

CISS INTERCEPTOR

Quick Start Guide

A quick start guide reference document for CISS INTERCEPTOR



Revision: Quick_Satart_Guide_1.0

September 2018

Cyber Forza Inc. Confidential and Proprietary

Copyright © 2018, Cyber Forza Incorporation. All rights reserved.

This document contains information that is considered proprietary and the property of Cyber Forza Inc. The content of this document may not be used in any way, duplicated, or distributed by any means without the express written permission of Cyber Forza Inc

Cyber Forza Inc. may change specifications and product description at any time, without notice.

Contact Cyber Forza Inc. to obtain latest specification.

Revision History

Date	Author(s)	Description
09/18/18	CyberForza Team	Initial version: 1.0

Table of Contents

1. System Prerequisites	5
2. CISS Interceptor.....	6
2.1. Introduction	6
2.2. Data Flow Diagram	7
2.3. Feature List.....	7
2.4. Log In Page	8
2.5. Dashboard.....	8
2.6. Change Administrator Password.....	9
3. Databases	11
3.1. LDAP Database.....	11
3.2. Radius Database	14
4. Real Time Monitoring (RTM)	16
4.1. Add Windows And Linux Server	17
4.2. Add Devices	18
4.3. Add Contact.....	19
4.4. Remove Device	20
5. Threat analytics (TA).....	21
5.1. ADD Agent	22
5.2. Multiple KEY Generation	23
5.3. ADD Contact.....	24
5.4. Set Alert Levels	25
6. Breach Detection and Malware Protection	26
7. Configuration Management	26
8. Regulatory Compliance	27

List of Figures

Figure 1 CISS Interceptor Data Flow Diagram	7
Figure 2 Change Administrator Password	10
Figure 3 LDAP Login Page	11
Figure 4 LDAP Dashboard	11
Figure 5 LDAP Create Object.....	13
Figure 6 Radius Database Login Page	14
Figure 7 Radius Database Dashboard	15
Figure 8 Real Time Monitoring Login Page	16
Figure 9 Real-Time Monitoring Dashboard	16
Figure 10 RTM Dropdown List	17
Figure 11 Add Windows or Linux Server.....	17
Figure 12 Add a Device	18
Figure 13 Add a Contact	19
Figure 14 Remove a Device.....	20
Figure 15 Threat Analytics Dashboard	21
Figure 16 Adding an Agent.....	22
Figure 17 Key Generated	23
Figure 18 Multiple Key Generation	24
Figure 19 ADD contact	24
Figure 20 Change Alert Level.....	25
Figure 21 Breach Detection and Malware Protection Dashboard	26
Figure 22 Regulatory Compliance Dashboard	27

1. System Prerequisites

● Disk Size: 60 GB
● OS type: 64-bit
● Memory: 8 GiB
● Processor: Intel Core 2 Duo CPU E8400 @ 3.00GHz x 2

2. CISS Interceptor

2.1. Introduction

CISS Interceptor is Powered by **Cognitive AI (10-IN-1) Engine Cyber Security Product** that provides granular-level insight into the internal network, infrastructure, applications, IOT, security policies, regulatory compliance, real-time monitoring and reporting of threats. This provides comprehensive visibility of all activities, to IT and network administrators. Interceptor enables improved data integrity, data forensic analysis and facilitates risk assessment. Proactively detecting cyber footprint and behavioral patterns in a single platform, to identify threat intensity and prevent insider attacks before they can occur.

Traditional existing solutions are bound to the TCP/IP protocol stack and only recognize IP addresses of devices on the network, not the actual user. Threats have become more sophisticated, internal users can also carry out major attacks. Real-Time Monitoring and reporting the internal cyber threats is a major challenge for organizations. Advanced user identity co-relations provide IP address, username or user group. Interceptor provides the ability to either allow or deny access to files, Internet sites and applications based on a user's access rights, determined by the user's or the user group's business needs.

2.2. Data Flow Diagram

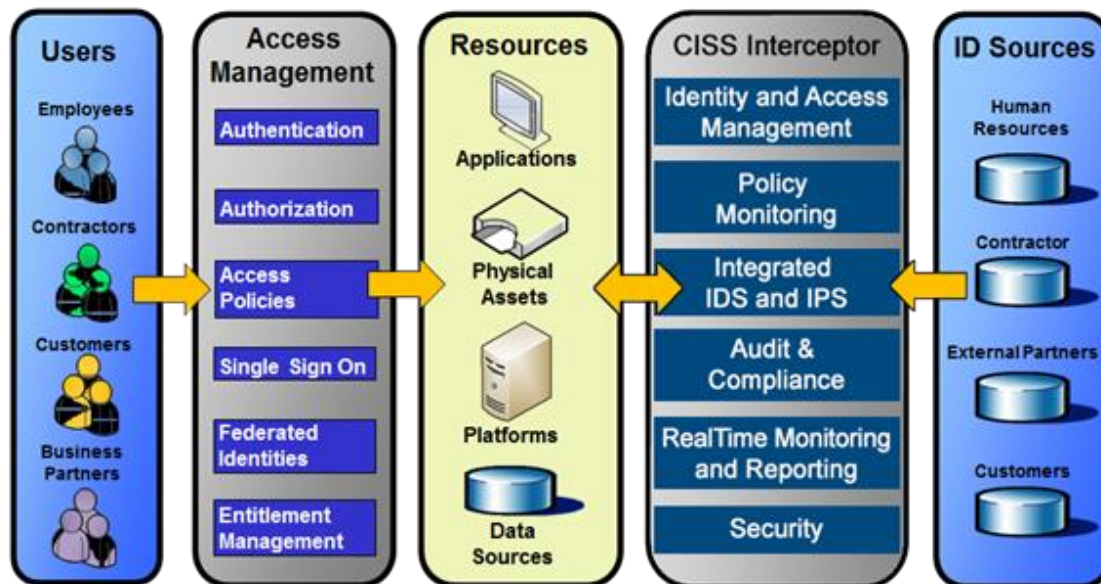


Figure 1 CISS Interceptor Data Flow Diagram

2.3. Feature List

- Data Loss Protection
- Data Integrity
- Data Forensics
- Integrated IDS / IPS
- Identity Access Management (IAM)
- Single Sign-On (SSO)
- Multi-Factor Authentication (MFA)
- IP Theft Protection
- Corporate Security Policy Monitoring
- Data Centers, Servers and IOT Real-time Monitoring
- Real Time Security Alerts
- Regulatory Compliance
- PCI-DSS, HIPAA, SOX, FISMA, CIS, CDI, CUI, DFARS Compliance
- Real-time Reporting and Notifications
- Security Audit and Report Generation

2.4. Log In Page

- Enter the following the credentials to Login into CISS – Interceptor.
- **Username: administrator**
- **Password: radius**

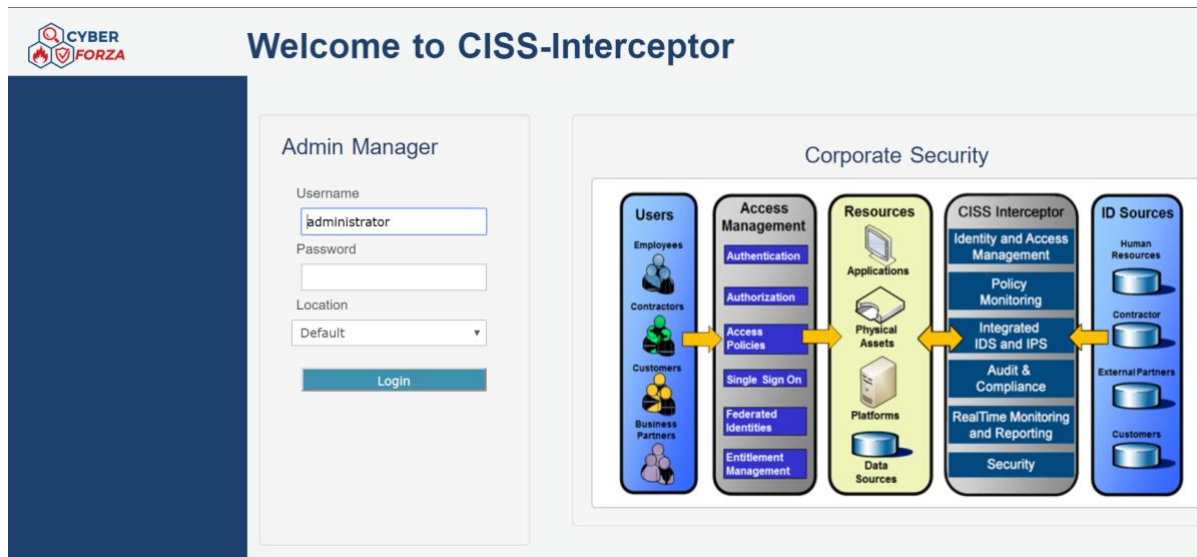


Figure 2 CISS-Interceptor Login Page

After you login, Interceptor Dashboard opens as in fig. 3

2.5. Dashboard

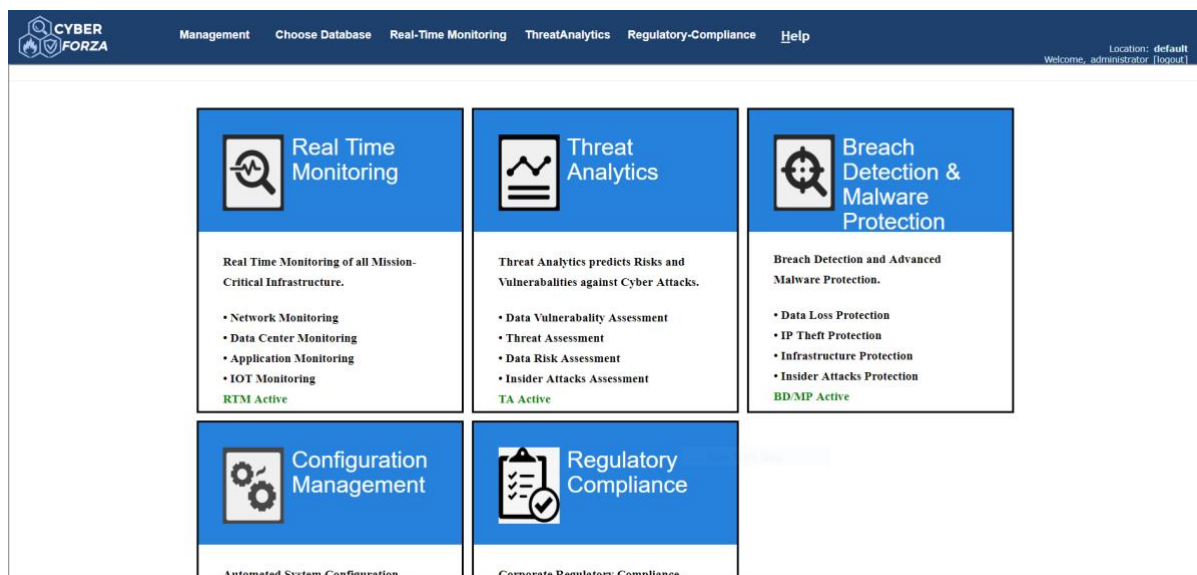
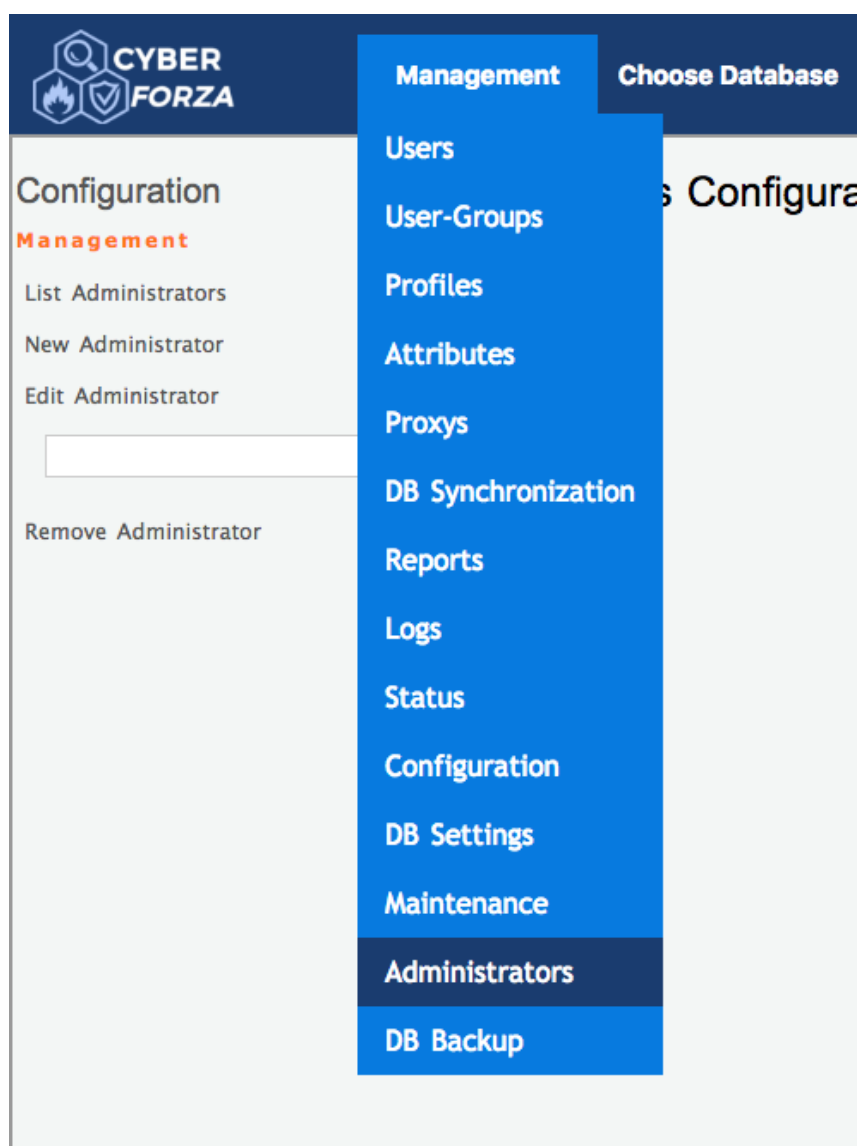


Figure 3 CISS-Interceptor Dashboard

2.6. Change Administrator Password

- Under **Management Tab** click **administrators**, it will open up administrator configuration page.
- In configuration page select **List Administrators** to view all the administrators added.
- Select the desired administrator and change password on the next page, **Edit Administrator Settings** and click apply to save the new **password**



Configuration
Management
List Administrators
New Administrator
Edit Administrator
Remove Administrator

Administrators Configuration +

Configuration
Management
List Administrators
New Administrator
Edit Administrator
Remove Administrator

Administrators Listing +

SELECT: [ALL](#) [NONE](#)

1

ID	Username	Password
<input type="checkbox"/> 6	administrator	radius123
<input type="checkbox"/> 7	test	test

PAGE 1 OF 1

Configuration
Management
List Administrators
New Administrator
Edit Administrator
Remove Administrator

Edit Administrator Settings +

Administrator Info
Contact Info
ACL Settings

Administrator Password

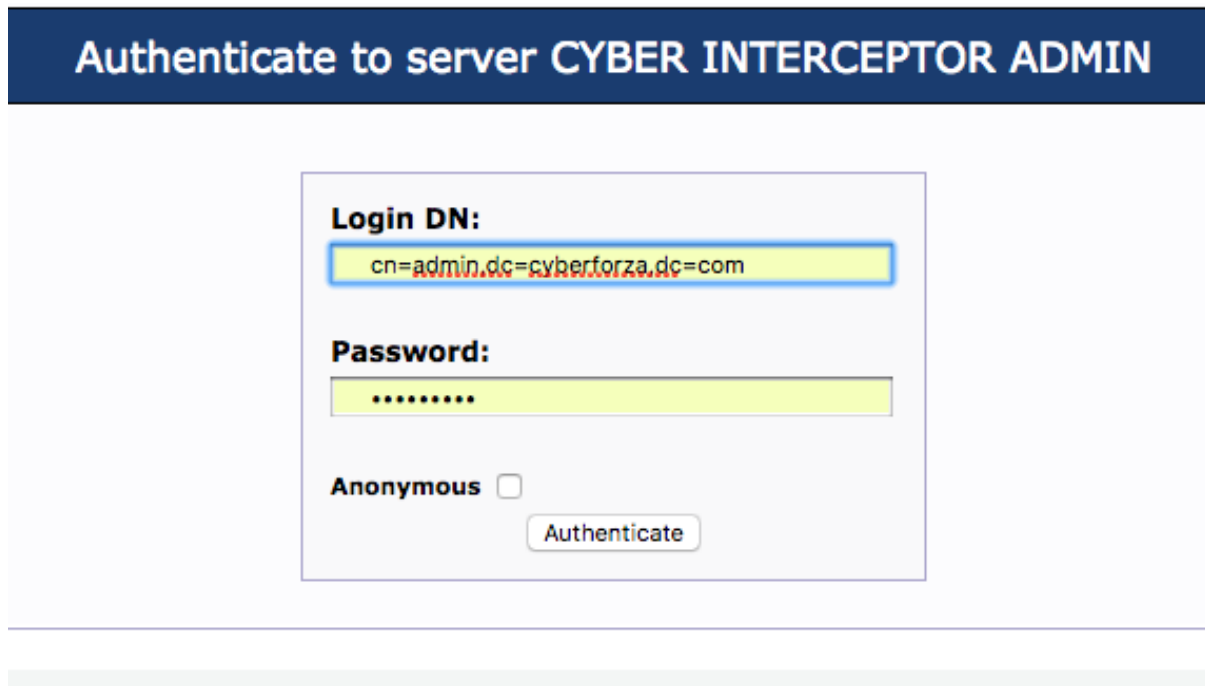
Figure 2 Change Administrator Password

3. Databases

3.1. LDAP Database

- Click **LDAP database** under **Choose Database** dropdown to create a LDAP database and account.
- A login page pops up, to which, enter the following credentials.

Password: radius123



The image shows a login page titled "Authenticate to server CYBER INTERCEPTOR ADMIN". It contains a form with the following fields and elements:

- Login DN:** A text input field containing "cn=admin,dc=cyberforza,dc=com".
- Password:** A password input field with masked characters (dots).
- Anonymous:** A checkbox that is currently unchecked.
- Authenticate:** A button to submit the login credentials.

Figure 3 LDAP Login Page

Creating a **LDAP User Admin** to gain access to **Real Time Monitoring**.

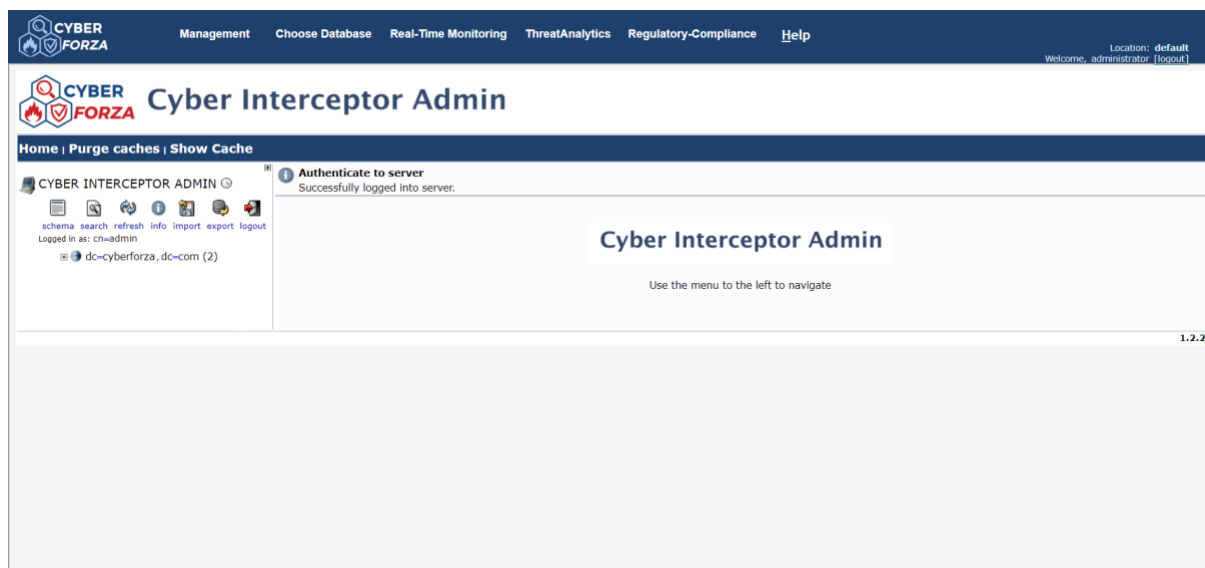
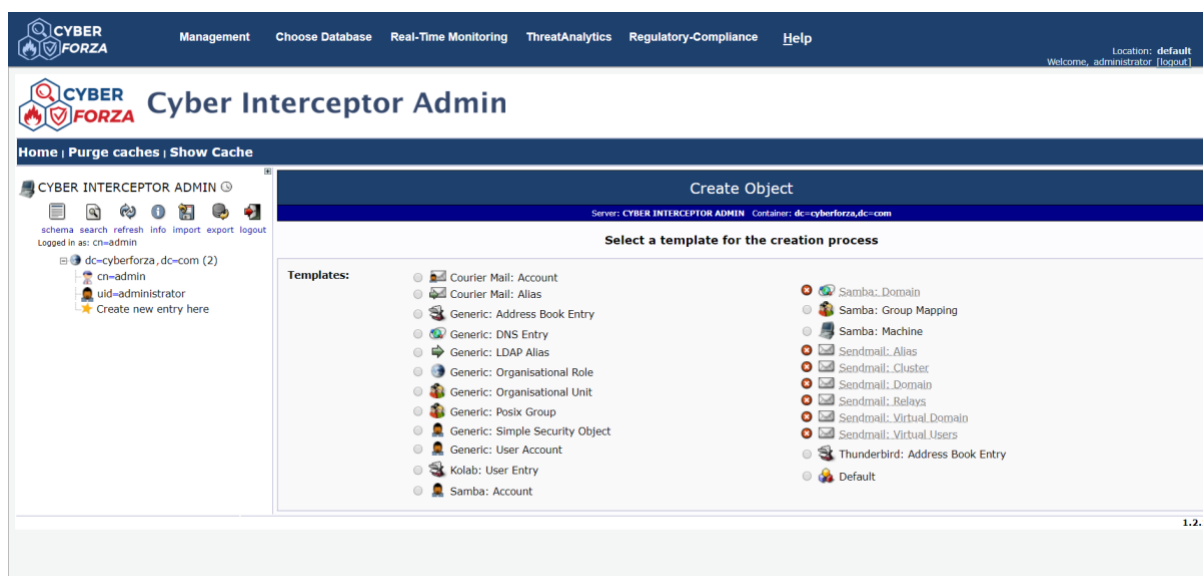


Figure 4 LDAP Dashboard

- select the plus button (+) in front of dc=cyberforza,dc=com (1) option,
- select the **create new entry here** option,
- select the **Generic: Simple Security Object**,
- Create username and password for user, with the following credentials:
Username: administrator
Password: sai123
- Click **Create Object** and on the next page click **Commit** to save the user.



CYBER FORZA Cyber Interceptor Admin

Home | Purge caches | Show Cache

Create Object

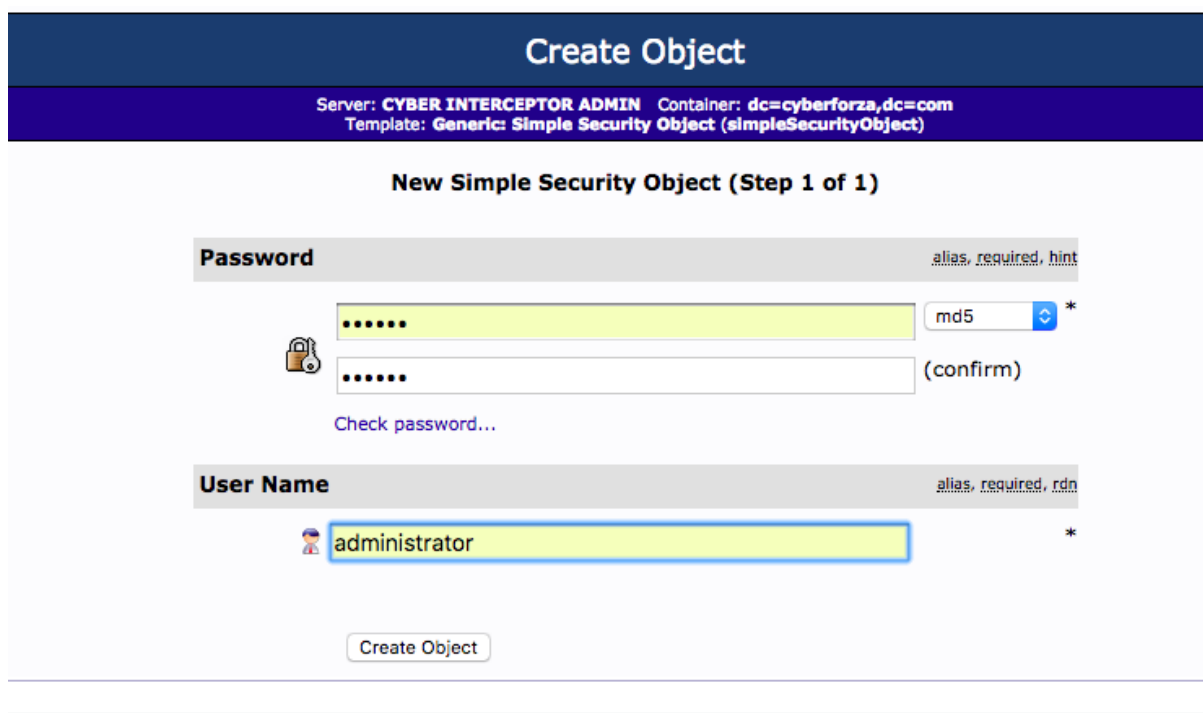
Server: CYBER INTERCEPTOR ADMIN Container: dc=cyberforza,dc=com

Select a template for the creation process

Templates:

- Courier Mail: Account
- Courier Mail: Alias
- Generic: Address Book Entry
- Generic: DNS Entry
- Generic: LDAP Alias
- Generic: Organisational Role
- Generic: Organisational Unit
- Generic: Posix Group
- Generic: Simple Security Object
- Generic: User Account
- Kolab: User Entry
- Samba: Account
- Samba: Domain
- Samba: Group Mapping
- Samba: Machine
- Sendmail: Alias
- Sendmail: Cluster
- Sendmail: Domain
- Sendmail: Relays
- Sendmail: Virtual Domain
- Sendmail: Virtual Users
- Thunderbird: Address Book Entry
- Default

1.2.2



Create Object

Server: CYBER INTERCEPTOR ADMIN Container: dc=cyberforza,dc=com
Template: Generic: Simple Security Object (simpleSecurityObject)

New Simple Security Object (Step 1 of 1)

Password alias, required, hint

..... md5 *

..... (confirm)

Check password...

User Name alias, required, rdn

administrator *

Create Object

Create LDAP Entry

Server: **CYBER INTERCEPTOR ADMIN** Container: **dc=cyberforza,dc=com**

Do you want to create this entry?

Attribute	New Value	Skip
userid=administrator,dc=cyberforza,dc=com		
objectClass	account simpleSecurityObject	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
User Name	administrator	<input type="checkbox"/>

Figure 5 LDAP Create Object

3.2. Radius Database

- Select the **Radius Database** under **Choose Database tab**.
- Enter the following credentials to login.
- **Username: admin**
- **Password: password**



The image shows the login page for the Cyber Interceptor DB. At the top left is the CYBER FORZA logo. To its right is the text "Cyber Interceptor DB". Below the logo is a "Language" dropdown menu with "English" selected. Below that is a "Log in" button with a user icon. Underneath the button are two input fields: "Username:" and "Password:". At the bottom right of the form is a "Go" button.

Figure 6 Radius Database Login Page

Primary Functions:

- Authenticates users or devices before allowing them access to a network.
- Authorizes those users or devices for specific network services.
- Accounts for and tracks the usage of those services.

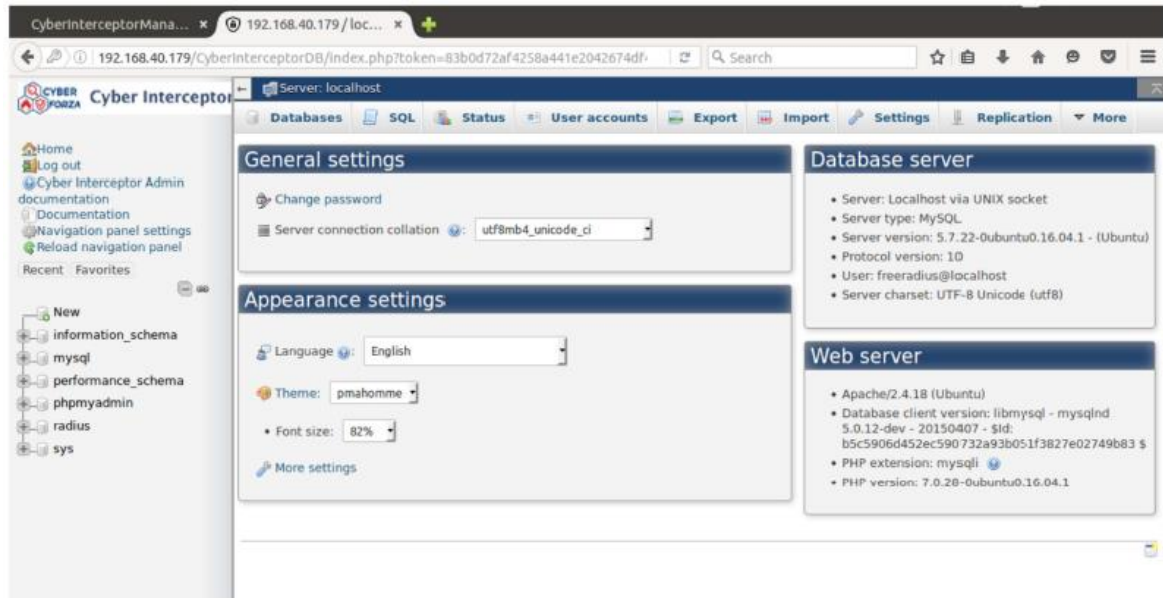
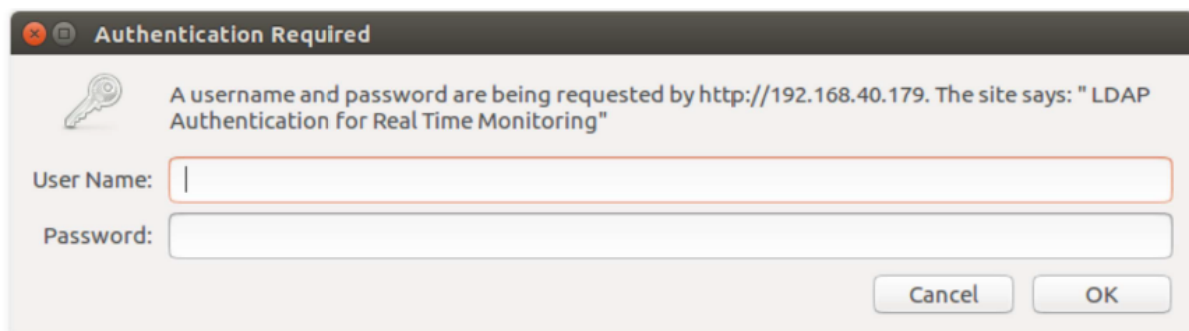


Figure 7 Radius Database Dashboard

4. Real Time Monitoring (RTM)

- Under Real Time Monitoring click on Launch Real Time Monitoring and login into the application using the following credentials.
- **Username: administrator**
- **Password: sai123**



Authentication Required

A username and password are being requested by http://192.168.40.179. The site says: "LDAP Authentication for Real Time Monitoring"

User Name:

Password:

Cancel OK

Figure 8 Real Time Monitoring Login Page

Once logged in, you can see the **RTM Dashboard**.



CYBER FORZA

Management Choose Database Real-Time Monitoring ThreatAnalytics Regulatory-Compliance Help

Location: default
Welcome, administrator [logout]

Cyberforza Interceptor Monitoring Tool

This is a monitoring powerful tool that provides you with instant awareness of your organization's mission-critical IT infrastructure. This monitoring tool allows you to detect and repair problems and mitigate future issues before they affect end-users and customers. Monitoring switches and routers can either be easy or more involved - depending on what equipment you have and what you want to monitor.

As they are critical infrastructure components, you'll no doubt want to monitor them in at least some basic manner.

Switches and routers can be monitored easily by pinging them to determine packet loss, RTA, etc. If your switch supports SNMP, you can monitor port status.

General

- Home
- Current Status**
 - Tactical Overview
 - Map
 - Hosts
 - Services
 - Host Groups
 - Summary
 - Grid
 - Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages
- Quick Search:
- Reports**
 - Availability
 - Trends
 - Alerts
 - History
 - Summary
 - Histogram
 - Notifications
 - Event Log
- System**
 - Comments
 - Downtime
 - Process Info
 - Performance Info
 - Scheduling Queue
 - Configuration
- Logout**
 - Logout RTM session

Data Breach

Cyber Attack

Figure 9 Real-Time Monitoring Dashboard

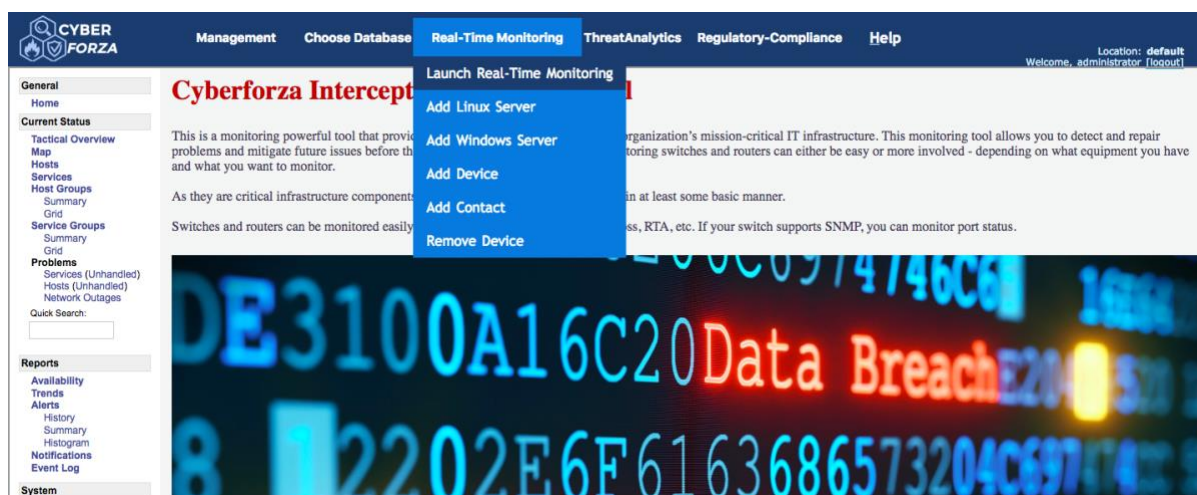


Figure 10 RTM Dropdown List

4.1. Add Windows And Linux Server

- To add either a **Windows or Linux** server, select **Add Windows Server** and **Add Linux Server** respectively from the dropdown list under **Real Time Monitoring** tab.
- When clicked the following pages open. Fill the required fields and click ADD to complete.

ADD WINDOWS SERVER

Enter Name:

Enter Alias:

Enter IP:

Add Windows Server

clear

ADD UNIX/LINUX SERVER

Enter Name:

Enter Alias:

Enter IP:

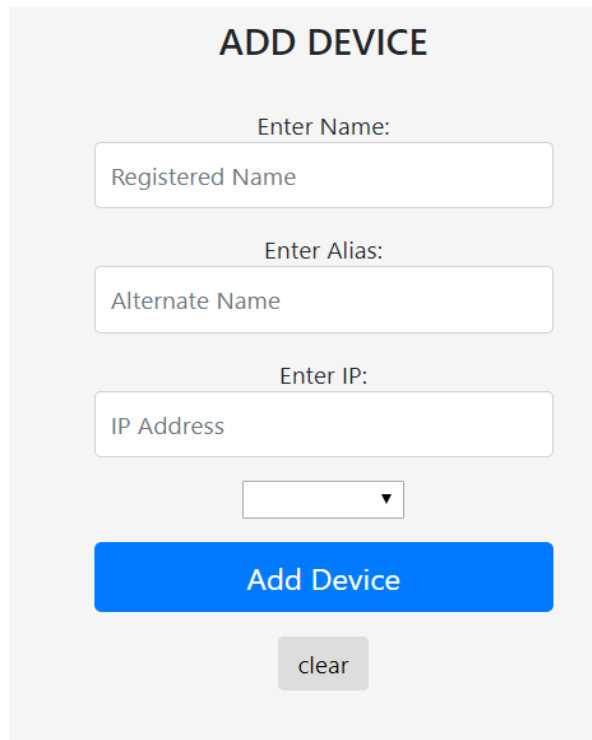
Add Unix/Linux Server

clear

Figure 11 Add Windows or Linux Server

4.2. Add Devices

- To add **Linux, Windows, IOT, Printer, Switch** devices select **ADD Device** from the dropdown list under **Real Time Monitoring** tab.
- When clicked the following page open. Fill the required fields, select appropriate device (**Linux, Windows, IOT, Printer, Switch**) from drop down list and click ADD to complete.

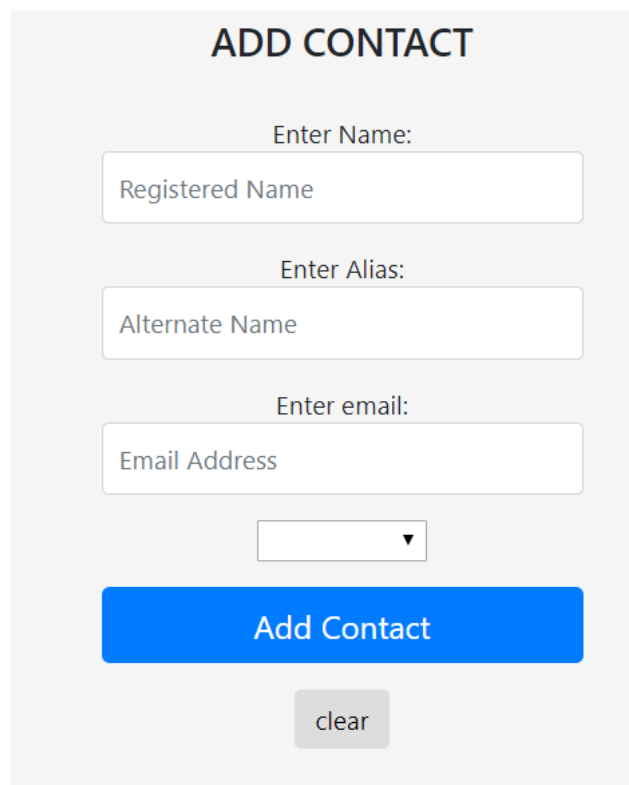


The screenshot shows a web form titled "ADD DEVICE" in a light gray container. The form contains the following elements from top to bottom: a label "Enter Name:" above a text input field with the placeholder "Registered Name"; a label "Enter Alias:" above a text input field with the placeholder "Alternate Name"; a label "Enter IP:" above a text input field with the placeholder "IP Address"; a small dropdown menu with a downward arrow; a large blue button labeled "Add Device"; and a small gray button labeled "clear".

Figure 12 Add a Device

4.3. Add Contact

- To add a **Contact** under RTM select **ADD Contact** from the dropdown list under **Real Time Monitoring** tab.
- When clicked the following page open. Fill the required fields, select device type from the drop down list and click ADD to complete.

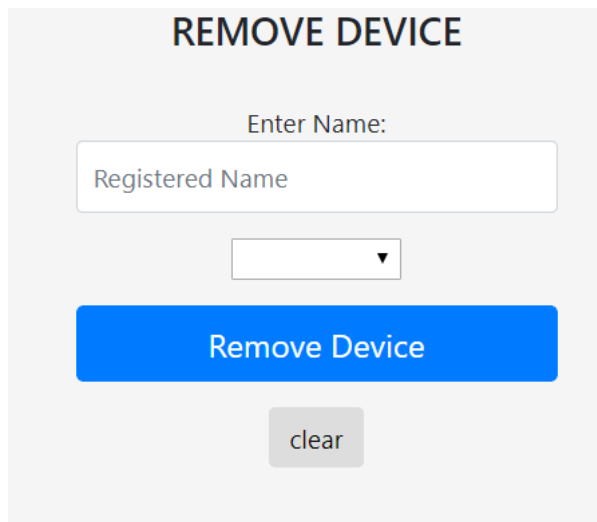


The screenshot shows a web form titled "ADD CONTACT" in a light gray box. The form contains the following elements from top to bottom: a label "Enter Name:" above a text input field with placeholder text "Registered Name"; a label "Enter Alias:" above a text input field with placeholder text "Alternate Name"; a label "Enter email:" above a text input field with placeholder text "Email Address"; a small dropdown menu with a downward arrow; a large blue button with the text "Add Contact"; and a small gray button with the text "clear".

Figure 13 Add a Contact

4.4. Remove Device

- To remove a **Device** under RTM select **Remove Device** from the dropdown list under **Real Time Monitoring** tab.
- When clicked the following page open. Fill the required fields same as the entries given when adding a Device, click Remove Device to complete



The screenshot shows a web form titled "REMOVE DEVICE". It contains a text input field labeled "Enter Name:" with the placeholder text "Registered Name". Below the input field is a dropdown menu with a downward arrow. At the bottom of the form are two buttons: a prominent blue button labeled "Remove Device" and a smaller, light gray button labeled "clear".

Figure 14 Remove a Device

5. Threat analytics (TA)

Threat Analytics collects and analyses system data looking for any suspicious activity, trigger alerts, register new clients/agents, integrated to perform vulnerability analysis. Agents are capable of reporting applications inventory data so the manager can use it to detect risks and vulnerabilities.

Select launch **Threat Analytics** to navigate to Threat Analytics dashboard

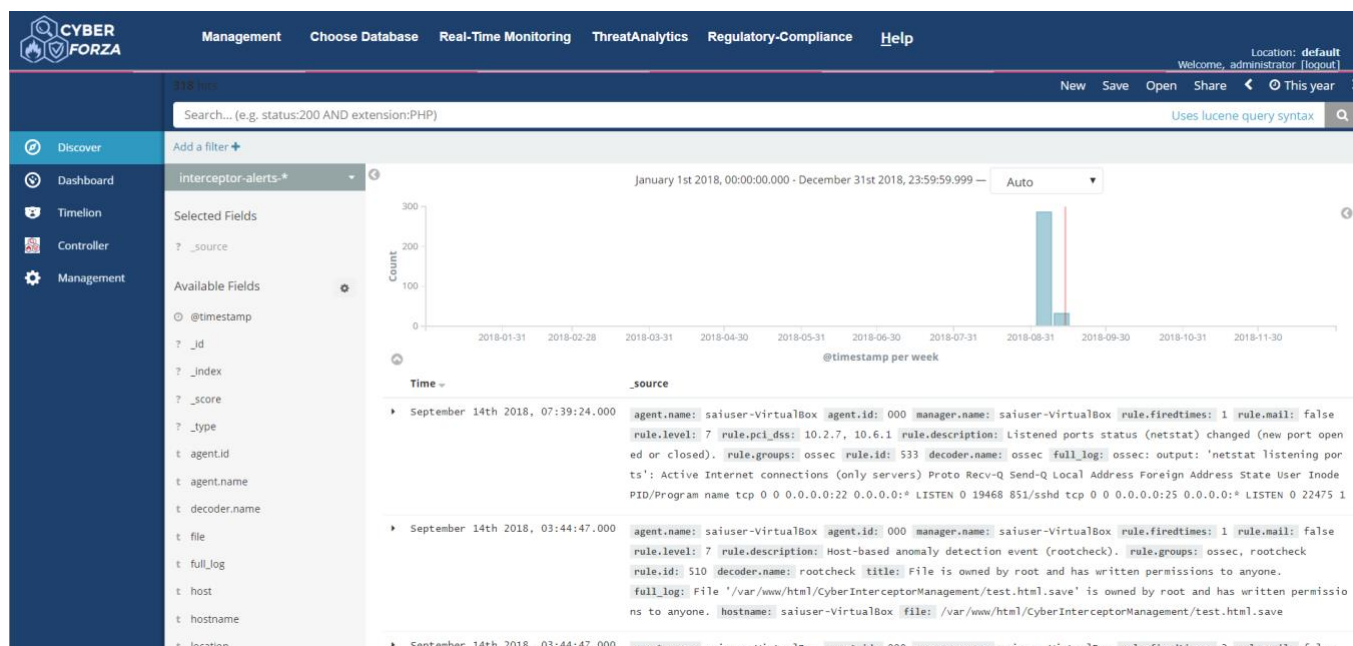
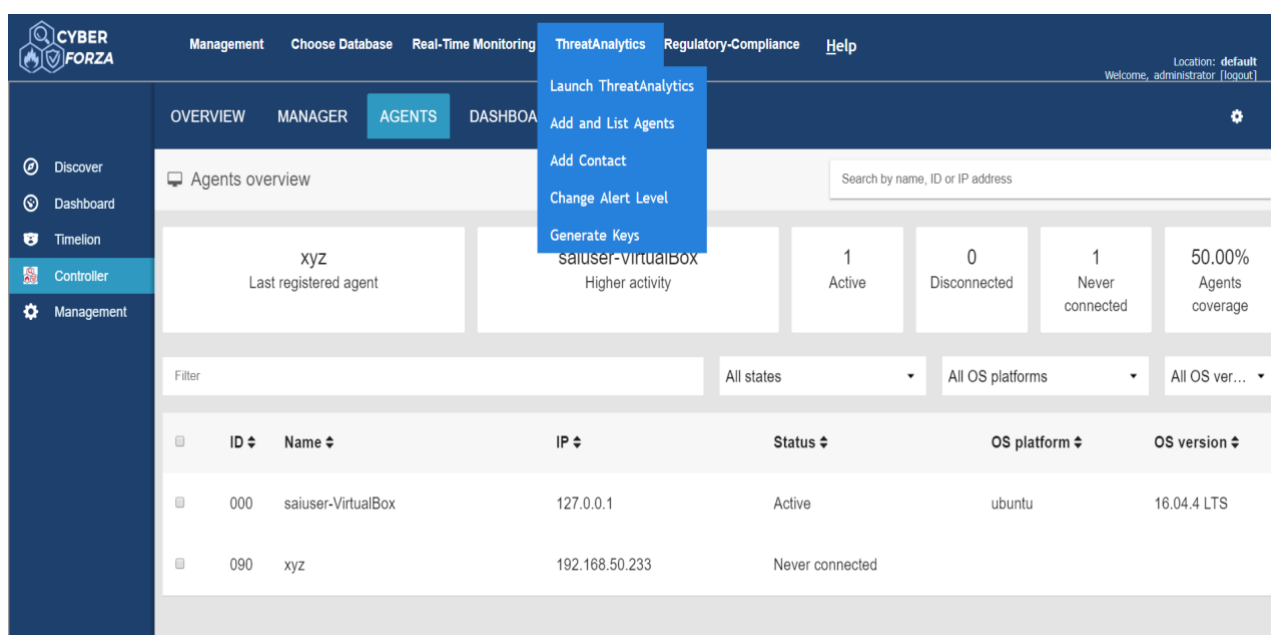


Figure 15 Threat Analytics Dashboard

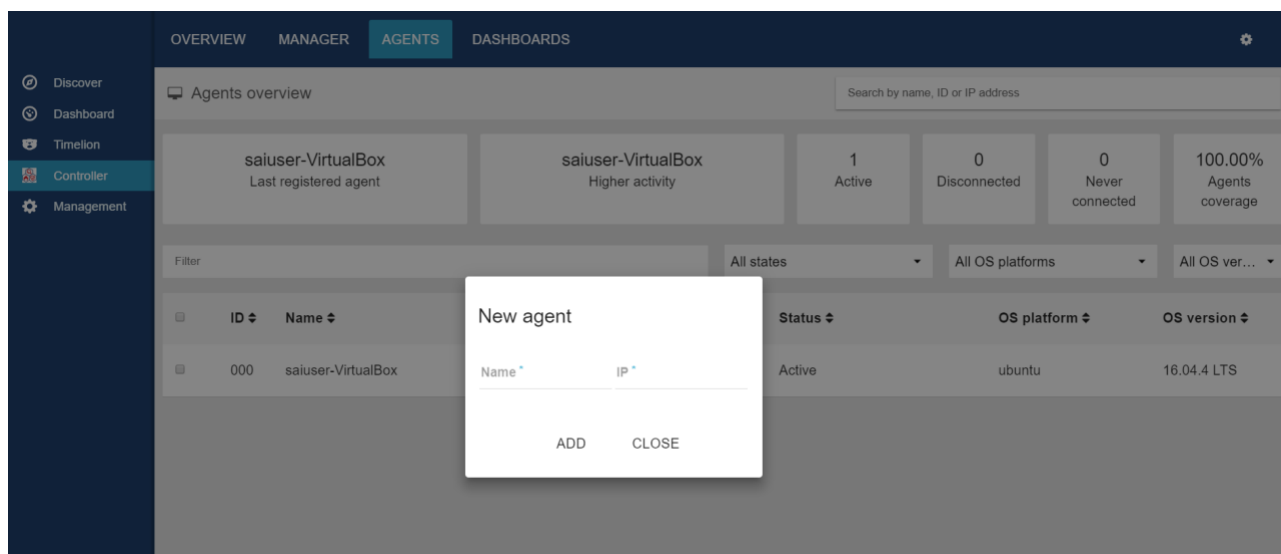
5.1. ADD Agent

To add an agent, under Threat Analytics click **ADD and List Agents**, or can also be navigated to **ADD Agent** page by clicking on **Controller** → ADD Agents on Threat Analytics Dashboard.



The screenshot shows the CYBER FORZA Threat Analytics dashboard. The 'AGENTS' tab is selected. A dropdown menu is open under 'ThreatAnalytics' with the option 'Add and List Agents' selected. The dashboard shows an 'Agents overview' section with a table of agents.

ID	Name	IP	Status	OS platform	OS version
000	saiuser-VirtualBox	127.0.0.1	Active	ubuntu	16.04.4 LTS
090	xyz	192.168.50.233	Never connected		



The screenshot shows the CYBER FORZA Threat Analytics dashboard. The 'AGENTS' tab is selected. A 'New agent' dialog box is open, allowing the user to add a new agent.

ID	Name	IP	Status	OS platform	OS version
000	saiuser-VirtualBox		Active	ubuntu	16.04.4 LTS

Figure 16 Adding an Agent

- Click on + sign at the right bottom of the page.
- Give appropriate IP and unique Name.
- Click ADD, a Key is generated.

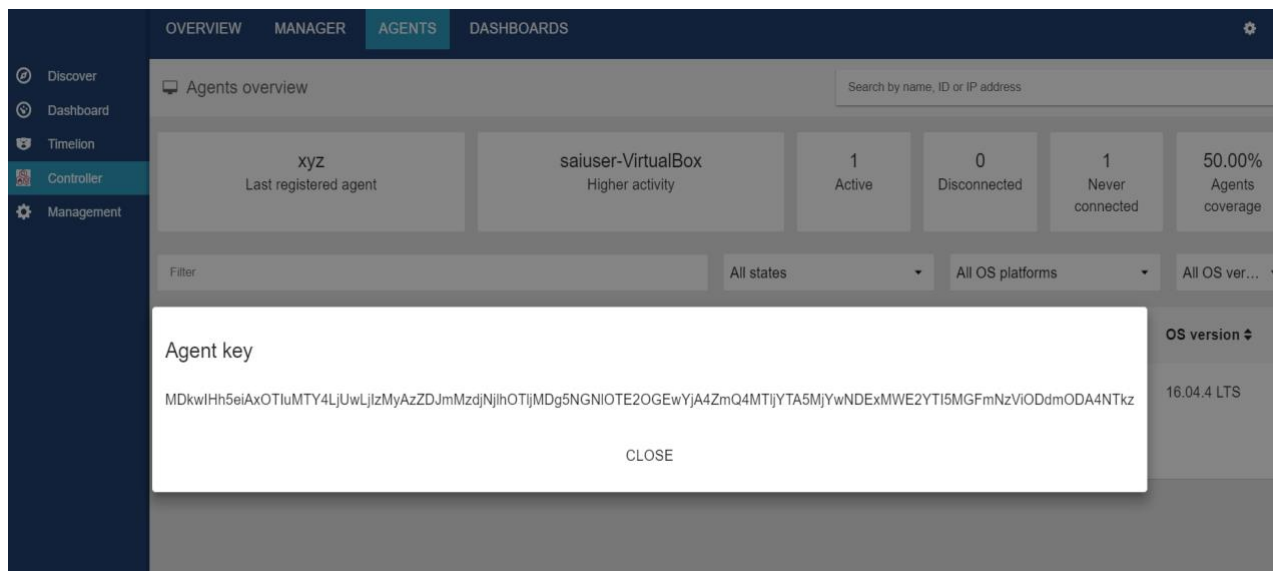


Figure 17 Key Generated

Adding the generated key on an Agent System, and to establish connection between Agent and Manager

- Go to C:\Programfiles(x86)\ossec-agent.
- Right click on win32ui and select “Run as an administrator”.
- Add Manager IP, and generated Key.
- Click on Manage and click restart and verify if the connection has been established if so, the status turns to Active on Agent list.

5.2. Multiple KEY Generation

- To add multiple agents and generate keys for the same, select Generate Keys under Threat Analytics Dropdown.
- Following page opens up. Enter name and IP address in the format Name (space) IP address.
- Click generate and multiple keys are generated in the window, it can also be downloaded as a Xcel file.

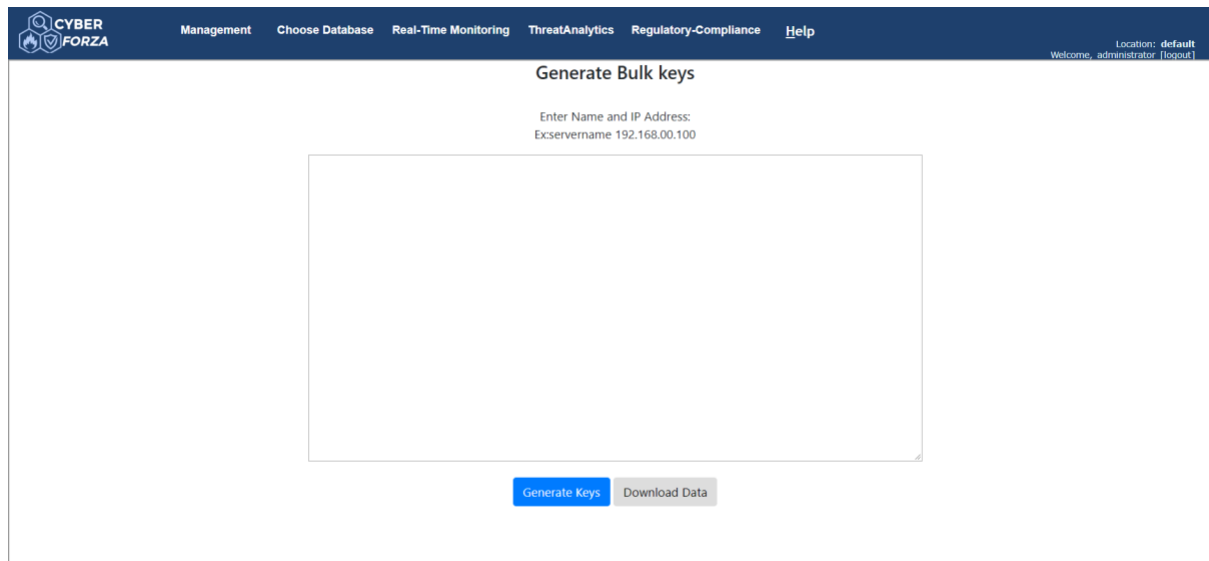


Figure 18 Multiple Key Generation

5.3. ADD Contact

To Add a Contact for Threat Analytic notifications, click on ADD Contact under Threat Analytics dropdown menu.

Enter the required email and click add contact.

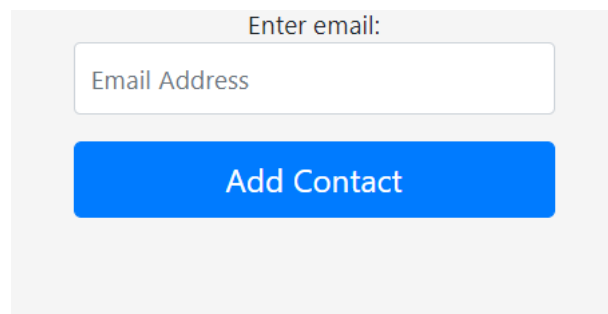
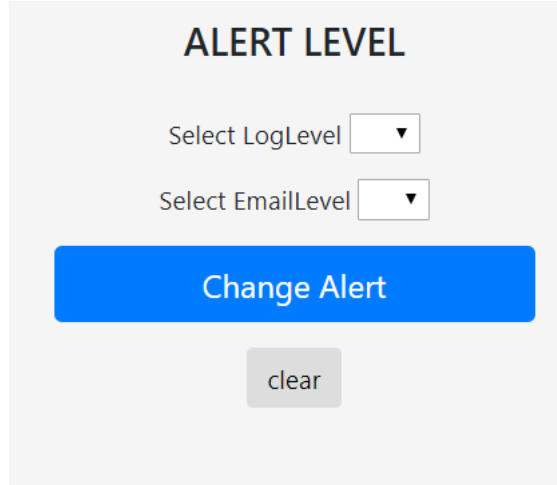


Figure 19 ADD contact

5.4. Set Alert Levels

To set Alert Levels for Logs and Emails, go to Change Alert Level under Threat Analytics dropdown menu. Set the desired level for each and click Change Alert.



ALERT LEVEL

Select LogLevel

Select EmailLevel

Change Alert

clear

Figure 20 Change Alert Level

6. Breach Detection and Malware Protection

Breach Detection has to be hyper-sensitive and lab-grade forensic. Forensic-level intrusion detection, self-learning to expose the vulnerabilities. By adopting a layered security approach, the Cyber Attacks Surface presented by information systems can be minimized. Breach Detection has to be operated within a security best practice framework and change control discipline is critical. Prevention measures are still essential and effective, but do not guarantee systems are ever 100% hack-proof. Host Intrusion Detection technology using Malware Protection, therefore performs a vital contingency function - if and when defences are breached, you are alerted and can take action before data theft and damage goes too far.



Figure 21 Breach Detection and Malware Protection Dashboard

7. Configuration Management

Automation is the key to speed, consistency and repeatability. These properties are critical to managing an infrastructure, whether it is comprised of a few servers or a few thousand servers. Configuration Management helps by automating the process of provisioning servers from bare metal, or when deploying virtual machines onto various hypervisors.

Configuration Management provides Package Management, Network Management, Application Management and Infrastructure Management.

8. Regulatory Compliance

CISS Interceptor provides continuous tracking of compliance and if anything changes immediately: real-time, dynamic compliance. All major security standards are covered and built-in and multiple standards can be assessed simultaneously. Generates audit control reports. CISS-Interceptor provides compliance for PCI-DSS, HIPAA, SOX, FISMA, CIS, CUI, CDI, GRC, GDPR, NIST framework, FISCAM - Federal Information System Controls Audit Manual.

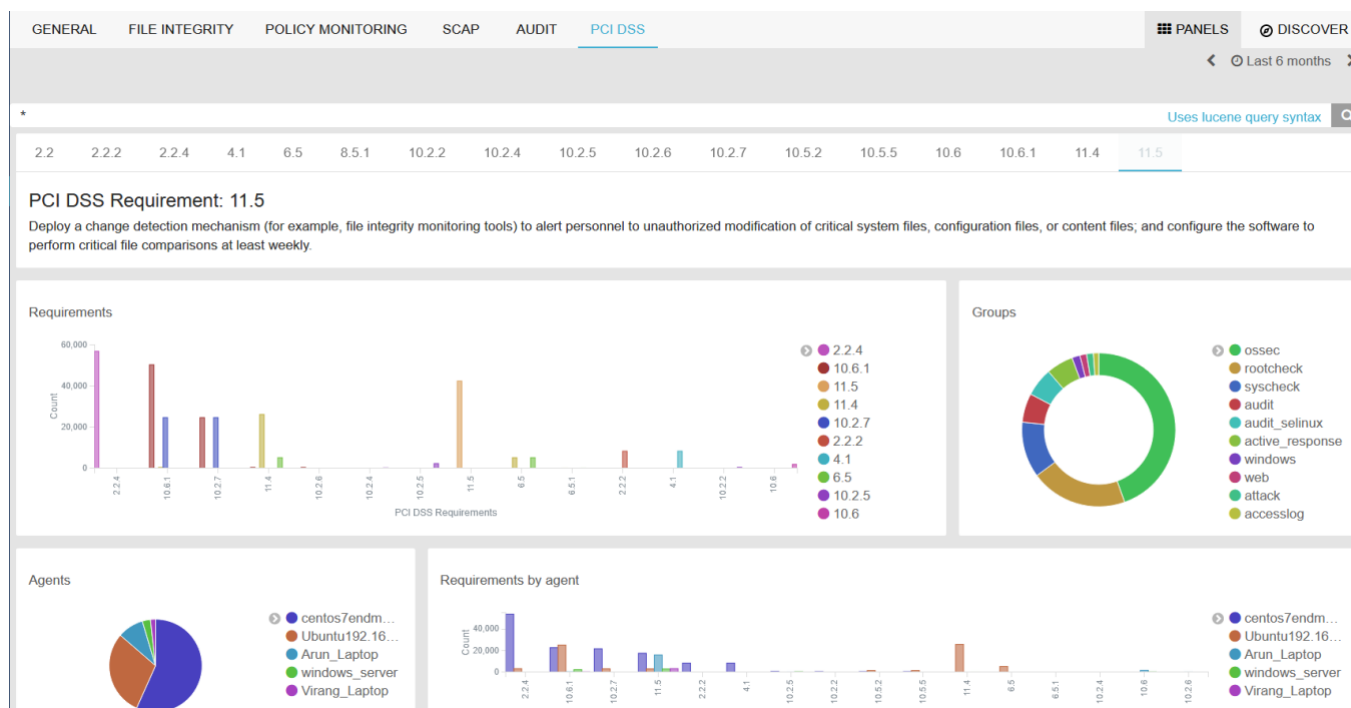


Figure 22 Regulatory Compliance Dashboard