Thirtyseven4 EDR Security 8.3

Administrator's Guide

Thirtyseven4, LLC.

www.thirtyseven4.com

Release Date

June, 2024

Contents

Introducing Thirtyseven4 EDR Security

For every organization, security of valuable data and resources is of paramount concern. Today Web technology is an integral part of business processes for all organizations. This puts them more at risk from new and unknown threats and attacks. Thirtyseven4 EDR is designed to provide complete security solutions to small and enterprise-level networks against various kinds of malicious threats such as viruses, Trojans, worms, backdoors, spyware, riskware, adult content, and hackers.

Thirtyseven4 EDR Security is a Web-based management solution that integrates desktops, laptops and network servers. It allows you to access all clients and servers in the network and manage them remotely. You can deploy antivirus software applications, configure security policies, signature pattern updates, and software updates on the clients and servers. You can also monitor clients to check whether there are any policy breaches or security threats within the organization, and take appropriate actions for ensuring security across the networks.

How Does Thirtyseven4 EDR Work?

Thirtyseven4 EDR Security works on the Client/Server architecture where the console manages all the client agents deployed on the network. The console and client agents can be installed on almost all flavors of Microsoft Windows operating systems. The client agents can also be installed on the machines with Mac operating systems. For a detailed description of console and client agent system requirements and compatibilities, see System Requirements.

Thirtyseven4 EDR Security helps the administrators deploy Thirtyseven4 Antivirus remotely on the specified computers, groups or domains, which are the part of the same domain. Whenever the server copy of Thirtyseven4 Antivirus is updated, all computers configured to update from the server will be automatically updated without user intervention. Thirtyseven4 EDR Security monitors these processes so that an administrator can view the computers that have Thirtyseven4 Antivirus installed, the virus database date of Thirtyseven4, whether Virus Protection is enabled, and if viruses are active in the memory of workstations. If any virus is found active in the memory of a workstation, that workstation gets disconnected from the network. If it detects that Thirtyseven4 is uninstalled from any workstation(s), it reinstalls Thirtyseven4 remotely without user intervention. This keeps the computers and the network safe from virus threats.

New in this release

With this release, the following features are added to the Thirtyseven4 8.3 release.

- **High Availability (HA)**

  High Availability (HA) refers to the design and implementation of systems and architectures that ensure continuous and uninterrupted access to services, applications, and data, even in the case of hardware failures, software glitches, or other disruptions.

  This feature:

  - Provides high availability for the Thirtyseven4 EDR Security 8.3solution.
  - Automates deployment of complete clustering components through Ansible.
  - Supports directory synchronization for log backups.
  - Deploys cluster maintenance and alert scripts using Ansible.

- **Custom Server Certificate**

  Thirtyseven4 EDR Security 8.3by default supports self-sign certificates. Now, there is a provision to replace the public key certificate if a customer has it. This enhancement lets you replace the custom certificate. It can be done more than once.

- **OVA**

  You can now deploy OVA on the VirtualBox and set up Thirtyseven4 EDR Security server.

- **Application Control – Block All**

  In addition to the Allow All settings, now Block All is added. With these settings, all applications are blocked by default except for the applications present in the Allowlist.

- **EDR**
  - **MISP Integration**
    - MISP Threat Sharing, an open-source threat intelligence platform is now included in the EDR setup.
    - High threat level malicious data is pulled from the open source MISP server in endpoint threat hunting and the automated ETH scan is performed on clients. This activity is run daily or weekly so that the actions can be performed on real-time hashes present on client.
  - **OS Query – Endpoint Interactivity for Information Gathering**

    Live Query is a new Thirtyseven4 EDR Security feature from which a query can be run on endpoints in real-time and identify areas of improving security.

- **Blocking IOCs Based on Hash Values**

Apart from the existing on demand/scheduled ETH scan, real-time searching and blocking of hashes is added as a new feature.

- **Web Security**
  - YouTube Access Controller
    - YouTube videos can now be allowed/blocked based on categories.
    - Selected publishers and channels on YouTube can now be blocked/allowed by using the block or allow list.
    - Google Chrome (version 92 and above) or Microsoft Edge (version 110 and above) are the only supported browsers.
  - Google Access Controller
    - With the Thirtyseven4 EDR Security's new extension 'Web Access Controller', administrator can ensure that the users within the organization can only sign into the Corporate Google Accounts on the endpoints. (For specific domains that are configured by the Administrator).
    - Google Chrome (version 92 and above) or Microsoft Edge (version 110 and above) are the only supported browsers.
- **Dashboard**
  - ETH Widgets - UI
    - ETH related data can be availed from UI. There is a separate tab for ETH widgets that is EDR tab.
- **Admin Settings**
  - Email notifications are now part of Admin settings
    - Email Configuration is now tenant level setting instead of policy level setting.
    - Instead of Groups, now it will be applicable to all the registered endpoints.
- **Installer**
  - Thirtyseven4 EDR Security 8.3Installation via FQDN
    - Now we support FQDN based Thirtyseven4 EDR Security server installation along with IP Address based installation. The Server Console URL can now have a fully qualified domain name.
- **Configure Update Agent by IP Address**
  - Now you can assign Update Agent role to the selected endpoint by IP address as well as domain name.
- **Linux**

    - **Self-Protection Support**
        - The Self-protection feature is to provide a common framework to protect Thirtyseven4 EDR Security installation files and folders from unauthorized modification.
    - **Roaming Support**
        - Added roaming support for Linux agents.
- **Https Communication**
    - Added capabilities for MAC and Linux.
        - Communication over Https protocol.
        - AV updates on Https only for MAC whereas Linux continues taking updates using Http protocol.
        - URL Categorisation.
- **Heartbeat Interval**
    - Default heartbeat: 3 minutes. It can be configured from 1 minute to 5 minutes from the Admin settings.
- **Device Control**
    - **Temporary USB Access Control Duration to 30 Days**
        - Now we support USB device access for a maximum of 30 days.
        - Supports Windows.
    - **USB Tethering**
        - Administrators can now block internet sharing through mobile phones/dongles.
- **Logging Support for MAC**
    - This feature allows you to enable Web Security logs under the product installation directory.
    - If any issue occurs on the Mac client related to Web Security, then you can enable debug log.
    - This feature is applicable to only MAC clients.
- **[Mac, Linux] Web Protection Unknown Category Support**
    - [Mac, Linux] Web Protection 'Unknown' and 'Cyber Security Awareness and Training Simulation Site' category Support.
- **Client Install/Uninstall Notification**
    - Client Agent now sends Installation Notification to the server. This notification is sent to the server after successful AV Installation as well successful activation of AV.

  - Client Agent also sends an uninstallation notification to the server once AV uninstallation is successful on specific endpoint.

- **Export Excluded Devices List**
  - Export list of excluded devices in excel format which are used under policy.
  - CSV export functionality is available for device control configuration.
  - Navigation: Reports > Advance device control > tabular.
  - A new default query should be added to view exception list.
  - After clicking View, tabular data is shown, without any filter (same as host integrity).
  - Following column details are displayed in Device Exceptions Report:
    - Device Name, Device Type, Model Name, Serial Number, Policy Name, Policy type, Encryption Status, Authorized, Vendor ID, Product ID.
- **Port - IP Whitelisting for (IDS level only)**
- **Group wise Endpoint Migration from Thirtyseven4 EDR Security 7.6 SP5 to Thirtyseven4 EDR Security 8.3**
  - Added capabilities to move endpoints by the group.
- **Alert Enhancement for Email**
  - If the SMTP server is down for some reason, an alert message appears on the screen as **Failed to send Email as SMTP server is not reachable.**

  It appears once in 24 hours.

Available Flavors

The following table lists the features that are available in the packages:

Features	**EDR**
Antivirus	Yes
Anti Ransomware	Yes
Email Protection	Yes
IDS/IPS Protection	Yes
Firewall Protection	Yes
Phishing Protection	Yes
Browsing Protection	Yes
SMS Notification	Yes
Vulnerability Scan	Yes
Roaming Client	Yes

Asset Management	Yes
Spam Protection	Yes
Web Security	Yes
Advanced Device Control	Yes
SIEM Integration	Yes
Application Control – Blocklist	Yes
Application Control – Safelist	Yes
Tuneup	Yes
File Activity Monitor	Yes
Patch Management	Yes
YouTube Access Controller	Yes
Google Access Controller	Yes
Rapid Query to Endpoints	Yes
Automated IoC Blocking	Yes
Realtime IoC Blocking	Yes
Endpoint Threat Hunting	Yes
Data Loss Protection	Yes
File Sandbox	Optional
Encryption	Yes

As per the flavor purchased, the features are available in the portal. In this guide, all the features are explained.

8.3 Feature Parity with the OS

Features	Windows	MAC	Linux
Antivirus	Yes	Yes	Yes
Anti Ransomware	Yes	No	No
Email Protection	Yes	Yes	No
IDS/IPS Protection	Yes	No	No
Firewall Protection	Yes	No	No
Phishing Protection	Yes	Yes	Yes
Browsing Protection	Yes	Yes	Yes
SMS Notification	No	No	N/A
Vulnerability Scan	Yes	No	No
Roaming Client	Yes	Yes	Yes
Asset Management	Yes	Yes	Yes
Spam Protection	Yes	Yes	No
Web Security	Yes	Yes	Yes
Advanced Device Control	Yes	Yes	Yes
SIEM Integration	Yes	No	No
Application Control – Blocklist	Yes	No	No
Application Control – Safelist	Yes	No	No
Tuneup	Yes	No	No
File Activity Monitor	Yes	Yes	No
Patch Management	Yes	No	No
YouTube Access Controller	Yes	No	No
Google Access Controller	Yes	No	No
Rapid Query to Endpoints	Yes	No	N/A
Automated IoC Blocking	Yes	No	N/A
Realtime IoC Blocking	Yes	No	N/A
Endpoint Threat Hunting	Yes	No	N/A
Data Loss Protection	Yes	Yes	N/A
File Sandbox	Yes	No	N/A

Best Cyber Security Practices

Best cyber security practices for Enterprises to stay cyber secure in wake of the rising incidences of targeted attacks on enterprises, there is no way organizations can afford to ignore the importance of cyber security. Regardless of the size and type of enterprise, even a small data breach or cyber-attack could mean millions of dollars of loss, crippling the economy of the enterprise.

It is for this reason that as a thumb rule, enterprises start following these good cyber security practices, to be cyber secure against known and unknown threats:

- Invest in Security Solutions – An enterprise may be subjected to various kinds of threats and thus, to ensure enterprise-wide security, it is a good practice to invest in a variety of security solutions that cover the changing needs of an organization.
- Use Complex & Unique Passwords – As a thumb rule, enterprises must encourage employees to use strong and unique passwords and prohibit them from sharing their credentials.
- Invest in Training – Educate and train employees about cyber security so that they are cautious about clicking suspicious links, sharing sensitive data and responding to security alerts.
- Backup Your Data – Follow the 3-2-1 rule when it comes to data backup, meaning that maintain 3 varying copies of your crucial data in 2 different formats, where at least 1 of the data storage locations should be offline.
- Robust Security Policies – To ensure that both employees and third parties follow the security policies, it is important to strictly convey the enterprise security policies and expectations.
- Use Updated Software – Using expired software is as good as counting on a dead security solution. Thus, it is a good practice to keep your software updated to the latest version, to safeguard your organization against evolving threats.
- Data Encryption – It is advisable to encrypt all the saved and backed-up data while providing access rights to only limited and specific personnel.
- Two-Factor Authentication – An additional and reliable login procedure is to use two-factor authentication that uses a secondary device like a mobile for access authentication.
- Have an MDM Plan – It is important to monitor and regulate the mobile device usage of employees since, they often use it for accessing sensitive data and company Emails, while using the company's wireless network. This may serve as a soft vulnerability for attacks.

- Change Default Credentials – Several IoT devices come with default passwords that make it easy for malware to target such IoT devices. Thus, it is a good practice to change these default credentials.
- Secured Wi-Fi – A device can connect to only those Wi-Fi networks which have a known SSID. Thus, to prevent an unknown device from connecting to the Wi-Fi network of your enterprise, a good security mechanism is to use a hidden SSID to prevent it from getting broadcast.
- Limited Access Right Grant – Anyone who requests access to a resource, should be provided with minimum access rights and that too for the shortest duration necessary. Such restricted delegation of access rights can limit attackers from intruding into systems.
- Server OS Hardening – To address the security of your enterprise adequately, it is advisable to configure and harden the operating system. This typically involves removing all the unnecessary applications, services and network protocols.

Installing Thirtyseven4 EDR Security Server Via OVA File

Overview

This section helps you to deploy OVA on the VirtualBox and set up Thirtyseven4 EDR Security server.

OVA (Open Virtualization Appliance) file contains a compressed version of a virtual machine. When you deploy an OVA file, the virtual machine is extracted and imported into the virtualization software installed on your computer.

The OVA build file is provided to address any of the following scenarios at the customer end.

- Ubuntu 22.04 LTS machine is not available.
- Only Windows machine is available.

This OVA will create an Ubuntu 22.04 LTS machine on top of the VirtualBox and then you can proceed through the configuration of the pre-installed Thirtyseven4 EDR Security server.

OVA Details

- OVA File name: Thirtyseven4 EDR Security_8.3_UBUNTU22.ova
- Oracle Virtual box version: 7.0.8
- RAM: 8 GB

Prerequisites

- Physical Windows Machine with RAM >= 16 GB
- Windows 10 and above OR Windows server 2019 and above
- Disk space: 60 GB and above.
- CPU: 4 Core (x86-64) or above.
- The VT-x must be enabled in the physical machine's BIOS.
- Oracle Virtual Box 7.0.8
- EPS_8.2_UBUNTU22.ova build file.
- Keep the following details ready and handy.
    - Product Key
    - Static IP Address

- Gateway
- Subnetmask
- DNS

Note: For seamless working of OVA over virtual box, it is recommended to have only one hypervisor installed on the system. Other than the Oracle Virtual Box, ensure that no other hypervisor is installed on the system.

Step 1: Deploy OVA on VirtualBox

Follow these steps to deploy OVA on the VirtualBox.

1. Download and install Oracle VM VirtualBox on Windows machine.
2. Open the VirtualBox.
3. Go to File > Import Appliance.
4. In this step, choose a virtual appliance file to import. Click **Browse** and select Thirtyseven4 EDR Security_8.3_UBUNTU22.ova file.
5. Click **Next** and follow the wizard.
6. Click **Import**. When the Import is complete, VirtualBox creates VM with Ubuntu. On this, you will configure the pre-installed Thirtyseven4 EDR Security 8.3server.
7. Start the VM. The Network Error prompt appears.
8. Click Change Network Settings. The error prompt disappears.
9. Go to Settings > Network. Click **Ok**.
10. Oracle VM VirtualBox Manager window appears. OVA is deployed successfully on the VM.
11. Click Start icon to start the VM. The VM is ready for use.

Step 2: Configure Thirtyseven4 EDR Security Server

On the VM, login with the given credentials.

Note: It is recommended to change the password after installing the Thirtyseven4 EDR Security server.

1. Provide the following details one after another and hit [Enter].
   - Static IP Address
   - Subnetmask

- Gateway
- DNS

2. Software License Agreement appears. Read the License Agreement carefully. Installation and usage of Thirtyseven4 EDR Security is subject to your formal acceptance of the Thirtyseven4 EDR Security end-user license terms and conditions. To continue, hit [Enter] or press R key to read more.
3. Terms & Conditions appear. To continue, hit [Enter] or press R key to read more. To continue, type A and hit [Enter] to accept the terms and conditions; D option is to decline. If you decline, the installation process is stopped.

   Wait till the system is configured for user. It might take 5 to 6 minutes.
4. The Proxy Settings screen appears. If you are using a proxy server to connect to the Internet, type 1 and hit enter.

   To enable and configure proxy settings:

   a. Type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com) and hit [Enter].

   b. Type the port number of the proxy server (For example: 80) and hit [Enter].

   c. Type 1 to Authenticate to connect through the Proxy server. Type 2 to continue without authentication.

   d. Type User Name.

   e. The success message appears if the connection to the proxy server is successful.
5. If you want to continue without enabling Proxy Settings, type 2 and hit enter. The Proxy Setting information is used by Thirtyseven4 EDR Security server for internet connectivity, activation and for downloading updates.
6. The Product Key screen appears. Enter the Product key without the hyphen. The Product Key will be validated. The success message appears.
7. The Customer Information screen appears. Verify information about the customer step by step. This information is important to activate Thirtyseven4 EDR Security on your machine. If you are a new customer, enter the information step by step.

   Note: If you are reactivating using the same key, there are two options:

   a. Type 1 to continue with existing information.

   b. Type 2 to update the information.

   Note: The maximum length for the first name is 50 characters.

8. The Authentication screen appears. Create Thirtyseven4 EDR Security administrator password to access the Web console and endpoint password to access the endpoint settings at the endpoint side.

   a. Type in Administrator Email Address and hit [Enter] or you can continue with the existing Email address. To continue, hit [Enter].

   b. Type in your password and hit [Enter]. Type password again to confirm the password and hit [Enter]. You cannot view the typed password.

   c. You can provide client credentials. This is optional. Type 1 to specify client credentials and hit [Enter]. Type in client password and hit [Enter]. Type client password again to confirm the password and hit [Enter]. You cannot view the typed password.

   d. This helps prevent unauthorized users from accessing the Web console and make changes in your settings or remove the endpoints.

   e. Type 2 to continue without providing client credentials and hit [Enter].

9. The installation summary screen appears. Activation and Server Configuration data is displayed. Please note the Thirtyseven4 EDR Security console URL.

   a. Type 1 to save summary file and hit [Enter].

   b. Type 2 to continue without saving and hit [Enter].

10. The installation process starts. Tenant onboarding starts.

    It prompts you to change the password.

11. After changing the password, you need to log in again. To continue:

    a. Type Y to continue using the system and hit [Enter].

    b. Type N to log out and hit [Enter].

12. If you enter Y, the following screen appears.
13. Enter your choice and hit [Enter].

Step 3: Log on to Thirtyseven4 EDR Security Server

1. Paste the console access URL in the browser. Example: https://login/eps.

   Supported Web Browsers:

   - Google Chrome 62, 63, 64 or 65
   - Mozilla Firefox 56, 57, 58, 59, 62, 64 or 65
   - Microsoft Edge.

2. Provide the credentials.

Thirtyseven4 EDR Security console is ready to use.

Exiting the Setup

To exit from the setup:

1. Press **Control C** keys. Confirmation message appears.
2. Again, press Control C keys to exit the setup.

Signing in your Thirtyseven4 EDR Account

Signing in with Active Directory Domain

To sign into Thirtyseven4 EDR Security, follow these steps.

1. Paste the login URL in the browser of your system.

   The Sign in Dialog appears.

2. Enter Email address in the **Email ID** text box. This is your registered Email address you provided during installation.
3. Enter **Password**.
4. If Active Directory Settings are enabled, then only Active Directory Domain Name field appears. Select the **Active Directory Domain** Name from the list. Example: If Thirtyseven4 EDR.com was added as Active Directory Domain Name, appears here.
5. Click **Sign In**.

   The home page of Thirtyseven4 EDR Security appears.

Signing in with MFA

Multifactor Authentication (MFA) provides two-step verification which provides stronger security for your account by requiring a second verification step when you sign in. Here, after providing credentials, you need to provide OTP for authentication.

Only the Super Admin User can enable the MFA setting.

To sign in to your Thirtyseven4 EDR account, follow these steps.

1. Click the Thirtyseven4 EDR Console login link.

   The Sign-in Dialog appears.

2. Enter your registered **Email address** and **Password** in the text boxes.
3. Click **Sign in**.

   The OTP dialog appears. Only if the MFA setting is enabled by Admin.

   An OTP is sent to your registered Email address. The OTP is valid for 15 minutes.

4. Enter the **OTP**.
5. Click **Submit**.

   The home page of Thirtyseven4 EDR Security appears.

   If you did not receive the OTP, you can click **Resend OTP** link.

Only three attempts of OTP entry are allowed. If you enter the wrong OTP three times or more, the account will be locked for 30 minutes. You can try signing in after 30 minutes.

Signing in without MFA

To sign in to your Thirtyseven4 EDR account, follow these steps.

1. Click the Thirtyseven4 EDR Console login link.

   The Sign-in Dialog appears.

2. Enter your registered **Email address** and **Password** in the text boxes.
3. Click **Sign in**.

   The home page of Thirtyseven4 EDR Security appears.

Dashboards

The Dashboard area displays the statistics and charts only when the endpoints are deployed. As a new user, when you land on this page, the message appears to deploy the endpoints. Click the Deployment button if you want to deploy the endpoints at that moment.

The Dashboard area on the Home page displays the widgets for Status, Compliance, DLP and Custom tabs. You can refresh the widget with the refresh button. You can remove the widget with the remove button (X). The removed widget name appears in the Customize Dashboard > Unassigned Widgets section.

Current Status Summary

Feature	Description
Endpoints	Displays total number of endpoints in the network at that time. Clicking the icon below endpoint count, redirects to the Virus Scan report page.
Protection Disabled (All Endpoints are Protected)	• Displays number of endpoints on which the following features are disabled: ▪ Virus protection ▪ Phishing protection ▪ Browsing Protection Clicking the icon below endpoint count redirects to the Status page. • When the above features are enabled on all the endpoints, "All Endpoints are Protected" message appears.
Infected Endpoints (All Endpoints are Clean)	• Displays number of infected endpoints in last 7 days. Clicking the icon below endpoint count, redirects to the Virus Scan page. • When no virus attacks are found, "All Endpoints are Clean" message appears.
Vulnerable Endpoints (No vulnerabilities)	• Displays number of vulnerable endpoints in the network. • Clicking the icon below endpoint count, redirects to the Vulnerability Scan page.

	• When no vulnerabilities are found, "No vulnerabilities" message appears.

Status

Feature	Tab	Description
Infection Detected	Infected Systems	Gives a graphical representation of the infection in the network for the selected time period. The graphs can be viewed for the following time periods: Last 7 Days: Displays the report of the last seven days. Last 15 Days: Displays the report of the last 15 days. Last 30 Days: Displays the report of the last 30 days. Clicking the data points on the chart, redirects to the Virus Scan page.
	Top 10 Infected Systems	Gives a progress bar chart that displays top 10 infected systems in the network for the selected time period. The chart can be viewed for the following time periods: Last 7 Days: Displays the chart of the last seven days. Last 15 Days: Displays the chart of the last 15 days. Last 30 Days: Displays the chart of the last 30 days. Clicking the infection count redirects to the **Virus Scan** report page.
Host Integrity Report		Gives a doughnut chart that displays the number of compliant and non-compliant endpoints. An endpoint is protected and compliant if all the following conditions are true. Client Agent version is the latest Virus Database is updated Virus protection is enabled Behaviour Detection System is enabled No malware is found on it Clicking the slice of the chart, redirects to the Host Integrity report page.
Update Status		Gives a doughnut chart which displays the number of endpoints on which the virus definitions are up-to-date and not up-to-date for 1, 3, 7, 15 and 30 days.

	Clicking the slice of the chart, redirects to the Status page.
Top 10 Malware Detected	Gives a progress bar chart that displays top 10 malware detected systems in the network for the selected time period. The chart can be viewed for the following time periods: Last 7 Days: Displays the chart of the last seven days. Last 15 Days: Displays the chart of the last 15 days. Last 30 Days: Displays the chart of the last 30 days. Clicking the Detection count redirects to the Anti-Malware Scan report page.
Operating System	Gives a doughnut chart which displays the total number of endpoints installed on Windows, Linux and Mac platform. Clicking the slice of the chart, redirects to the Status page.
Managed and Unmanaged Endpoints	Gives a bar graph which displays the number of managed and unmanaged endpoints. This is the enumeration result for the selected clients. For more information, see Enumerate Network. Clicking the bar of the chart, redirects to the Status page.
License Usage Status	Gives two half pie charts, one chart for Thirtyseven4 EDR License and the other for DLP License. The chart displays the number of licenses utilized and licenses remaining. Clicking the slice of the chart, redirects to the Status page. This widget is not applicable for postpaid clients.
Last Connected Endpoints	Gives a doughnut chart which displays the number of endpoints which are connected last and not connected for last 3, 7, 15 and 30 days. Clicking the slice of the chart, redirects to the Status page.
Agent Versions	Gives a doughnut chart which displays the agent versions of all the endpoints. Clicking the slice of the chart, redirects to the Status page.

Compliance

Advanced Device Control

Feature	Description
Device Violations	Gives a graphical representation of the device violations on the endpoints for the selected time period. The graphs can be viewed for the following time periods: • Last 7 Days: Displays the report of the last seven days. • Last 15 Days: Displays the report of the last 15 days. • Last 30 Days: Displays the report of the last 30 days. Clicking the data points on the chart, redirects to the Advanced Device Control report page.
Policy violations by Devices	Gives a doughnut chart which displays the number of policy violations by various devices for last 7, 15 and 30 days. Clicking the slice of the chart, redirects to the Advanced Device Control report page.

Application Control

Feature	Tab	Description
Blocked Applications	Blocked Applications	Gives a graphical representation of the blocked applications for the selected time period. The graphs can be viewed for the following time periods: – Last 7 Days: Displays the report of the last seven days. – Last 15 Days: Displays the report of the last 15 days. – Last 30 Days: Displays the report of the last 30 days. Clicking the data points on the chart, redirects to the Blocked Applications on Access report page.
	Top 10 Blocked Applications	Gives a progress bar chart that displays top 10 blocked applications for the selected time period. The chart can be viewed for the following time periods: – Last 7 Days: Displays the chart of the last seven days. – Last 15 Days: Displays the chart of the last 15 days. – Last 30 Days: Displays the

Feature	Tab	Description
		chart of the last 30 days. Clicking the Block count redirects to the Application Control on Access Report page.
Blocked Application Category	Blocked Application Category	Gives a doughnut chart which displays the number of blocked application categories for last 7, 15 and 30 days. Clicking the slice of the chart, redirects to the Blocked Applications on Access report page.
	Top 10 Blocked Application Categories	Gives a progress bar chart that displays top 10 blocked application categories for the selected time period. The chart can be viewed for the following time periods: – Last 7 Days: Displays the chart of the last seven days. – Last 15 Days: Displays the chart of the last 15 days. – Last 30 Days: Displays the chart of the last 30 days. Clicking the Block count redirects to the Application Control on Access Report page.
Top 10 users who attempted to access blocked applications		Gives a progress bar chart that displays top 10 users who attempted to access blocked applications for the selected time period. The chart can be viewed for the following time periods: – Last 7 Days: Displays the chart of the last seven days. – Last 15 Days: Displays the chart of the last 15 days. – Last 30 Days: Displays the chart of the last 30 days. Clicking the Block count redirects to the Application Control on Access Report page.

Web Security

Feature	Tab	Description
Blocked Websites	Blocked Websites	Gives a graphical representation of the Blocked Websites for the selected time period. The graphs can be viewed for

Feature	Tab	Description
		the following time periods: – Last 7 Days: Displays the report of the last seven days. – Last 15 Days: Displays the report of the last 15 days. – Last 30 Days: Displays the report of the last 30 days.
	Top 10 Blocked Websites	Gives a progress bar chart that displays top 10 blocked websites for the selected time period. The chart can be viewed for the following time periods: – Last 7 Days: Displays the chart of the last seven days. – Last 15 Days: Displays the chart of the last 15 days. – Last 30 Days: Displays the chart of the last 30 days. Clicking the Block count redirects to the Web Security Report page.
Web categories	Blocked Web Categories	Gives a doughnut chart which displays the number of Websites blocked by categories for last 7, 15 and 30 days.
	Top 10 Blocked Web Categories	Gives a progress bar chart that displays top 10 blocked web categories for the selected time period. The chart can be viewed for the following time periods: – Last 7 Days: Displays the chart of the last seven days. – Last 15 Days: Displays the chart of the last 15 days. – Last 30 Days: Displays the chart of the last 30 days. Clicking the Block count redirects to the Web Security Report page.

Assets

Feature	Description
Hardware changes	Gives a graphical representation of hardware changes detected on endpoints with Windows and Mac operating systems for the selected time period. The graphs can be viewed for the following time periods: – Last 7 Days: Displays the report of the last seven days. – Last 15 Days: Displays the report of the last 15 days. – Last 30 Days: Displays the report of the last 30 days. Clicking the data points on the chart, redirects to the Asset Management report page.

Feature	Description
Software changes	Gives a graphical representation of software changes detected on endpoints with Windows and Mac operating systems for the selected time period. The graphs can be viewed for the following time periods: – Last 7 Days: Displays the report of the last seven days. – Last 15 Days: Displays the report of the last 15 days. – Last 30 Days: Displays the report of the last 30 days. Clicking the data points on the chart, redirects to the Asset Management report page.

Top 10 Vulnerabilities

Feature	Description
Top 10 Vulnerabilities	Gives a progress bar chart that displays top 10 Vulnerabilities detected in the systems in the network. Clicking the Detection count redirects to the Vulnerability Scan report page.

Data Loss Prevention

Feature	Tab	Description
DLP Policy Violations	Violating Endpoints	Gives a graphical representation of DLP violations detected on endpoints for the selected time period. The graphs can be viewed for the following time periods: • Last 7 Days: Displays the report of the last seven days. • Last 15 Days: Displays the report of the last 15 days. • Last 30 Days: Displays the report of the last 30 days. Clicking the data points on the chart, redirects to the Data Loss Prevention report page.
	Top 10 Violating Endpoints	Gives a progress bar chart that displays top 10 DLP policy violating endpoints for the selected time period. The chart can be viewed for the following time periods:

	Last 7 Days: Displays the chart of the last seven days. Last 15 Days: Displays the chart of the last 15 days. Last 30 Days: Displays the chart of the last 30 days. Clicking the Block count redirects to the Data Loss Prevention Report page.
Top 10 users who attempted to breach DLP policy	Gives a progress bar chart that displays top 10 users who attempted to breach DLP policy for the selected time period. The chart can be viewed for the following time periods: – Last 7 Days: Displays the chart of the last seven days. – Last 15 Days: Displays the chart of the last 15 days. – Last 30 Days: Displays the chart of the last 30 days. Clicking the Block count redirects to the Data Loss Prevention Report page.
Data Leaks through Data Transfer Channel	Gives a doughnut chart which displays the number of data leaks through data transfer channel for last 7, 15 and 30 days. Clicking the slice of the chart, redirects to the Data Loss Prevention report page.
Type of Data Leaks	Gives a doughnut chart which displays the type of data leaks for last 7, 15 and 30 days. Clicking the slice of the chart, redirects to the Data Loss Prevention report page.

EDR

Feature	Description
Top 10 Hash Codes	Gives a progress bar chart that displays top 10 Hash occurrences in the network for the selected action. The chart can be viewed for the following actions: – No action – Deleted – Quarantined – Quarantined and Block

Feature	Description
	Clicking the data points on the chart, redirects to the ETH report page.
Malicious Hash Instances	Gives a graphical representation of Malicious Hash instances detected on endpoints for the selected time period. The graphs can be viewed for the following time periods: – Last 7 Days: Displays the report of the last seven days. – Last 15 Days: Displays the report of the last 15 days. – Last 30 Days: Displays the report of the last 30 days.
Total affected endpoints due to malicious hashes	Gives a graphical representation of the total affected endpoints due to malicious hashes for the selected time period. The graphs can be viewed for the following time periods: – Last 7 Days: Displays the report of the last seven days. – Last 15 Days: Displays the report of the last 15 days. – Last 30 Days: Displays the report of the last 30 days.

Patch Management

Feature	**Description**
Number of missing patches by severity	Displays the number of missing patches according to their severity (critical, important, moderate, low, and unspecified) in the form of a bar chart.
Patch scan overview	Displays the information for the patch scans. The count of endpoints with missing patches, endpoints not scanned, Up-to-Date endpoints are displayed.

Custom Dashboard

You can create your own dashboard as per your requirement. The custom dashboard is displayed by default.

You can include widgets as per your choice. You can set the sequence of widgets as per your requirement.

Customizing Dashboard

To create your own dashboard, follow these steps:

On the Dashboard page, click **Customize Dashboard** option.

The Customize Dashboard window appears. The list of Unassigned widgets is shown.

The four Dashboard Views columns are shown with their widgets.

Drag and drop the widgets in the Dashboard Views as per your requirement. You can drag the widgets from the Unassigned list and from other dashboard views and drop in the desired view.

Click **Save**.

You can also edit the Dashboard View name.

User

The User page displays the information of all the users including Active Directory Users in the table format. The table includes information such as User Name, User Role, Email, Mobile No., and Status.

You can customize the User table as per column names.

To select all the users from the table, select the check box in the header row.

To select an individual user, select the check box in that row.

You can search the user with the help of search criteria.

For the users of only Thirtyseven4 EDR SECURITY

If you have purchased only Thirtyseven4 EDR SECURITY, you have full access to this page.

You can add, delete, edit User from this page. You can also change the password of the user except for Active Directory User.

Here you can view the details of the user. Also, you can create a user, and assign user role. You can rename, edit or delete the user. You can enable or disable the user.

User Session

The user session begins when the user logs on to Thirtyseven4 EDR Security and ends when the user logs off.

However, the session is timed out if the current session is inactive for 20 minutes.

Adding a User

This feature helps you create a user and assign user role.

Adding a User

To add a user, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to User. The Users page appears displaying list of users.
3. Click **Add User** button.
4. Click **Add**.
   The Add User dialog appears.

Active Directory User switch appears only when **Active Directory** settings are enabled. Keep the switch at No position.

5. Enter **First Name, Last name, Email ID, Password, Confirm Password, and Mobile No.**
6. Select the **User Role** from the list. The selected role will be assigned to the user.
7. The User role can be changed to the other role as and when required.
   If you assign the User Role as **Group Admin,** click **Next**.
   In the dialog, a list of groups appears. Select the group to be assigned to the Group Admin. Only one group can be assigned to the Group Admin here.If the Parent group is selected, all child and sub child group are selected automatically. You can select only one child or a subchild group from the hierarchy. One group can have multiple Group Admins.
8. Click **Add**.
   The new user is added to the list. You can create maximum 49 users.
   When you log on to Thirtyseven4 EDR Security as Group Administrator, the Status page is displayed by default. Only pages having privileges for Group Admin are displayed.

Adding an Active Directory User

To add an Active Directory (AD) user, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to User. The Users page appears displaying a list of users.
3. Click **Add User** button.
4. Click **Add**. The Add User dialog appears. Active Directory User switch appears only when Active Directory settings are enabled.
5. Toggle the **Active Directory User** switch to **Yes**.
6. Enter **AD User name**. AD Username is required for authentication The Password and Confirm Password fields are disabled as AD credentials of the user are used for authentication.
7. Enter **First Name, Last name, Email ID**, and **Mobile No**.
8. Select the **User Role** from the list. The selected role will be assigned to the user.
9. Click **Add**.

The new AD user is added to the list.

When you log on to Thirtyseven4 EDR Security as an AD User, you need to provide AD credentials.

Changing Password of User

Password cannot be changed for Active Directory User.

To change the password of the normal User, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to User. The Users page appears displaying a list of users.
3. Click **Change Password** link of the user for which you want to change the password. The Change Password dialog appears.
4. Enter new password. Enter the new password again to confirm.
5. Click **Change Password.**

The password of the user is changed.

Enabling a User

To enable a user, follow these steps:

1. Select the check box of the user that you want to enable. An action bar is enabled above the table.
2. Select **Enable**.
3. Click **Submit** button.
4. The confirmation message appears. Click **Yes**.
   The selected user is enabled.

Disabling a User

To disable a user, follow these steps:

1. Select the check box of the user that you want to disable. An action bar is enabled above the table.
2. Select **Disable**.
3. Click **Submit** button.
4. The confirmation message appears. Click **Yes**.
   The selected user is disabled.

Note

The disabled user cannot log on the Thirtyseven4 EDR Security portal.

Deleting a User

To delete the user, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to User. The Users page appears displaying list of users.
3. Select the check box of the user that you want to delete. An action bar is enabled above the table.
4. Select **Delete**.
5. Click **Submit** button.
6. The confirmation message appears. Click **Yes**.
   The selected user is removed.

Note
You cannot edit or delete the default user.

If you delete the Group Admin, the policies created by the Group Admin can be deleted if the policies are not assigned to any group and endpoints.

Editing a User

For the users of only Thirtyseven4 EDR SECURITY

If you have purchased only Thirtyseven4 EDR SECURITY, you have full access to this page.

Here you can edit the user information. You can edit name, Email address or mobile number of users. You can also change the user role. If you change the role to Group Admin, you can assign group.

To edit the user, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **User**. The Users page appears displaying list of users.
3. Click the Edit icon of the user that you want to edit.
   The Edit User dialog appears.
4. Edit the information.
5. If you assign the User Role as **Group Admin**, click **Next**.
6. In the dialog, a list of groups appears. Select the group to be assigned to the Group Admin.If the Parent group is selected, all child and sub child group are selected automatically. You can select only one child or a subchild group from the hierarchy.

7. Click **Save**.
   User information is updated.

Note: You cannot edit or delete the default user.

Importing a user

You can import maximum 49 users at a time through a CSV file.

To import the users, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Users**. The Users page appears displaying list of users.
3. Click **Add User > Import**.
4. In the Import User dialog, import a CSV file by clicking **Browse**. The file size must be less than or equal to 1 MB.
   The CSV file content should be in the following format:

First Name	Last Name	EMAIL	Password	Confirm Password	Country Code	MOBILE NUMBER	User RoleName	Domain Name	ActiveDir User Name
aaa	rrr	aaa@mail.com	**********	*********	+91	11111111	ADMIN	Thirtyseven4 EDR.com	Administrator
bbb	sss	bbb@gmail.com	********	********	+44	2222222222	REPORT_ONLY		
ccc	ddd	ccc@gmail.com	**********	*********	+1	3333333333	ADMIN	Hawk.com	Admin

   Password must contain 6 to 19 characters. There must be at least one uppercase letter, 1 lowercase letter, a number, and a special character.

   As you see in the above example, the Country Code should contain + sign.
   The User Role name (REPORT_ONLY, ADMIN) should be in Capital letters.

   Only for the Active directory user, **Domain Name** and **ActiveDir User Name** are required. For the normal user, these columns should be blank.

5. Click **Import**.

Groups

On the Groups page, you can view, create, and manage groups and subgroups. In the left pane, a tree like structure of groups and subgroups is displayed. The synchronized groups with Active Directory have AD tag in their name. In the right pane, the group name and number of endpoints assigned to that group is displayed. One group may have multiple Group Admins. Names of Group Admins are also displayed. You can edit Group Admin.

In the 'Assigned policies to the group' section, a table shows the assigned policies to the selected group. The policy applied on the group is applicable to all the endpoints within the group.

This feature helps you create groups and subgroups, and apply a policy to a group (or a subgroup). You can delete or rename a group or set different policies for different groups. You can also change Group Admin of the group.

Adding a Group

To add a new group, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Groups.
3. Select the root if you want to create the new group at the root level. Select a group to create subgroup.
4. Click **Add Group**. The Add Group screen appears.
5. In the **Group Name** text box, type a group name.
6. Select the policy for endpoint from the list.
7. Click **Add**.
   The new group/subgroup is added.

Note
No subgroup can be created under the Default group.

Assigning Group Admin to the Group

1. Add a new group. See Adding a group.
2. Go to User. The Users page appears displaying list of users.
3. Click Edit icon of the Group Admin that you want to assign to your group.
   Edit User dialog appears.

4. Click **Next**.
5. In the dialog, a list of groups appears. Select your group to assign to the Group Admin. Only one group can be assigned to the Group Admin here. If the Parent group is selected, all child and sub child group are selected automatically. You can select only one child or a subchild group from the hierarchy. One group can have multiple Group Admins.
6. Click **Save**.
   The confirmation dialog appears.
7. Click **Ok**.
   The Group Admin is assigned to the group. On the Groups page, when you select the group, you can view assigned Group Admin in the right pane.

   Group Admin can view all the endpoints of the assigned groups and subgroups.

Setting Policy to a Group

Policies may include different client settings for different groups in an organization.

If the policy is pushed from MSSP, it will get applied on default Thirtyseven4 EDR group and that policy will be read only.

To set a policy to a group, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Groups.
3. In the left pane, select a group to apply the policy. The list of policies for endpoints is displayed.
4. To change the policy, click **Change Policies** option. The Change Computer Policies dialog appears.
5. In the Default Policies tab, select the policy that you want to apply.
6. In the Override Policies tab, select the features for which you want to override the policy.
7. Click **Assign**.

The policy is applied to the selected group.

The policy created by Super Admin or Admin when applied on the group is read only for Group Admin.

For more information about policies, see Policies.

Deleting a Group

To delete a group/subgroup, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Groups.
3. In the left pane, select a group/subgroup.

   Note
   You cannot delete the group if Group Admin is assigned to that group.

4. In the right pane, click the **Delete** button. A confirmation message is displayed.
5. Click **Yes**.

The selected group/subgroup is deleted.

If you delete the group, all the sub groups available under that group will be deleted. The endpoints assigned to the subgroup and groups will be moved to Default group. The policy of default group is applied on the moved endpoints except the feature policy assigned on the endpoint.

If you delete the subgroup, the endpoints assigned to the subgroup will be moved under its parent group and policy of parent group is applied on the moved endpoints except the feature policy assigned on the endpoint.

Moving Group

To move a group/subgroup, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Groups.
3. In the left pane, select a group/subgroup. Drag the group to a desired group where you want to move.

The endpoints and policies associated with the group remain the same, but under new parent group.

Renaming a Group

To rename a group, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Groups.
3. In the left pane, select a group/subgroup to rename. The Group details appears.
4. Click the **edit** icon in the Group Name. Edit the Group Name.
5. To save changes, click the **tick** mark.

The group/subgroup name is modified. However, the policy applied earlier to this group does not change. To change a policy, you have to apply a new policy.

Changing Group Admin

To change a group/subgroup assigned to Group Admin, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Groups**.
3. In the left pane, select a group/subgroup.
4. In the right pane, the details of the group appears. The names of Groups Admins with edit icon appears. Click the **edit** icon of the Group Admin that you want to change.
5. The Change Group dialog appears. In the dialog, a list of groups appears. Select the group to be assigned to the Group Admin. Only one group can be assigned to the Group Admin here. If the Parent group is selected, all child and sub child group are selected automatically. You can select only one child or a subchild group from the hierarchy. One group can have multiple Group Admins.
6. Click **Apply**.

The changed group is assigned to the Group Admin.

Status

The Status page displays the current status of all the endpoints of the selected group. The status includes the following information of the endpoint.

Column Name	Description
Endpoint Name	Displays the name of the endpoint.
IP Address	Displays the IP address of the endpoint.
Endpoint Status	Endpoint Status column provides information whether the endpoint is online, offline or roaming. The status and meanings are as follows: Online – Endpoint Status is Online when the client and Server communication happens in both ways. Offline – Endpoint status is changed to offline according to set missed heartbeat count to turn endpoint offline. For more details, see Admin Settings. Roaming – Endpoint Status is Roaming when the Roaming Service is assigned to the selected endpoint. For more details, see Roaming Service. Disconnected – The status Disconnected means infected endpoint is disconnected from the network when a non-repairable virus is found and a suspicious file is found by the DNA scan.
Domain Name	Displays the name of the domain to which the selected client logs in.
Group Name	Displays the group name to which the selected client belongs.
User Name	Displays the user name of endpoint.
Policy	Displays the policy applied on the endpoint.
Virus DB Date (GMT+5:30)	Displays VDB date along with Update time.
Last Connected	Displays the date when the endpoint was last connected.

Column Name	Description
Last Scanned	Displays the date when the endpoint was last scanned.
MAC Address	Displays the MAC address of the endpoint.
Client Version	Displays the installed Thirtyseven4 EDR client version.
Operating System	Displays the name of the operating system of the endpoint.

The following options help to customize and search the desired endpoints:

- **Columns**: You can use this option to customize the status list as per column names.
- **Filter by**: You can use this option to filter the status list according to the Operating Systems platforms, Endpoints with DLP, Endpoints without DLP and Clients Need Upgradation. The legend for Assigned DLP License and Assigned Update Agent Role are displayed for the respective endpoints.
- **Endpoint Name**: You can use this option to search the endpoints with different parameters.

You can initiate client actions by selecting the endpoint. The list of client actions is OS specific.

To select all the endpoints from the list, select the check box in the header row.

To select an individual endpoint, select the check box in that row.

Viewing status of selected endpoint

To view status of an endpoint, click the name of the endpoint for which you want to view the status. The Endpoint Status page appears displaying detailed status of the endpoint. For more details, see Endpoint Status.

Patch Install

This feature allows you to install the missing patches on the selected endpoints.

To install the missing patches, follow these steps:

1. Log on to the Thirtyseven4 EDR Security Web console.

   Go to **Computer** > **Status**. Click **Patch Install**.

   Patch Install page appears. A list of the missing patches appears.

2. You can filter the list with the help of the four filters described in the following tables:

Severity options:

Severity	Description
Critical	Vulnerability may allow code execution without user interaction.
Important	Vulnerability may result in compromise of the confidentiality, integrity, or availability of user data. The client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability.
Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Unspecified	Vulnerability may result in random malfunctions.

Category options:

Category	Description
Security Updates	A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low.
Update Rollups	A tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a component of a product, such as Internet Information Services (IIS).
Applications	Application (software) is a subclass of computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wishes to perform.
Service Packs	A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.

Feature Packs	New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.
Updates	Updates are code fixes for products that are provided to individual customers when those customers experience critical problems for which no feasible workaround is available.
Definition Updates	A widely released and frequent software update that contains additions to a product's definition database. Definition databases are often used to detect objects that have specific attributes, such as malicious code, phishing websites, or junk mail.
Critical Updates	A widely released fix for a specific problem that addresses a critical, non-security-related bug.
Drivers	Software that controls the input and output of a device.

Restart Required options:

Restart Required	**Description**
All	Display result for all the options.
Not Required	The patch does not require the system restart.
Required	The patch requires the system restart. Restart the system to take the patch effect.
May Require	The patch may require the system restart.

EULA Status options:

EULA Status	**Description**
All	Display result for both the options, Accepted and Not Accepted.
Accepted	End User License agreement is accepted.
Not Accepted	End User License agreement is not accepted.

3. To generate the result with help of filters and/or record details, click **Generate Report**.
4. Select the **Show patches within subgroup** check box to display the name of the patches that are in the subgroup from the list of the endpoints without actually exploring the network.
5. To change the restart setting, click **System Restart Settings** button. Restart settings are applicable only if the patch requires the system restart.

6. Select the **Allow auto-restart the system** check box to restart the system automatically. Clear the check box to restart the system manually.
7. From the missing patches list, select the patches that you want to install.
    a. Click the patch name.

       The Patch Details dialog appears.

    b. In the list, click the number in the column **No. of Endpoint Affected**. Endpoint(s) affected dialog appears.

    Select the endpoints where you want to install the missing patch.

    Click **Apply**. The list of endpoints is saved. The count in the column **No. of Endpoint selected** is updated.
8. Click **Start Install**. To cancel the selection, click **Refresh.**

Update Agent

Important

Only Windows machine can be assigned the update agent role. So, Windows client system is a must for the update agent.

Update Agent helps you to download and manage the updates for Thirtyseven4 EDR Security. It provides you the flexibility to download the updates on a single machine. All the Thirtyseven4 EDR Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Thirtyseven4 EDR Security for enhancements or bug fixes.

Viewing Update Agent Status

You can view information of all types of updates downloaded by the Update Agent.

To view the update agent status, follow these steps:

1. On the Status page, identify and click the endpoint name with update agent role.
2. The Endpoint Status page appears. You can see the label as Update Agent. Click the **Switch to Update Agent** button.
3. The Update Agent page appears. The endpoint name and IP address of the endpoint where update agent is installed is displayed.
4. In the Status tab, the status of the update Agent is shown in the tabular format with the following details:

Fields	Description
Product Name	Displays the name of the Thirtyseven4 EDR product for which update can be downloaded.
Version	Displays the version of the Thirtyseven4 EDR product.
Service Pack	Displays information about the service pack.
Virus Database Date	Displays the updated Virus Database date.

Note
A label 'Outdated' is displayed for the product only if the product is not updated since last 72 hours.

5. You can do one of the following:
   - **Update Now** – Click this button to send a Notification to the Update Agent to download the updates.
   - **Rollback** – Click this button to take the Update Agent back to the previous update state.

Update Agent Settings

To do the update agent setting, follow these steps:

1. On the Status page, identify and click the endpoint name with update agent role.
2. The Endpoint Status page appears. You can see the label as Update Agent. Click the **Switch to Update Agent** button.
3. The Update Agent page appears. The endpoint name and IP address of the endpoint where update agent is installed is displayed.
4. In the Settings tab, you can see the following list of settings with expand sign and toggle button. Expand and enable settings.
   - Update Settings
   - Proxy Settings
5. To save the changes, click **Save**.

Update Settings

1. Under Update Type, you can select either of the following update options:

- **Automatic**: Select this option to enable automatic update of Thirtyseven4 EDR Security. However, this feature is enabled by default. It is recommended that you do not disable this feature.
- **Custom**: If you select this option, configure the following options:
  a. In **Frequency**, select either the Daily or Weekly option. If you select the Weekly option, select the weekday from the list.
  b. In **Start At**, set time in hours and minutes.
  c. If you want to repeat the update of the Update Agent, select the Repeat Update check box and set the frequency in hours to repeat the update.

2. Select the update mode from the following options:

- **Download from Internet Center**: Helps you download the updates from the default Internet Center.
- **Download from Specified URL**: Helps to obtain the updates from a specified endpoint that has the updates downloaded by the connected system.
  a. In the **Server** text box, type the URL.
  b. In the **Port** text box, type the port number.

  Note
  The msg32.htm file should be present at the update location in the system with Internet connection. To create the msg32.htm file, rename a text file as msg32.htm file.

- **Pick from specified path**: Helps you pick the updates from a specified local folder from your computer without Internet connection. You can specify the path of the local folder from where the updates are to be copied.
  For example, if you have downloaded the updates on other system, you can copy them into a CD/DVD or pen drive and then paste in the local folder. Update Agent will fetch the updates from this local folder path.
  a. Select the **Pick from specified Path** option.
  b. Type the path to the folder from where the updates need to be copied.
  c. Select the updates available for download from the list.
  d. Under Other Settings, select the **Download the EDR security service pack** check box. This feature is enabled by default.
  e. Select the **Always take backup before downloading new update** check box. Helps you take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. This feature is enabled by default.

f. Select the **Restrict download speed (kbps)** check box if you want to restrict the download speed. Enter the speed in the text box.

g. Select the **Delete report after** check box. This helps you delete the reports as per the time interval selected by you. This feature is enabled by default. The default value of time interval is 10 days.

h. Verify the path mentioned in **Download updates to** box. All the Thirtyseven4 EDR Endpoints Security products will take the updates from this centralized location.

Proxy Settings

1. Select Proxy Type from the list.
2. In the **Server** text box, type the IP address of the proxy server or domain name (Example: proxy.yourcompany.com).
3. In the **Port** text box, type the port number of the proxy server (Example: 80).
4. Under Authenticate in case of firewall or proxy server section, type your logon credentials in the **User Name** and **Password** boxes to authenticate.

Action Log

View Action Log of selected endpoint

You can view the action log (history) of all actions performed on the endpoints. To view the action log, click the row of the endpoint for which you want to view the history. The action log appears in the lower pane of the page in the tabular format. The Action Status column displays the corresponding status of the action. The status and meanings are as follows:

- Queued – After initiating, the action is in the queued state until the endpoint pulls the action.
- Success – The initiated action has been reached the endpoint. The endpoint has acknowledged the request to the server.
- Skipped – The multiple requests for the same action are skipped.
- Failed –The scenario can be one of the following:
    - The similar action is in progress at the endpoint side.
    - The antivirus is not installed so cannot carry the selection action.
    - The action is not applicable for the selected endpoint.

    By default, you can view the action log of last 7 days. You can view the log for last 3,7, and 15 days by selecting from the list.
    The activity logs will be deleted as per settings done in Admin > Settings.

If the antivirus is not installed, the action logs about only the following actions are displayed:

- Enumerate Network
- Remote Uninstall
- Remove selected endpoints
- Temporary Device Access
- Provides the facility of automatically updating Thirtyseven4 EDR Security for enhancements or bug fixes.

Endpoint Status

You can keep a watch on the system information, hardware information, and software installed. You can also view the hardware changes, if any, that are made to the configuration of the systems in your network. You can also keep a tab on the list of the endpoints where the changes have been carried out.

To view status of an endpoint, click name of the endpoint for which you want to view the status. The Endpoint Status page appears displaying detailed status of the endpoint.

The System Details tab displays the system information in detail. OS Product key of the Windows OS appears.

Note

The OS Product key is available only in the clients with Windows Vista and above operating systems.

The Hardware and Software details tab will be displayed only after Asset scan. For more information, see Asset Management.

The Hardware Details tab displays the hardware information in detail.

The Software details tab displays the details of software installed on the system.

Note

The MS Office Product key is available only for MS Office 2010 and above.

The Product key of MS Office is not available in the clients with MAC operating system.

The license status of MS Office appears in the License column.

The following table mentions possible License status and their description in the tool-tip for MS Office.

License status	Description
Unlicensed	The product is not licensed.

License status	Description
Licensed	The product is licensed.
OOBGrace	The MS Office license is in the grace period.
OOTGrace	The MS Office license requires reactivation.
NonGenuineGrace	The MS Office license has failed online validation and is in the grace period.
ExtendedGrace	The grace period of the MS Office license is extended.
Notification	The MS Office license is either out of the grace period or failed validation.

Export

1. To export status in the CSV format, click **CSV** button. Export To CSV File dialog appears.
2. Select one of the following,
   - **Export data displayed on Status page only**. If you select this option, .csv is downloaded.
   - **Export comprehensive data of endpoints listed on Status Page**. The data includes System details, Software and Hardware details and System User Details. If you select this option, Comprehensive Asset Reports zip file is downloaded.
3. Click **Export**.

Client Action

Using the options in the Client Action list, you can perform different actions on the endpoints.

You can remotely initiate scan for individual endpoints or endpoints in a group, customize scan settings, and stop scanning as per your preference. You can improve the performance of your endpoints by initiating Tune-up scan which can clean up disk space, registry entries, and schedule defragmentation at next boot. You can update the Thirtyseven4 EDR Security virus database for the endpoints.

The following table shows a comparison of the features in Client Action that are applicable for different Thirtyseven4 EDR Security clients on different operating systems. Only supported feature list will be displayed as per the OS.

Features	Clients		
	Windows	Mac	Linux
Scan	Yes	Yes	Yes
Update	Yes	Yes	Yes
Tuneup	Yes	No	No
Temporary Device Access	Yes	Yes	No
Enumerate Network	Yes	No	No
Remote Uninstall	Yes	Yes	Yes
DLP	Yes	Yes	No
Update Agent Role	Yes	No	No
Delete Backup Data	Yes	No	No
Assign Custom Policy	Yes	Yes	Yes
Upgrade Clients	Yes	Yes	No
Application Control	Yes	No	No
Vulnerability Scan	Yes	No	No
ETH Scan	Yes	No	No
Move to Group	Yes	Yes	Yes
Remove Selected Endpoint(s)	Yes	Yes	Yes

The Client Actions button helps you to initiate actions on the selected endpoints.

Scan

This feature allows to initiate scanning on remote endpoints. You can initiate a manual scan with preconfigured policies or custom scan. This feature reduces the additional task of personally overseeing each target endpoint.

To initiate scanning, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **Scan**.
3. In the Please Select list, select **Start Scan**.
4. Click **Submit**.
   Start Scan dialog appears.
   Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.
   You can stop scanning by clicking **Stop Scan** at any time you prefer.
   You can customize the scan settings if required.
5. To customize the scan settings, click **Scan Settings**.
6. In the Scan Settings section, do the following:
    a. In Scan type section, select either **Quick Scan** or **Full System Scan**. Quick Scan includes scanning of the drive where operating system is installed, and Full System Scan includes scanning of all fixed drives.
    b. Select **Scan Priority**. The Scan Priority is Normal by default. You can change the priority to Low or High, if required.
    c. Select either **Automatic** or **Advanced** scan mode.
    Automatic scanning involves optimum scanning and is selected by default.
    When the Advanced scan mode option is selected, all the related attributes get enabled. Do the following:
        a. From the **Select the items to scan** options, select either **Scan executable files** option or **Scan all files** option. Scanning of all files takes a longer time.
        b. The **Scan packed files** and **Scan archive files** check boxes are selected, by default. You can select the **Scan mailboxes** check box if required.
        c. In **Archive Scan Level**, set the scan level. You can set the level for scanning in an archive file up to 16. The default scan level is 2. Increasing the default scan level may affect the scanning speed.

d. To remove an infected file from your system, Select action from the drop down list:
– Select action when a virus is found in the archive file, whether you want to **delete, quarantine,** or **skip** the file.
– Select action when a virus is found in your active folder/drives, whether you want to **delete, quarantine,** or **skip** the file.

d. Under Antimalware Scan Settings, Perform Antimalware scan is selected, by default.

e. Select action when a malware is found, whether you want to clean or skip the file. The action selected here will be taken automatically.

f. Under Boot Time Scan Settings, Perform Boot Time Scan is selected, by default. The Select Boot Time Scan Mode option is activated. Select one of the following scan options:

- Quick Scan
- Full System Scan

g. After configuring the scan setting, click **Apply Changes**.

The new setting is applied. You can reset the Scan setting to default with Reset button, if required.

Note

- *Scan packed files, Scan mailboxes, Antimalware Scan Settings, and Boot Time Scan Settings are available only in the clients with Windows operating systems.*
- *Notification for Scan from the Thirtyseven4 EDR Security console will not be sent if the user is not logged on to the Mac system.*

Update

Thirtyseven4 EDR releases updates regularly to fix technical issues and provide protection against new threats. Hence, it is recommended that you update the virus definitions of your software protection regularly. Using this feature, you can take the update remotely.
To take the update, follow these steps:

1. On the Status page, select the endpoints you want to update.
2. The client action bar is enabled above the table. In the Client Actions list, select **Update**.
3. Click **Submit**. The action will be initiated on the client as per the set polling interval. The selected endpoints are updated with the latest virus definitions.

Roaming Service

This feature allows you assign Roaming Service manually to the selected endpoints.

To assign Roaming Service, you must enable Roaming Service with Manual mode. To enable Roaming Service, see Roaming Service.

Assign Roaming Service

To assign Roaming Service, follow these steps:

1. On the Status page, select the endpoints you want to assign Roaming Service.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **Roaming Service**.
3. In the Please Select drop down, select **Assign**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.

   The Roaming Service is assigned to the selected endpoint. On the Status page, in the Endpoint status column the status appears as Roaming for the respective endpoint.

   As the Roaming Service is assigned, the client will be able to communicate to the Server even if moves out of organizational network.

Revoke Roaming Service

This feature allows you to revoke Roaming Service for the selected endpoint.

To revoke Roaming Service, follow these steps:

1. On the Status page, select the endpoints for which you want to revoke Roaming Service.
2. In the **Client Actions** drop down, select **Roaming Service**.
3. In the **Please Select** drop down, select **Revoke.**
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.

   The Roaming Service is revoked for the selected endpoints.

   As the Roaming Service is revoked, the client will not be able to communicate to the Server if moves out of organizational network.

Patch Scan

This feature allows you to scan the missing patches on the selected endpoints in the network.

To initiate scanning of the missing patches, follow these steps:

1. Log on to the Thirtyseven4 EDR Security Web console. Go to **Computer** > **Status**.
2. On the Status page, select the endpoints you want to scan.
3. The client action bar is enabled above the table. In the Client Actions drop down, select **Patch Scan**.
4. In the Please Select drop-down menu, select **Start Scan**.
5. Click **Submit**.

   You can stop scanning by clicking **Stop Scan** at any time you prefer.

Tuneup

This facility improves the performance of the endpoints by defragmentation and by cleaning unwanted and junk files and invalid and obsolete registry entries. While you work in applications, computers write junks on the drives or when you visit any Websites, the temporary files are created on your computer. Such junks and files occupy spaces in the memory resulting in slowing down of the endpoints. Tuning up your computers cleans up these files by improving their performance.
Tuneup settings allow you to carry out different types of clean-ups such as; disks, registry entries, or schedule a defragmentation at next boot.
Disk Clean up: Helps you find and remove invalid and unwanted junk files from the hard disk. These files consume hard disk space and slow down the system considerably. Disk Clean up deletes these files and provide free space that can be used for other applications and helps in improving system performance. This feature also deletes temporary files, Internet cache files, improper shortcut files, garbage name files, and empty folders.

Registry Clean up: Helps you remove invalid and obsolete registry entries from the system, such entries may appear due to improper uninstallation, non-existent fonts, etc. Sometimes during uninstallation, the registry entries are not deleted. This leads to slower performance of the system. The Registry Clean up removes such invalid registry entries to increase the performance of the system.

Defragment: Helps you defragment vital files, such as page files and registry hives for improving the performance of the endpoint. Files are often stored in fragments in different locations slowing down the system performance. Defragmentation reduces the number of fragments and clubs all the fragments into one contiguous chunk to improve your endpoint performance.

Note
The Tuneup feature is available only in the clients with Windows Desktop operating systems.
The Tuneup feature is not available for Windows Server operating system.

To tune up the endpoints, follow these steps:

1. On the Status page, select the endpoints you want to tuneup.
2. The client action bar is enabled above the table. In the Client Actions dropdown, select **Tuneup**.
3. In the Please Select dropdown, select **Start Scan**.
4. Click **Submit**. Start Scan dialog appears.

   Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.
   Tuneup notifications are sent to the selected endpoints and tune up is performed on those endpoints.
   You can stop Tuneup activity by clicking **Stop Scan** at any time you prefer.
   You can customize the Tuneup settings if required.
5. To customize the Tuneup settings, click **Tuneup Settings**.
6. Select any of the following:
   - Disk Cleanup
   - Cleanup
   - Defragment at next boot

     However, all these options are selected by default.
7. To save your settings, click **Apply Changes**. You can reset the Tuneup settings to default with **Reset** button, if required.

Temporary Device Access

This feature allows you to permit temporary access to a device on the client for a specific period. If a user wants temporary access to a device on the client, the user can send a request to the Administrator to grant temporary access. The Administrator will generate OTP and will share with the user. The client uses this OTP to access the device for the specific period.
To enable Temporary Device Access, follow these steps:

1. On the Status page, select the endpoints to send the temporary device access request.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **Temporary Device Access**.
3. Click **Submit**.
4. On the Temporary Device Access dialog, in the **Allow temporary access for** list, select minutes.
5. In the **Use OTP within** list, select minutes.

6. Click **Generate OTP**. The OTP appears.
7. Click **Notify By Email** and the email containing the OTP is automatically received by the client. Temporary access is allowed as per the settings effective from that minute. The action will be initiated on the client as per set polling interval.
   At the client side, after successful validation of the OTP, temporary device access is enabled for the specific period.

Enumerate Network

This feature allows you to get a list of all the unmanaged endpoints available in the client network.
To generate a list of unmanaged endpoints, follow these steps:

1. On the Status page, select the endpoints to send the request.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **Enumerate Network**.
3. Click **Submit**. The action will be initiated on the client as per set polling interval.
   The enumeration result will appear on the Thirtyseven4 EDR console dashboard based on the Heartbeat interval set for the client. You can view the enumeration results on the dashboard widget only.

Remote Uninstall

With Remote Uninstall, you can initiate remote uninstallation of Thirtyseven4 EDR client along with the antivirus program from the computers on your network.
To uninstall the client through Remote Uninstall, follow these steps:

1. On the Status page, select the endpoints you want to uninstall.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **Remote Uninstall**.
3. In the **Please Select** dropdown, select Start.
4. Click **Submit**.
   The uninstallation initiates on the selected endpoints as per set polling interval.
   To stop the remote uninstallation, In the **Client Actions** list, select **Remote Uninstall > Stop**.
   Click **Submit**. The Stop command will be executed only if the uninstallation is not started.

DLP

Assign DLP License

This feature allows you to assign Data Loss Prevention (DLP) license to the selected endpoint.
To assign the DLP license, follow these steps:

1. On the Status page, select the endpoints you want to assign the DLP license.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **DLP**.
3. In the **Please Select** dropdown, select **Assign DLP License**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.
   The DLP license is assigned to the selected endpoint. On the Status page, the legend for DLP License Assigned is displayed for the respective endpoints.

Revoke DLP License

This feature allows you to revoke the DLP license to the selected endpoint.
To unassign the DLP license, follow these steps:

1. On the Status page, select the endpoints you want to unassign the DLP license.
2. In the **Client Actions** dropdown, select **DLP**.
3. In the **Please Select** dropdown, select **Revoke DLP License**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.
   The DLP license is unassigned to the selected endpoint.

Data-At-Rest Scan

Using Data-At-Rest Scan, you can scan and detect any confidential data present in your endpoints and removable devices. You can scan the desired location such as drive, folder, or removable devices on the endpoints and detect the confidential or sensitive information present. You can view the information related to the detected confidential data such as the file path, threat type, and matched text.

Note
To perform Data-At-Rest scan, you must enable DLP on the endpoints.

Start Data-At-Rest scan

To initiate scanning, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **DLP**.
3. In the **Please Select** dropdown, select **Start Data-At-Rest Scan**.
4. Click **Submit**.
   Start Scan dialog appears.
   Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.
   The selected endpoints are scanned for compliance.
   You can customize the Data-At-Rest scan settings if required.

Customize the DAR scan settings

1. To customize the DAR scan settings, click Data-At-Rest Scan Settings and select one of the following:
   - **Quick Scan**: Select this option to scan the drive on which your operating system is installed.
   - **Full System**: Select this option to scan all the drives.
   - **Scan Specific Folder(s)**: Select this option to scan a particular folder(s). To scan specific folder, follow these steps:
     a. Click Configure.
     b. Enter the path of the folder that you want to scan.
     c. Click **Add**.
     d. You can also choose to scan the subfolders by selecting the **Include Subfolder** check box.
     e. You can also remove a path from the list by clicking **Delete**.
     f. Click **Apply**.
2. Select **Scan Priority**. The Scan Priority is **Normal** by default. You can change the priority to Low or High, if required.
3. In the Select data to scan section, click the **File Types** tab.
4. Select the file types (format) that you want to scan.
5. Click the **Confidential Data** tab.
6. Select the **Confidential Data to scan**.
7. Click the **User Defined Dictionaries** tab and select the User Defined Dictionaries to scan.
8. Click **Apply Changes**.
9. You can reset the DAR scan settings to default with **Reset** button, if required.

10. Click **Start Scan**.

Note
Email Notifications are not supported for Data-At-Rest Scan feature.
Data-At-Rest Scan feature will be available only if DLP feature pack is enabled for that Thirtyseven4 EDR server.

Exclusion

You may exclude folders for scanning.
To exclude the folder, enter the name of the folder in the text box and click **Add**.
To remove the folder from the excluded folders list, select the folder from the list and click **Delete**.

Stop Data-At-Rest scan

To stop Data-At Rest scanning, follow these steps:

1. On the Status page, select the endpoints you want to stop Data-At-Rest scan.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **DLP**.
3. In the **Please Select** dropdown, select **Stop Data-At-Rest Scan**.
4. Click **Submit**.
   The Stop command has been sent.

Update Agent Role

This feature allows you assign update agent role to the selected endpoint. The Update Agent downloads and manages the updates for Thirtyseven4 EDR Security. The Update Agent provides you the flexibility to download the updates on a single machine. All the Thirtyseven4 EDR Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Thirtyseven4 EDR Security clients for enhancements or bug fixes.
To assign the update agent role, follow these steps:

1. On the Status page, select the endpoints you want to assign the update agent role.
2. The client action bar is enabled above the table. In the **Client Actions** dropdown, select **Update Agent Role**.
3. In the **Please Select** dropdown, select **Assign**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.
6. The update agent role is assigned to the selected endpoint. On the Status page, the legend for Update Role Assigned is displayed for the respective endpoint.

Revoke Update Agent Role

This feature allows you to revoke the update agent role for the selected endpoint.
To revoke the update agent role, follow these steps:

1. On the Status page, select the endpoints for which you want to revoke the update agent role.
2. In the Client Actions dropdown, select **Update Agent Role**.
3. In the **Please Select** dropdown, select **Revoke**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.
   The update agent role is revoked for the selected endpoint.

Delete Backup Data

Data Backup feature automatically takes a backup of files for ransomware protection. This feature takes backup as per predefined configuration in the Miscellaneous policy. Here you can delete the backup data. For more information, see Miscellaneous policy.
To delete Backup Data, follow these steps:

1. On the Status page, select the endpoints for which you want to delete the backup data.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **Delete Backup Data**.
3. In the **Please Select** list, select one of the following:
   - **Old Backup Data** – Backup taken by the older clients on this endpoint
   - **Current Backup Data** – Backup taken by the current client on this endpoint
4. Click **Submit**. The action will be initiated on the client as per the set polling interval.
   The backup data will be deleted.

Assign Custom Policy

This feature allows you to assign custom policy to the selected endpoint. You can override the settings of Container policy by selecting the custom policies.

To assign custom policy, follow these steps:

1. On the Status page, select the endpoints you want to assign the policy.
2. The client action bar is enabled above the table. In the Client Actions list, select **Assign Custom Policy**.
3. Click **Submit**. The Assign Custom Policy dialog appears. The list of custom policies appears. Select the policies and click **Assign**.

The policies are assigned to the selected endpoint. You can view the assigned policies on the Status page and in the Assign Custom Policy dialog.

Upgrade Clients

To upgrade the clients, follow these steps:

1. On the Status page, select the endpoints you want to upgrade the clients.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **Upgrade Clients**.
3. Click **Submit**. The action will be initiated on the client as per the set polling interval. The client will be upgraded with the latest version.

Application Control

This feature allows you to check whether security compliance policies framed by your organization are being followed on each endpoint. It also helps you in verifying whether endpoints have any unauthorized applications other than the authorized ones running on them.
The Application Control scan is done in the following two ways,

- When you request the scan through Client Action. For details, see Application Control Scan explained below.
- When you set the Application Control policy. 'On access' reports are generated in this case. For details, see Application Control policy.

Application Control Scan

To initiate scanning, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the **Client Actions** dropdown, select **Application Control**.
3. In the **Please Select** list, select **Start Scan**.
4. Click **Submit**. Start Scan dialog appears.
5. Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval. You can stop scanning by clicking **Stop Scan** at any time you prefer. You can customize the scan settings if required.
6. To customize the scan settings, click **Application Control Settings**.
7. Select one of the following scan options:

- **Unauthorized applications**: Helps you initiate scanning only for the unauthorized applications present on a client machine.
- **Unauthorized and authorized applications**: Helps you initiate scanning for both, unauthorized and authorized applications present on the client machine.
- **All installed applications**: Helps you initiate scanning for all applications installed on a client.
  Scanning by first two options may take longer time.

8. Select Scan Priority. The Scan Priority is Normal by default. You can change the priority to Low or High, if required.
9. After configuring the scan setting, click Apply Changes.
   The new setting is applied. You can reset the Scan setting to default with Reset button, if required.

Vulnerability Scan

This feature helps you to set vulnerability scan for the clients so that the clients are scanned for possible vulnerabilities. This scan helps for vulnerability assessment of the operating system on the client.

To initiate vulnerability scan, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **Vulnerability Scan**.
3. In the Please Select list, select **Start Scan.**
4. Click **Submit**.

   Start Scan dialog appears.
5. Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.

   You can stop scanning by clicking **Stop Scan** at any time you prefer.

   You can customize the vulnerability scan settings if required.
6. To customize the scan settings, click **Vulnerability Scan Settings**.
7. Under Scan Type, select one of the following options to scan for vulnerability against following software vendors
   - Microsoft applications and other vendor applications
   - Microsoft applications only

- Other vendor applications only

8. The **Scan Priority** is Normal by default. You can change the priority to Low or High, if required.
9. The **Scan Severity** is Low by default. You can change the priority to Medium or High, if required.
10. After configuring the scan setting, click **Apply Changes**.

The new setting is applied.

You can reset the Scan setting to default with Reset button, if required.

ETH Scan

Endpoint Threat Hunting (ETH) Scan is an easy way to search for files that match malicious hashes (MD5, SHA1, SHA256) across your network.

You may have hash codes of latest malware. ETH Scan searches those malicious hashes in the endpoints of your network, then action is taken as per your selection, you can quarantine or delete malicious files.

The following 2 modes are available to search the hash types.

Manual Search – If you want to search 1 to 5 entries at a time, select Manual Search.

Bulk Search - If you want to search more entries, select Bulk Search. You can search for 5 to 20 entries at a time with Bulk Search. Multiple Hash codes are searched by uploading a CSV file.

Manual Search

To initiate scanning in Manual Search mode, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **ETH Scan**.
3. In the Please Select list, select **Start Scan**.
4. Click **Submit**.

   Start Scan dialog appears.
5. In the **New Scan** tab, enter **Search Name** and **Description**.
6. Select **Action** from the list. You can select **Quarantine** or **Delete** or **No action** option.

   Manual Search mode is selected by default. With Manual Search, you can search 1 to 5 entries at a time.

7. Enter **Hash Code** that you want to search in the text box. The **Hash Type** of the code appears in the corresponding box.
8. Click **+Add Entry** to add search entry.

   You can enter maximum 5 search entries in Manual Search mode.

   You can delete the search entry with help of delete icon of the corresponding entry.
9. Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.

Bulk Search

To initiate scanning in Bulk Search mode, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **ETH Scan**.
3. In the Please Select list, select **Start Scan**.
4. Click **Submit**.

   Start Scan dialog appears.
5. In the **New Scan** tab, enter **Search Name** and **Description**.
6. Select **Action** from the list. You can select **Quarantine** or **Delete** or **No action** option.
7. Select Search Mode as **Bulk Search** .
8. Download the CSV template from the link.
9. Fill hash codes that you want to search in the CSV file.
10. Save the file. The file size must be less than or equal to 1 MB.
11. Click **Upload CSV file** to upload the file. The file name appears when the file is uploaded successfully.
12. Click **Start Scan**.

Existing Scan

You can initiate scan on the existing search also.

To initiate scanning of existing search, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **ETH Scan**.

3. In the Please Select list, select **Start Scan**.
4. Click **Submit**.

   Start Scan dialog appears.
5. In the **Existing Scan** tab, you can view the following information about Search.

Fields	Description
Date & Time	Displays the date and time of the Search.
Search Name	Displays the name of the Search.
Description	Displays the description of the Search.
Action	Displays the action taken on the files.

6. Select the Search you want to initiate.
7. The action bar is enabled above the table. Click **Start Scan**.

Notes

The Endpoint Threat Hunting feature is available only in the clients with Microsoft Windows operating system.

Move to Group

This feature allows you to move the selected endpoint to a group.
To move the endpoint, follow these steps:

1. On the Status page, select the endpoints you want to move.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **Move to Group**.
3. Click **Submit**. The Assign to Group dialog appears.
4. Select a group/subgroup where you want to move the selected endpoint.
5. Click **Move**.
6. A confirmation message appears. Click **OK**.
   The policies of the parent group are applied to the moved endpoint.

Remove Selected Endpoints

This feature allows you to remove the clients from a group.
To remove the client, follow these steps:

1. On the Status page, select the endpoints you want to remove.
2. The client action bar is enabled above the table. In the **Client Actions** dropdown, select **Remove Selected Endpoint(s)**.
3. Click **Submit**.
4. A confirmation message appears. Click **OK**.
   The endpoints are removed.

Debug Log

Important: This feature is applicable only for the Mac clients.

This feature allows you to enable Web Security logs under the product installation directory. If any issue occurs on the Mac client related to Web Security, then enable debug log from here. Generate the issue and collect the logs from /Library/Application Support/Thirtyseven4 EDR/Thirtyseven4 EDR/logs.
The log file name is 'emlprod.logs'. Share the emlprod.logs file with Thirtyseven4 EDR team for further analysis.

Enable Debug Logs

To enable Debug Logs, follow these steps:

1. On the Status page, select the Mac endpoints for which you want to enable Debug Logs.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **Debug Logs**.
3. In the Please Select drop down, select **Enable**.
4. Click **Submit**.

As per heartbeat interval set for the client, emlprod.logs start to generate.

Thirtyseven4 EDR recommends disabling the 'Debug Logs' once the required logs have been collected. Failure to do so may result in a slowdown of the Mac system or potential system hang-ups if the log size increases.

Disable Debug Logs

To disable Debug Logs, follow these steps:

1. On the Status page, select the Mac endpoints for which you want to disable Debug Logs.
2. The client action bar is enabled above the table. In the Client Actions drop down, select **Debug Logs**.
3. In the Please Select drop down, select **Disable**.
4. Click **Submit**.

As per heartbeat interval set for the client, log creation will be stopped.

Deployment

The Deployment page helps you to deploy the EDR Security client on different endpoints.

Deployment Methods

Select one of the following methods to deploy the EDR Security client as applicable. A brief about each method is mentioned below.

- Online Installer: Create and download client installer for manual installation.
- Standalone Installer: Download Standalone Installer and then create a client installer.
- Email Install Link: Send e-mail notification containing URL to install the client.
- Remote Installer: Download Remote Installer, which helps you to remotely deploy Thirtyseven4 EDR Security clients on Microsoft Windows and Mac endpoints.
- Active Directory: Download Active Directory Tool, which helps you to deploy Thirtyseven4 EDR Security clients with help of active directory synchronization. The following table shows different operating systems that support the client deployment methods:

Features	**Clients**		
	Windows	**Mac**	**Linux**
Online Installer	Yes	Yes	Yes
Standalone Installer	Yes	Yes	Yes
Email Install Link	Yes	Yes	No
Remote Installer	Yes	Yes	No
Active Directory	Yes	No	No

This page helps you to create and download the Client Installer for manual installation of client on different endpoints.

Automatic uninstallation of Thirtyseven4 EDR clients

If you start deploying client on the endpoints which already has on-premises Thirtyseven4 EDR client, the on-premises client will be uninstalled and Thirtyseven4 EDR Security client will be

installed on the endpoint.
This feature is available in the clients with Windows and Mac operating systems.

Supported Thirtyseven4 EDR versions

- Windows client – Thirtyseven4 EDR version 6.0 and later
- Mac client – Thirtyseven4 EDR version 6.4 and later

System Requirements for Thirtyseven4 EDR Server

Server that supports up to 0 to 5000 endpoints

- Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 60 GBs or above
- Available RAM: 8 GBs or above
- Processer: 4 Core (x86-64), 2.60GHz or above

Server that supports up to 5001 to 15000 endpoints

- Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 100 GBs or above
- Available RAM: 16 GBs or above
- Processer: 8 Core(x86-64), 2.60GHz or above

Server that supports up to 15001 to 25000 endpoints

- Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 150 GBs or above
- Available RAM: 32 GBs or above
- Processer: 16 Core(x86-64),2.60GHz or above

System Requirements for Thirtyseven4 EDR Clients

For Installing Thirtyseven4 EDR Security client through client install utility, the System requirements are as follows:

Any one of the following operating systems:

Windows OS

- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)

- Microsoft Windows 7 Home Basic/ Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (64-bit)
- Windows 10 November 2019 Update
- Microsoft Windows Server 2022 Standard / Datacenter / Essentials

Note:

- For Windows 2008 Server R2, you need to install updates, please See KB4474419 and KB4490628.
- For Windows 7, you need to install updates, please See KB4474419 and KB4490628.
- For Windows 2016, Windows Server 2019 and Server 2022, you need to uninstall Windows Defender.

MAC

Processor: Intel core or Apple's M1, M2 chip compatible

Mac OS: X 10.12, 10.13, 10.14, 10.15, 11, 12, 13, and 14

Linux 32-bit

- GNU C Library 2.5 and later
- SAMBA version 4.16 and earlier

Supported Distributions for Thirtyseven4 EDR client:

- Debian 9, 10
- Ubuntu 14.04,16.04
- Boss 6.0
- Linux Mint 19.3

Linux 64-bit

- GNU C Library 2.5 and later
- SAMBA version 4.16 and earlier

Supported Distributions for Thirtyseven4 EDR client:

- Fedora 30, 32
- Linux Mint 19.3, 20
- Ubuntu 16.04, 18.04, 20.4, 22.04
- Debian 9, 10
- CentOS 7.8, 8.2
- RHEL 7.5, 7.8, 8.2, 8.6 Enterprise
- SUSE Linux 12. SP4 / Enterprise Desktop 15
- Rocky Linux 8.4
- Boss 6.0, 8.0, 9.0
- Oracle Linux 7.1, 7.9 and 8.1

General Requirements

Windows

Processor

- Minimum: 1 GHz 32-bit (x86) or 64-bit (x64) processor
- Recommended: 2 GHz 32-bit (x86) or 64-bit (x64) processor

RAM

- Minimum: 1 GB
- Recommended: 2 GB free RAM

Hard disk space

- 3200 MB free space

Web Browser

- Internet Explorer 7 or later

Network protocol:

- TLS 1.2

- MAC

Processor

- Intel core or Apple's M1, M2 chip compatible

RAM

- Minimum: 512 MB
- Recommended: 2 GB free RAM

Hard disk space

- 1200 MB free space

Linux

Processor

- Intel or compatible

RAM

- Minimum: 512 MB
- Recommended: 1 GB free RAM

Hard disk space

- 1200 MB free space

Note:

- For installing the client on Window 2016 OS, uninstall Windows Defender with the following link, See docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-on-windows-server-2016#install-or-uninstall-windows-defender-av-on-windows-server-2016
- From Thirtyseven4 EDR Cloud 1.6 onwards, Apple M1 chip is supported and from version 1.8 onwards, Apple M1, M2 chip is supported.
- From version 1.6 onwards, Thirtyseven4 EDR Security Cloud uses only SHA2 Certificate for code-signing. For more details on patches mandated by Microsoft, click here https://bit.ly/3vqRhKU

Online Installer

The Online Installer will take you to next dialog to build Client Installer set up. This may take a longer time to download the Client Installer set up.
To create a new client installer, follow these steps:

1. Click the **Create Client Installer** button to create the Client Installer.
2. In the Create Client Installer window that opens, enter the required information in the **Create Installer, Proxy Settings, Set Password** tabs.
3. Click **Create**.
   The Client Installer is ready for download.
   To install Thirtyseven4 EDR Client, see Installing Thirtyseven EDR Security Client.

Standalone Installer

The standalone installer will download a Client Installer. If network speed is slow and you want to create client installer faster, use this option. This requires at least one system with Windows platform.
To create a new client installer, follow these steps:

1. Click **Standalone Installer** button.
2. The Client Installer zip file is downloaded. Extract the files.
3. Execute the Installer.
4. In the Client Installer, enter the required information in the Create Installer, Proxy Settings and Password tabs.
5. Click **Create**.
   A help file is provided in the Client Installer.

To install Thirtyseven4 EDR Security Client, see Installing Thirtyseven4 EDR Security Client.

Email Install Link

This facility allows you to send an email with a Client Installer download link for client installation to the endpoints.
To send Email with the link, do the following,

1. In the To text box, enter the Email address.
2. Click **Send Email**. A confirmation message appears.
3. Click **OK**. The Email is sent from the Thirtyseven4 EDR console.

Installing Thirtyseven4 EDR Client on Windows

1. Open the link in the Email on Windows system.
2. Download Windows client. The cainstlr.zip file is downloaded.
3. Extract the zip file.
4. Execute camininst.exe file. This installs clients on the system.
5. After Thirtyseven4 EDR client installation is finished, the Thirtyseven4 EDR Antivirus installation will be initiated by the Thirtyseven4 EDR client.

Installing Thirtyseven4 EDR Client on Mac

1. Open the link in the Email on Mac system.
2. Download Mac client. The tar file is downloaded.

3. Extract the tar file.
4. Execute MCLAGNT.DMG file. This installs clients on the system.
5. After Thirtyseven4 EDR client installation is finished, the Thirtyseven4 EDR Antivirus installation will be initiated by the Thirtyseven4 EDR client.

Remote Installer

This page helps you to download **Remote Installer Utility,** which allows you to remotely deploy Thirtyseven4 EDR Security on all supported Windows and Mac endpoints.

Installing Thirtyseven4 EDR Windows Client

To do remote Installation on multiple Windows endpoints, follow these steps:

1. Download Remote Installer.
2. Run Remote Installer.
3. You can initiate remote installation in one of the following ways:
   - Add endpoints by selecting from the list
   - Add by IP Address
4. Enter the IP Address.
5. Click **Add** to add endpoints.
6. In the Add User dialog, type the **User Name** and **Password** with Administrator privilege.
7. Click **Finish** to add all selected endpoints to the installation list.
8. Click **Install** to initiate installation.
   This feature allows you to deploy the client on all supported Windows operating systems at a time.

Installing Thirtyseven4 EDR Mac Client

You can install Thirtyseven4 EDR Mac client in one of the following ways:

- Installing using Apple Remote Desktop or Casper
- Connecting remotely using Secure Shell
    - Using Terminal (for Mac and Linux OS)
    - Using PuTTY (for Windows OS)

Creating Mac Client Installer

To create Mac client installer, follow these steps:

1. On the Thirtyseven4 EDR Security, go to **Deployment**.
2. In the Client Installer tab, click **Create Client Installer** button. The Create Client Installer dialog opens.
3. Enter **Package Name** and select **Group**.
4. In the **OS platform** list, select Mac.
5. Select validity period in the list box. The validity period can be of 30, 60 or 90 days.
6. Click **Create**. The .TAR file is created.
   The installer without AV setup is created and appears in the list on Deployment > Client Installer page. You can download this installer.

Note
With Standalone Installer, you can create Mac client installer with antivirus setup.

Installing using Apple Remote Desktop or Casper

Apple Remote Desktop (ARD) helps you to connect to the Mac client computers remotely in the network, send software to them, install software on them, help other end users in real time, and perform various tasks.

Prerequisites

Before you install Thirtyseven4 EDR Mac client, ensure the following requirements.

- The administrator computer with ARD or Casper installed must have Mac OS X 10.9 or later / OS X server.
- Mac Thirtyseven4 EDR Client installer must be created on Thirtyseven4 EDR Security. To know about how to create client installer, see Creating Mac client mentioned above.
- Administrator must have an account on the Mac client computers with admin privileges.
- Enable Remote Management on the Mac client computers.
- Your administrator computer must have Packages installed on it. Packages is a Mac OS application that helps you to create bundle for your payload and installation. To download Packages, visit http://s.sudre.free.fr/Software/Packages/about.html.
- For macOS Catalina and above only, do the following on your Mac system,
  1. Open System Preferences.
  2. Go to **Security & Privacy > Privacy** tab.
  3. Click the **lock** icon and provide password if it is locked.
  4. Select **Full Disk Access** in the left pane.
  5. Add the following process in the given path and then select the processes in the **Security & Privacy Full Disk Access** window,

/Library/PrivilegedHelperTools/fr.whitebox.packages/packages_dispatcher

Installing Mac client using Apple Remote Desktop or Casper

This procedure helps you install Mac client on the remote Mac client computers using ARD or Casper. For more details, you may refer the documentation of the respective software applications.

Creating Mac Client Package

1. On the Thirtyseven4 EDR Security, download UEMREMOTEINST.TAR from the URL: http://updates.thirtyseven4.com/builds/thirtyseven4/uemcp/en/UEMREMOTEINST.tar
2. Download Mac client installer (with/without AV) from the Thirtyseven4 EDR server. These builds will be in the TAR format.
3. Rename the Mac client installer as follows:
   Mac client installer (without AV) – MCCLAGNT.TAR
   Mac client installer (with AV) – MCCLAGAV.TAR
4. Extract UEMREMOTEINST.TAR.
5. Copy MCCLAGNT.TAR or MCCLAGAV.TAR to '/UEMREMOTEINST'.
6. Open Terminal.app on the administrator Mac computer and go to the UEMREMOTEINST folder.
7. Enter the following commands.
   cd ./Remote_Installation/PKG
   sudo sh ./ClientAgentInstaller/CreatePackage.sh

Note
Administrator rights are required for executing this command.

When the package creation completes successfully, ClientAgentInstaller.pkg file is created in the ./Remote_Installation/PKG/ClientAgentInstaller/ folder.

If the Client Packager is failed to create on macOS Catalina and above, do the following,

1 Open **System Preferences**.

2 Go to **Security & Privacy > Privacy** tab.

3 Click the **lock** icon and provide password if it is locked.

4 Select **Full Disk Access** in the left pane.

5 Select the **packages_dispatcher** check box.

6 Now again try to create Client Packager, it will be created successfully.

Deploying Thirtyseven4 EDR Mac Client using Apple Remote Desktop

In addition to the Prerequisites described above, follow this prerequisite.

Prerequisite

Before deploying Thirtyseven4 EDR Mac client, ensure that you get Apple Remote Desktop (ARD) tool installed on your administrator computer. To download ARD, visit https://www.apple.com/in/remotedesktop/.

To deploy Thirtyseven4 EDR Mac client using Apple Remote Desktop, follow these steps:

1. Open Apple Remote Desktop.
2. Select the Mac client computers from the list of all available computers and then click ***Install*** to add the package.
3. Click the plus (+) sign to locate and add ClientAgentInstaller.pkg and then click **Install** to begin deployment.

Deploy Thirtyseven4 EDR Mac Client using Casper

In addition to the Prerequisites described above, follow this prerequisite.

Prerequisite

Before deploying Thirtyseven4 EDR Mac client, ensure that you get Casper tool installed on your administrator computer. Casper helps to install software and run scripts remotely on the client computers. To download Casper, visit http://www.jamfsoftware.com/products/casper-suite/.

To deploy Thirtyseven4 EDR Mac client using Casper, follow these steps:

1. Log on to Casper Admin.
2. Drag ClientAgentInstaller.pkg to the window and then select **File > Save**.
3. Log on to Casper Remote.
4. In the *Computers* tab, select the Mac client computers from the list of available computers.
5. In the *Packages* tab, select ClientAgentInstaller.pkg.
6. Click **Go**.

Connecting Remotely using Secure Shell

Secure Shell (SSH) is a network protocol that is used to connect to the remote Mac client computers over secure data communication through command line to manage client computers.

Using Terminal (for Mac or Linux OS)

The administrator computer having either Mac or Linux OS can install the client using this method.

Prerequisites

Before you install Thirtyseven4 EDR Mac client, ensure the following requirements.

- Administrator must have an account on the Mac client computers with admin privileges.
- Enable Remote Login and either allow access for all users, or only for specific users, such as Administrators. You can find this setting on the Mac computer under **System Preferences > Sharing > Remote Login**.
- Ensure that the firewall does not block the port that Secure Shell (SSH) uses, which is by default TCP port 22. This port allows the required communication for remote login.
- If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through Search Network.
- To disable stealth mode on the Mac computers, do the following,
  a. In System Preferences, go to **Security and Privacy**.
  b. Click the **Lock** icon and provide password if it is locked.
  c. Select **Firewall > Firewall Options**.
  d. Clear the **Enable stealth mode** check box if it is selected.
  e. Click **OK**.
- Mac Thirtyseven4 EDR Client installer must be created on the Thirtyseven4 EDR Security.

Installing Thirtyseven4 EDR Mac Client

To install Thirtyseven4 EDR Mac client using Terminal, follow these steps on the administrator Mac computer:

On the Thirtyseven4 EDR Security, download UEMREMOTEINST.TAR from the URL, http://updates.thirtyseven4.com/builds/thirtyseven4/uemcp/en/UEMREMOTEINST.tar

Download Mac client builds (with/without AV) from the Thirtyseven4 EDR server. These builds will be in the TAR format.

1. Rename the Mac client installer as follows:
   - Mac client installer (without AV) – MCCLAGNT.TAR
   - Mac client installer (with AV) – MCCLAGAV.TAR

2. Extract UEMREMOTEINST.TAR.
3. Copy MCCLAGNT.TAR or MCCLAGAV.TAR to "< Download directory>/UEMREMOTEINST". Download directory is the directory where you have downloaded and extracted UEMREMOTEINST.TAR.
4. Open Terminal.app and go to the UEMREMOTEINSTRemote_Installation folder.
5. Enter the following command
   sh ./Scripts/copy.sh

   Parameter description
   sh ./Scripts/copy.sh is static.
   specifies the user name of the remote Mac computer such as 'test'.
   specifies the IP address of the remote Mac computer such as '10.10.0.0'.
   Example: sh ./Scripts/copy.sh "test" "10.10.0.0"
6. Enter the password of the remote computer to connect to it.
7. Enter the command sudo sh /tmp/install.sh.
8. Enter the password of the remote computer when prompted.
9. A confirmation message appears – "If earlier version of Thirtyseven4 EDR Security client is found on the system, then it will be uninstalled automatically. Do you want to continue?? [Yes/No]:".
10. Enter **Yes** or **No**.
    - If you enter **Yes,** installation will proceed.
    - If you enter **No,** installation will be aborted with message "Option No has been selected. Installation aborted."
11. Enter the command exit to close remote SSH session.
12. Repeat steps 6 through 10 to install Thirtyseven4 EDR Mac client on a different remote computer.

Using PuTTY (for Windows OS)

The administrator computer having Windows OS can install the Mac client using this method.

Prerequisites

Before you install Thirtyseven4 EDR Mac client, ensure the following requirements.

- Administrator must have an account on the Mac client computers with admin privileges.

- Enable Remote Login and either allow access for all users, or only for specific users, such as Administrators. You can find this setting on the Mac client computer under **System Preferences > Sharing > Remote Login**.
- Ensure that the firewall does not block the port that Secure Shell (SSH) uses, which is by default TCP port 22. This port allows the required communication for remote login.
- If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through Search Network.
- To disable stealth mode on the Mac computers, do the following,
  a. In System Preferences, go to **Security and Privacy**.
  b. Click the Lock icon and provide password if it is locked.
  c. Select **Firewall > Firewall Options**.
  d. Clear **the Enable stealth mode** check box if it is selected.
  e. Click **OK**.
- Mac Thirtyseven4 EDR client installer must be created on the Thirtyseven4 EDR Security. To know about how to create client installer, see Creating Mac client Installer.

Installing Thirtyseven4 EDR Mac Client

To install Thirtyseven4 EDR Mac client using PuTTY, follow these steps:

1. On the Thirtyseven4 EDR Security, download UEMREMOTEINST.TAR from the URL:http://updates.thirtyseven4.com/builds/thirtyseven4/uemcp/en/UEMREMOTEINST.tar Download Mac client builds (with/without AV) from the UEM server. These builds will be in the TAR format.
2. Rename the Mac client installer as follows:
   Mac client installer (without AV) – MCCLAGNT.TAR
   Mac client installer (with AV) – MCCLAGAV.TAR
3. Extract UEMREMOTEINST.TAR.
4. Copy MCCLAGNT.TAR orMCCLAGAV.TAR to "/UEMREMOTEINST". Download directory is the directory where you have downloaded and extracted UEMREMOTEINST.TAR.
5. Open cmd.exe and go to the folder "< Download directory>/UEMREMOTEINST".
6. Do one of the following:
   - Enter the following command if antivirus is included in the client installer .Remote_InstallationSoftwarespscp.exe . MCCLAGAV.TAR .Remote_InstallationScriptsinstall.sh username>@<ip_address< a="">:/tmp/</ip_address<>

- Enter the following command if antivirus is not included in the client installer .Remote_InstallationSoftwarespscp.exe .MCCLAGNT.TAR .Remote_InstallationScriptsinstall.sh username>@<ip_address< a="">:/tmp/</ip_address<>

Note
When MCCLAGAV.TAR as well as MCCLAGNT.TAR files are present, priority is given to the MCCLAGAV.TAR for installing the Thirtyseven4 EDR Mac client.

Parameter description

- *<username>specifies the user name of the remote Mac client computer such as 'test'.*
- *<ip_address> specifies the IP address of the remote Mac client computer such as '10.10.0.0'.*

  Example: .Remote_InstallationSoftwarespscp.exe .MCCLAGNT.TAR .Remote_InstallationScriptsinstall.sh test@10.10.0.0:/tmp/.

7. Open .Remote_InstallationSoftwaresputty.exe.
8. Enter the IP address of the remote Mac client computer and click *Open*.
9. In the PuTTY terminal Window, enter the username and password of an administrator user on the remote computer.
10. Upon getting connected to the remote computer, type the following command sudo sh /tmp/install.sh.
11. A confirmation message appears – "If earlier version of Thirtyseven4 EDR Security client is found on the system, then it will be uninstalled automatically. Do you want to continue?? [Yes/No]:".
12. Enter **Yes** or **No**.
    - If you enter **Yes,** installation will proceed.
    - If you enter **No,** installation will be aborted with message "Option No has been selected. Installation aborted."
13. Type the command exit to close SSH connection.
    Repeat steps 6 through 11 to install on a different Mac client computer.

Note
While installing the Mac client for the first time on Mac OS 10.13 and later, user should allow permission for loading the drivers manually when prompted.

Active Directory

This page helps you to download Active Directory Tool. With Active Directory Tool you can synchronize the Thirtyseven4 EDR server group with active directory organizational unit (OU)/container/computer. After synchronization, the clients will be installed on all the endpoints of your domain network. A periodic check is carried out to find if any new endpoint is added to your network. When a new endpoint is added, the client gets automatically installed on that endpoint.
You can also exclude certain endpoints from the Thirtyseven4 EDR server group so that the client is not installed on these endpoints.

Note

- *This installation method is available only with Microsoft Windows operating system.*
- *To synchronize the Thirtyseven4 EDR server with Active Directory OU, the Active Directory Tool should be installed on the domain machine or should be a member of the domain.*
- *Synchronization cannot be done with Default group.*
- *On the Groups page, groups are shown with AD tag, which are already synchronized with Active Directory.*
- *The user should have permissions of Domain Admins to synchronize with Active Directory.*

Synchronizing with Active Directory

To install Thirtyseven4 EDR Active Directory Tool on your computer, follow these steps:

1. Click **Active Directory Installer** button.
2. The Active Directory zip file is downloaded. Extract the files.
3. Double click adinst.msi file. The Active Directory installer opens and guides you through the steps required to install Thirtyseven4 EDR Active Directory Tool on your computer.

   Note
   This system should be powered on 24X7 for periodic check in synchronization process.
4. Follow the instructions in the wizard. Thirtyseven4 EDR Active Directory Tool will be installed on your computer.
5. Launch the Thirtyseven4 EDR Active Directory Tool.
   A help file is provided in the Thirtyseven4 EDR Active Directory Tool.

Installing Thirtyseven4 EDR Security Client

The procedure to install Thirtyseven4 EDR Client on different operating systems is as follows:

Installing Thirtyseven4 EDR Client on Windows

1. Copy the Client Installer created from Online/Standalone Installer to Windows system.
2. Extract the zip file on the system.
3. Execute the installer file. The name of installer file, as per the options selected is as follows,
   - 32-bit with AV – clagav32
   - 32-bit without AV – clagnt32
   - 64-bit with AV – clagav64
   - 64-bit without AV – clagnt64
   - Minimal – minimal.exe
4. On executing the installer file, the Thirtyseven4 EDR Client Agent is installed.

Installing Thirtyseven4 EDR Client on Mac

1. Download the .TAR file from the Thirtyseven4 EDR console.
2. Extract the tar file.
3. Double-click the installer file (MCLAGNT.DMG). The EDR Security icon is mounted on the desktop.
4. Double click the EDR Security icon. An installer window will appear.
5. Double click the Thirtyseven4 EDR Installer icon in the window. "Verifying Client Agent installer" message is displayed.
6. After the verification is complete, a message appears, "Client Agent Installer" is an app downloaded from the Internet. Are you sure you want to open it?"
7. Click **Open** button.
8. Provide username and password of the system when prompted by the installer.
9. Click **OK**.
   Note
   If password-protected Client Installer is being executed, then it will ask for Client Installer password first and then it will ask for System password.
10. The Client Agent will be installed. A message, "EDR Security Client installed successfully" appears.
11. Click **OK**.
    The AV will be automatically downloaded and installed in the background. After installation, AV will get activated and its status will be sent to the server.

Note

To install EDR Security on macOS Catalina, refer KB article,
Thirtyseven4 EDR Security compatibility with macOS Catalina

To install EDR Security on Big Sur, refer KB article,
Thirtyseven4 EDR Security supports macOS Big Sur 11

Installing Thirtyseven4 EDR Client on Linux

1. Log in as root and go to the terminal.
2. Go to the directory containing Thirtyseven4 EDR Security installation folder and run ./install script. The installation script will copy the necessary files to the /usr/lib/Thirtyseven4 EDR/Thirtyseven4 EDR folder.
3. Configure Thirtyseven4 EDR and save your settings.

Disk Imaging

You can also deploy Thirtyseven4 EDR Security client through disk imaging like Sysprep.

To deploy clients through Disk Imaging, follow these steps:

1. Disconnect the endpoint from the network that will be used as a source for disk imaging, or ensure that this endpoint is not able to communicate with Thirtyseven4 EDR Security server.
2. Install operating system and other applications.
3. Install Client.

   To install Client, follow these steps:

   c. Create a Client Packager without AV Build.
   d. Create a Client Packager with AV Build.
4. Run the application remguid.exe from the client agent folder <installation directory>\Thirtyseven4 EDR\Client Agent 10.7>.
5. Create a disk image.

Post disk image, do the following steps.

6. Start Client Agent Services Client Agent 10.7 from the Services panel.
7. Execute Client Agent service, < Client Agent 10.7> .

Note

Whenever the CA service is executed, GUID will be generated automatically and will be sent the GUID to server during registration.

The Disk Imaging feature is available only in the clients with Windows operating systems.

Thirtyseven4 EPS 7.6 Migration

Thirtyseven4 EDR recommends customers of Thirtyseven4 EPS 7.6 should migrate to Thirtyseven4 EDR Security 8.3.
For the current Thirtyseven4 EPS 7.6 customers, Thirtyseven4 EDR is providing a tool to migrate data of clients, groups, and policies from Thirtyseven4 EPS 7.6 to Thirtyseven4 EDR 8.3.
This page will guide you through the step-by-step migration process to migrate Thirtyseven4 EPS 7.6 data of clients, groups, and policies to Thirtyseven4 EDR 8.3 This page is active for only 60 days from the activation date of Migration feature.

System requirements

- Service Pack 5.0 applied on Thirtyseven4 EPS 7.6 Server and clients
- **Windows and Linux**
  For System requirements for Thirtyseven4 EDR Security clients, refer System Requirements.
  ### Important
- If the OS requirements are not met, the client and groups data will not be migrated to Thirtyseven4 EDR 8.3.
- The client is installed in the default path. You can modify the client installation path, if required. If you want to change the path, you should change the path before migration. To change the client installation path, go to Thirtyseven4 EDR 8.3 console > Configurations > Client Installation.

Migrating Data

Thirtyseven4 EPP 7.6 Migration process means migrating the data of clients, groups, and policies from the Thirtyseven4 EPS Server 7.6 to the Thirtyseven4 EDR Server 8.3.

Migrating Clients, Groups, and Policies

To migrate Thirtyseven4 EPS 7.6 data of clients, groups, and policies to Thirtyseven4 EDR 8.3, follow these steps:

1. Go to Thirtyseven4 EDR 8.3 console > Deployment > Thirtyseven4 EPP 7.6 Migration page.
2. Click the **Export Tool** button. The tool is downloaded.
3. Execute the Export Tool on the Thirtyseven4 EPS 7.6 server.

4. After the Export Tool is executed, '**Do you want to change export location? [y/n]**', question appears. To provide local system path to export data of the Groups and clients, type '**y**' and type the path.
   To export the data to the default path, type '**n**'. The default export path is <installation directory>\Thirtyseven4 EDR\EPS Security 7.60\Admin\Export
   After validating the path, the data is exported in the .DAT format at the set path.
   The Client.dat and Groups.dat files will be zipped automatically to **Export.zip** by the Export Tool.
5. Go to **Thirtyseven4 EDR 8.3 console> Deployment > Thirtyseven4 EPP 7.6 Migration** page.
6. Click the **Import Data** button.
   The Import Data dialog appears. By default, the Client, Groups, and Policy check boxes are selected, so all clients, groups, and policies are imported.

   You can clear the Groups or Policy check boxes if you don't want to import. If you don't import Groups and you import only Policy, all clients will be imported in the default group. The policy will be imported but will not be assigned to any group.
7. Click **Browse** to Import Export.zip file.
8. Click **Import**. The data is imported successfully. The success message appears.
   Note:
   Maximum no. of groups to be imported: 999

   Maximum no. of policies to be imported: 198

   Important: Group and Policy Migration

   - If a duplicate group is found on both Thirtyseven4 EPS 7.6 and Thirtyseven4 EDR 8.3, it will be skipped. But if the applied policies are different on duplicate groups, the policy applied on Thirtyseven4 EDR 8.3 remains the same.

     Example: If 'Group1' is present on both Thirtyseven4 EPS 7.6 and Thirtyseven4 EDR 8.3, after migration, the policy assigned to Group1 on Thirtyseven4 EDR 8.3 remains the same.
   - While importing the Firewall policy, ensure the following things.
     - In Thirtyseven4 EPS 7.6, if multiple Remote IP addresses are added to the Firewall exception, then in the imported policy in Thirtyseven4 EDR 8.3 multiple exceptions will be created for each IP.
     - Domain name exceptions are ignored.
   - If a duplicate name is found in Thirtyseven4 EPS 7.6 and Thirtyseven4 EDR 8.3 of the following components while importing, a timestamp will be appended to the imported name.

- Policy
- Device name
- User Defined Dictionary

9. For **Windows**, do the following.
   a. If you want to change the default client installation path, go to Thirtyseven4 EDR 8.3 console > Configurations > Client Installation. Else, client will be installed at default location.
   b. Go to Thirtyseven4 EDR 8.3 console > Deployment > Thirtyseven4 EPP 7.6 Migration page.
   c. Click the **Client Migration Tool** button.
   d. The Client Migration Tool, migrate.zip is downloaded.
   e. Extract the zipped file on the Thirtyseven4 EPS 7.6 server and execute acsvpack.exe. This will apply Service pack on the endpoint.
   f. Restart the endpoint when the restart prompt will appear on the endpoint. You will receive 2 restart prompts during migration process in case you have not rebooted the system after Thirtyseven4 EPS 7.6 client installation.
10. For Linux, do the following.
    a. Go to Thirtyseven4 EDR 8.3 console > Deployment > Online Installer page.
    b. Download latest Linux Thirtyseven4 EDR Client packager on the Linux client.
    c. The Client Installer tar file is downloaded. Extract the files on the Linux client.
    d. Execute the Installer. Uninstallation of previous version and installation of latest version will be done automatically.

The data of clients, groups, and policies will be migrated successfully.
Migrated Clients will appear online on the Thirtyseven4 EDR 8.3 console.

Removing Inactive Clients from Thirtyseven4 EPS 7.6

The migrated clients appear offline/inactive on the Thirtyseven4 EPP 7.6 Web console.
To remove inactive clients, follow these steps:

1. Log on to the Thirtyseven4 EPS Security 7.6 Web console.
2. Go to Admin Settings > Clients.
   The Client Installation page appears.
3. Under Inactive Client Settings, select the **Enable automatic removal of inactive clients** check box.
4. In the **Remove a client if inactive for** list, select number of days after which Thirtyseven4 EDR Security considers a Client is inactive.

5. To apply the setting, click **Apply**.

Limitations

- Thirtyseven4 EPS Migration 7.6 does not support the clients with Mac operating systems.
- The Default client on the Thirtyseven4 EPS Server will not be migrated to Thirtyseven4 EDR 8.3.
- Update Agent upgrade is not supported.
- Master Secondary setup not supported for Thirtyseven4 EDR 8.3.
- Migration of Thirtyseven4 EDR Users, and reports are not supported.

Custom Server Certificate

Thirtyseven4 EDR 8.3 by default supports self-sign certificates. Now, there is a provision to replace the public key certificate if a customer has it. This enhancement lets you replace the custom certificate more than once.

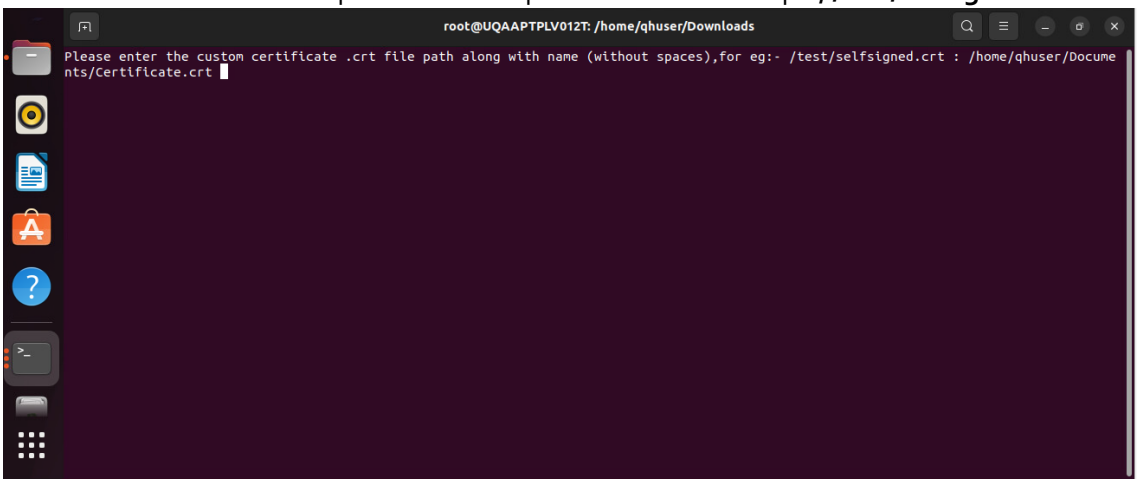
Note: Ensure that the file names such as .**crt** or **.key** files do not consist of any space.

Replacing the Custom Certificates

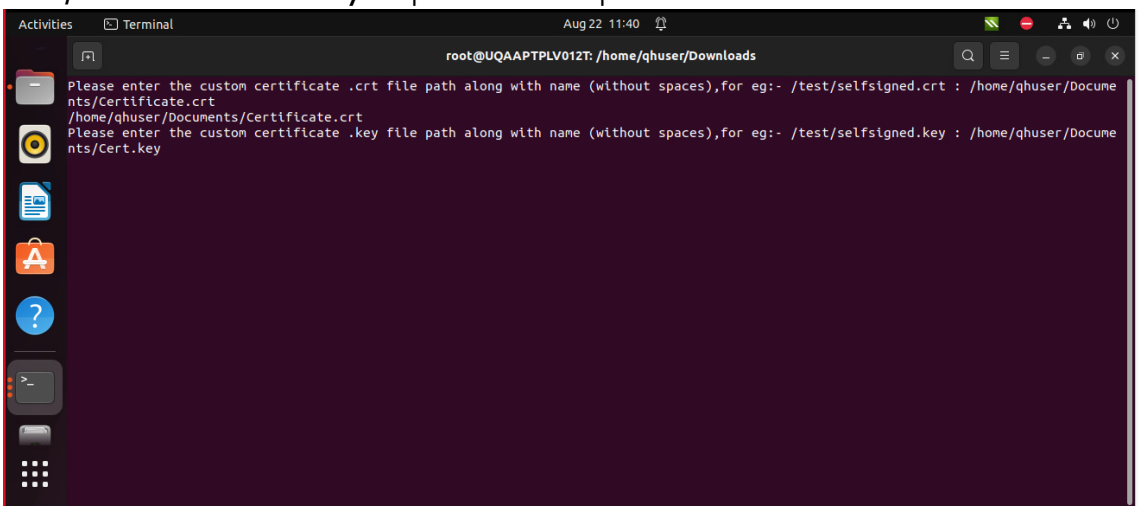
Follow these steps to replace the custom certificates.

Note: Only a root user or a super user is authorized to run the script and replace the certificate.

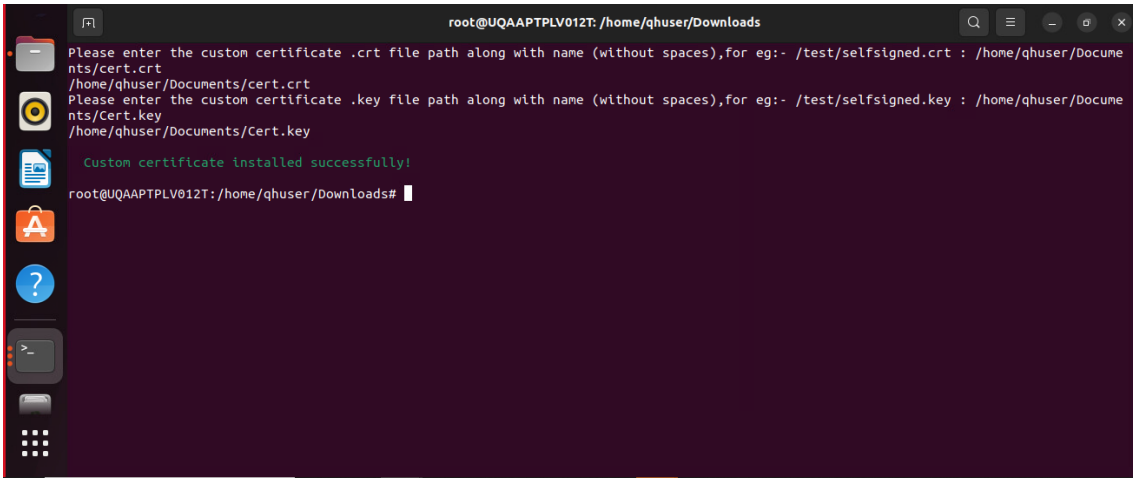
1. Copy the script (updcustcertificate.sh) provided by Thirtyseven4 EDR to your local machine. Click here to download the script: updcustcertificate.sh
2. Have your certificate saved on your system and have the path handy.
3. Go to the terminal.
4. Run the bash command. (*bash updcustcertificate.sh)*.
5. It asks to enter the .cert file path. Enter the path name. For example, **/test/selfsigned.crt**



6. Then, it asks to enter the **.key** file path. Enter the path.



7. Hit enter.



A success message appears as **Custom certificate installed successfully.**

High Availability

High availability refers to the design and implementation of systems that are resilient and reliable, with minimal downtime and disruptions.
The goal of high availability is to ensure that services and applications remain accessible and operational even in the case of hardware failures, software glitches, or other types of failures.
The design proposes having three nodes. Two nodes with Thirtyseven4 EDR and other stateful services and one auxiliary node that supports the clustering services by participating in the quorum election of these individual clustering services.

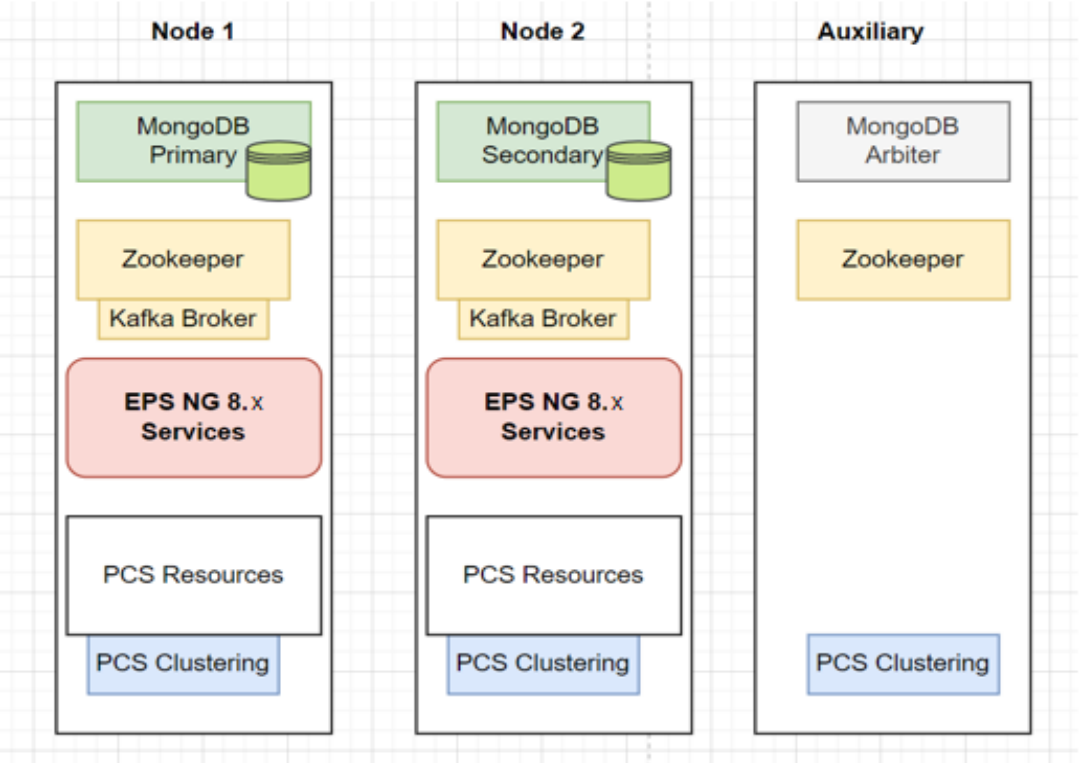
- 3-node architecture with Thirtyseven4 EDR 8.3 installed on two nodes.
- State maintained in MongoDB and Kafka.
- Native replication of MongoDB and Kafka used to form independent clusters.
- Service control of Thirtyseven4 EDR 8.3 services managed through Pacemaker and Corosync (pcs) clustering.

Term	Definition
Thirtyseven4 EDR 8.2	Thirtyseven4 EDR Security 8.2, the main suite of products for which the High Availability feature is being designed. Interchangeably used as Thirtyseven4 EDR Security 8.2.
Node	The **Primary Node**, also known as the Active Node, is used for initial bootstrapping and hosts operational Thirtyseven4 EDR services. The **Secondary Node**, referred to as the Passive Node, remains in standby mode. It also hosts Thirtyseven4 EDR services (not running), and in the event of a primary node failure, the application will seamlessly switch to the secondary node.
Node 1	One of the two data bearing and Thirtyseven4 EDR 8.3 installed nodes, used as a primary for initial bootstrapping.
Node 2	One of the two data bearing and Thirtyseven4 EDR 8.3 installed nodes.
Auxiliary Node	A third node that is not installed with Thirtyseven4 EDR 8.2, however, it hosts some auxiliary services like MongoDB Arbiter, Zookeeper, and PCS clustering which help in electing a node in cluster and avoid split brain.
Virtual IP	A floating IP address that is used to move the IP connectivity between the nodes controlled by clustering tools.
Ansible	Configuration management to consistently deploy the HA tools on the nodes
Lsyncd	For performing automatic syncing of directory changes with rsync or other sync mechanisms.
Arbiter	An arbiter in a MongoDB replica set is responsible for participating in the voting process during elections for selecting a primary node. When a primary node fails or becomes unavailable, replica set members (which include both data-bearing nodes and arbiters) participate in an election to determine the new primary node.

Pacemaker	Pacemaker is a cluster resource manager that coordinates the distribution and failover of resources within a cluster. It manages resource groups, monitors their status, and performs automatic failover when a node or resource fails.
Corosync	Corosync is a messaging layer that provides communication and synchronization between cluster nodes. It ensures that all nodes are aware of each other's status and helps maintain the integrity of the cluster.
PCS	PCS is a set of tools and utilities used to configure, manage, and monitor a high-availability cluster using the Pacemaker and Corosync components. It provides a convenient command-line interface for setting up and maintaining a cluster environment.
MongoDB	Main database for the Thirtyseven4 EDR 8.3 stack Runs in Active-Passive (Primary – Secondary) mode with both bearing the data and primary replicating the data to the secondary. Supports automatic failover to secondary when primary fails.
ZooKeeper + Kafka Broker	The message broker for the Thirtyseven4 EDR 8.3Stack consists of Kafka brokers that operate in an Active-Active configuration, while ZooKeeper manages the metadata for these brokers and facilitates the election of a leader from the two available brokers

Architecture

The diagram below shows the high-level components that are distributed across the nodes.



Failover Conditions:

- If the primary node is restarted or is crashed, the application will failover to the secondary node.
- If any service under PCS cluster of Primary Node gets corrupted or if the service goes down, the application will failover.
- If the secondary node fails, no failover as system continues to have the VIP and other services on the primary node.
- If Kafka in the primary node goes down, the application will start using Kafka of secondary node – Node will not failover in current condition.
- If the Mongo in the primary node goes down, the application will start using Mongo of secondary node – Node will not failover in current condition.
- Monitoring: Alerts will be generated if any service is stopped or started in the Node.

Policies

Policies feature helps you to create policies that help centrally control and manage the users belonging to a group. You can create two types of policies,

- **Container policy** – Container policy is a combination of all features.
- **Feature policy** – Feature policy is used for specific feature. The feature policy overrides the container policy.
  On the Policies page, you can manage policies.
  Managing Policy

  You can manage policies as per your requirement.

Creating a New Policy

To create a new policy, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Policies. The Policies page appears displaying list of policies.
3. Click **Create Policy** button.
4. The Create Policy dialog appears. Enter Policy Name.
5. Select the Policy Type, either **Container Policy** or **Feature Policy**. If you select the Feature policy option, select the feature from the list.
6. Enter **Description** of the policy.
7. Click **Create**. The Policy Settings page appears. Configure the policy.
8. Click **Save Policy**.
   The policy is created.

Deleting a Policy

To delete a policy, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Policies. The Policies page appears displaying list of policies.
3. Select the policy that you want to delete, and then click **Delete** button. A confirmation message appears.
4. If you are sure to delete the selected policy, click **YES**.
   If the selected policy is applied to a group, it cannot be deleted, and a failure message appears.

Note

- *You cannot delete the default policy.*
- *If a policy is applied to a group or to an endpoint and you want to delete it, then apply a different policy to that group or unassign the policy applied to the endpoint. Then you can delete the policy.*

Duplicating a Policy

To duplicate a policy, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Policies. The Policies page appears displaying list of policies.
3. Click the duplicate icon of the policy that you want to duplicate.
4. The duplicated policy appears in the next row. Edit the name of the policy. Click check mark icon to save the policy. The selected policy is duplicated. The policy settings remain same. You can also change the policy settings if required.
5. To save your setting, click **Save Policy**.

Updating a Policy

To update a policy, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Policies. The Policies page appears displaying list of policies. The name of the policy owner and date of policy creation appears.
3. Click the edit icon of the policy that you want to update. The Policy Settings page appears.
4. Update the settings.
5. To save your setting, click **Save Policy**.

Note
You cannot update Default_MSSP policy.

Schedule Settings

Scanning regularly keeps the systems clean and safe. In a large organization the client systems may be installed in physically separated environments.
To centrally manage all the systems about how to scan and when to initiate scanning, the administrator must have a policy. This feature helps you create policies for scheduling scans for the client systems.
To configure policy for Schedule Settings, follow these steps:

1. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.
    - Scheduled Tuneup
    - Scheduled Client Scan
    - Data-At-Rest Scan
    - Asset Management
    - Application Control
    - Vulnerability Scan
2. To save your settings, click **Save Policy**.
   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the **Reset Default** button.

Scheduled Tuneup

Scheduled Tuneup setting allow you to carry out different types of clean-ups such as; disks, registry entries, or schedule a defragmentation at scheduled time at next boot.
To schedule Tuneup settings, follow these steps:

1. In **Frequency** (Weekly), select a day of the week.
2. In **Start At**, set time in hours and minutes.
3. Select the **Run task immediately if missed** check box if you want to run the scan immediately if missed the set schedule.
4. In Tuneup settings, select either or all of the following options:
    - Disk clean-up
    - Registry clean up
    - Defragment at next boot
      However, all these options are selected by default.

Scheduled Client Scan

This feature allows you to create policies to initiate scanning the clients automatically at a convenient time. You can define whether the scan should run daily or weekly, select scan mode (Quick Scan, Full System Scan). You can also enable Antimalware while scanning. This will supplement other automatic protection features to ensure that the client systems remain malware-free.

1. In **Frequency**, select either the Daily or Weekly option.
2. In **Start At**, set time in hours and minutes.

3. Select the **Run task immediately** if missed check box if you want to run the scan immediately if missed the set schedule.

   Note

   Missed schedule scan is not supported on Windows XP SP3 (32- bit) operating system.

   For Microsoft Windows Vista and above operating systems, missed schedule scan will not work if Schedule task is not run at least once.

4. In Scanner Settings section, Under How to Scan, select a scan mode from the following:
5. Quick Scan (Scan Drive where operating system is installed)
6. Full System Scan (Scan all the fixed drives)
7. Select **Scan Priority**. The Scan Priority is **Low** by default. You can change the priority to Normal or High, if required.
8. Under **Select scan mode,** to set optimal setting, select the Automatic option.
9. To set advanced setting, select the **Advanced** option.
10. If you select the Advanced option, further settings such as, scan items and scan types are activated.
11. Under Select items to scan, select any of the following:
    - Scan executable files
    - Scan all files (Takes longer time)
    - Scan packed files
    - Scan mailboxes
    - Scan archives files
12. If you select the **Scan archives files** option, you can set the following also:
13. Archive Scan Level: You can set up to level 16.
14. Select action to be performed when virus is found in archive file: You can select one of the actions from Delete, Quarantine, and Skip.
15. In Select action to be performed when a virus is found section, select an action from the following: **Repair, Delete,** and **Skip**.
16. To enable scanning for malware, select the **Perform Antimalware scan** check box.
17. In Select action to be performed when malware found, select an action from the following: **Clean** and **Skip**.
18. Under Boot Time Scan Settings, select the **Perform Boot Time Scan** check box.
19. Select Boot Time Scan Mode option from the following,

- Quick Scan (Scan the areas where operating system and applications are installed)
- Full System Scan (Scan all the fixed drives)
  Boot time scan will be executed whenever the endpoint system restarts.

Note
Scan packed files, Scan mailboxes, and Antimalware Scan Settings are available only in the clients with Windows operating system.

Data-At-Rest Scan

With Data-At-Rest scan, you can search for a particular type of data in various formats and detect any confidential data that is present in your endpoints and removable devices. To perform Data-At-Rest scan, you must enable DLP on the endpoints. To do this, see DLP License.

1. In **Frequency**, select either the Daily or Weekly option.
2. In **Start At**, set time in hours and minutes.
3. If you want to repeat scanning of your clients, select Repeat Scan and set the frequency to repeat the scan.
4. Select the **Run task immediately if missed** check box if you want to run the scan if missed the set schedule.
5. Select a scan mode from the following:
   - Quick Scan (Scan Drive where operating system is installed)
   - Full System Scan (Scan all the fixed drives)
   - Scan Specific Folder(s): Select this option to scan a particular folder(s).
     a. Click **Configure**.
     b. Enter the path of the folder that you want to scan. You can also choose to scan the subfolders by selecting the Include Subfolder check box.
     c. Click **Add**. You can also remove a path from the list by clicking Remove.
     d. Click **Apply**.
6. Select **Scan Priority**. The Scan Priority is **Low** by default. You can change the priority to Normal or High, if required.
7. Configure the settings for File Types, Confidential Data, and User Defined Dictionary.

Asset Management

Assets Management helps you keep a watch on the system information, hardware information, and software installed. You can also view the hardware changes and software

changes, if any, that are made to the configuration of the systems.
Select the following check boxes:

- Track Software Changes
- Track Hardware Changes. This check box is selected by default.

Application Control

Application Control helps you define schedules to scan applications at a preferred or specified frequency.
To configure Application Control Schedule Scan, follow these steps:

1. In **Frequency**, select either the Daily or Weekly option. If you select the Weekly option, select the weekday from the list.
2. In **Start At**, set time in hours and minutes.
3. If you want to repeat scanning for the applications, select the **Repeat Scan** check box and set the frequency of interval after which the scan should be repeated.
4. Select the **Run task immediately if missed** check box.
5. Select one of the following scan options:
   - Unauthorized applications: Helps you initiate scanning only for the unauthorized applications present on a client machine.
   - Unauthorized and authorized applications: Helps you initiate scanning for both, unauthorized and authorized applications present on the client machine.
   - All installed applications: Helps you initiate scanning for all applications installed on a client.
6. Select **Scan Priority**. The Scan Priority is **Low** by default. You can change the priority to Normal or High, if required.

Vulnerability Scan

Vulnerability Scan helps you define schedules to initiate vulnerability scan of the clients as per your convenience.
To configure Vulnerability Scan Schedule Scan, follow these steps:

1. Select the weekday from the list.
2. In **Start At**, set time in hours and minutes.
3. If you want to repeat scanning for the applications, select number of weeks to repeat the scan.
4. Select the **Run task immediately if missed** check box.

5. Under Scan and report, select one of the following options to scan for vulnerability against following software vendors:
    - Microsoft applications and other vendor applications
    - Microsoft applications only
    - Other vendor applications only
6. Select **Scan Priority**. The Scan Priority is **Normal** by default. You can change the priority to Low or High, if required.
7. Select **Scan Severity** . The Scan Severity is **High** by default. You can change the priority to Low or Medium, if required.You can reset the Scan setting to default with Reset Default button, if required.

Patch Scan

This feature allows you to configure a schedule for scanning missing patches.

To configure a patch scan schedule, follow these steps.

1. Select a weekday from the drop down menu.
2. In **Start At,** set time in hours and minutes.
3. If you want to repeat scanning of your clients, set the frequency to repeat the scan in weeks.
4. Select the **Run task immediately if missed** checkbox if you want to run the scan if missed the set schedule.
5. Under Patch Install Settings, select the **Automatic install the missing software patches** check box.
6. Select the **Allow auto-restart the system** check box.

ETH Scan

Here you can define schedules to do ETH scan at a preferred or specified frequency.
To configure ETH Schedule Scan, follow these steps:

1. In **Frequency**, select either the Daily or Weekly option. If you select the Weekly option, select the weekday from the list.
2. In **Start At**, set time in hours and minutes.
3. If you want to repeat ETH scanning, select the **Repeat Scan** check box and set the frequency of interval after which the scan should be repeated.
4. Select the **Run task immediately if missed** check box.

Feature Policies

Scan

This feature allows you to define a policy on how to initiate the scan of the endpoints. The policy can be refined to enable Virus Protection or DNA scanning or include blocking of any suspicious packed files, and other settings.
To configure policy for Scan, follow these steps:

1. Create Container/feature policy for Scan.
2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.
    - Scanner
    - Virus Protection
    - Exclude Files and Folders
    - Exclude Extensions
    - Advanced DNA Scan
    - Disconnect Infected Endpoints from the network
    - Block suspicious packed files
    - Automatic Rogueware Scan
    - Scan External Drive
    - Autorun Protection
3. To save your settings, click **Save Policy**.
   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Reset Default button.

Scanner

Under Scanner, you can select either of the following scanning options:

- **Automatic**: This is the default scan setting that ensures optimum protection to the clients.
- **Advanced**: If you select this option, you may further need to customize the configuration of scanning options as per your requirement. When you select this option,

Features	Description
Select items to scan	Select either of the options to scan: Scan executable files: Includes scanning of executable files only. Scan all files: Includes scanning of all files, but takes longer time for scanning.
Scan Packed Files	Scans packed files inside an executable file.
Scan Mailboxes	Scans Emails inside the mailbox files.
Scan Archive Files	Scans compressed files such as ZIP and ARJ files including other files.
Archive Scan Level	You can set the level for scanning in an archive file. The default scan level is set to 2. You can increase the scan level up to 16, however, that may affect the scanning speed.
Action to be performed when virus is found in archive file.	You can select an action that you want to take when a virus is found in archive file during an on-demand scan. You can select any one of the following actions: · Delete – Deletes the entire archive file even if a single file within the archive is infected. · Quarantine – Quarantines the archive containing the infected files. · Skip – Takes no action even if a virus is found in an archive file.
Action to be performed when a virus is found.	You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions: · Repair – All the infected files are repaired automatically. The files that are not repairable are deleted. · Delete – All the infected files are deleted automatically. · Skip – Takes no action even if a virus is found in a file.

other features are activated that are described as follows:

Virus Protection

This feature helps you continuously monitor the endpoints against viruses that may infiltrate from sources such as email attachments, Internet downloads, file transfer, and file execution. By default, Virus Protection is enabled to keep the endpoints clean and secure from any potential threats.

Features	Description
Load Virus protection at Start up	Enables real-time protection to load every time the system is started.
Display Alert messages	Displays an alert message with virus name and file name, whenever any infected file is detected by the virus protection.
Report source of infection	Displays the source IP address of the system where the virus is detected.
Select action to be performed when a virus is found	You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions: – Repair – All the infected files are repaired automatically. The files that are not repairable are deleted. – Delete – All the infected files are deleted automatically. – Deny Access – Access to an infected file is blocked.

Exclude Files and Folders

This feature helps you decide which files and folders should be omitted from scanning for known viruses, Advanced DNA Scan, and Suspicious Packed files. It is helpful in case you trust certain files and folders and want to exclude them from scanning.
To add a file or a folder, follow these steps:

1. In Exclude File and Folders section, click Add.
2. On the Exclude Item screen, select either of the following:
    - **Exclude Folder**: If you select Exclude Folder, type the folder path in the Enter folder path text box. If you want to exclude a subfolder also from scanning, select Include Subfolder.
    - **Exclude File**: If you select Exclude File, type the file path in the Enter file path text box.

- **Exclude MD5 checksum**: If you select Exclude MD5 Checksum, type the checksum in Exclude MD5 Checksum text box. MD5 checksum is a 32-character hexadecimal number which is the fingerprint of the file. With MD5 checksum, you can verify whether your downloaded file got corrupted or not in transit.

3. In Exclude from section, select the following options as per your requirement:
   - Known Virus Detection
   - DNAScan
   - Suspicious Packed Files Scan
   - Behaviour Detection
   - Anti-Ransomware

     When you select the Exclude MD5 checksum option, all the above options are selected, by default. Anti-Ransomware option is available only in the Exclude MD5 checksum selection.

4. To save your settings, click **OK**.

   Note

   If you select Known Virus Detection, DNAScan and Suspicious Packed File Scan will also be enforced, and all the three options will be selected.

   If you select DNAScan, Suspicious Packed File Scan will also be enforced, and both the options will be selected.

   However, you can select Suspicious Packed File Scan or Behaviour Detection as a single option.

Exclude Extensions

This feature helps you to exclude the files from scanning using their extensions to provide a real-time virus protection. This is helpful in troubleshooting performance related issues by excluding certain categories of files that may be causing the issue.
To exclude a file extension from scanning, follow the step:

1. Type an extension in the Enter Extension text box, and then click **Add**.
   The file extension should be without any dots in the following format: xml, html, zip etc.

Note
The Exclude Extensions feature is available only in the clients with Windows and Mac operating systems.

Advanced DNA Scan

Helps you safeguard the client systems even against new and unknown malicious threats whose signatures are not present in the virus definition database. DNAScan is an indigenous technology of Thirtyseven4 EDR to detect and eliminate new types of malware in the system.

DNAScan technology successfully traps suspected files with very less false alarms. Advanced DNAScan Settings also includes the following:

Features	Description
Enable DNAScan	Helps in scanning the systems based on Digital Network Architecture (DNA) pattern.
Enable Behavior detection system	Helps in scanning the files and systems based on their behavior. If the files or systems behave suspiciously or their behavior changes by itself is considered as suspicious. This detection can be categorized based on their criticality level as Low, Moderate, and High. You can select the detection criticality level depending on how often the suspicious files are reported in your systems.
Submit suspicious files	Helps in submitting suspicious files to the Thirtyseven4 EDR research lab automatically for further analysis.
Show notification while submitting files	Displays a notification while submitting DNA suspicious files.

Note

The Advanced DNAScan Settings feature is available only in the clients with Windows operating systems.

The 'Behavior detection system' scan setting is not applicable for Windows Server platforms.

Disconnect Infected Endpoints from the Network

This feature when enabled disconnects the infected endpoints from the network when non-repairable virus is found.

Select the When non-repairable virus found check box to disconnect infected endpoint.

Note
Disconnect Infected Endpoints feature is not supported on Mac operating system.

Block Suspicious Packed Files

This feature helps you identify and block access to the suspicious packed files. Suspicious packed files are malicious programs that are compressed or packed and encrypted using a variety of methods. These files when unpacked can cause serious harm to the endpoint systems.

It is recommended that you always keep this option enabled to ensure that the clients do not access any suspicious files and thus prevent the spread of infection.

Note
The Block suspicious packed files feature is available only in the clients with Windows operating systems.

Automatic Rogueware Scan

This feature automatically scans and removes rogueware and fake antivirus software. If this feature is enabled, all the files are scanned for possible rogueware present in a file.

Note
The Automatic Rogueware Scan feature is available only in the clients with Windows operating systems.

Scan External Drives

Whenever your system comes in contact with any external devices, your system is at risk that viruses and malwares may infiltrate through them. This feature allows you to set protection rules for external devices such as; CDs, DVDs, and USB-based drives.
With External Drives Settings, you can scan the USB-based drives as soon as they are attached to your system. The USB-based drives should always be scanned for viruses before accessing it from your system, as these devices are convenient mediums for transfer of viruses and malwares from one system to another.

Autorun Protection

The Autorun Protection protects your system from autorun malware that tries to sneak into the system from USB-based devices or CDs/DVDs using the autorun feature of the installed operating system.

Email

This feature allows you to customize the protection rules for receiving emails from various sources. You can set rules for blocking spam, phishing, and virus infected emails.

To configure policy for Email Settings, follow these steps:

1. Create Container/feature policy for Email Settings.
2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and Enable settings that you want to configure.
    - Email Protection
    - Trusted Email Client Protection
    - Spam Protection

3. To save your settings, click Save Policy.
   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Reset Default button.

Email Protection

With this feature, you can apply the protection rules to all incoming emails. These rules include blocking infected attachments (malware, spam, and viruses) in the emails.
This feature is turned on by default which provides the optimal protection to the mailbox from malicious emails. We recommend that you always keep Email Protection turned on to ensure email protection. Once the feature is enabled, all the incoming emails will be scanned before they are sent to the Inbox.

1. The **Block attachments with multiple extensions** check box is selected by default. This option helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
2. The **Block emails crafted to exploit vulnerability** check box is selected by default. This option helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients. Emails such as MIME, IFRAME contain vulnerability.
3. The **Enable attachment control** option helps you block email attachments with specific extensions or all extensions. If you select this option, the following options are enabled:
   - **Block all attachments**: Helps you block all types of attachments in emails.
   - **Block user specified attachments**: Helps you block email attachments with certain extensions. If you select this option, the Configure button is activated. For further settings, click Configure and set the following options:
     a. In the User Specified Extensions dialog, select the extensions so that the email attachments with such extensions are blocked.
     b. If certain extensions are not in the list that you want to block, type such extensions in the Enter Extension text box and then click **Add** to add them in the list.
     c. Click **OK** to save changes.
4. Select the Enable Email scanning over SSL check box to enable incoming mail scanning for mail accounts configured over SSL. Ensure that you perform the procedure mentioned below to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.
5. In the Configure Ports for Email Scan section, do the following:
   - Enter **POP3** and **IMAP** ports for incoming mails.
   - Enter **POP3** and **IMAP** ports for incoming mails over SSL.
   - Enter **SMTP** port and **SMTP port (SSL)** port for outgoing mails.

Note
The Email Protection feature is available only in the clients with Microsoft Windows and Mac operating systems.

Configuring Email Clients

For MS Outlook mail client, Thirtyseven4 EDR Email Scanner certificate is imported automatically. No action required.
For your reference, procedure to import Thirtyseven4 EDR Email Scanner certificate for Mozilla Thunderbird mail client is quoted here,

1. Launch Thunderbird mail client.
2. Select Options **Menu > Advanced > Certificates** tab.
3. Click **View Certificates**.
4. In Certificate Manager dialog, select **Authorities** tab, click **Import**.
5. Select **Thirtyseven4 EDR Email Scanner CA.der certificate** from installation directory.
6. Click the **Trust this CA to identify websites** check box and click **Ok**.
7. In Certificate Manager dialog, click **Ok**.
8. In Options dialog, click **Ok**.
   Similarly, for other mail clients, to import Thirtyseven4 EDR Email Scanner certificate, refer their technical documentation.

Trusted Email Clients Protection

Since email happens to be the most widely used medium of communication, it is used as a convenient mode to deliver malware and other threats. Virus authors always look for new methods to automatically execute their viral codes using the vulnerabilities of popular email clients. Worms also use their own SMTP engine routine to spread their infection.
Trusted Email Clients Protection is an advanced option that authenticates email-sending application on the system before it sends the emails. This option prevents new worms from spreading further. It includes a default email client list that is allowed to send emails. Email clients in the default list includes Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator.
Trusted Email Clients Protection supports most of the commonly used email clients such as; Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator. If your email client is different from the ones mentioned, you can add such email clients in the trusted email client list.

Note
The Trusted Email Clients Protection feature is available only in the clients with Windows operating systems.

Spam Protection

This feature allows you to differentiate genuine emails and filter out unwanted email such as spam, phishing, and adult emails. We recommend you to always keep Spam Protection enabled. If you enable Spam Protection, the Spam Protection Level, Whitelist, and Black list options are also activated.

Whitelist

Whitelist is the list of trusted email addresses. The content from the whitelisted email IDs is allowed to skip the spam protection filtering policy and is not tagged as SPAM.
This is helpful if you find that some genuine email IDs are detected as SPAM or if you have blacklisted a domain but want to receive emails from certain email addresses from that domain.

Blacklist

Blacklist is the list of email addresses from which all emails are filtered irrespective of their content. All the emails from the addresses listed here are tagged as "[SPAM] -".
This feature is useful particularly if your server uses an open mail relay, which is used to send and receive emails from unknown senders. This mailer system can be misused by spammers. With blacklist, you can filter incoming emails that you do not want or are from unknown senders both by email IDs and domains.

Configuring Spam Protection

1. Under Spam protection level, set the protection level from the following:
    - **Soft**: Applies soft filtering spam protection policy.
    - **Moderate**: Ensures optimum filtering. It is always recommended to enable the moderate filtering. However, this is selected by default.
    - **Strict**: Enforces strict filtering criteria. However, it is not ideal as it may even block genuine emails. Select strict filtering only if you receive too many junk emails.
2. Select **Enable white list** to implement protection rules for whitelisted emails.
3. In the **Email ID** text box, type an email address or a domain and then click **Add**. You can import email addresses or domains from text file using the **Import** button.
4. Select **Enable black list** to implement the protection rules for blacklisted emails.

5. In the **Email ID** text box, type an email address or a domain and then click **Add**. You can import email addresses or domains from text file using the **Import** button.

   Note
   • An email address should be in the format: abc@abc.com.
   *• A domain name should be in the format: *@mytest.com.*
   • The same email ID cannot be entered in both blacklist and whitelist.

6. To save your settings, click **Save Policy**.

IDS IPS

When you create a network where numerous machines are deployed, security is of paramount concern. With IDS/IPS, you can detect attacks. This detection implements a security layer to all communications and cordons your systems from unwanted intrusions or attack. You can also take actions like blocking the attacker's IP for certain time and send an alert message to the administrator.

Note
The IDS/IPS feature is available only in the clients with Microsoft Windows.

You can create different policies with varying IDS/IPS settings and apply them to the groups so that each has separate policies based on the requirement.
To configure policy for IDS/IPS, follow these steps:

1. Create Container/feature policy for **IDS/IPS**.
2. In the Host IDS/IPS section, enable **IDS Rules** by selecting the check box. By default, this option is selected.
3. Select the Detect Port Scanning Attack check box, if required. On selecting this check box, **customize** link gets enabled.
4. You can add IP Port exceptions if required.
5. Select the Detect DDOS (Distributed Denial of Service) Attack check box, if required. On selecting this check box, **customize** link gets enabled.
6. From the following options, select an action to be performed when attack is detected:
   - Block Attackers IP for ... Minutes. By default, this option is selected, and 5 minutes are set. Select the time, if required.
   - Display alert message when attack is detected. This option helps you to take an appropriate action when attack is detected.
7. To save your settings, click **Save Policy**.
   Importantly, if you have customized the settings and later you want to revert to the default settings, click the **Reset Default** button.

Customizing Port Scanning

You can customize settings for Detect Port Scanning Attack and Detect DDOS (Distributed Denial of Service) Attack as follows:

1. On IDS/IPS policy page, select the **Detect Port Scanning Attack** check box.

   The Customize link gets enabled.

2. Click the **Customize** link.

   Settings –Port Scanning dialog appears.

3. Select one of the following levels:

   - **Soft**: Detect attack if many ports are scanned
   - **Normal**: Detect attack if multiple ports are scanned
   - **Strict**: Detect attack if few ports are scanned
   - **Custom**: Helps you customize the number of scanned ports and attack duration.

4. To exclude an IP address you do not want to be scanned, click **Add** in the Excluded IP Addresses section.
5. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.
6. To exclude a port that you do not want to be scanned, click **Add** from the Excluded Ports section.
7. On the Add Port screen, type a Port or Port range and then click **OK**.

Customization for Distributed Denial of Service

Further customization settings for Distributed Denial of Service Attacks are as follows:

1. On IDS/IPS policy page, select the **Detect DDOS (Distributed Denial of Service) Attack** check box.

   The Customize link gets enabled.

2. Click the **Customize** link.

   The Settings – Denial of Service dialog appears.

   Select one of the following levels:

   - **Soft**: Detect attack if many attacks are detected
   - **Normal**: Detect attack if multiple attacks are detected
   - **Strict**: Detect attack if few attacks are detected
   - **Custom**: Helps you customize the number of attack sources and attack duration.

3. To exclude an IP address that you do not want to be scanned, click **Add** in the Excluded IP Addresses section.

4. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.
5. To exclude a port that you do not want to be scanned, click **Add** in the Excluded Ports section.
6. On the Add Port screen, type a port or port range and then click **OK**.

Creating the Exceptions

1. In Exceptions section, the list of Exceptions appears.
2. To create new exception, click **Add**.
3. On the Add/Edit Exception screen, do the following.
    1. Type a name in the **Exception Name** text box
    2. Select a protocol. The protocol includes: **TCP** and **UDP**.
    3. Select one of the Direction from the following and click **Next**.
        - Inbound Connections
        - Outbound Connections
        - Inbound – Outbound Connections
    4. Click **Next**.
4. Under Local IP Address, do one of the following,
    1. Select the **Any IP Addresses** option, you need not type an IP address as all IP addresses will be allowed or blocked.
    2. Select the **IP address** option and type the IP address. Click **Add** to add the IP address. You can add multiple IP addresses here.
       You can add up to 25 IP addresses per exception. However, the combined count of all IP addresses in all exceptions in a policy must be equal to or less than 255.
       You can delete the IP address with help of the **Delete** button.
       You can also import the IP addresses from a text file using the **Import** button. The maximum limit to import valid IP addresses is 25 per exception.
    3. Select **IP Address Range** option. Enter **Start IP Address and End IP Address**.
5. Click **Next**.
6. Under Local TCP/UDP Ports, do one of the following,
    1. Select the **All Ports** option to select all ports.
    2. Select the **Specific Ports** option and type the port numbers. Use comma in between to add multiple ports.
    3. Select the **Port Range** option. Enter **Start Port Number** and **End Port Number**.
7. Click **Next**.
8. Under Remote IP Address, do one of the following,
    1. Select the **Any IP Addresses** option, you need not type an IP address as all IP addresses will be allowed or blocked.
    2. Select the **IP address** option and type the IP address. Click **Add** to add the IP address. You can add multiple IP addresses here.
       You can add up to 25 IP addresses per exception. However, the combined count of all IP addresses in all exceptions in a policy must be equal to or less than 255.
       You can delete the IP address with help of **Delete** button.

You can also import the IP addresses from a text file using **Import** button. The maximum limit to import valid IP addresses is 25 per exception.

3. Select **IP Address Range** option. Enter **Start IP Address** and **End IP Address**.

9. Click **Next**.
   If you mention remote IP or port, that exception will be for outgoing communications.

10. Under Remote TCP/UDP Ports, do one of the following,
    1. The **All Ports** option is selected by default.
    2. Select the **Specific Ports** option and type the port numbers. Use commas in between to add multiple ports.
    3. Select the **Port Range** option. Enter **Start Port Number** and **End Port Number**.
11. Click **Next**.
12. Click **Finish**.
    The Exception is added at the top position in the Exceptions list. The sequence of the exceptions decides the precedence of the rule. The precedence is in descending order. You can move the exception rule with the **Move Up** and **Move Down** buttons.
13. Click **Save Policy**.

Editing the Exceptions Rule

You can edit the exceptions rule which are created by you. To edit the Exceptions rule, follow these steps:

1. In Exceptions section, select the exception that you want to edit.
2. On the Add/Edit Exception screen, you can edit the name in the Exception Name text box and edit the protocol. The protocol includes: TCP, and UDP.
3. Edit Direction option if required.
4. Click **Next**.
5. Edit Local IP Address if required, and then click **Next**.
6. Edit Local TCP/UDP Ports if required, and then click **Next**.
7. Edit Remote IP Address if required, and then click **Next**.
8. Edit Remote TCP/UDP Ports if required, and then click **Next**.
9. Click **Finish**.
10. Click **Save Policy**.

Deleting the Exceptions Rule

You can delete the exceptions rule that you have created. To delete the Exceptions rule, follow these steps:

1. In Exceptions section, select the exception that you want to delete.
2. The action bar is enabled above the table. In the drop down, select **Delete**.
3. Click **Submit**. The selected exception rule is deleted.
4. Click **Save Policy**.

Exporting the Exceptions Rule

You can export the exceptions rule that you have created. To export the Exceptions rule, follow these steps:

1. In Exceptions section, select the exceptions that you want to export.

2. Select Action > Export. The Opening ids_exception.json dialog appears.
3. Select **Save File**.
4. Click **Ok**.
   The database file, ids_exception.json is downloaded.

Importing the exceptions Rule

You can import the exceptions rule that you have created in the earlier versions of Thirtyseven4 EDR. To import the Exceptions rule, follow these steps:

1. In Exceptions section, click Add > Import. The File Upload dialog appears.
2. Select the database file, ids_exception.json.
3. Click **Open**.
   The database file, ids_exception.json is imported.

Firewall

Firewall shields your endpoint by monitoring both inbound and outbound network connections. It analyses all incoming connections whether it is secure and should be allowed through, and checks whether the outgoing communication follows the compliance that you have set for security policies. Firewall works silently in the background and monitors network activity for malicious behavior.
You can create different policies for various groups/departments like enabling Firewall protection, applying Firewall security level with an exception rule and other settings according to the requirements. For example, you can apply security level as High for the Accounts Department, and apply an exception rule by entering the policy with additional policy settings. You can also apply the Display alert message when firewall violation occurs and Enable firewall reports options. While for Marketing Department, you can create a policy with security level as Low without an exception rule and apply the Enable firewall reports options only.

Note
The Firewall feature is available only in the clients with Microsoft Windows.

Configuring Firewall

To configure policy for Firewall, follow these steps:

1. Create Container/feature policy for **Firewall**.
2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and Enable settings that you want to configure.
   - Firewall – When you enable this, a prompt appears, "This action will disable Windows Firewall on your endpoint. Do you want to continue?"
     Click **OK**.
   - Exceptions

3. To save your settings, click **Save Policy**.
   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Reset Default button.

Firewall Levels

1. In the Level option, select one of the following:
   - Block all
   - High
   - Medium
   - Low

Level	Description
Block all	Blocks all Inbound and Outbound connections without any exception. This is the strictest level of security.
High	Blocks all Inbound and Outbound connections with an exception rule. The exception policy can be created for allowing or denying connections either for inbound or outbound through certain communication protocols, IP address, and Ports such as TCP, UDP, and ICMP.
Medium	Blocks all Inbound and allows all Outbound connections with an exception rule. The exception policy can be created for allowing or denying either inbound or outbound connections through certain communication protocols, IP address, Ports such as TCP, UDP, and ICMP. For example, if you allow receiving data from a certain IP address, the users can receive data but cannot send to the same IP address. To take more advantage of this security level policy, it is advisable that you allow receiving inbound connections and block outbound connections.
Low	Allows all Inbound and Outbound connections. When you apply Low security level, it is advisable that you create an exception rule for denying particular inbound or outbound data with the help of certain Protocols, IP address, and Ports to take more advantage of the security level policy.

2. By default, the **Monitor Wi-Fi Networks** check box is selected. This option helps to receive alert messages when connected with unsecured Wi-Fi network and when an attempt is detected to access unsecured client Wi-Fi (hotspot). Also, the reports are generated at the server.
3. If you want an alert message about firewall violation, select the **Display alert message when firewall violation occurs** check box.
4. If you want reports for all blocked connections, select the **Enable firewall reports** check box.

Note
If the Firewall policy is set as Block All, Firewall will block all connections and generate many reports that may impact your network connection.

Exceptions

With Exceptions, you can allow genuine programs to perform communication irrespective of the Firewall level whether set as High or Medium. With Exceptions, you can block or allow Inbound and Outbound communication through IP addresses and ports.

Creating the Exceptions

1. In Exceptions section, the list of Exceptions appears.
2. To create new exception, click **Add**.
3. On the Add/Edit Exception screen, do the following.
    a. Type a name in the **Exception Name** text box.
    b. Select one of the protocols from the following:
        - TCP
        - UDP
        - ICMP
    c. Under Application, **All Applications that meet the specified conditions** option is selected by default. If you want any specific application, select **Specified Applications path** option and enter the path of the application.
    d. Click **Next**.
4. Depending on the selection of protocol, the steps are followed.

ICMP Protocol

If you select ICMP Protocol, do the following.

d. Under Local IP Address, do one of the following,

- Select the **Any IP Addresses** option, you need not type an IP address as all IP addresses will be allowed or blocked.
- Select the **IP address** option and type the IP address. Click **Add** to add the IP address. You can add multiple IP addresses here.

  You can add up to 25 IP addresses per exception. However, the combined count of all IP addresses in all exceptions in a policy must be equal to or less than 255.

  You can delete the IP address with help of the **Delete** button.

  You can also import the IP addresses from a text file using the **Import** button. The maximum limit to import valid IP addresses is 25 per exception.
- Select **IP Address Range** option. Enter **Start IP Address** and **End IP Address**.

e. Click **Next**.

f. Configure ICMP Settings. Select the check boxes as required. **The default** button sets the default settings of ICMP. Click **Next**.

g. Under Status, select either **Enable** or **Disable**.

h. Click **Finish**.

TCP or UDP

If you select TCP or UDP option for Protocol, do the following

i. Select one of the Direction from the following and click **Next**:

- Inbound Connections
- Outbound Connections
- Inbound - Outbound Connections

j. Under Local IP Address, do one of the following,

- Select the **Any IP Addresses** option, you need not type an IP address as all IP addresses will be allowed or blocked.
- Select the **IP address** option and type the IP address. Click **Add** to add the IP address. You can add multiple IP addresses here.

  You can add up to 25 IP addresses per exception. However, the combined count of all IP addresses in all exceptions in a policy must be equal to or less than 255.

  You can delete the IP address with help of **Delete** button.
- Select **IP Address Range** option. Enter **Start IP Address** and **End IP Address**.
- Click **Next**.

k. Under Local TCP/UDP Ports, do one of the following,

- Select the **All Ports** option to select all ports.

- Select the **Specific Ports** option and type the port numbers. Use comma in between to add multiple ports.
- Select the **Port Range** option. Enter **Start Port** Number and **End Port** Number.
- Click **Next**.

l. Under Remote IP Address, do one of the following,

- Select the **Any IP Addresses** option, you need not type an IP address as all IP addresses will be allowed or blocked.
- Select the **IP address** option and type the IP address. Click **Add** to add the IP address. You can add multiple IP addresses here.

  You can add up to 25 IP addresses per exception. However, the combined count of all IP addresses in all exceptions in a policy must be equal to or less than 255.

  You can delete the IP address with help of **Delete** button.

  You can also import the IP addresses from a text file using **Import** button. The maximum limit to import valid IP addresses is 25 per exception.
- Select **IP Address Range** option. Enter **Start IP Address** and **End IP Address**.
- Under Domain Name, type the Domain Name. Click **Add** to add the Domain Name. You can add multiple Domain Names here.

  You can add up to 25 Domain Names per exception. However, the combined count of all Domain Names in all exceptions in a policy must be equal to or less than 255.

  You can delete the Domain Name with help of the **Delete** button.

  You can also import the Domain Names from a text file using the **Import** button. The maximum limit to import valid Domain Names is 25 per exception.
- Click **Next**.

  If you mention remote IP or port, that exception will be for outgoing communications.

m. Under Remote TCP/UDP Ports, do one of the following,

- The **All Ports** option is selected by default.
- Select the **Specific Ports** option and type the port numbers. Use commas in between to add multiple ports.
- Select the **Port Range** option. Enter **Start Port** Number and **End Port** Number.

- Click **Next**.

n. Under Action, select either **Allow** or **Deny**.

o. Under Status, select either **Enable** or **Disable**.

p. Click **Finish**.

The Exception is added at the top position in the Exceptions list. The sequence of the exceptions decides the precedence of the rule. The precedence is in descending order. You can move the exception rule with the **Move Up** and **Move Down** buttons.

5. Click **Save Policy**.

Editing the Exceptions Rule

You can edit the exceptions rule which are created by you. To edit the Exceptions rule, follow these steps:

1. In Exceptions section, select the exception that you want to edit.
2. On the Add/Edit Exception screen, you can edit the name in the Exception Name text box and edit the protocol. The protocol includes: TCP, UDP, and ICMP.
3. Click **Next**.
4. Edit Local IP Address if required, and then click **Next**.
5. Edit Local TCP/UDP Ports if required, and then click **Next**.
6. Edit Remote IP Address if required, and then click **Next**.
7. Edit Remote TCP/UDP Ports if required, and then click **Next**.
8. Under Action, you can select either **Allow** or **Deny**.
9. Under Status, you can select either **Enable** or **Disable**.
10. Click **Finish**.
11. Click **Save Policy**.

Deleting the Exceptions Rule

You can delete the exceptions rule that you have created. To delete the Exceptions rule, follow these steps:

1. In Exceptions section, select the exception that you want to delete.
2. The action bar is enabled above the table. In the drop down, select **Delete**.
3. Click **Submit**. The selected exception rule is deleted.
4. Click **Save Policy**.

Exporting the Exceptions Rule

You can export the exceptions rule that you have created. To export the Exceptions rule, follow these steps:

1. In Exceptions section, select the exceptions that you want to export.
2. Select Action > Export. The Opening firewall_exception.json dialog appears.
3. Select **Save File**.
4. Click **Ok**.
   The database file, firewall_exception.json is downloaded.

Importing the exceptions Rule

You can import the exceptions rule that you have created in the earlier versions of Thirtyseven4 EDR. To import the Exceptions rule, follow these steps:

1. In Exceptions section, click Add > Import. The File Upload dialog appears.
2. Select the database file, firewall_exception.json.
3. Click **Open**.
   The database file, firewall_exception.json is imported.

Web Security

This feature helps you create security policies for an endpoint or group where Browsing and Phishing Protection can be enabled. This blocks malicious and phishing Web sites. You can restrict or allow access to the internet and Web sites as per your requirement.
The following settings are provided under Web Security:

- Browsing and Phishing
- Block Web Categories
- Block Specific Websites
- Schedule Internet Access
- Alerts and Reports
- Google Access Controller
- YouTube Access Controller

Browsing Protection

While users visit malicious Web sites some files may get installed on their systems. These files can spread malware, slow down the system, or corrupt other files. These attacks can cause substantial harm to the system.

Browsing Protection ensures that malicious Web sites are blocked while the users in a group are accessing the Internet. Once the feature is enabled, the site that is accessed is scanned and is blocked if found to be malicious.

Phishing Protection

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. These emails usually appear to have been sent from seemingly well-known organizations and sites such as banks, companies and services seeking for your personal information such as credit card number, social security number, account number or password. Administrators can enable Phishing Protection that prevents users from accessing phishing and fraudulent Web sites. As soon as a site is accessed, it is scanned for any phishing behaviour. If found fraudulent, then it is blocked to prevent any phishing attempts.

Web Categories

There are certain concerns that most organizations may face:

- System infection by malware.
- Users browsing unwanted Web sites.
- The employees idling away time.
  To avoid these concerns the administrators need to have a policy that regulates users and their Web access activities.
  The Web Categories feature helps the administrators centrally control and manage the browsing behavior of the users. The administrators can create different security policies for different groups according to their requirements and priorities.

Creating a new Web Security Policy

To configure policy for Web Security, follow these steps:

1. Create Container/feature policy for Web Security.
2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and Enable settings that you want to configure.
   - Browsing and Phishing
   - Block Web Categories
   - Block Specific Websites
   - Schedule Internet Access
   - Alerts and Reports
3. Expand **Browsing and Phishing**. Select either of the following or both the check boxes:
   - Browsing Protection

- Phishing Protection

4. Enable and Expand Block Web Categories.
5. Select **Protection level**, Low, Medium, or High.
6. This restricts or allows access to the Web sites based on their categories as per the security policy of your organization. If you block a category, all the Web sites referring to the category will be blocked.
   - The Web categories are enabled, and you can allow or deny access to each category.
   - From Status column, select either **Allow** or **Deny**.
7. Enable and expand Block specified websites. You can enter the Web sites that you want to block. For details, see Block specified websites.
8. Enable and expand Schedule Internet Access and do the following:
9. Select one of the following options:
   - Always allow access to the internet
   - Allow access to the internet as per schedule – When you select the option, Allow access to the internet as per schedule, you can add the schedule time.
     a. Click **Add** to add the schedule. Add Time Interval dialog appears.
     b. Select the **Weekday** from the list.
     c. Select the **Start at** and **End at** hours.
     d. Click **OK**.
     You can delete the schedule entry if the entry is not required.

   Note
   SSL versions earlier than 3.1 are not supported for Schedule Internet Access.

10. Enable and expand Alerts and Reports.
11. Select either of the following or both the check boxes:
    - **Display Alert Message** – when website is blocked.
    - **Generate Web Security Reports** – To generate reports for all blocked Web sites. If you select this option, a large number of reports will be generated depending upon the Web usage.
12. To save your settings, click **Save Policy**.
    Importantly, if you have customized the settings and later you want to revert to the default settings, click the Reset Default button.

Exclusion for Browsing Protection and Phishing Protection

Exclusion enables you to apply an exception rule to the protection policy for Browsing Protection and Phishing Protection. This helps you exclude the URLs of the sites that are actually genuine, but get erroneously detected either as malicious or phishing sites. You are recommended to exclude only those URLs that you trust to be safe and genuine.
You can exclude the URLs in the following way:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Policies > Container Policies > Web Security.
3. In the Browsing and Phishing section, under Exclude URLs, type the URL and then click Add. The Report Miscategorized URL dialog appears. You can report about miscategorization of the URL to the Thirtyseven4 EDR lab if the URL is detected as malicious or phishing site.
4. Select one of the reasons from the following:
   - URL is getting detected as Malicious
   - URL is getting detected as Phish
5. To report about miscategorization, click **Yes**. If you do not want to report about miscategorization, click **No**. The URL is added in the Exclude URL list.
6. To save your settings, click **OK**.
   In the action bar, you can perform the following actions:

Action	Description
Add	Helps you exclude a URL from being detected as malicious or phishing.
Delete	Helps you delete a URL from the Excluded URL list.
Report	Helps you report if a URL is miscategorized.

Exclusion for Web Categories

Exclusion helps you apply an exception rule to the protection policy for Web Categories. This helps you when you want to restrict access to a Web site category, but you want to allow certain Web sites from the restricted category.
You can enlist such Web sites in the Exclusion list in the following way:

1. Log on to the Thirtyseven4 EDR Security.

2. Go to Policies > Container Policies > Web Security.
3. Click the **Exclusion** button. The Exclude URLs dialog appears.
4. In the Block Web Categories section, under Exclusions, type the URL and then click **Add**. The URL is added in the Exclude URL list.
5. To exclude the subdomains, in the column **Exclude Subdomain**, select option **Yes** or **No**.
6. To save your settings, click **OK**.

Action	Description
Add	Helps you exclude a URL from being restricted even if it belongs to the blocked category.
Delete	Helps you delete a URL from the Excluded URL list.

Block Specified Websites

This feature is helpful in restricting access to certain Web sites or when a Web site does not fall into an appropriate category. It is also helpful if you have a shorter list of the Web sites that you would prefer to restrict the Web sites than blocking the entire category.
To block Web sites, follow these steps:

1. Log on to Thirtyseven4 EDR Security.
2. Go to Policies > Container Policies > Web Security. The Block specified websites features (Add, Delete, Delete All) are activated.
3. Type a URL and then click **Add**.
4. If you want to block the subdomains, select the option **Yes** or **No** in **Block Subdomains** column. For example, if you block www.google.com and enable 'Block Subdomains', all its subdomains such as mail.google.com will also be blocked.
   You can delete the URL, if required.

   Note
   The Block Subdomains feature is not applicable for the clients with Mac operating systems.

Google Access Controller

Here you can add Email domains related to your organization to log in to your Google account.

1. Enable and expand **Google Access Controller**.
2. The settings done on the Configuration page are displayed here. You can change the settings if required.

3. Enter **Email Domains** to log in to your Google Account in the correct domain name format. The domain name should include the domain name and top-level domain.
4. Click **Add**.

The entry is added to the Domain list. This feature allows user to access google account only through the Email domains added in the list.

You can delete the domain names if not required.

YouTube Access Controller

On the YouTube platform, channels and videos are arranged using YouTube video categories.
Some examples of YouTube Video Categories are,

- Film & Animation
- Autos & Vehicles
- Music
- Pets & Animals
- Sports
- Short Movies

Here you can block or allow YouTube categories to watch the videos.

1. Enable and expand **YouTube Access Controller**.
2. The settings done on the Configuration page are displayed here. You can change the settings if required.
3. By default, the YouTube Categories Access is selected as **Allow all**. You can select the option **Deny all** to deny all the YouTube Categories.
   To allow some categories and deny some categories, select the option **Custom**. You can select Allow or Deny option as per required access to the YouTube Categories.

Exclusions by YouTube Attribute
Exclusion enables you to apply an exception rule to the YouTube Categories Access policy. This helps you to allow YouTube videos that you want to watch from blocked categories.
You can exclude YouTube category by channel or publisher. YouTube Channel is a personalized home where all the videos the creator uploads. The YouTube Channel handle terminology is named as **Publisher** here for easy understanding.
For more information about Handles, see YouTube Handle.
To exclude YouTube category, do the following steps:

1. Click **Add**.
   The Exclusion by YouTube attribute dialog appears.
2. Select **Channel** or Publisher.
3. Enter the **Channel/Publisher name**.
4. Click **Add**.

The entry is added to the list.
You can delete entry if not required.

Block by YouTube Attribute
Blocking helps you to block YouTube videos from allowed categories.
You can block by channel or publisher. YouTube Channel is a personalized home where all the videos the creator uploads. The YouTube Channel handle terminology is named as **Publisher** here for easy

understanding.
For more information about Handles, see YouTube Handle.
To block YouTube category, do the following steps:

1. Click **Add**.
   The Block by YouTube attribute dialog appears.
2. Select **Channel** or Publisher.
3. Enter the **Channel/Publisher name**.
4. Click **Add**.

The entry is added to the list.
You can delete entry if not required.

Exclusion for Schedule Internet Access

You can exclude certain known websites from getting it blocked. Excluded URLs/Websites will not get blocked even if internet is restricted.
You can enlist such Web sites in the Exclusion list in the following way:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Policies > Container Policies > Web Security.
3. In the Schedule Internet Access section, under Exclusions, type the URL and then click **Add**. The URL is added in the Exclude URL list.
4. To save your settings, click **OK**.

Action	Description
Add	Helps you exclude a URL from being restricted even if internet is restricted.
Delete	Helps you delete a URL from the Excluded URL list.

Application Control

Organizations usually face the following concerns while using applications:

- No illegal or fake applications should be installed on client systems.
- Malicious applications should not infect the systems.
- Unnecessary applications should not clog the systems.
  With this feature, you can authorize or unauthorize the users to access and work with certain applications, so that no one accesses an unwanted application.
  You can create various policies based on the requirement of the groups or departments. For example, for the users of the Marketing Department, you can allow access to File

Sharing Applications and Web Browser while restrict access to all other applications. For the Accounts Department, you can allow access to Archive Tools and Web Browsers only.

Note
The Application Control feature is available only in the clients with Windows operating systems.

Application Control

To configure policy for Application Control, follow these steps:

1. Create Container/feature policy for Application Control.
2. On the Application Control page, the following settings are available. You can use only one of them at a time.
   - Allow All Applications
   - Block All Applications
3. Click **Save Policy**.

Allow All Application

1. Toggle On the **Allow All Application** setting and expand.
2. You can authorize/unauthorize application as per your requirement. To customize the access to the application, click the corresponding option in the Custom column. The list of applications under the selected category is displayed in the table.
3. On the Feature Policy page, If you want to send a notification when a blocked application is accessed, select **Notify when an unauthorized application is blocked**.

Block All Applications

1. Toggle ON the **Block All Applications** Settings and expand.
2. To add allowlist, click **Add**.
   Add allowlists dialog appears. A list of existing allowlists is displayed with details.
   You can select existing allowlist.
3. Select an allowlist from the list. You can create a new allowlist on the Configuration > Application Control page.
4. Click **Add**.
5. Select one of the following modes.
   - **Monitoring** (Recommended): Use Monitoring mode to analyze the unauthorized application usage for a few days. Fine-tune the allowlist prior to switching to Enforcement mode. Unauthorized applications will only be reported.

- **Enforcement**: Unauthorized applications will be blocked and reported.
  Select the **Notify user when an unauthorized application is blocked** check box to receive a notification when an unauthorized application is blocked.

Advanced Device Control

While working with data storage devices such as CD/DVDs and USB-based devices such as pen drives, organizations are concerned with the following:

- Autorun feature does not activate any infection.
- Unnecessary data or applications do not clogs the systems.

This feature allows the administrators to create policies with varying rights. For example, administrators can block complete access to removable devices, give read-only and no write access so that nothing can be written on the external devices. They can also customize access to admin configured devices. Once the policy is applied to a group, the access rights are also applied. You can use the exception list to exclude the devices from the device control policy.

Advanced Device Control

To configure policy for Advanced Device Control, follow these steps:

1. Create Container/feature policy for **Advanced Device Control**.
2. On the Feature Policy page, you can see list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.
3. Enable **Advanced Device Control**.
4. Expand **Storage Devices**. The following list of storage devices is displayed:
   - USB Storage Device
   - CD/DVD
   - Internal Card Reader
   - Internal Floppy Drive
   - ZIP Drive
     For the above devices, select the permissions as per your requirement.
5. Enable and expand **Card Readers**. The following list of Card Readers is displayed:
   - Card Reader Device (MTD)
   - Card Reader Device (SCSI)
     For the above devices, select the permissions as per your requirement.
6. Enable and Expand **Wireless**. The following list of Wireless networks is displayed:

- Wi-Fi (Customize)
- Bluetooth
  For the above network, select the permissions as per your requirement.

7. To authorize Wi-Fi connections, click **Customize** link.The 'Authorized Wi-Fi Connections' dialog appears.
   Select one of the following options.
   a. Allow for all Wi-Fi access points
   b. Allow only for authorized Wi-Fi access points – If you select this option, do the following.
   c. Enter SSID in the text box.
   d. Enter MAC address in the text box.
   e. Click Add. The network data is added. You can delete the data with help of Delete button.
   f. Click Ok.

   Note
   Customize (Authorized Wi-Fi connections) feature is not supported on Mac operating system.

8. Enable and expand **Mobile & Portable Devices**. The following list of Mobile & Portable Devices is displayed:
   - Windows Portable Device
   - iPhone
   - iPad
   - iPod
   - BlackBerry
   - Mobile Phones (Symbian)
   - Scanner & Imaging Devices
     For the above devices, select the permissions as per your requirement.
9. Enable and expand **Interface**. The following list of Interface mode is displayed:
   - FireWire Bus
   - Serial Port
   - SATA controller
   - Thunderbolt
   - PCMCIA Device

- USB
  For the above interfaces, select the permissions as per your requirement.

10. Enable and expand **Camera**. For Webcam, select the permissions as per your requirement.
11. Enable and expand **Others**. The following list of other devices is displayed:
    - Local Printers
    - Teensy Board
    - Network Share
    - Unknown Device
      For the above devices, select the permissions as per your requirement.
12. Enable and expand **Exceptions**. Ensure that you have added the devices in Configuration > Device Control > Add devices. Then do the following:
    a. Click **Add**. The 'Managed Devices' dialog appears.
    b. Select one or more devices to add to the exception list.
    c. Click **Add**. The devices are added in the Exceptions list.
    d. Set the access permissions as required.You can delete the devices with help of **Delete** button.
13. To save your setting, click **Save Policy**.
    This policy is applied to all the devices that are configured in the list. Even if you add a device, the same policy will apply unless you customize the policy.
    Importantly, if you have customized the settings and later you want to revert to the default settings, click the **Reset Default** button.

For Windows Clients

- Only NTFS is supported for Partial encryption.
- USB Pen Drives with GUID Partition Table (GPT) Partition Style cannot be added for authorization.
- If an authorized and encrypted device is formatted, the device will be treated as unauthorized. Hence, Administrator will need to add the device again in Device Control and configure the policies accordingly.
- Some devices (e.g. Nokia phones, BlackBerry phones) may need system reboot or device reattachment for device access rights to be applied.
- On blocking SATA Controller from Advanced Device Control, you may frequently see SATA Controller blocked prompts even when actual blocking is not performed.

- While any ongoing session of Webcam or Bluetooth is in progress, changing access right to block will not interrupt this current ongoing session. The device may need reattachment or system reboot for access rights to be applied.

For Mac Clients

- If the option Read only is selected in Advanced Device Control of SThirtyseven4 EDR and a USB device is attached, such a device may not be accessible from the left pane in Finder for some time.
- If a USB device is already attached to the machine and you are installing Mac client, the device may not be shown as mounted for a fraction of seconds.
- If an NTFS USB device is attached to the machine during installation of Mac client, two copies of the attached USB may be visible for a few seconds.
- If a USB device is to be shown as mounted or un-mounted using terminal commands, the Device Control policy will not apply to that device.
- If you are installing Mac client on Mac OSx 10.9 while an FAT USB device is attached to the machine, such a device will not be displayed as mounted. To show the device mounted, you need to disconnect the device and reconnect it.
- iDevices, Internal Card Reader, Webcam, CD-DVD, mobile phones and HFS encrypted devices may need device reattachment for device access rights to be applied.
- Exception functionality will not be applicable for Bluetooth, Wi-Fi, Webcam, External CD-DVD.
- Mobile phones except iDevices that are connected in 'USB Mass Storage' mode will be detected under USB storage device category.
- Mobile phones connected in MTP mode will be detected under 'Windows Portable Devices' category.
- Blocking functionality will not work for Blackberry mobile if the mobile is connected to Mac system in Sync Media.
- USB storage device would not be formatted with Mac OS extended (Journaled, Encrypted) file format.

For Linux clients

- The Read only option set for internal CD/DVD on the Thirtyseven4 EDR server, is treated as Blocked on the Linux client.
- Wireless adapters are not supported.
- Bluetooth USB dongle may not be supported on some operating systems.
- In all supported Linux OS, internal CD-DVD tray will not open if block mode is set for CD-DVD"

- If DC configuration is changed from Read-only mode to Allow mode, the USB drives may not work accordingly.
- UMS Mobile Phones do not work in Read-only mode. Changing the mode using the option available in the device will connect it to the endpoint. If the device is plugged out, the device in a particular mode does not change the mode automatically.

Data Loss Prevention

You can prevent unauthorized loss, pilferage, or leakage of confidential company data using the Data Loss Prevention (DLP) feature.
It is necessary to enable DLP on endpoints. To do this, see DLP License.
The DLP policy can stop an unauthorized activity that is carried out through the following channels:

- Using the Print Screen option to save the screenshot (Applicable only for Windows platform). The file/data is not monitored.
- Using Removable Devices to copy data (Applicable only for Windows platform)
- For selected File Types, the Removable Devices go to 'Read Only' mode when 'Monitor Removable Devices' option is selected.
- Using Network Share accessed using UNC Path or Mapped Network Drive (Applicable only for Windows platform).
- Using the Clipboard to paste information from one application to another.
- Using printer activity, printing through local and network printer. The file/data is not monitored. (Applicable only for Windows platform)
- Using online services of third-party Application/Services to send data such as email, file sharing apps, cloud services, Web browsers and other applications using social media.

Note
User need to purchase a DLP pack separately to avail this policy.

Data Loss Prevention

To configure policy for Data Loss Prevention, follow these steps:

1. Create Container/feature policy for **Data Loss Prevention**.
2. On the Feature Policy page, you can see list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.
    - Data Loss Prevention
    - Add-on Features
    - Data Transfer Channels

- Data Settings
- Exceptions

3. Enable Data Loss Prevention. Select the Display alert message on DLP policy violation check box.
4. Select Action to configure the action to be performed after the attempts is carried out, either Report only or Block and Report. Alert prompts will not be displayed for Report Only action.
    1. In the Add-on section, the following 2 add-on features are available.
        - File Classification
        - Optical Character Recognition (OCR)
        - Select the **Always show pop-up to classify a new file** check box if you want to view pop-up every time when you create a new file.
        - Select the **Optical Character Recognition (OCR)** check box. You can view list of supported OS versions for OCR by clicking the link, Supported OS list.

        File Classification

        When a new Microsoft Office file is generated, DLP asks to classify the file as Confidential or Public. You can classify existing files also. Files classified as confidential are treated as sensitive files and any operation to leak is blocked/reported as per DLP policy. This is regardless of the content of the file.

        Files classified as Confidential will be monitored only for the following Data Transfer Channels,

        - Removable Devices
        - Network Share
        - Application/Online Services

Select the **Always show pop-up to classify a new file** check box if you want to view pop-up every time when you create a new file.

5. When you create a new MS Office file, save and close it, a Thirtyseven4 EDR File Classification dialog appears. The dialog appears only for MS Office files.
6. Select the classification level as **Public** or **Confidential**.
7. Click **OK**.

The overlay icon of classified file appears as per classification.

When you copy a file, classify the copied file as per above procedure.

The overlay icon of classified file appears after system or Windows Explorer is restarted after client is installed.

To classify existing files, follow the given steps:

8. Select the files to be classified. You can select maximum 100 files at a time.
9. Right click the selected files and select **Thirtyseven4 EDR File Classification** > classification level as **Public** or **Confidential** or **Unspecified**.

   A Thirtyseven4 EDR File Classification dialog appears showing result. The lay over icon of classified files appears as per classification.

You can remove the classification, by selecting **Unspecified** option.

Manual classification is supported only on NTFS.

Optical Character Recognition (OCR)

Optical Character Recognition feature is disabled by default.

The confidential/user defined data from image files is identified in case of data leak and action is performed as per policy. The image details are mentioned in the DLP report.

OCR supports the following image formats,

- JPEG (or JPG) - Joint Photographic Experts Group
- PNG - Portable Network Graphics
- GIF - Graphics Interchange Format
- TIFF - Tagged Image File
- BMP - Bitmap image files

OCR is applicable only for the following Data Transfer Channels,

- Removable Devices
- Network Share
- Application/Online Services

Limitations

- OCR does not support embedded images scanning.
- Only Roman (English) alphanumeric script is detected from the images.
- Only clear and high-quality images are detected by OCR. The blur, distorted, too small or too large images may not be detected.

OCR feature in DLP is available in Microsoft Windows Vista SP2, Windows 7 SP1, and above Personal computer versions and Windows Server 2008 SP2, Windows Server 2008 R2 SP1, and above Server versions.

10. Expand Data Transfer Channels. Select the channels that you want to monitor from the following options:
    - Print Screen (applicable only in Windows platforms)
    - Removable Devices (applicable only in Windows platforms)
    - Network Share (applicable only in Windows platforms)
    - Clipboard
    - Printer Activity (applicable only in Windows platforms)
    - Application/Online Services
11. Select the applications that you want to monitor for attempts at data pilferage by clicking the Applications list. Do one of the following:
    You can select all the applications in the group.
    - Select the applications one by one after expanding the group caret.
    - Select all Mac platform applications by clicking the Mac group icon.
    - Select all Windows applications by clicking on the Windows icon.
    - Select all Web Browsers or one by one after expanding the group caret.
    - Select all E-mail applications or one by one after expanding the group caret.
    - Select all Instant Messaging applications or one by one after expanding the group caret.
    - Select all File Sharing/Cloud Services applications or one by one after expanding the group caret.
    - Select All Social Media/Others applications or one by one after expanding the group caret.
12. To configure email SSL settings, select the Enable Email scanning over SSL check box. This is applicable only when you select Email option in the Application / Online Service. Ensure that you perform the procedure to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.
13. Expand Data Settings to configure the settings for File Types, Confidential Data, and User Defined Dictionary.
14. Select the Monitor File Types check box. Select the File Types caret from the following:
    - Graphic Files (Audio, Video, Images)
    - Office Files (MS Office, Open Office, Kingsoft Office)

- Programming Files
- Other Files (Compressed files etc.)

15. To add the Custom Extensions, do the following:
    a. Select the **Custom Extensions** check box.
    b. Click **Add** button. Add Custom Extensions dialog appears.
    c. Type an extension in the text box and press enter.
    d. Click **Add**.
    You can delete the custom extension with the help of delete icon.
16. Select the Monitor Confidential Data check box. Select the Confidential data carets from the following:
    - Confidential data such as Credit/Debit Cards
    - Personal information such as Social Security Number (SSN), Email ID, Phone Numbers, Driving License Number, Health Insurance Number, Passport Number, ID, International Banking Account Number (IBAN), Individual My Number, Corporate My Number, Pin Code, Aadhar Number, Vehicle Registration Number, Drug Enforcement Agency Number, Australia Tax File Number, Australian Business Number, and Australia Medical Account Number.
    - Select the Monitor User Defined Dictionary check box. The User Defined Dictionaries are created at Data Loss Prevention.
    - The words/strings must be flagged if used in communication.

    Note
    You can either choose to be notified through email notification when an attempt is made to leak information, or prevent the attempt from being carried out successfully.
17. Expand Action to configure the action to be performed after the attempts is carried out, either Block and Report or Report only. Alert prompts will not be displayed for Report Only action.
18. Expand Exceptions. To add the domain names that you want to exclude from Data Loss Prevention, do the following:
    a. Enter the domain name in the text box.
    b. Click **Add**. You can see the list of domain names. You can edit, delete and export the domain names.
    c. To import the domain name, click **Import**. The File Upload dialog appears.
    d. Select the valid exported domain data file.

e. Click **Open**. The database file is imported.

Note

- *Domain Exceptions support the Windows platform only.*
- *Domain Exceptions support Microsoft Outlook and Thunderbird email clients only.*
- *If sender and receiver are from different domains, add both domain names in Domain Exception.*

19. In Application Whitelisting, you can import application in .dat file format to exclude applications from Data Loss Prevention. Do the following:
    a. To download DLP Application Whitelisting Tool, click **Download**.
    b. After downloading the Whitelisting Tool, add applications for DLP whitelisting in the tool.
    c. Generate DLPAppWhiteList.dat file.
    d. Click **Import** to import DLPAppWhiteList.dat file. The applications are whilelisted.
20. To add the network paths, do the following:
    a. Enter the Network path the text box.
    b. Click **Add**.
    c. You can see the list of Network path. You can edit, delete and export the Network path.
    d. To import the Network path, click **Import**. The File Upload dialog appears.
    e. Select a valid exported network share data file.
    f. Click **Open**. The database file is imported.

    Note

    Network path supports the Windows platform only.
21. Click Save Policy.

Note
For Mac Client:

- *Confidential & User Dictionary Data will not be blocked in subject line, message body of email or messenger communication.*
- *Prompts and report will be generated in case if monitored file type is downloaded.*
- *Certain file types (POT, PPT, PPTX, DOC, DOCx, XLS, XLSX, RTF) containing unicode data will not be blocked.*

- *Thirtyseven4 EDR provides you an advanced scanning feature, Data-At-Rest Scan. With this feature you can search for a particular type of data in various formats.*

Update

When a work environment has a large number of systems installed, the challenge that the administrators usually face is how to update all the endpoints for security patches.
This feature allows you to create policies for taking the updates automatically for the endpoints. You can create policies that help different clients take the updates from different sources. Taking the updates from different sources reduce the load on a single server.

To configure policy for Update Settings, follow these steps:

1. Create Container/feature policy for **Update**.
2. Enable and expand **Automatic Update**.
3. To display notification window when the updates are taken, select the **Show update notification window** check box.
4. Under **Frequency**, set the schedule when you want to take the updates.
   - Automatic
   - Custom
     If you select **Custom**, **Daily Start at** and **Repeat after**, lists are activated, you can set the schedule as per your requirement.
5. Under Update Mode, when Thirtyseven4 EDR is installed on private IP (Private IP natted to Public IP), the following update settings can be configured:
   - Download from Internet
   - Download from Specified Update Agents
     If you select **Download from Specified Update Agents**, Update agent list is activated. Select the Update Agent from the list. The Antivirus Setup will be downloaded from the first Update Agent. If any Update Agent fails, the updates will be downloaded as per the sequence in this list. You can reorder this list to change the sequence.
     If all the Update Agents fail, then the Antivirus Setup will be downloaded from the Thirtyseven4 EDR Internet center.
6. To save your settings, click **Save Policy**.
   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the **Reset Default** button.

Internet

This feature gives the administrators a wider choice of creating policies for the client modules that need Internet connection to function. You can configure different settings for the server

and port so that the client modules such as; Quick Update, Spam Protection, Web Security, and Messenger have Internet connection. This is very helpful in allowing the client modules to function in a secure work environment where default Internet connection is not allowed.
To configure policy with Internet Settings, follow these steps:

1. Create Container/feature policy for **Internet**.
2. Enable **Proxy Setting**. The proxy settings details are activated.
3. Select the **Proxy Type** as HTTP Proxy, Socks V 4 or SOCKS V 5 as per your settings.
4. In the **Proxy Server** text box, type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com).
5. In the **Port** text box, type the port number of the proxy server (For example: 80).
6. In the **User Name** and **Password** text boxes, type in your proxy server credentials.
7. Click Next.
8. To save your settings, click **Save Policy**.
   Importantly, if you have customized the settings and later you want to revert to the default settings, you can use the **Reset Default** button.

   Note
   The Internet Settings feature is applicable for the clients such as Microsoft Windows, and Mac operating systems.

Miscellaneous

This feature helps to receive notification to the given Email ID, give access to client settings. This feature allows you to create a policy that authorizes the clients to receive notification to the given Email ID, to access client settings and change their own password, enable or disable Safe Mode Protection, Self Protection, and News Alert.

Miscellaneous

1. Create Container/feature policy for **Miscellaneous**.
2. Enable and expand **SNMP Configuration**. Here you can enter the IP address of the Simple Network Management Protocol (SNMP) server in your network. This SNMP Server IP Address is sent to the client. As soon as the virus/ransomeware attack incident occurs, the client sends SNMP notification to the SNMP server and to the Thirtyseven4 EDR server also. In the network without SNMP server, the virus attack notification is sent to the Thirtyseven4 EDR server only as per heartbeat interval set for the client. Enter the SNMP Server IP Address in the text box.

3. The Trap notifications can be viewed in the SNMP server where the configuration file, Thirtyseven4 EDR.mib is imported.
4. To give access to the client settings, Enable and expand **Client Password**.
5. In **Enter Password,** type the password and then re-type the same password in Confirm Password field. The clients will have to use these passwords for accessing the client settings.
   The Safe Mode Protection check box is selected by default. Thirtyseven4 EDR recommends that you do not disable this feature.
6. The **Self Protection** setting is enabled by default. Thirtyseven4 EDR recommends that you do not disable this feature.
7. Expand **Data Backup**. Data Backup automatically and periodically (multiple times a day) takes a backup of all your important and confidential files present on the endpoint. If you update any file, then this feature automatically takes backup of the latest copy. In the Data Backup section, do the following,
   a. Default Backup Location is selected by default. The backup data is stored at the default location, by default. Thirtyseven4 EDR server searches all volumes on the local PC and then selects the drive with maximum free space to store the backup data locally.
   b. Select **New Backup Location** option if you want to store your backup data at ther location. Enter the folder path.
   c. Select **Network Path Location** option if you want to store your backup data of all machines on a particular system in the network. Enter the Network Path Location.
   d. Enter **Username** and **Password**.
   e. Click **Test** to verify the location.
      - You may receive an error message, because the server does not have access to the Network Path Location, but client may have access to the Network Path Location.
      - You may receive a success message but ensure that client have access to the Network Path Location.
      - Shared drive will be created using Samba for Linux and Mac.
   f. You can view the list of default extensions by clicking the View Button.
   g. You can add custom extensions to the list as per your requirement. Enter extension and maximum file size in the text boxes.
   h. Click **Add**. You can delete the extension with Delete button.

i. To exclude file extension from the data backup, enter the extension in Exclude File Extension box. Click **Add**. You can delete the excluded extension with Delete button.
While performing backup, avoid including large size files such as PST, media files to ensure stable system performance and network operations. After successful client installation, backup starts after 6 hours. Disable this feature if you have any other provision for data backup (Example: File server backup, Data backup server, etc.)
We have provided a backup facility with Thirtyseven4 EDR. To restore your data, contact Thirtyseven4 EDR Support Team.

8. Expand Desktop Shortcut and Tray Icon. As per requirement, select the check boxes to create shortcuts for the following:
   - Safe Banking
   - Secure Browse
   - You can configure number of days to change the colour of the tray icon if the client is not updated for a set number of days.
     Select number of days to turn the tray icon to red.

     Note
     Desktop Shortcut and change Tray icon colour feature is not supported on Mac operating system.
9. To save your setting, click **Save Policy**.

Patch Scan Policies

This feature allows you to configure patch server for the policies in the network. This helps to install the missing patches on the endpoints.

To configure the patch server, follow these steps:

1. Log on to the Thirtyseven4 EDR Security Web console.
2. Go to **Policies**. Click the Edit icon next to the policy for which you want to configure the patch server.
3. Under Policy Settings, click **Patch Server**.
4. Switch the Configure Patch Server toggle button to turn it on.
5. Expand this section by clicking the Expand icon.
6. From the drop down menu, select the patch server to scan.
7. Select the Use Microsoft patch.....roaming endpoints check box if required.
8. Click Save Policy.

   A success dialog appears.

ETH Scan

To configure policy for ETH Scan, follow these steps:

1. Create Container/feature policy for **ETH Scan**.

   The list of searches which are already been added is displayed.

2. Select all or any of the searches to schedule an ETH scan.

   To select all the searches from the list, select the check box in the header row.

   To select an individual search, select the check box in that row. You can select multiple searches also.

To save your settings, click **Save Policy**.
You can go to Configurations > Endpoint Threat Hunting to create or manage ETH searches.

File Activity Monitor

This feature lets you monitor any suspicious activity related to the confidential files on your computer, local drive, or a removable drive. By default, all files are monitored, you can customize and select the file types and folder paths which you want to exclude from monitoring.

You can exclude the selected file types and folder paths from monitoring actions such as copy, delete, or extension change. Copy action on the local drive is not supported.

You can generate a report for the file activity from the Reports page.

The File Activity Monitor feature is available in clients with Windows and Mac operating systems.

To configure policy for File Activity Monitor, follow these steps:

1. Create Container/feature policy for File Activity Monitor.
2. Enable **File Activity Monitor** with a toggle switch.
3. Select location, Removable Drive and /or Local Drive.

   By default, **Removable Drive** is selected.

4. Select the event check boxes, **Copy, Delete** or **Extension Change** as per drive. By default, Copy event for the Removable drive is selected. Copy operations only to Removable Drive are monitored.
5. In the Exclude File Extensions section, do the following.

   By default, the **Use from Configurations -> File Activity Monitor** check box is selected. So, the list of extensions that are added on the Configurations -> File Activity Monitor page is excluded.

The list of extensions that are already added on this page are displayed.

a. If you want to add custom extensions on this page, clear the Use from Configurations -> File Activity Monitor check box.

b. Enter the extension in the Enter Extension text box, and then click Add.

The file extension should be written without a dot in the following format: xml, html, zip, etc.

The extension is added to the list.

If you want to remove the extension from the list, click the Delete button which appears when you click the list entry.

6. In the Exclude Folders section, do the following.

By default, the Use from Configurations -> File Activity Monitor check box is selected. So,the list of folders that are added on the Configurations -> File Activity Monitor page is excluded.

The list of folders that are already added appears.

a. If you want to add custom folders on this page, clear the **Use from Configurations -> File Activity Monitor** check box.

b. Enter the folder path that you want to exclude, for example. C:\Thirtyseven4 EDR, in the Folder Path text box, and then click **Add**.

For Mac OS, use only forward slash (/) in the folder path. Example: /Users/Admin/ExcludeList.

User can also add path like %Windir%\ which is also supported by Windows OS.

To remove the folder path from the list, click the **Delete** button which appears when you click the list entry.

Note

After adding custom extensions/folders, if you select the Use from Configurations -> File Activity Monitor check box, the custom extensions/folders you have added will be overwritten or lost. Either you can use the list from the Configuration page or the list added on this page.

7. To save your settings, click **Save Policy**.

If the exclusion list in Configurations -> File Activity Monitor is updated, the changes will be reflected in the respective FAM policy, when the **Use from Configurations -> File Activity Monitor** check box is selected.

EDR

Live Query

Configure Live Query settings

For the first time, when you land this page, you need to configure Live Query Settings.

1. Log on to the Thirtyseven4 EDR Security server console.
2. Go to EDR > Live Query.
3. When you open this page for the first time, as Live Query Settings are not configured, you see the message about configuring Live Query Settings. Click **Configure Live Query Settings**.
4. You are redirected to the Configurations > EDR page. For more details, go to EDR OVA Deployment

Run Live Query on Thirtyseven4 EDR Console

Before running a live query, ensure the Live Query Server is reachable.

To run a Live Query, follow these steps.

1. Log on to the Thirtyseven4 EDR Security.
2. Go to EDR > Live Query.
3. From the Platform list, select Windows.
4. Select a table from the list. There is 100+ auto-suggested tables available on the list. Visit this URL https://www.osquery.io/schema/5.6.0 for more reference.
5. Select the host from the list. This is the endpoint on which you want to run the query.
6. The Query appears in the box. Click **Run Query**.
7. Within 30 seconds, the result of the query appears. If the query is more complex and unable to resolve within 30 seconds, an error message appears.
8. You can export the query result by using **Export as XLS** button.
   You can search for a parameter with the Search facility.

Query Limitations: Query execution time: 30 seconds

EDR OVA Deployment

Set up OVA to use EDR Feature

This feature helps you deploy OVA on VirtualBox. OVA (Open Virtualization Appliance) file contains a compressed version of a virtual machine with Live Query and MISP server features. When you deploy an OVA file, the virtual machine is extracted and imported into the virtualization software installed on your computer.

OVA Details

- OVA File name: Thirtyseven4 EDR Security_8.3_UBUNTU22.ova
- Oracle Virtual box version: 7.0.6

Prerequisites

- Thirtyseven4 EDR Security 8.3Server is installed and reachable from the host machine where the virtual machine (VM) is installed.
- Disk space: Minimum 25 GB; Recommended 100 GB and above.
- CPU: Minimum 2 vCPU; Recommended 4 vCPU and above.
- Enable Virtualization in the BIOS of the host machine where the VM will be created. You can refer to your hardware documentation; how to enable virtualization."
- Oracle VM Virtual Box Manager, 7.0.6 or later
- RAM: Minimum 4 GB; Recommended 8 GB and above.
- edr_ova.ova build file
- Internet connection is mandatory to use EDR feature.

Step 1: Download EDR Setup – Fresh Install

1. Log on to Thirtyseven4 EDR Security 8.2.
2. Go to Configuration > EDR.
3. Click the Download EDR Setup button to download the setup OVA file. The OVA file is downloaded.

This is a one-time activity to configure EDR setup.

Step 2: Deploy OVA on VirtualBox

1. Download and install Oracle VM VirtualBox Manager.
2. Open the Oracle VM VirtualBox Manager.

3. Go to File > Import Appliance.
4. In this step, choose a virtual appliance file to import. Click **Browse** and select OVA file downloaded as mentioned above.
5. Click **Next** and follow the wizard.
6. Click **Import**.
7. In the Application Settings, verify the requirement of RAM and HDD. If required, edit the values.
8. Click **Finish**. OVA is imported successfully on the VM.
9. Click **Start** icon to start the VM. The VM is ready for use.

Step 3: Configure EDR Setup

1. Start the VM by double-clicking the icon.
2. Enter Username and password.

   username: livequery

   password: LQfeature001#

   When the user logs in for the first time, a one-time initialization script is invoked.

   This is an interactive communication where the user is required to provide the requested inputs as follows.

3. Enter hostname (FQDN) and hit [Enter]. This Hostname is used for logging into the MISP server and configuring live Query on the Thirtyseven4 EDR Security console.
4. A message about Certificate management appears. To generate a new certificate, type 1 and hit [Enter].

   If the certificate already exists, type 2 and hit [Enter]. Copy and paste the certificate content and hit [Enter].

5. Set the console URL. Provide the IP/Hostname of the Thirtyseven4 EDR Security server.
6. Enter Port Number for Live Query TLS server. TLS Server port number is 6443 by default. You can change it if required. To continue, hit [Enter].
7. Port number for MISP Server is 8443. You can change it if required. To continue, hit [Enter].
8. Live Query TLS server will be configured. Wait for a few seconds as the Live Query TLS server is initializing.

The success message appears.

Link to access MISP UI appears. Note down the link.

MISP credentials appear. Note down username and password which are required to generate an "Authentication Key" to be entered on Thirtyseven4 EDR Console UI.

MISP and Live Query server are installed successfully.

1. After OVA configuration, to initialize the system the following options are available.
2. View MISP Settings
3. Certificate Management
4. Set console URL.
5. Restart Livequery
6. Check for updates – Check for Live Query updates
7. Reboot System Now
8. Shutdown System Now
9. Quit

You can select the option and type the corresponding number and hit [Enter].

About Updates

- Every midnight the updates are checked and applied automatically
- On-demand updates can be set through the option 5 mentioned above
- Updates are available for Live query only

Configurations

On the Configurations page, you can perform the following:

- Active Directory
- Client Installation
- Device Control
- Data Loss Prevention
- Application Control
- Asset Management
- SMTP Settings
- Internet Settings
- Roaming Service
- Endpoint Threat Hunting
- Patch Management
- File Activity Monitor

Active Directory

Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.

In organizations (Medium/Large), Active Directory is used for maintaining user databases, configuring central policies, and pushing applications to users. For any organization, it is very important that you can log in to any application using existing active directory users. You don't have to create other users specific to the application itself.

Active Directory Users can log in to any application within the network. Active Directory User credential is used to log in to the applications.

Here provide Active Directory details so that the user can log in to the Active Directory. This feature is accessible for Admin User only.

To connect with the Active Directory, follow these steps.

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configuration** > **Active Directory**.
3. Select the **Enable Active Directory Settings** check box.

4. In the **Domain Name** text box, type the Active Directory domain name. Please note the Domain Name. To log on to Thirtyseven4 EDR for the next session, you will require this Domain Name.
5. For user authentication, type the user name in the **Domain Admin User name** text box.
6. In the **Password** text box, type the password.
7. Click **Test Connection**. The success message appears if the connection to the Active Directory server is successful.
8. Click **Apply**. The configuration success message appears.

   The Active Directory Server is configured successfully.

Client Installation

On this page, you can verify the client installation path and set the automatic uninstallation of another antivirus software.

Client Installation Path

On this page, the client installation path appears. The client will be installed at this path.

You can modify the path if required.

Uninstalling another Antivirus Software

While installing the client, if another antivirus software is already present on your endpoint, client installation does not proceed further until you uninstall the other installed antivirus software to avoid conflicts.

If this option is selected, the client will uninstall other antivirus products after client agent installation. Thirtyseven4 EDR client installation will fail if it's not able to uninstall another antivirus. The failure notifications will be displayed on Thirtyseven4 EDR Web Console **Dashboard > Notifications**.

Thirtyseven4 EDR installation will not be completed until the other antivirus is uninstalled manually.

Before you begin,

- Turn off the following settings for other antivirus (AV) present on the endpoints
  - Password protection
  - Self/Tamper protections
- Turn Off Windows Defender of the server OS. For Windows Server 2019 and Server 2022, you need to uninstall Windows Defender.

- Before mass deployment, test on one endpoint whether the Thirtyseven4 EDR is able to uninstall another antivirus.

Please note,

- Some antivirus products require a password while uninstallation. User need to provide password if prompted.
- The other Avs where user interface is displayed while uninstallation.
  - if the user is logged off, the other AV will be uninstalled when the user logged in.
  - Uninstallation is supported for the users logged in with Admin privileges.
- The other AVs with silent uninstall support, will be uninstalled seamlessly.
- If the other AV uninstallation is interrupted (Example: password not provided, uninstallation user interface closed by user, etc.), uninstallation will be attempted in the next periodic interval.
- If the other AVs do not have uninstall support or If Thirtyseven4 EDR is not able to uninstall another AV, you need to uninstall the other AV manually.

Set the automatic uninstallation of another antivirus

On this page, you can set the automatic uninstallation of another antivirus software.

1. To uninstall the currently existing other antivirus from the endpoints automatically, select the **Uninstall other Antivirus if present** check box.

   By default, the check box is not selected.

   As the option is not selected, if other antivirus is already installed, then the Thirtyseven4 EDR client installation will fail.

   On a console, you will receive a notification.
2. Click **Apply**.
3. Download the client packager for Thirtyseven4 EDR client installation.

Note: If the client agent was already created when '**Uninstall other Antivirus if present**' check box is disabled, you will need to create it again by enabling '**Uninstall other Antivirus if present'** checkbox and reinstall client agent again with this client packager.

Select preference to download client build

You can select the option from where you can download the client build. You can select one of the following options.

- **Download from Thirtyseven4 EDR Server** – If you select this option, the client build is downloaded from the Thirtyseven4 EDR server. If the **Fall back to download from**

Thirtyseven4 CDN location check box is enabled, the endpoint will download client build from Quick Heal CDN Location if the Thirtyseven4 EDR server is busy.

- **Download from Thirtyseven4 CDN location**. – If you select this option, the endpoint will directly download client build from TS4 CDN location.
- **Download from your own custom file server** – Before you select this option, copy the builds folder from '/opt/Thirtyseven4 EDR_EndPoint_Security/deployment/clientpackager/' location to your own file server.
  Now here give the path of the file server where the client builds folder is copied.

This feature is applicable only for the clients with Microsoft Windows operating system.

Device Control

This feature helps you to add USB. If your organization has a large number of USB storage devices of the same make and model, you can add these USBs by model name.

You can add other devices also, Example: Scanner, Card Reader, Local printers, Mobile phones etc.

Adding USB Device

To add USB device, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Device Control**.
3. The list of devices which are already added appears. Click the **Add devices** button and select USB Devices. The Add Device dialog appears.
4. Follow the procedure mentioned in the dialog.
5. Click **Browse** to upload the Device Control file.
6. Click **Add**.

Adding USB Device by Model Name

To add USB device by Model name, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Configurations > Device Control.
3. The list of devices which are already added appears. Click the Add devices button and select USB by Model to add device by Model. The Add Device by Model Name dialog appears.
4. Enter Device name.
5. Select a mode from the Mode to add Model Name list. Select one of the following modes:

- From the list: A list of pre-specified device model names appears. Select a model name from the list.
- Manually: Enter model name.

6. Follow the procedure mentioned in the For Windows / For MAC tab as per the endpoint operating system.
7. Click Add.

   Note:
   To add multiple USB devices, remove all the connected USB devices. Attach the USB device that you want to add and follow the above procedure.

8. Select the devices that you want to manage from the displayed list and click OK.
   After the device appears in the list, toggle the button under Authorized to Yes or No as required. You can also use the Edit icon that appears to change the device name as it appears or use the Trashbox icon to delete the device from the list.

   Note
   If you set the device authorized permission to 'No', then that device cannot be added to the exceptions list.

9. To add the device to the exceptions list, go to **Policies > Advanced Device Control**.
10. Click **Exceptions**.
11. Click **Add**. The Managed Devices dialog box appears.
12. Select one or more devices to add to the exception list.
13. Click **Add**.
14. The devices are now added in the list of exceptions.
15. You can delete the devices with help of **Delete** button.
16. Set the access permissions as required.
17. Click **Save Policy**.

    Note:
    To add multiple USB devices, remove all the connected USB devices. Attach the USB device that you want to add and follow the above procedure.

Adding USB by Serial Number

You can use this option to add the USB by serial number without connecting the USB.

To add a USB by Serial Number, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.

2. Go to **Configurations > Device Control**.
3. The list of devices which are already been added appears. Click the **Add devices** button and select USB by Serial Number. The Add Device by Serial Number dialog appears.
4. Enter **Device Name**.
5. Enter **Serial Number** of the device.
6. Click **Add**.

After the device appears in the list, toggle the button under **Authorized** to **Yes** or **No** as required. You can also use the Edit icon that appears to change the device name as it appears. Use the Delete button to delete the device from the list.

Adding Other Devices

To add other devices, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Device Control**.
3. The list of devices which are already added appears. Click the **Add devices** button and select **Other Devices**. The Add Device dialog appears.
4. Select Device Type from the list.
5. Enter **Device Name**.
6. Enter **Description** of the device.
7. Enter **Vendor ID**.
8. Enter **Product ID**.
9. Enter **Serial Number**.
10. Click **Add**.

After the device appears in the list, toggle the button under **Authorized** to **Yes** or **No** as required. You can also use the Edit icon that appears to change the device name as it appears. Use the Delete button to delete the device from the list.

Viewing Details of Devices

To view details of devices, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Device Control**. The list of devices which are already added appears. The list displays the following details of the devices:

Fields	Description
Device Name	Displays the device name.
Device Type	Displays the device type of the device.
Serial Number	Displays the serial number of the device.
Model Name	Displays the model name of the device.
Encryption Status	Displays whether the device is encrypted or not.
Authorized	Displays status of the authorization, whether ON / OFF.

Deleting the Device

To delete the device, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Device Control**. The list of devices which are already added appears.
3. Select the device that you want to delete.
4. Click **Delete** button.

Updating the Device

To update the device, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Device Control**. The list of devices which are already added appears.
3. Click the Update icon for the device that you want to update.
4. Edit Device name dialog appears. Update the device name.
5. Click **Save**.

Data Loss Prevention

You can add certain key words, or phrases that might contain, or refer to confidential information in the User Defined Dictionary. If any of the documents on your endpoints contains the text or phrase that you have added to the User Defined Dictionary, the Data-At-Rest Scan or Data Loss Prevention feature displays the path or location of these documents. On this page, User Defined Dictionaries can be created or managed which will be monitored through Data Loss Prevention Settings.

Adding Dictionary

To add dictionary, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Data Loss Prevention**.
3. Click **Add > Add**.
4. Enter the details such as name, description and the word that you want to add.
5. Click **Add**.
   You can add multiple words to the dictionary.
   You can delete a word from the list by selecting a particular word and clicking **Delete**.

Importing Dictionary

You can also import a dictionary that you prefer to use.
To import the dictionary, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Configurations > Data Loss Prevention.
3. Click **Add > Import**.
4. In the Import Dictionary dialog, click **Browse**. The File Upload dialog appears.
5. Select the valid exported dictionary json file (Example: DLP_Dictionary.json).
6. Click **Open**.

   The json file is imported.

Deleting Dictionary

You can delete a dictionary that you do not require.
To delete the dictionary, follow these steps:

7. Log on to the Thirtyseven4 EDR Security.
8. Go to **Configurations > Data Loss Prevention**.

9. The page appears displaying list of dictionaries.
   Select the check box of the dictionary that you want to delete.
10. An action bar is enabled above the table.
    Select **Delete**.
11. The confirmation message appears. Click **Yes**.

    The selected dictionary is removed.

Application Control

This feature allows you to add a new application to the default list. Adding and unauthorizing an application or file that belongs to the operating system or other system specific aspects may cause system malfunction. Hence, it is advised to add an application that is not a part of operating system or other system related programs.
You can add an application as follows:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Application Control**.
3. Go to **Configurations > Application Control**.
4. Select one of the following settings and expand.
   - Allow All Applications
   - Block All Applications

Allow All Application

Allow All Application – By default all applications are allowed except applications present in blocklist.

5. To add an application, click the **Add Application** button.
6. To add an application, select one of the following option:
   - Select Process Name and type process name.
   - Application Signature Maker – You can import application signature file. To create application signature file, do the following:
7. To download Application Signature Maker, click **Download**.
8. After downloading the Maker, add the application name to create the application signature.
9. Click **Save to File**. The AppSignature.dat file is created.
10. Click **Browse** and select the path of the AppSignature.dat file.

11. In the **Application Name** text box, type an application name.
12. In the **Application Category** list, select a category.
13. Write a reason for adding a new application to the default list of applications. This helps Thirtyseven4 EDR to improve the quality of the software product.
14. You can also submit the application metadata to the Thirtyseven4 EDR lab.
15. Click **Save**. The application is added in the 'User Added Applications' subcategory under the selected application category.

Block All Applications

Block All Applications – By default all applications are blocked except applications present in the allowlist.

Here you can download Allowlist Creation Utility. This utility helps you create an allowlist.

On this page, you can do the following actions.

- Download Allowlist Creation Utility to create a new Allowlist
- View list of existing allowlists
- Import Allowlist
- Duplicate Allowlist
- Edit Allowlist
- Delete Allowlist

Creating Allowlist

To create a new Allowlist, follow these steps.

1. Download Allowlist Creation Utility.
2. Extract the zip file. After extracting the zip file, allowlist_creator.exe and baselineconf files are available.
3. On the command prompt, run allowlist_creator.exe.
   This application discovers all installed applications on the OS drive and creates the allowlist json file.
4. Enter allowlist title and description. Press enter.
   The allowlist is created. The allowlist location and result summary appear.

Duplicating Allowlist

To duplicate an Allowlist, follow these steps:

1. Go to Configurations > Application Control> Block All Applications.The page expands displaying the list of Allowlist.
2. Click the duplicate icon of the Allowlist that you want to duplicate.
3. The duplicated Allowlist name appears in the next row. Edit the name of the Allowlist. Click the checkmark icon to save the Allowlist. The selected Allowlist is duplicated.

Deleting Allowlist

To delete an Allowlist, follow these steps.

1. Go to Configurations > Application Control> Block All Applications. The page expands displaying the list of Allowlist.
2. Select the Allowlist you want to delete, then click the **Delete** button. A confirmation message appears.
3. If you are sure to delete the selected Allowlist, click **YES**.
   If the selected Allowlist is applied to a group, it cannot be deleted, and a failure message appears.

Importing Allowlist

To import an Allowlist, follow these steps:

1. Go to Configurations > Application Control> Block All Applications. The page expands displaying the list of Allowlist.
2. Click **Import Allowlist** button.
3. In the Import Allowlist dialog, import a json file by clicking **Browse**. The file size must be less than or equal to 70 MB.
4. Enter **Allowlist Name**.
5. Enter **Allowlist Description**.
6. Click **Import**.
   The Allowlist is imported.

Editing Allowlist

To edit an Allowlist, follow these steps:

1. Go to Configurations > Application Control> Block All Applications.
   The page expands displaying the list of Allowlist.
2. Click the edit icon of the Allowlist that you want to edit.
3. The edit page appears with the Allowlist Name and Description. The following 4 settings are provided.
   - **Tree View**
   - **Allowed Directories**
   - **Manage Applications**
   - **Allowed Publishers**
4. Expand and edit the settings as per requirement.
5. Click **Update Allowlist**.
   The Allowlist is updated.

Tree View

Tree view is a visualization type that lets users expand and collapse nodes to show information at varying levels of detail.
When you expand Tree View, the directory and applications tree of the system appear.

To add directory, follow these steps.

1. Select the name of the directory you want to add, then click the **Add** button.
2. The success message appears. Click **OK**. The directory is added in the list of allowed directories.

To delete directory, follow these steps.

1. To Delete the Directory, select the Directory that you want to delete.
   The Delete button appears.
2. Click the **Delete** Button.

Allowed Directories

The list of allowed directories is displayed here. You can search for a directory by providing the name of the directory.
The directory added in the Tree view appears here. A toggle switch can help you to change the rights of the directory.
To add a directory, follow these steps.

1. To add a directory, click Add. Add Directory dialog appears.
2. Enter the **Directory name**.
3. Select the option **Yes** or **No** to allow the directory.
4. Click **Add**.
   The directory is added in the list of allowed directories.

To delete directory, follow these steps.

1. To Delete the Custom Directory, select the Custom Directory that you want to delete.
   The Delete button appears.
2. Click the **Delete** Button.

Manage Applications

The list of explicitly allowed/blocked applications is displayed here.
To add an application, follow these steps.

1. To add an application, click **Add**. Add Application dialog appears.
2. Enter the **Application name**.
3. Select the option **Allowed** or **Blocked**.
4. Click **Add**.
   The application is added in the list of applications with the status as per selection while adding the application.
   You can search for an application by providing the name of the application.

To delete directory, follow these steps.

1. To Delete the application, select the application that you want to delete.
   The Delete button appears.
2. Click the **Delete** Button.

Allowed Publishers

The list of allowed publishers is displayed here. You can search for a publisher by providing the name of the publisher.

If User wants strict Publisher check, select the **Block application from allowed directory if publisher is not allowed** checkbox.
A toggle switch can help you to change the rights of the publisher.
To add a publisher, follow these steps.

1. To add a publisher, click Add. Add Publisher dialog appears.
2. Enter the **Publisher name**.
3. Select the option **Yes** or **No** to allow the publisher.
4. Click **Add**.
   The publisher is added in the list of allowed publishers.

To delete directory, follow these steps.

1. To Delete the publisher, select the publisher that you want to delete.
   The Delete button appears.
2. Click the **Delete** Button.

Submit Application Metadata to Thirtyseven4 EDR Lab

With this option, you can send metadata of an application to the Thirtyseven4 EDR lab for including it in the application categories. Metadata includes information of application such as its Name, Version, Company Name, and MD5. You can also provide the reason for adding the application. This information will help us to improve the Application Control module.
Application Categories include thousands of applications based on their functionalities. If you block a category, all the applications in that category are blocked.
However, if you have unauthorized an application category but an application is not yet blocked, you can submit that application. Thirtyseven4 EDR analyzes the application and then enlists it in the category.

- User may get application blocked prompt even while copying or renaming any unauthorized application.
- Some unauthorized applications may start in case the application executable is updated due to software update. Such applications can be added to Thirtyseven4 EDR Security and you are recommended to submit the Metadata to the Thirtyseven4 EDR lab.

Allowlist Creation Tool

This command line application iterates through the file system of the Windows machine and creates the allowlist file in the JSON format. The Allowlist file contains the list of all executable files, folders, and machine information.

Using the Allowlist Creation Tool

1. Run the tool, **allowlist_creator.exe** by double-clicking or from the command prompt.
2. The Tool will start with administrative privileges.
3. Provide **Title** and **Description** of the tool.
   Rules to provide Title:

- Length of title should not exceed 50 characters.
- Should not start with a special character.
- Should not start with a number.
- Should not contain any special character except "_ (underscore)".

Rule to provide Description:

- Length of description should not exceed 110 characters.

4. After the Title and Description are provided, the tool will read the configuration from the config file (baselineconf.dat).
5. By iterating through the file system, the tool will create the Allowlist file, (JSON file) at the same location.
6. The following Allowlist result summary is displayed,
   - Total file/folder discovered
   - Total Supported files
   - Allowed file/folder count
   - Allowed executable publisher count
   - Start Time
   - End Time

Supported Windows Platform

- Windows 10 (32-bit and 64-bit)
- Windows 11 (64-bit)
- Windows 7 (32-bit and 64-bit)

Asset Management

To view the complete product key on the Endpoint Status page, select the OS Product key check box. If you do not select this check box, only partial product key will be displayed. This feature is applicable only for the clients with Microsoft Windows operating system.

SMTP Settings

This feature helps you set the SMTP Host Details. All emails from Thirtyseven4 EDR Security such as Notification mails and Report mails will be sent to the SMTP Server for further routing.

To configure the SMTP Settings, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > SMTP Settings**.
3. Select the **Enable SMTP Settings** check box.
4. In the **SMTP Server** text box, type the IP Address or domain name of SMTP server.
5. In the **Port** text box, type the port number.
6. In the **Sender's Email Address** text box, type the email address.

This email address will appear as From Address in all the emails sent from Thirtyseven4 EDR server.

7. Select the **Require Server Authentication** check box.
8. For user authentication, type the user name in the **Username** text box.

   The Username field depends on your SMTP server. It may ask you to provide either user name or email ID.

9. In the **Password** text box, type the password.
10. In **User Authentication Method**, select one of the following:
    - None: Select this option to send email notification through HTTP protocol.
    - SSL: Select this option to send email notification through SSL (Secure Sockets Layer) protocol.
    - TLS: Select this option to send email notification through TLS (Transport Layer Security) protocol.
11. Thirtyseven4 EDR recommends, that to ensure the SMTP host details are correct, test the SMTP settings.
12. To test the SMTP settings, click Test Mail. After successful verification, click Apply.
13. In the Test Mail for SMTP dialog, in the **To** text box, enter the email ID of the user.
14. Click **Send Email**.

Thirtyseven4 EDR cannot send emails if the SMTP settings are configured using public mail server (Example: Gmail) and if Allow less secure apps setting is disabled in the public mail servers.

Internet Settings

If you are using proxy settings to connect to the Internet, then provide the Proxy Server details.

To configure the Internet Settings, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Configurations > Internet Settings**.
3. Select the **Enable Proxy Settings** check box.
4. In the **Proxy Server** text box, type the IP Address of the proxy server or domain name (For example, proxy.yourcompany.com).
5. In the **Port** text box, type the port number of the proxy server (For example: 80).

6. Select the **Authenticate to connect through Proxy** check box. Username and Password fields are enabled.
7. In the **Username** and **Password** text boxes, type in your proxy server credentials.
8. Click **Test Connection**. The success message appears if the connection to the proxy server is successful.
9. Click **Apply**.

Roaming Service

Roaming Service allows the Thirtyseven4 EDR clients to interact with the Thirtyseven4 EDR Server when the clients move outside the organizational network.

Roaming Service also allows the Thirtyseven4 EDR clients to carry out the actions which local clients does normally. The Thirtyseven4 EDR roaming client can update their status, fetch policies, perform client actions, send reports to the Server, download latest update from the Thirtyseven4 EDR Server, etc.

Note: **An Internet connection is required for using Roaming Service.**

Process Flow of Roaming Service

The UI of this page is dynamic, will change according to completed steps. On this page first, you need to register for Roaming Service.

After successful registration, Roaming Service is enabled by default. Manual mode to setup the clients for roaming is selected by default. You need to enable Roaming Service on endpoints. The procedure is explained below.

Register for Roaming Service

Fresh Installation / First time User

If you are using the Roaming Service for the first time, follow these steps.

1. To Register for Roaming Service, click **Register for Roaming Service** button.
2. A confirmation message appears. Click **OK**.

The Server is registered for Roaming Service successfully.

This is a one-time process.

Reactivation

If you have reactivated Thirtyseven4 EDR Security, follow these steps.

1. To Register for Roaming Service, click **Register for Roaming Service** button.
2. The Email Confirmation dialog appears. Confirm the Email address to receive the OTP. The Email address is of Super Admin.

3. Click **Confirm**.

4. The OTP will be sent immediately to the confirmed Email address. Copy the OTP from that Email. The OTP is valid for only 24 hours.

5. To register immediately, follow these steps.
    a. In the Enter OTP dialog, enter the **OTP**.
    b. Click **Verify**. If you want to register later, follow these steps.
    c. In the Enter OTP dialog, click **Close**.
    d. The **I have an OTP** button appears on the page for 24 hours only. Click **I have an OTP** button.
    e. In the Enter OTP dialog, enter the **OTP**.
    f. Click **Verify**.

After successful verification, Roaming Service connection is established.

Enabling Roaming Service

After successful registration, Roaming Service is enabled by default.

Now on the page, you can view an accordion of **Enable Roaming Service** with expand sign and toggle button. By default, the switch is **ON** that means Roaming Service is enabled so the roaming clients and the Thirtyseven4 EDR server can communicate. If you turn **OFF** the switch, that means Roaming Service is disabled so the roaming clients and the Thirtyseven4 EDR server cannot communicate.

Modes to Setup Endpoints for Roaming

When you expand the accordion of Enable Roaming Service, the following mode options appear.

- **Manual Mode** - By default, this mode is selected. In this mode, only endpoints on which the Roaming Service is enabled, can communicate with the server if they go out of organizational network. By default, Roaming Service is disabled for all endpoints.

  To enable Roaming Service on endpoints, go to the **Status** page. For more information, see Roaming Service.

- **Automatic Mode** - In this mode, all endpoints can communicate with the server if they go out of organizational network.

If you want to set the Automatic Mode, select the **Automatic Mode** option.

Click **Save** to save your settings.

Endpoint Threat Hunting

On this page also, you can create and manage ETH searches.

To add Search, do the following.

1. Go to **Configurations > Endpoint Threat Hunting**.
2. The list of searches which are already added appears. Click the **Add** button. The Add Search dialog appears.
3. Enter **Search Name** and **Description**.
4. Select **Action** from the list. You can select **Quarantine** or **Quarantine and Block** or **Delete** or **No action** option.
5. Select **Search Mode**.
   a. **Manual Search** mode is selected by default. With Manual Search, you can search 1 to 5 entries at a time.
   b. Enter Hash Code that you want to search in the text box. The Hash Type of the code appears in the corresponding box.
   c. Click **+Add Entry** to add search entry.

      You can enter maximum 5 search entries in Manual Search mode.

      You can delete the search entry with help of delete icon of the corresponding entry.
6. If you want Bulk Search, select Search Mode as **Bulk Search** .
   a. Download the CSV template from the link.
   b. Fill hash codes that you want to search in the CSV file.
   c. Save the file. The file size must be less than or equal to 1 MB.
   d. Click **Upload CSV file** to upload the file. The file name appears when the file is uploaded successfully.
7. Click **Save**.

The search is saved in the Existing Scan table. To initiate the scan with your newly added Search, refer Existing Scan.

Deleting search

1. In the search table, select the check box of the search that you want to delete. An action bar is enabled above the table.
2. Select **Delete**.
3. Click **Submit** button.
4. The confirmation message appears. Click **Yes**.
5. The success message appears. Click **OK**.
   The selected search is removed.

Viewing Details of the Search

1. In the search table, click the **Details** link of the search to view more details. A dialog appears showing Hash Code and Hash Type.
2. Click **Close**.

Blocked Hashes

You can view the table of blocked hashes.
The Block hash action is supported for ETH on-demand search flow only.
The hashes are blocked for 15 days only. The table shows the expiry date along with other details.
You can click the **Details** link of the search to view more details.

Unblocking Hashes

1. In the search table, select the check box of the search for which you want to unblock hash.
   An action bar is enabled above the table.
2. Select **Unblock**.
3. The confirmation message appears. Click **Yes**.
4. The success message appears. Click **OK**.
   The hash is unblocked.

Patch Management

Operating System Requirement for the Patch Server

- Microsoft Windows 10 (64-bit) and above
- Microsoft Windows Server 2012 (64-bit) and above

Adding a Patch Server

Prerequisite

If you are adding the patch server by Hostname, you need to add the hostname and IP address, manually in the 'hosts' file located in the operating systems 'etc' folder.

To add a patch server, follow these steps.

1. Go to Configurations > Patch Management.
2. Click the **Patch Server Installer** button to download the setup file.
3. Follow the steps displayed on the UI to proceed.
4. Click **Add Patch Server**.

   The Add Patch Server dialog appears.
5. Enter the patch server name for the patch.
6. Enter the patch server IP/ Hostname.
7. Enter the **SSL Port number**, if need to change the default port 6201.
8. Enter the **Thirtyseven4 EDR server IP/Hostname**.

9. After entering these details, click **Add**.

   The new patch server is added now and appears on the Patch Management page.

   You can add multiple Patch Servers.

   If multiple patch servers are added, you can sort the list as per Patch Server Name, Patch Server IP/Hostname, and Status.

Editing the Patch Server

To edit a patch server, follow these steps.

1. Go to **Configurations** > **Patch Management**. Existing patch servers are listed.
2. Click the Edit icon of the patch server that you want to edit.
3. The patch server details appear. In Patch Synchronization and Configuration tab, you can view previous patch synchronization status with time stamp.
4. Here you can edit the SSL port number. Also, you can edit the Patch Synchronization details, as required.
5. By default, the Upstream Server is Microsoft Patch Server. You can change the Upstream Patch Server if required. If you select the option **Local Thirtyseven4 EDR Patch Server**, select the server from the list.
6. In the Internet Settings tab, change proxy settings if required.
7. Click **Save.**

Schedule Patch Synchronization

1. Select the **Enable Schedule Patch Synchronization** check box.
2. Select the **Frequency** of patch synchronization, either Weekly or Monthly.
3. Select **Weekday** from the list to run patch synchronization.
4. Select the time to run patch synchronization by selecting hours and minutes in the **Start At** list.
5. Click **Apply Filters** to specify filters for patch synchronization.
6. Click **Start sync** to run patch synchronization instantly.

   Click **Stop sync** to stop patch synchronization if it is running. A notification is sent to the patch management server.

Applying Filters

If you select the Parent patch server as **Microsoft**, then only these filters are applicable.

If you select the Parent patch server as **WSUS**, all metadata available on WSUS is synchronized. Microsoft filters are not applicable.

If you select the **Upstream Patch Server** as **Local** Thirtyseven4 EDR Patch Server, then filters enabled on the selected server are applicable.

To apply filters, follow these steps.

1. If you want to apply filters for downloading and synchronizing the patches, click **Apply Filters**. The Filters dialog appears.
2. In **Categories** accordion, click + to expand. Either you can select the **All Categories** check box to select all categories to be synchronized for Microsoft applications or select the type of patches from the list, as required.
3. In **Languages** accordion, click + to expand.
   Here you can select the languages for the patches for Microsoft applications. Select one of the following options.
   - Download patches in all languages
   - Download patches in the following selected languages – If you select this option, select the languages from the list.
4. In **Products** accordion, click + to expand.
   Here you can select the products for which you want to receive the patches. Either you select All products or select products as required from the list.
5. Click **Apply**.

The patch settings are updated.

Patch Management supports the following applications along with Microsoft applications,

- Adobe
- VideoLAN
- Adobe Systems, Inc.
- Microsoft
- PuTTY
- Notepad++, Inc.
- Oracle Corp.
- 7-Zip
- Mozilla Foundation

Patch Synchronization

To start patch synchronization, follow these steps.

1. Go to Patch Server Task Scheduler>Task Scheduler Library.

2. Run Thirtyseven4 EDR Schedule Patch Sync to trigger on demand Patch Sync.

When the patch synchronization is complete as per applied filters, patch synchronization status is shown as **Successful** with timestamp.

When the patch synchronization is failed as per applied filters, patch synchronization status is shown as **Failed** with timestamp.

Deleting the Patch Server

To delete a patch server, follow these steps.

1. Go to **Computer** > **Configurations** > **Patch Management**. Existing patch servers are listed.
2. Click the **Trash** icon of the patch server that you want to edit.
3. Click **Yes** on the confirmation dialog box. The patch server is deleted.

File Activity Monitor

On this page, you can add file extensions and folders that you want to exclude from the File Activity Monitor policy.

To exclude file extensions and folders from monitoring, follow the given steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Configurations > File Activity Monitor.

   In the Exclude File Extensions section, the list of extensions that are already added appears.
3. Enter the extension that you want to exclude from monitoring in the **Extension** text box, and then click **Add**.

   The file extension should be written without a dot in the following format: xml, html, zip, etc.

   The extension is added to the list.
4. To remove the extension from the exclusions, click the **Delete** button which appears when you click the list entry.
5. In the Exclude Folders section, the list of folders that are already added appears.

   Enter the folder path that you want to exclude from monitoring, for example. C:\Thirtyseven4 EDR, in the **Folder Path** text box, and then click **Add**.

   For Mac OS, use only forward slash (/) in the folder path. Example: /Users/Admin/ExcludeList.

   User can also add path like %Windir%\ which is also supported by Windows OS.

To remove the folder path from the exclusions, click the **Delete** button which appears when you click the list entry.

Endpoint Detection & Response

EDR OVA Deployment

Set up OVA to Use EDR Feature

This feature helps you deploy OVA on VirtualBox. OVA (Open Virtualization Appliance) file contains a compressed version of a virtual machine with Live Query and MISP server features. When you deploy an OVA file, the virtual machine is extracted and imported into the virtualization software installed on your computer.

OVA Details

- OVA File name: edr_ova.ova
- Oracle Virtual box version: 7.0.6

Prerequisites

- Thirtyseven4 EDR Security 8.3Server is installed and reachable from the host machine where the virtual machine (VM) is installed.
- Disk space: Minimum 25 GB; Recommended 100 GB and above.
- CPU: Minimum 2 vCPU; Recommended 4 vCPU and above.
- Enable Virtualization in the BIOS of the host machine where the VM will be created. You can refer to your hardware documentation; how to enable virtualization."
- Oracle VM Virtual Box Manager, 7.0.6 or later
- RAM: Minimum 4 GB; Recommended 8 GB and above.
- edr_ova.ova build file
- Internet connection is mandatory to use EDR feature.

Step 1: Download EDR Setup – Fresh Install

1. Log on to Thirtyseven4 EDR Security 8.2.
2. Go to Configuration > EDR.
3. Click the **Download EDR Setup** button to download the setup OVA file. The OVA file is downloaded.
   This is one-time activity to configure EDR setup.

Step 2: Deploy OVA on VirtualBox

1. Download and install Oracle VM VirtualBox Manager.
2. Open the Oracle VM VirtualBox Manager.

3. Go to **File > Import Appliance**.
4. In this step, choose a virtual appliance file to import. Click **Browse** and select OVA file downloaded as mentioned above.
5. Click **Next** and follow the wizard.
6. Click **Import**.
7. In the Application Settings, verify the requirement of **RAM** and **HDD**. If required, edit the values.
8. Click **Finish**. OVA is imported successfully on the VM.
9. Click **Start** icon to start the VM. The VM is ready for use.

Step 3: Configure EDR Setup

1. Start the VM by double-clicking the icon.
2. Enter Username and password.
   username – Thirtyseven4 EDR
   password – QHThirtyseven4 EDR001#
   When the user logs in for the first time, a one-time initialization script is invoked.
   This is an interactive communication where the user is required to provide the requested inputs as follows.
3. Enter hostname (FQDN) and hit [Enter]. This Hostname is used for logging into the MISP server and configuring live Query on the Thirtyseven4 EDR console.
4. A message about Certificate management appears. To generate a new certificate, type 1 and hit [Enter].
   If the certificate already exists, type 2 and hit [Enter]. Copy and paste the certificate content and hit [Enter].
5. Set Thirtyseven4 EDR URL. Provide the IP/Hostname of the Thirtyseven4 EDR server.
6. Enter Port Number for Live Query TLS server. TLS Server port number is 6443 by default. You can change it if required. To continue, hit [Enter].
7. Port number for MISP Server is 8443. You can change it if required. To continue, hit [Enter].
8. Live Query TLS server will be configured. Wait for a few seconds as the Live Query TLS server is initializing.
   The success message appears.
   Link to access MISP UI appears. Note down the link.
   MISP credentials appear. Note down username and password which are required to generate an "Authentication Key" to be entered on Thirtyseven4 EDR Console UI.
   MISP and Live Query server are installed successfully.

After OVA configuration, to initialize the system the following options are available.

1. View MISP Settings
2. Certificate Management

3. Set Thirtyseven4 EDR URL
4. Restart Livequery
5. Check for updates – Check for Live Query updates
6. Reboot System Now
7. Shutdown System Now
8. Quit

You can select the option and type the corresponding number and hit [Enter].

About Updates

- Every midnight the updates are checked and applied automatically
- On-demand updates can be set through the option 5 mentioned above
- Updates are available for Live query only

Live Query Settings

Live Query

Live Query is a new Thirtyseven4 EDR feature that is part of other Thirtyseven4 EDR product Endpoint Detection & Response (EDR). With Live Query, you can ask questions of endpoints in real-time and identify areas for improving security.

This feature is only available to customers with the following licenses.

- Thirtyseven4 EDR Server 8.3onwards only.
- EDR

Supported Platforms

- Thirtyseven4 EDR 8.3is available only on Ubuntu 22.
- EDR – Windows 64-bit client only, Win 7 and above

To run live query, do the following steps.
Step 1 : Download EDR Setup on Thirtyseven4 EDR Console
Step 2: On Oracle VM VirtualBox, fresh install MISP and Live Query server
Step 3: Configure Live Query Server on Thirtyseven4 EDR console
Step 4: Run live query on Thirtyseven4 EDR console

Step 1 : Download EDR Setup on Thirtyseven4 EDR Console

1. Log on to the Thirtyseven4 EDR Security.
2. Go to EDR > Live Query.
3. When you open this page for the first time, as Live Query Settings are not configured, you see the message about configuring Live Query Settings. Click Configure Live Query Settings.

4. You are redirected to the Configurations > EDR page. Click Download EDR setup.

Step 2: On Oracle VM VirtualBox, fresh install MISP and Live Query server

For the fresh installation of MISP and Live Query server procedure, see EDR OVA Deployment.

Step 3: Configure Live Query Server on Thirtyseven4 EDR console

After MISP and Live Query server are installed successfully, to configure Live Query server, follow these steps.

1. Go to Configurations > EDR.
2. Select the **Enable Live Query** check box .
3. Enter host name in the **Server** text box.
4. Enter **Port** number. By default, the value is 6443. You can change the port number if required.
5. To test the Live Query server connection, click **Test connection**.
6. After successful verification, click **Apply**.
   The Live Query server is configured.

Note: After configuring and applying the Live Query server settings, the Live query server installation starts for available machines. If installation fails, you will receive 'Live Query Installation failed' notification.
Repeat Test Connection step and apply again to retry the installation.

External Threat Feed Settings

Thirtyseven4 EDR is providing an option to customers for integrating with External Threat Feed to enable detailed threat analysis.
To integrate External Threat Feed with Thirtyseven4 EDR, do the following steps.
Step 1 : Download EDR Setup on Thirtyseven4 EDR Console
Step 2: On Oracle VM VirtualBox, fresh install MISP and Live Query server
Step 3: Get Authentication Key of MISP server
Step 4: Configure MISP server and scheduler on Thirtyseven4 EDR console

Step 1: Download EDR Setup on Thirtyseven4 EDR Console

1. Log on to the Thirtyseven4 EDR Security.
2. Go to EDR > Live Query.
3. When you open this page for the first time, as Live Query Settings are not configured, you see the message about configuring Live Query Settings. Click **Configure Live Query Settings**.
4. You are redirected to the Configurations > EDR page. Click Download EDR setup.

Step 2: On Oracle VM VirtualBox, fresh install MISP and Live Query server

For the fresh installation of MISP and Live Query server procedure, see EDR OVA Deployment.

Step 3: Get Authentication Key of MISP server

1. Log on to MISP console.
2. Go to Global Actions > My Profile > Auth Keys section.
3. click **+ Add authentication** key.
4. The authentication key is displayed. Take note of it on paper or store it properly.
   NOTE: The authentication key will only be displayed once, so take note of it manually else it will be lost.

Step 4: Configure MISP server and scheduler on Thirtyseven4 EDR console

To configure MISP server and Scheduler, follow these steps.

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Configurations > EDR.
3. Select the **Enable External Threat Feed** check box.
4. Enter host name in the **Server** text box.
5. Enter **Port** number. By default, the value is 8443. You can change the port number if required.
6. Enter the **Authentication Key**.
7. In Schedule settings: **Frequency**, select either the **Daily** or **Weekly** option. If you select the Weekly option select Day.
8. In **Start At**, set the time in hours and minutes.
9. Select **Hash** Type, MD5 (default) or SHA1 or SHA256.
10. Select **Action to be taken** at the endpoint when file matching hash is found from the list. You can select **Quarantine** or **No action** option.
11. To test the External Threat Feed server connection, click **Test connection**.
12. After successful verification, click **Apply**.
    The MISP server is configured.
    The automated searches are generated with Name format as Automated_Search_yyyyMMddHHmmss.

Web Access Controller Settings

Thirtyseven4 EDR Security is launching a new extension called Web Access Controller. This extension ensures that users within your organization can only sign into their Corporate Google Accounts on the Endpoint's Google Chrome or Microsoft Edge Browser for specific domains that are configured by the Administrator. This implementation ensures compliance and prevents any misuse or abuse.

Additionally, this extension offers an additional layer of security by restricting users within your organization from watching YouTube videos solely on the Endpoint's Google Chrome or Microsoft Edge Browser. Users can only access videos of specific categories, channels, and publishers, enhancing compliance and preventing unauthorized usage.

This extension must be used with Thirtyseven4 EDR Security; cannot be used independently.

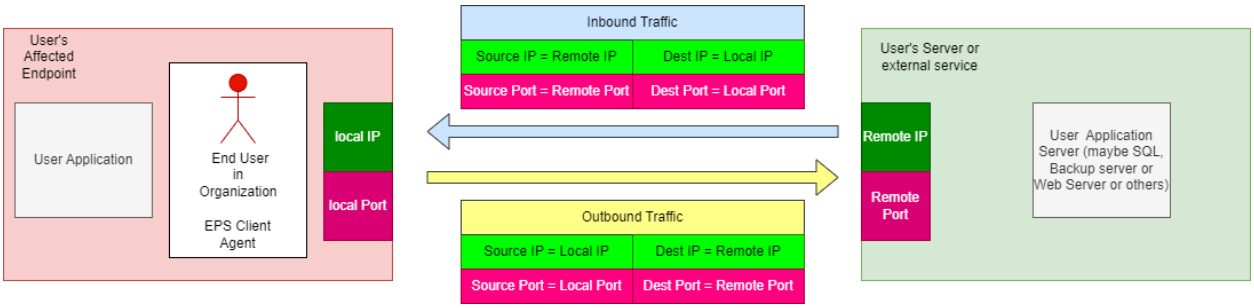
Web Access Controller Extension Settings

On this page, you can configure extension application settings.

Web Access Controller extension is installed by Thirtyseven4 EDR Security automatically.

1. In Extension Installation Settings section, select one of the following options.
    - **Manually restart Browser to apply Extension** – You need to restart the browser manually. When the fresh browser session starts, Thirtyseven4 EDR Extension is applied.
    - **Automatically terminate Browser to apply Extension** – The current session of the browser will be terminated automatically, and the extension will be applied when the next browser session will be started.
2. Select the **Protect Web Access Controller Extension** check box to disable the installation of other Browser Extensions. If you enable this, you cannot install any new browser extensions.
   Web Access Controller extension will be applied according to above settings to the browser.

FAQ Networking



What is a Local Machine?

=> A Machine/system / Endpoint under observation on which the Thirtyseven4 EDR Client Agent is installed and affected is the Local Machine.

What is a Remote Machine?

=> When a "Local Machine" interacts on network with any other Machine that may be (1) other Machine in the organization (2) Machine of a Vendor of the organization(3) A Server on the internet outside your organization which is used as a server or service for your application running on their "Local Machine" is the Remote Machine.

What is Inbound Traffic?

=> The network traffic travelling from "Remote Machine" to "Local Machine" is called Inbound traffic.

What is Outbound Traffic?

=> The network traffic travelling from "Local Machine" to "Remote Machine" is called Outbound traffic.

What is Local Port/IP?

=> The Port and IP that solely belong to the "Local Machine" is the Local Port/IP.

What is Remote Port/IP?

=> The Port and IP that solely belong to the "Remote Machine" is the Remote Port/IP.

What is Source Port/IP?

=> The following are two cases of the Source Port/IP,

For Inbound traffic: Source Port/IP will be Remote Port/IP

For Outbound traffic: Source Port/IP will be Local Port/IP

What is Destination Port/IP?

=> The following are two cases of the Destination Port/IP,

For Inbound traffic: Destination Port/IP will be Local Port/IP

For Outbound traffic: Destination Port/IP will be Remote Port/IP

File Sandbox

File Sandboxing helps you submit a suspicious file for analysis to determine if the file is malicious or safe. The major advantage of the File Sandbox is that it can reliably detect unknown threats.

This feature is accessible for the Admin and Super Admin only.

If you suspect a file to be malicious in your environment, you can submit that file to the sandbox for detonation.

Sandbox detonation - Sandbox security testing detects malware by running suspicious code in a safe and isolated environment and monitoring the behavior and outputs of the code. This is known as "detonation".

Supported File Types (Extensions):

"sh", "js", "7z", "py", "doc", "rtf", "xls", "ppt", "pps", "ps1", "bat",

"eml", "exe", "jar", "txt", "odt", "odp", "ods", "swf", "msg", "msi",

"pdf", "rar", "vbs", "zip", "cab", "lnk", "xml", "dll", "tar", "hta",

"elf", "docx", "docm", "link", "xlsx", "xlsm", "xlsb", "pptx",

"ppam", "html"

To submit a file to the sandbox, do the following steps.

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **File Sandbox**.
3. Click **Browse** to upload the file.
4. Click **Submit**.
5. The success message appears.

Notes

The maximum file size to submit to the sandbox is 64 MB.

The maximum no. of files you can submit depends upon your subscription to File Sandboxing-Total Detonations.

Reports of File Sandbox

1. In the File Sandbox Report section, existing reports if any are listed.
2. Select the Period and Detonation Status for which you want to generate the report.
3. To add filters, click **Add Filters**. The parameters in the Add Filters are File Name and Threat Type. Select or clear the filter that you want to add or remove.
4. To generate the report on the selected parameters, click **Generate Report**. The report in tabular format will be displayed.
   The report displays the following details of detonation analysis.

Fields	Description
File Name	Displays the file name which is submitted in the sandbox.
Detonation Status	Displays one of the following detonation statuses. • Completed • In progress • Queued • Analyzing • Failed
Threat Type	Displays the threat type (if any) the file contains.
Submission Date	Displays the date and time when the file was submitted for detonation.

Completion Time	Displays the date and time when the file detonation was complete.
Report	Redirects to the detailed detonation report.
Details	Displays further details of the threat. To view the details, click the Details link.

Exporting the Report

Select the CSV option from the **Export as** list to export the tabular report in CSV format.

Select the **PDF** option from the **Export as** list to export the tabular report in PDF format.

The Email containing a link to download the report will be sent to your registered Email address. The link is valid for 72 hours only.

Reports

The Reports page provide the latest information of all clients and keeps comprehensive logs about virus incidents, policy breaches, and updates.

You can view and generate reports for the listed categories. You can create your own custom category as per your requirement. There are default reports displayed for each category. You can create your own query and generate the custom reports. You can manage the generated queries.

On the reports page, you can do the following.

- View charts of the listed categories
- Create queries to generate custom reports
- Add custom category to generate reports
- Download the archived monthly reports from server

Note

Custom created reports can be viewed only by the user who has created the reports.

The following are the listed categories for the reports:

- Virus Scan – You can view the virus incidents after scanning the clients. You can also view the statistics of unscanned endpoints since the last 1 ,3 ,7 ,15, and 30 days.
- Anti-Malware Scan – You can view the malware incidents after scanning the clients.
- Web Security – You can view statistics of Web sites blocked through the Browsing Protection, Phishing Protection, or block Web site modules.
- Tune-up – You can view the number of clients tuned up and not tuned up at all.
- Advanced Device Control – You can view whether removable devices have been blocked and what actions were taken against unauthorized device access.
- Device Exception – You can view details of devices added as exceptions in the Advance Device Control policy. This report is only in the tabular format, not in the chart format.
- Data Loss Prevention – You can view statistics about attempts of sending the data outside the organization in an unauthorized manner. Data-at-Rest scan reports are included in DLP on demand report. You can view the information related to the detected confidential data such as; the file path, threat type, and matched text. You can generate a DLP report for a single endpoint at a time.
- IDS/IPS – You can view whether there was any Port scanning attack, DDOS (Distributed Denial of Service) attack, or any attempt of intrusion, and actions taken.

- Firewall – You can view number of violations for Firewall such as; the blocked connection for communications (Inbound or Outbound) and Firewall security level.
- Asset Management – You can view reports related to the hardware/software assets of the Endpoints.
- Application Control – You can view statistics about how many applications were authorized or unauthorized. You can also view the application control scan reports here.
- Backup for Ransomware Protection – You can view reports when the backup is failed. The reports display the reason for the failure of backup. This report is only in the tabular format, not in the chart format.
- Vulnerability Scan – You can view reports of vulnerabilities present on the endpoints in the network.
- Host Integrity – You can view reports of compliant and non-compliant endpoints. This report is only in the tabular format, not in the chart format.
- ETH Scan - You can view the following reports of ETH Scan.
    - Last Scan - Information of last ETH scans.
    - Historical Data - Information of all ETH scans till date.

  This report is only in the tabular format, not in the chart format.
- Patch Management – You can view reports of the installed/ missing patches on the endpoints in the network. In the Patch Management report, you can view the name of the patch in the hyperlink format. You can click the name to view details of the patch. This report is only in the tabular format, not in the chart format.
- File Activity Monitor by Event – You can view reports of file activity. The report shows how many files are deleted, how many files are modified/copied, and how many file extensions are changed.

The procedures written below are same for all the above categories including custom category.

On the reports page, you can do the following.

- Viewing chart report
- Viewing tabular report
- Managing Query
- Custom Category
- Archived Monthly Reports

Viewing Chart Report

To view the reports, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports** > Select the category for which you want to view the report. The default chart report of last 7 days appears. The chart reports are in Line chart and Pie chart format. The data points on the line chart are interactive.
3. Hover the chart, a tool-tip appears showing the count of that part.
4. Click the data point/slice, a pop-up appears displaying details of that part of chart.
   You can generate a new chart by adding a query. You can create maximum 25 reports for each category. The reports are displayed in expand / collapse format.
   The following table shows the types of chart reports per category.

Category	Types of Reports
Virus Scan	Virus Incidents
Anti-Malware Scan	Anti-Malware Incidents
Web Security	– Blocked Websites – Websites blocked by categories
Tune-up	Tune-up Status
Advanced Device Control	– Number of device violations – Policy violations by devices
Data Loss Prevention	– DLP violations – Data leaks through data transfer channel – Type of Data Leaks
IDS/IPS	Intrusion Incidents
Firewall	No. of violations

Category	Types of Reports
Asset Management	– Software & Hardware changes – Platforms – Applications installed
Application Control	– Blocked Applications – Blocked Applications as per category
Vulnerability Scan	Vulnerabilities by Vendor Vulnerabilities by Severity

You can refresh the chart report with the Refresh icon for the latest data.
You can edit the chart report with the Edit icon.
You can remove the custom chart with the Close icon.

Viewing Tabular Report

To view the reports, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports** > Select the category for which you want to view the report. The default chart report appears.
3. To view the tabular report, click Tabular icon.
4. The list of queries appears. Click the **View** link of the query that you want to view.
5. The Report page opens. The Group and Period appears as per the query.
6. To add filters, click **Add Filters**. The parameters in the Add Filters are Endpoint Name and User Name. Select or clear the filter that you want to add or remove.
7. To generate the report on the selected parameters, click Generate. Click **Save** to save the selected parameters. The filter is changed after saving.
   After clicking **Generate** button, the report in the tabular format will be displayed. In addition, if you want to change the columns then you can do it by using **Columns** list.
   You can save the report in the csv format using the **CSV** button.

Downloading Report

To download the tabular report in the CSV format, select the **CSV** option from **Export as a** list. The report will be downloaded immediately on the working machine.

Exporting Report in PDF Format

To export the tabular report in PDF format, select the **PDF** option from **Export as a** list.

To download the Report in PDF format, make sure you have configured SMTP settings.

If SMTP settings are not configured, click Configure SMTP.

You will be redirected to Configurations > SMTP settings.

For more information, see SMTP Settings.

The Email containing a link to download the report will be sent to your registered Email address. The link is valid for 72 hours only.

To receive the email successfully, ensure the following things.

- Server should have internet connectivity either via SMTP for sending email. If proxy is enabled, internet connectivity via proxy should be working.
- Correct SMTP settings should be configured.

Note
You can download the reports in the CSV format for maximum of 15,000 records.
For records, more than 15,000, use option export as PDF.

Managing Query

There are default reports displayed for each category. You can create and manage your own query and generate the custom reports.

Adding a Query

To add a query, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports** > Category for which you want to create a chart.
3. The list of default queries appears. Click the **Add Report** button to create new query.
4. The Add Report dialog appears. Select the Sub-Type. The Sub-Type option is for Web Security, Advanced Device Control, Data Loss Prevention, Asset Management categories only.
5. Enter **Report Name** and **Description**.
6. By default, All Groups option is selected. You can select the group if required.
7. By default, Last 7 Days option is selected in Periods. You can change the period for report.
8. Click **Add**. The query is generated.

Updating a Query

To update the query, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports** > Category for which you want to update the chart.
3. The list of queries appears. Click the Edit icon of the query that you want to update. The report page opens.
4. Select a Group or type the group name. By default, all groups option is selected.
5. In the **Period** list, select period of the report. Select number of days. You can also select Custom option and then select the start and end dates for the reports.
6. As per the filter, Endpoint Name and User Name parameters are displayed. If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text box. The reports will be generated for that endpoint name.
7. Enter user name in the **User Name** text box.
8. To add filters, click Add Filters. The parameters in the Add Filters are Endpoint Name and User Name. Select or clear the filter that you want to add or remove.
9. Select the columns to be displayed in the report. By default, all parameters are selected.
10. To generate the report on the selected parameters, click **Generate Report**. You can save the set of parameters. Click **Save** to save the selected parameters. When you visit this page next time, the reports of this saved parameters are displayed. The filter is changed after saving.

Note
You cannot edit the default query.

Deleting a Query

To delete the query, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports** > Category for which you want to delete the chart. The list of queries appears.
3. Select the check box of the query that you want to delete.
4. In The **Please Select** list, select **Remove Query**.
5. Click Submit.

6. The confirmation message appears. Click **OK**.
   The selected query is removed.

   Note
   You cannot delete the default query.

Duplicating a Query

To duplicate the query, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports** > Category for which you want to duplicate the chart. The list of queries appears.
3. Click the duplicate icon of the query that you want to duplicate.
4. The duplicated query appears in the next row. Edit the name of the query. Click tick icon to save the query.
   The selected query is duplicated.

Moving a Query

You can move the query only to the custom category.
To move the query, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports** > Category for which you want to move the chart. The list of queries appears.
3. Select the check box of the query that you want to move.
4. In The **Please Select** list, select **Move To**.
5. Select the custom category where you want to move the query.
6. Click **Submit**.
7. The confirmation message appears. Click **OK**.
   The selected query is moved.

   Note
   You cannot move the default query.

Custom Category

You can create a custom category as per your requirement. In this category, you can move queries from the other categories, generate queries as per your requirement and generate custom reports.

Adding a Custom Category

To add a custom category, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Reports**. The Reports page opens.
3. Click the **Add Category** button to create new category.
4. Enter name of the new category.
5. Click **Add**.
   The new category is added in the category list.
   You can edit or delete the custom category with help of icons.

Archived Monthly Reports

Every month a report is generated from the 1st day of the month to the last day of the month, by default.

This report will start generating on the first Friday of each month after 10.00 pm (IST) and then will be sent to the registered Email address automatically.

On Archived Monthly Reports page, you can view list of last 15 monthly archived reports.

Thirtyseven4 EDR recommends taking backups of all the reports on your local machine to keep it safe.
To download the report, follow these steps:

1. Click the link of the month for which you want to download the report.
   The report is downloaded in the archive file format, zip. The zip report file is password protected. The first three letters of your password are the first three letters of your first name, followed by last three digits of your mobile number (as entered while registering).
2. Extract the zip file.
   Thirtyseven4 EDR recommends using a third-party archive tool like 7-Zip, WinRar, WinZip, or PeaZip to extract the zip file. The window 10 default extract tool may not support extracting of this report zip file.

Admin

License

This page will be visible only to the customers who have purchased **only Thirtyseven4 EDR Security**.

On this page, you can manage Thirtyseven4 EDR Security licenses. You can check the status of your Thirtyseven4 EDR Security license and DLP licenses information. For post-paid license, license information is not displayed.

License Status

In the License Status window, you can check the current status of your license information. The license information includes the following details:

Title	Description
Company Name	Displays the name of the company to which Thirtyseven4 EDR Security is registered.
Product Name	Displays the product name, Thirtyseven4 EDR Security.
Product Edition	Displays the product edition.
Product Key	Displays the Product Key of Thirtyseven4 EDR Security.
License Expiry Date (GMT+5:30)	Displays expiry date of the Thirtyseven4 EDR Security license. This field is not shown if the license type is Subscription.
Tenant Id	Displays Tenant Id.

The license status displays three half pie charts, one chart for Thirtyseven4 EDR License, the other for DLP License and one for File Sandbox License. The chart displays the number of licenses utilized and licenses remaining.

Update License Information

This feature is useful to synchronize your existing license information with Thirtyseven4 EDR Activation Server. You can update your license information whenever required by clicking the **Update License Information** button.

Licence Order

In the License Order window, you can place an order to renew your license, add new licenses to your existing setup, or buy additional features packs.

To place an order, follow these steps:

1. Select one of the following options:
    - **Renew my license**: Helps you renew your current license.
    - **Add license for new endpoints**: Helps you buy additional licenses.
    - **Edition Upgrade/Buy additional feature**: Helps you upgrade the edition or buy additional features packs as per the following table:
2. Click **Place an Order.**
   An order is created, and an automated Email is sent to the back-end team to process your order.

Activity Logs

This page helps you check the activity logs of all the incidents occurred on the server.
You can select the number of days, either 7 or 15, for which the activities are generated. By default, you can view logs of the last seven days. You can also select **Custom** option and then select the **start** and **end dates** for the activity logs.
To export complete activity log, click **CSV** button. ActivityLog.csv file is downloaded.

User Roles

The User Roles page displays the list of all the user roles. The table of the user role displays information such as Role Name, Role, Role Type, Last Updated and Action.
To select all the user roles from the list, select the check box in the header row.
To select an individual user role, select the check box in that row.
You can view the user role privileges of the default role types by clicking the view icon.
This feature helps you create, modify, duplicate, and delete roles for different types of user roles. The following are default user roles.

- Thirtyseven4 EDR User Roles
    - Super Admin
    - Admin
    - Report Viewer
    - Group Admin

You cannot delete default User Roles.
You can create custom roles as per your requirement.

Thirtyseven4 EDR User Roles

For Thirtyseven4 EDR, the following user roles are added.

Super Admin

A Super Admin user has all the privileges to access, manage and delete the features of Thirtyseven4 EDR Security. You cannot edit the privileges. The role type is default. There can be only one user with Super Admin privilege. The default user role name for Super Admin is "Super Admin".

Admin

User with Admin privileges has privileges to access, manage and delete the features of Thirtyseven4 EDR Security. The default user role name for Admin is "Admin". You can create multiple user roles for Admin, if required.

Report Viewer

A user with the Report Viewer role has only access privileges, this user cannot manage or delete roles. The default user role name for Report Viewer is "Report Viewer". You can create multiple user roles for Report Viewer, if required.

Group Admin

A Group Admin user can view and manage its own group only. The default user role name for Group Administrator is "Group Admin". You can create Group Admin for each group. You can assign multiple Group Admins to one group.
Super Admin and Admin user can create/edit/delete the Group Admin user and assign/unassign the Group Admin to any group.
Group Admin can generate reports in table /chart formats for assigned group only.
When Group Admin logs on, the Status page is displayed by default. The Group Admin has limited access to pages of Thirtyseven4 EDR Security.

Add User Role

To add a user role, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Admin > UserRoles**.
3. On the User Roles page, click **Add User Role**. The Add User role page appears.

4. From the Role list, select the type of role for which you want to create a user role.
5. In the **Role Name** text box, type the name of the role.
6. Configure access rights by selecting/clearing the check boxes.
7. To save your access rights, click **Add**.

Edit User Role

To modify the settings of an existing user role, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Admin > User Roles. A list of all user roles appears.
3. Click the Edit icon for the user role that you want to edit.
4. Modify the access rights.
5. To save the modified access rights, click Save.

Note
You cannot edit or delete the default user role.

Deleting User Role

To delete an existing user role, follow these steps:

1. Log on to Thirtyseven4 EDR Security.
2. Go to **Admin > User Role**. A list of all user roles appears.
3. Select the user role that you want to delete.
4. The delete action bar is enabled above the table. Select **Delete**. You can delete a user role if you have the right privileges to do so. A confirmation message appears.
5. To delete the user role, click **Yes**.
   Note
   You cannot edit or delete the default user role.

Duplicating the User Role

To duplicate the user role, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Admin > User Role**. A list of all user roles appears.
3. Click the duplicate icon of the user role that you want to duplicate.

4. The duplicated user role appears in the next row. Edit the name of the user role.
5. Click tick icon to save the user role. The selected user role is duplicated. The privileges remain same. You can change the privileges if required.

Notification

This page helps you set rules for sending notifications for events such as when update Agent virus definition are older and virus outbreak.
You need to create a rule and a list of Email addresses to send the notifications.

Set Rules to Send Notification

1. Select the **Enable Notifications Settings** check box to set the rules. You can see the list of settings with > sign to expand and toggle button. Expand and enable Email that you want to configure.
2. Enable and expand **Virus Infection**. You can select the respective **Email** check boxes for **Virus detected on endpoints** and **Virus active on endpoints**.
3. For Virus outbreak in network, select values for the following to send the notification when the values are attended:
    - Number of virus incidents exceeds
    - Number of affected endpoints
    - Time span (minutes)
4. For **Ransomware detected on endpoints,** select the **Email**. check box.
5. Enable and expand **IDS/IPS**. You can select the respective **Email** check boxes for the following.
    - Intrusion detected on endpoint
    - Port Scanning incident detected on endpoint
    - DDOS Attack detected on endpoint
6. Enable and expand **Advanced Device Control**. You can select the respective **Email** check box for the following.
    - Attempt to breach the Device Control policy
7. Enable and expand **DLP**. You can select the **Email** check box for the following.
    - Attempt to breach DLP policy
8. Enable and expand **Application Control**. You can select the **Email** check box for the following.

- Attempt to access unauthorized application

9. Enable and expand **Update**. Select the number of days for the following if you want to change the default value of 15:
    - Endpoint virus definition is older than N Days
    - Update Agent virus definition is older than N Days
10. Enable and expand Asset Management. You can select the **Email** check box for the following.
    - Hardware change detected on endpoints
11. Enable and expand **Install through Active Directory**. You can select the **Email** check box for the following.
    - Synchronization with Active Directory failed
12. Enable and expand **Client Deployment**. You can select the respective **Email** check boxes for the following.
    - Endpoint installation successful
    - Endpoint uninstallation successful
    - Unprotected Endpoints
13. SMTP must be configured to add Email address for event notification. If SMTP is not configured, Configure SMTP button is displayed.
    Click **Configure SMTP** button then you will be redirected to SMTP Settings page to configure SMTP.
14. Enter Email address in the text box and click **Add**. When the set rule condition is attended, a notification is sent to the Email addresses added here. You can delete or edit the Email addresses.
15. Click **Save**.

General Settings

On this page, you can configure an interval for deleting older Activity Logs, Action History, Reports, Notifications, Alerts and News. You can set Client-Server communication interval time.
To do Admin Settings, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Admin > General Settings tab.

3. The following actions are displayed in the tabular format. Set the interval in days/Minutes for these actions. Set the switch to ON or OFF to apply the action.

   - Delete Activity Log older than 7 or 15 days
   - Delete Action History older than 7 or 15 days
   - Delete Notifications older than 7 or 15 days
   - Delete Alerts older than 7 or 15 days
   - Store Data-At-Rest scan reports for last 1, 2, 3 scans
   - Heartbeat interval of 1 to 120 minutes
   - Set missed heartbeat count to turn endpoint offline, 1 to 200. When you select the count, duration appears next to the count in the format of DAY HRS MIN. This duration is calculated by multiplying Heartbeat interval time with set missed heartbeat count. After this duration, endpoint will be offline.
   - Store Application Control scan reports for last 1, 2, 3 scans
   - Remove endpoint if inactive for 15 or 30 or 60 days. Selecting Never option will not remove the endpoint in spite inactive.
   - Apply Service Pack automatically, by default the Enable check box is selected, enabling this option will apply the Service Pack (SP) automatically. If you disable, you will receive notification in Alerts when the SP will be available. You need to apply the SP manually.
   - Output file base path You can enable this option and enter a new local Linux directory path for storing the reports. Make sure the path is of a local directory, not a network path.
   - Multifactor Authentication (MFA) - Select the **Enable** check box to enable the Multifactor Authentication. Only Super Admin User can view and enable this setting. SMTP must be configured before enabling MFA.

     If SMTP is not configured, the **Configure SMTP** button is displayed. Click **Configure SMTP** button then you will be redirected to SMTP Settings page to configure SMTP.

Scheduled Report Settings

Every month a report is generated from the 1st day of the month to the last day of the month, by default. This report is sent to the registered Email address on 1st day of next month automatically. Example: The reports are generated for the period of 1 October to 31 October and are sent on 1st November automatically.
You can also generate Weekly reports. You need to select the day. Reports of last 7 days from the selected day are generated and sent to the registered Email address. Example: If you select "Monday", the reports are generated from last Monday to Sunday.
On Scheduled Report Settings page, you have provision to configure Monthly or Weekly reports.

To do Scheduled Report Settings, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. Go to Admin > Scheduled Report Settings tab.
3. On the Scheduled Report Settings page, you can see the following list of settings with expand sign button.
   • Monthly Reports
   • Weekly Reports
4. To configure Monthly Reports, follow these steps:
   a. Expand Monthly Reports option.
   b. Here you can add Email addresses to whom the consolidated monthly reports will be sent. Add at least 1 Email address, maximum 5 Email addresses are allowed.
   Type an Email address in the Add Email address text box, and then click Add.
   You can delete the Email address if not required with the help of Delete icon.
   The monthly reports are deleted after 15 months.
5. To configure Weekly Reports, follow these steps:
   a. Expand and Enable Weekly Reports option.
   b. Schedule your weekly report by selecting Day.
   c. Add Email addresses to whom the consolidated weekly reports will be sent. Add at least 1 Email address, maximum 5 Email addresses are allowed.
   Type an Email address in the Add Email address text box, and then click Add.
   You can delete the Email address if not required with the help of Delete icon.
   d. Under Report Type, select at least 1 type of report.
   The weekly reports are deleted after 3 weeks.
6. To save your settings, click Save.
   The Monthly reports will be sent to the added Email addresses on 1st of next month.
   Also, you can download the monthly reports from the Reports > Archived Monthly Reports page.
   The Weekly reports will be sent to the added Email addresses on the selected day.

SIEM Integration

SIEM Integration helps to push all the events logs from Thirtyseven4 EDR Server to the configured SIEM server. This feature is accessible for Admin User only.

This feature works with many SIEM vendors that support CEF and LEEF formats.

On this page, provide the credentials of the SIEM Server. Then, select the events of which the data will be pushed to the SIEM server.

You can view the event logs on the configured SIEM server.

To push the event data to the SIEM server, follow these steps.

1. Log on to the Thirtyseven4 EDR Security.
2. Go to **Admin > SIEM Integration**.
3. In SIEM Configuration, select the **Enable SIEM Settings** check box.
4. Enter **Syslog Server IP\URL**.
5. Enter **SIEM Server Port** number between 1 and 65535.
6. Select **Protocol** either UDP or TCP.
7. Select **Data format** either LEEF or CEF.

   Note: The data formats supported are LEEF (Log Event Extended Format) and CEF (Common Event Format) only.
8. In the Event Selection section, select the events as required. The events list is displayed as per your Thirtyseven4 EDR product license.
9. Click **Test**. The success message appears if the connection to the SIEM server is successful.
10. Click Apply. The configuration success message appears.
11. The SIEM Server is configured successfully.

    Note

    The data of only selected events will be uploaded to the configured SIEM Server.

Uninstallation of Thirtyseven4 EDR Security

To uninstall Thirtyseven4 EDR Security, follow these steps:

1. Execute the Uninstaller by typing the following command.

   sh /opt/Thirtyseven4/<uninstall.sh>
2. Uninstall screen appears. Click Yes to confirm the uninstallation.
3. Authentication screen appears. Enter Username and Password of the root user.
4. Click Next. Uninstallation process starts.
5. Click Close.

Uninstallation will remove Thirtyseven4 EDR Security components from the endpoint.

Support

The Support option includes FAQ where you can find answers to the most frequently asked questions, options to submit your queries, send emails about your queries, or call us directly.

Accessing support options

To access the Support options, follow these steps:

1. Log on to the Thirtyseven4 EDR Security Web console.
2. On the top right on the Thirtyseven4 EDR Security Dashboard, click the Support button.

Support includes the following options:

- Web Support: To view the frequently asked questions, click the Visit FAQ button or click the Visit Forums button to share tips, solutions, and to submit your queries.
- Email Support: Email your query to support@thirtyseven4.com.Our Support team will respond to your query at the earliest.
- Live Chat Support: This feature allows you to chat with the Thirtyseven4 technical executives to get your issues resolved.
- Phone Support: Includes phone numbers. You can call our support team and get your issues resolved.
- Remote Support: This feature helps you to call the Thirtyseven4 technical experts for instant support.

  Contact number for phone support: 1-877-374-7581

  Contact time: Monday – Friday between 8.00 AM to 5.00 PM.

If the Product Key is Lost

Product Key serves as your identity to your Thirtyseven4 EDR Security product. If you lose the Product Key, please contact Thirtyseven4 Technical Support to get the Product Key. A nominal charge is levied for re-issuing the Product Key.

http://support.thirtyseven4.com

Head Office Contact Details

Thirtyseven4, L.L.C.

P.O. Box 1642,

Medina, Ohio 44258

United States

Phone number: 1-877-374-7581

Fax number: 1-866-561-4983

Email: support@thirtyseven4.com

Thirtyseven4 Support: http://support.thirtyseven4.com

Web: http://www.thirtyseven4.com

Sales: sales@thirtyseven4.com

Header Icons

Alerts

Critical Alerts

The Alerts icon on the header displays alert messages and actions for the following critical situations:

Alerts	Action Button
Update Manager not updated	Update Now
License Suspended or Blocked	Renew Now
License limit reached	Renew Now
License about to expire	Renew Now
DLP License count is updated	Update Now
External Threat Feed Server not reachable	EDR Configuration
SMTP Server not reachable.	Configure SMTP

If you want to take action on the alert, click **action** button for the respective alert. You are directed to the page to take the action.

Client Agent and Tools Installer Alerts

Whenever client agent and tools installer are updated or newly developed, alerts are displayed here. You must take respective action mentioned in the following table.

Alert Types	Action to do
New/updated AD tool for Windows is available.	Download New/updated AD tool for Windows.

Alert Types	Action to do
New/updated AV 32-bit installer for Windows is available.	Download New/updated AV 32-bit installer for Windows.
New/updated AV 64-bit installer for Windows is available.	Download New/updated AV 64-bit installer for Windows.
New/updated Client Installer tool for Windows is available.	Download New/updated Client Installer tool for Windows.
New/updated Device Control tool is available.	Download New/updated Device Control tool.
New/updated DLP Whitelisting tool for Windows is available.	Download New/updated DLP Whitelisting tool for Windows.
Updated Migration tool for Windows/Linux is available.	Download updated Migration tool for Windows/Linux.
New/updated Patch Management Installer for Windows is available.	Download New/updated Patch Management Installer for Windows.
New/updated 32-bit Installer for Linux is available.	Download New/updated 32-bit Installer for Linux.
New/updated 64-bit Installer for Linux is available.	Download New/updated 64-bit Installer for Linux.
Updated Mac Installer with AV is available.	Download updated Mac Installer with AV.
Updated Mac Installer without AV is available.	Download updated Mac Installer without AV.
Updated Email Installer for Mac is available.	Download updated Email Installer for Mac.
Updated Application Allowlist tool is available.	Download updated Application Allowlist tool.

Alert Types	Action to do
New UA installer is available. re-assign UA role to clients.	New UA installer is available. re-assign UA role to clients.
New UA installer is available. re-assign UA role to clients.	New UA installer is available. re-assign UA role to clients.
New/updated package for Windows/Mac/Linux clients is available.	Download New/updated package for Windows/Mac/Linux clients.

Deleting alerts

1. If you want to delete the Alert, click **Delete** to delete the selected alert message. A confirmation message appears.
2. Click **OK** to confirm.

- Update Manager not updated
- License Suspended or Blocked
- License limit reached
- License about to expire
- DLP License count is updated

1. Click **Update Now** to update the selected alert. The request of update is sent.
2. Click **OK**.
3. Click **See all alerts,** to view the list of all alerts.
4. Click **Update Now** to update the selected alert. The request of update is sent.
5. Click **Delete** to delete the selected alert message. A confirmation message appears.
6. Click **OK** to confirm.
   Renew/Buy option also available to renew expired licenses or add an additional endpoint.

Notifications

The Notification icon on the header displays the list of Notifications. Notifications such as Update Agent installation failed, and Client deployment failed are displayed. When you click

the notification, a new window of Notification Details appears showing the details.
Click **See all Notification** to go to Notifications page.
The Notifications table appears. You can view details of the notification by clicking View icon.

Deleting the Notification

To delete the notification, follow these steps:

1. On the notification page, you can view list of notifications.
2. Select the check box of the notification that you want to delete. An action bar is enabled above the table.
3. Select **Delete**.
4. The confirmation message appears. Click **OK**.

Editing the User Profile

User profile is the information about the registered user. You can view name, contact details and Role of the logged-on user.
To edit the user profile, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. On the header, click the arrow next to the human icon.
3. Click **Edit Profile**.
4. Edit the user details as per your requirement.
5. Click **Save**.
   You can cancel the changes, with **Reset** button, if required.

Change Password

This page will be visible only to the customers who have purchased **only Thirtyseven4 EDR Security**.

To change the password, follow these steps:

1. Log on to the Thirtyseven4 EDR Security.
2. On the header, click the arrow next to the human icon.
3. Click **Change Password**. The Change Password page appears.
4. Enter old password and new password. Enter the new password to confirm.
5. Click **Change Password**.

Log Off

To log off from the Thirtyseven4 EDR Security portal, follow these steps:

1. On the header, click the arrow next to the human icon.
2. Click **Logout**.

News

The Alerts icon on the header displays the news published by Thirtyseven4 EDR about security information, new service pack released, new Thirtyseven4 EDR Security version released etc.

Doc Publishing Date: 18 July 2024