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

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

List of Figures

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

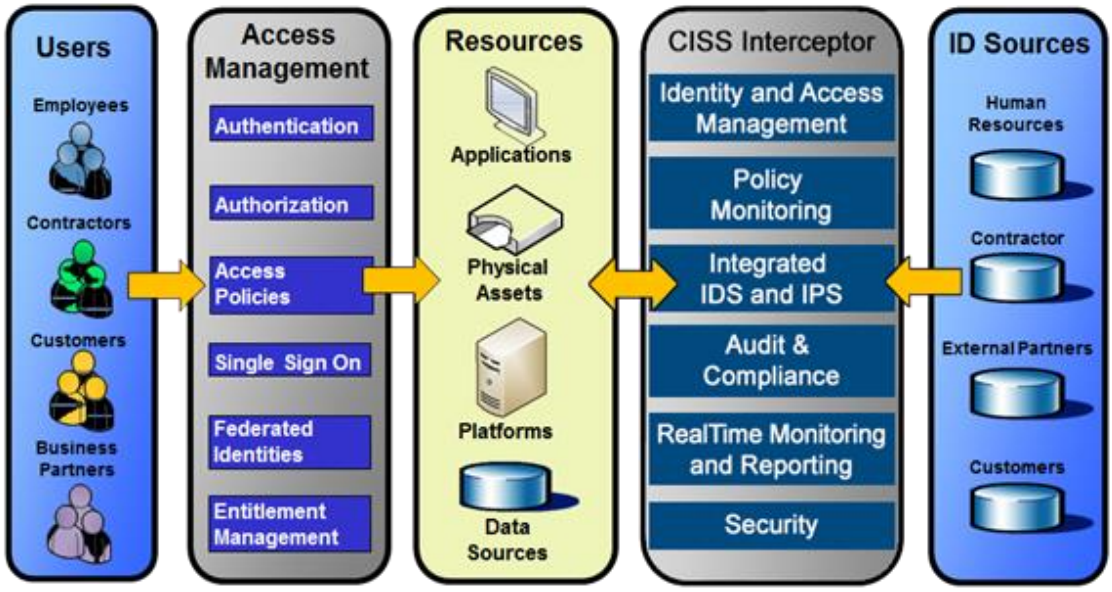


Figure 1 CISS Interceptor Data Flow Diagram

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**

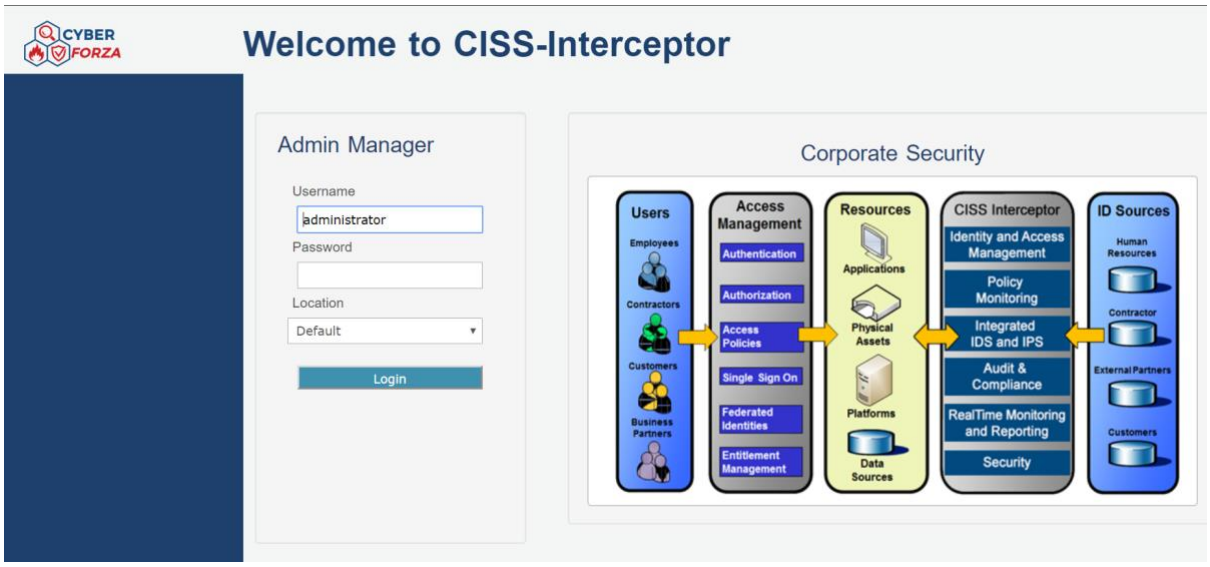


Figure 2 CISS-Interceptor Login Page

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

2.5. Dashboard

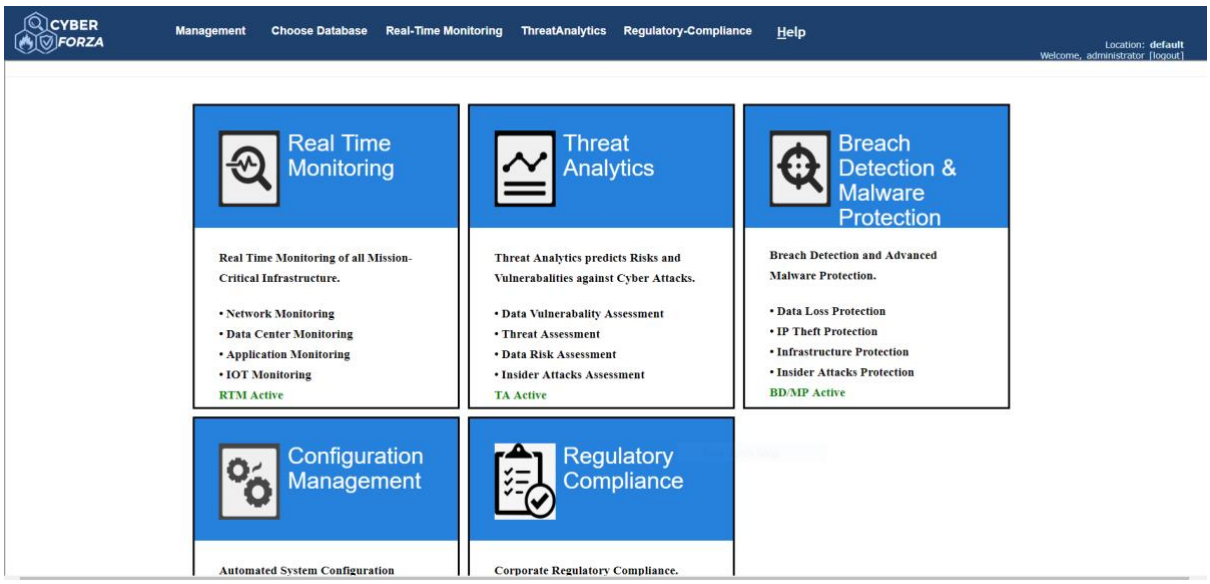
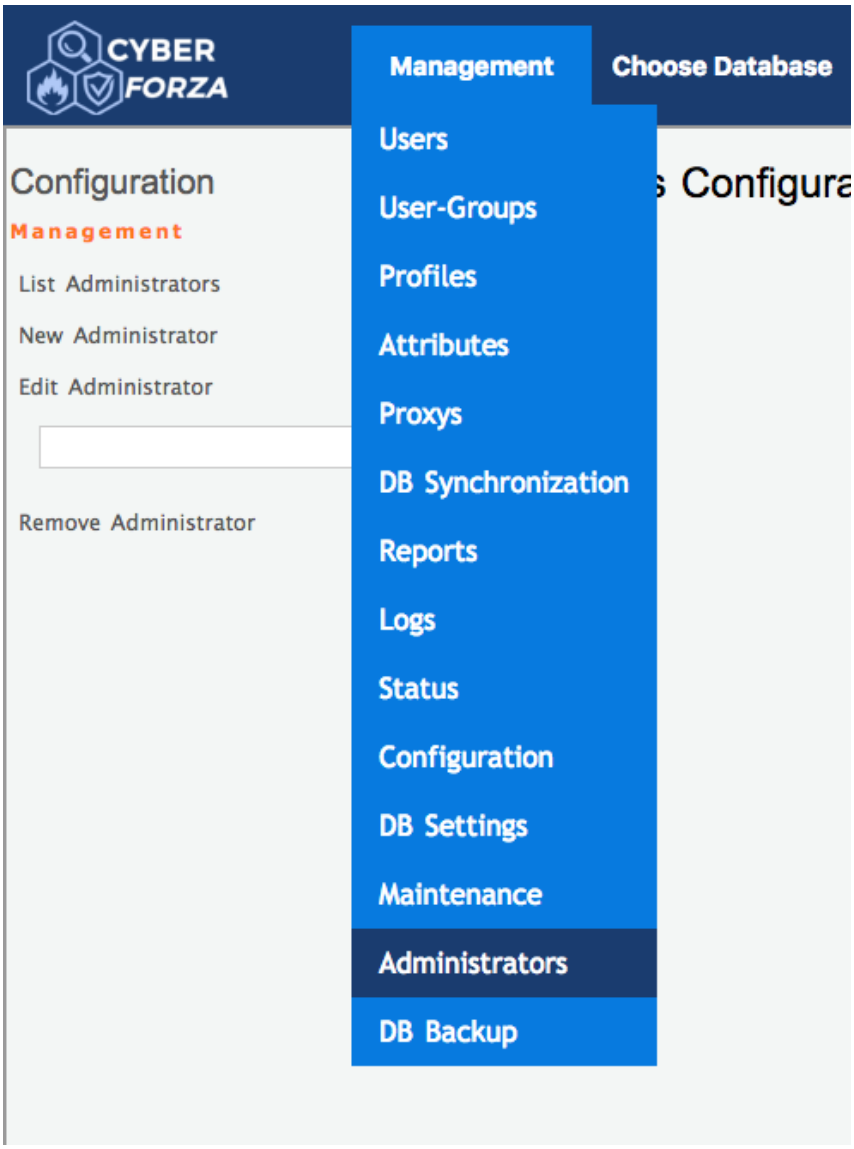


Figure 3 CISS-Interceptor Dashboard

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**



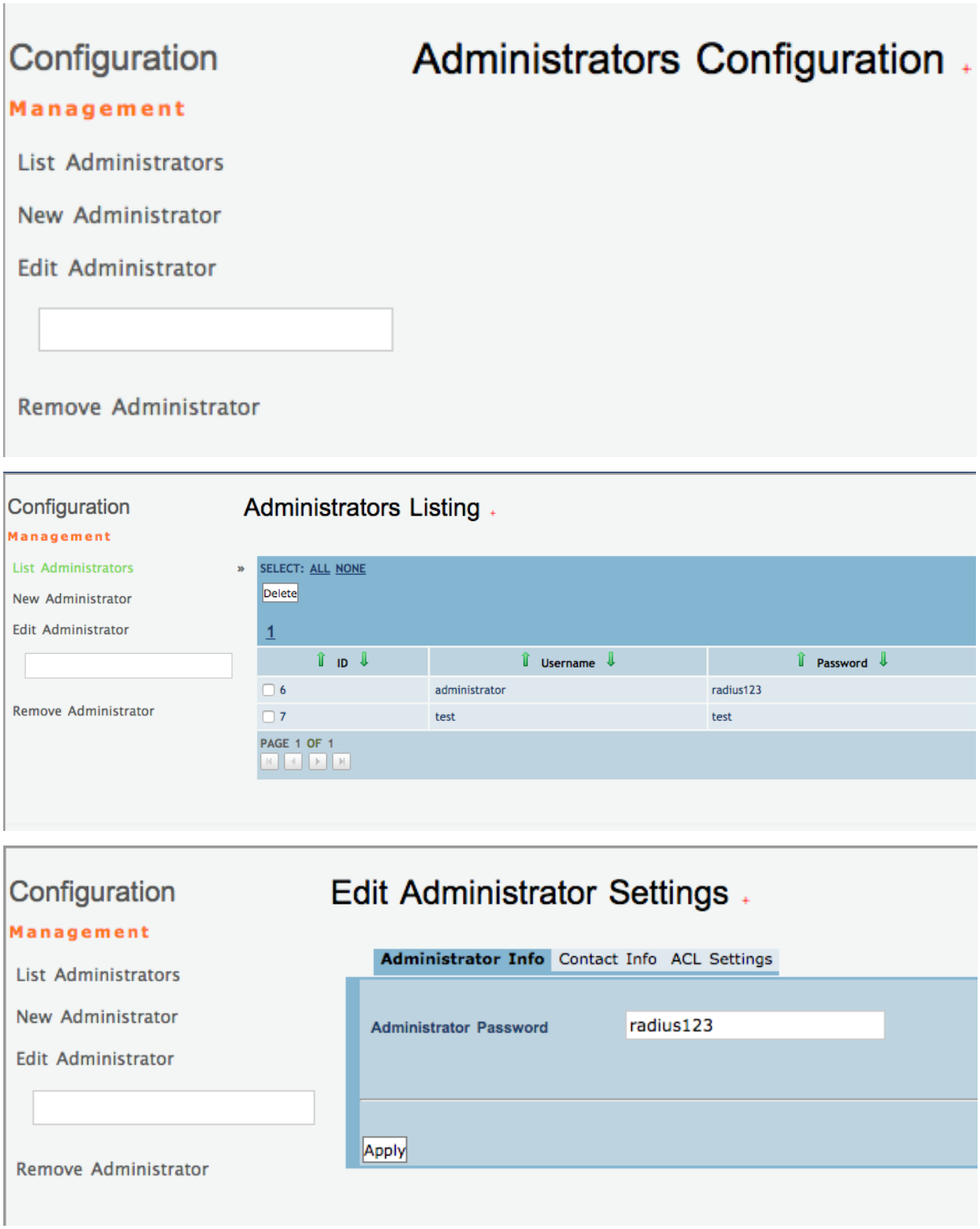


Figure 2 Change Administrator Password

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

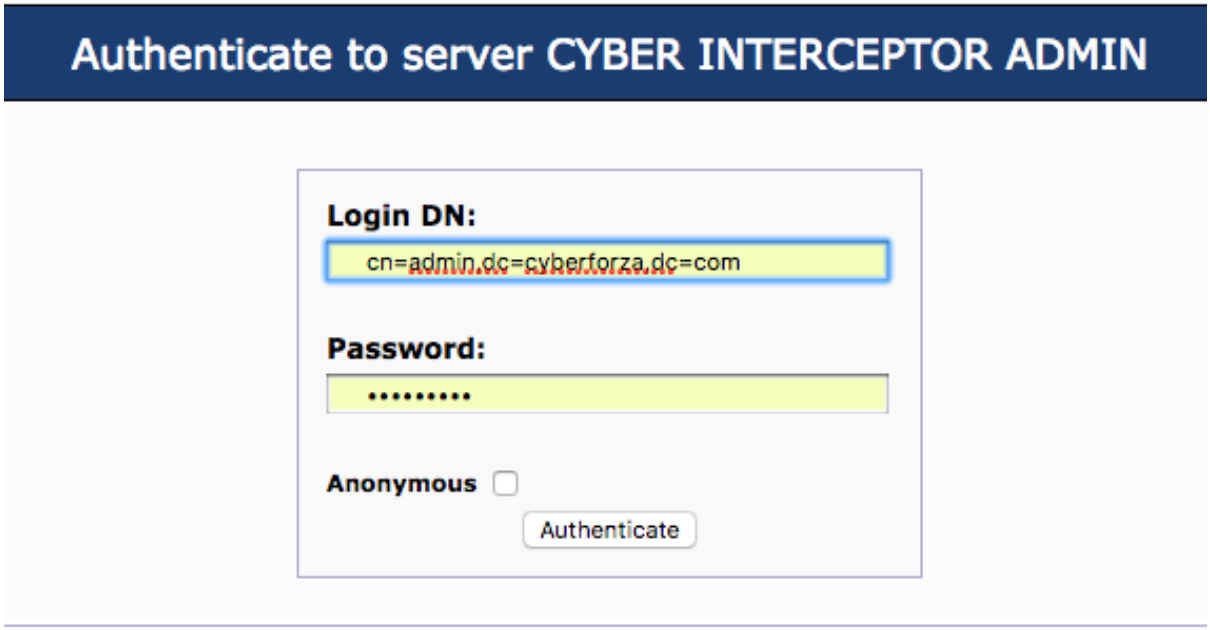


Figure 3 LDAP Login Page

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

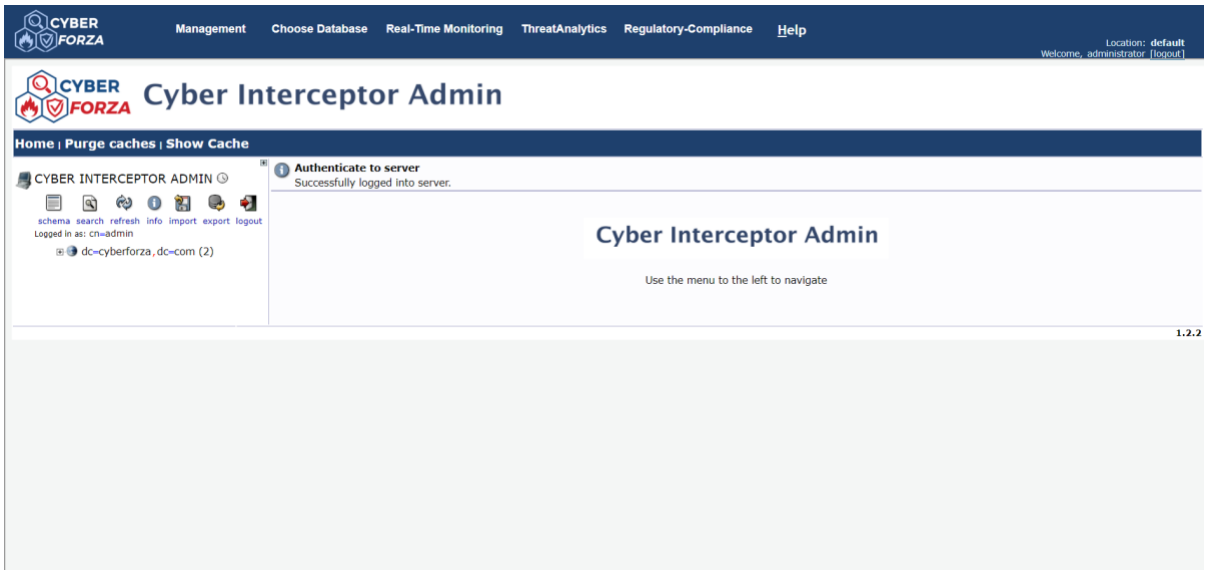
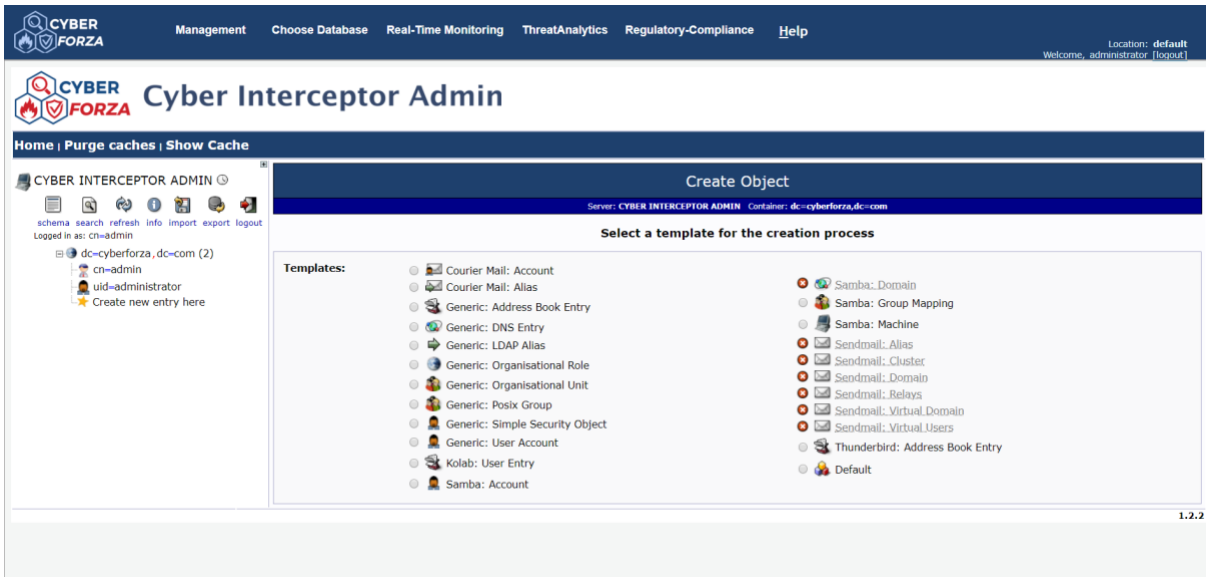


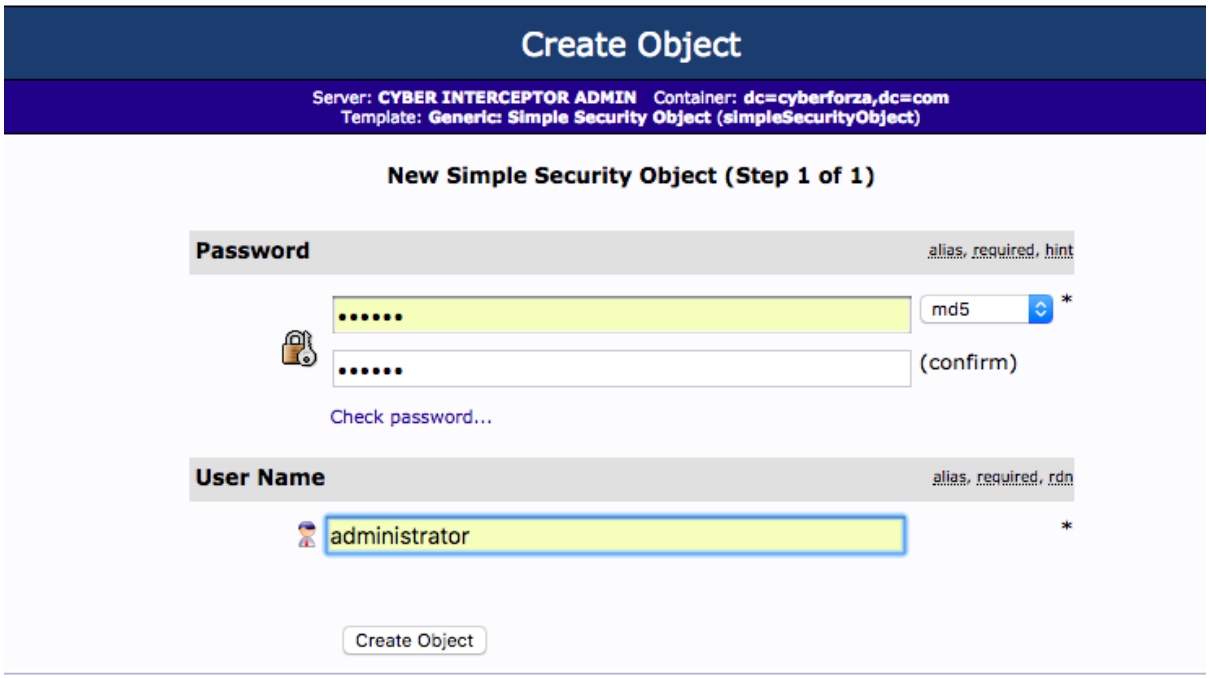
Figure 4 LDAP Dashboard

- 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.





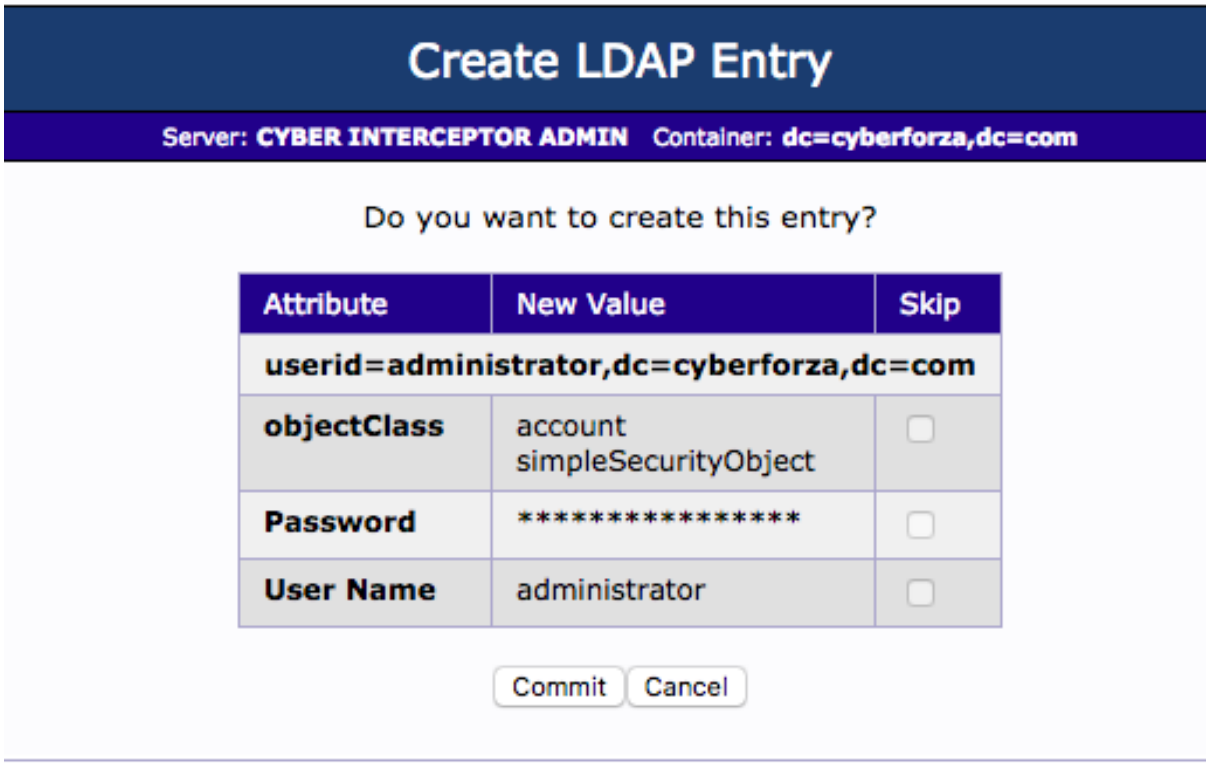


Figure 5 LDAP Create Object

3.2. Radius Database

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

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.

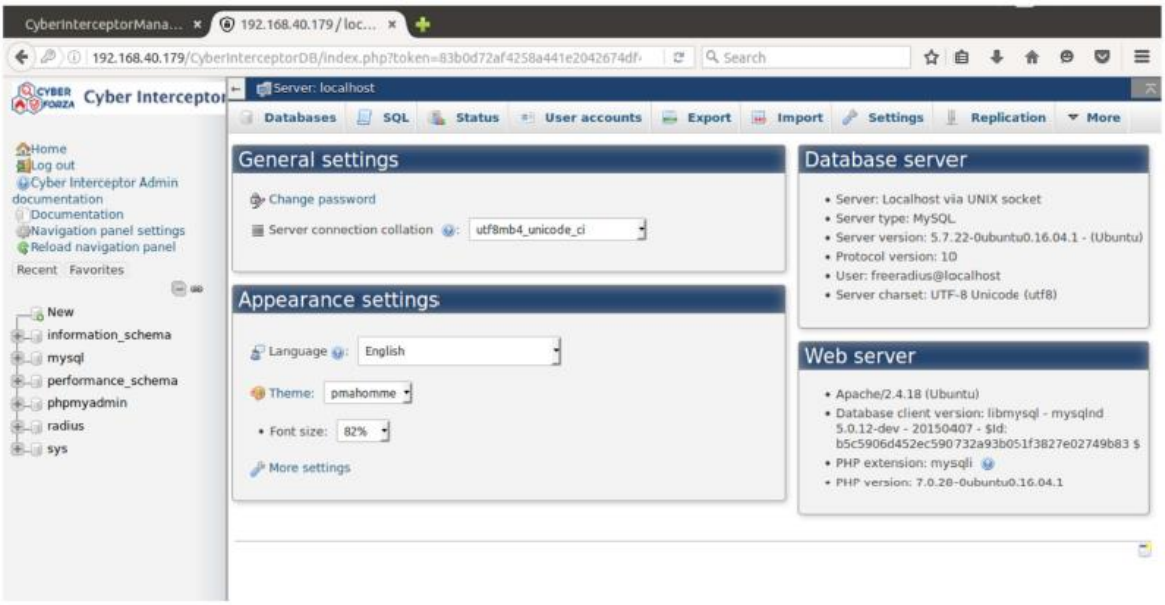


Figure 7 Radius Database Dashboard

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**

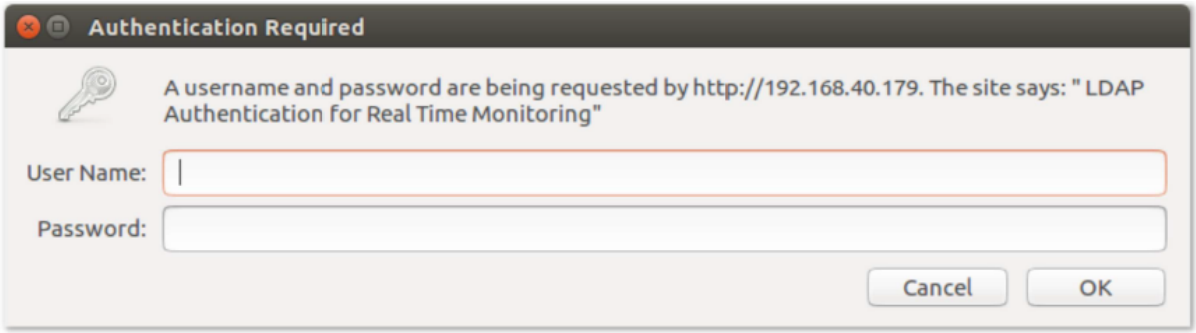


Figure 8 Real Time Monitoring Login Page

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

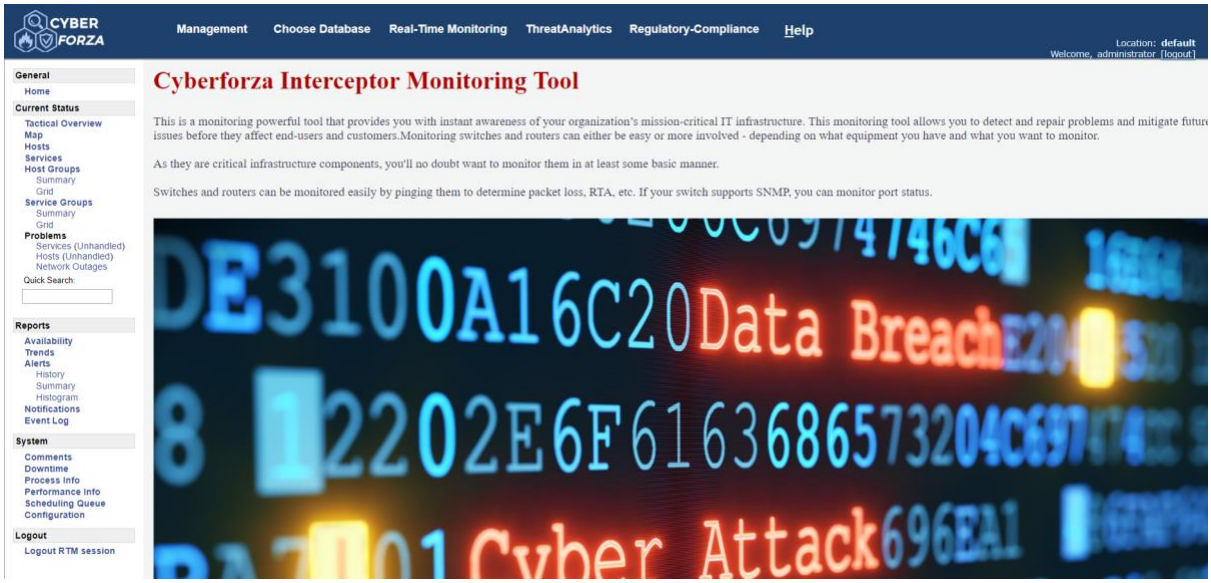


Figure 9 Real-Time Monitoring Dashboard

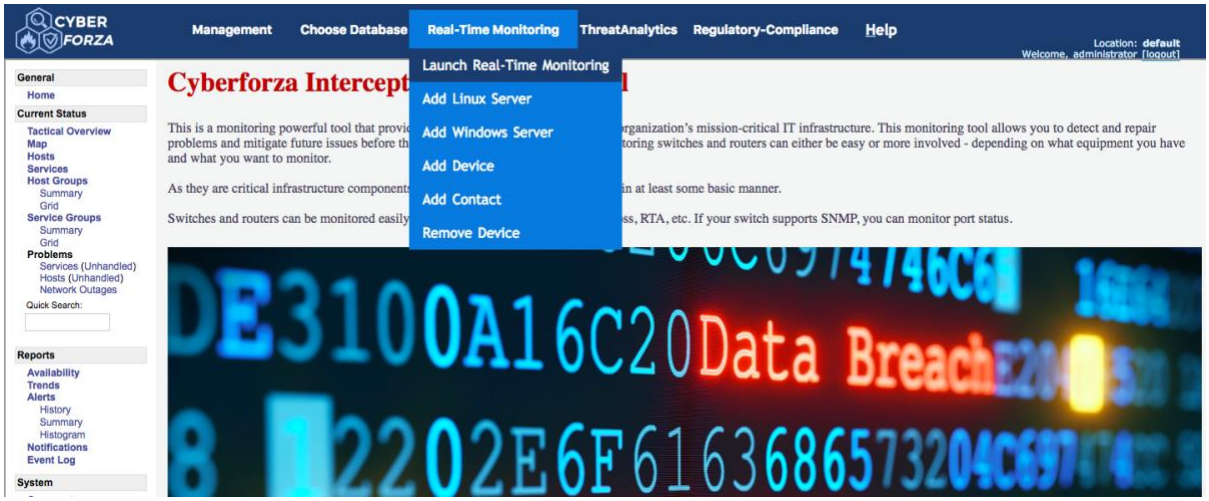
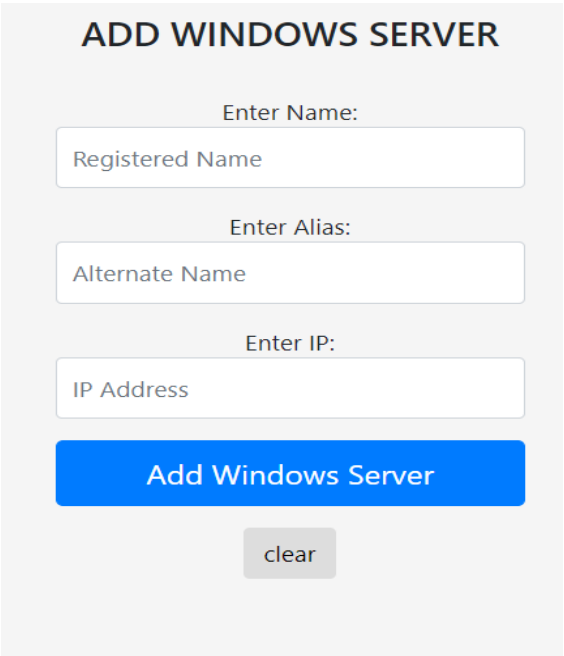


Figure 10 RTM Dropdown List

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.



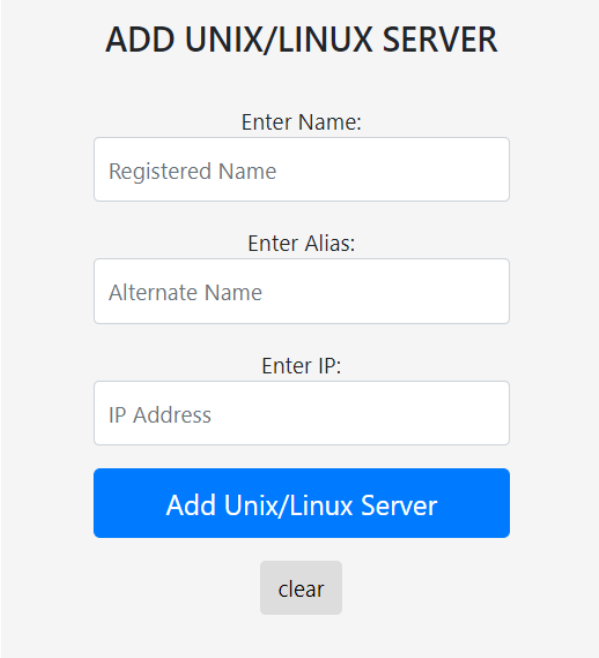


Figure 11 Add Windows or Linux Server

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.

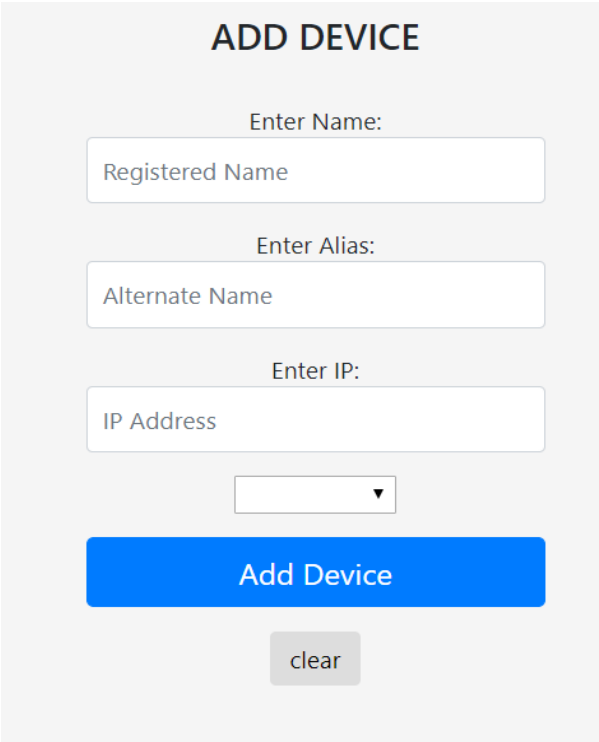


Figure 12 Add a Device

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.

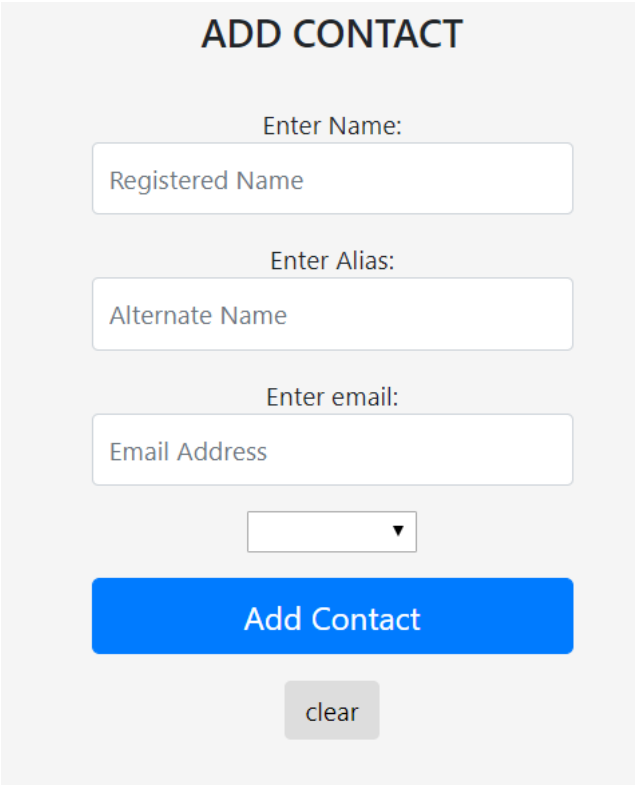


Figure 13 Add a Contact

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

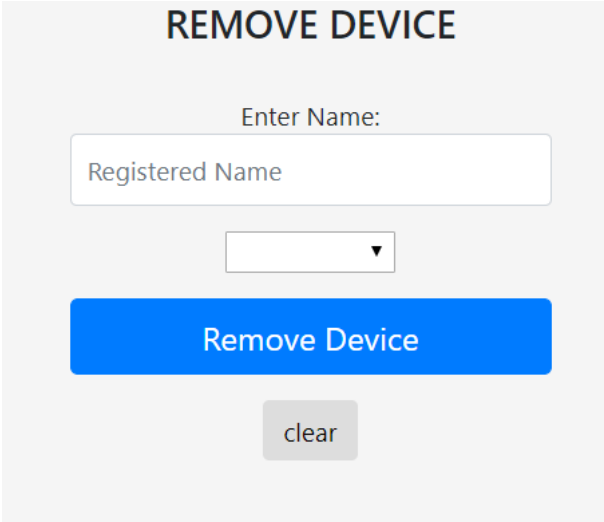


Figure 14 Remove a Device

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

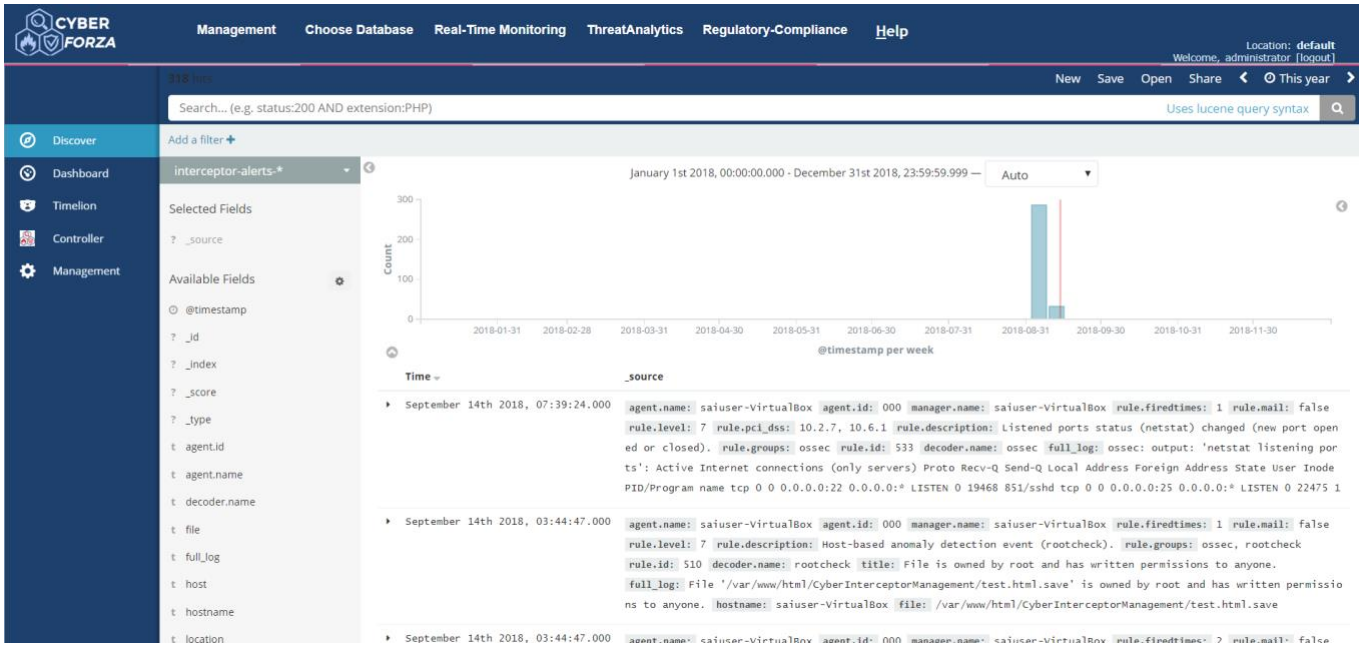
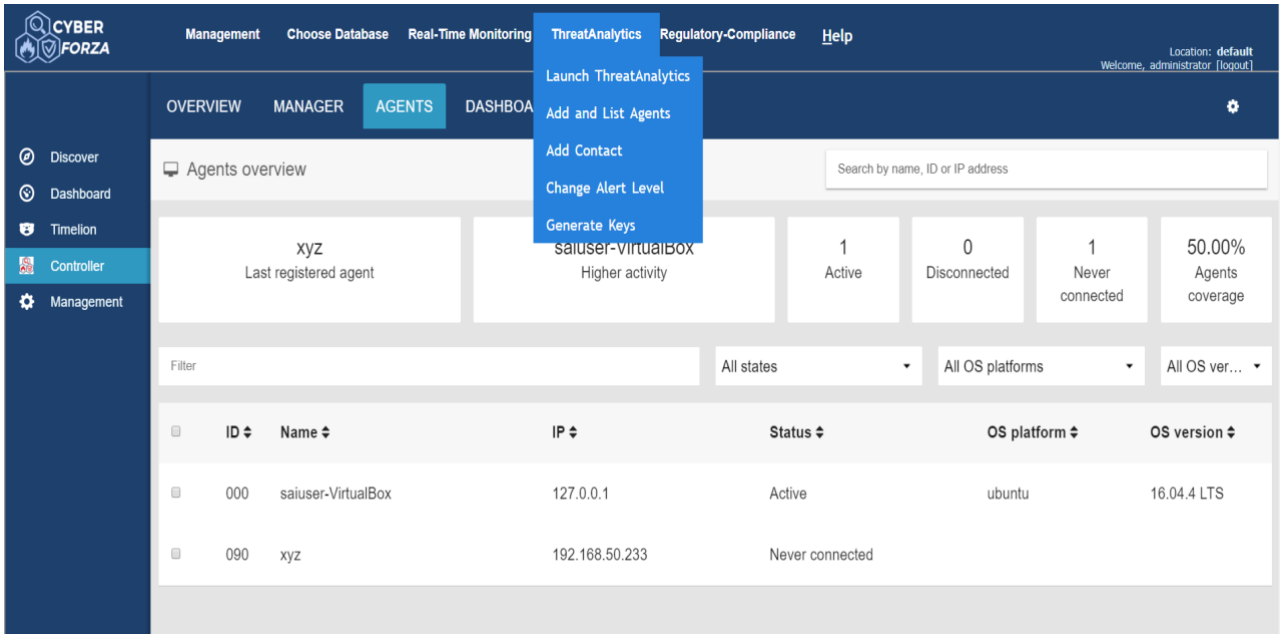


Figure 15 Threat Analytics Dashboard

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.



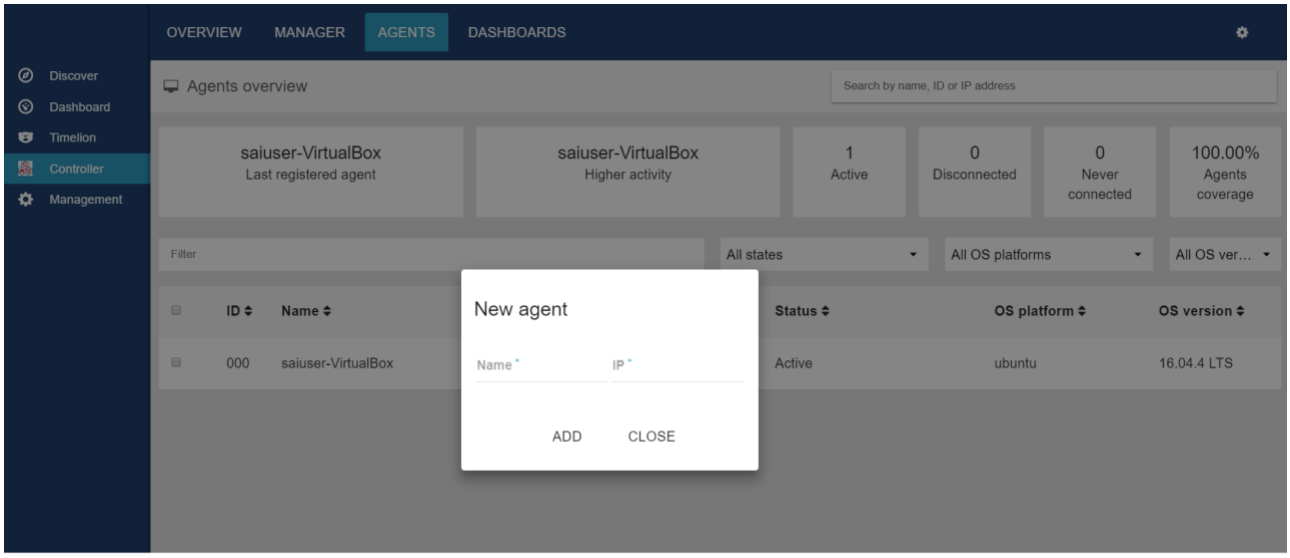


Figure 16 Adding an Agent

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

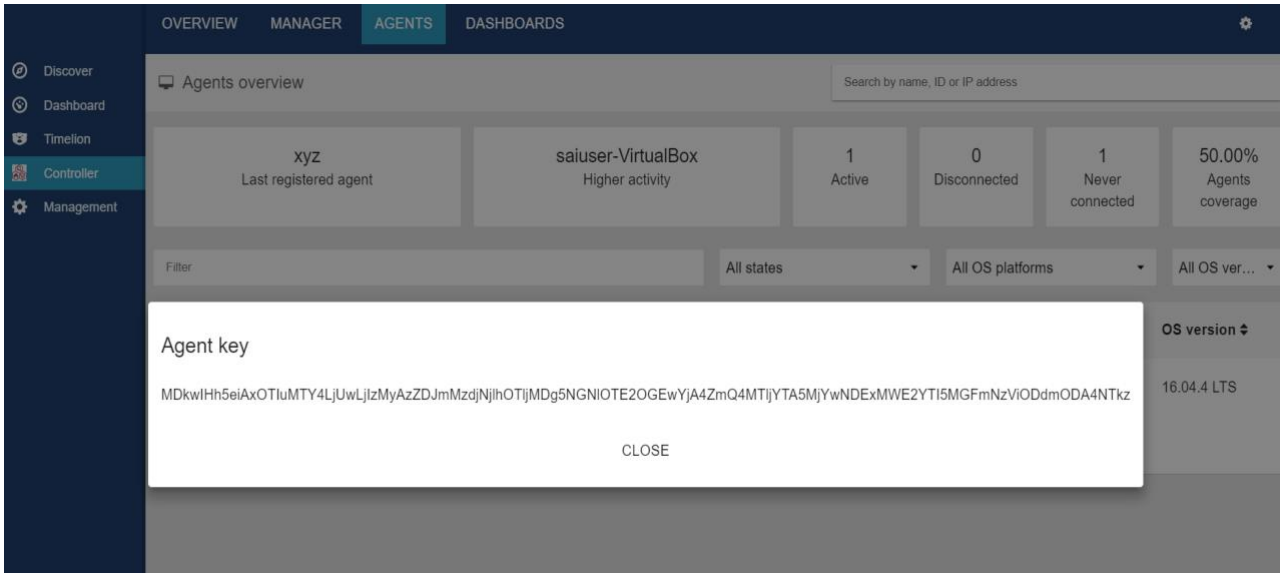


Figure 17 Key Generated

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.

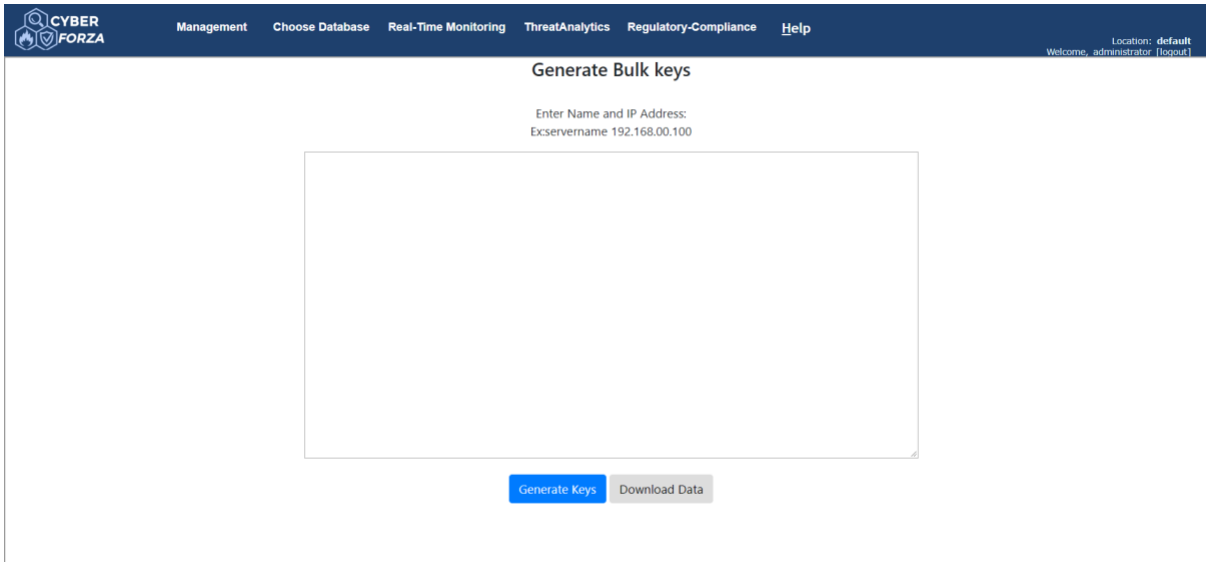


Figure 18 Multiple Key Generation

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.

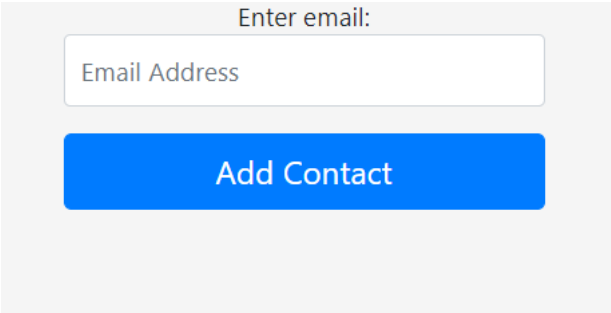


Figure 19 ADD contact

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.

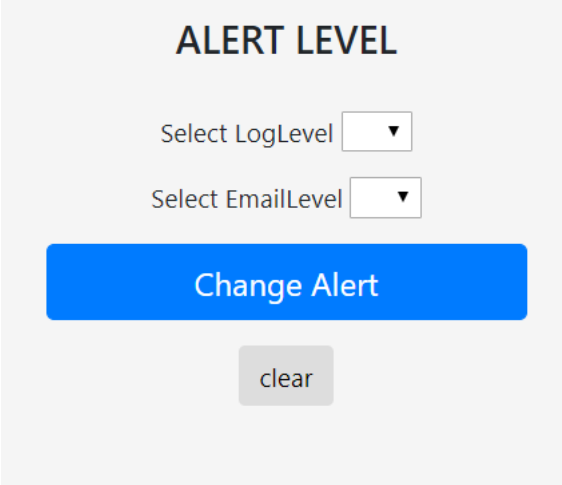


Figure 20 Change Alert Level

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.


March 18th 2018, 16:52:30.221 - September 18th 2018, 16:52:30.221 — Auto

```
May 10th 2018, 17:46:29.000   full_log: Windows Malware: Anti-virus site on the hosts file. File: C:\Windows\System32\Drivers\etc\HOST
                              S. agent.name: windows_server agent.id: 036 agent.ip: 192.168.50.124 manager.name: centos7endmc19
                              rule.firedtimes: 1 rule.mail: false rule.level: 9 rule.description: Windows malware detected.
                              rule.groups: ossec, rootcheck rule.id: 513 decoder.name: rootcheck title: Windows Malware: Anti-virus
                              site on the hosts file. path: /var/ossec/logs/alerts/alerts.json @timestamp: May 10th 2018, 17:46:29.00

May 10th 2018, 17:46:29.000   full_log: Windows Malware: Anti-virus site on the hosts file. File: C:\Windows\System32\Drivers\etc\HOST
                              S. agent.name: windows_server agent.id: 036 agent.ip: 192.168.50.124 manager.name: centos7endmc19
                              rule.firedtimes: 1 rule.mail: false rule.level: 9 rule.description: Windows malware detected.
                              rule.groups: ossec, rootcheck rule.id: 513 decoder.name: rootcheck title: Windows Malware: Anti-virus
                              site on the hosts file. path: /var/ossec/logs/alerts/alerts.json @timestamp: May 10th 2018, 17:46:29.00

May 10th 2018, 17:46:29.000   full_log: Windows Malware: Anti-virus site on the hosts file. File: C:\Windows\System32\Drivers\etc\HOST
                              S. agent.name: windows_server agent.id: 036 agent.ip: 192.168.50.124 manager.name: centos7endmc19
                              rule.firedtimes: 1 rule.mail: false rule.level: 9 rule.description: Windows malware detected.
                              rule.groups: ossec, rootcheck rule.id: 513 decoder.name: rootcheck title: Windows Malware: Anti-virus
                              site on the hosts file. path: /var/ossec/logs/alerts/alerts.json @timestamp: May 10th 2018, 17:46:29.00
```

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.

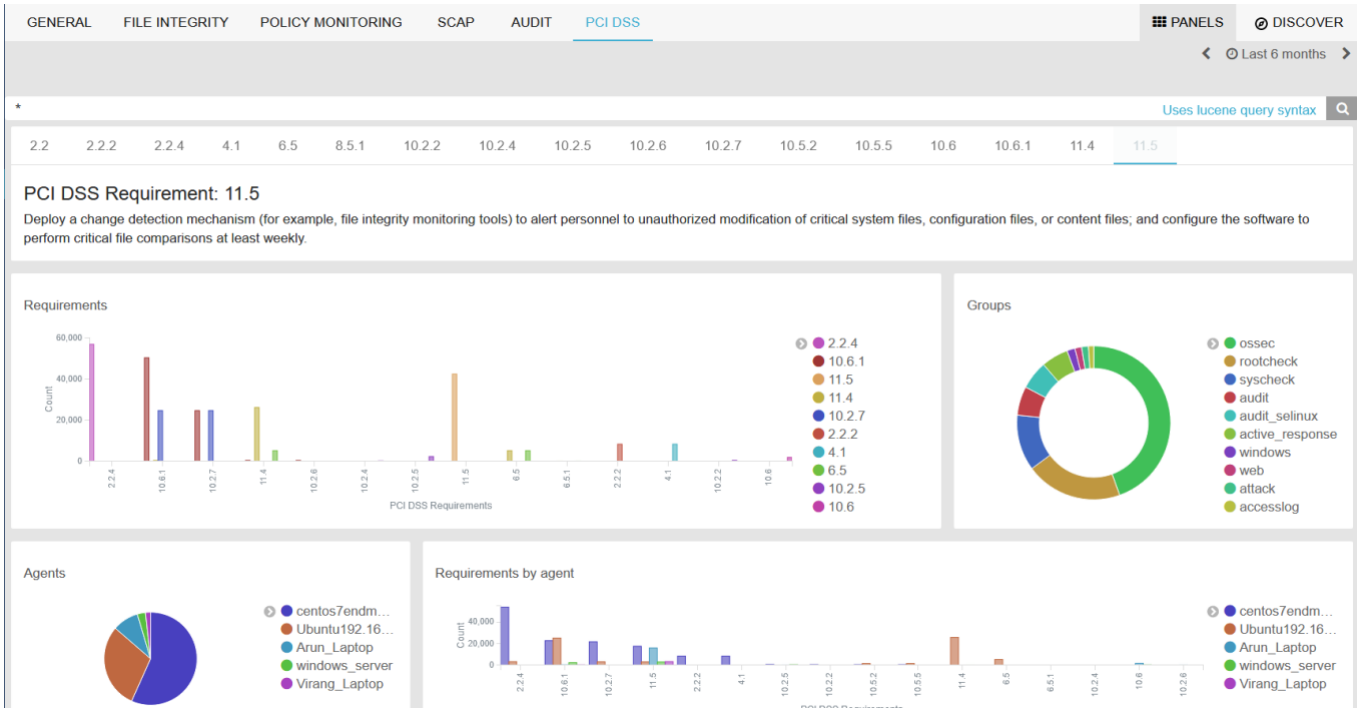


Figure 22 Regulatory Compliance Dashboard