# REPORT - INT 301

# Open Source Technologies

**B.Tech. CSE**

**Submitted to - Rajeshwar Sharma Sir**


LOVELY PROFESSIONAL UNIVERSITY

**PROJECT- Using desired Open Source Software trace API calls and behavior of files; give detailed reports; analyze malicious files. Start UniFi Network Controller / Network Application and upgrade/update automatically.**

**Submitted by-**

**1. Sanjay Singh**

*Department of Computer science and engineering LPU*

*** GITHUB-Repository -**
**https://github.com/Sanjay0Singh/INT301**

# 1.Introduction -

## 1.1 Objective of the project

- **Using desired open source software, Here we are going to use Sysinternals.**
- **Trace API calls.**
- **Analyze behaviour of files .**
- **Analyze malicious files.**
- **Start the UniFi Network Controller and upgrade/update it automatically using Sysinternals.**
- **To upload the report to the GITHUB-Repository.**

## 1.2 Description of the project

**The goal of this project is to use Sysinternals(desired open source software) to trace API calls and behavior of files, and to analyze potentially malicious files. Sysinternals is a suite of advanced system utilities and tools for Windows, developed by Microsoft. The main tool used in this project is Process Monitor, which can monitor and trace the activities of running processes, including their file and registry access.**

**Sysinternals is a suite of advanced system utilities and tools for Windows, including Process Monitor, which can be used to monitor and trace the activities of running processes, including the UniFi Network Controller.**

**Sysinternals tools are powerful and can have an impact on system performance if not used carefully. When monitoring processes with Process Monitor, it's important to set specific filters to avoid capturing unnecessary data, and to stop capturing events when you're done monitoring to minimize the impact on system resources.**

### 1.2 Scope of the project

**The scope of the project is focused on using Sysinternals tools to trace API calls and behavior of files, and to analyze potentially malicious files, with the goal of troubleshooting issues or diagnosing problems, or identifying and removing malware from a system.**

# 2.SYSTEM DESCRIPTION -

### 2.1 Target system description

**The target system should be capable of running the necessary software tools and utilities required to trace API calls and behavior of files, and to analyze potentially malicious files, with the goal of troubleshooting issues, diagnosing problems, or identifying and removing malware from the system.**

**The target system should have the following software tools installed:**

1. **Microsoft Windows operating system, version 7 or later.**
2. **Sysinternals suite of advanced system utilities and tools, available for download from the Microsoft website.**

### 2.2 Assumptions and dependencies

- **The project assumes that the user has basic knowledge of using open source software like Sysinternals suite.**
- **The project depends on the Sysinternals suite to trace API calls and analyze the behaviour of files.**

- **The project assumes that the user has a stable internet connection to download and install the Sysinternals suite.**

## 2.3 Functional dependencies

- **The Sysinternals suite must be downloaded and installed on the target system to enable the use of Process Monitor and other system utilities.**
- **The target system must have administrative privileges to allow for the installation and configuration of software tools and utilities.**
- **The target system must have a web browser installed to access online resources related to the project.**
- **The user must have the necessary permissions and legal authority to analyze potentially malicious files on the target system.**

## 2.4 Non-Functional dependencies

- **The performance of the target system may affect the efficiency of the Sysinternals tools and utilities, especially when monitoring resource-intensive processes or large files.**
- **The accuracy of the output from Sysinternals tools and utilities may depend on the configuration and filters set by the user, and the context in which the monitoring is performed.**
- **The legal and ethical considerations related to the analysis of potentially malicious files may vary depending on the jurisdiction and specific use case.**
- **The compatibility of the target system with the Sysinternals suite and other software tools may depend on the specific hardware and software configurations of the system.**

# 3.Analysis Report-

## STEP 1: Download and install Sysinternals Process Monitor from the Microsoft website.

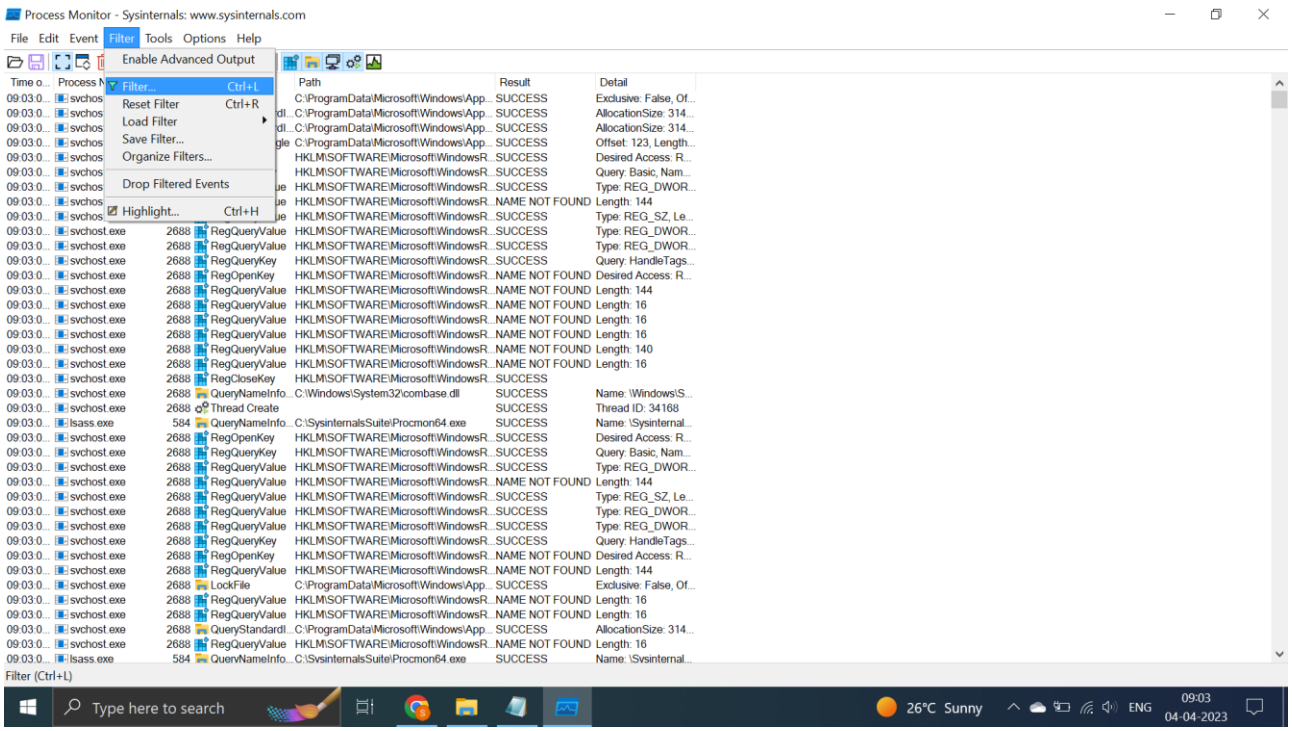
**The Sysinternals suite is a collection of more than 70 free Windows system utilities developed by Microsoft. These tools can be used to monitor and troubleshoot Windows-based systems, as well as to diagnose and remove malware.**

### Some of the benefits of using Sysinternals suite include:

- **Process Monitor - A tool that shows real-time file system, registry, and process/thread activity.**
- **Process Explorer - A tool that displays information about running processes, including DLLs, network connections, and threads.**
- **Autoruns - A tool that shows all the programs and services that are configured to start automatically when the system boots up.**
- **TCPView - A tool that shows all active TCP and UDP endpoints on a system.**
- **Sysmon - A tool that monitors and logs system activity to detect and respond to malicious activity.**
- **PsExec - A tool that allows administrators to execute processes on remote systems.**
- **Disk Usage - A tool that shows the disk space usage for a specified directory.**

**The Sysinternals suite is widely used by IT professionals and security researchers to diagnose and troubleshoot issues, as well as to identify and remove malware. The tools in the suite are easy to use and provide detailed information about system activity, making them an essential resource for any Windows administrator or security analyst.**

## STEP 2: Launch Process Monitor and click on the "Filter" menu.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Enable Advanced Output
Filter... Ctrl+L
Reset Filter Ctrl+R
Load Filter
Save Filter...
Organize Filters...
Drop Filtered Events
Highlight... Ctrl+H
Time o... Process N... PID Operation Path Result Detail
Filter (Ctrl+L)
Type here to search
26°C Sunny
ENG
09:03
04-04-2023

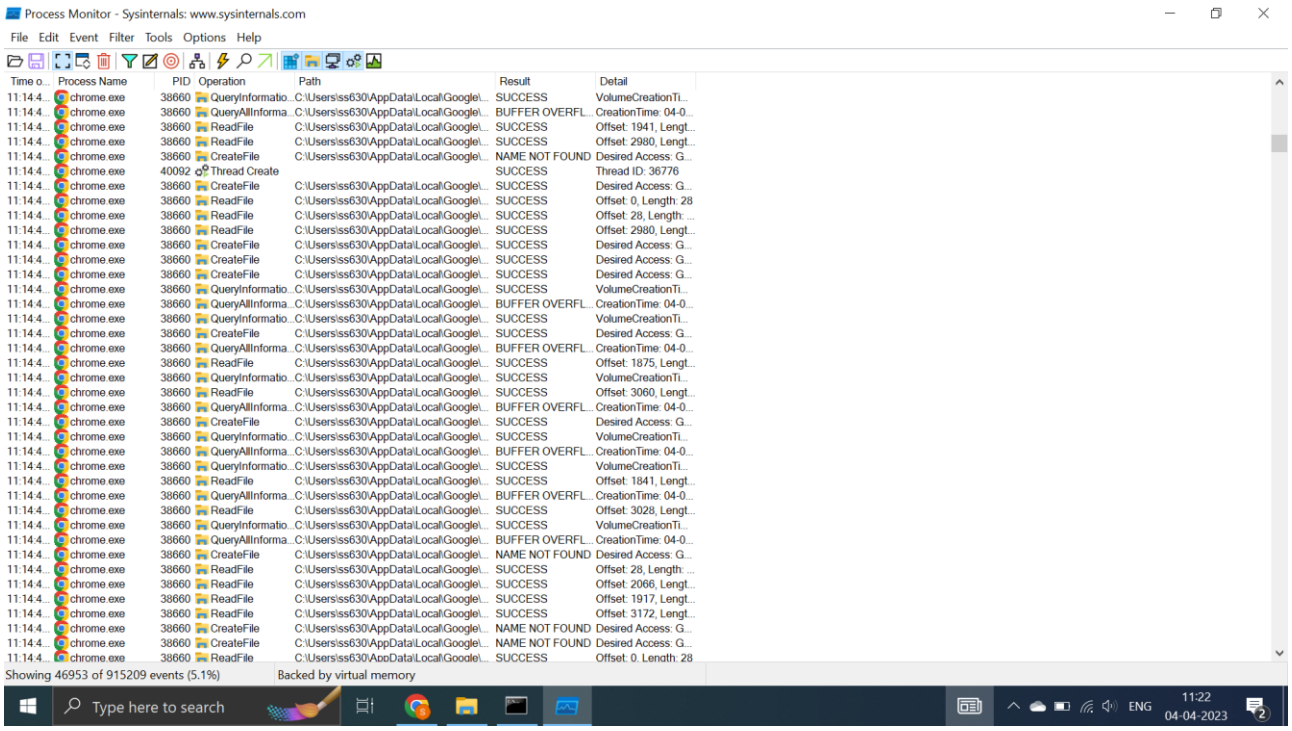
**STEP 3: Choose "Filter..." from the drop-down menu to open the filter settings.**

**STEP 4: In the "Process Monitor Filter" dialog box, select the "Process Name" filter.**

**STEP 5:In the "Process Name" field, type the name of the process you want to monitor, such as "chrome.exe".**

**STEP 6: Click "Add" to add the filter to the list. Click "OK" to save the filter settings and close the dialog box.**

**STEP 7: The Process Monitor window will now only show activity related to the specified process.**




**STEP 8: To filter the events to only show API calls, click on the "Filter" button in the toolbar and select "Filter..." from the drop-down menu.**

**STEP 9:In the "Process Monitor Filter" dialog box, select the "Operation" filter.In the "Operation" field, type the name of the API call you want to monitor, such as "RegQueryValue" for registry queries.**

**STEP 10: Click "Add" to add the filter to the list.Click "OK" to save the filter settings and close the dialog box.**

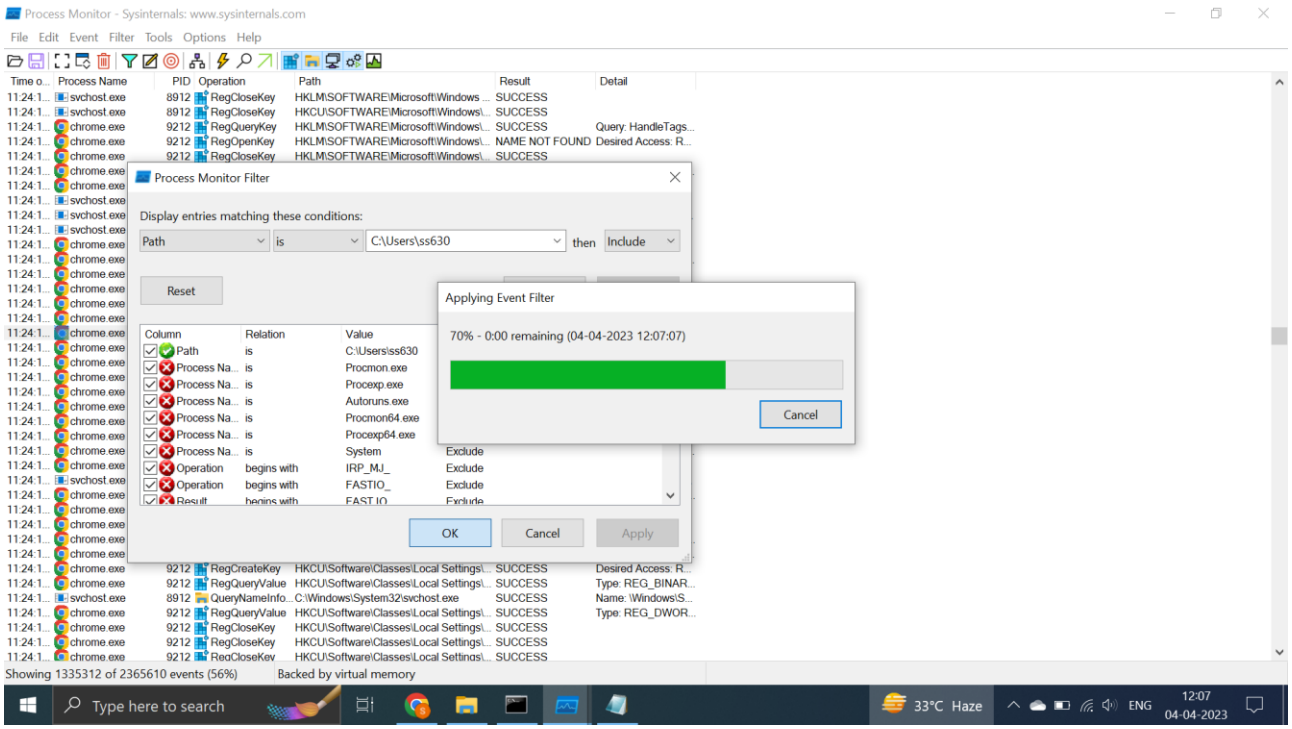
**The Process Monitor window will now only show API calls that match the specified filter.**

**STEP 11: Once you have completed the action, click the "Capture" button again to stop monitoring.The Process Monitor window will display all the events that occurred during the monitoring period, including API calls and their associated details.**

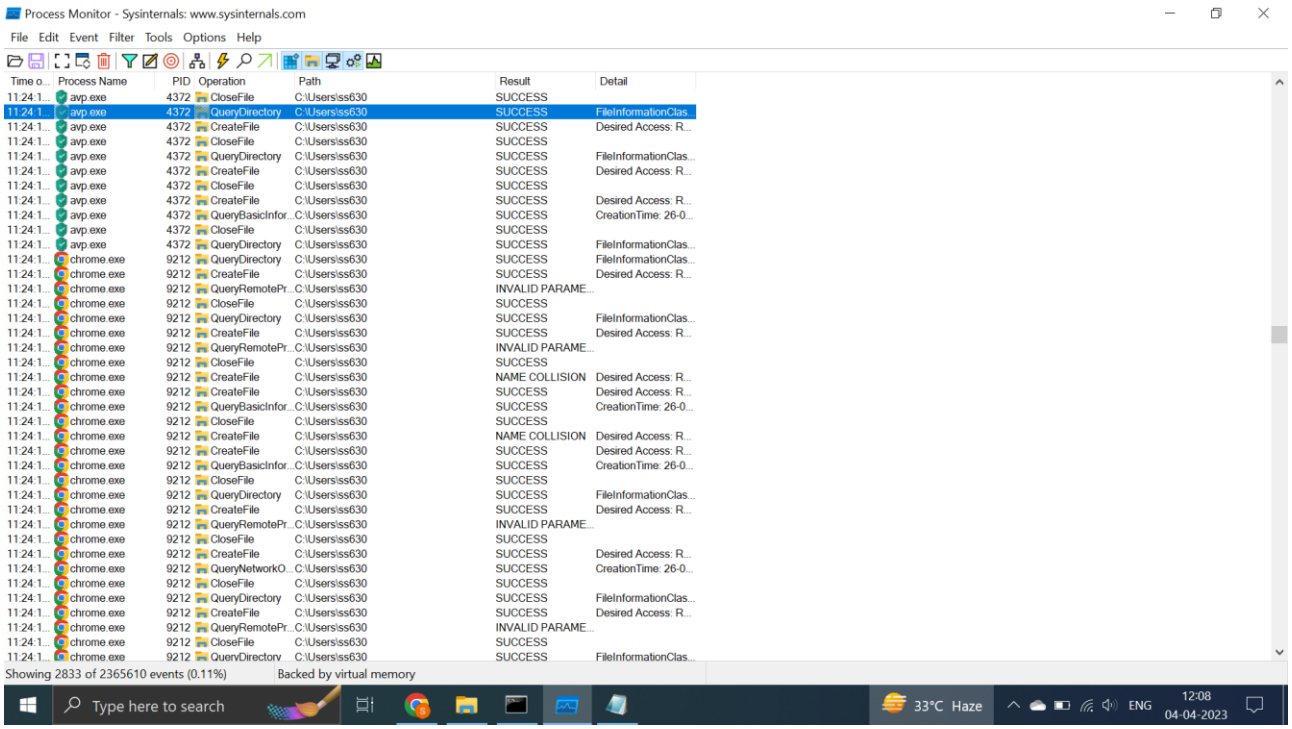
**STEP 12: Analyze the captured data to identify any issues or suspicious activity related to the specified API calls.**

**STEP 13: To analyze behaviour of files or malicious files, In the "Process Monitor Filter" dialog box, select the "Path" filter.**

**In the "Path" field, type the full path to the file you want to analyze. For example, if the file is located at "C:\Users\ss630", type that path in the field.**




**STEP 14: Click "Add" to add the filter to the list. Click "OK" to save the filter settings and close the dialog box.**


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
11:24:1... avp.exe 4372 CloseFile C:\Users\ss630 SUCCESS
11:24:1... avp.exe 4372 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
11:24:1... avp.exe 4372 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... avp.exe 4372 CloseFile C:\Users\ss630 SUCCESS
11:24:1... avp.exe 4372 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
11:24:1... avp.exe 4372 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... avp.exe 4372 CloseFile C:\Users\ss630 SUCCESS
11:24:1... avp.exe 4372 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... avp.exe 4372 QueryBasicInfor... C:\Users\ss630 SUCCESS CreationTime: 26-0...
11:24:1... avp.exe 4372 CloseFile C:\Users\ss630 SUCCESS
11:24:1... avp.exe 4372 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
11:24:1... chrome.exe 9212 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... chrome.exe 9212 QueryRemotePr... C:\Users\ss630 INVALID PARAME...
11:24:1... chrome.exe 9212 CloseFile C:\Users\ss630 SUCCESS
11:24:1... chrome.exe 9212 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... chrome.exe 9212 QueryRemotePr... C:\Users\ss630 INVALID PARAME...
11:24:1... chrome.exe 9212 CloseFile C:\Users\ss630 SUCCESS
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 NAME COLLISION Desired Access: R...
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... chrome.exe 9212 QueryBasicInfor... C:\Users\ss630 SUCCESS CreationTime: 26-0...
11:24:1... chrome.exe 9212 CloseFile C:\Users\ss630 SUCCESS
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 NAME COLLISION Desired Access: R...
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... chrome.exe 9212 QueryBasicInfor... C:\Users\ss630 SUCCESS CreationTime: 26-0...
11:24:1... chrome.exe 9212 CloseFile C:\Users\ss630 SUCCESS
11:24:1... chrome.exe 9212 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... chrome.exe 9212 QueryRemotePr... C:\Users\ss630 INVALID PARAME...
11:24:1... chrome.exe 9212 CloseFile C:\Users\ss630 SUCCESS
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... chrome.exe 9212 QueryNetworkO... C:\Users\ss630 SUCCESS CreationTime: 26-0...
11:24:1... chrome.exe 9212 CloseFile C:\Users\ss630 SUCCESS
11:24:1... chrome.exe 9212 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
11:24:1... chrome.exe 9212 CreateFile C:\Users\ss630 SUCCESS Desired Access: R...
11:24:1... chrome.exe 9212 QueryRemotePr... C:\Users\ss630 INVALID PARAME...
11:24:1... chrome.exe 9212 CloseFile C:\Users\ss630 SUCCESS
11:24:1... chrome.exe 9212 QueryDirectory C:\Users\ss630 SUCCESS FileInformationClas...
Showing 2833 of 2365610 events (0.11%)
Backed by virtual memory
Type here to search
33°C Haze
ENG
12:08
04-04-2023

**STEP 15:To begin monitoring, click the "Capture" button in the toolbar.**

**Run the file you want to analyze. If the file is malicious, be sure to do so in a sandboxed or isolated environment to avoid infecting your system.**

**Once you have completed analyzing the file, click the "Capture" button again to stop monitoring.**

**The Process Monitor window will display all the events that occurred during the monitoring period, including file system activity and their associated details.**

**Analyze the captured data to identify any suspicious activity related to the file, such as attempts to modify system files or communicate with unknown network addresses.**

**STEP 16: To start the UniFi Network Controller and enable automatic upgrades/updates using Sysinternals, In the Process Monitor window, click on the "Filter" menu and select "Filter..." from the drop-down menu.**

**STEP 17: In the "Filter" dialog box, set the filter to include only events from the UniFi Network Controller executable file. To do this, select the "Path" filter and set the "contains" field to the path of the UniFi Network Controller executable file. For example, if the file is located at "C:\Program Files\UniFi\UniFi Network Controller\bin\mongod.exe", enter "mongod.exe" in the "contains" field.**

**STEP 18: Click "OK" to apply the filter.**
**Launch the UniFi Network Controller by running the appropriate executable file or shortcut.**
**Once the controller is open, log in using your administrator credentials.**
**Check the "Auto Update" box in the "Settings" menu to enable automatic upgrades/updates for the UniFi Network Controller.**

4. References- www.google.com
www.youtube.com