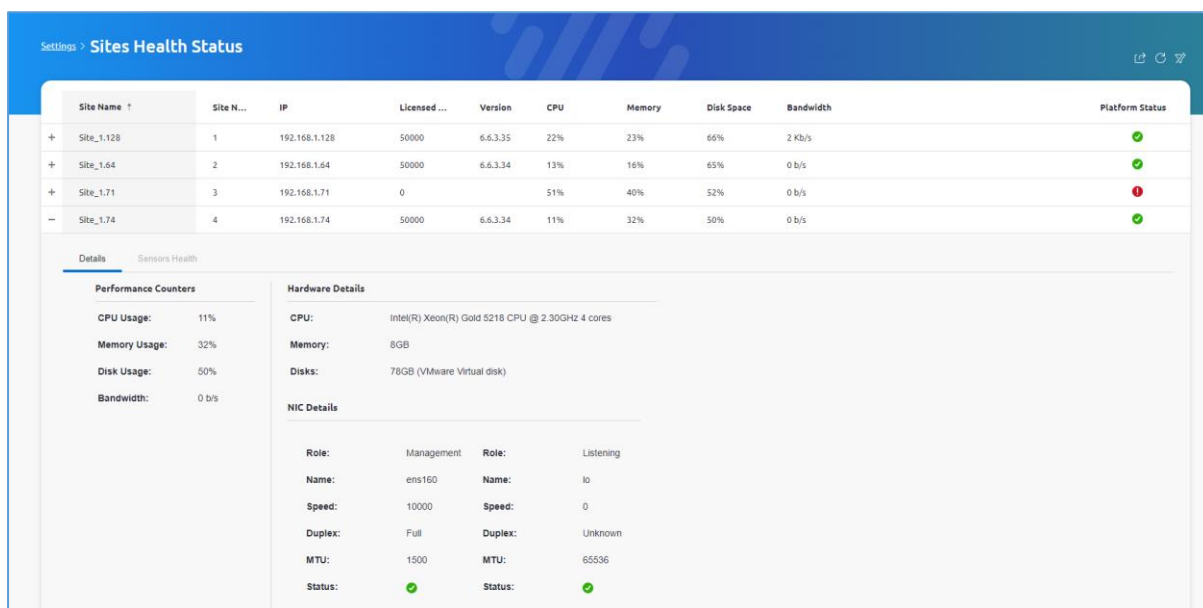


Figure 47: Sites Health Check Status



The Sites Health Status page displays the following information per site:

Table 13: Sites Health Status Fields

Field	Description
Site Name	The name of the site.
Site Number	The number of the site.
IP	IP address of the site.
Licensed Assets	The list of the licensed assets.
Version	The software version of the SCADAfence platform in the site.
CPU	CPU usage (% of total capacity)
Memory	Memory usage (% of total capacity)
Disk Space	Disk space usage (% of total capacity)
Bandwidth	Most recent traffic volume measurement, in bits per second
Platform Status	The SCADAfence Platform's status.
	Connected
	Disconnected

For detailed information on performance, interfaces, and the hardware in use, per site, select a site, and click on the "+" button. The following detailed information will be displayed:

Table 14: Sites Health Status Detailed Information

Field	Description
Performance	
CPU Usage	CPU usage (% of total capacity)
Memory Usage	Memory usage (% of total capacity)
Disk Space Usage	Disk space usage (% of total capacity)
Bandwidth	Most recent traffic volume measurement, in bits per second
Hardware Details	
CPU	CPU vendor, model, and clock speed
Memory	RAM memory capacity
Disks	Disk space capacity
NIC Details	
Role	The role of the Network Interface Card (NIC).
Name	The name of the NIC
Speed	Maximum speed of the NIC
MTU	Maximum Transmission Unit (MTU) of the NIC
Status	The status of the NIC.
	 Connected
	 Disconnected

8.1.3. Configuration Profile Management

Profiles allow you to prepare a group of configurable parameters settings as a pre-defined profile and use it to configure a selected site, instead of parameter-by-parameter provisioning.

To perform profiles configuration, click on the **Configuration Profiles Management** arrow (see Figure 39). The Configuration Profiles Management page appears as shown in the figure below.

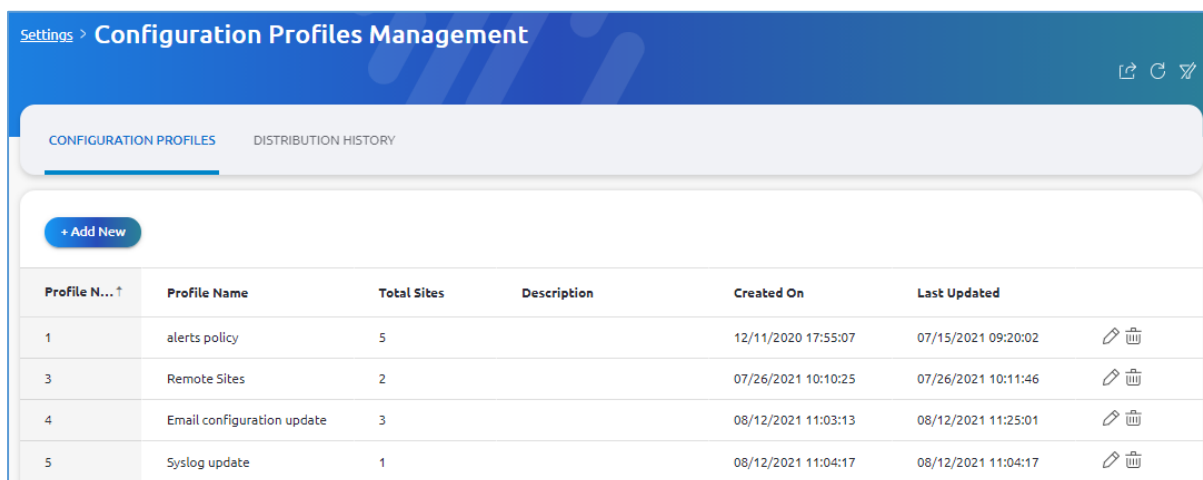


Figure 48: Configuration Profiles Management Page

The Configuration Profiles Management page displays the following information on the pre-configured profiles:

Table 15: Configuration Profiles Management Fields

Field	Description
Profile No	The profile number.
Profile Name	The profile name.
Total Sites	The number of sites to which the profile is distributed.
Description	A short profile description.
Created on	The creation time of the profile.
Last Updated	Time of the last profile update.

Click on the **Distribution History** tab (located at the top of the page), to display the system's distribution information of the profiles.

The Distribution History tab displays the following information:

Table 16: Distribution History Fields

Field	Description
Profile Name	The profile name.
Distribution No.	The number of the applied distributions.
Total sites	The total sites to which the profile has been distributed.
Distributed Date	The time of the profile distribution.
Status	The status of the distribution. Possible values: Succeeded, Failed.

8.1.3.1. Adding a New Configuration Profile

➔ **To add a new profile:**

1. Click on the **+Add New** button.
2. The Add New Configuration Profile Page is displayed as shown in the figure below:

Figure 49: Add New Configuration Profile

3. Enter the site information as described in the table below:


Table 17: Add New Profile Configuration Window Fields

Field	Description
Profile Name	The name of the profile.
Description	A short profile description.

4. Click on the **Select Sites** field, and use the drop-down menu to select the relevant sites.
5. Click **Save**.


8.1.3.2. Deleting a Configuration Profile

➔ **To Delete a profile:**

1. In the Profiles Management page, click on the **Delete** icon  of a selected profile.
2. Confirm the deletion.

8.1.3.3. Editing an Existing Configuration Profile

➔ **To edit an existing profile information:**

1. In the Profiles Management page, click on the **Edit** icon  of a selected profile.
2. The Edit Profile page allows you to set various parameters of the selected profile, using the following tabs:
 - [Profile Info](#). Allows the modification of the profile's information.
 - [Configuration Management](#). Allows the modification of the configuration parameters that the profile includes for distribution.
 - [Site Distribution](#). Allows the distribution of the configuration to the selected site.
 - [Distribution History](#). Displays the distribution history of the selected profile.

8.1.3.4. Profile Info

1. The Profile Info page is displayed as shown in the figure below:

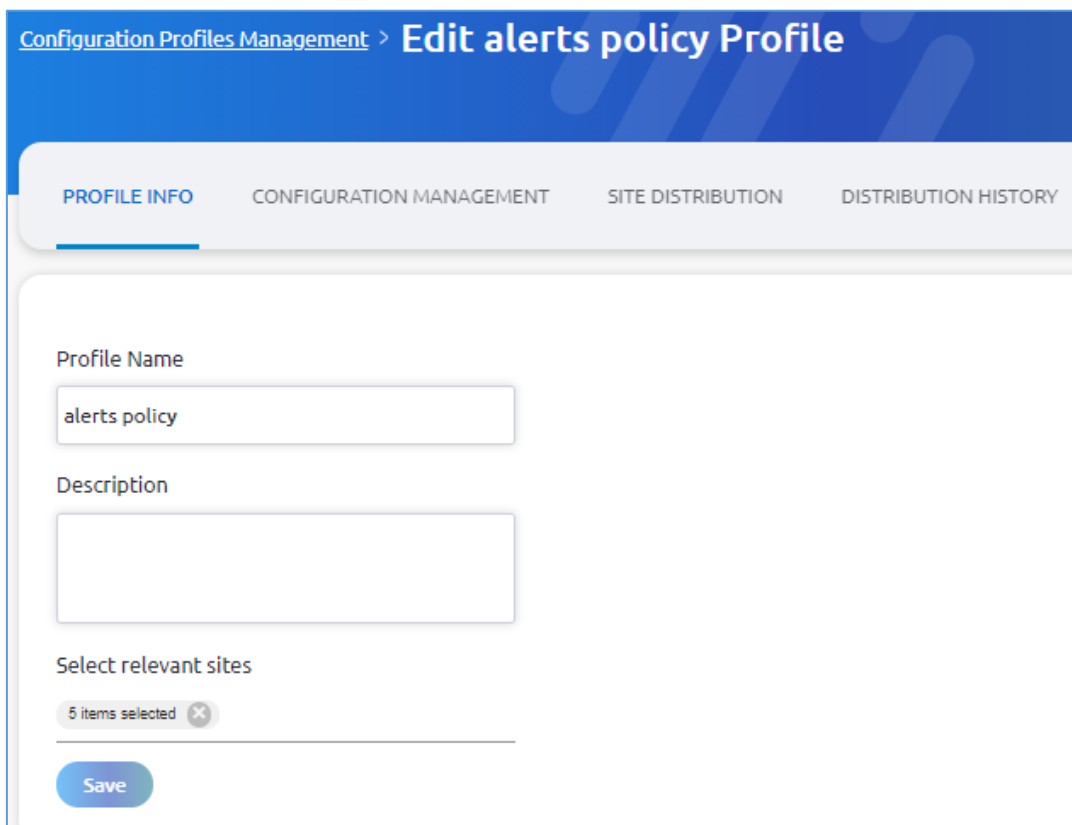


Figure 50: Editing a Configuration Profile

2. Enter the site information as described in Table 10 above.
3. Click **Save**.

8.1.3.5. Configuration Management

The Configuration Management page allows you to modify the configuration parameters of a selected profile.

➔ **To modify the configuration parameters:**


1. Click on the Configuration Management tab, and in the Configuration Management page, select one of the below configuration categories:
 - [Alert Configuration](#)
 - [IP Groups](#)
 - [Syslog Configuration](#)
 - [Email Configuration](#)
 - [Email Scheduler Configuration](#)
 - [Active Directory Configuration](#)

NOTE

The minimum version of the SCADAfence Platform that supports the configuration settings, is 6.5.0.99.

8.1.3.5.1. Alerts Configuration

➔ **To configure the alerts:**

1. Click on the Edit icon  in the selected row.
2. The following window opens:

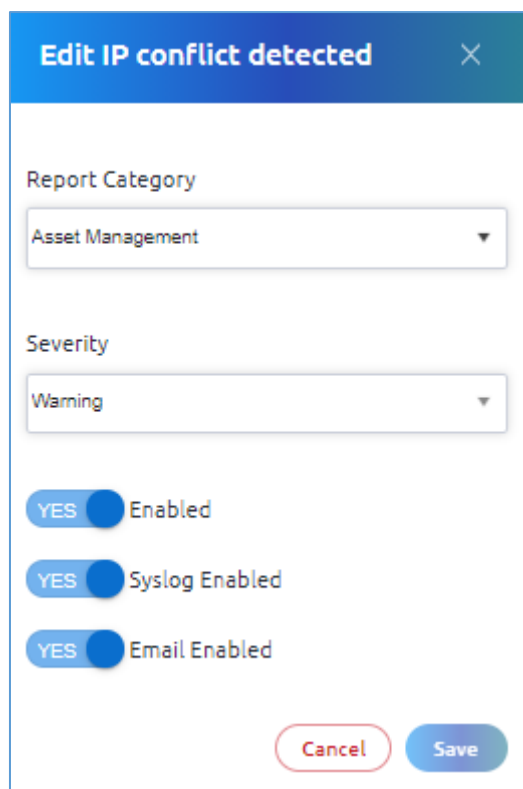


Figure 51: Alert Configuration Window

3. Enter the field values, as described in the table below:

Table 18: Alert Configuration Fields

Field	Description
Report Category	User Modifiable Field. The alert category possible values: <ul style="list-style-type: none"> Operational Exposure Threat Customer Other
Severity	User Modifiable Field. Sets the severity for alerts of this type: <ul style="list-style-type: none"> Log Information Warning Threat Severe Critical
Enabled	User Modifiable Field. If “enabled” the alert type is activated. If “disabled”, new alerts of this type will not be raised.
Syslog Enabled	User Modifiable Field. If “enabled”, then when an alert of this type is raised, it will be recorded in the syslog.
Email Enabled	User Modifiable Field. If “enabled”, then when an alert of this type is raised, an email will be generated.

4. Click on the **Save** button.

8.1.3.5.2. IP Groups

➔ **To configure the IP Groups:**

1. Set the "Explicit definition of internal IP ranges" parameter. Possible values:
 - OFF. The system determines whether an IP address is internal or external, based on the network's behavior. On changing the value to **ON**, the following message is displayed:

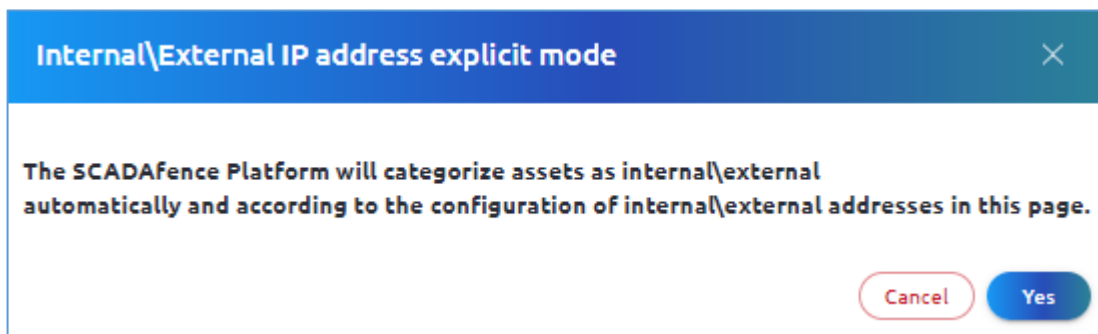


Figure 52: Confirmation for Explicit Definition of Internal IP addresses

- ON. The system overrides the above mechanism by explicitly defining the internal IP addresses, while other addresses are defined as external. When changing the value to **OFF**, the following message is displayed:

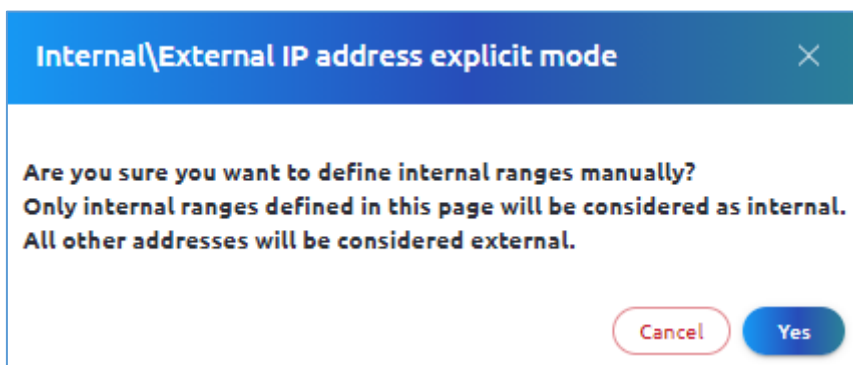



Figure 53: Confirmation for Automatic Definition of Internal IP addresses

2. Click on the Edit icon  in the selected row to edit an existing IP Group configuration, or click on the +Add New button to define a new group.
3. The following window opens:

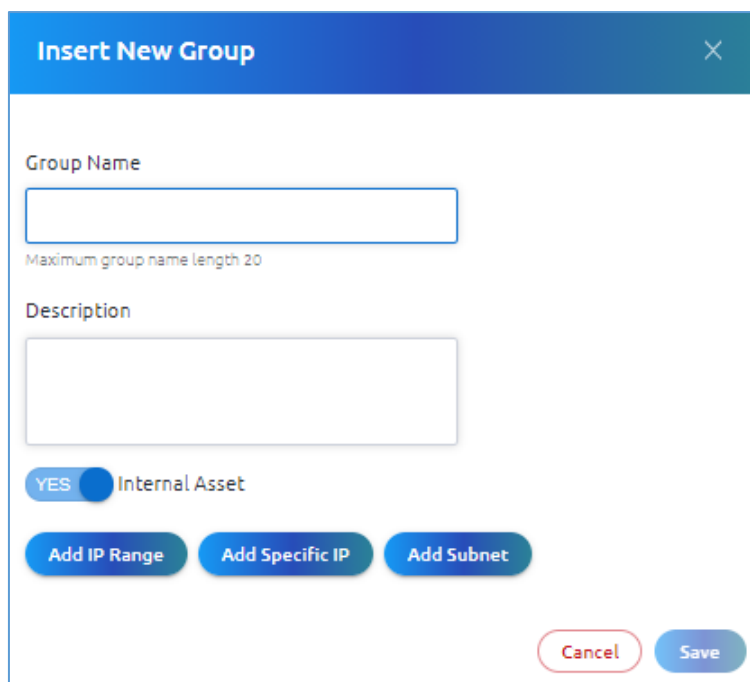


Figure 54: IP Group Configuration Window

4. Enter the Group Name, and a short description on IP Group.
5. Specify if the group is internal or external (applicable when **Explicit definition of internal IP ranges** is set to No).
6. Select one of the following options:
 - Add IP Range. Enter the IP address range: from IP address to IP address.
 - Add Specific IP. Enter a specific IP address.
 - Add Subnet. Enter IP address / subnet field.
7. Click on the **Save** button.

8.1.3.5.3. Syslog Configuration

See section 8.1.5.

8.1.3.5.4. Email Configuration

➔ **For Email Configuration:**

1. Click on the **Email Configuration** tab.
2. The following window opens:

Figure 55: Email Configuration Window

3. Enter the field values, as described in the table below:

Table 19: Email Configuration Fields

Field	Description
SMTP Server	The URL of the SMTP email server that will receive alerts from the system in the form of SMTP messages
Port	The connection port number on the SMTP email server
SMTP User	The SMTP user name
SMTP User Password	The SMTP user's password
Sender Address	Enter the sender platform's URL
Use TLS	If checked, Transport Layer Security (TLS) is enabled

4. Click on the **Save** button.

8.1.3.5.5. Email Scheduler Configuration

➔ **To configure an email scheduler:**


1. Click on the Edit icon  in the selected row, or click on the +Add New button to define a new email scheduler.
2. The following window opens:

Figure 56: Email Scheduler Configuration Window

3. Enter the field values, as described in the table below:

Table 20: Email Scheduler Fields

Field	Description
Report Type	The type of notification to be received: <ul style="list-style-type: none"> • SCADAfence alert notification. Immediate notification regarding a single alert. • SCADAfence system health notification. Immediate notification regarding the system's health. • Periodic alert report. A periodically generated report containing a compilation of all alerts that occurred during the period.
Severity	[Relevant for SCADAfence alert notification only.] The alert severity threshold. Alerts at this level of severity or higher will trigger the transmission of an alert notification to the user by email.
Period of Time	[Relevant for periodic alert report only.] The interval (in days) between periodic alert reports.
Email Address	The recipient's email address

4. Click on the **Save** button.

8.1.3.5.6. Active Directory Configuration

Microsoft's **Active Directory (AD)** provides a broad range of directory-based identity-related services for Windows domain networks. The Active Directory Configuration page allows you to configure the Active Directory's parameters needed for the mapping of the users.

- ➔ **To configure the Active Directory:**

1. Click on the Active Directory Configuration tab.
2. The following window opens:

Figure 57: Active Directory Configuration Window

3. Enter the field values, as described in the table below:

Table 21: Active Directory Fields

Field	Description
Active Directory Server	Enter the URL or the IP address of the AD Server, which runs the active directory services.
Distinguished Name	The root directory of the AD domain.
Base Group Name	The SCADAfence users group name in the AD domain.

4. Click on the **Save** button.

8.1.3.6. Site Distribution

➔ **To distribute the configuration to the selected sites:**

1. Click on **Site Distribution** tab.
2. The Site Distribution page opens:

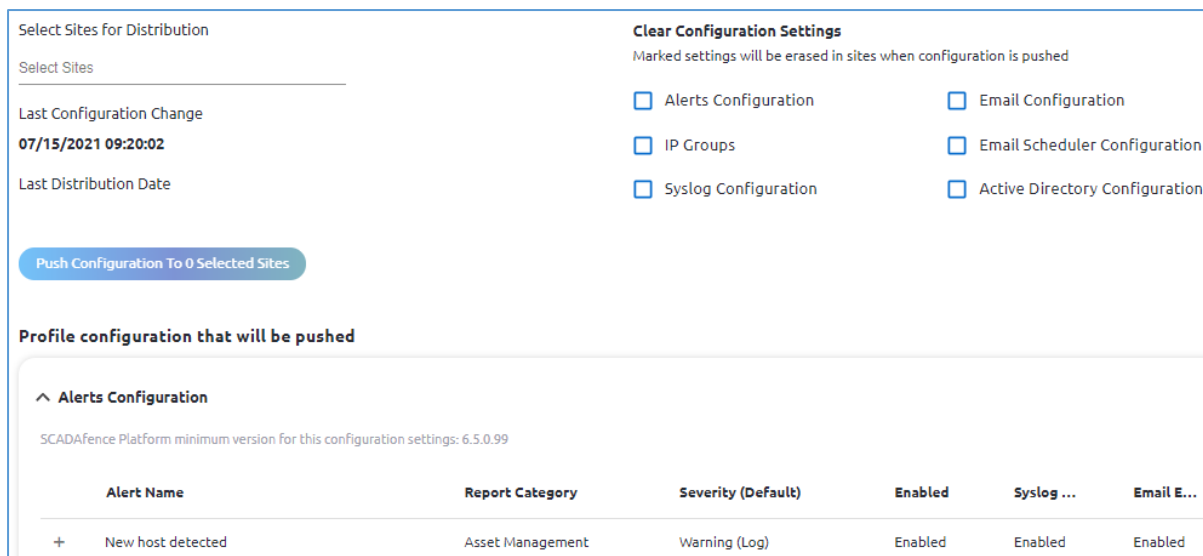


Figure 58: Site Distribution Page

3. Select sites for distribution by clicking on the **Select Site** box, and check the selected sites' check boxes.
4. The Last Configuration Change, and the Last Distribution dates are displayed, if they exist.
5. Select the settings you want to erase in the selected sites, prior to distribution.
6. Click on the **Push Configuration** button to start the distribution.
7. The distributed profile configuration will be listed.

8.1.3.7. Distribution History

➔ **To view the Distribution History of the selected profile:**

1. Click on the **Distribution History** tab.
2. The Distribution History page displays the following information:

Table 22: Profile's Distribution History Fields

Field	Description
Distribution No.	The number of the applied distributions.
Total sites	The total sites to which the profile has been distributed.
Distributed Date	The time of the profile distribution.
Status	The status of the distribution.

8.1.4. Account API Keys Management

API keys are used for message authentication when connecting to the SCADAfence database.

➔ **To create the keys**

1. Click on the **Account API Keys Management** arrow (see Figure 39Error! Reference source not found.).

2. The API Keys Management page appears as shown in the figure below.

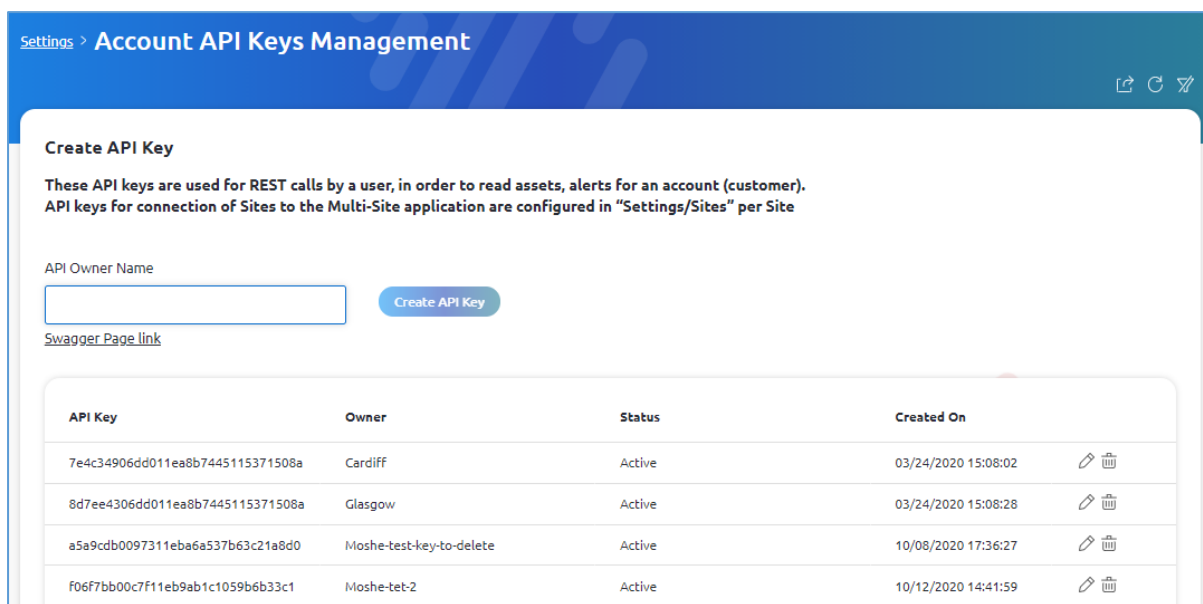
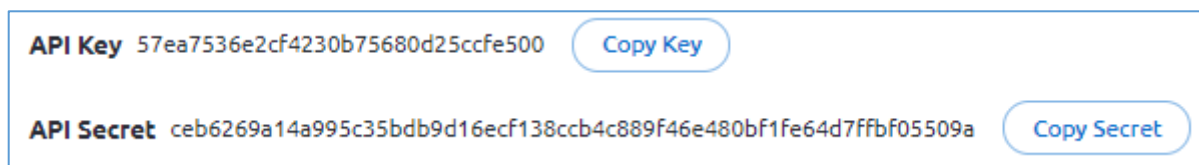


Figure 59: Account API Keys Management Settings


3. Enter the **API Owner Name**.
4. Click on the **Create API Keys** button to create the public and the secret keys to be distributed to users.



The following table describes the parameters listed in the API Keys Management Window.

Table 23: Account API Keys Management Fields

Field	Description
API Key	The API key created by the system.
Owner	The name of the owner of the key, inserted by the user.
Status	The key's status: <ul style="list-style-type: none"> • Active. The key is active and can be used for authentication. • Suspend. The key is suspended. • Invoked. The key is already in use.
Created On	The key creation timestamp.

5. To modify the owner's name or the key status, click on the Edit icon  of a selected row.
6. Click on the Swagger Page link to view the SCADAfence API documentation.

8.1.5. License Management

The system allows the upload of the license to all the SCADAfence platforms.

- ➔ **To upload the license to all the platforms:**
 1. Select the License Management option in the Settings menu.
 2. The License Management page is displayed:

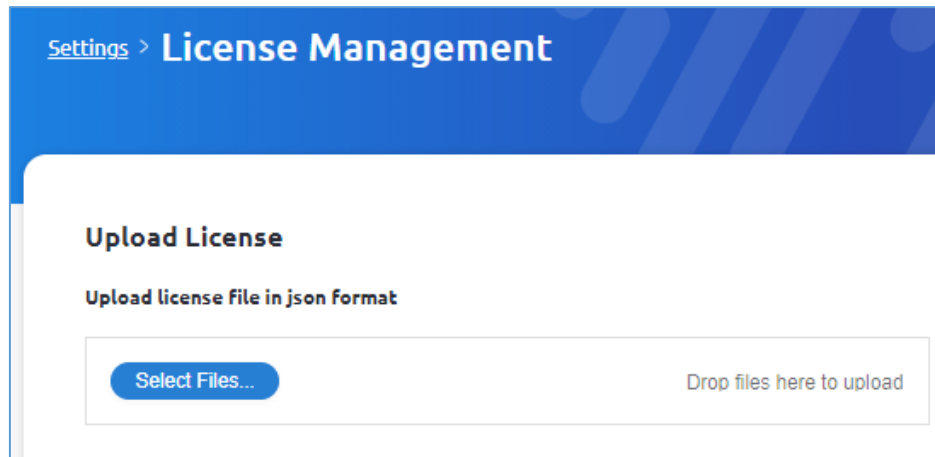


Figure 60: License Management Page

3. Press the Select Files button to browse the license file.
4. Click on the Upload button.

8.1.6. Syslog Configuration

- ➔ **To configure the Syslog:**
 1. Click on the **Syslog Configuration** arrow (see Figure 39).
 2. The Syslog Configuration page appears as shown in the figure below.

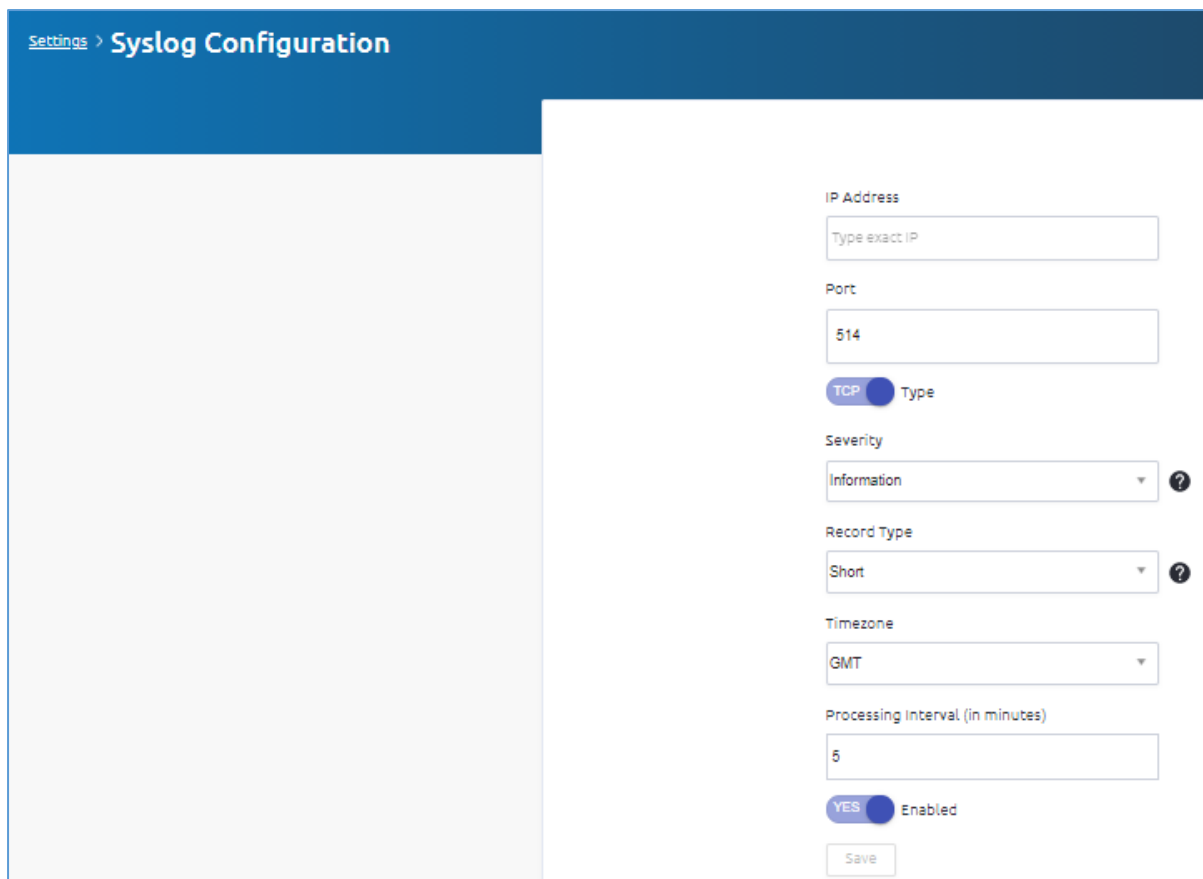


Figure 61: Syslog Configuration Settings

- Enter the syslog configuration parameters, as listed in the table below:

Table 24: Syslog Configuration Fields

Field	Description
IP Address	The IP address of the target Syslog server.
Port	The connection port number on the target Syslog server.
Type	The transport layer protocol used: <ul style="list-style-type: none"> TCP UDP
Severity	The alert severity threshold. Alerts at this level of severity or higher will trigger the transmission of an alert message to the Syslog server.
Record Type	The record type: <ul style="list-style-type: none"> 'short' - with the default set of fields 'long' - extended record with more fields, such as description, solution, etc.
Time zone	Select the appropriate time zone, using the drop-down window.
Interval	The syslog's processing interval (in minutes). Default value = 5 minutes.
Enabled	Switch the toggle to Yes to enable the connection.

- Click **Save**.

8.1.7. Alerts Sources

➔ To view the alert sources:

1. Click on the **Alerts Sources** arrow (see Figure 39).
2. The Alert Sources page appears as shown in the figure below.

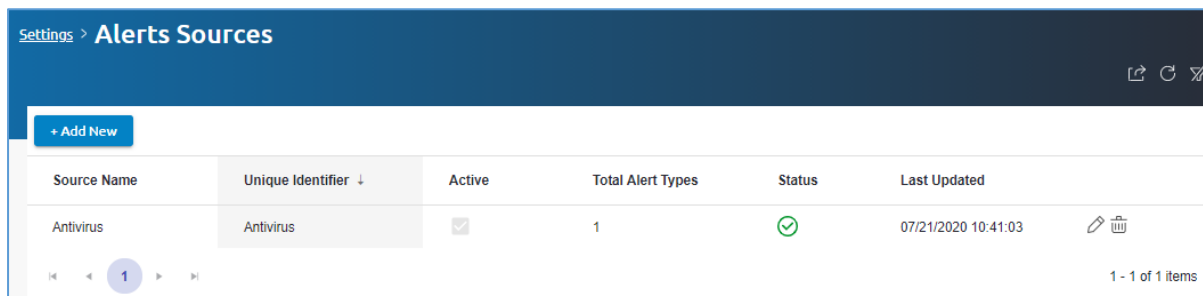




Figure 62: Alert Sources Settings

The fields in the Alert Sources window are described in the table below:

Table 25: Alert Sources Fields

Field	Description
Source Name	The name of the entity that sourced the alert.
Unique Identifier	The unique identifier of the alert source.
Active	The alert source status: <ul style="list-style-type: none"> • Active. The source is currently active. • Inactive. The source is not active.
Total Alert Types	The number of alert types associated with the source.
Status	 Connected
	 Disconnected

8.1.7.1. Adding a New Alert Source

➔ To add a new alert source

1. Click on the **+Add New** button.
2. The Add New External Source window opens:

Figure 63: Adding a New Alert Source

3. Enter the parameters (see Table 25).
4. Click **Save**.

8.2. User Management and Security Settings

Using the User Management and Security Settings menu, you can manage the following settings (see Figure 38):

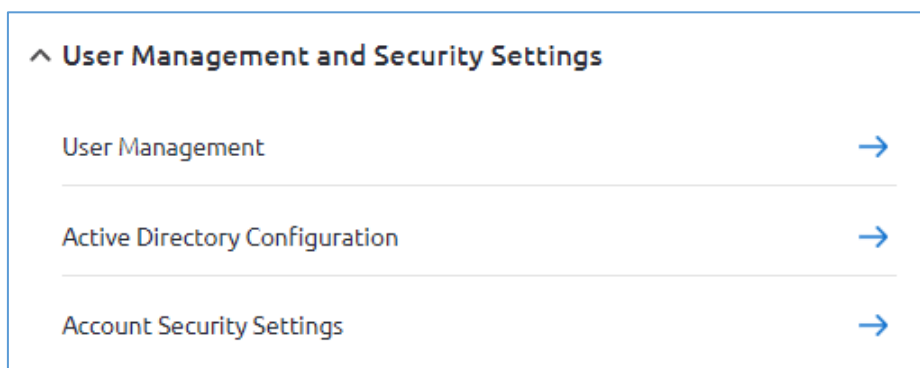


Figure 64: User Management and Security Settings Menu

- [User Management](#)
- [Active Directory Configuration](#)
- [Account Security Settings](#)

➔ **To manage the user and database permissions:**

1. Click on the **User Management** arrow (see Figure 64).

2. The User Management page appears as shown in the figure below.

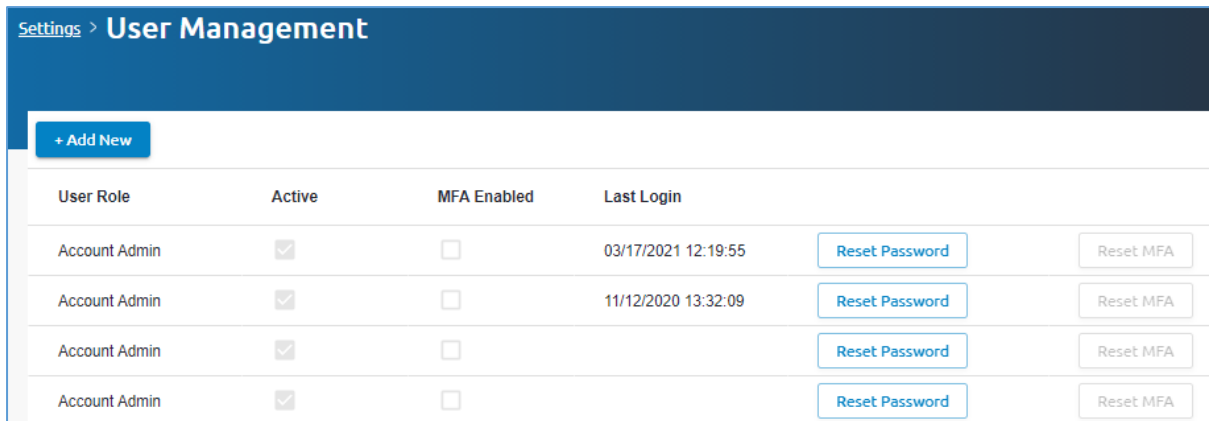


Figure 65: User Management Settings

The user management parameters are listed in the below table:

Table 26: User Management Fields

Field	Description
User Name	The user name.
Active	User's status: <ul style="list-style-type: none"> • Active. The user has access to the system. • Inactive. The user does <i>not</i> currently have access to the system.
MFA Enabled	Multiple Factor Authentication activation status.
Last Login	Timestamp of the last user login.
Reset Password	Click to reset the user's password

8.2.1.1. Adding a New User

➔ To add a new user to the system:

1. Click on **+Add New**.
2. The Add User window opens:

Figure 66: Add User

3. Enter the user information as listed in the below table:

Table 27: User's Fields

Field	Description
Username	The user name.
Email	The user's email address.
Role Name	The user's role: <ul style="list-style-type: none"> • Account Admin. User with full administrator privileges. • Account User. User without administrator privileges.
New Password	Enter the user's password. Click on the "eye" icon to display the entry.
Confirm Password	Enter the user's password a second time for confirmation. Click on the "eye" icon to display the entry.
First Name	The user's first name
Last Name	The user's last name
Active	User's status: <ul style="list-style-type: none"> • Active. The user has access to the system. • Inactive. The user does <i>not</i> currently have access to the system.

4. Click **Save**.

8.2.2. Account Security Settings

This section enables the user to enhance the system's security by enabling the MFA option, and setting an access list.

8.2.2.1. Enabling the MFA Option

The Multi-Factor Authentication (MFA) adds an additional layer of security to the user's account, by using the Google Authenticator.

This page allows the admin to enable the MFA mechanism for all users. When MFA is enabled here, users can enable the MFA for their own accounts.

➔ **To enable the MFA for all users:**

1. Click on the **Account Security Setting** arrow (see Figure 64).
2. The **Account Security Setting** page appears as shown in the figure below.
3. Toggle the **MFA Enabled** button to Yes.
4. Click on Save MFA State.

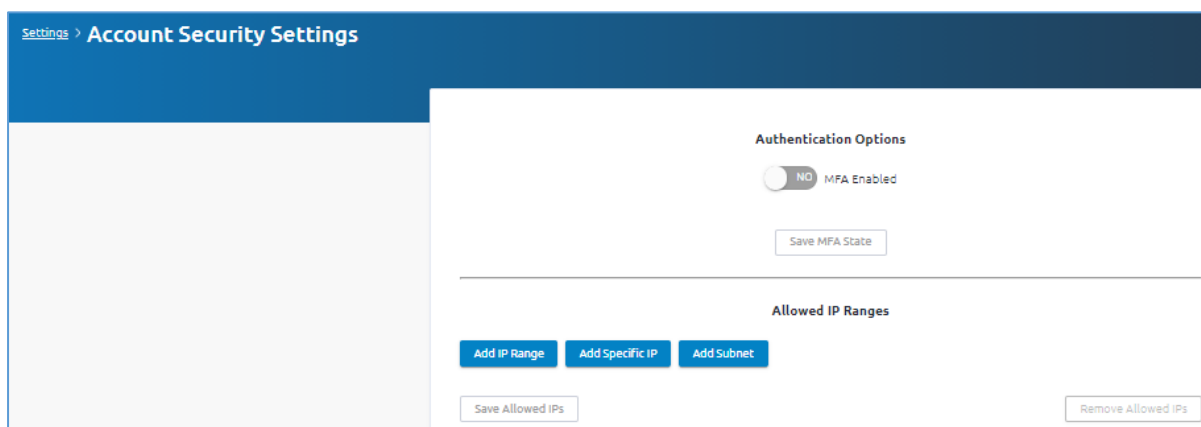


Figure 67: Enabling the MFA

8.2.2.2. Configuring an IP Address White List

➔ **To configure an IP address white list:**

1. Specify the IP addresses that are authorized to access the system, by setting the following:
 - **Add IP Range.** Enter a range of authorized IP addresses, using the **From** and **To** fields
 - **Add Specific IP.** Enter a specific authorized IP address.
 - **Add Subnet.** Enter an authorized subnet mask.

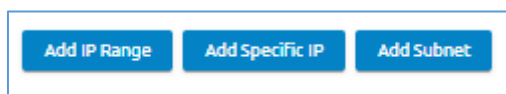
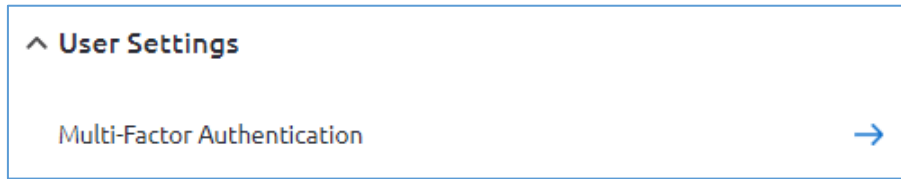


Figure 68: White List Options

2. Click on **Save Allowed IPs** to save the white list entry.

8.3. User Settings

Using the User Settings menu, you can manage the following setting (see Figure 38):



8.3.1. Multi-Factor Authentication

This page allows an individual user to add an additional layer of security to the user's own account, by using the Google Authenticator.

➔ **To enable the user's MFA:**

1. Toggle the **MFA Enabled** button to Yes.
2. Click on Save MFA State.
3. Enter your account password.

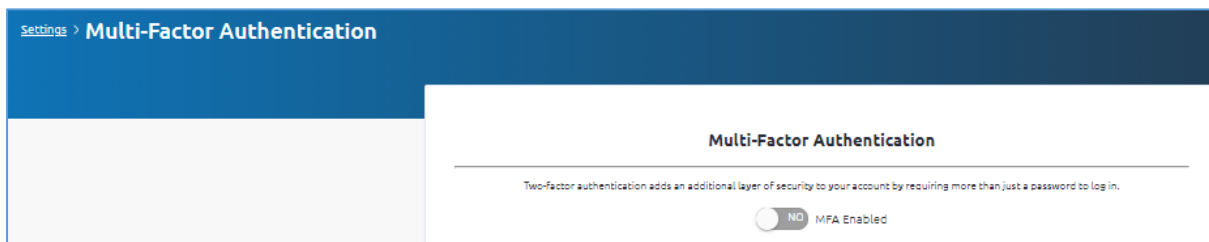


Figure 69: Adding the Additional Password

4. Click **Validate**. The following window opens:

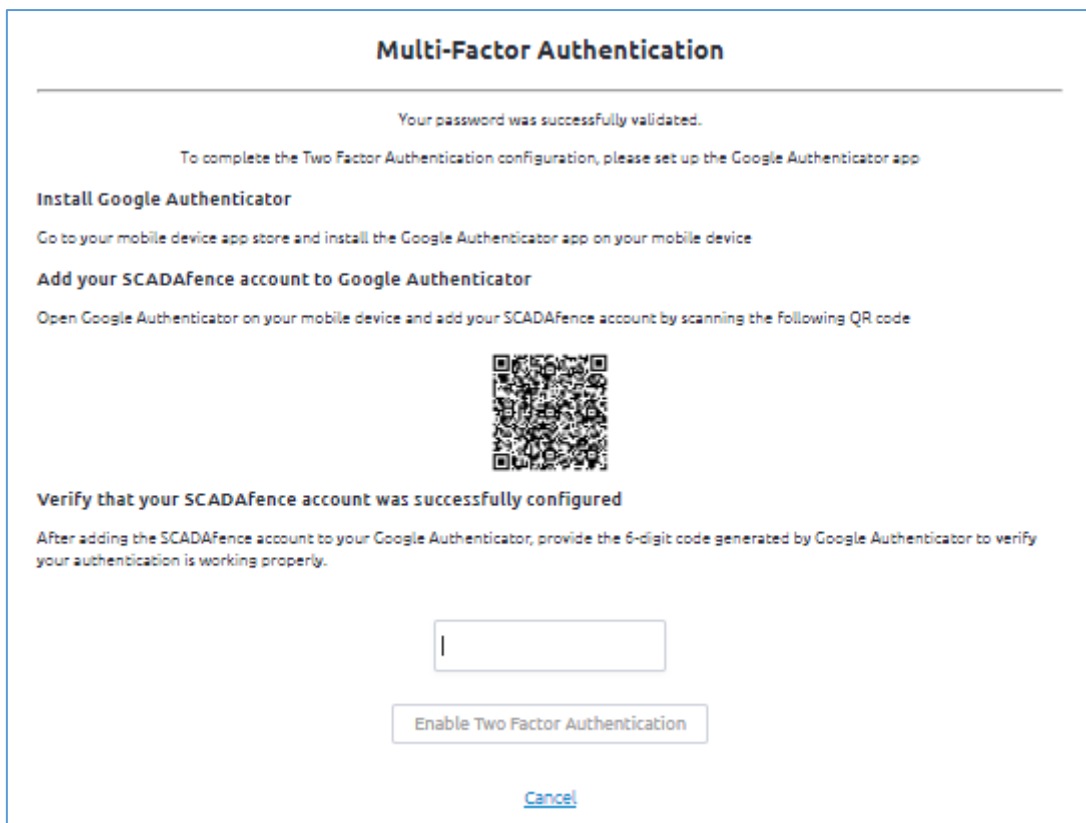


Figure 70: Google Authentication Entry

5. Enter your Google's 6-digit code, and Click on Enable.

8.4. System Language Settings

➔ To configure the language used in the SCADAfence Multi-Site GUI:

1. Click on the **System Language** drop down list (see Figure 38).
2. Select a language from the list.

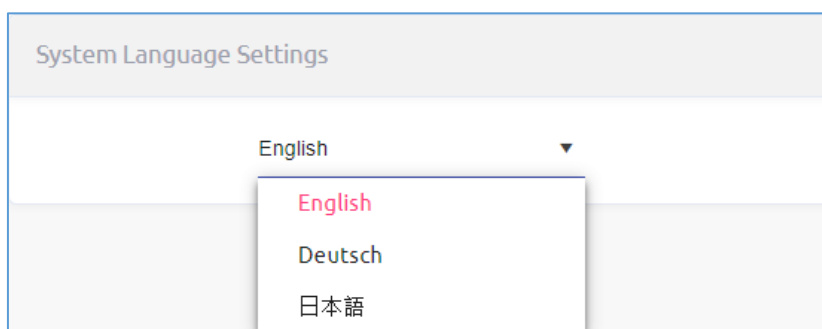


Figure 71: User Interface Language Setting

8.5. Admin Settings

To modify the admin settings, click on the **Settings** icon in the sidebar menu to display the setting options, as shown in the figure below.

- [Change Password](#)

- [Logout](#)

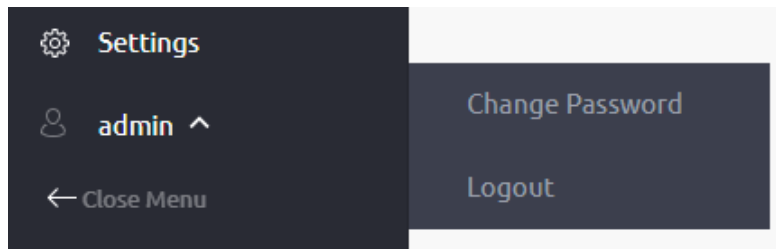


Figure 72: Admin Settings Menu

8.5.1. Change Password

➔ To change a password:

1. Click on the **Admin Settings** icon in the sidebar menu
2. Select **Change Password** (see Figure 72). The Change Password window opens:

Figure 73: Changing the Password

3. The password requirements are as follows:
 - Minimum 8 characters
 - Minimum one uppercase letter
 - Minimum one lowercase letter
 - Minimum one digit
4. Enter the new password and re-enter it for confirmation.
5. Click on Change Password

8.5.2. Logout

➔ To logout the system:

1. Click on the **Admin Settings** icon in the sidebar menu.
2. Select **Logout** (see Figure 72).

3. Confirm the logout in the message box below:

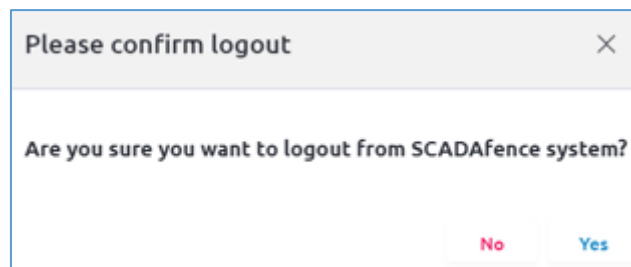


Figure 74: Logout Confirmation

To login, follow the [Login](#) steps in section 3.1.

END OF DOCUMENT