Predict | Protect | Prevent

ARCON|PAM

EPM User Guide

arcon

Table of Contents

1 Introduction

Organizations face a perpetual barrage of threats due to risky end-user behavior. When an end-user has unauthorized access to (endpoints, applications, processes) and unlawfully uses this information in a corporate network, it negatively affects the confidentiality, integrity of the organization's critical assets, and sensitive business information. They turn out to be the organizations weakest link and it may be really difficult to monitor and secure these entities. Focusing on end-users' activities gives you the utmost perspective in identifying threats before they become damaging breaches. Some of the most common end user-based threats include insider threats, compromised accounts, theft, misuse, and exploitation of user accounts.

ARCON | EPM gives you the power to monitor threats and behavioral changes present within users and entities (endpoints, applications, processes). It also serves as a global operations management product that provides visibility into your organization's operations on a real-time basis. ARCON | EPM detects insider threats, compromised accounts, and other malicious attempts on the endpoints. It has a powerful **User Behavior Analytics** component that takes note of the normal conduct of users and identifies typical, atypical behavior of users and other entities within a network. It models behavior in order to create a baseline, which is then used to assess potential risks. The component is made up of advanced technologies such as artificial intelligence and data science that effectively identify advanced threats. You can build standard monitoring profiles/baselines and behaviors for users and entities (endpoints, applications, processes) across time with its **Smart Rule Engine** component. It captures data in logs, alerts the security personnel uncovering activities that might otherwise go undetected while reducing your time to detect and respond to threats.

ARCON | EPM is supported in Windows 7, Windows 8, Windows 8.1, Windows 10 & Windows 11 for the endpoints and Windows Server 2012/16/18 for the servers.

2 Features

- Configure an alert on any user behavior, including browsing activities, email, file access, application access, instant messaging and more by setting up this rule to detect a specified keyword, keyword group, process, or multiple processes.
- The Intelligent Rules Engine can be used to enforce data protection and access control rules on the compromised user to prevent data exfiltration and other malicious attempts.
- It can monitor, on-premise as well as cloud-based remote employees.
- It enables the configuration of privileges so that users can request privilege elevation at specific times, for a duration of time and on certain endpoints for required applications.
- Get scheduled activity reports (daily, weekly, monthly).
- It provides predictive and circumstantial analytics derived from the neural network.
- It can leverage risk information and recognize new activity that conflicts with expected patterns.
- Uses dynamic risk scoring, identify at-risk user, to proactively protect other users and the organization from threats before they become critical issues.
- Data visualization reports such as Sunburst graphs illustrate the use of processes by the user. It captures the duration of time spent on particular processes. It has sliced components and each slice displays the duration in time spent on particular processes. A built-in drill down gives the ability to click and focus on one item at runtime and drill down into its details which helps more complex data analysis.
- It records a violation of incidents as evidence and takes action to alert, halt, restrict the activities.
- It is loaded with time tracking, workforce monitoring, productivity enhancement features.
- It helps you with your day to day business decisions, performance reviews, workplace safety, and protection from legal liability.
- It helps you unlock the full potential of your human resources and digital Investments by identifying time spent by these entities that impacts your customers and enterprise.
- It can be used for the administration of business practices for ensuring strong planning, control, and improvement of an organization's resources and processes.
- EPM supports Remote Access feature which is a great tool for IT Support Team to take a remote session of a end user’s system to troubleshoot issues or facilitate installations & patching.
- EPM has some lightweight DLP capabilities restricting access to USB mass storage devices, Bluetooth file sharing, preventing data transfer on cloud storage services
- EPM can also help in vaulting local admin passwords along with ARCON | PAM

3 ARCON | EPM Approach

Monitor: Build standard baselines and monitor users and entities (endpoints, applications, processes) across time.

Identify: Spot risky user activity by identifying anomalous behavior.

Investigate: Investigate suspicious activities in minutes, not days.

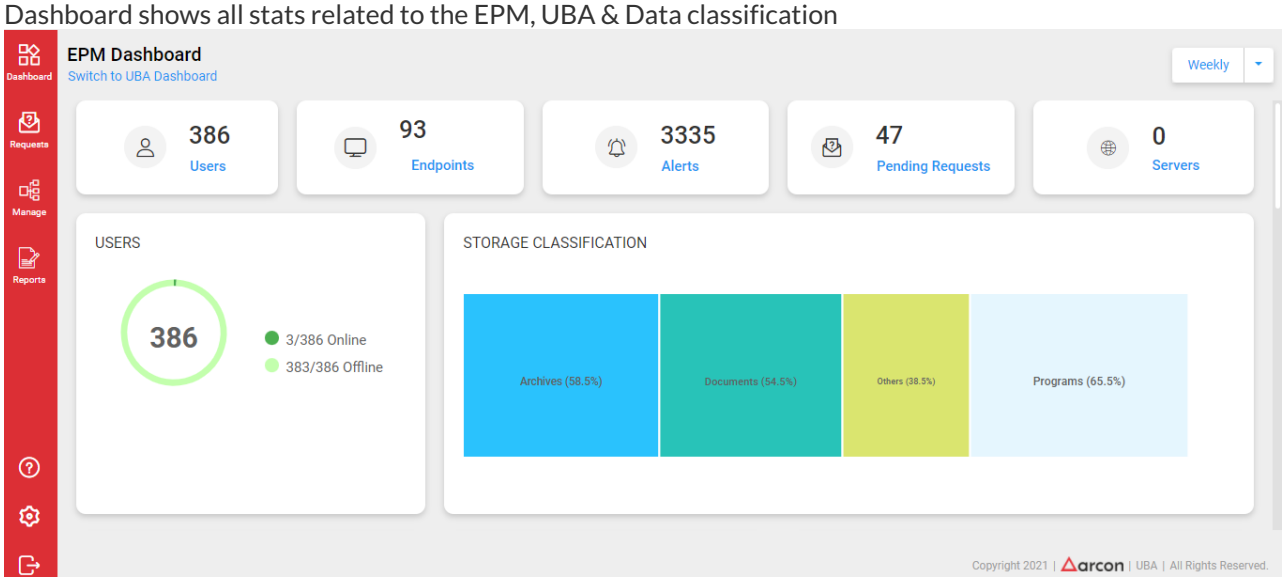
Prevent: Eliminate risk with real-time user alerts and blocking.

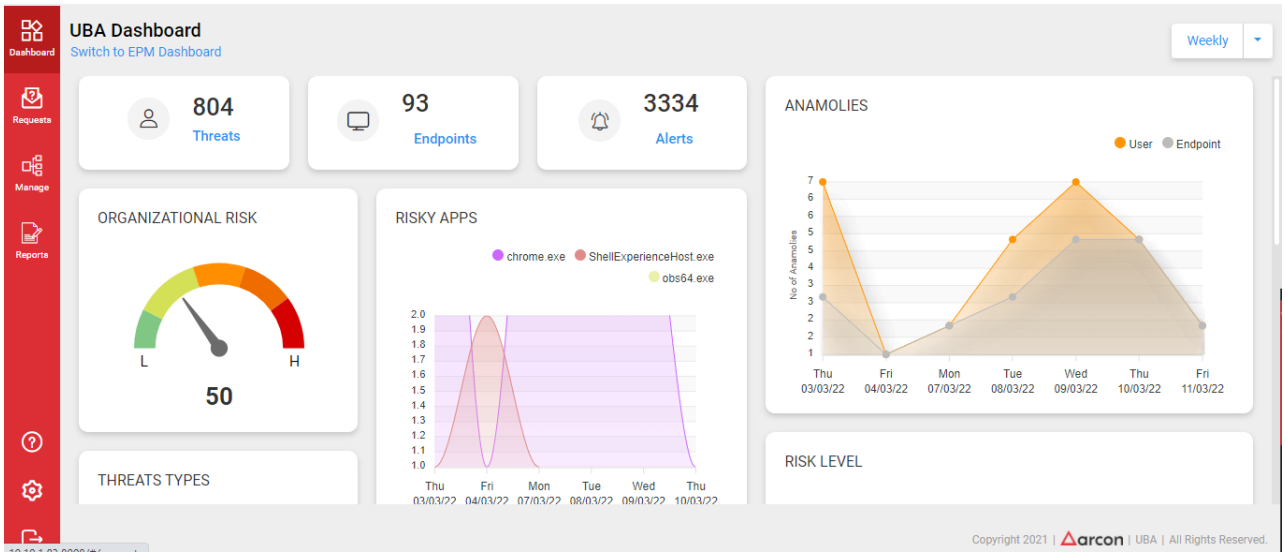
Meet compliance regulations: Meet key compliance requirements regarding insider threats in a streamlined manner.

4 Dashboard

When logged in as an administrator, the **Dashboard** exhibits the following information:

Dashboard shows all stats related to the EPM, UBA & Data classification



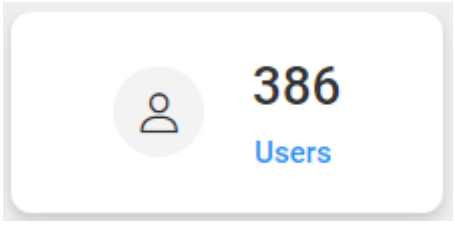


4.1 EPM Dashboard

The EPM Dashboard shows all stats related to the EPM which consists of the following counts & graphs

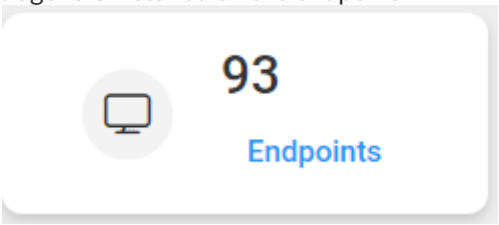
- Users

The users card shows total number of onboarded users in the application. Users can be onboarded automatically when the agent is installed on the endpoint or using a sync to the Active Directory



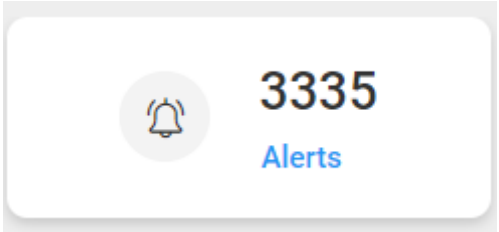
- Endpoints

The endpoints card shows total number of endpoints that are onboarded in the application. The endpoints are automatically onboarded when the agent is installed on the endpoint



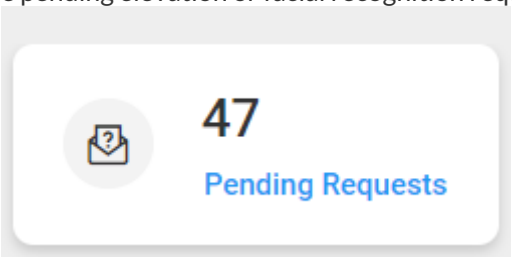
- Alerts

Alerts card shows total number of alerts that are raised in the selected selected period like daily, weekly or monthly



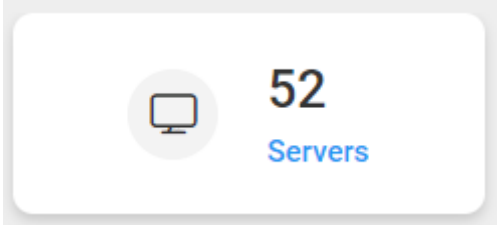
- Pending Request

Pending request card shows all the pending elevation or facial recognition requests raised by the end users.



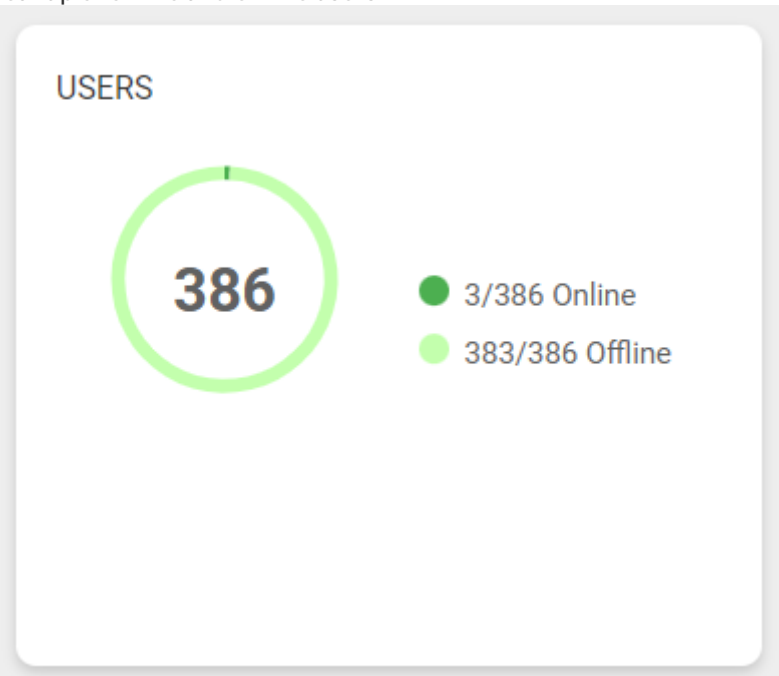
- Servers

Servers card shows all the servers that are onboarded in the application



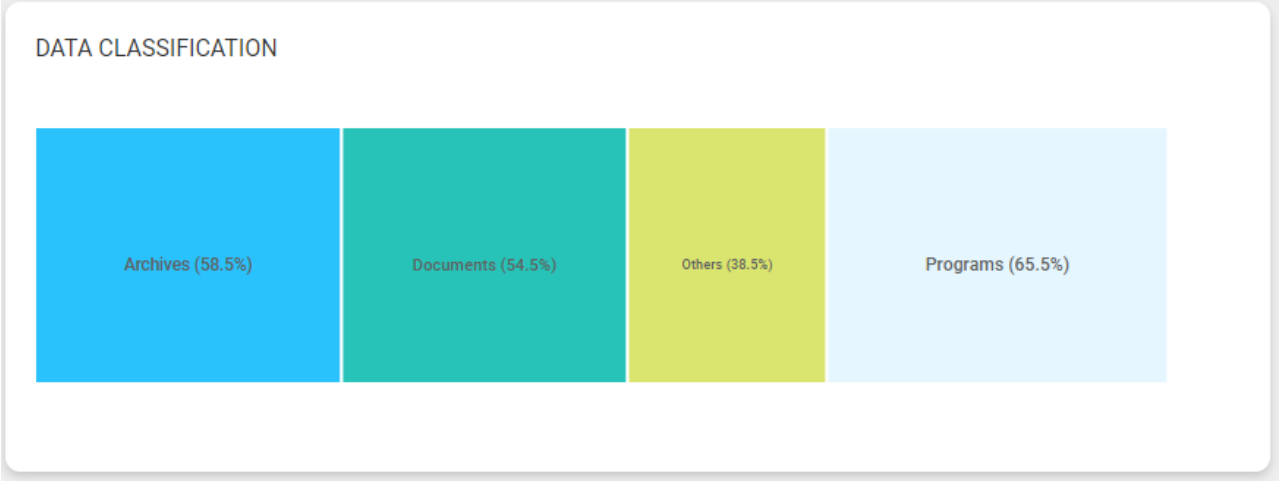
- User graph

User graph shows a breakup of online and offline users



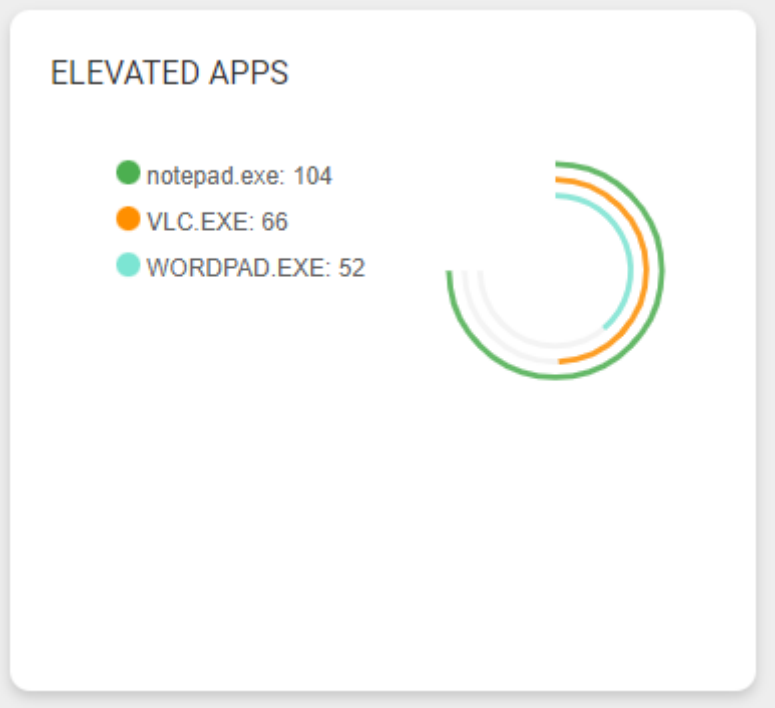
- Data classification

Data classification shows a breakup of all the data in the organization. Data is distributed under different categories like archives, documents, photos, programs, etc



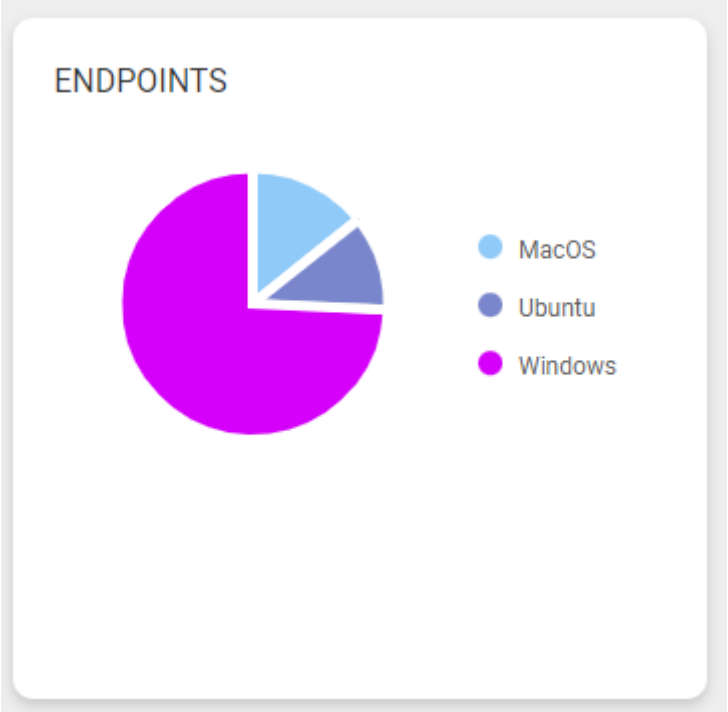
- Elevated Apps

Elevated apps graph shows the most elevated apps in the selected period



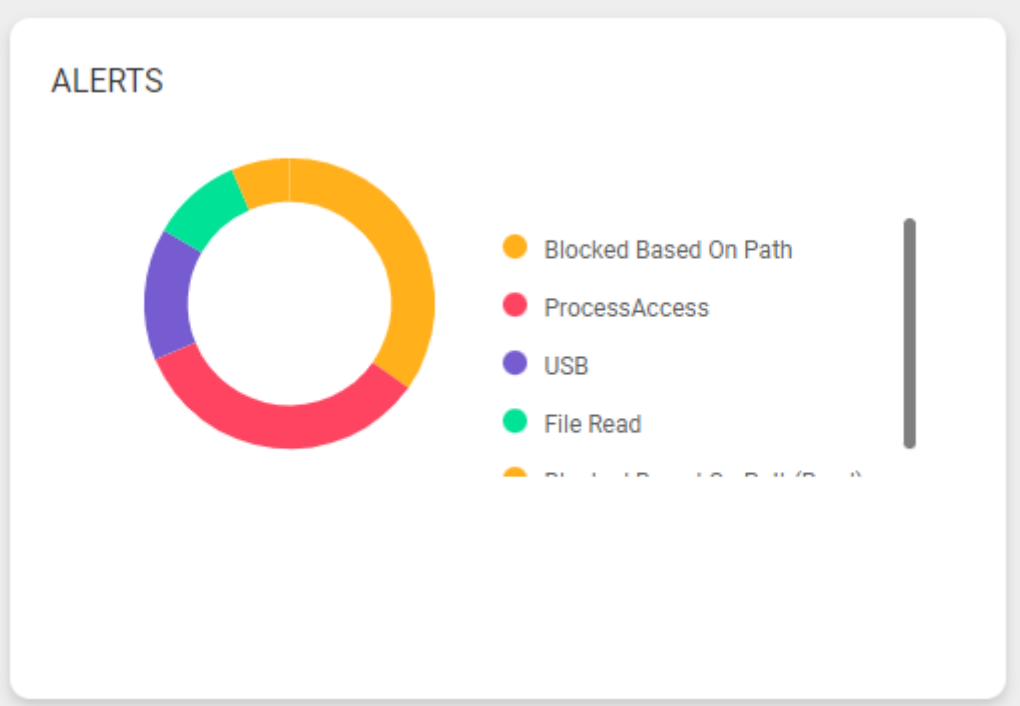
- Endpoint graph

Endpoint graph shows a split of all the endpoints with respect to the type of operating system



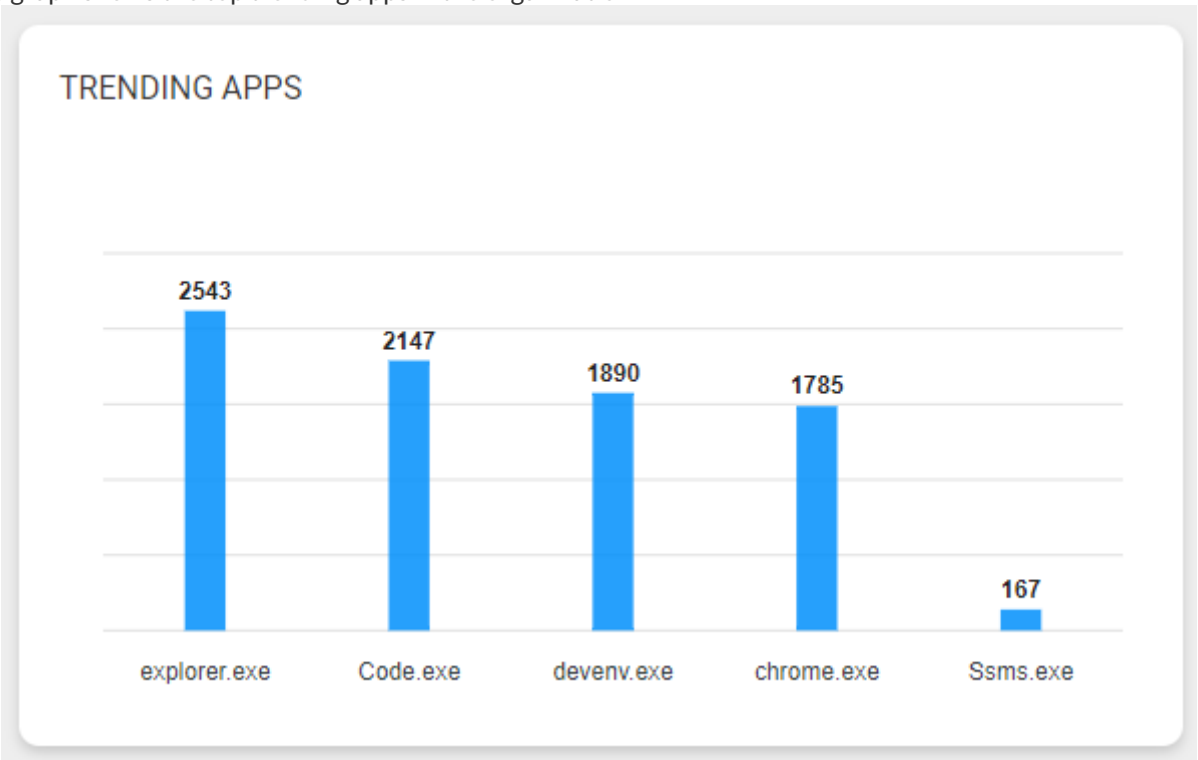
- Alert graph

Alerts shows a split of different types of alerts like process restriction, file restriction, usb restriction, etc.



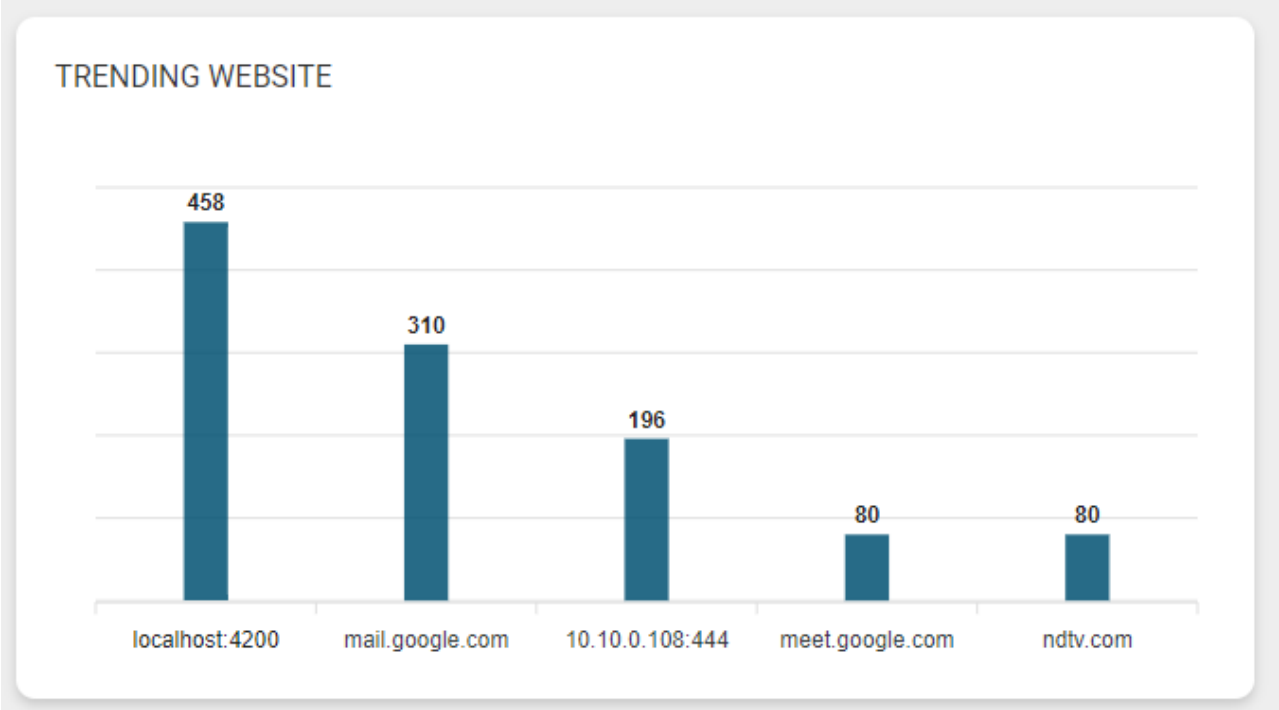
- Trending apps

This graph shows the top trending apps in the organization



- Trending Websites

This graph shows the trending websites in the organization



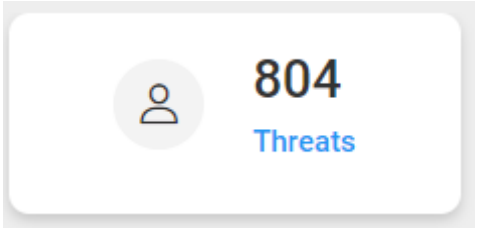
- Endpoint location graph

4.2 UBA Dashboard

The UBA Dashboard shows all states related to the UBA which consists of the following counts & graphs

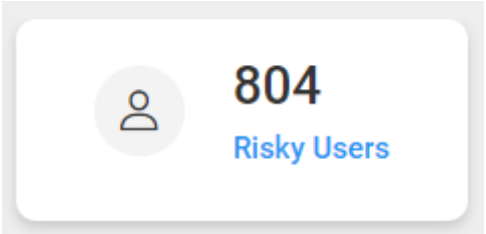
- Threats

Threats card shows the total number of threats that are detected in the selected period



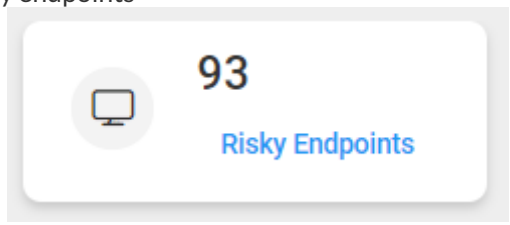
- Risky Users

This card shows a count of all risky users



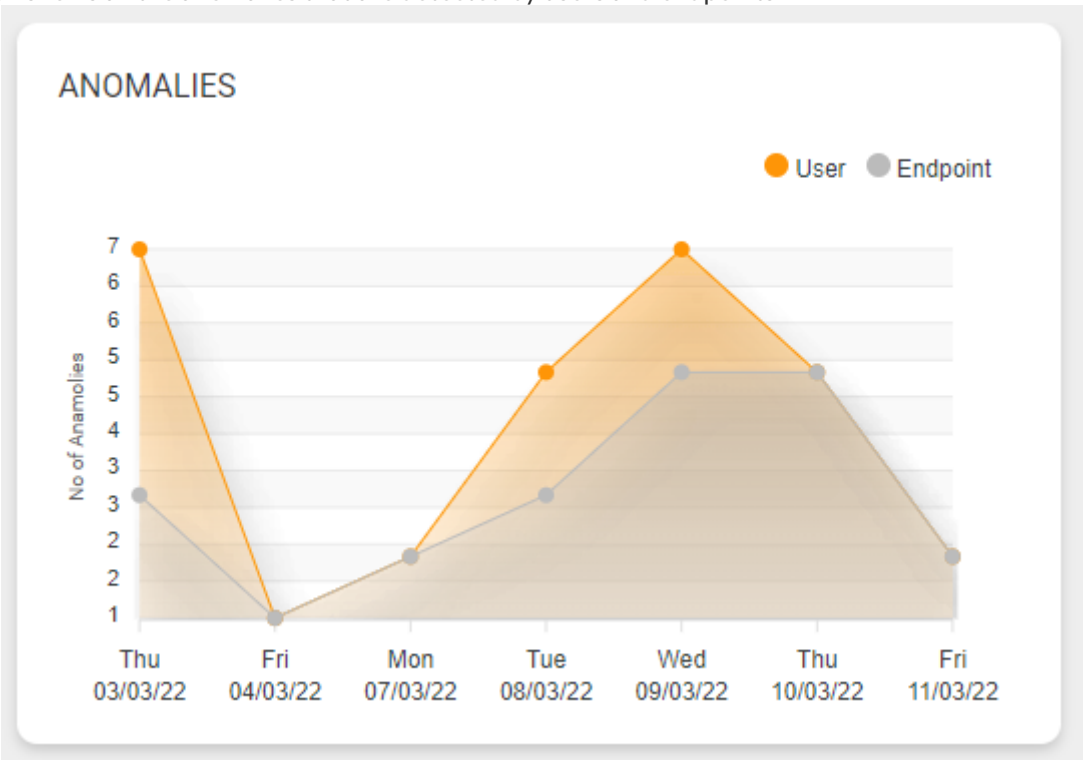
- Risky Endpoints

This card shows a count of all risky endpoints



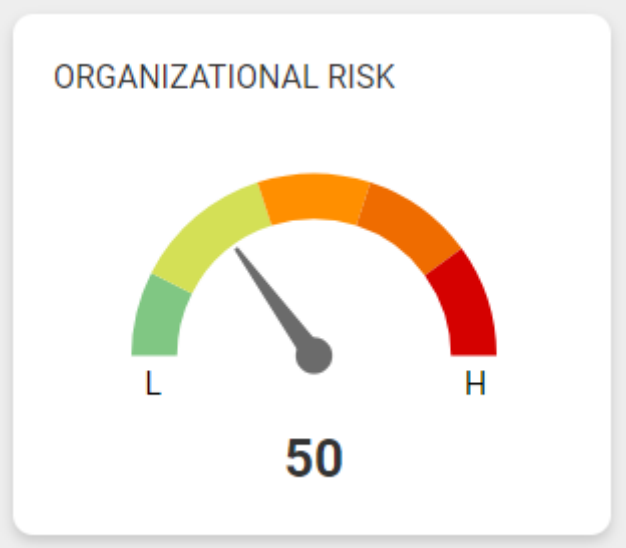
- Anomalies

This graph shows all the anomalies that are detected by users and endpoints



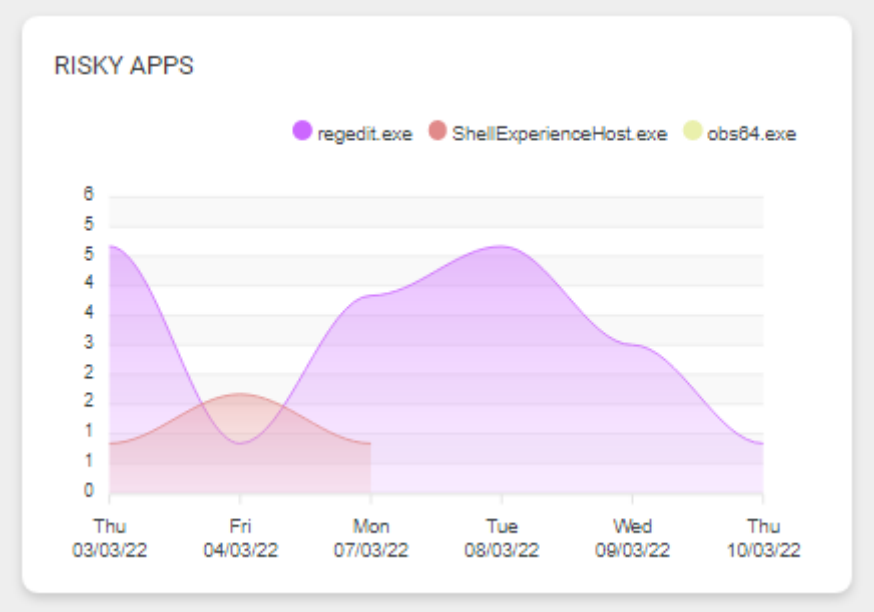
- Organizational Risk

This graph shows an overall organizational risk based on the anomalies detected



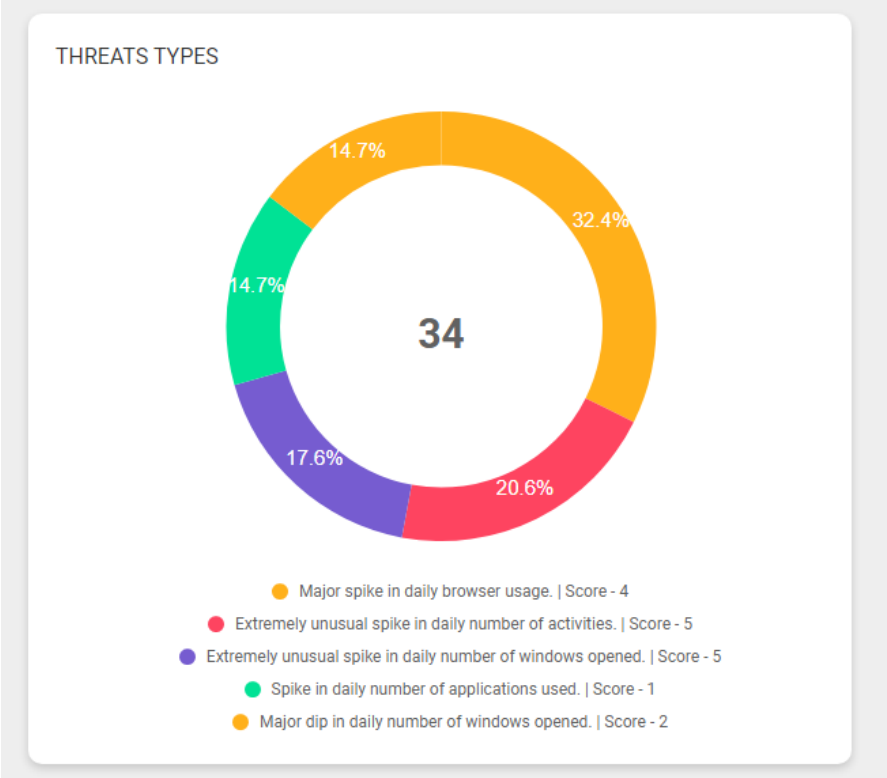
- Risky Apps

This graph shows all the risky apps for which anomalies



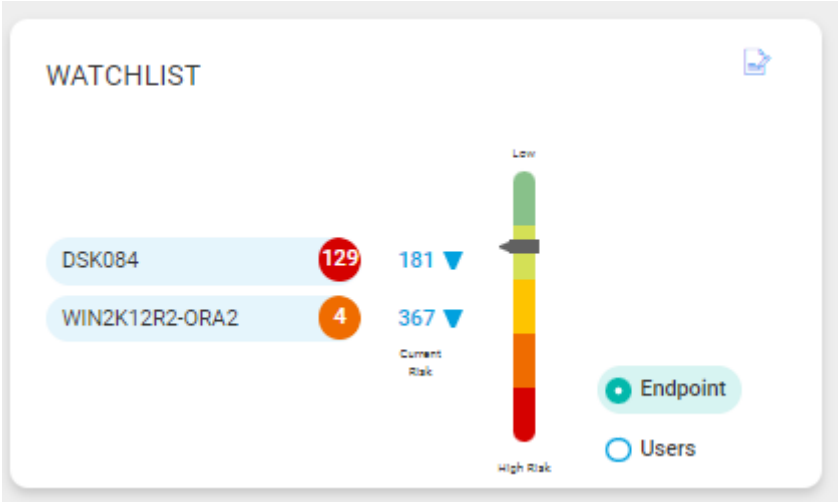
- Threat Types

This graph shows a split of different types of threats like new application detected, unsigned application launched, etc.



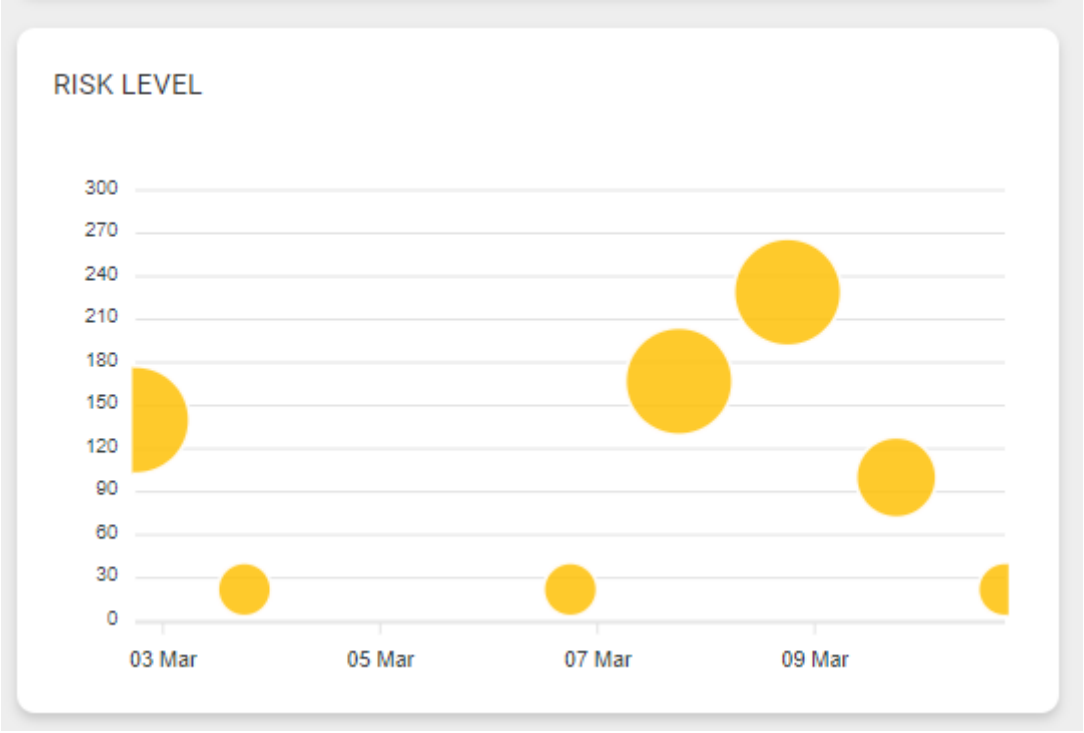
- Watchlist

This feature allows certain users or endpoints to be added to the watchlist so there risk scores can be closely monitored



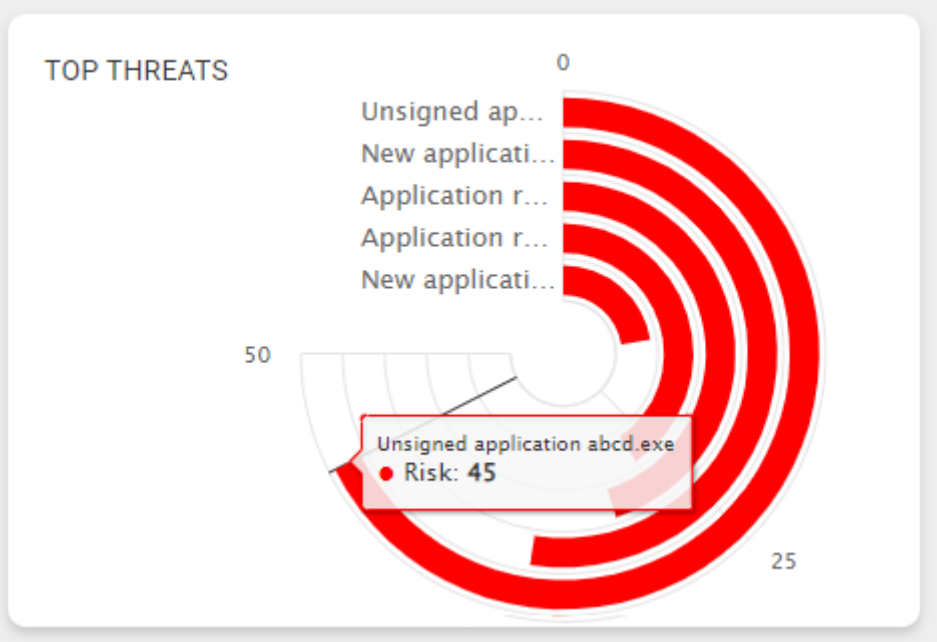
- Risk Level

This graph shows a bubble chart that shows the risk for the selected period. The amount of daily risk is marked on the y axis and the date is marked on the x-axis and the size of the bubble is a number of anomalies that are detected.



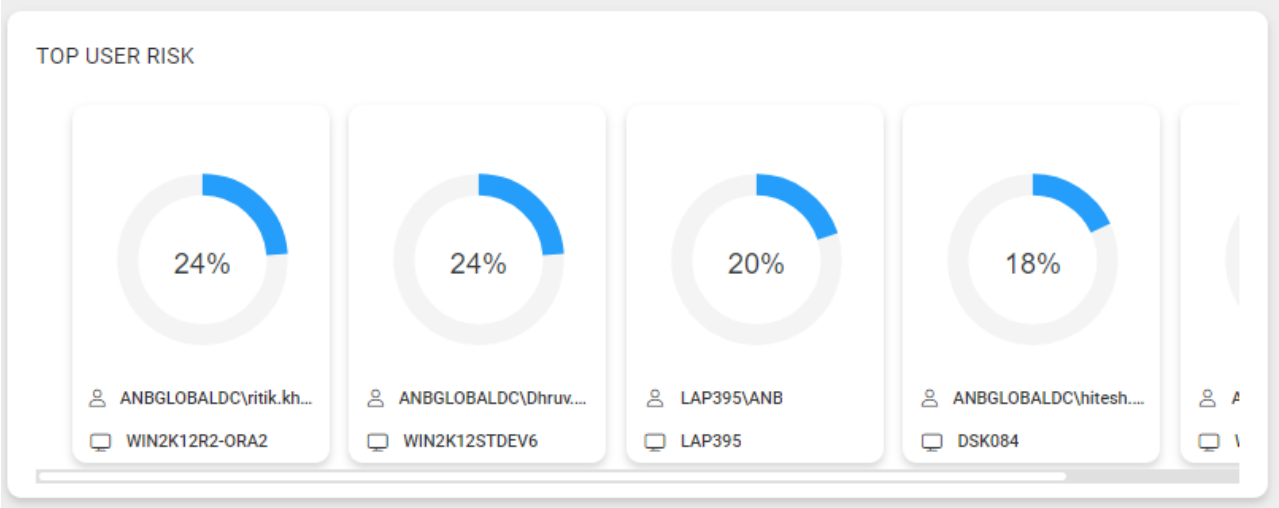
- Top threats

This radial graph shows the top threats that were detected in the selected period with respect to their risk scores



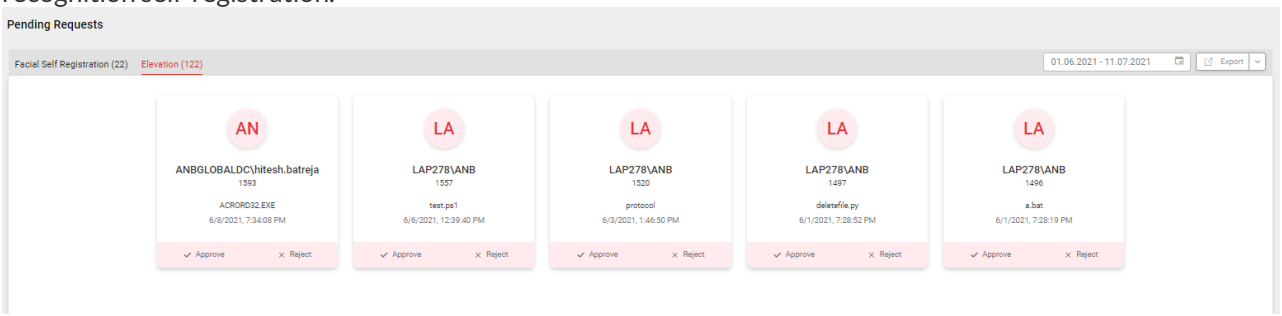
- Top User Risk

This section displays the top risky users in the organization, they are ranked by their risk scores


TOP USER RISK
24%
ANBGLOBALDC\ritik.kh...
WIN2K12R2-ORA2
24%
ANBGLOBALDC\Dhruv....
WIN2K12STDEV6
20%
LAP395\ANB
LAP395
18%
ANBGLOBALDC\hitesh....
DSK084

5 Pending Requests

This module allows you to accept the pending requests by the users for elevation (online and offline) and facial recognition self-registration.



5.1 Filter

You can filter report data by applying the following filters/search criteria:

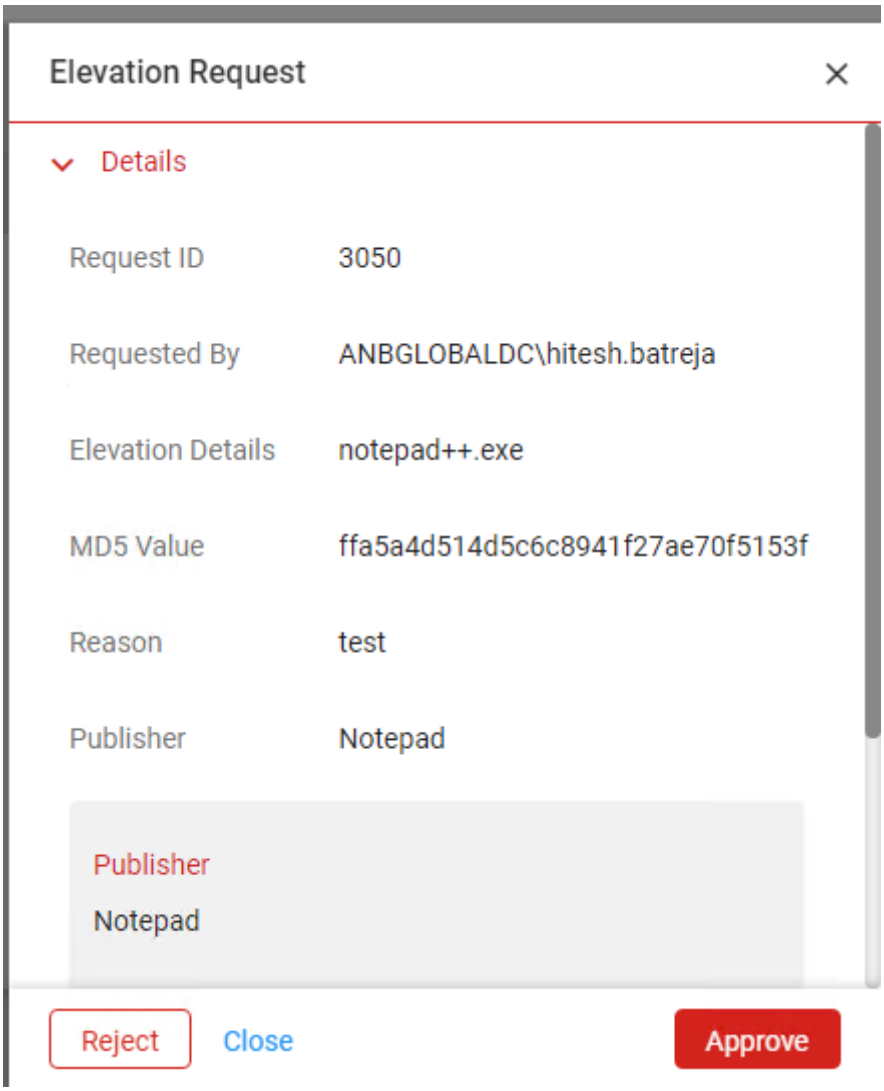
Select the required details and click **Search**,

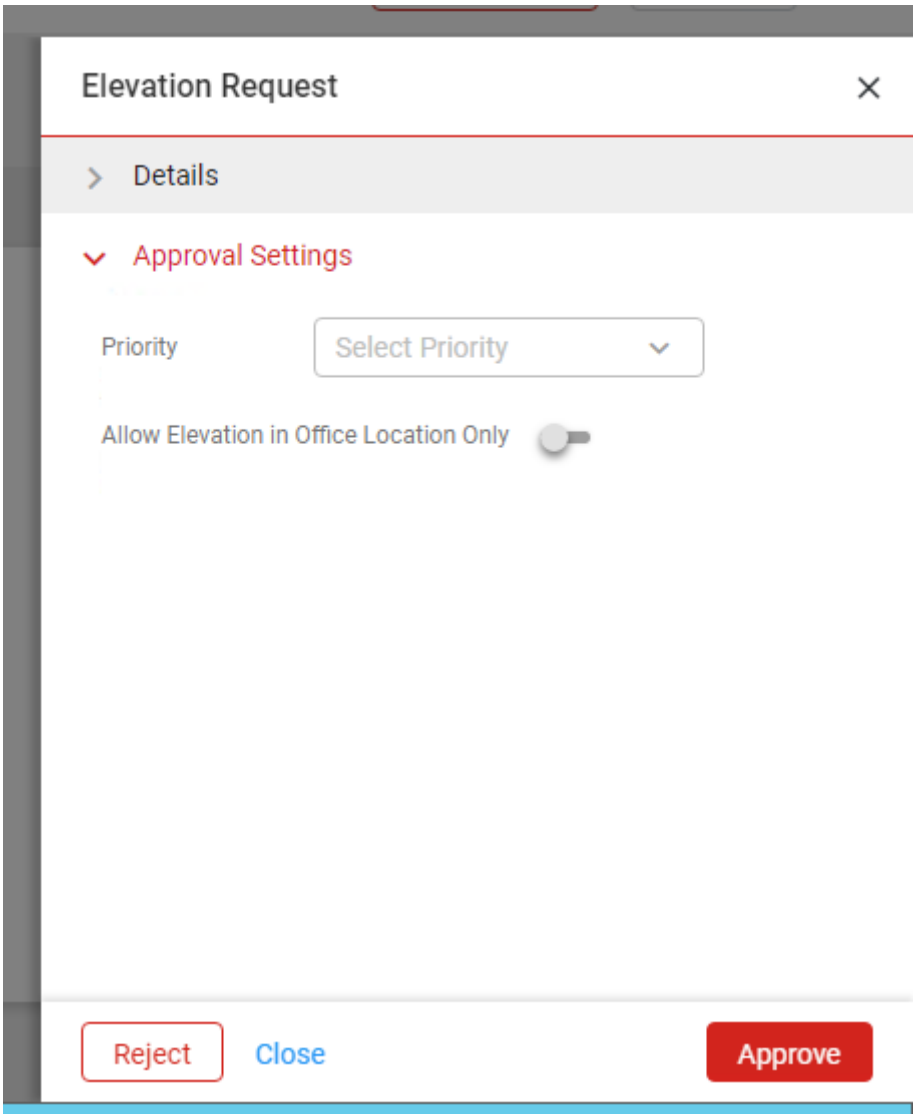
Field	Description
From Date	Select the From Date for which you want to fetch the report Click the calendar icon to select the From Date
To Date	Select the To Date for which you want to fetch the report Click the calendar icon to select the To Date

Refer to the following table to understand each of the fields on the report:

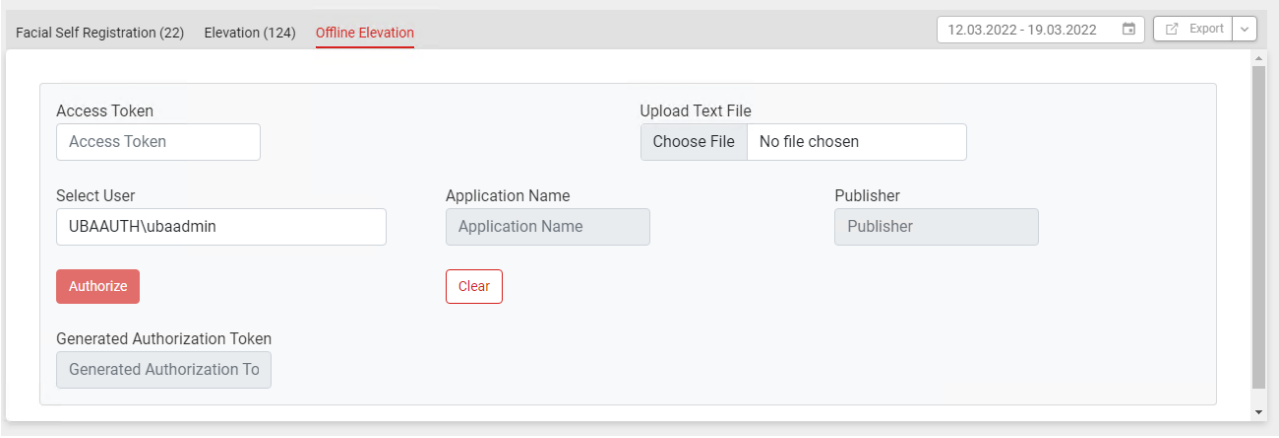
Field	Description
Request ID	This field displays the request-id
Application Name	This field displays the Application Name for which elevation request was raised
Requested By	This field displays the name of the user who raised the elevation request
Created On	This field displays the date when the elevation request was created
Allow Child Process	This feature restricts or allows child process elevation
Allow access only in corporate network	This will allow access only in the corporate network

Field	Description
Actions	:Check: Click on this button to approve the elevation request :Cross: Click on this button to reject the elevation request



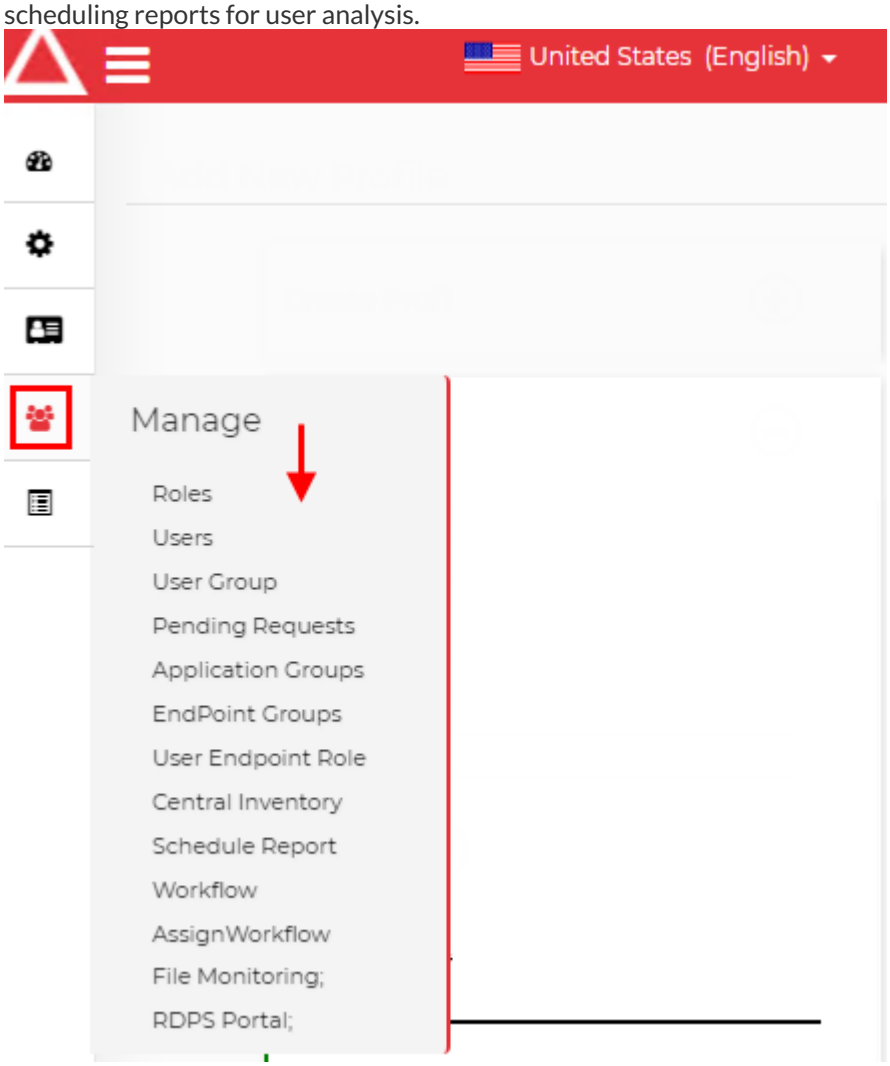


A user can raise an offline elevation request and get a access token which can be used to generate an authorization code below



6 Manage

With the help of the **Manage** menu, users can organize various tasks such as enabling roles, user settings, or scheduling reports for user analysis.



The Manage menu on the UBA application helps users to manage the following tasks:

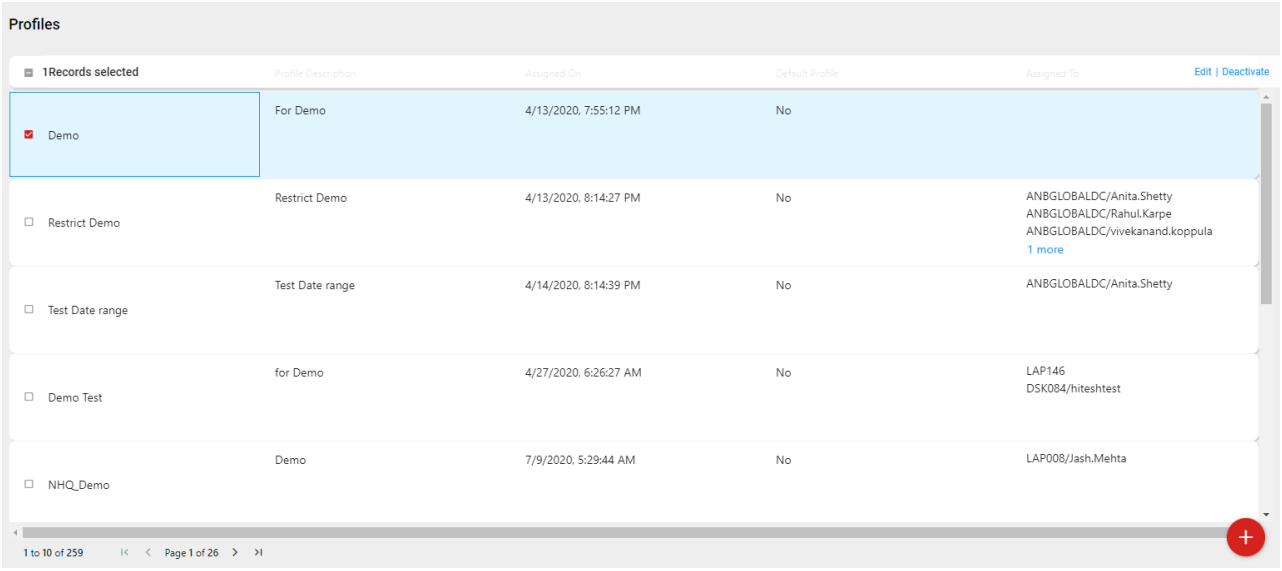
- Roles
- User
- User Group
- Pending Requests
- Application Groups
- End Point Groups
- User End Point Role
- Central Inventory
- Schedule Report
- Workflow
- Assign Workflow
- File Monitoring

6.1 Profiles

The Profiles module displays all the Profiles.

Refer to the following table to understand each of the fields in the Profiles section:

Fields	Description
Profile Name	This field displays the name of the Profile
Profile Description	This field displays the Profile description
Assigned On	This field displays the date and time when the profile was assigned
Default Profile	The **Default Profile** is a generic profile not specific to the user When a user is onboarded and if no specific profile is assigned to a user, a **Default Profile** gets applied to them This field displays two values **Yes** or **No** If the profile is a **Default Profile** the value of this field is **Yes** and if the profile is not a default profile the value of this field is displayed as **No**
Assigned To	This field displays the users assigned to a profile
Actions	This field gives you the option to Edit and deactivate a Profile Actions has the following icons.  **Edit:** Click on this button to edit the selected profile **Deactivate:** Click to deactivate the Profile



Add New Profile

This Add(+) button can be used to create monitoring profiles for users, groups, or departments based on your monitoring needs.

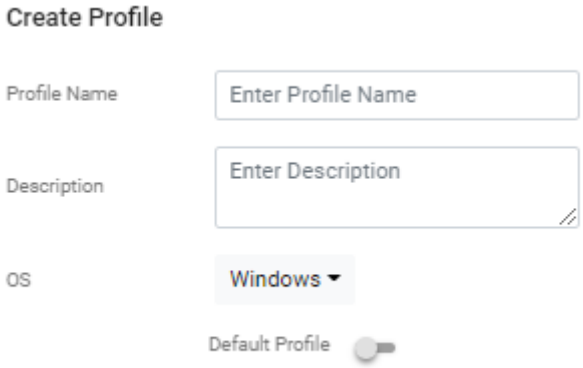
Administrators can make individual settings for every user depending on their individual duties.

It allows you to set up fully customizable rules & alerts, enforce good user behavior, and get Instant notifications with violation details.

You can take immediate actions like notify, alert, warn, restrict when rule violation is detected.

Refer to the following table to understand each of the fields in the Create Profile:

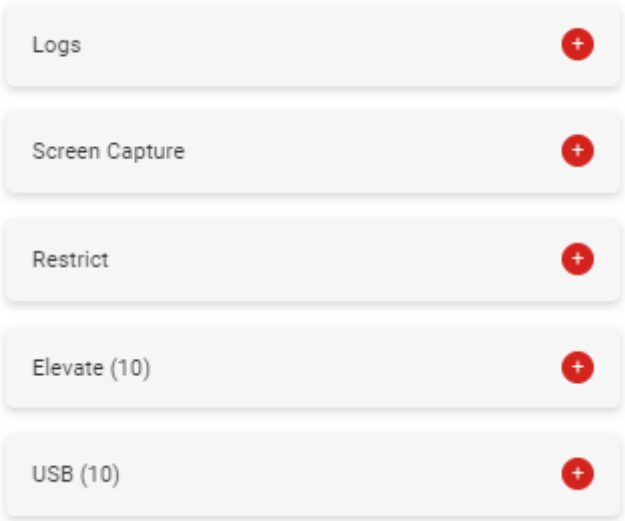
Field	Description
Profile Name	Specify the profile name in this field
Description	Specify the profile description in this field
Active	Enable this button to make the profile Active
Default Profile	Enable this button to define this profile as a Default profile
OS	This field display the OS option, select the OS installed in the system
Save Profile	Click this button to save the profile



6.1.1 Rules

The Add Rules section has the following tabs/Rules:

- Log
- Screen Capture
- Restrict
- Elevate
- USB



6.1.1.1 Log

You can record/capture all the activities on the endpoint with the help of Keystroke Logging, Clipboard Monitoring, URL capture, Keyboard Monitoring, Process Monitoring.

Every activity recorded includes the timestamp of the event.

With Monitoring/Recording, you get total visibility on the following items:

- Time spent actively using work and non-work related applications/processes
- Application usage
- Emails sent and received
- Social media activity
- Chats & instant messages

- Browsing habits
- File Downloads/Uploads
- Keystrokes typed
- Document/Files or copied to a USB stick
- Clipboard activity
- Sensitive File Monitoring

You can also configure an alert on any of the above user behavior by setting up this rule to detect a specified keyword, keyword group, process, or multiple processes.

Field	Description
All	**Logs → Details → All** When you select this button, the option to select or add individual Process, Process Group, Keyword, Keyword Group will not be available When you enable this switch all the Keywords, Keyword Groups, Process, Process Groups and video logs will be monitored
Raise alert	**Logs → Details → Raise Alert** Administrators can enable the **Raise Alert** button to raise alerts when users types in selected keywords or selected processes in this section
Outside PAM Monitoring	When this toggle is enabled all the activity will be captured for every process when the user will log into the machine without using PAM
Key Stroke	**Logs->Details-> Key Stroke** Enable the **KeyStroke** button to capture the keystrokes during keyword and process monitoring Gain insight into employee's daily activity through video log, attitude, and productivity with keystroke logging and detect potentially dangerous keywords even as the users type them

Field	Description
Clipboard	**Logs->Details-> Clipboard** Administrators can set this rule to retrieve any information that was once copied to the clipboard. It captures clipboard content in various formats i.e. text, images, files It captures all the text data, which has been copied or cut and then pasted into documents, files, applications, browser address bar, etc on the end machines It captures all image data, which has been copied or cut and then pasted into documents, files, applications, etc on the end machine It also captures file activities such as print, copy, paste, and download
Keyword	**Logs->Details-> Keyword** This filter can be used to monitor keywords. You can configure these rules for single or multiple keywords Enter specific words that cannot be used by users or that you want to monitor on the endpoint For instance, enter a piece of a trade secret or business process and whenever they are typed the text logs/monitoring will start • **Enter Keyword** Select the **Enter Keyword** radio button and add the keywords in a comma-separated format in the **Keywords** textbox. Enter single or multiple keywords in the textbox This allows you to: • Automate a large portion of your administrative duties • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communication

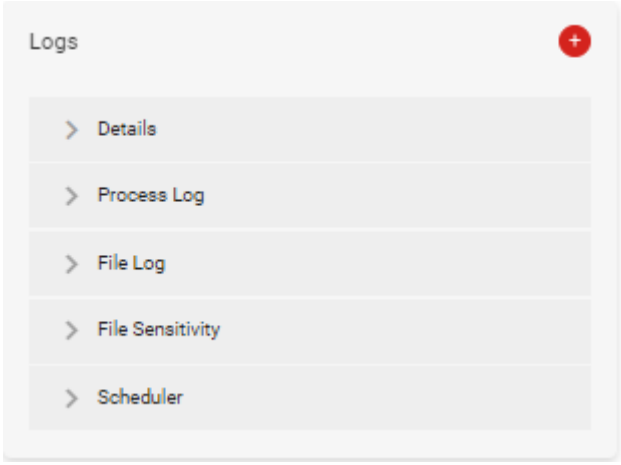
Field	Description
Keyword Group	**Logs->Details-> Keyword Group** This filter can be used to monitor Keyword Group. You can configure these rules to monitor single or multiple Keyword Groups For instance, enter group of keywords related to business trade secret or process and whenever they are typed the text logs/monitoring will start • **Select Keyword Group** When you select the **Select Keyword Group** radio button **Select Keyword Group** dropdown will appear along with the **Add Keyword Group** link Click on the **Add Keyword Group**, a popup named **Keyword Group** opens up Add the following details and save to save the keyword group • **Group Name:** Add the name of the group • **Add Keywords:** Add the keywords in a comma-separated format in this textbox **Save:** Click this button to save the Keyword Group. **Close:** Click this button to close the popup This allows you to: • Automate a large portion of your administrative duties • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communication

Field	Description
Process	**Logs->Details-> Process** This filter can be used to monitor processes. You can configure these rules to monitor single or multiple processes The **Process** dropdown has predefined processes, Select single or multiple processes from the dropdown You can configure these rules for different activities such as browsing, email, file access, application access, instant messaging and more This allows you to: • Automate a large portion of your administrative duties • Evaluate the steps a user takes to complete a task in real-time • Saves on Licensed Software by identifying non usable expensive licensed software is not being used • Track Application Usage to Manage Costs • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communications

Field	Description
Process Group	**Logs->Details-> Process Group** This filter can be used to monitor process groups. You can configure these rules for single or multiple Process Groups The Process *Group* dropdown has different process groups, Select single or multiple process groups from the dropdown You can configure these rules for different activities such as browsing, email, file access, application access, instant messaging, and more This allows you to: • Automate a large portion of your administrative duties • Evaluate the steps a user takes to complete a task in real-time • Saves on Licensed Software by identifying non usable expensive licensed software is not being used • Track Application Usage to Manage Costs • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communication
File Path	File path can be defined for monitoring and getting the logs
Files Extension	Files can be defined for monitoring and getting the logs
File Keywords	File keywords can be defined for monitoring and getting the logs of specified keywords in the files
Path Exclusions	Path exclusions can be defined
File Exclusions	File exclusions can be defined
Process Exclusions	Processes can be selected from the dropdown list for excluding them

Field	Description
File Sensitivity	**Logs->Details-> File Sensitivity** Enable the File Sensitivity to monitor the selective files and obtain logs
Enter Sensitive Keyword	The Enter Sensitive Keyword filter can be used to monitor keywords. You can configure these rules for single or multiple keywords. Enter specific words that cannot be used by users or that you want to monitor at the endpoint.
Select Sensitive Keyword Group	The Select Sensitive Keyword Group filter can be used to select, monitor and process groups. You can configure these rules for single or multiple Process Groups. The Select Sensitive Keyword Group dropdown has different process groups. Select single or multiple process groups from the dropdown that you want to monitor.
File Keywords	File keywords can be defined to monitor and restore logs of specified keywords in files
File Extension	File Extension can be defined for monitoring and restoring the logs
Log When in Office Location	Enable the Log When in Office Location to upload or restore the logs to the server from the office network location
Log When System Idle	Enable the Log When System Idle to upload or restore the logs when the system is idle
URLs	Specify the URLs of the application hosted
Outside PAM Monitoring	Enable Outside PAM Monitoring to access UBA without logging into PAM via RDPS portal

Field	Description
Scheduler	**Logs->Details-> Scheduler** Schedule the monitoring to only occur during designated work hours Select the timeslot from the following options: • **Daily** Specify the time interval **(Start Time, End Time)** for which you want to Schedule the monitoring Select this option to monitor work daily, at a designated time • **Weekly** Click this radio button to monitor work on weekly basis, at a designated time and day of the week Specify the time interval **(Start Time, End Time)** for which you want to Schedule the monitoring • **Range** Click this radio button to monitor work for the selected dates/ date range, at a designated time Specify the date range **(Start Date, End Date)** for which you want to Schedule the monitoring Specify the time interval **(Start Time, End Time)** for which you want to Schedule the monitoring
Save	Click on the **Save** button to save the details



6.1.1.2 Screen Capture

Configure this rule for monitoring and video recording purpose for selected Keywords, Keyword Groups, Processes, or Process Groups.

ARCON | EPM uses an on-screen video recording facility that captures individual user activities.

Each video is saved and attached to the related user activity log. The user activity logs along with the videos deliver a searchable summary of all user actions. This enables administrators to view user activities on the endpoint.

The keyboard and Process monitoring rule for video logs records all information to comprehensive video logs which can be used to formulate a base of user-based behavior analytics. It also provides insight into the management of users.

Extensive history logs allow past recordings to be searched and retrieved in seconds. Recorded files can be exported and downloaded.

The Rule also helps you in identifying specific fragments of the video, when the user, for example, interacted with a certain website or a program; you can also see the violations that may have happened.

Field	Description
All	**Screen Capture->Details->All** When you select this button, the option to select or add individual Process, Process Group, Keyword, Keyword Group will not be available When this toggle is enabled all the activity will be captured for every process When you enable **All** this option also functions as a screen capture of the work area of end-user every 2 seconds, the recorded videos accessed by admin and monitored
Outside PAM Monitoring	When this toggle is enabled all the activity will be captured for every process when the user will log into the machine without using PAM

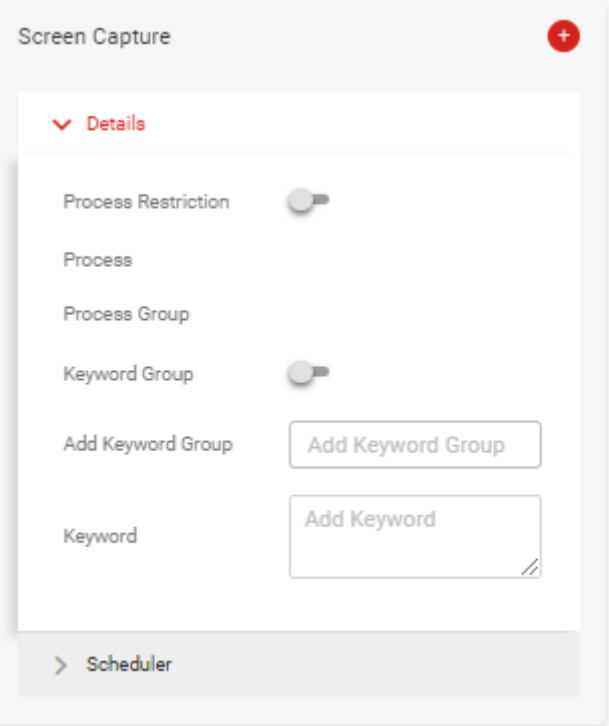
Field	Description
Keyword	**Screen Capture->Details-> Keyword** This filter can be used to monitor keywords. You can configure these rules for single or multiple keywords Enter specific words that cannot be used by users or that you want to monitor on the endpoint For instance, enter a piece of a trade secret or business process and whenever they are typed the screen capture/video monitoring will start • **Enter Keyword** Select the **Enter Keyword** radio button and add the keywords in a comma-separated format in the **Keywords** textbox. Enter single or multiple keywords in the textbox. This allows you to: • Automate a large portion of your administrative duties • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communication

Field	Description
Keyword Group	**Screen Capture->Details-> Keyword Group** This filter can be used to monitor Keyword Group. You can configure these rules to monitor single or multiple Keyword Groups For instance, enter group of keywords related to business trade secret or process and whenever they are typed the screen capture/video monitoring will start • **Select Keyword Group** When you select the Select **Keyword Group** radio button ***Select Keyword Group*** dropdown will appear along with the **Add Keyword Group** link Click on the **Add Keyword Group**, a popup named **Keyword Group** opens up Add the following details and save to save the keyword group • **Group Name:** Add the name of the group • **Add Keywords:** Add the keywords in a comma-separated format in this textbox **Save:** Click this button to save the Keyword Group. **Close:** Click this button to close the popup This allows you to: • Automate a large portion of your administrative duties • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communication

Field	Description
Process	**Screen Capture->Details-> Process** This filter can be used to monitor processes. You can configure these rules to monitor single or multiple processes The **Process dropdown** has predefined processes, Select single or multiple processes from the dropdown You can configure these rules for different activities such as browsing, email, file access, application access, instant messaging, and more This allows you to: • Automate a large portion of your administrative duties • Evaluate the steps a user takes to complete a task in real-time • Saves on Licensed Software by identifying non usable expensive licensed software is not being used • Track Application Usage to Manage Costs • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communication

Field	Description
Process Group	**Screen Capture->Details-> Process Group** This filter can be used to monitor process groups. You can configure these rules for single or multiple Process Groups The **Process Group** dropdown has different process groups, Select single or multiple process groups from the dropdown You can configure these rules for different activities such as browsing, email, file access, application access, instant messaging, and more This allows you to: • Automate a large portion of your administrative duties • Evaluate the steps a user takes to complete a task in real-time • Saves on Licensed Software by identifying non usable expensive licensed software is not being used • Track Application Usage to Manage Costs • View what your users are searching for and where they are doing so • Which employees spend half the day on Facebook, Amazon, etc • Determine whether the right amount of resources is used to deliver a service, product or activity • Ensure that sharing of confidential data will be monitored when it is shared with others through email, applications, websites, and other forms of online communication

Field	Description
Scheduler	**Logs->Details-> Scheduler** Schedule the monitoring to occur only during designated work hours Select the timeslot from following options: • **Daily** Specify the time interval **(Start Time, End Time)** for which you want to Schedule the monitoring Select this option to monitor work daily, at a designated time • **Weekly** Click this radio button to monitor work on weekly basis, at a designated time and day of the week Specify the time interval **(Start Time, End Time)** for which you want to Schedule the monitoring • **Range** Click this radio button to monitor work for the selected dates/ date range, at a designated time Specify the date range **(Start Date, End Date)** for which you want to Schedule the monitoring Specify the time interval **(Start Time, End Time)** for which you want to Schedule the monitoring
Save	Click on the **Save** button to save the details



6.1.1.3 Restrict

ARCON | EPM Restriction Rule quickly spots user negligence and violations. Restriction rule triggers alerts when certain restricted keywords are used, certain restricted programs, are started, or restricted applications or files with listed names are opened.

The user gets automatic notifications on violation of the restriction rule.

There are two types of Restrictions. They are:

- **Blacklist Restriction**
- **Whitelist Restriction**

6.1.1.3.1 Blacklist Restriction

The Blacklist Restriction defines which entities should be blocked. The entities that are defined under BlackList Restriction will be blocked. Select the BlackList Restriction from the dropdown and define all entities that need to be blocked.

Refer to the following table to understand each of the fields in the Blacklist Restriction section:

Field	Description

Process	**Restrict-> BlackList Restriction->Process** This filter is used to restrict single or multiple Processes You can configure these restriction rules for different processes such as browsing activities, email, file access, application access, instant messaging, and more by setting up this rule to restrict a single process, or multiple process This allows you to: • Automate a large portion of your administrative duties • Restrict employee's from accessing unnecessary sites • Restrict sharing of confidential data via email, applications, websites, and other forms of online communication
Process Group	**Restrict -> BlackList Restriction-> Process Group** This filter is used to restrict single or multiple Process Group You can configure these rules for different processes such as browsing activities, email, file access, application access, instant messaging, and more by setting up this rule to restrict a single process group, or multiple process groups This allows you to: • Automate a large portion of your administrative duties • Restrict employee's from accessing unnecessary sites • Restrict sharing of confidential data via email, applications, websites, and other forms of online communication
Outside PAM Restrict	When this toggle is enabled all the user will not be able to login to any server\Desktop without PAM. And when user tries to login the server\desktop without PAM the admin will receive the alert. 

Command Line Argument	**Restrict ->BlackList Restriction->Command Line argument** Now you can restrict the end-user from executing a specific command. This functionality allows them to execute a limited set of commands in the same process/ processes as per their feasibility. It can be done via the following settings Select single or multiple Processes from the **Process** dropdown or Process Groups from the **Process Group** dropdown In the **Command Line argument** textbox add the command or set of commands corresponding to the specific processes that you want to block
Product Version	Products can be restricted to be based on versions
File Version	Files can be restricted to be based on versions
Facial Recognition	If this toggle is enabled the process can be restricted, user can access that application after successful validation of Facial Recognition
Select Notification Policy	Select the notification policy from this dropdown You can use the Notification Policy to notify the administrators via email with violation details when rule violation happens due to user negligence or otherwise
Select severity	Select severity Configure the severity based of violations of rule. **Severity:** *__Low__ - Rules that match this exception are of low importance. The rule violation is minor. *__Medium__ - Rules that match this exception are of medium importance. The rule violation is moderate. *__High__ - Rules that match this exception are of High importance. The rule violation is severe.

Keyword	**Restrict ->BlackList Restriction-> Keyword** This filter is used to restrict single or multiple Keywords Enter specific words that you want to restrict on the endpoint For instance, enter a piece of a trade secret or business process and whenever they are typed the window is automatically closed • **Enter Keyword** Select the **Enter Keyword** radio button and add the keywords in a comma-separated format in the **Keywords** textbox. Enter single or multiple keywords in the textbox This allows you to: • Automate a large portion of your administrative duties • Restrict employee's from accessing unnecessary keywords • Restrict sharing of confidential data via email, applications, websites, and other forms of online communication

Keyword Group	**Restrict ->BlackList Restriction->Keyword Group** This filter is used to restrict single or multiple Keyword Groups Enter specific Keyword Groups that you want to restrict on the endpoint For instance, enter a piece of a trade secret or business process and whenever they are typed the window is automatically closed • **Select Keyword Group** When you select the **Select Keyword Group** radio button *Select* **Keyword Group** dropdown will appear along with the **Add Keyword Group** link Click on the Add Keyword Group, a popup named Keyword Group opens up Add the following details and save to save the keyword group • **Group Name:** Add the name of the group • **Add Keywords:** Add the keywords in a comma-separated format in this textbox **Save:** Click this button to save the Keyword Group. **Close:** Click this button to close the popup Once you save the Keyword Group, it will be visible under **"Select Keyword Group"** This allows you to: • Automate a large portion of your administrative duties • Restrict employee's from accessing unnecessary keywords • Restrict sharing of confidential data via email, applications, websites, and other forms of online communication
Enter Publisher Name	Enter the Application Publisher Name in this textbox that you want to block

Other Restrictions	You can add other restrictions in this dropdown such as: **User Creation** - Restrict users from new user creation **Software Installation** - Restrict users from installation of software **Printer Installation** - Restrict Printer installation/ usage to a specific entity/set of people as per organization's requirements **Multiple Network Connections** - Restrict end user to only one way of accessing network- only corporate ethernet or only wifi access **MTP Restrictions** - Restrict the users from connecting to any portable media devices like Mobile phone **USB Modem and Tethering** - Restrict USB Modem and Tethering capability from the endpoint for the endpoint user **Print screen** - Restrict all screen capturing capability for eg. Prt Scr button etc. for the endpoint user

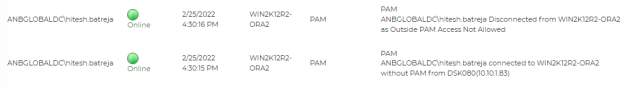
Control Panel Restrictions	**Restrict ->BlackList Restriction->Control Panel Restrictions** You can restrict end-users from accessing the tabs under the **Internet Options** dialog box The **Control Panel Restrictions** dropdown gives you options either to block all the tabs or individual tabs under **Internet Options** dialog box This devoids end-users from tweaking and making unwanted configuration changes to **Internet Options** To block all the tabs under the **Internet Options** dialog box, select **All Internet Options** from the **Control Panel Restrictions** dropdown To block individual tabs, select the desired option from the following list available in the **Control Panel Restrictions** dropdown **Date Time Setting:** Restrict the user from making changes to the date-time and timezone settings on the end machine **Internet Security:** Restrict the user from making changes to internet sites, trusted sites or restricted sites or sites found in the intranet **Internet Privacy:** Restrict the user from making changes to internet privacy **Internet Content:** Restrict the user from making changes to content-related settings including Parental Controls, Content Advisor, Certificates, AutoComplete, and Feeds and Web Slices **Internet Connections:** Restrict the user from making changes to internet privacy **Internet Programs:** Restrict the user from making changes to internet programs. Restriction the user from making changes to internet programs **Internet Advanced:** Restrict the user from making changes to advanced settings

Upload/Download Restrictions	**Restrict ->BlackList Restriction->Upload/Download Restrictions** You can restrict end-users from upload/download files from **google drive** and **dropbox** by selecting the requried tabs under the dropdown dialog box. The **Upload/Download Restrictions** dropdown gives you options either to block all the tabs or individual tabs. The download or upload of files for personal use is restricted for end-users. To block all the tabs under the dialog box, select **All Options** from the **Upload/ Download Restrictions** dropdown. To block individual tabs, select the desired option from the following list available in the Upload/ Download Restrictions dropdown: • **Upload (Google Drive):** Enable the upload Google Drive option to restrict the user from uploading files and data to Google Drive. • **Download (Google Drive):** Enable the download Google Drive option to restrict the user from downloading files and data from Google Drive. • **Upload (Dropbox):** Enable the Upload Dropbox option to restrict the user from uploading files and data to Dropbox. • **Download (Dropbox):** Enable the Download Dropbox option to restrict the user from downloading files and data from Dropbox.
Allowed Wifi	Allowed Wifi can be defined which will restrict the users from connection other Wifi network. In recent work from home scenarios, whenever an end user is connected to an unverified public wifi, ARCON| EPM detects the same and restricts the access to the same. It allows connection only for corporate and verified networks
Select Service	Services can be selected from the list to be restricted
Select Access	Start or Stop to be restricted for the service can be defined
Save	Click this button to save the details

6.1.1.3.2 Whitelist Restriction

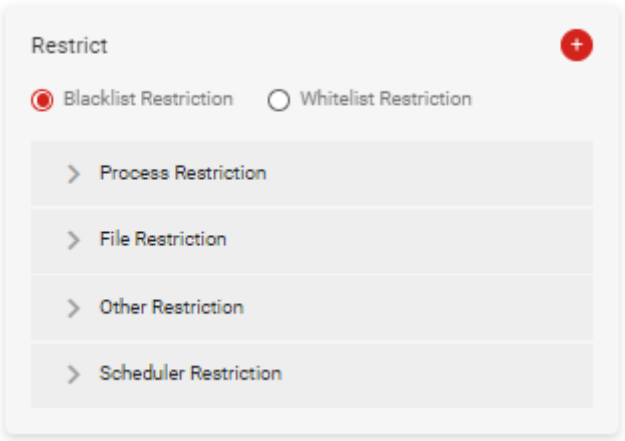
The Whitelist Restriction defines which entities should be allowed. The entities that are defined under the Whitelist Restriction will be allowed and the rest will be blocked. Select the Whitelist Restriction from the dropdown and define all entities that need to be allowed.

Refer to the following table to understand each of the fields in the Whitelist Restriction:

Field	Description
Process	**Restrict->Whitelist Restriction->Process** This filter is used to allow single or multiple Processes and restrict all other processes You can configure these restriction rules for different processes such as browsing activities, email, file access, application access, instant messaging, and more by setting up this rule to restrict a single process, or multiple process This allows you to: • Automate a large portion of your administrative duties • Restrict employee's from accessing unnecessary sites • Restrict sharing of confidential data via email, applications, websites, and other forms of online communication
Process Group	**Restrict -> Whitelist Restriction-> Process Group** This filter is used to restrict single or multiple Process Group You can configure these rules for different processes such as browsing activities, email, file access, application access, instant messaging, and more by setting up this rule to restrict a single process group, or multiple process groups This allows you to: • Automate a large portion of your administrative duties • Restrict employee's from accessing unnecessary sites • Restrict sharing of confidential data via email, applications, websites, and other forms of online communication
Outside PAM Restrict	When this toggle is enabled all the user will not be able to login to any server\Desktop without PAM. And when user tries to login the server\desktop without PAM the admin will receive the alert. 

Field	Description
Select Notification Policy	**Restrict -> Whitelist Restriction-> Select Notification Policy** Select the notification policy from this dropdown You can use the Notification Policy to notify the administrators via email with violation details when rule violation happens due to user negligence or otherwise
Select severity	**Restrict -> Whitelist Restriction->Select severity** Select severity Configure the severity based of violations of rule **Severity:** *__Low__ - Rules that match this exception are of low importance. The rule violation is minor *__Medium__ - Rules that match this exception are of medium importance. The rule violation is moderate *__High__ - Rules that match this exception are of High importance. The rule violation is severe
Enter Path Exclusions	**Restrict -> Whitelist Restriction->Enter Path** Add all the application paths that will be accessible to the end-user in the **Enter Path** field Add all the application paths that will not be accessible to the end-user in the **Exclusions** field
Enter Publisher Name Exclusions	**Restrict -> Whitelist Restriction->Enter Publisher Name** Add all the application publisher names that will be accessible to the end-user in the **Enter Publisher Name** field Add all the application publisher names that will not be accessible to the end-user in the **Exclusions** field
Priority	**Restrict -> Whitelist Restriction ->Priority** **Priority:** *__Low__ – Rules that are saved with this options are of low importance *__Medium__ - Rules that are saved with this options are of medium importance *__High__ - Rules that are saved with this options are of High importance

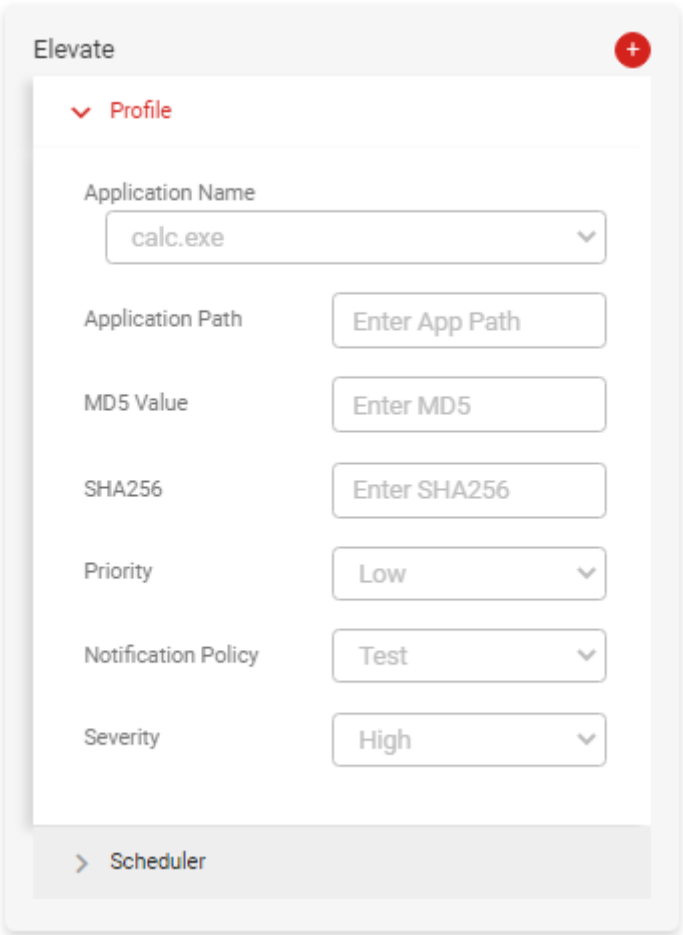
Field	Description
Scheduler	**Restrict -> Whitelist Restriction-> Scheduler** Schedule the restriction to only occur during designated work hours Select the timeslot from following options: • **Daily** Specify the time interval **(Start Time, End Time)** for which you want to Schedule the restriction policies Select this option to monitor work daily, at a designated time • **Weekly** Click this radio button to monitor work on weekly basis, at a designated time and day of the week Specify the time interval **(Start Time, End Time)** for which you want to Schedule the restriction policies • **Range** Click this radio button to monitor work for the selected dates/ date range, at a designated time Specify the date range **(Start Date, End Date)** for which you want to Schedule the restriction policies Specify the time interval **(Start Time, End Time)** for which you want to Schedule the restriction policies
Save	Click this button to save the details



6.1.1.4 Elevate

Application Elevation policy is a management method that assures that users have no access to any of the applications unless such access has been explicitly granted. Discovers elevated apps report.

Administrators can explicitly elevate certain applications for end-users.



Refer to the following table to understand each of the fields in the Details tab:

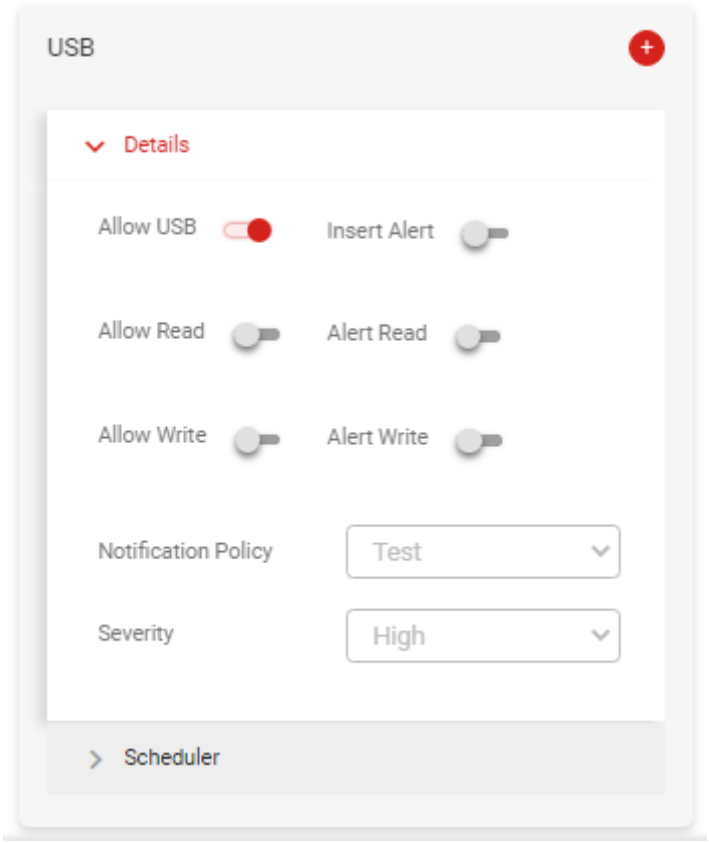
Field	Description
Application Name	Specify the application name that you want to elevate for the end-user
Application Path	Specify the application path of application that you want to elevate for the end-user
MD5 Value	MD5 Value of the application to be elevated
SHA256	SHA256 Value of the application to be elevated
Priority	**Priority:** *__Low__ – Rules that are saved with this options are of low importance *__Medium__ - Rules that are saved with this options are of medium importance *__High__ - Rules that are saved with this options are of High importance

Field	Description
Select Notification Policy	Select the notification policy from this dropdown You can use the Notification Policy to notify the administrators via email with violation details when rule violation happens due to user negligence or otherwise
Select Severity	Select severity Configure the severity based of violations of rule **Severity:** *__Low__ - Rules that match this exception are of low importance. The rule violation is minor *__Medium__ - Rules that match this exception are of medium importance. The rule violation is moderate *__High__ - Rules that match this exception are of High importance. The rule violation is severe
Scheduler	Schedule the elevation to only occur during designated work hours Select the timeslot from following options: • **Daily** Specify the time interval **(Start Time, End Time)** for which you want to Schedule the elevation policy Select this option to elevate applications daily, at a designated time • **Weekly** Click this radio button to elevate applications on weekly basis, at a designated time and day of the week Specify the time interval **(Start Time, End Time)** for which you want to Schedule the elevation policy • **Range** Click this radio button to elevate applications for the selected dates/ date range, at a designated time Specify the date range **(Start Date, End Date)** for which you want to Schedule the elevation policy Specify the time interval **(Start Time, End Time)** for which you want to Schedule the elevation policy

6.1.1.5 USB

Stop users from reading/writing to USB, or uploading files to the endpoint, or sending certain e-mail attachments to the USB drive.

Configure alerts on the insert, read, write operations for USB.



Refer to the following table to understand each of the fields in the Details tab:

Field	Description
Allow USB	When you enable this button following options will get displayed: • Allow Read • Alert On Read • Allow Write • Alert On Write

Field	Description
Allow Read	Enable this button to allow end-users to read from the USB When you enable this button the **Select Restriction** dropdown will get displayed It has following fields: • **BlackList Restriction** • **Whitelist Restriction** If you select **BlackList Restriction** the **Select Extension** gets displayed, add the extensions in this textbox that you want to block or don't want end-user to read from the endpoint If you select **Whitelist Restriction** the **Select Extension** gets displayed, add the extensions in this textbox that you want to allow the end user to read and block the rest
Alert On Read	Select this option to send an alert when data is read from the USB
Allow Write	Enable this button to allow end-users to write to the USB When you enable this button the **Select Restriction** dropdown will get displayed It has following fields: • **BlackList Restriction** • **Whitelist Restriction** If you select **BlackList Restriction** the **Select Extension** gets displayed, add the extensions in this textbox that you want to block or don't want end-user to write to the endpoint If you select **Whitelist Restriction** the **Select Extension** gets displayed, add the extensions in this textbox that you want to allow the end user to write and block the rest
Alert On Write	Select this option to send an alert when data is written to the USB
Select Notification Policy	On dropdown, select the required notification policy
Select Severity Level	On dropdown, select the required severity
Insert Alert	Enable this option to generate alerts on data read and write options

Field	Description
Save	Click this button to save the details

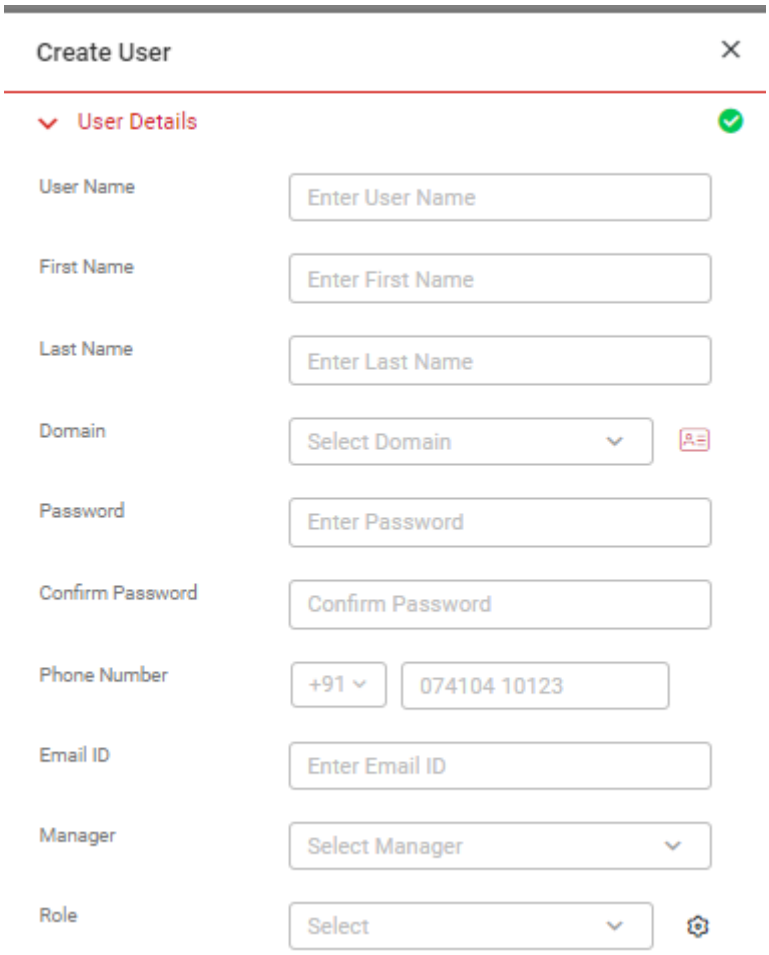
6.2 Users

The **User** module helps you to onboard a user manually or view all onboarded users.

6.2.1 Add User

Refer to the following table to understand each of the fields in the Add User tab:

Field	Description
User Name	Specify the name of the new user in this field
First Name	Specify the first name of the new user
Last Name	Specify the last name of the new user
Email Id	Specify the email id of the new user in this field
Phone No	Specify the phone no of the new user in this field
Domain	Specify the user domain in this field
Role	Specify the role in this field
Manager	Specify the manager details in this field
Password	Select the password to login for the new user
Confirm Password	Confirm the password to login for the new user



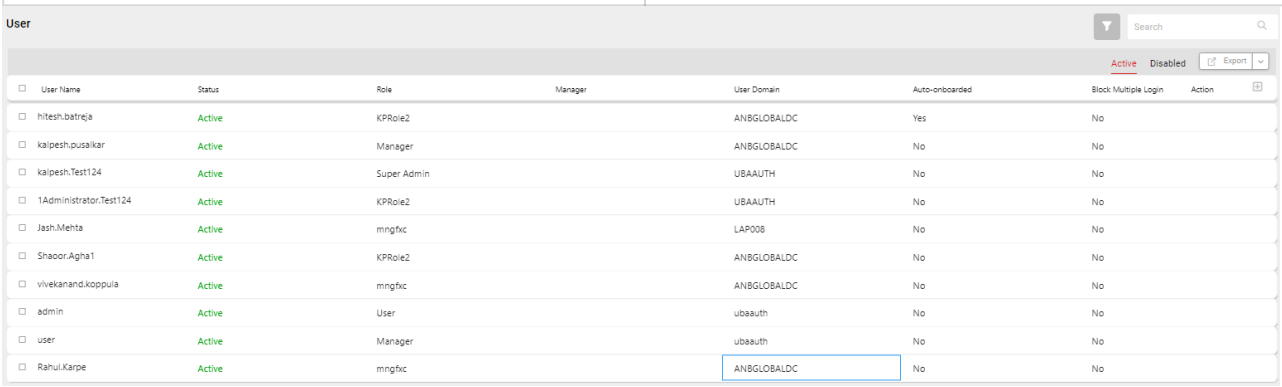
6.2.2 View / Edit User

Once you add users, you can view these users in the Edit/View Users module.

Refer to the following table to understand each of the fields in the Edit/View Users tab:

Field	Description
User Name	This field displays the name of the new user
Role	This field displays the role assigned to the new user
Manager	This field displays the manager assigned to the new user
User Domain	This field displays the domain name of the new user
Status	If the value of this field is Active, it means user is Active. If the value of this field is Inactive, it means user is not active.

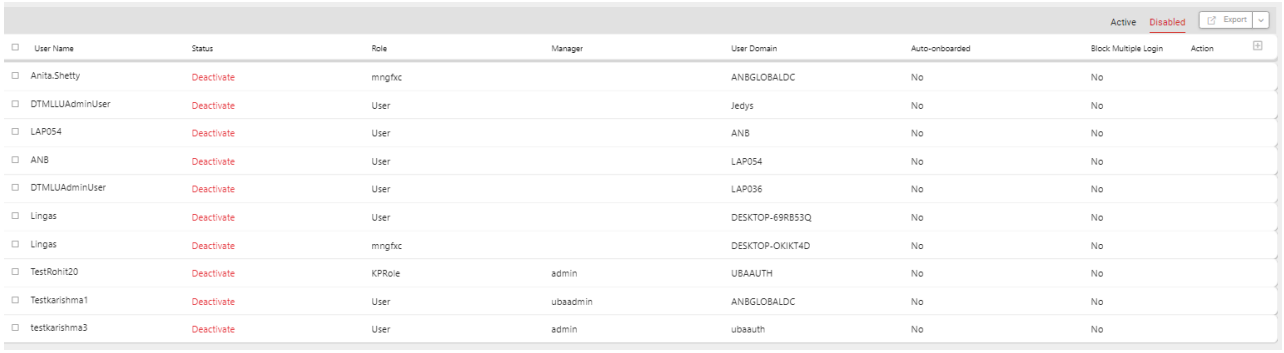
Field	Description
Auto-onboarded	If the value of this field is **Yes**, it means user is auto-onboarded. If the value of this field is **No**, it means user is manually onboarded.
Actions	**Edit:** Click this button to edit the user record **Deactivate:** Click this button to deactivate the user record.



6.2.3 Deactivated Users

Refer to the following table to understand each of the fields in the Deactivated Users tab:

Field	Description
User Name	This field displays the name of the deactivated user
Role	This field displays the role of the deactivated user
Manager	This field displays the manager of the deactivated user
User Domain	This field displays the domain of the deactivated user
Status	This field displays the status of the deactivated user
Auto-onboarded	If the value of this field is **Yes**, it means user was auto-onboarded. If the value of this field is **No**, it means user was manually onboarded.
Actions	**Activate:** Click this button to activate the user record



Active Disabled Export

User Name	Status	Role	Manager	User Domain	Auto-onboarded	Block Multiple Login	Action
Anita.Shetty	Deactivate	mngfxc		ANBGLOBALDC	No	No	
DTMLLUAdminUser	Deactivate	User		Jedys	No	No	
LAP054	Deactivate	User		ANB	No	No	
ANB	Deactivate	User		LAP054	No	No	
DTMLUAdminUser	Deactivate	User		LAP036	No	No	
Lingas	Deactivate	User		DESKTOP-69RB53Q	No	No	
Lingas	Deactivate	mngfxc		DESKTOP-OKIKT4D	No	No	
TestRohit20	Deactivate	KPRole	admin	UBAAUTH	No	No	
Testkarishma1	Deactivate	User	ubaadmin	ANBGLOBALDC	No	No	
testkarishma3	Deactivate	User	admin	ubaauth	No	No	

6.2.4 Facial Recognition

To access Facial Recognition, administrators can navigate to **Manage → Users ->Edit->Facial Recognition**

The facial recognition feature captures end-users face during login.

The facial recognition algorithm then transforms it into digital data and compares the image captured to that held in the database to check if the end-user is a valid user.

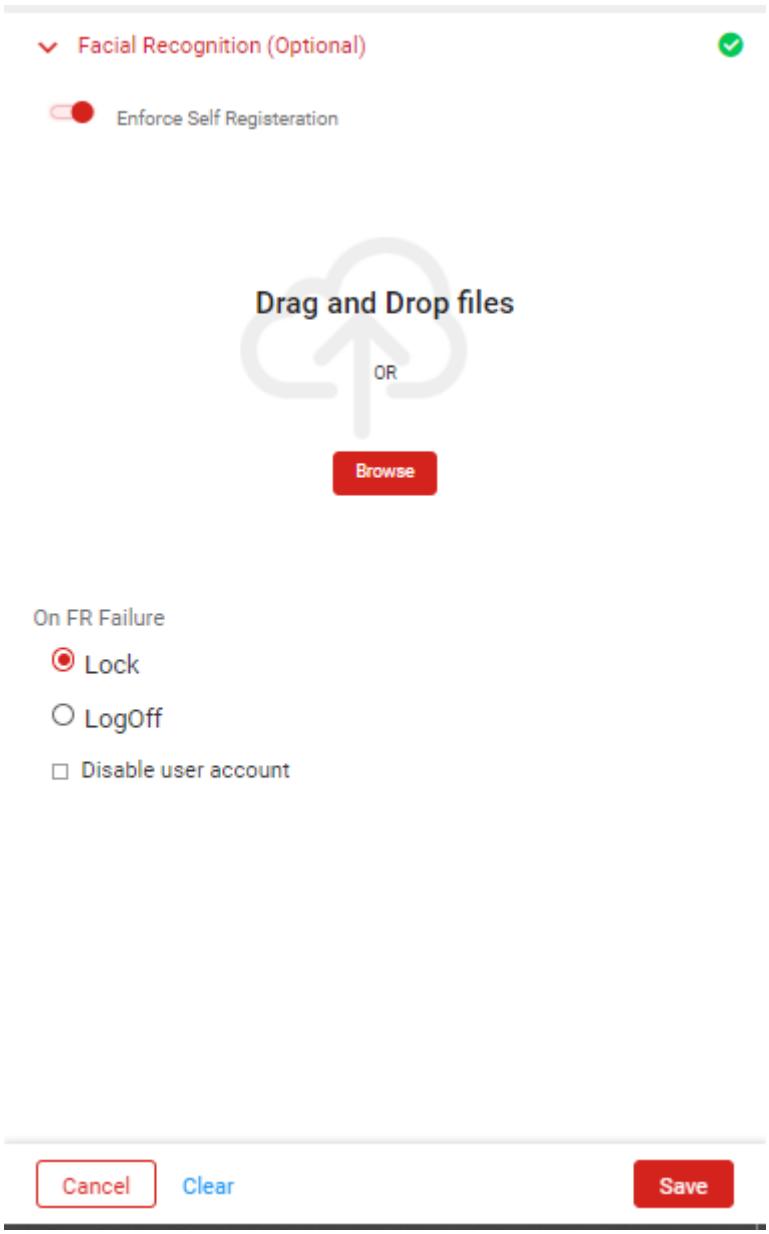
If after validation, the face captured during login doesn't match the face in the database, the end-user is allowed a fixed number of attempts.

After every failed attempt, the Admin/ immediate Manager is notified about the same.

For example, if the number of attempts configured in the console is 3.

After 3 failed login attempts, the end-user should be logged off of the end machine.

The admin can register the user either by uploading the end-users image or the admin can enforce self-registration for the end-user.



Self Registration Enforcement Method for Facial Recognition:

Navigate to **Manage → Users ->Edit ->Facial Recognition**

Click on the user for which you want to enforce the self-registration process.

A pop-up **Edit Users** appears, enable the option **Enforce Self Registration** on this pop-up and click on **Save User.**

Next time when the end-user logs into the machine they will get a window for self-registration called **Facial Recognition Registration.**

The end-user will be able to see their face in the given frame take a picture of themselves and click on submit to freeze the snapshot.

Once done they will get an alert **Face data captured Successfully**.

Once the image is submitted, the admin will get a notification in the notification center -> **New FR self-registration Request from User/ Domain.**

Admin can validate the image captured on the end machine by going back to the user under **Manage → Users ->Edit ->Facial Recognition.**

The **Edit Users** pop-up now displays an uploaded image and there is an option to accept or reject the image. Admin can either Accept or Reject the image.

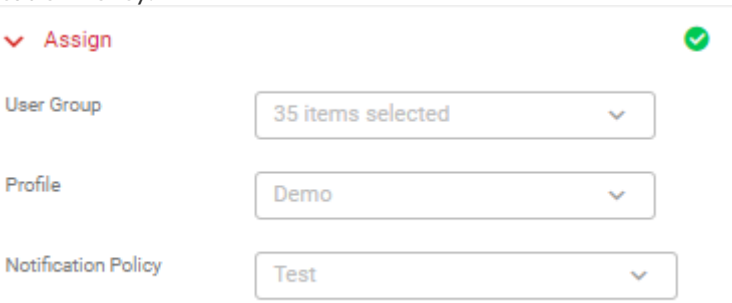
If the admin clicks on the **Accept** button the **Enforce Self Registration** button gets disabled and this particular uploaded image will be used for the end user's Facial Recognition for future events.

The admin can upload the image for the user using **Choose File** button to browse and image.

The admin can select the action of Facial Recognition failure like **Lock** and **Log Off**.

Assign

The Assign module allows you to Assign and Revoke profiles to, User. Along with profile we can also assign user to User Group and Notification Policy.



6.3 Groups

This section allows you to create different types of groups such as User group, Endpoint group and Application group.

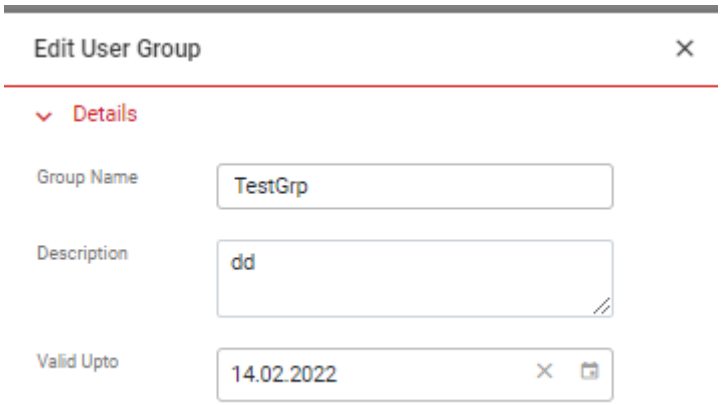
6.3.1 User Group

Administrators can create User groups to make it easier to apply similar profiles or to fetch reports for multiple users.

6.3.1.1 Create/Edit User group

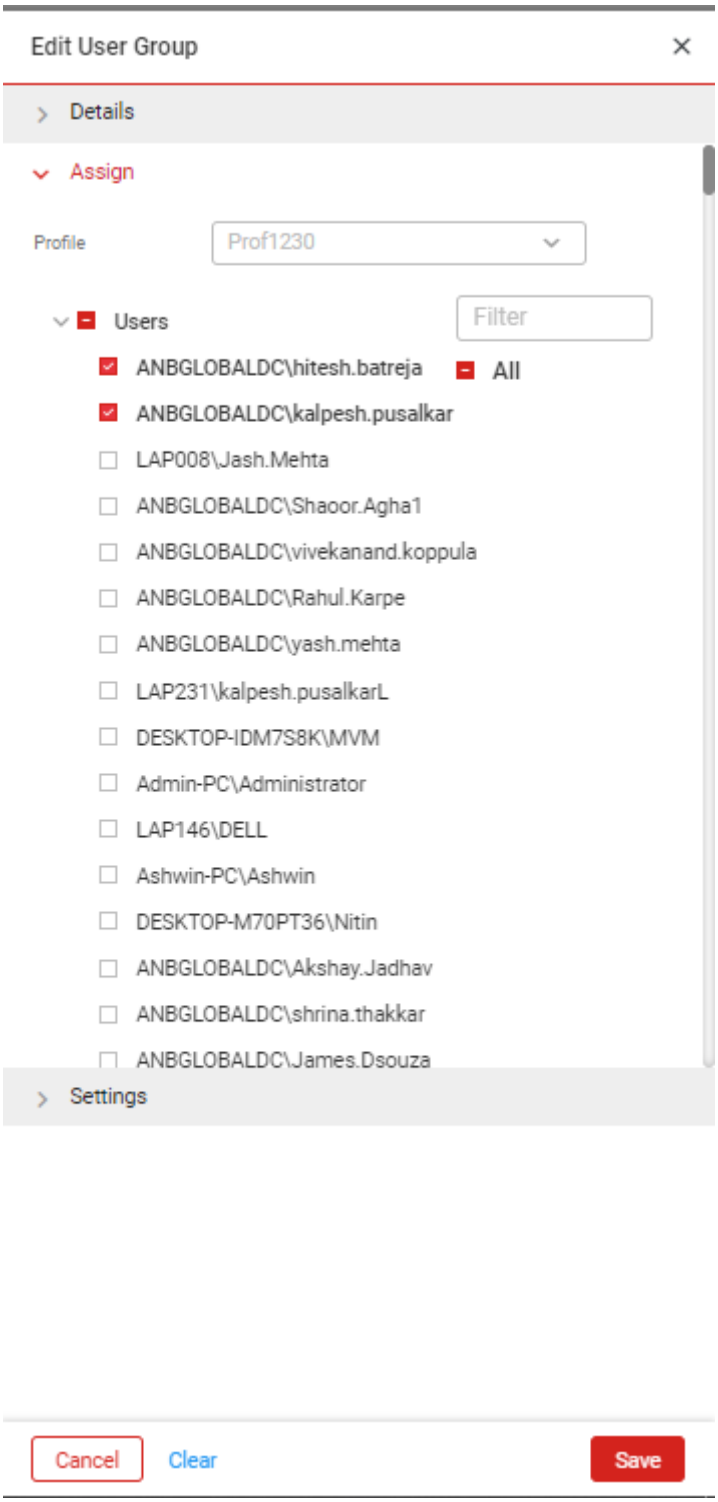
Refer to the following table to understand each of the fields on the Add/Update user group screen:

Field	Description
Group name	Specify the name of the group
Valid upto	Specify the validity of the group
Save	Click the Save button to save the details



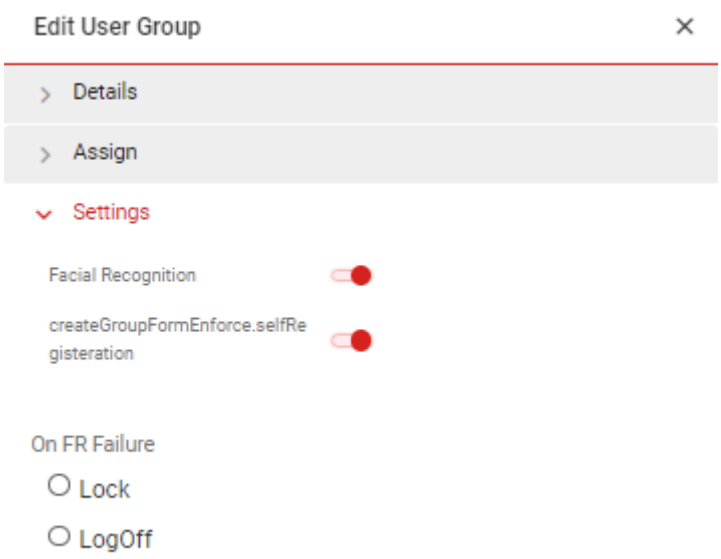
Assign

The Assign module allows you to Assign and Revoke profiles to User Group. We can also assign users to the group.



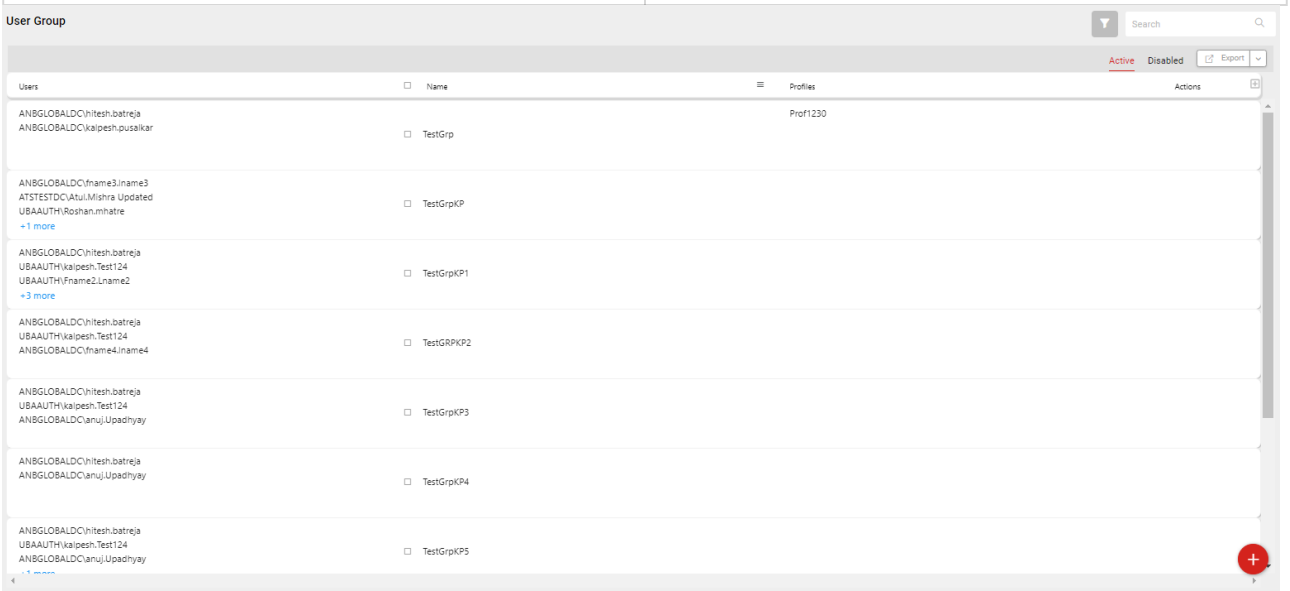
Settings

This module allows you to do Facial Recognition setting according to user group.



The **List view** displays the following fields:

Field	Description
Name	This field displays the name of the Group
Users	This field displays the users assigned to the Group
Profiles	This field displays the profiles assigned to the group.
Action	**Edit:** Click this button to edit the user record **Deactivate:** Click this button to deactivate the user record.

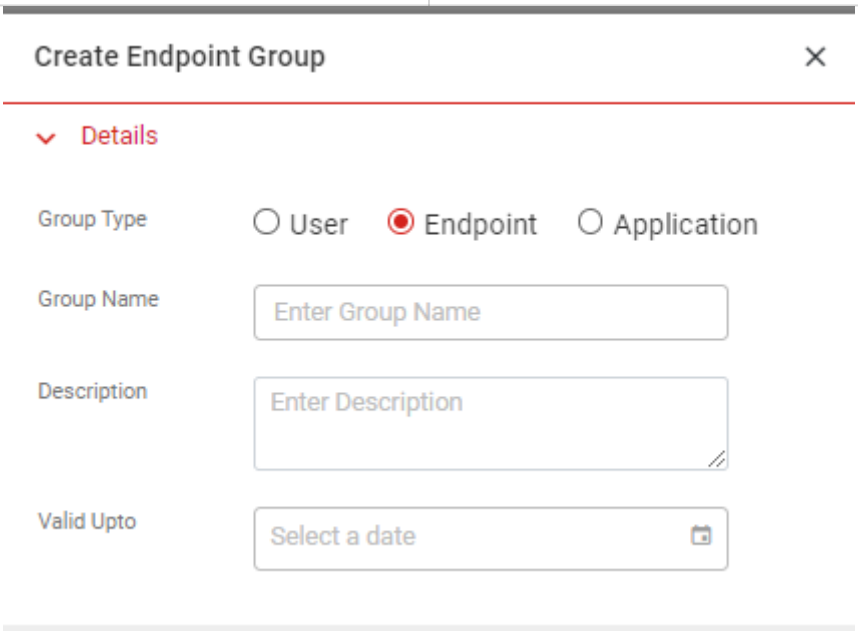


6.3.2 Endpoint Groups

Endpoint Groups module can be used to create groups of endpoints based on the IP range and Hostname.

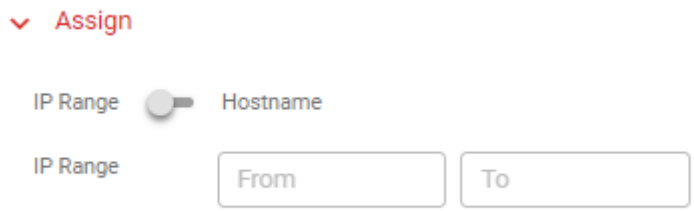
Refer to the following table to understand each of the fields in the Endpoint Groups screen:

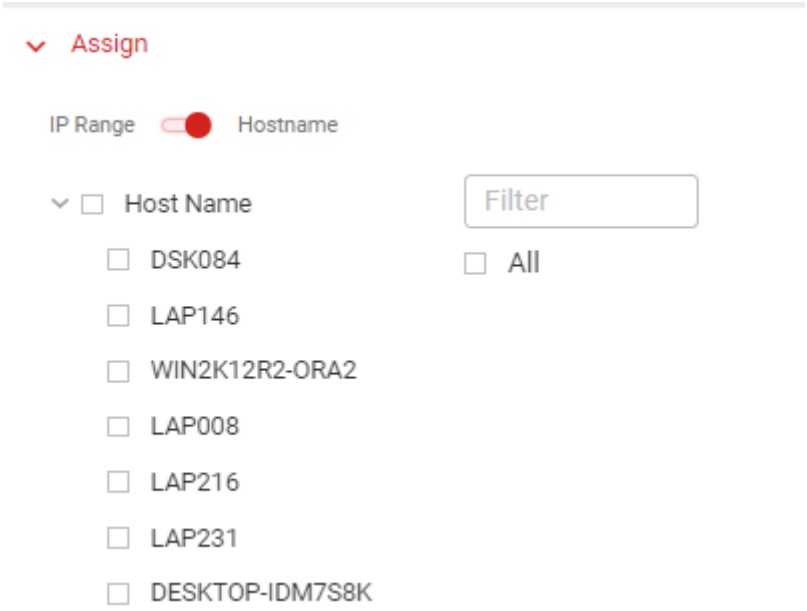
Fields	Description
Group Name	Add group name in this field
Group Description	Add the description to the group in this field
Valid Upto	Select the data from the calendar until you want this group to be valid



Assign

The Assign module allows you to Assign and Revoke hosts to group based on IP Range or Hostname.





6.3.3 Application Groups

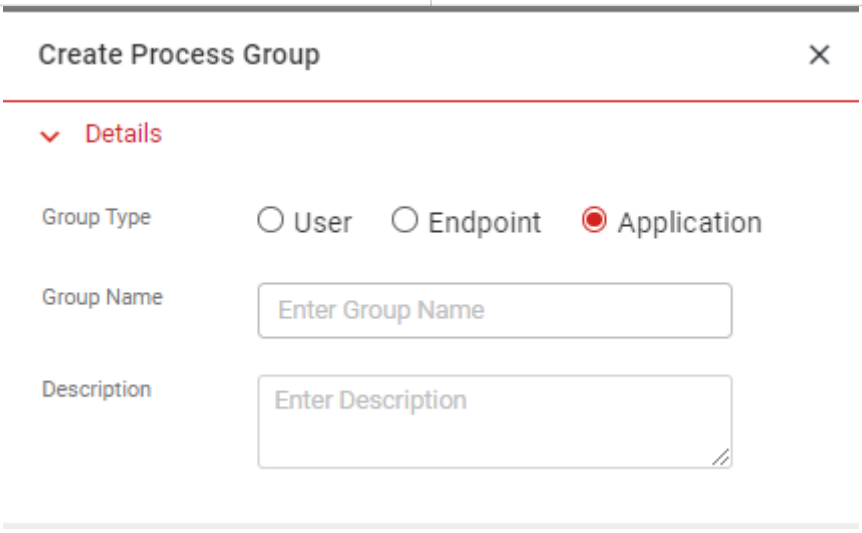
The **Application Group** module allows you to club the different processes under a single group.

This helps you to group a number of processes that you can monitor together as a single instance.

6.3.3.1 Add Application Group

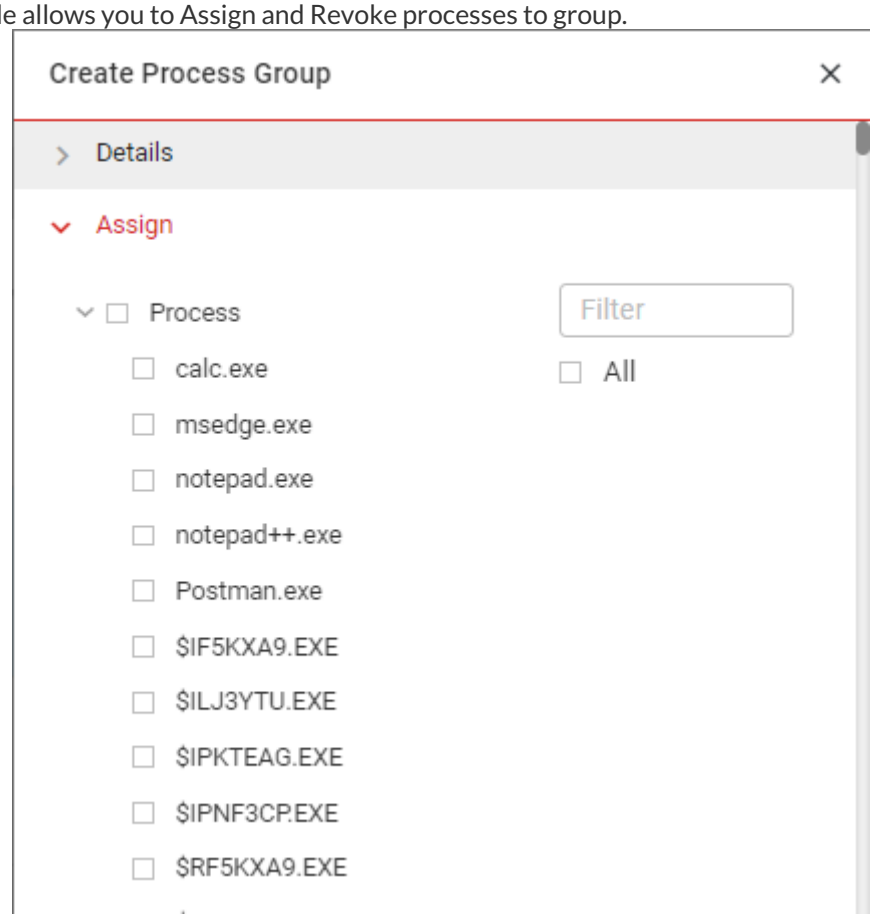
Refer to the following table to understand each of the fields in the Add Process Group tab:

Field	Description
Name	Add the group name in this field
Group Description	Add the group description in this field
Process	Select the Processes from the dropdown
Submit	Click this button to create a Process Group



Assign

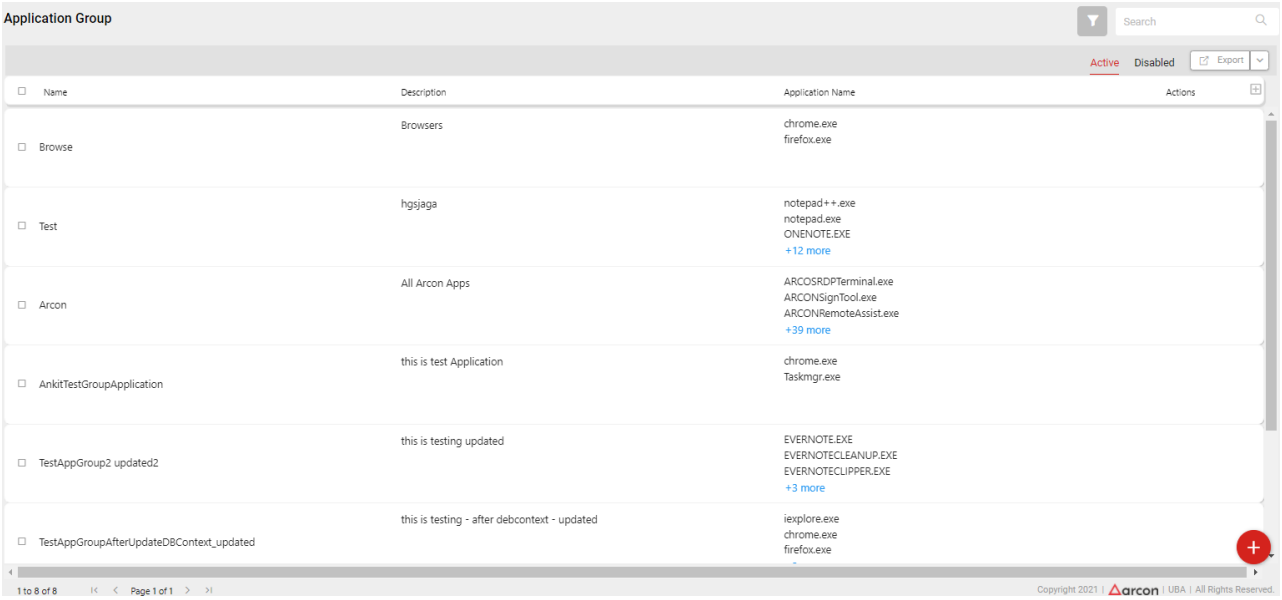
The Assign module allows you to Assign and Revoke processes to group.



6.3.3.2 Application Group

Refer to the following table to understand each of the fields in the Application Group:

Field	Description
Name	This field displays the process group name
Description	This field displays the process group description
Application Name	This field display all the processes assigned to the Process Group
Edit	**Edit:** Click this button to edit the user record **Deactivate:** Click this button to deactivate the user record.



6.4 User Endpoint Role

Field	Description
Host Name	This field displays the hostname for which you want to grant or revoke the admin privileges
UserName	This field displays the username for which you want to grant or revoke the admin privileges
Is Admin	The status of this field could be **Yes** or **No** **Yes:** Denotes that the user is an admin user **No:** Denotes that the user is a non-admin user
Actions	This field allows you to grant or revoke admin-level privileges as follows: **Grant**: Click on this option to grant admin-level privileges to the user. Once done you get an alert "Request Saved Successfully" **Revoke**: Click on this option to revoke admin-level privileges of the user.Once done you get an alert "Request Saved Successfully"

When you click on **Grant** or **Revoke** a popup **Create Admin Request** opens up and has the following fields:

Field	Description
Host Name	This field displays the hostname for which you want to grant or revoke the admin privileges

Field	Description
UserName	This field displays the username for which you want to grant or revoke the admin privileges
Action Type	This field displays the action type
Permanent/Temporary	You can select the options from this dropdown as Permanent or Temporary **Permanent:** If you permanently want to grant or revoke access **Temporary**: If you temporarily want to grant or revoke access

6.5 Central Inventory

The Central Inventory module provides a list of all the applications installed on the end-user machine. ARCON | EPM admin can view this list of applications, recoup unused software and avoid purchasing a new license for the requested software put forward by the end-user using this module. ARCON | EPM admins can also take decisions while granting privileges or restricting access to certain applications using application inventory. Unpatched software or older versions of software can pose a serious security risk for an organization. ARCON | EPM admins can verify that all applications are incorporated and configured with the appropriate tools that will keep software applications up-to-date.

6.5.1 View Inventory

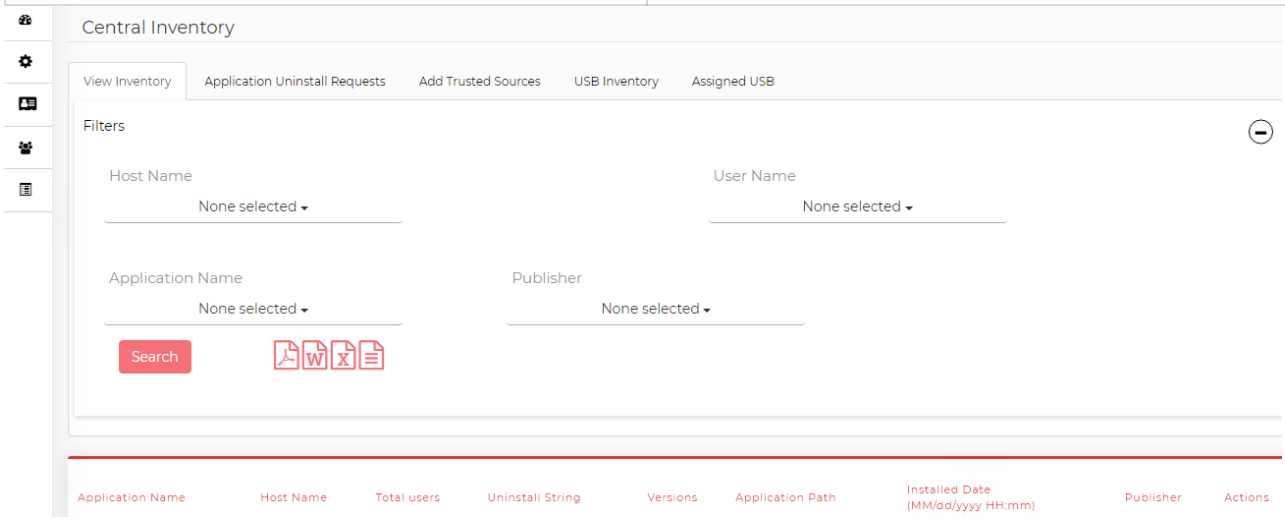
You can use the following search filters to fetch the report data. Select the required details and click on the **Search** button.

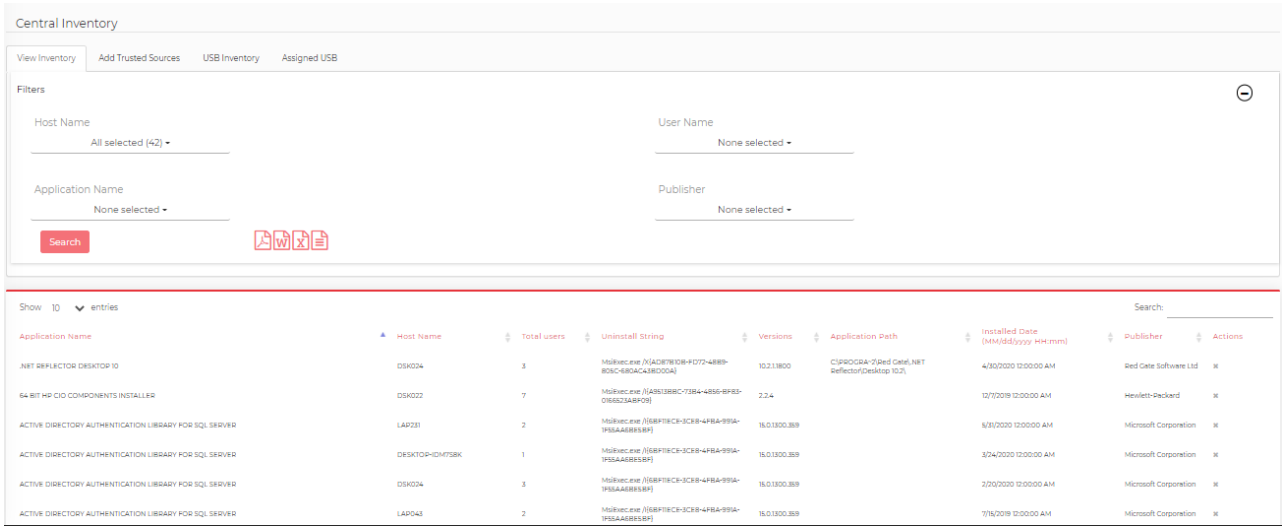
Field	Description
Host Name	Select the hostname for which you want to view the Application details
Application Name	Filter the applications for which you want to view details corresponding to the hostname/end-user
Username	Select the username which which you want to view the details
Publisher	Filter the application Publisher for which you want to view details

The report displays the following data in a tabular format:

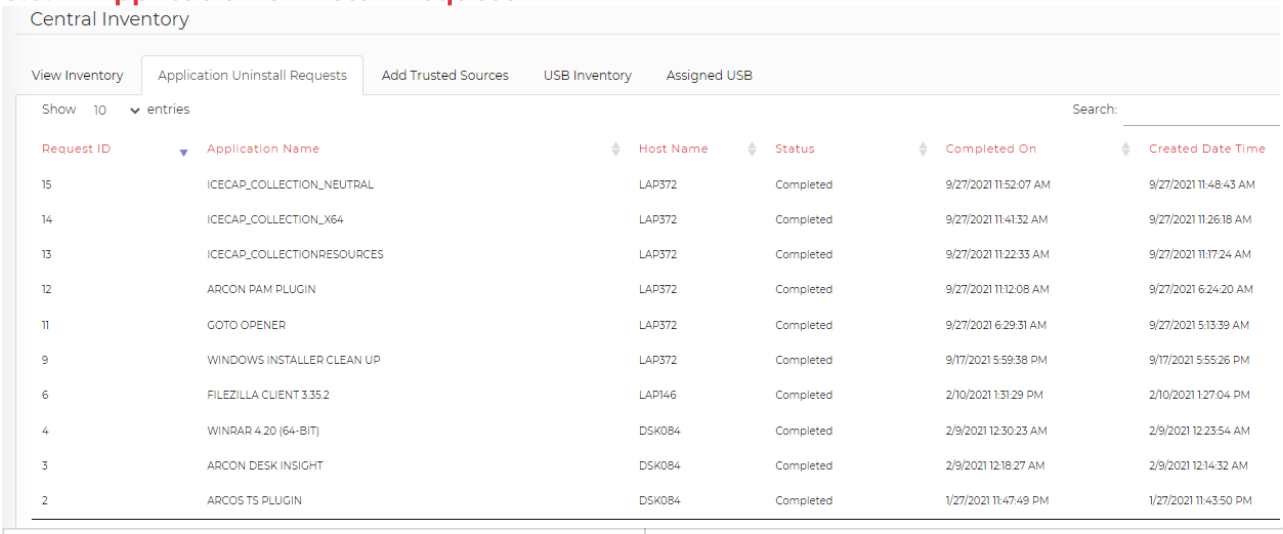
Field	Description
Application Name	This field displays the Application name
Host Name	This field displays the hostname of the end machine
Total Users	This field displays the total number of user having that application installed

Field	Description
Uninstall String	This field displays the registry UninstallString which is used to uninstall/remove software
Versions	This field displays the application version that is installed on their end machines
Application Path	This field displays the path where the application is located (application folder path)
Installed Date (MM/dd/yyyy HH:mm)	This field displays the application install date
Publisher	This field displays the application Publisher name
Actions	The admin can uninstall the application





6.5.2 Application Uninstall Request



Field	Description
Request ID	This field displays request ID number
Application Name	This field displays the Application name
Host Name	This field displays the hostname of the end machine
Status	This field displays the status of users applications uninstalled
Completed On	This field displays the completed uninstallation date and time
Created Date Time	This field displays the date and time of application created to uninstall

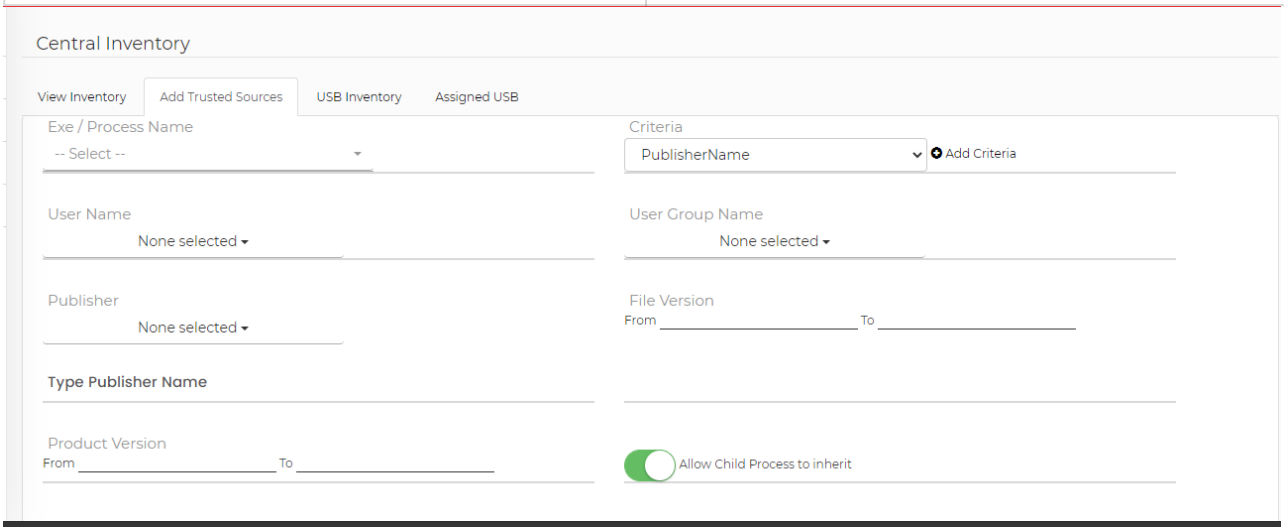
6.5.3 Add Trusted Source

The applications can be added to trusted sources based on Product Name, Publisher Name, File Version, and Product Version.

It prevents the privilege elevation of sub-processes (child processes) with the help of "Trusted Source" applications for the administrator. If the Admin wants to trust a process and automatically elevate a Windows application for eg. command prompt running with a privileged elevation of the Administrator account but doesn't want to elevate other subprocesses that are automatically triggered by command prompt then the Admin can simply use a toggle on to block subprocess elevation. Allow creation of an intuitive trusted source application inventory to avoid too many elevation requests to be generated after a central software upgrade.

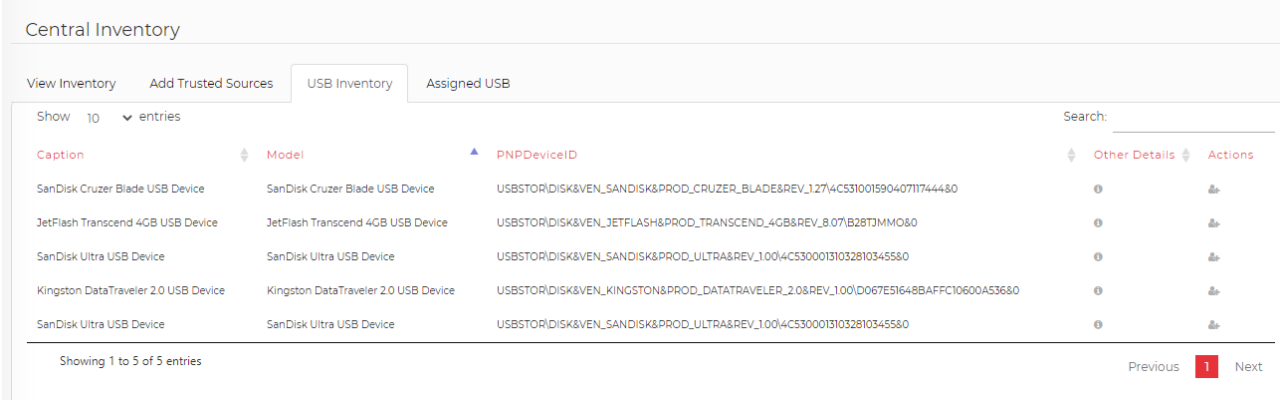
Fields	Description
Process Name	Process selected to be added to trusted source
Criteria	Criteria to be selected as Publisher Name, Product Name, File Version and Product Version
Username	User to be selected for the policy

Fields	Description
User group name	User groups can be selected
Product Name	Product name to be defined to add as trusted source
Publisher Name	Publisher name to be selected to add as trusted source
File Version	File Versions can defined to be added as trusted source
Product version	Product versions can be defined
Allow child process to inherit	This toggle button will enable or diasable the policy for child process



6.5.4 USB Inventory

Maintains a USB inventory for managing all USB sticks that were plugged into various endpoints in the organization all in one place for ease of access.



6.6 Schedule Report

Administrators can automate the generation and distribution of the reports to the relevant end-users via email at regular intervals.

The module allows you to specify when the report will be sent, who to send it to, and the report format to use. You can specify which reports you want to include, which columns in the report should be included; specify the list of recipients, specify at what times or intervals you want to send the reports (daily, weekly, or monthly basis, quarterly, yearly). The report could be sent as a Word, PDF, CSV, or Excel attachment.

6.6.1 Add Scheduler

Refer to the following table to understand the fields in the Add Scheduler tab:

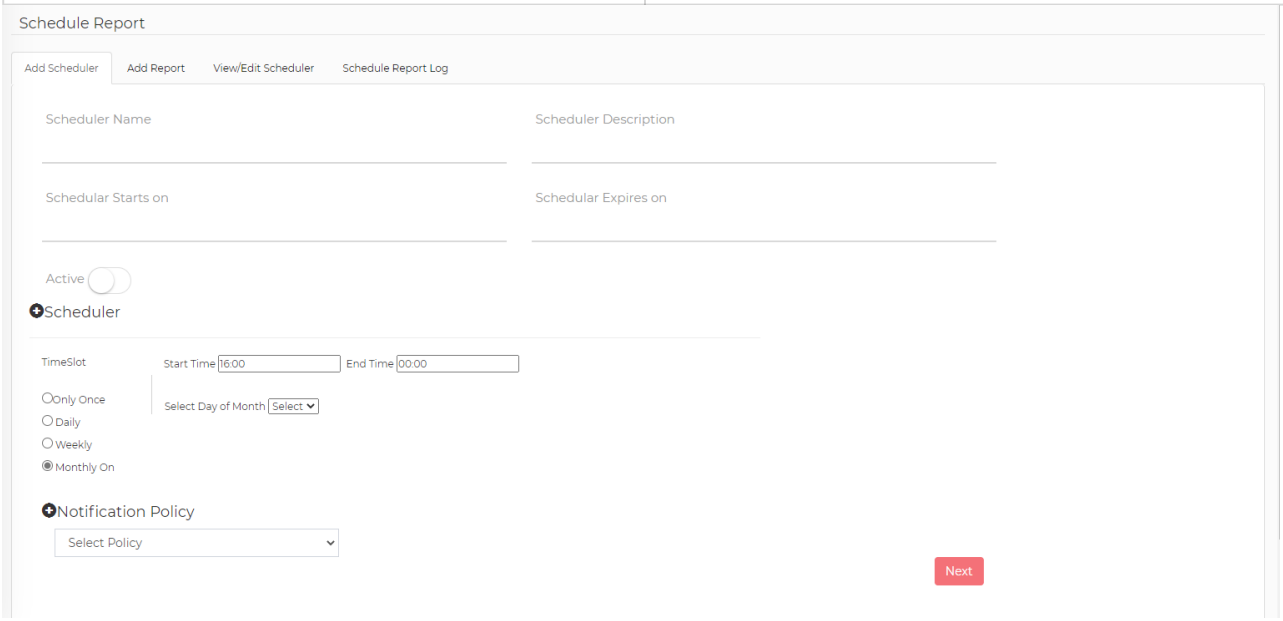
Field	Description
Scheduler Name	Specify the scheduler name in this field
Scheduler Description	Specify the scheduler description in this field
Schedular Starts on	Specify the scheduler start date in this field
Schedular Expires on	Specify the scheduler expiry date in this field
Active	Enable this button to set the status of the scheduler as Active

6.6.2 Scheduler

Refer to the following table to understand the fields in the Scheduler tab:

Field	Description
TimeSlot	Specify the Report frequency and the date range in this section Specify the time interval/ date range (**Start Time, End Time**) for which you want to send the report
Only Once	Click this radio button to schedule the report only once for a particular duration of time. Enter the **Start Time** and click on **Apply** to select the start time, Enter the **End Time** and click on Apply to select the end time
Daily	Click this radio button to schedule the report daily for a particular duration of time. Enter the **Start Time** and click on **Apply** to select the start time, Enter the **End Time** and click on Apply to select the end time
Weekly	Click this radio button to schedule the report on a particular day of the week for a particular duration of time. Enter the **Start Time** and click on **Apply** to select the start time, Enter the **End Time** and click on Apply to select the end time When you click this button, all the weekdays gets displays, check the relevant checkbox and select the relevant day of the week for which you want to schedule the report

Field	Description
Monthly	Click this radio button to schedule the report on a monthly basis for a particular duration of time. Enter the **Start Time** and click on **Apply** to select the start time, Enter the **End Time** and click on Apply to select the end time
Quarterly	Click this radio button to schedule the report on a quarterly basis for a particular duration of time. Enter the **Start Time** and click on **Apply** to select the start time, Enter the **End Time** and click on Apply to select the end time
Yearly	Click this radio button to schedule the report on a yearly basis for a particular duration of time. Enter the **Start Time** and click on **Apply** to select the start time, Enter the **End Time** and click on Apply to select the end time
Notification Policy	Select the Notification Policy to notify a user or group of users when the report is generated
Next	Click on the Next button to go to the **Add Report** tab

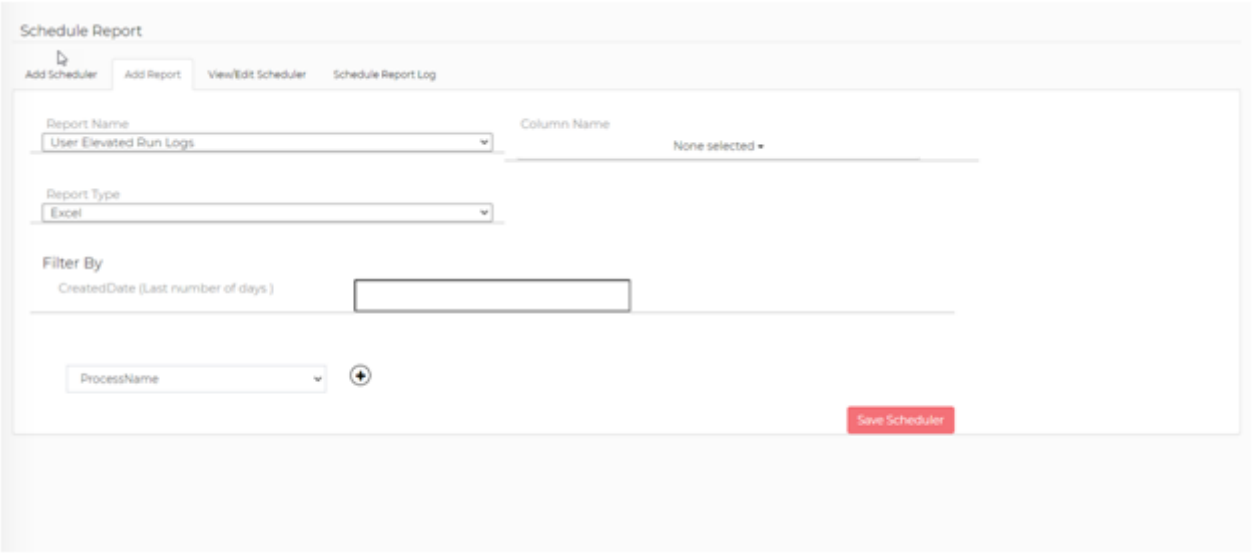


6.6.3 Add Report

Refer to the following table to understand the fields in the Add Report tab:

Field	Description
Report Name	Select a report from the Available Reports in the dropdown

Field	Description
Column Name	Select the report columns corresponding to the report selected under the **Report Name** dropdown
Report Type	The report could be sent as a Word, PDF, CSV, or an Excel attachment
Save Scheduler	Click to save the scheduler

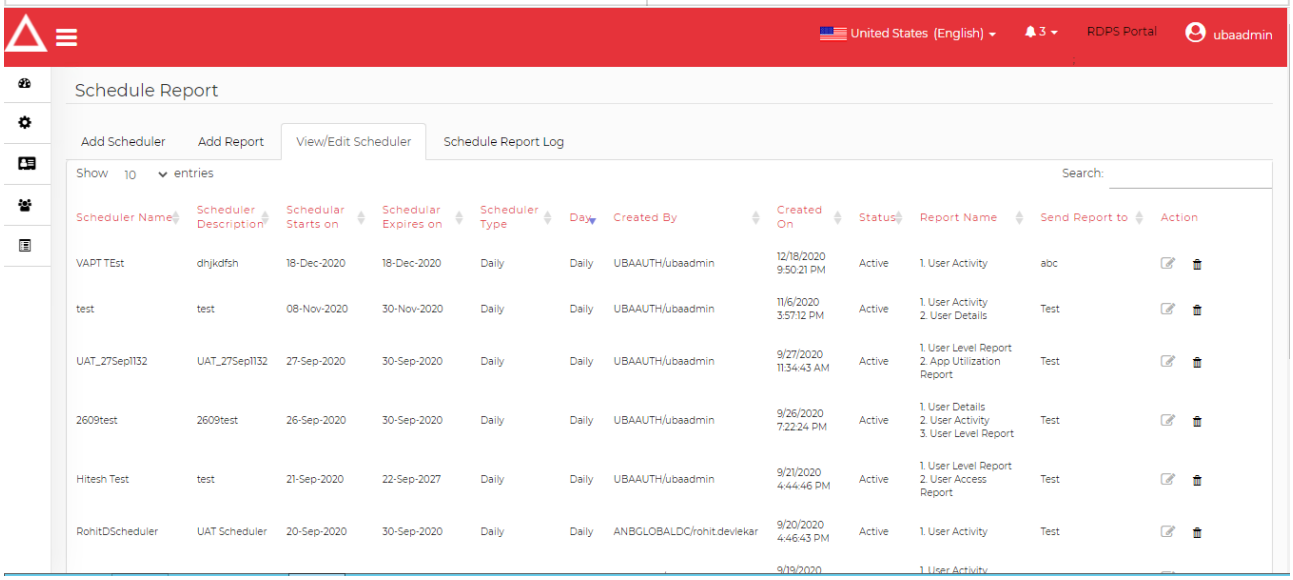


6.6.4 View/Edit Scheduler

Refer to the following table to understand the fields in the View/Edit Scheduler tab:

Field	Description
Scheduler Name	This field displays the scheduler name
Scheduler Description	This field displays the scheduler description
Scheduler Starts on	This field displays the scheduler start date
Scheduler Expires on	This field displays the scheduler expiry date
Scheduler Type	This field displays the report frequency (**Only Once, Daily, Weekly, Monthly, Quarterly, Yearly**)
Day	This field shows the intended time range in the following frequencies: • Daily • Weekly • Monthly
Created By	This field displays the name of the User for whom the report is generated

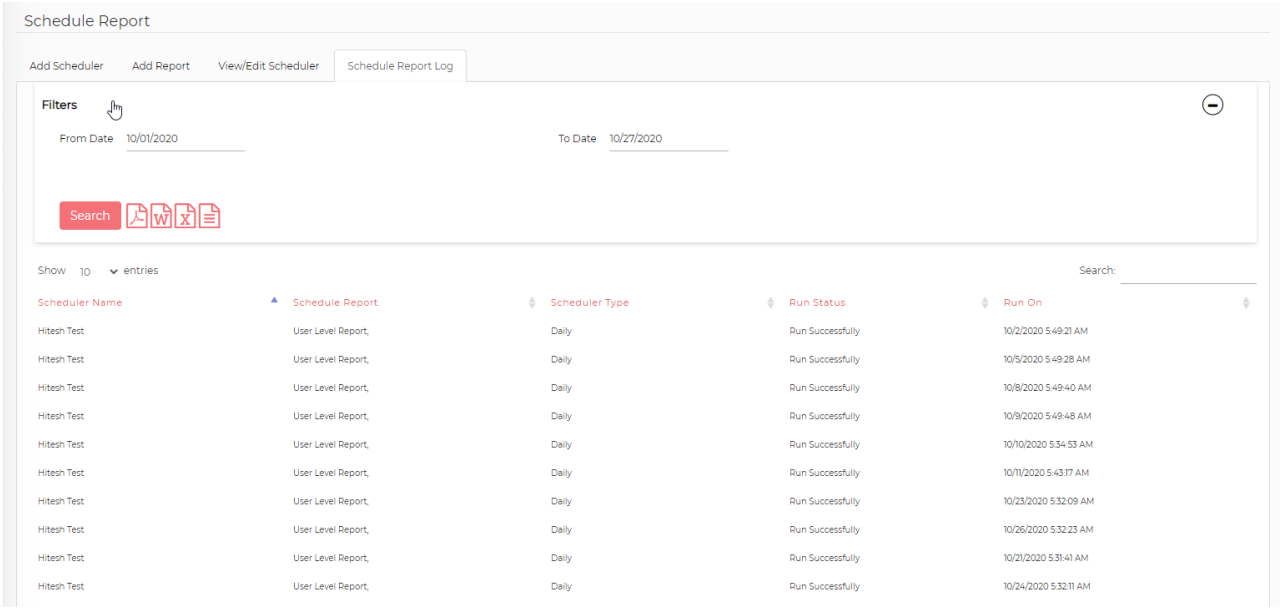
Field	Description
Created On	This field displays the date when the scheduler was created
Status	This field displays the scheduler status
Report Name	This field displays the report name
Send Report to	This field displays the recipient details
Action	:Edit2: Click on this icon to edit the details :1: Click on this icon to delete the details



6.7 Schedule Report Log

6.7.1 Filter

You can filter report data by applying the following filters/search criteria. Select the required details and click **Search**.



Refer to the following table to understand each of the fields in the Filters screen:

Field	Description
From Date	Select the From Date for which you want to fetch the report Click the calendar icon to select the From Date
To Date	Select the To Date for which you want to fetch the report Click the calendar icon to select the To Date

Refer to the following table to understand each of the fields in the Schedule Report Log:

Field	Description
Scheduler Name	This field displays the scheduler name.
Schedule Report	This field displays the name of the scheduled report
Scheduler Type	This field displays the scheduler type
Run Status	This field displays the scheduler run status. If the report was successfully scheduled/delivered the status will be displayed as "Run Successfully"
Run On	This field displays the date and time when the scheduler was successfully executed

6.8 Workflow

Workflow is an approval process where one or more Admins will approve the changes that have been made. The transactions between users, and user groups can undergo approval before any action is done.

6.8.1 Creating Workflow

1. To add a Workflow, go to **Manage** → **Workflows**. The below page is displayed:

Refer to the following table to understand each of the fields in the WorkFlow tab:

Field	Description
WorkFlow Name	Name for the Workflow
Valid Upto	Date till which the workflow will be active for
Approvers Level	Number of Approvers for the Workflow. A maximum of 10 approvers can be assigned. We have selected 2 in the above example
Approvers	Search and select the approvers for the workflow

2. Enable the **Active** slider button to activate the Workflow.

3. Click on **Submit**, to create the Workflow.

6.8.2 Viewing All Workflows

To view All Workflows, go to **Manage** → **Workflow** and select the **All Workflows** tab. The screen below is displayed.

Refer to the following table to understand each of the fields in the All WorkFlow tab:

Field	Description
WorkFlow Name	Name for the Workflow
Active	Whether the Workflow is active or not. For Active the value is true and for inactive it will false
Approvers Level	Number of Approvers for the Workflow. A maximum of 10 approvers can be assigned. We have selected 2 in the above example
Valid Upto	Date until which the workflow is active
Action	Admin users can edit or delete the workflow through the Action column

Workflows can also be searched from the **Search** field.

6.9 Assign Workflow

On creating a workflow, admin users can assign them to a Group or a specific user.

To assign a workflow, go to **Manage** → **Assign WorkFlow**. The screen below is displayed:

Refer to the following table to understand each of the fields in the Assign WorkFlow tab:

Field	Description
Group / User	Select to whom the workflow needs to be assigned to In case of Group, select the group name or click on the View List button, to view all the group that are available In case of User, select the name of the user
Workflow	Name of the available workflows that need to assigned
Assigned For	Workflow can be assigned for Elevation, Facial Recognition or both

6.9.1 Viewing Assigned Workflows

To view Assigned Workflows, go to **Manage** → **Assign WorkFlow** and select the **Assigned WorkFlow** tab. The screen below is displayed.

Refer to the following table to understand each of the fields in the Assigned WorkFlow tab:

Field	Description
Assigned To	Name of the Group or Person to whom the Workflow has been assikgned
UserName	Name of the user to whom the Workflow has been assigned
WorkFlow	Name of the Workflow
Assigned For	Reason why the workflow has been assigned for: Elevation, Facial Recognition or both
Action	Admin users can edit or delete the workflow through the Action column

7 Settings

The **Settings** menu helps in configuring the required settings for EPM that can be used to generate different types of reports or logs for user analysis. Before setting up the EPM, organizations need to take decisions that can help them to embed user analytics for their systems, which can be technical or strategic decisions based on the requirements and can further be optimized for user analysis.

EPM Settings allows to perform the below tasks through the settings menu:

1. Add Applications
2. Notification Policy
3. Domain Integration
4. SMTP Configuration
5. SMS Gateway Configuration
6. Configure Version
7. General Configurations
8. Group Setting

7.1 Notification Policy

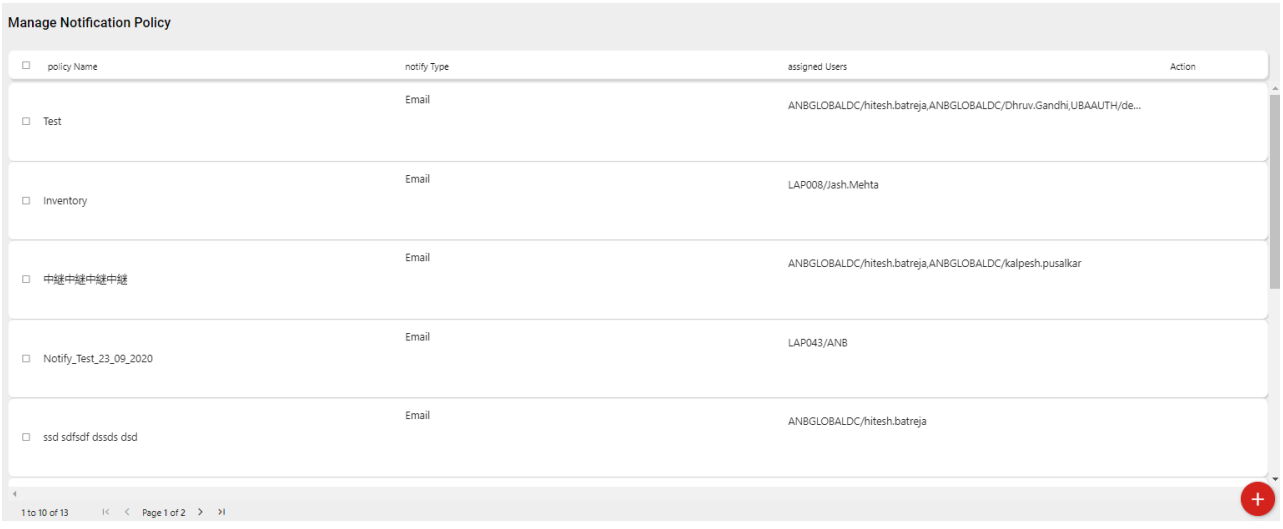
The Notification Policy menu allows administrators to define email notifications. A user can receive these notifications when there is a violation of rules identified by the system. It is based on the user behavior or if there is a deviation from the normal behavioral characteristics of the user.

These policies are simple rules that are defined by an organization and assigned to users who are accessing the system and are alerted or prompted through Email notifications when a threat is identified.

Administrators can create new notification policies or edit the existing ones through the Notification Policy menu.

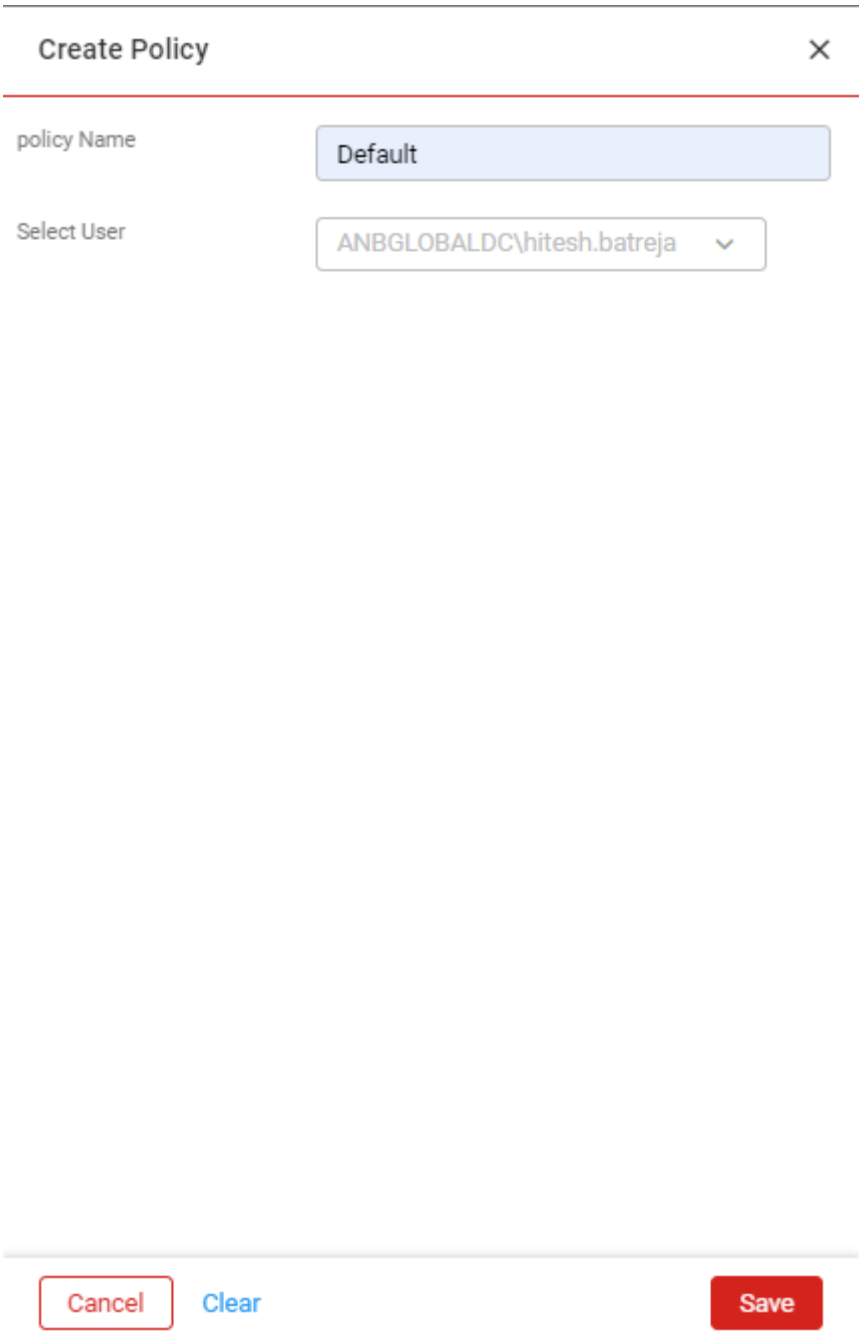
To add a Notification Policy, perform the following steps:

1. Login to EPM and click on the **Settings** icon from the left pane.
2. Select **Notification Policy** as an option. The **Manage Notification Policy** screen is displayed as shown below.



7.1.1 Add Notification Policy (Email)

To Add Notification Policy, specify the required details in the fields as shown in the screen below and then click on the **Save**button.



Field	Description
Policy Name	Enter a name for the policy
Select User	Select a user from the list to assign the new notification policy. Users once assigned will start getting a notification through Email

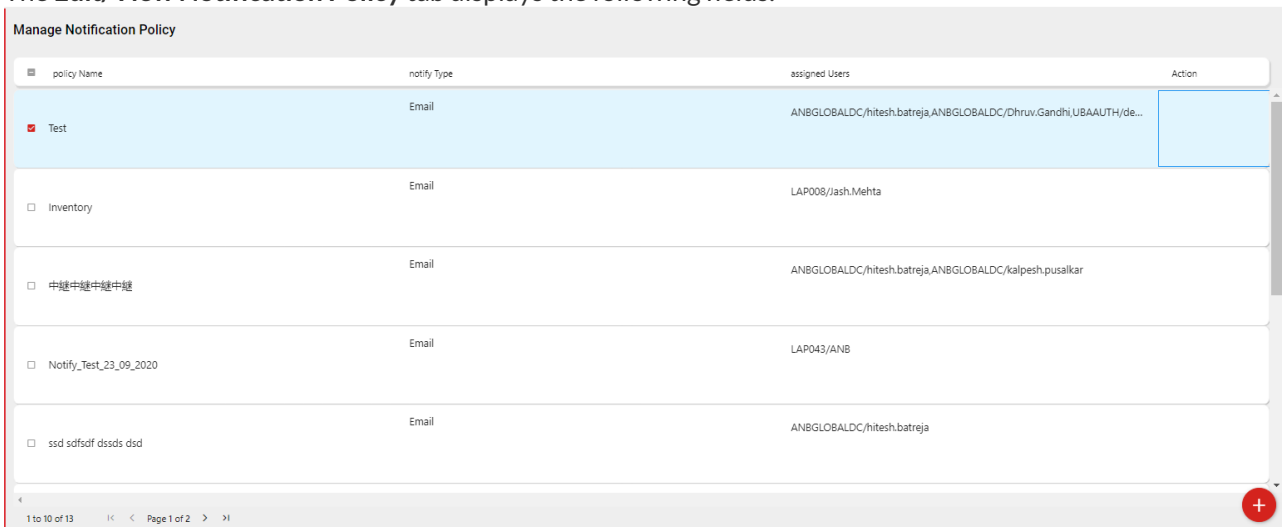
You will now get a message "**Notification Saved Successfully**".

7.1.2 Edit / View Notification Policy

You can edit or view an existing notification policy from the **Notification Policy → Edit Notification Policy**.

The screen below shows the **Edit Notification Policy** window.

The **Edit/View Notification Policy** tab displays the following fields:



Field	Description
Notification Policy Name	This field displays the name of the policy
Notify Type	This field defines the channels through which Notifications are sent e.g. email
Users	This field displays the users to whom and how often notification emails will be sent in the event of any violation of rules or deviation from the normal behavioral baseline
action	Click on the Edit icon to edit an existing notification ***Edit Notification Policy*** **Policy Name:** You can edit the policy name from this field **Select User**: You can edit the users from this field **Submit**: Click to save the changes **Close**: Click to close the edit notification policy window

1. Click on the Edit icon to edit an existing notification.
2. In the pop-up screen that appears, which is as shown below, you can edit the Policy Name and add or remove users by selecting them.
3. Click on the Submit button to make the changes or you can deny the changes by clicking on the Close button.

7.2 Domain Integration

Domain integration is necessary for authentication and authorization of all users and systems in a Windows domain type.

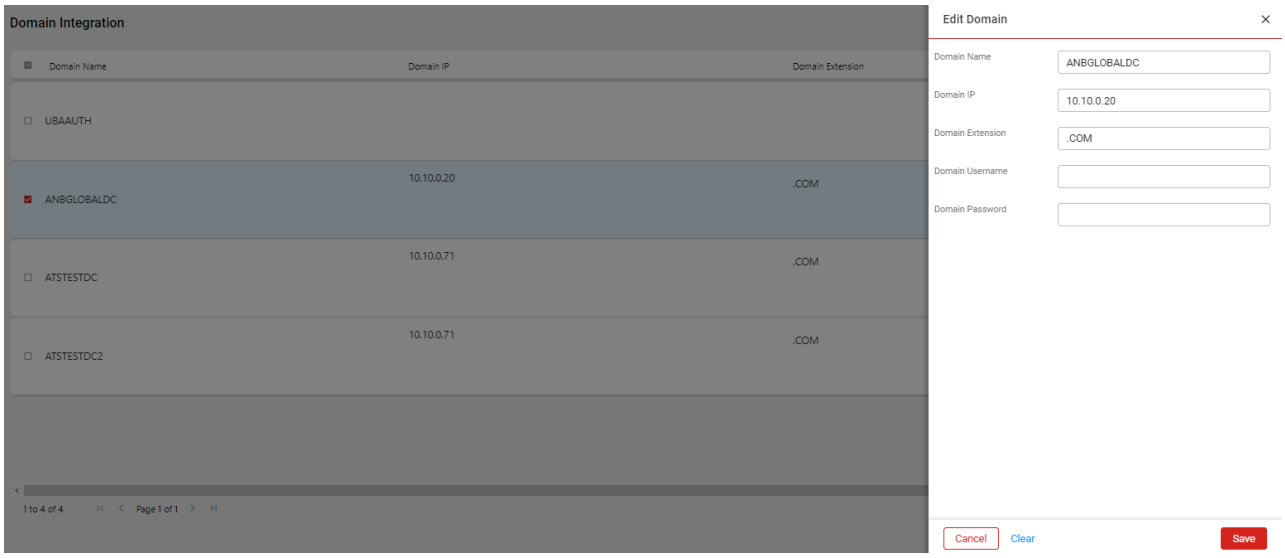
To configure a domain:

1. Login to EPM and click on the :Settings_icon: icon from the left pane.
2. Select **Domain Integration** as an option. The **Create Domain** window is displayed as shown below.

3. Add the required domain details as shown in the above screen and click on the **Create** button. The new domain is now configured.

Field	Description
Domain Name	Specify the Organization domain name in this field
Domain IP	Specify the Organization domain IP in this field
Domain Extension	Specify the domain extension in this field
Domain Username	Specify the domain username in this field
Domain Password	Specify the domain password in this field

You can edit an existing domain by clicking on Modify button. The screen below shows the **Edit Domain** window.



7.2.1 Edit/View Domain

You can edit or view an existing domain from the **Domain Integration** → **Edit/View Domain** tab. The screen below shows the **Edit/View Domain** tab.

The **Edit/View Domain** tab displays the following fields:

Field	Description
Domain Name	This field displays the Organization domain name
Domain IP	This field displays the Organization domain IP
Domain Extension	This field displays the domain extension
Sync icon	Click on the Sync icon button to synchronize user accounts, group, and credential hashes from an on-premises **AD** DS environment to the Cloud
Edit	Click on the :Edit_icon: icon button to edit an existing domain

7.3 Configure Version

Version module can be used to update agents automatically on the end machines for a **Full release** or **Test Release**.

The version module has the following tabs:

- **New Version**
- **Test Release**

7.3.1 New Version

You can use this module to update the new version of the agent on the end machine. You can upload the new package and set the rolling date.

The new version has the following sections:

- File Version
- Versions List

File Version

Refer to the following table to understand the fields on the File Version section:

Field	Description
File Upload	Click on the **Choose File** button and select the relevant package version from your machine you want to deploy on the end machine The Version Name should be of type N.N.N.N. Where N should be Number
Version Description	Add the version description in this field
Rolling Date	Select the date for the package deployment
OS (Leave Blank if its OS Independent)	Select the OS version relevant to the package from the following options: • **MacOS** • **Windows** • **Linux** • **Ubuntu**
32/64 Bit	Select the OS architecture from the following options 32 Bit/64 Bit
Upload	Click this button to upload the details

Versions List

The details that you submit in the **File Version** section are displayed here.

Field	Description
File Version	This field displays the package version
Version Description	This field displays the version description
Package Path	This field displays the path from where the package was uploaded
Rolling Date	This field displays the date of the package deployment
Created Date Time	This field displays the date when the package was uploaded
OS	This field displays the OS version for which the package is deployed
32/64 Bit	This field displays the OS architecture for which the package is deployed
Actions	Click this :1: icon to delete the record

7.3.2 Test Release

The Test Release section gives you the option to automatically update the agent on the end machine for testing purposes.

Refer to the following table to understand the fields on the Test Release section:

Field	Description
Select Version	You can select the relevant version in the Select Version field. The version is selected to update the agent on the end machine for testing purpose This dropdown displays all the package that was uploaded in the New Version section/ tab
Test Release Description	Add a description for the test release
Rolling Date	Select the deployment date for the test release
Selection of Users	There are two methods by which you can deploy the package to the end-users. You can either choose the specific end users for which you want to deploy the package or allow the application to automatically choose the end-users • To manually update the agents on the end machines, click on the **Manual** radio button, a dropdown appears which displays all the end-users. Select the users for which you want to update the agents on the end machines • To automatically update the agents on the end machines, click on the **Automatic** radio button
Submit	Click on this button to submit the details

Refer to the following table to understand the data displayed in each column:

Field	Description
Test Version ID	This field displays the test version id (agent package)
Test Release Description	This field displays the test release description
Assigned Users	This field displays the number of users for which the test release package is assigned. Click on this link to add more users to the test release
Test Rolling Date	This field displays the date on which the test release will be deployed on the end machines
Created Date Time	This field displays the date when the details were submitted
Actions	Click this :1: icon to delete the record for the Test Release

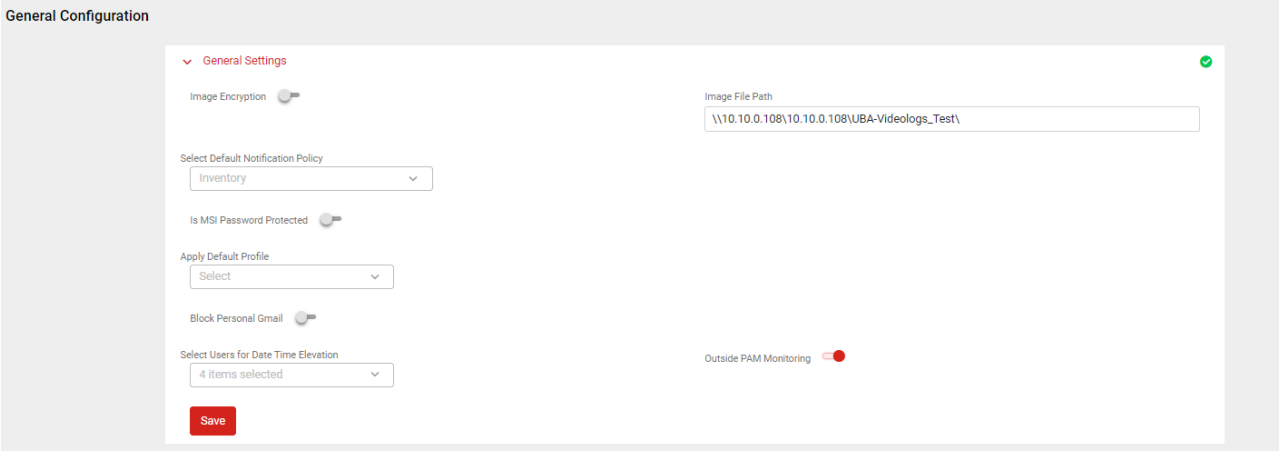
7.4 General Configurations

General Configuration is used for multiple settings of file paths and their activity, which is a technical decision based on the requirements and can be further monitored by the Admin.

7.4.1 General

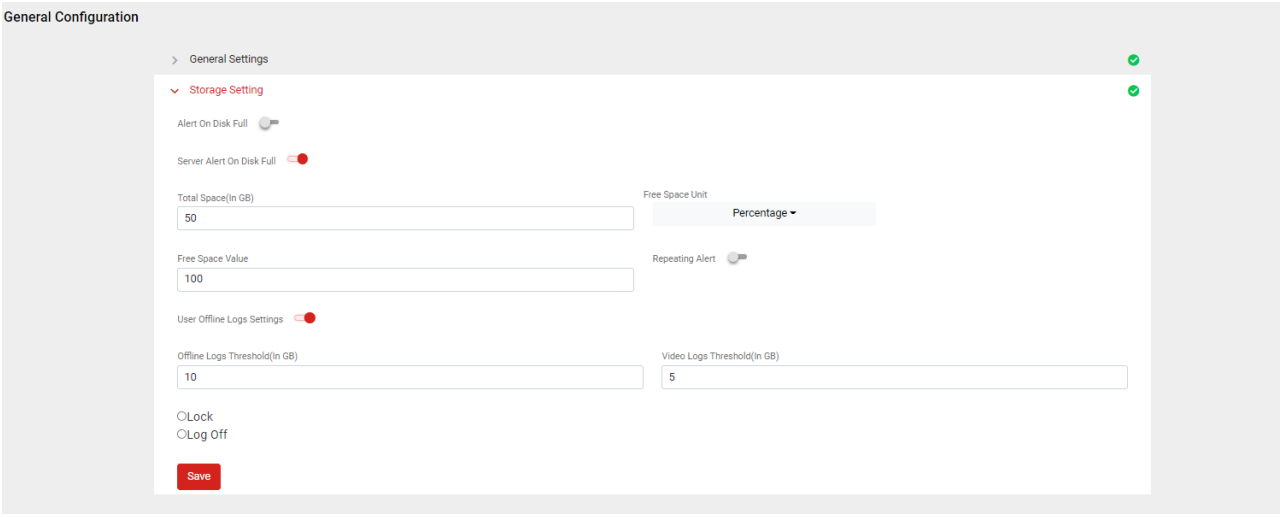
Refer to the following table to understand the fields in the General tab:

Field	Description
Image Encryption	Images captured for video logs to be encrypted
Image File Path	Path to save the images
Select Default Notification Policy	Global Notification Policy for getting emails



7.4.2 Storage Setting

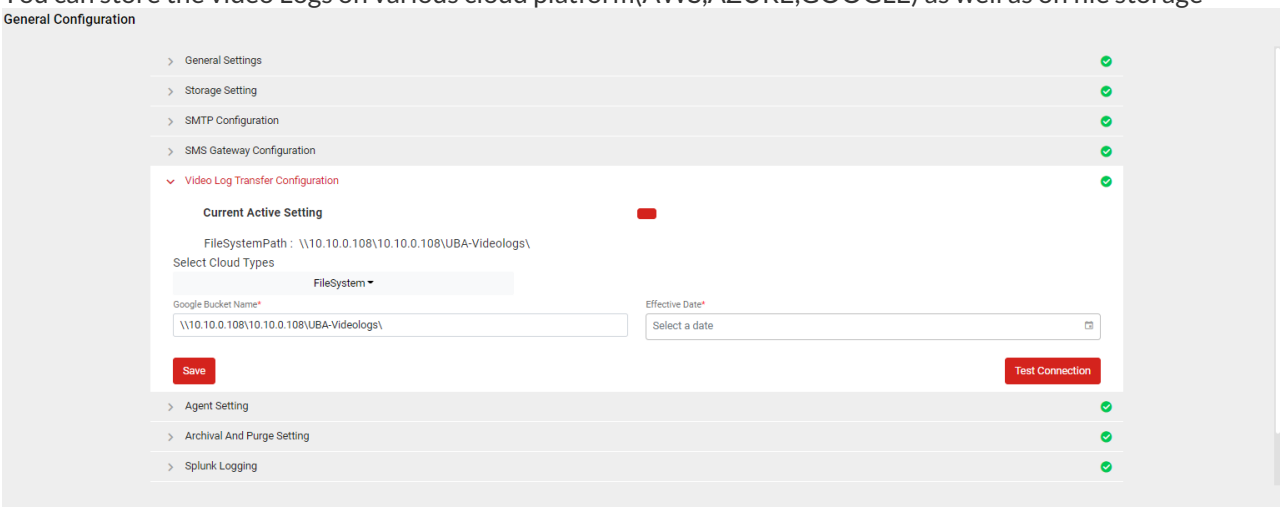
You can specify various storage related setting in the Storage setting tab as shown in the screenshots below.



7.4.3 Video Log Transfer Configuration

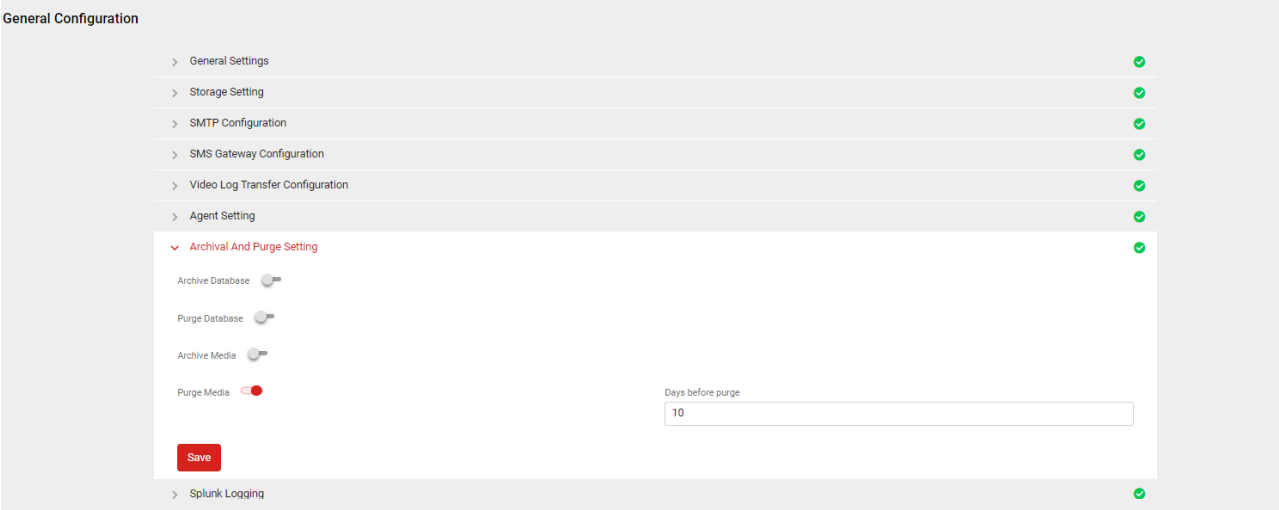
You can specify where you want to keep the Video Log as shown in the screenshots below.

You can store the video Logs on various cloud platform(AWS,AZURE,GOOGLE) as well as on file storage



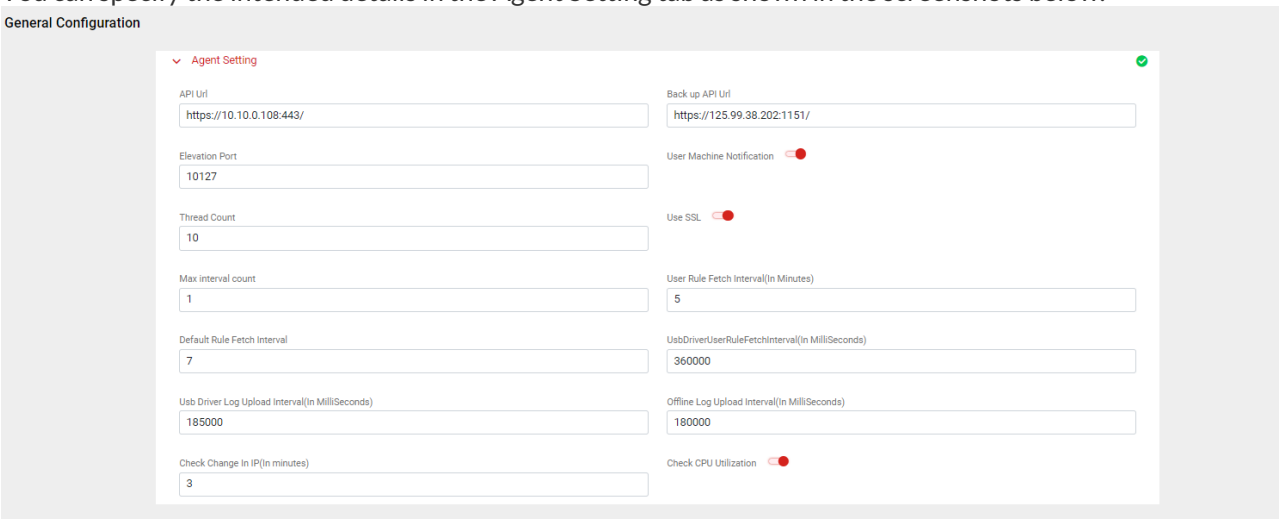
7.4.4 Archival and Purge Setting

You can specify the archiving and purging details of database and media tab as shown in the screenshots below.



7.4.5 Agent Setting

You can specify the intended details in the Agent Setting tab as shown in the screenshots below.



Refer to the following table to understand the fields on the Agent Setting tab:

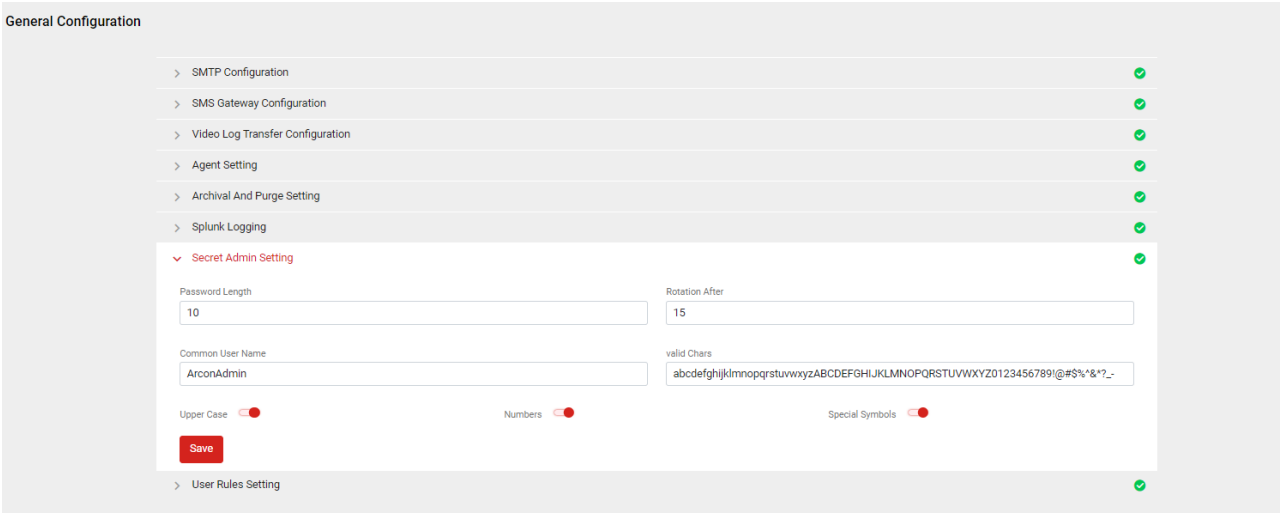
Field	Description
API Url	Specify the URL of application hosted
Back up API Url	Specify the Public IP of the application hosted
Elevation Port	Specify the Elevation Port
User Machine Notification	Toggle button to receive machine notification on the endpoints
Thread Count	Specify the thread count for the endpoints

Field	Description
Use SSL	Toggle button to enable or disable the SSL
Max interval count	Specify the maximum interval count for the endpoints
User Rule Fetch Interval(In Minutes)	Specify the interval in minutes for the endpoints to fetch the rules
Default Rule Fetch Interval	Specify the default rule fetch time for the endpoints to fetch the rules
UsbDriverUserRuleFetchInterval(In MilliSeconds)	Specify the USB rule fetch time for the endpoints to fetch the rules for USB restrictions
Usb Driver Log Upload Interval(In MilliSeconds)	Specify the USB log upload time for the endpoints to upload the logs on the application
Offline Log Upload Interval(In MilliSeconds)	Specify the offline log upload time to upload the logs saved locally on the endpoints
Check Change In IP(In minutes)	Specify the time for the agent to check the change in the IP address
Check CPU Utilization	Enable the toggle to check the CPU utilization from the endpoint
Check RAM Utilization	Enable the toggle to check the RAM utilization from the endpoint
Check Disk Utilization	Enable the toggle to check the Disk utilization from the endpoint
Check Network Utilization	Enable the toggle to check the Network utilization from the endpoint
Check Packet Utilization	Enable the toggle to check the packet utilization from the endpoint
Spawn Threads when locked	Enable the toggle to check the spwan threads when locked from the endpoint
Frequency Settings SleepTime	Specify the Sleep time frequency of the endpoint
Frequency Settings CPU Threshold	Specify the CPU threshold frequency for the endpoints
Frequency Settings RAM Threshold	Specify the RAM threshold frequency for the endpoint
Frequency Settings Sys MonitorConfig Frequency	Specify the system monitor frequency to check the performance of the system
Frequency Settings CPU Num	Specify the CPU frequency
Frequency Settings RAM Num	Specify the RAM frequency

Field	Description
FrequencySettings Data Interval	Specify the data interval frequency
Facial Recognition(FR) frequency in mins	Specify the frequency for the images to be captured for the Facial Recognition
FR Invalid attempts allowed	Specify the number of invalid attempts allowed for facial recognition failures
FR MaxOffline Usage	Specify the maximum offline usage time for facial recognition
Allow Multiple User's Presence during FR	Enable the toggle that records the multiple users presence during facial recognition when locked from the endpoint
Facial Recognition Liveness	TBD
Facial Object Detection	Enable the toggle that records the end-users performance every 2 seconds or as per the scheduler time settings

7.4.6 Secret Admin Settings

Field	Description
Password Length	Enter the length of the password to be created, eg: 8 or 15 characters
Rotation After	Enter the number of days after the password rotation must be done
Common User Name	Enter the common user name, eg: ArconAdmin
Upper Case	Enable the toggle for upper case compulsion in the password settings
Numbers	Enable the toggle for numbers compulsion in the password settings
Special Symbol	Enable the toggle for special symbol compulsion in the password settings

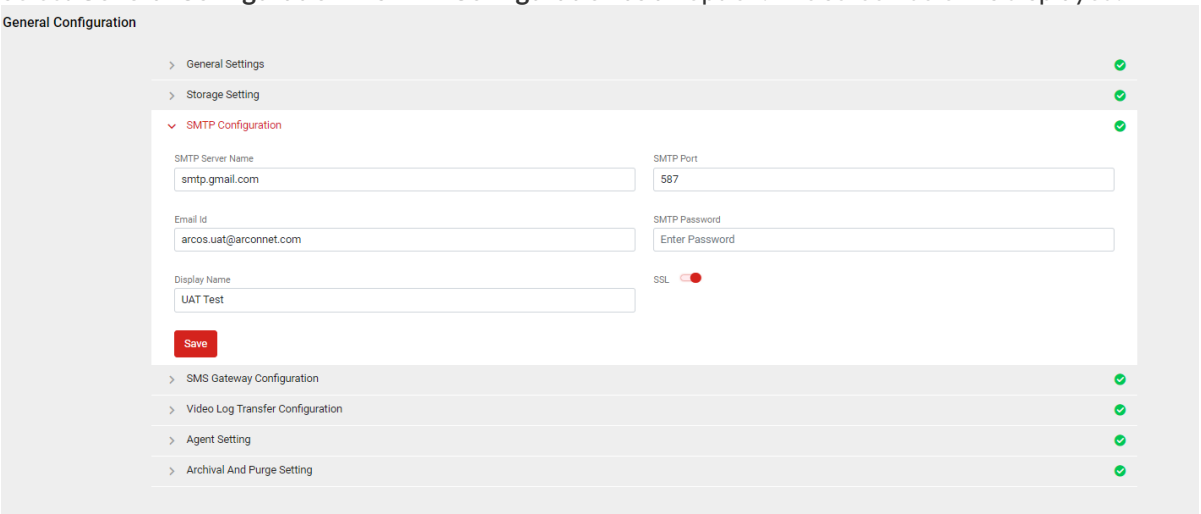


7.4.7 SMTP Configuration

To support the EPM Email notifications, administrators need to configure the SMTP settings.

You can configure the SMTP settings by following these steps:

1. Login to EPM and click on the :Settings_icon: icon from the left pane.
2. Select **General Configuration ->SMTP Configuration** as an option. The screen below is displayed.



3. Enter all the required SMTP details as shown in the screen above and click on the **Save** button. The SMTP service is now configured.

Field	Description
SMTP Server Name	Specify the SMTP Server Name in this field
SMTP Port	Specify the SMTP Port in this field
Email Id	Specify the email in this field
SMTP Password	Specify the SMTP password in this field
Display Name	Specify the display name in this field

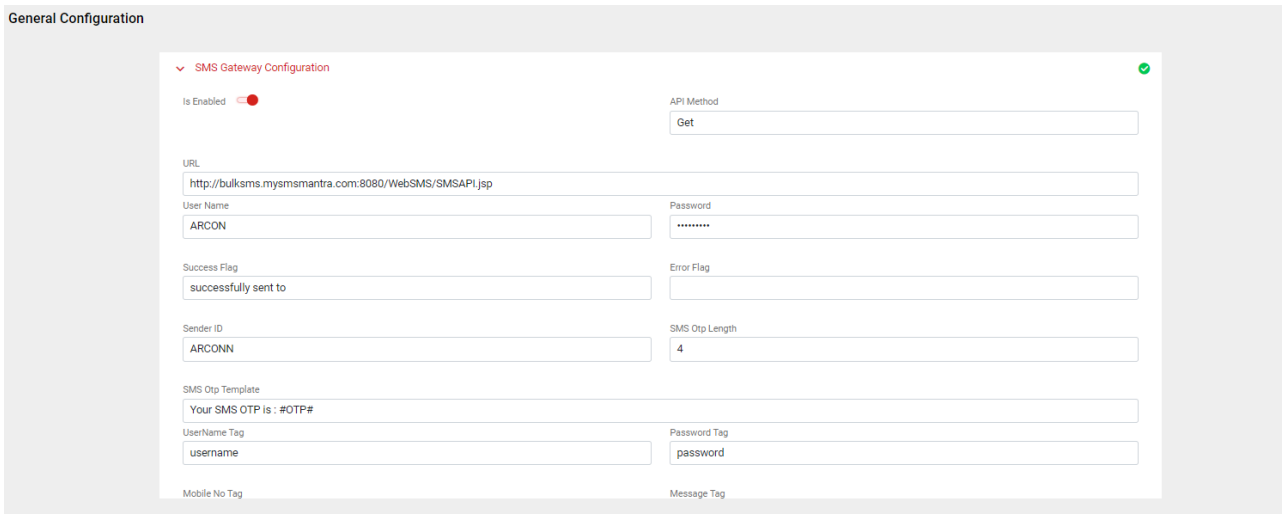
Field	Description
SSL	Slider button to Enable SSL

7.4.8 SMS Gateway Configuration

SMS notifications can be enabled for EPM by configuring the SMS Gateway settings.

To configure the SMS Gateway, perform the following steps:

1. Login to EPM and click on the :Settings_icon: icon from the left pane.
2. Select **General Configuration ->SMS Gateway Configuration** as an option. The screen below is displayed.



8 Reports

The Report module is configured to deliver multiple or the complete activities of the end-user to the Admin.

8.1 User Reports

8.1.1 User Activity

The user activity report (for process monitoring) delivers a searchable summary of all user actions. This enables administrators to read all user activities on the endpoint.

Determine the length of time a particular user worked on programs, processes applications, or tasks during a particular period of time.

> Log tab under the Create Profile module allows you to configure process monitoring rules. You can configure these rules for single or multiple processes.

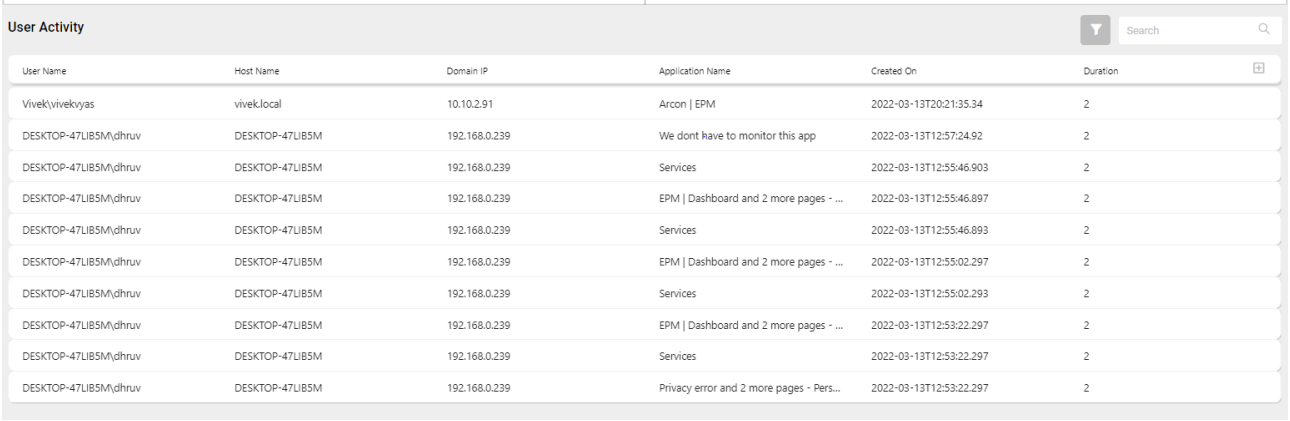
You can configure these rules for different processes such as browsing activities, email, file access, application access, instant messaging, and more by setting up this rule to detect/ monitor a
a single process, or multiple processes.

The text logs/reports can be exported and downloaded in PDF, Word, Excel, and CSV.

Filter

Refer to the following table and filter report data by applying the filters/search criteria:

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
User Name	Select single or multiple users from the drop-down to fetch the report
Hostname	Select single or multiple hosts from the drop-down to fetch the report



Refer to the following table to understand the data displayed on the report:

Field	Description
User Name	This field displays the username for which the report is fetched
Host Name	This field displays the hostname for which the report is fetched
Process Name	This field displays process names captured during the process monitoring
Application Name	This field displays application names captured during the process monitoring
Duration(DD:HH:mm)	This field displays length of time a particular user worked on programs, processes applications, or tasks during a particular period of time
Start Time	This field displays the time when the initial data capture started
Time Zone	This field displays the time zone for which data was captured
Machine IP	This field displays the machine IP address of the end machine
Public Ip	This field displays the public IP address that is used to access the Internet by the end-user
MAC Address	This field displays the hardware identification(MAC Address) number that uniquely identifies end machine on a network.
Process Owner	This field displays the process owner
Created On	This field displays the date and time when the record was created under the User Activity Report

You can download the reports in the following formats:

- Click this :pdf_icon: icon to download the report in PDF format
- Click this :word_icon: icon to download the report in Word format
- Click this :excel_icon: icon to download the report in Excel format
- Click this :csv_icon: icon to download the report in CSV format

8.1.1.1 Raised Alerts

Raised Alerts report displays alerts triggered during monitoring activities. Select users or users groups and view all the alerts triggered during monitoring.

The alerts that are displayed are defined in the Log, Restrict, and USB tabs under the Create profile module.

These alerts are configured for:

- Browsing Activities

- Email
- File Access
- Application Access
- Instant Messaging
- Detect a specified keyword, keyword group, process, or multiple processes
- When certain restricted keywords are used, certain restricted programs, are started, or restricted applications or files with listed names are opened
- USB insert, read, write operations

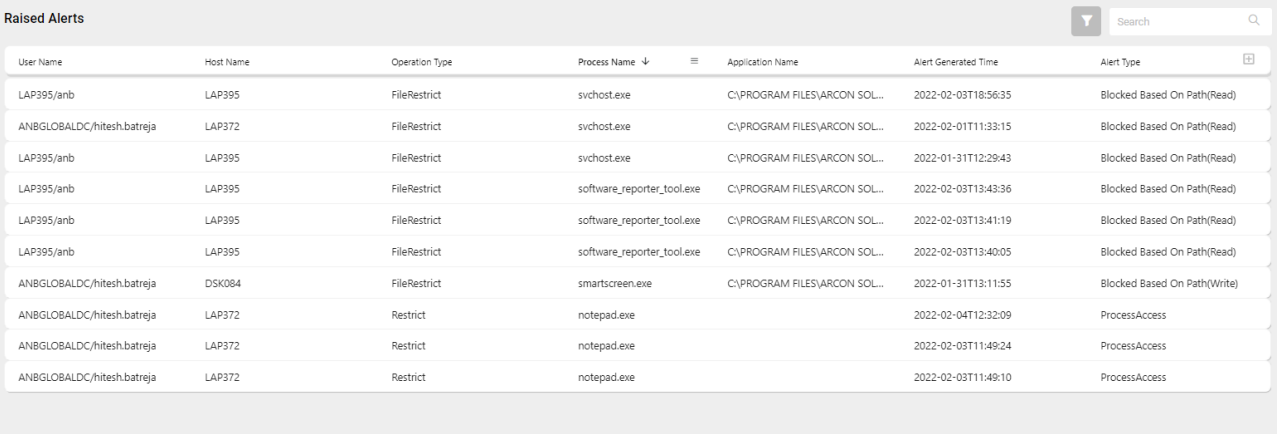
Refer to the following table to understand each of the fields in the Filter screen:

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
User Name	Select single or multiple users from the drop-down to fetch the report

Refer to the following table to understand each of the fields in the raised alerts report:

Field	Description
User Name	This field displays the Username for which alert was raised
Alert Time	This field displays the time when the alert was raised
Host Name	This field displays the hostname for which alert was raised
Operation Type	The Operation type depends on type of activity for which alert is raised It could be Alert or Restrict The operation Type is **Alert** if a alert is raised for keyboard or process monitoring or Facial Recognition Alert Type is **Restrict** if alert is raised when a restriction rule is violated
Process	Displays the process for which alert was triggered Example: FACIALRECOG TASKMGR.EXE SKYPE.EXE

Field	Description
Alert Type	Displays the alert trigger because of which the alert was raised Some of the alert trigger types are as follows: • Facial Identity Fail • ProcessAccess • Invalid Attempt 1/3 • Invalid Attempt 2/3 • Invalid Attempt 3/3



You can download the reports in the following formats:

- Click this :pdf_icon: icon to download the report in PDF format
- Click this :word_icon: icon to download the report in Word format
- Click this :excel_icon: icon to download the report in Excel format
- Click this :csv_icon: icon to download the report in CSV format

8.1.1.2 User Analysis Report

User Level report is an intelligent behavior analysis report that can detect anomalies that indicate a deviation from the normal behavioral baseline.

Dynamic risk scoring identifies insider activity before they represent a real threat. It provides advanced analytics to help solve the following challenges:

- Manage and enhance software application usage and spending.
- It displays a number of profiles applied to a particular user for a particular duration.
- The number of alerts generated during a period of time, last activity time, and percentage of risk that is calculated.

Filter

You can filter report data by applying the following filters/search criteria. Select the required details and click **Search**.

Field	Description
From Date	Select the From Date for which you want to fetch the report Click the calendar icon to select the From Date
To Date	Select the To Date for which you want to fetch the report Click the calendar icon to select the To Date
User Name	Select the Users from the dropdown
Host Name	Select the Host Name from the dropdown

The User Level Report exhibits the following tabs:

- **Overview:** The total number of time in seconds spent by the user on each application process during a particular period of time.
- **Profiles:** Profiles tab gives the details of all the profiles applied to the user during a particular period of time.
- **Alerts:** Alerts tab lists all the alerts fired at the time when the alert was fired for the operation type process name.
- **Activity:** Activity displays all the video logs gathered during Keyboard and process monitoring process.
- **Location**: Location displays the latitude and longitude of the machine accessed by the user and also whether the location is an office location or not.

Overview

The Overview tab exhibits the following three sections:

Section 1: This section displays Profiles, Alerts assigned to the user, and the Last Activity Time.

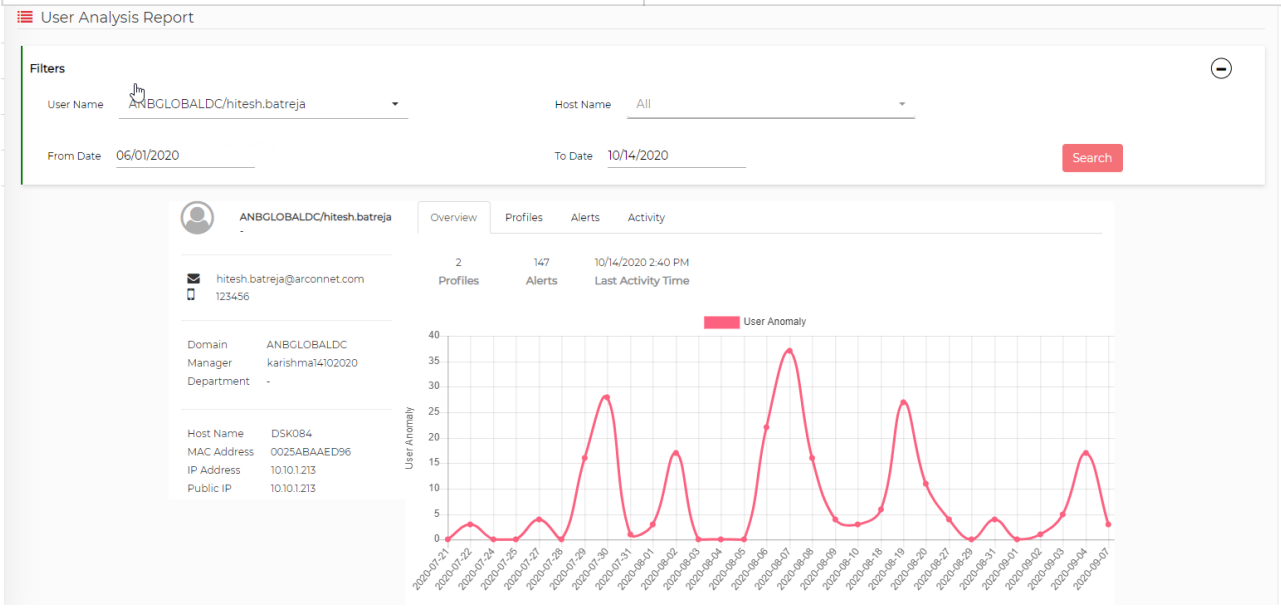
Field	Description
Profiles	This field displays the number of profiles assigned to the user
Alerts	This field displays the number of alerts generated for the user
Last Activity Time	This field displays the time when the user was last active

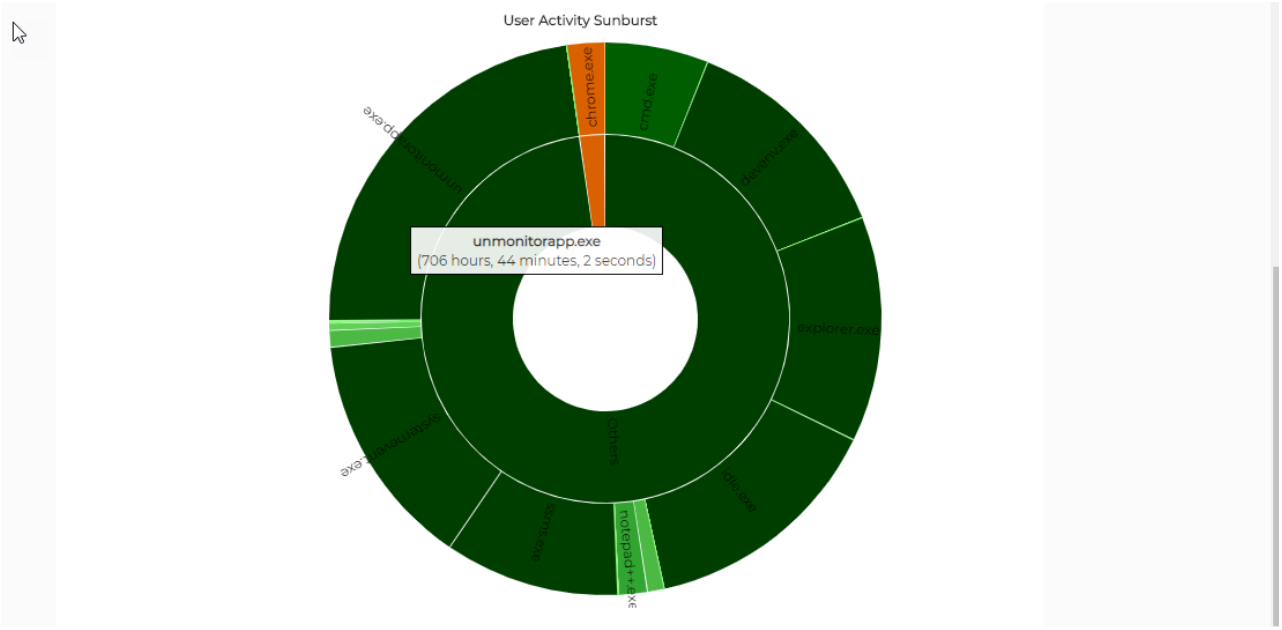
Section 2: This section displays the **User Activity Sunburst** chart.

Sunburst chart illustrates the use of processes by the user. It captures the duration of time spent on particular processes. It has sliced components and each slice displays duration in time spent on particular processes. A built-in drill down gives the ability to click and focus on one item at runtime and drill down into its details which helps in data analysis/investigation. Selecting a slice additionally displays it out of the sunburst chart, expanding alongside its original position and displaying its details.

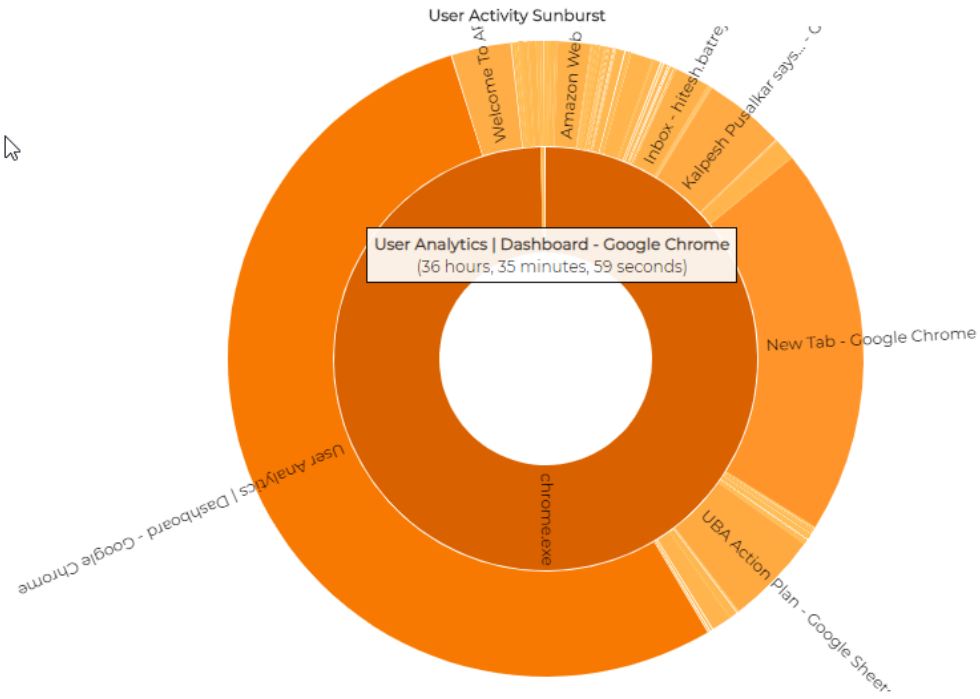
Section 3: This section displays the **User Activity** chart**.** It displays the total time in seconds spent on processes by the users.

Field	Description
Process	The x- axis displays all the processes used by the user over the selected period of time
Time(Seconds)	The y- axis displays time in seconds

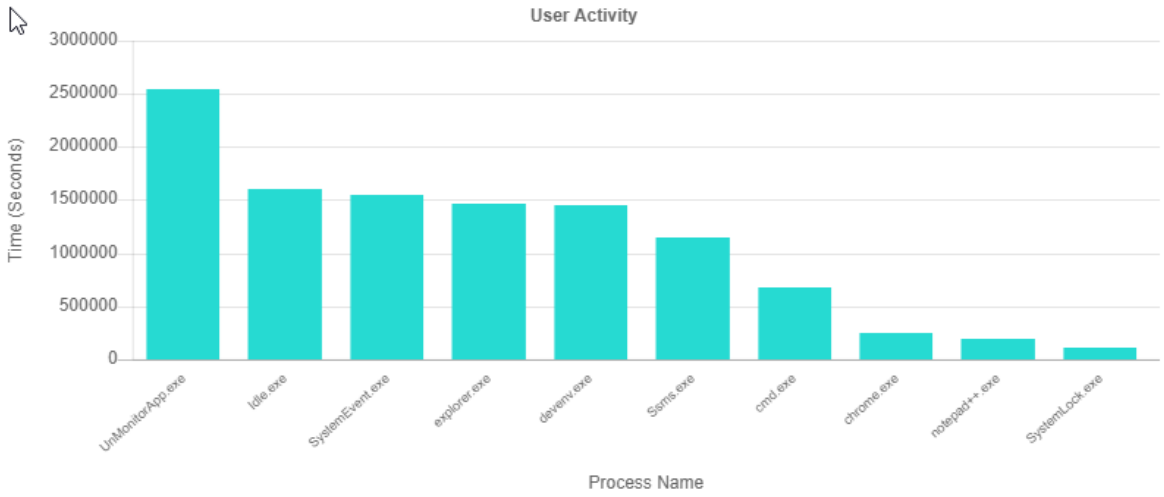




Sunburst chart



Sunburst chart

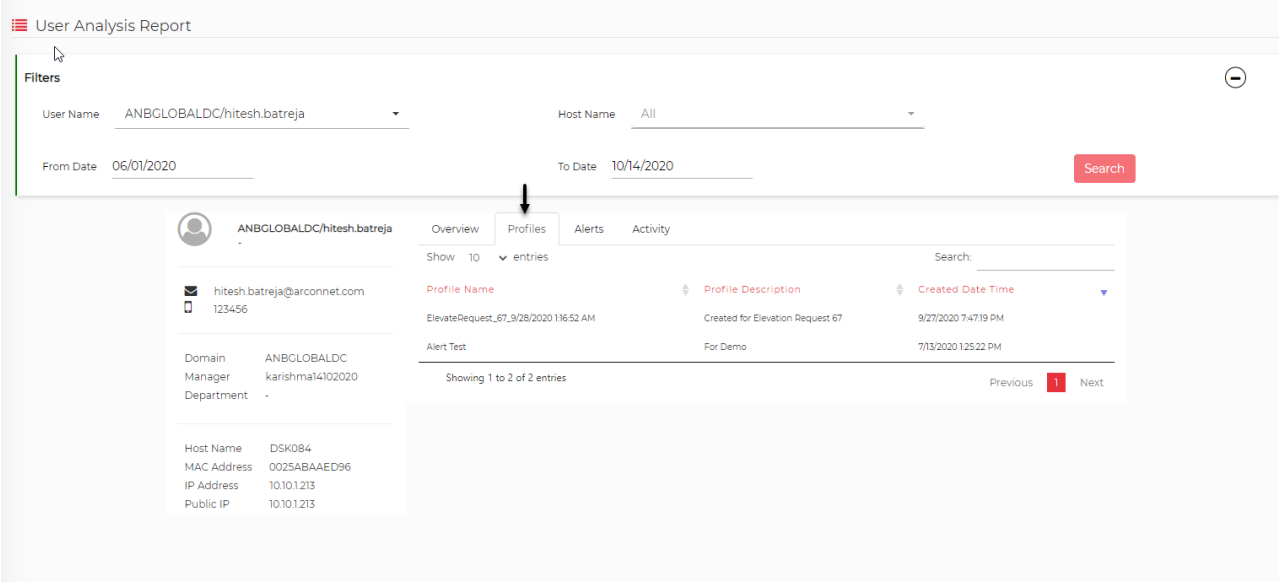


8.1.1.3 User Activity Chart

Profiles

The Profile tab exhibits the following fields:

Field	Description
Profile Name	This field displays the name of the profile assigned to the user
Profile Description	This field displays the profile description
Created Date Time	This field displays the date and time when the profile was created

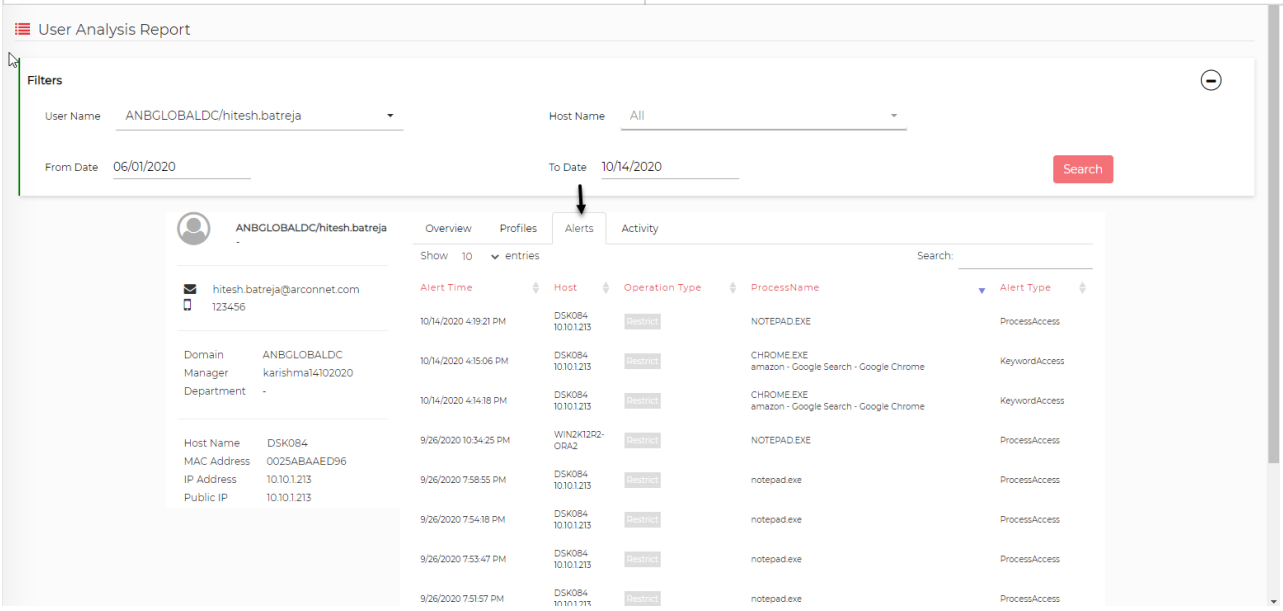


Alerts

The Alert tab exhibits the following fields:

Field	Description
Alert Time	This field displays the date and time when the alert was generated
Host	This field displays the hostname for which alert was generated
Operation Type	This field displays the date and time when the profile was created
ProcessName	This field displays the process name for which the alert was generated

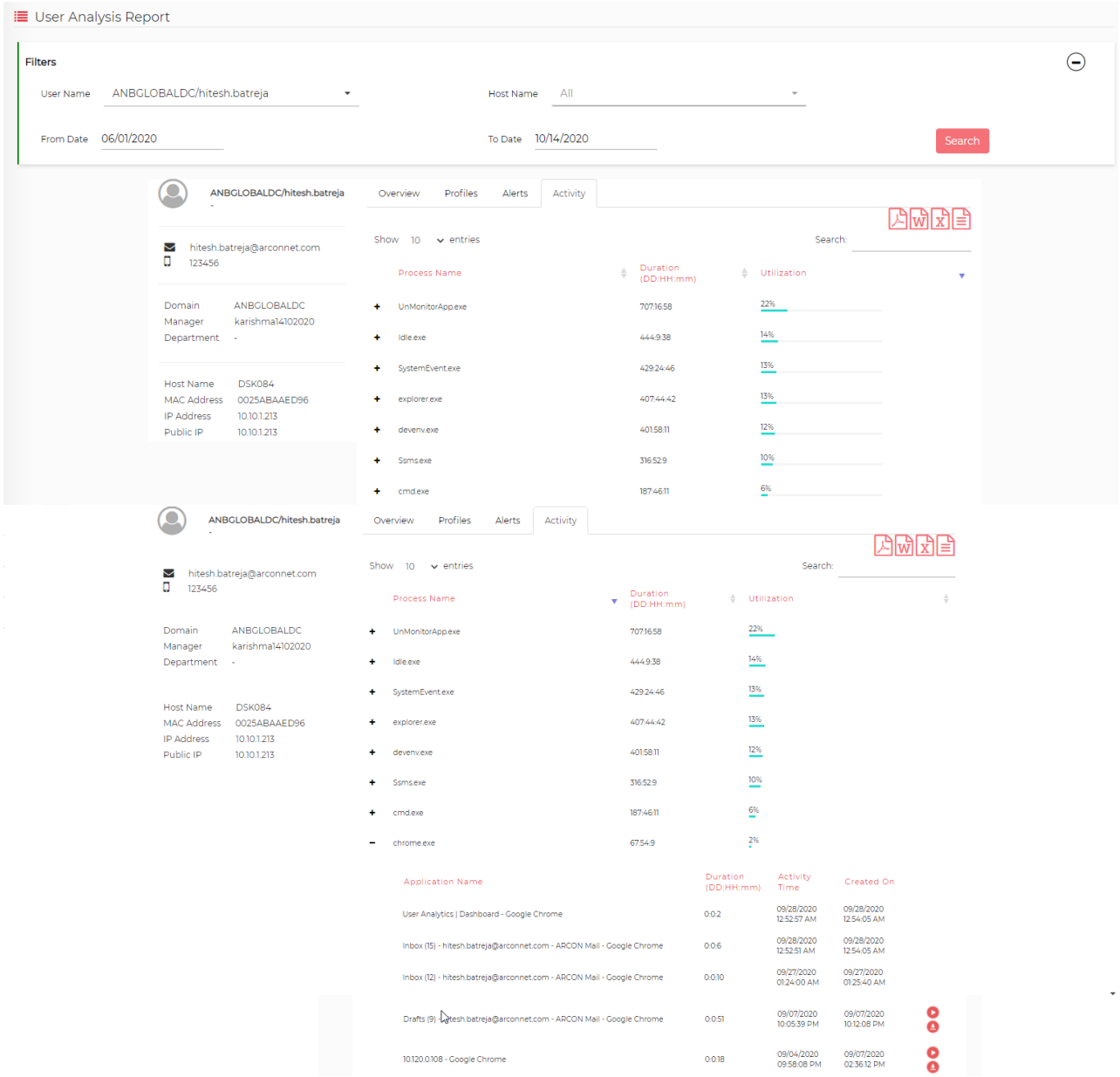
Field	Description
Alert Type	This field displays the type of activty for which alert is generated For example: • KeywordAccess • Process Access • Facial Recognition

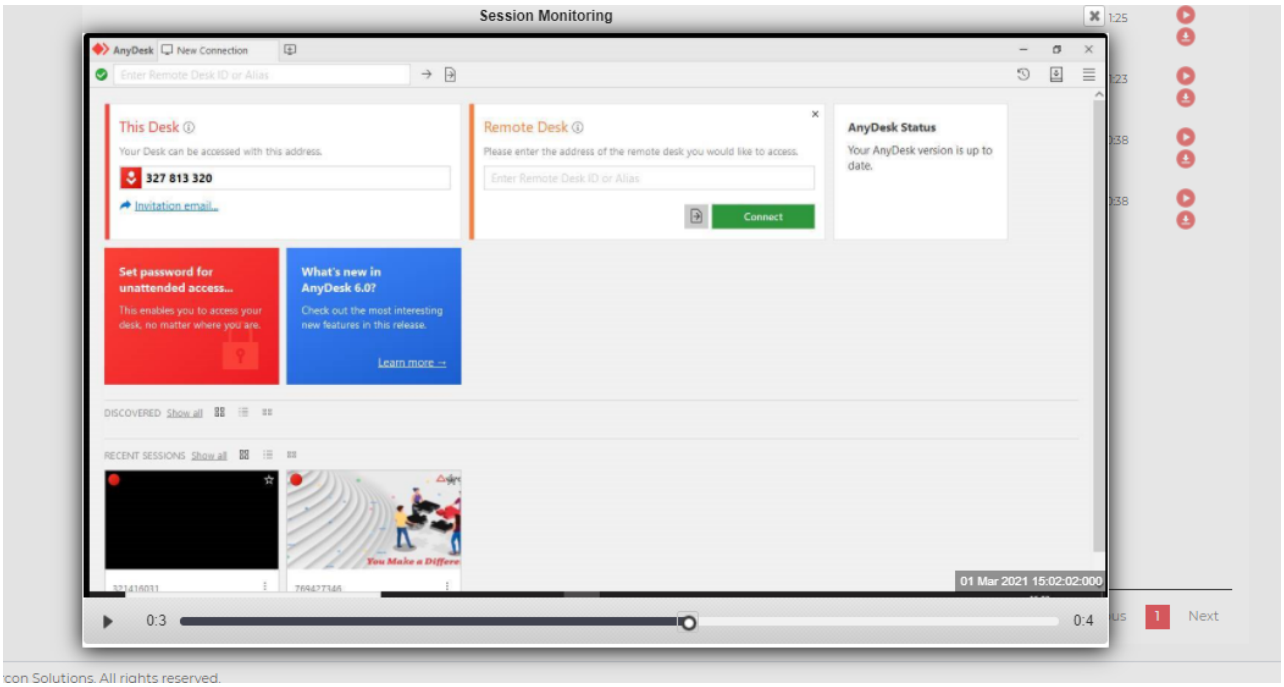


Activity

The Activity tab exhibits the following fields. This tab is where the session recording is displayed and can be recorded.

Field	Description
Process Name	This field displays the name of the processes used by the user
Duration	This field displays the total duration the user has on the process
Utilization	This field displays the total utilization in percentage for the process
:Record:	This button will play the session recording for the specific session
	This button will download the session recording

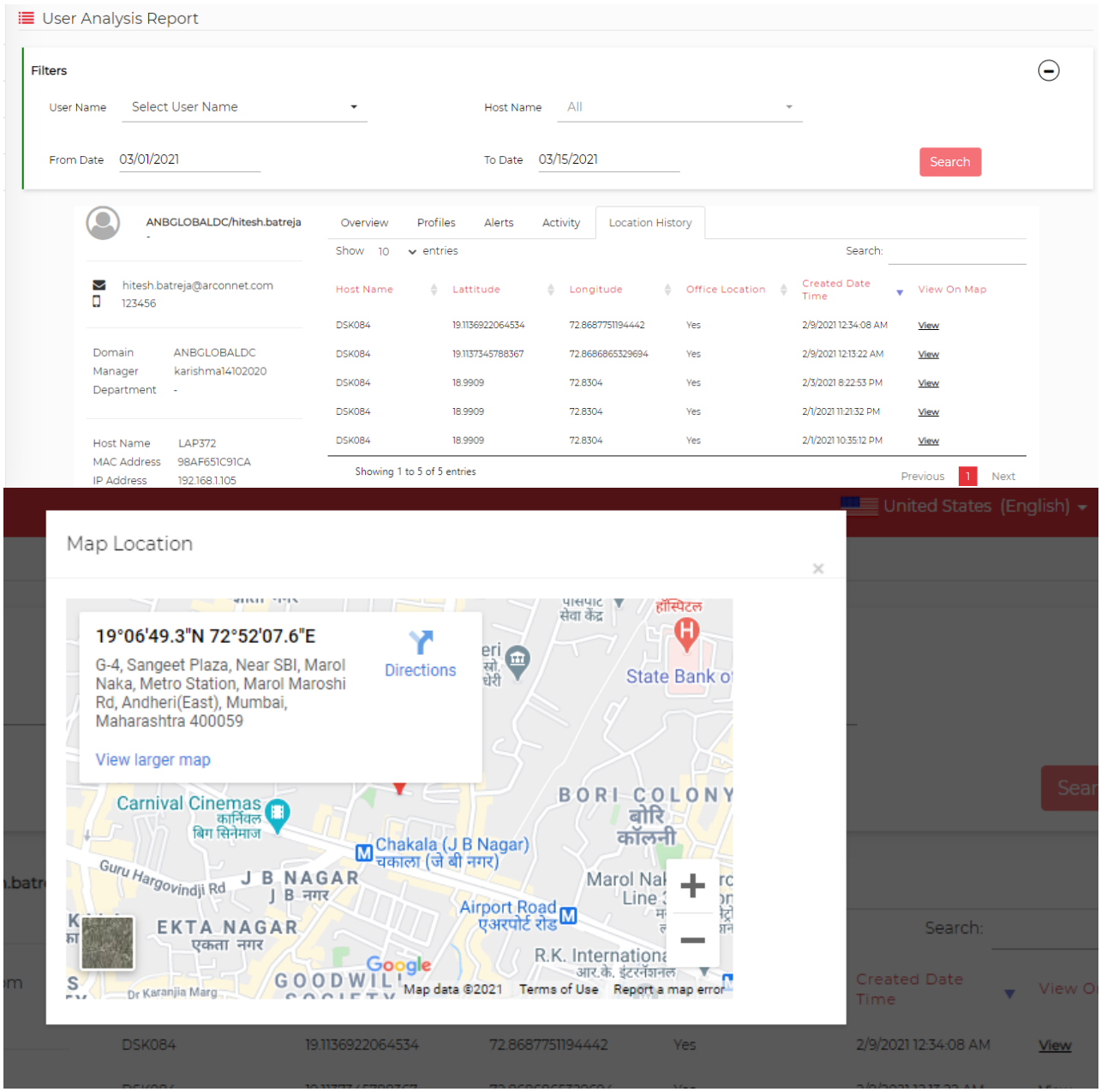

User Analysis Report
Filters
User Name
ANBGLOBALDC/hitesh.batreja
Host Name
All
From Date
06/01/2020
To Date
10/14/2020
Search
ANBGLOBALDC/hitesh.batreja
Overview
Profiles
Alerts
Activity
hitesh.batreja@arconnet.com
123456
Domain
ANBGLOBALDC
Manager
karishma14102020
Department
Host Name
DSK084
MAC Address
0025ABAAED96
IP Address
10.10.1.213
Public IP
10.10.1.213
Show 10 entries
Search:
Process Name
Duration (DD:HH:mm)
Utilization
UnMonitorApp.exe
707:16:58
22%
Idle.exe
444:9:38
14%
SystemEvent.exe
429:24:46
13%
explorer.exe
407:44:42
13%
devenv.exe
401:58:11
12%
Ssms.exe
316:52:9
10%
cmd.exe
187:46:11
6%
chrome.exe
67:54:9
2%
Application Name
Activity Time
Created On
User Analytics | Dashboard - Google Chrome
0:0:2
09/28/2020 12:52:57 AM
09/28/2020 12:54:05 AM
Inbox (15) - hitesh.batreja@arconnet.com - ARCON Mail - Google Chrome
0:0:6
09/28/2020 12:52:51 AM
09/28/2020 12:54:05 AM
Inbox (12) - hitesh.batreja@arconnet.com - ARCON Mail - Google Chrome
0:0:10
09/27/2020 01:24:00 AM
09/27/2020 01:25:40 AM
Drafts (9) - hitesh.batreja@arconnet.com - ARCON Mail - Google Chrome
0:0:51
09/07/2020 10:05:39 PM
09/07/2020 10:12:08 PM
10.120.0.108 - Google Chrome
0:0:18
09/04/2020 09:58:08 PM
09/07/2020 02:36:12 PM



Location

The location tab exhibits the following fields:

Field	Description
HostName	This field displays the hostname of the machine
Latitude	This field displays the latitude of the endpoint
Longitude	This field displays the longitude of the endpoint
Office Location	This field displays whether the user is in the office or not
Created Date Time	This field displays the date and time when this location was captured
View on Map	This field displays the location of the user on the map



8.1.1.4 User Elevated Application

Application Elevation policy is a management method that assures that users have no access to any of the applications unless such access has been explicitly granted. ARCON | EPM enables end-users to request an elevation request to obtain the rights they need to perform the tasks which further minimizes security risks. These elevation requests enable organizations to grant temporary privileges to the users on endpoints with a flexible model that caters to varying business needs. It enables the configuration of privileges so that users can request privilege elevation at specific times, for a duration of time, and on certain endpoints for required applications. ARCON | EPM admin has full right to limit the time duration for which approvals are valid.

Filter

You can filter report data by applying the following filters/search criteria. Select the required details and click **Search**.

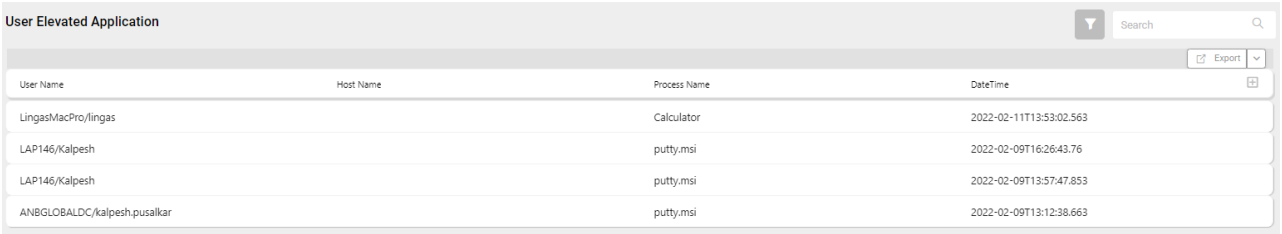
Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Users	Select single or multiple users from the drop-down for which you want to fetch the report

Refer to the following table to understand the data displayed on the report:

Field	Description
User Name	This field displays the name of the end users that raised the elevation request
Process Name	This field displays the process name for which elevation request is raised
Interval	This field displays the time interval for which the user has requested access to application/process
Start Time	This field displays the start time for which the user has requested access to application/process
End Time	This field displays the end time for which the request for elevation to access application/process ends
Created Date Time	This field displays exact Date and Time when elevation request was raised

You can download the reports in the following formats.

- Click this :csv_icon: icon to download the report in CSV format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :pdf_icon: icon to download the report in PDF format.



8.1.1.5 User Elevated Run Logs

User Elevated Run Logs displays the list of all the elevated applications accessed by Users on the endpoint. It displays details such as username, process name, and date-time on which the elevated process was accessed.

Filter

You can filter report data by applying the following filters/search criteria. Select the required details and click **Search**.

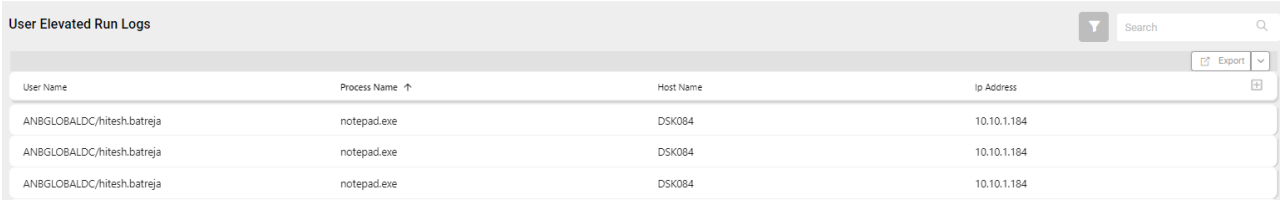
Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Users	Select single or multiple users from the drop-down for which you want to fetch the report

Refer to the following table to understand the data displayed on the report:

Field	Description
User Name	This field displays the name of the user that executes the elevated application on the end machine User runs an elevated application on the end machine using the following methods • Run • Run with EPM (arguments)
Process Name	This field displays the name of the elevated application/process that was run/accessed on the end machine
Access DateTime	This field displays the Date and time when the elevated application was run/accessed

You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.



Clipboard Report

ARCON |EPM console monitors/records clipboard activities on the end machine. It captures clipboard content of various types such as text, images, files, as follows:

- It captures all the text data, which has been copied or cut and then pasted into documents, files, applications, browser address bars, etc. on the end machines.

- It captures all image data, which has been copied or cut and then pasted into documents, files, applications, etc. on the end machine.
- It also captures file activities such as print, copy, paste, and download.
- Admin can view these logs of transactions under this report.
- Admins can customize the reports and categorize based on content type (text, image or file) and view the content description and content of the clipboard activities carried out at the endpoint.

Filter

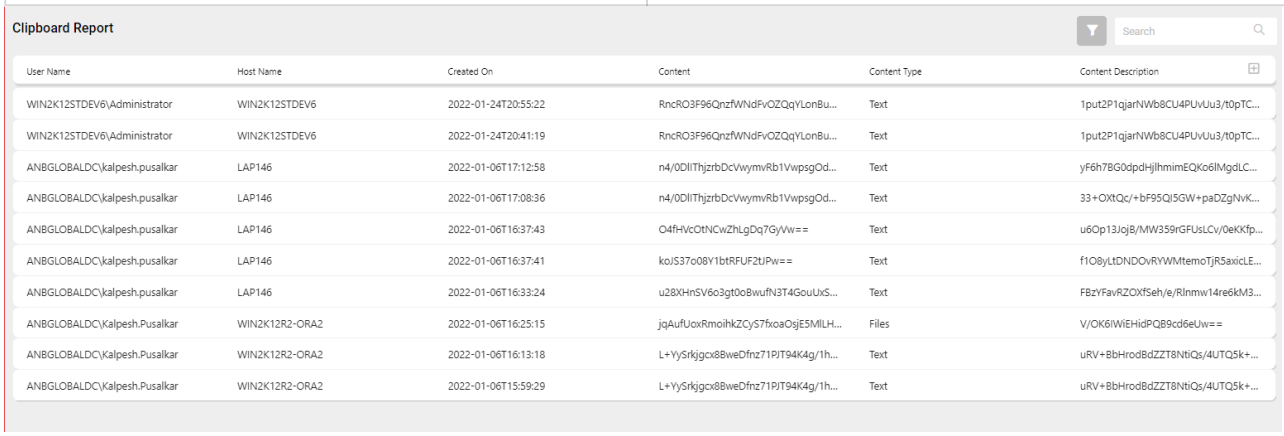
You can filter report data by applying the following filters/search criteria:

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Users	Select a single or multiple users from the drop-down for which you want to fetch the report
Select Host	Select a single or multiple hosts from the drop-down for which you want to fetch the report
Content Type	Select the Type of content for which you want to view reports from the following options:: • **Images** • **Files** • **Text**

Refer to the following table to understand the data displayed on the report:

Field	Description
User Name	This field displays the name of the users whose clipboard report is fetched
Host Name	This field displays the name of the host whose clipboard report is fetched
Content Type	• Images • Files • Text

Field	Description
Content Description	If the type of content is Image type, Content description would be such as below **Image is copied** If the type of content is Text type, Content description would be such as below **Number of characters in the copied text** If the type of content is File type, Content description would be such as below **Number of files copied to the clipboard**
Content	If the type of content is Image type, Content would be such as below **View Image** If the type of content is Text type, Content would be such as below **Actual text copied to the clipboard.** If the type of content is File type, Content would be such as below **Path of the file/ files.**
Created On	This field displays the date when content was copied to the clipboard



Clipboard Report

Search

User Name	Host Name	Created On	Content	Content Type	Content Description
WIN2K12STDEV6\Administrator	WIN2K12STDEV6	2022-01-24T20:55:22	RncRO3F96QnzfWNdFvOZQqYLonBu...	Text	1put2P1qjarNWb8CU4PUvUu3/t0pTC...
WIN2K12STDEV6\Administrator	WIN2K12STDEV6	2022-01-24T20:41:19	RncRO3F96QnzfWNdFvOZQqYLonBu...	Text	1put2P1qjarNWb8CU4PUvUu3/t0pTC...
ANBGLOBALDC\kalpesh.pusalkar	LAP146	2022-01-06T17:12:58	n4/0DlIThjzrbDcVwymvRb1VwpsgOd...	Text	yF6h7BG0dpdHjlhmimEQKo6lMgdLC...
ANBGLOBALDC\kalpesh.pusalkar	LAP146	2022-01-06T17:08:36	n4/0DlIThjzrbDcVwymvRb1VwpsgOd...	Text	33+OXtQc/+bF95QI5GW+paDZgNvK...
ANBGLOBALDC\kalpesh.pusalkar	LAP146	2022-01-06T16:37:43	O4fHVcOtNCwZhLgDq7GyVw==	Text	u6Op13JojB/MW359rGFUsLCv/0eKKfp...
ANBGLOBALDC\kalpesh.pusalkar	LAP146	2022-01-06T16:37:41	koJS37c08Y1btRFUF2tJPw==	Text	f1O8yLtDNDOvRYWMtemoTjR5axicLE...
ANBGLOBALDC\kalpesh.pusalkar	LAP146	2022-01-06T16:33:24	u28XHnSV6o3gt0oBwufN3T4GouUxS...	Text	FBzYFavRZOXfSeh/e/Rlnmw14re6kM3...
ANBGLOBALDC\Kalpesh.Pusalkar	WIN2K12R2-ORA2	2022-01-06T16:25:15	jqAufUoxRmoihkZCyS7fxoaOsjE5MlLH...	Files	V/OK6IWiEHidPQB9cd6eUw==
ANBGLOBALDC\Kalpesh.Pusalkar	WIN2K12R2-ORA2	2022-01-06T16:13:18	L+YySrkjgcx8BweDfnz71PJT94K4g/1h...	Text	uRV+BbHrodBdZZT8NtiQs/4UTQ5k+...
ANBGLOBALDC\Kalpesh.Pusalkar	WIN2K12R2-ORA2	2022-01-06T15:59:29	L+YySrkjgcx8BweDfnz71PJT94K4g/1h...	Text	uRV+BbHrodBdZZT8NtiQs/4UTQ5k+...

You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.

8.1.1.6 File Access Report

The **File Access Report** displays the information related to file access by the user. You can use this report to understand how the file is accessed and understand the activities performed on the files.

To fetch the report, add the following details in the Search / Filter criteria:

Filter

You can filter report data by applying the following filters/search criteria:

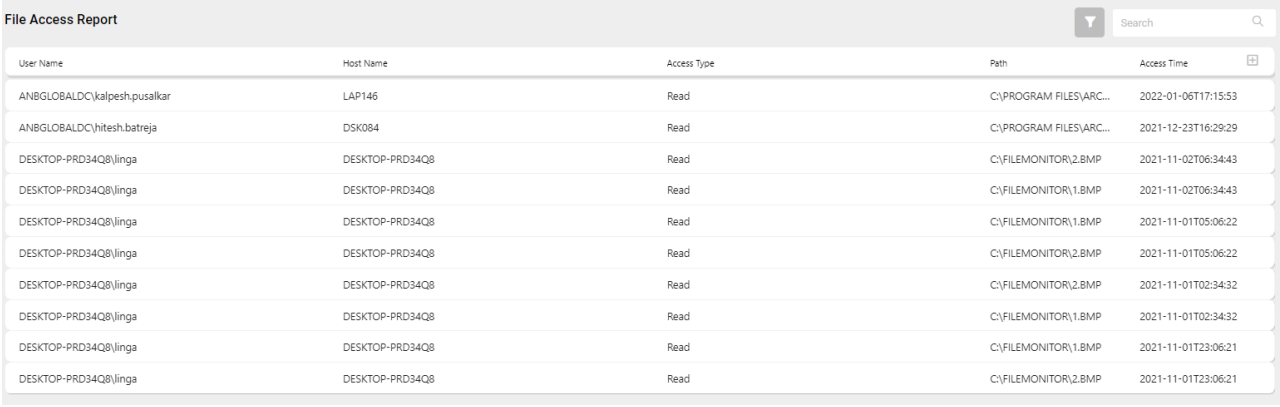
Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Users	Select single or multiple users from the drop-down for which you want to fetch the report, Check the checkbox next to users to select the desired users
Select Host	Select single or multiple hosts from the drop-down for which you want to fetch the report
Access Type	Select the access types of the file from the drop-down for which you want to fetch the report The access types are Viewed, Created, Modified and Deleted

Refer to the following table to understand the data displayed on the report:

Field	Description
Host Name	This field displays the hostname of the user who has accessed the file
User Name	This field displays the name of the user who has accessed the file
File /Folder Name	This field displays the file or the folder accessed
File / Folder Path	This field displays the path of the file or the folder accessed
Access Type	This field displays the access type of the file or folder accessed
Access Via	This field displays the medium used to access the file
Access Time	This field displays the time at which the file was accessed

You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.



User Access Report

User Access Report logs the time of the user's first activity and last activity on the endpoint as first and last access.

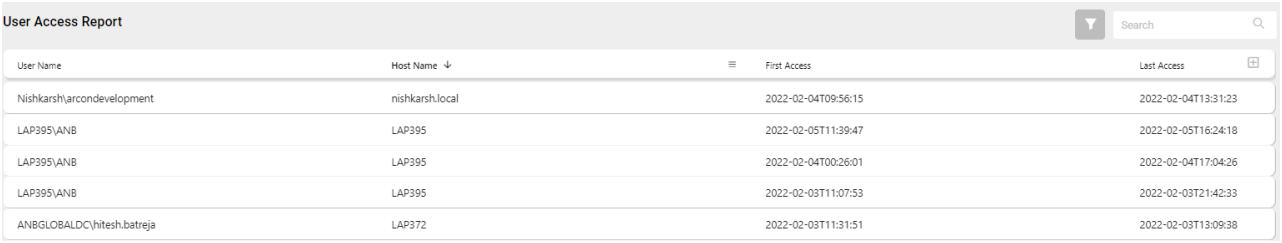
Filter

You can filter report data by applying the following filters/search criteria:

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Users	Select single or multiple users from the drop-down for which you want to fetch the report
Select Host	Select single or multiple hosts from the drop-down for which you want to fetch the report

Refer to the following table to understand the data displayed on the report:

Field	Description
User Name	This field displays the Users whose access data is listed
Host Name	This field displays the Hosts for which access data is listed
First Access	This field displays the timestamp for the user's first activity on the endpoint
Last Access	This field displays the timestamp for the user's last activity on the endpoint



You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.

8.1.1.7 User Directory

User Directory is used for storage classification and the report displays the list of users already added / onboarded to the console.

Filter

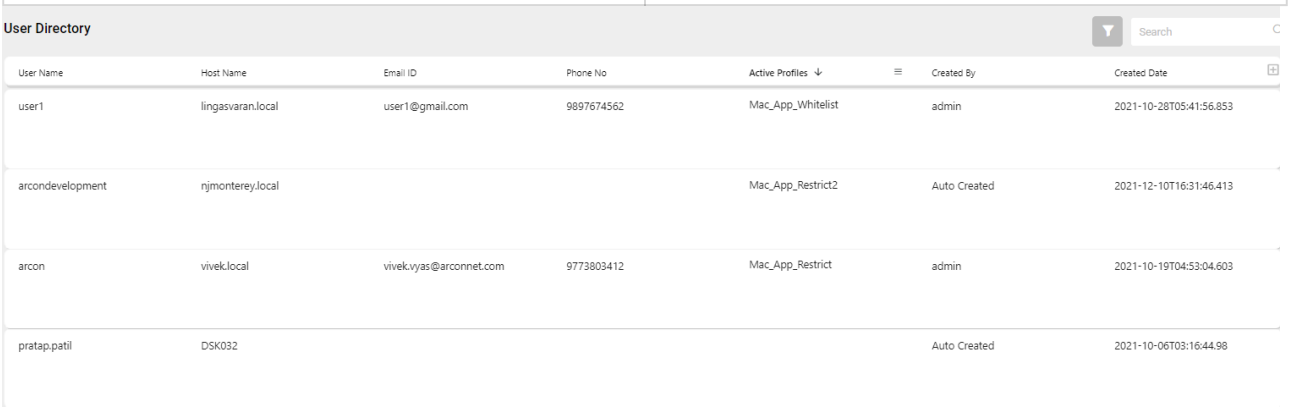
You can filter report data by applying the following filters/search criteria:

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Users	Select single or multiple users from the drop-down for which you want to fetch the report

Refer to the following table to understand the data displayed on the report:

Field	Description
User Name	This field displays the name of the user
Host Name	This field displays the host count. Click on this link it displays all the hostnames pertaining to the user
Email Id	This field displays the user email id
Phone No	This field displays the user phone number
Groups	This field displays the group count. Click on this link it displays all the groups the user is present in
Active Profile	This field displays the active profile count. Click on this link it displays all the active profile assigned to the user

Field	Description
Onboarding Mode	The Onboarding Mode could be Manual or Auto • The Manual mode indicates the user is created from the user module or synchronize via AD • The Auto mode indicates you have installed the agent on the endpoint and when the agent detects any new user it automatically onboard the user
Onboarded By	This field displays • The value of this field will be **name of the user** who onboarded the user in case of Manual Onboarding • The value of this field will be **Auto Created** in case the user was onboarded automatically
Onboarded On	This field displays the date and time when the user was onboarded



You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.

8.1.1.8 Productivity Report

Productivity Report displays the first and last activity of the users on the endpoint every day. It allows you to keep track of users' work time and identify deviations from the work schedules. The Productivity Report can be used to track the productivity of a single user or a group of users for a duration of time.

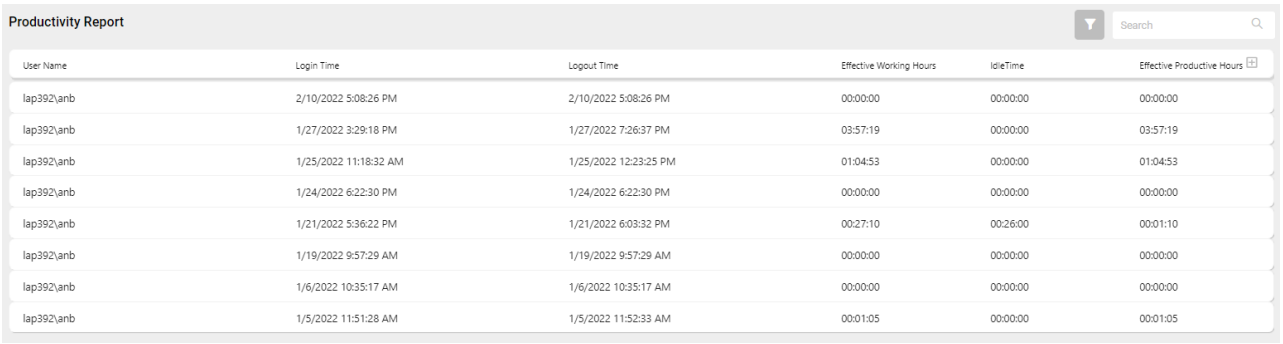
To fetch the report, add the following details in the Search/ Filter criteria:

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date

Field	Description
Select Users	Select single or multiple users from the drop-down for which you want to fetch the reports
Select User Group	Select a single or multiple user groups for which you want to fetch the reports

Refer to the following table to understand the data displayed on the report:

Field	Description
User name	This field displays the username for which you want to fetch the productivity details
Login Time	This field displays the time when the user logged in to the system/endpoint
Log out Time	This field displays the time when the user logged out of the system/endpoint
Effective Working Hours	This field displays the total **Elapsed time** between the user login and logout time
Idle Time	This field displays the summation of time such as lock time, time utilized by idle.exe
Effective Productive Time	This field displays the actual productive hours or work hours for the users
Date	This field displays the date for which the report is fetched



You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.

8.1.1.9 UBA Dashboard Activity

The UBA Dashboard activity reports track the activities performed by users through the EPM dashboard.

Navigate to **Reports** > **User Reports** > **UBA Dashboard Activity**. The below screen is displayed.

To fetch the report, add the following details in the Search/ Filter criteria.

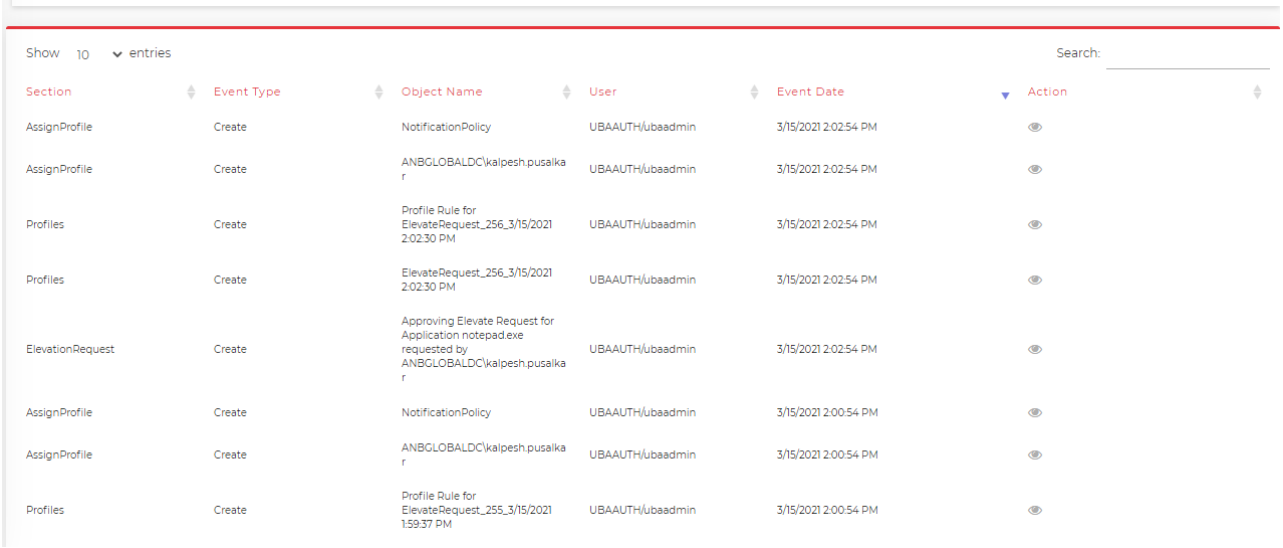
Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Section	Select the section for which you want to fetch the report. These are selection of the activity that have been perfomed
Select Users	Select single or multiple users from the drop-down for which you want to fetch the reports
Select User Group	Select a single or multiple user groups for which you want to fetch the reports
Select Action Type	Select the action type for which you want to fetch the report.

Refer to the following table to understand the data displayed on the report:

Field	Description
Section	This field displays the section of activity where change was made
Event Type	This field displays the event type of the activity
Object Name	This field displays the object name of the activity where change was made
Event Date	This field displays the date when the activity was preformed
Action	This field displays all the activity details related to the activity performed

You can download the reports in the following formats.

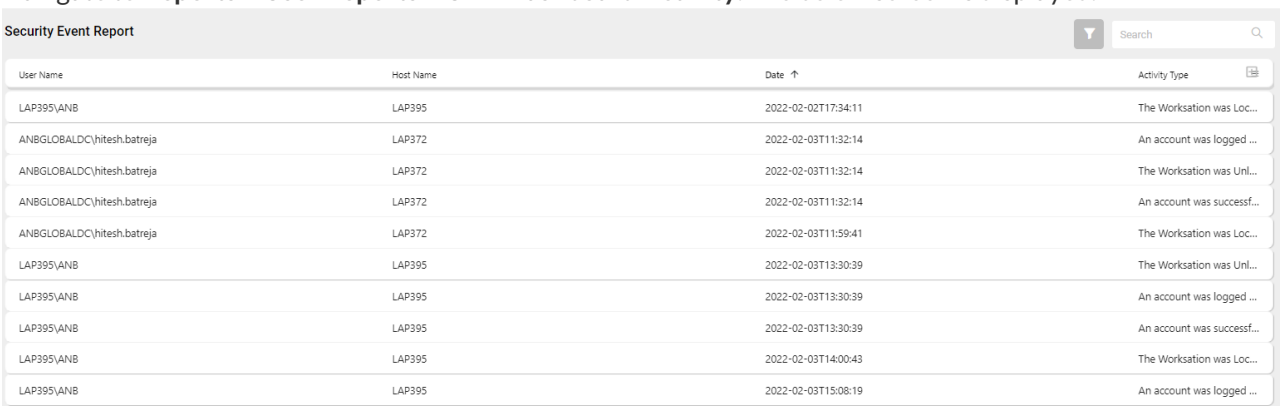
- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.



8.1.1.10 Security Event Report

The report displays the overall activities of users for Login in the Active Directory.

Navigate to **Reports** > **User Reports** > **UBA Dashboard Activity**. The below screen is displayed.



To fetch the report, add the following details in the Search/ Filter criteria.

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Activity Type	Type of activity that was performed by the user. Available options are: • Login Success • Login Failed • Password Change
Select Users	Select single or multiple users from the drop-down for which you want to fetch the reports

Field	Description
Select User Group	Select a single or multiple user groups for which you want to fetch the reports
Host Name	This will be the identifier of the device the user has accessed

Refer to the following table to understand the data displayed on the report:

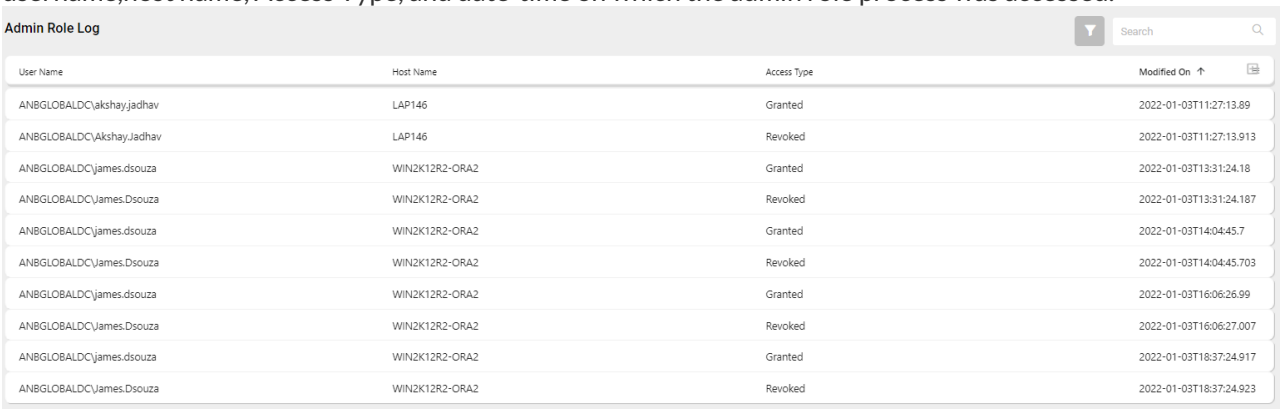
Field	Description
Date	Date when the activity was performed
User Name	Name of the user
Host Name	Machine or device identifier of the user
Activity Type	Type of activity that was performed
Details	Details of activity that was performed

You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.

8.1.1.11 Admin Role Log

User Admin Logs displays the list of all the admin role changes on the endpoint. It displays details such as username,host name, Access Type, and date-time on which the admin role process was accessed.



To fetch the report, add the following details in the Search/ Filter criteria.

Field	Description
Date Range	Select the From Date and To Date for which you want to fetch the report Click the calendar icon to select the From Date
Local User ○ Ad User ○	Enable the option to get the reports of required user . Available options are: • Local User • Ad User
Select Users	Select single or multiple users from the drop-down for which you want to fetch the reports
Select User Group	Select a single or multiple user groups for which you want to fetch the reports
Host Name	This will be the identifier of the device the user has accessed

8.2 Application Reports

8.2.1 Application Usage Timeline

With Application Usage Timeline you can track usage of a particular process for a particular duration of time.

Filter

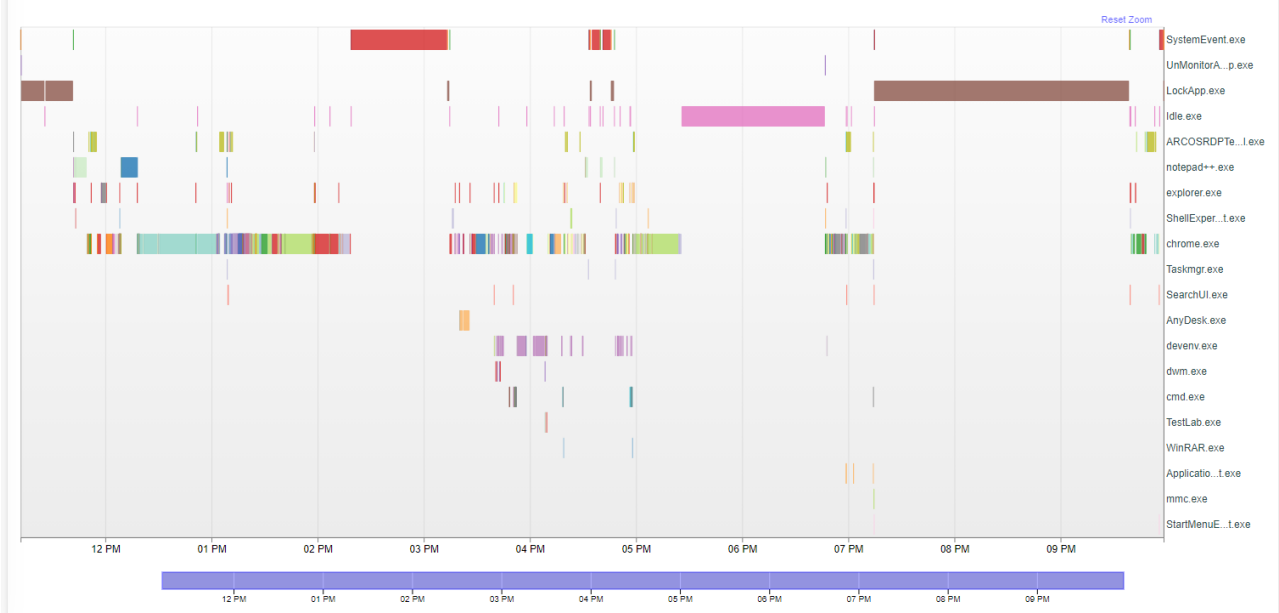
You can filter chart data by applying the following filters/search criteria:

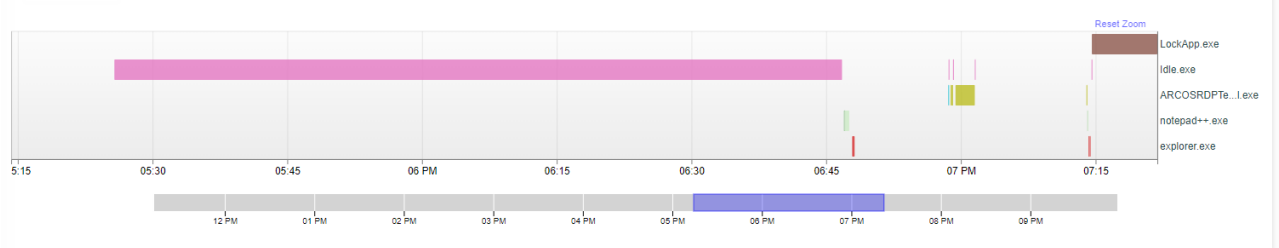
Field	Description
From Date	Select the From Date for which you want to fetch the report Click the calendar icon to select the From Date
To Date	Select the To Date for which you want to fetch the report Click the calendar icon to select the To Date
Select Users	Select the users from the drop-down for which you want to fetch the report
Host Name	Select a hostname from the drop-down for which you want to fetch the report

Note: The application Usage Timeline chart does not require an active internet connection to display the results.

The application Usage Timeline chart comprises of the following parameters:

Component	Description
X-axis	The x-axis of the chart displays the selected time period
Y-axis	Y-axis displays the name of the processes used during selected period of time Hover over the graph to view the task name, process name, and duration for which it is used. For example, there could be 5 tasks under process chrome.exe. Hover over different color codes for that process and it shows different tasks under the process Click on the particular task and you can view the video recording for the task/applicator on under the process
Click drag to zoom in	It has an interactive zooming feature. Just select a particular region or duration and zoom it to view the results in detail
Reset Zoom	Click on this button to reset the zoom function





8.2.2 Application Utilization Report

The **Application Utilization Report** tracks the usage information for a specified application/process defined in the database. You can use this report to determine how heavily a specific **application** is used. To fetch the report, add the following details in the Search/ Filter criteria.

Filter

You can filter report data by applying the following filters/search criteria:

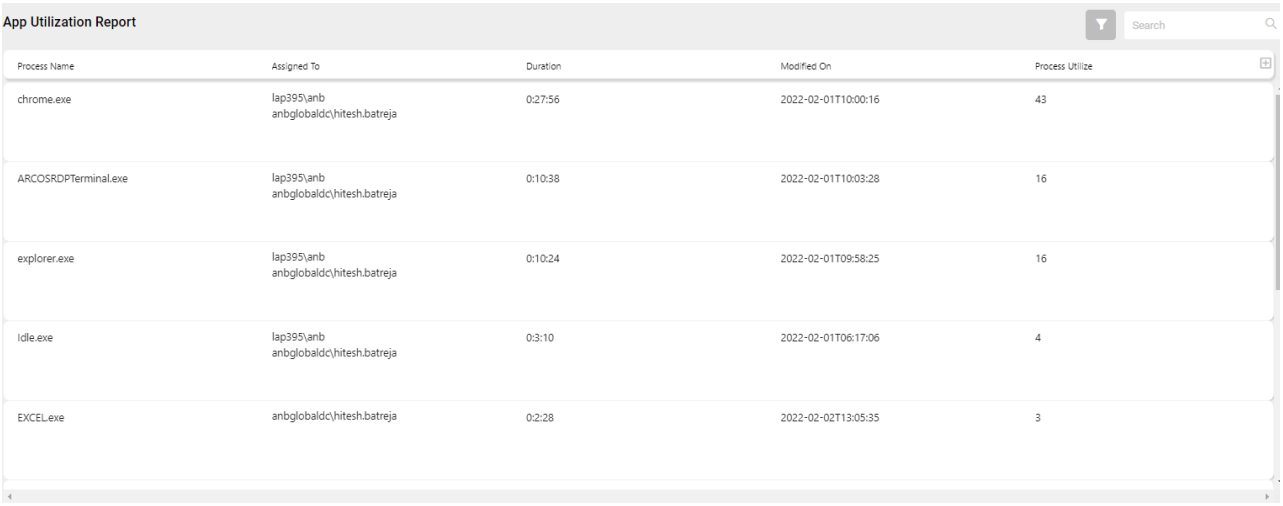
Field	Description
From Date	Select the From Date for which you want to fetch the report Click the calendar icon to select the From Date
To Date	Select the To Date for which you want to fetch the report Click the calendar icon to select the To Date
Select Users	Select single or multiple users from the drop-down for which you want to fetch the report, Check the checkbox next to users to select the desired users
Select User Group	Select single or multiple user group from the drop-down for which you want to fetch the report, check a user group you want to get a report on

Refer to the following table to understand the data displayed on the report:

Field	Description
Process Name	This field displays the name of the application/ process used for the selected time frame by a single user or a group of users. The processes are displayed in descending order with the most used process displayed on the top
Number of Users	This field displays the number of users for which the report is fetched
Date	This field displays the dates for which the report is fetched. The dates will be listed in ascending order
Duration	This field displays the time duration (in *hours* and minutes) for which a particular process is used
Utilization	This field displays the process utilization percentage for the selected time frame in a descending order

You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.



8.3 System Reports

8.3.1 System Utilization Report

The System Utilization Report tracks the system usage for users over a period of time.

Filter

You can filter report data by applying the following filters/search criteria. Select the required details and click **Search**.

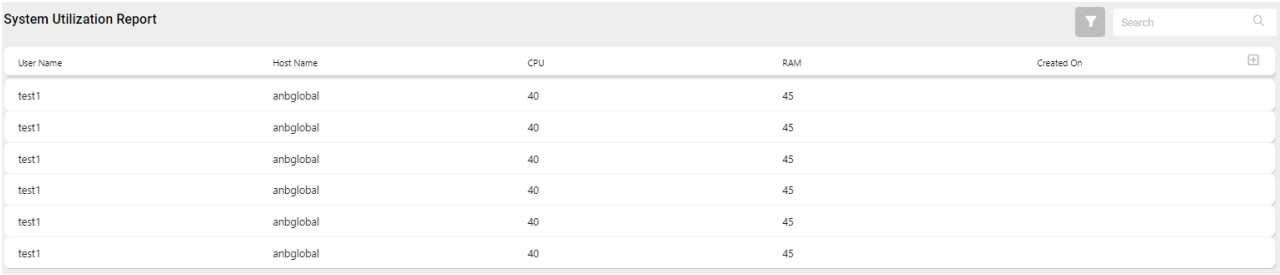
Field	Description
From Date	Select the From Date for which you want to fetch the report Click the calendar icon to select the From Date
Select Users	Select single or multiple users from the drop-down to fetch the report.
To Date	Select the To Date for which you want to fetch the report Click the calendar icon to select the To Date

Refer to the following table to understand the data displayed on the report:

Field	Description
User Name	This field displays the User name for which report is fetched
Host Name	This field displays the Host name for which report is fetched
Machine IP	This field displays the Machine IP for which report is fetched
OS	This field displays the operating system version

Field	Description
CPU %	**CPU%** The percentage of CPU usage indicates how much of the processor's capacity is currently in use by the end system **CPU%** can vary according to the type and amount of computing task because some tasks require heavy **CPU** time while others require less **CPU** time
RAM %	This field displays the memory usage in percentage that is in use on the end system
Disk Read (MBs)	This field displays Disk Read speed which displays how long it takes to open (read), something from the drive/ end machine It recorded with the letters "p/s (per second)" at the end of the measurement The end machine that has a read speed of X MBps means that it can record X MB (megabytes) of data every second
Disk Write (MBs)	This field displays Disk Write speed which determines how long it takes to save (write), something to the drive/ end machine It recorded with the letters "p/s (per second)" at the end of the measurement The end machine that has a write speed of X MBps means that it can record X MB (megabytes) of data every second
Net Sent (MBs)	The speed(in Mbs) at which the packets are sent over a network
Net Received (MBs)	The speed(in Mbs) at which the packets is received over a network
Net Packet Sent	The **packets** carry the data in the protocols that the **Internet** uses: Transmission Control Protocol/ **Internet** Protocol (TCP/IP) Net Packet displays the content (or data) being sent from the source A **packet** is a small amount of data sent over a network, such as a LAN or the **Internet**. Similar to a real-life package, each **packet** includes a source and destination as well as the content (or data) being transferred

Field	Description
Net Packet Received	The **packets** carry the data in the protocols that the **Internet** uses: Transmission Control Protocol/ **Internet** Protocol (TCP/IP) Net Packet displays the content (or data) being received at the destination
Created Date Time	Displays the date and time during which the time is captured



You can download the reports in the following formats.

- Click this :pdf_icon: icon to download the report in PDF format.
- Click this :word_icon: icon to download the report in Word format.
- Click this :excel_icon: icon to download the report in Excel format.
- Click this :csv_icon: icon to download the report in CSV format.

Language Support

The Dashboard has multilingual support that transforms the content into multiple languages using resource files.

The benefit of this is that multilingual users can view the dashboard in different languages.

Language Selection

On the top right corner, the language selector lists all the languages supported by the dashboard.

Use the selector to choose the language you want to use for displaying, content on the dashboard.

Supported Languages

The dashboard supports all of the following languages.

- United States(English)
- Australia(English)
- India (English)
- Japan (Japanese)
- Spain(Spanish)
- Taiwan(Chinese)

8.3.2 Endpoint Application

Application Elevation

Application Elevation policy is a management method that assures that users have no access to any of the applications unless such access has been explicitly granted.

It enables the configuration of privileges so that users can request privilege elevation at specific times, for a duration of time, and on certain endpoints for required applications.

ARCON | EPM admin has full right to limit the time duration for which approvals are valid.

EndUser/Endpoint: When a user wants to elevate an application to the endpoint. They can right-click on the application and raise an elevation request EPM → Request for Elevation.

Once done a pop-up appears with a message **EPM: Raise Elevation request**.

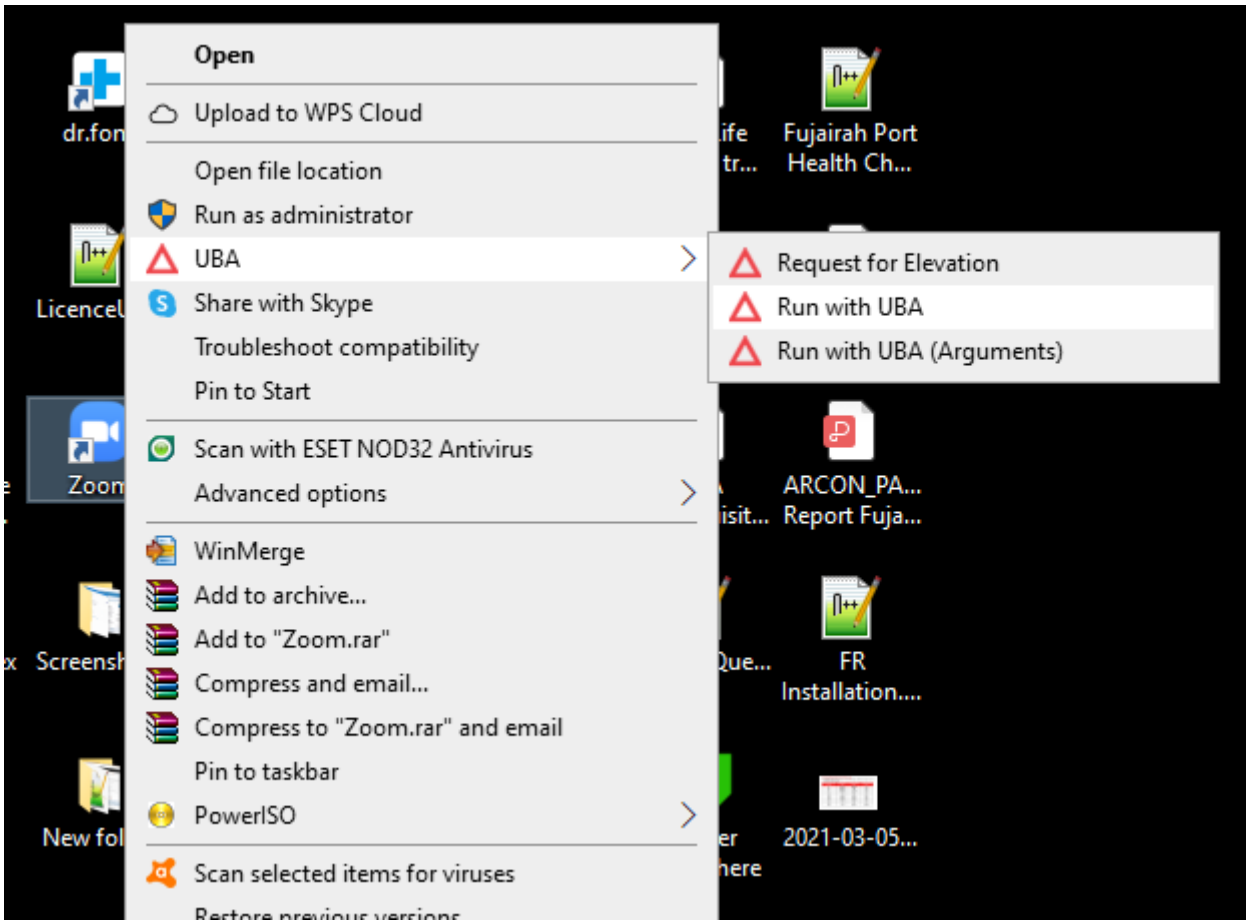
Refer to the following table and specify fields in the pop-up to submit an elevation request:

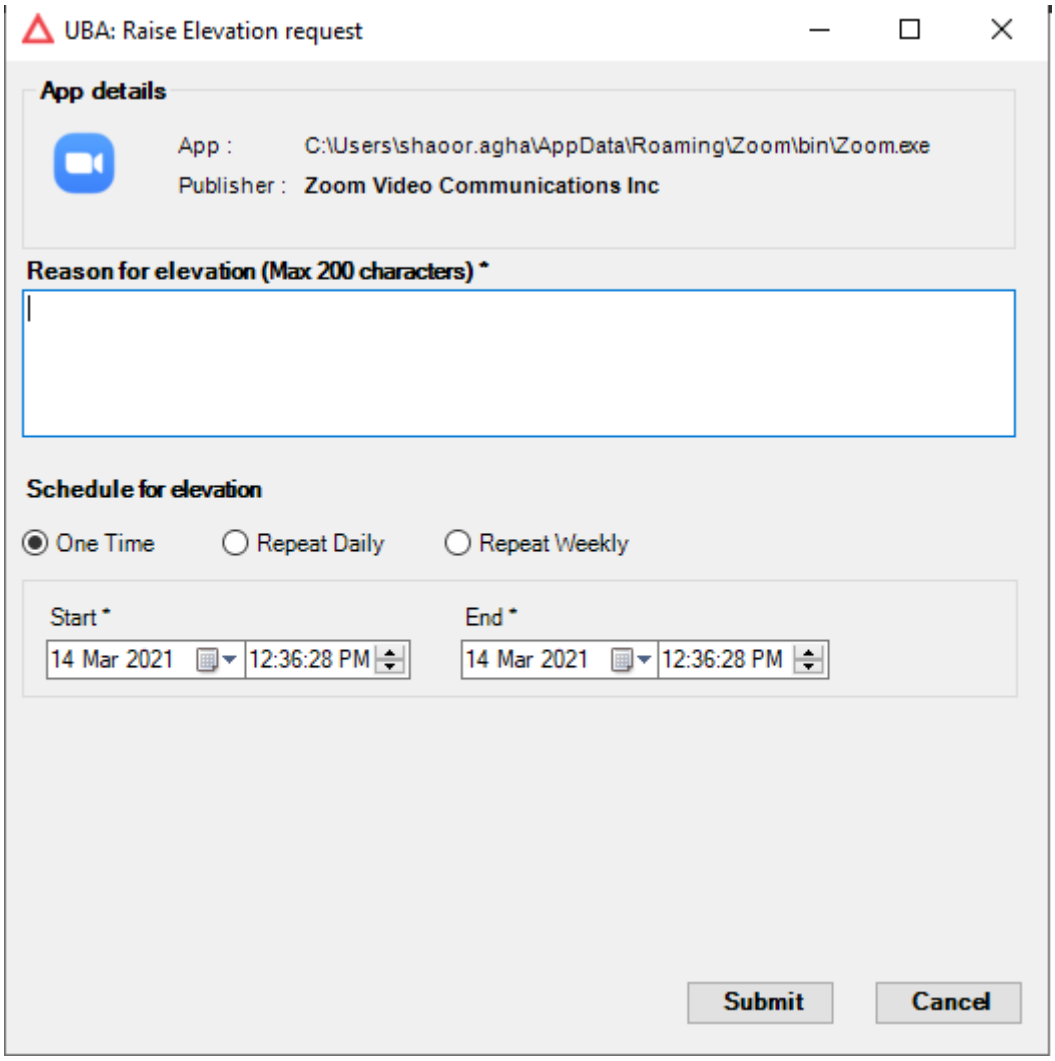
Field	Description
App	This field displays the application path
Publisher	This field displays the publisher's name
Reason for elevation(Max 200 characters)	Fill out a **reason** for the **elevation**

Schedule for elevation

Refer to the following table to understand each of the fields in the Schedule for elevation section:

Field	Description
Once Time	If you Select this radio button , the request will be raised for one time **Start** *: Enter the Start Date / Time **End***: Enter the End Date/ Time
Repeat Daily	If you Select this radio button, the request will be raised for daily on a particular day of the week Start *: Enter the Start Date / Time End*: Enter the End Date/ Time Check the day of the week from the weekday picker
Repeat Weekly	If you Select this radio button, the request will be raised for weekly for the selected days of the week Start Time*: Specify the Start Time End Time*: Specify the End Time Check the day of the week from the weekday picker
Submit	Click the Submit button to submit the request
Cancel	Click the Cancel button to cancel the request

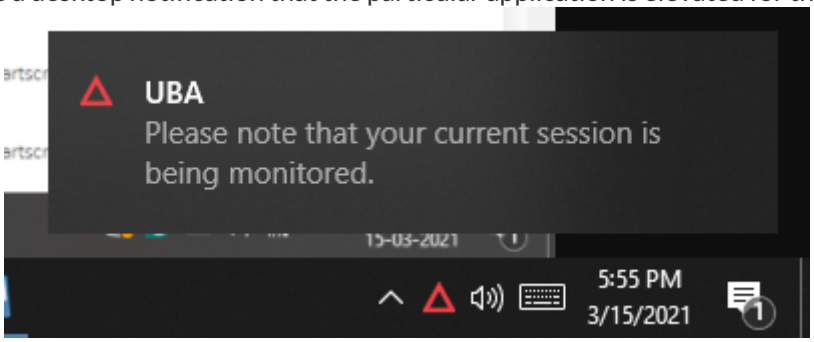

Open
Upload to WPS Cloud
Open file location
Run as administrator
UBA
Share with Skype
Troubleshoot compatibility
Pin to Start
Scan with ESET NOD32 Antivirus
Advanced options
WinMerge
Add to archive...
Add to "Zoom.rar"
Compress and email...
Compress to "Zoom.rar" and email
Pin to taskbar
PowerISO
Scan selected items for viruses
Request for Elevation
Run with UBA
Run with UBA (Arguments)
Fujairah Port Health Ch...
ARCON_PA... Report Fuja...
FR Installation....
2021-03-05...

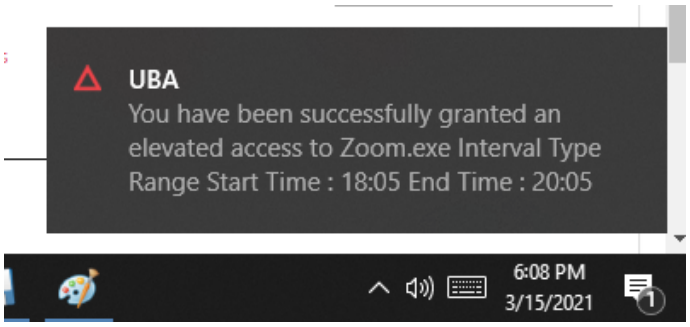


8.3.3 Endpoint Notification Centre

The endpoint notification center alerts end-user that they are being monitored every time they start the system. When an end-user raises an elevation request for accessing a particular application. And when it is approved from the EPM console.

End-user will receive a desktop notification that the particular application is elevated for the user.





8.3.4 Password Vault Report

The Password Vault Report shows last password change history. It also helps in tracking passwords to expire and password view report.

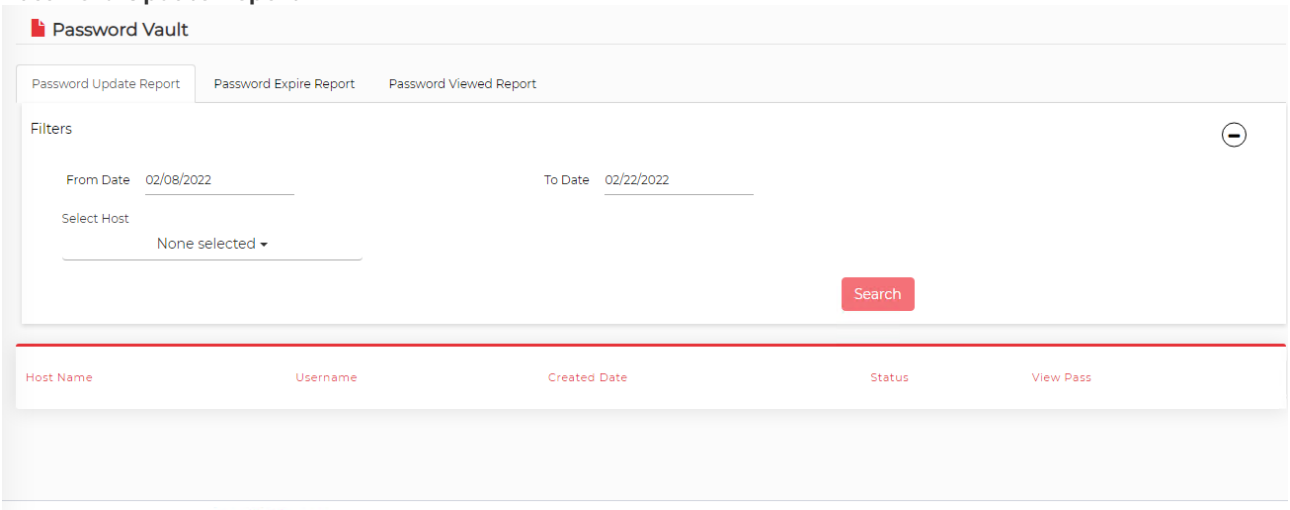
Note that the Filters are common across all three reports shown below.

Filters

Refer to the following table to understand each of the filters in the Password Vault Reports:

Field	Description
From Date	**Enter** the from date
To Date	**Enter** the to date
Select Host	**Select** the host name from the dropdown
Search	**Click** on search button

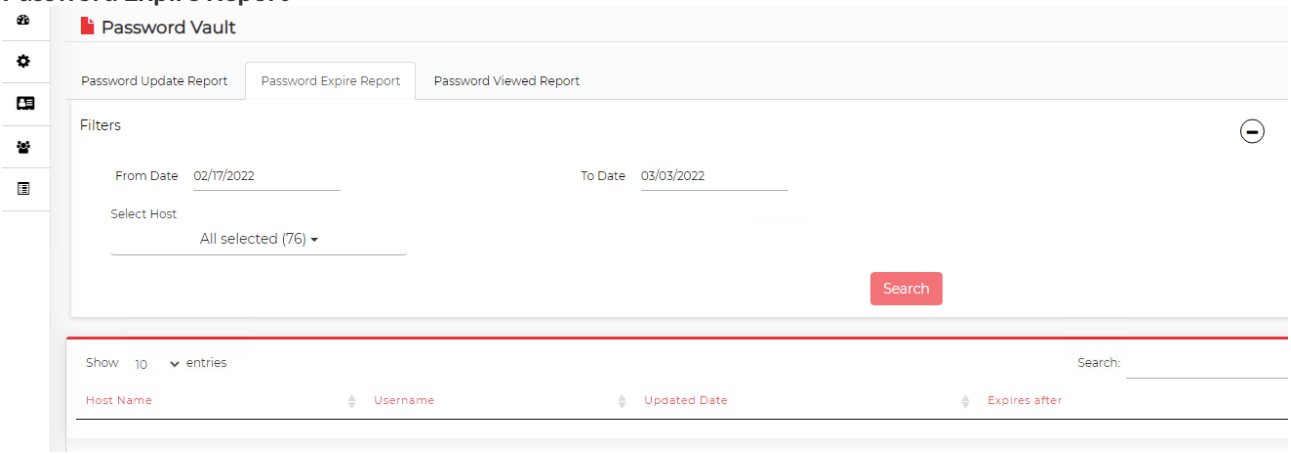
Password Update Report



Refer to the following table to understand each of the columns in the Password Update Report:

Field	Description
Host Name	This field will reflect the name of the host
User Name	This field will reflect the name of the user name
Created Date	This field reflects the password created date
Status	This field will reflect the status of the password
View Pass	This field allows the admin to view the password

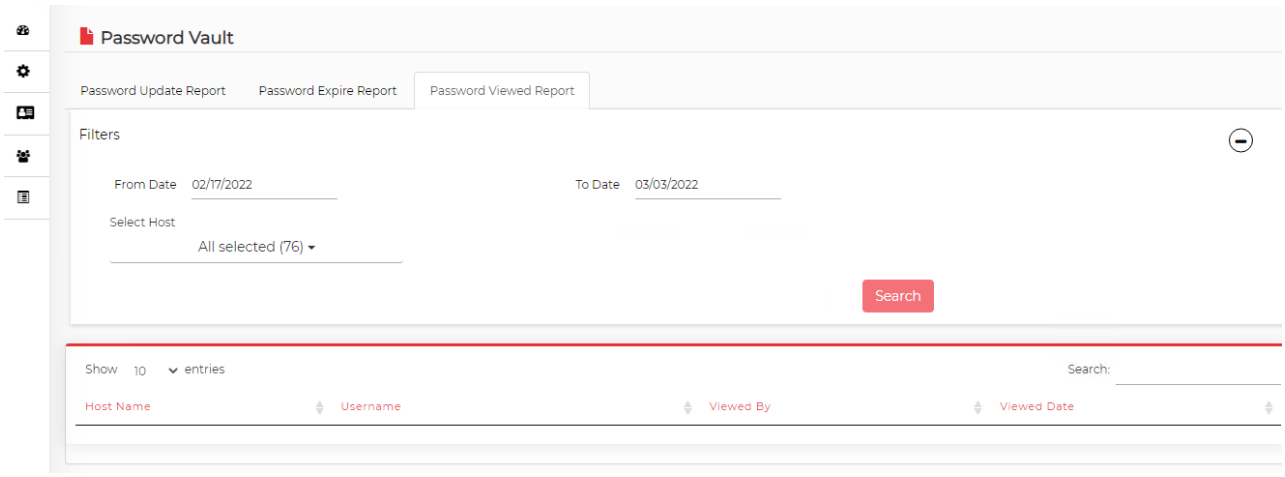
Password Expire Report



Refer to the following table to understand each of the columns in the Password Expire Report.

Field	Description
Host Name	This field will reflect the name of the host
User Name	This field will reflect the name of the user name
Updated date	This field reflects the date of password updated
Expires After	This field reflects the expire date of the password

Password Viewed Report



Refer to the following table to understand each of the columns in the Password Viewed Report.

Field	Description
Host Name	This field will reflect the name of the host
User Name	This field will reflect the name of the user name
Viewed By	This field reflects the viewed host name
Viewed Date	This field reflects the viewed date of the password

8.3.4.1 Elevated Apps

The end-user can right-click on the system tray icon, and click on Show All Elevated Applications icon, a form named EPM All Elevated Apps opens up it shows the list of all elevated apps.

The EPM All Elevated Apps form exhibits the following fields:

Field	Description
Application name	This field displays the name of the elevated application
Publisher	This field displays the Publisher of the elevated application
Requested on	This field displays date when the elevation request was raised
Approved on	This field displays date when the elevation request was approved
Schedule time	This field displays scheduled time for which the elevated application can be accessed

8.3.4.2 Elevated Apps

End-user can raise multiple elevation requests for the same application by specifying different dates and times and sending for admin approval.

Once it is approved by the admin end-user can run the elevated application on those specified days.

8.3.4.3 Facial Recognition - Endpoint

Facial Recognition authentication captures and detects the face of the end-user after every 5 minutes (by default) or the interval specified to verify/authenticate. If the assigned end-user is using the endpoint, an image must be assigned to the end-user.

This feature at the endpoint allows the self-registration of the end-user to capture his/her real-time image and upload it for the admin approval to be used for Facial Recognition. Else, the Admin has to upload an end user's image to allow facial recognition authentication.

The end-user will adjust the camera to fit the face in the frame and submit it to self-register.

Facial Recognition Test: The end-user can also do easy troubleshooting so that he/she can verify their captured face and camera on the endpoint before uploading the final image.

9 RDPS

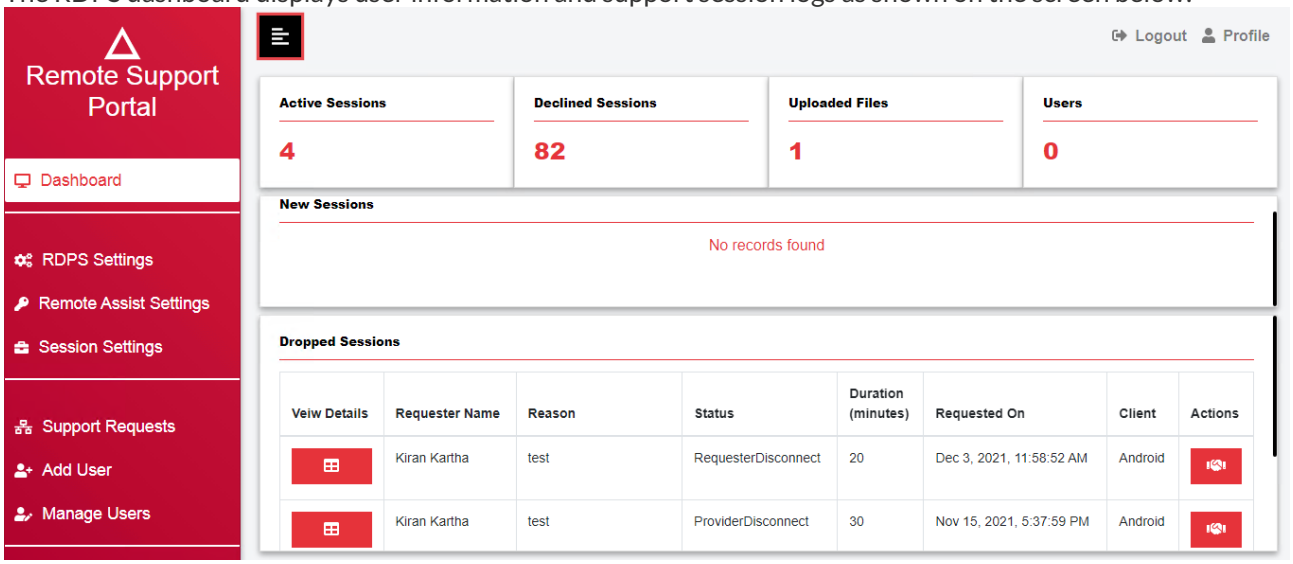
RDPS is also known as Arcon Remote Support Portal. RDPS can be used to provide remote support to the endpoint users.

RDPS provided following features:

1. The RDPS Portal allows administrators to provide remote support to the end users by taking remote sessions of the end point.
2. End point users can request for support, and administrators can provide support by accepting that request.
3. When administrator takes session of an end point machine via RDPS, end point user is elevated to the Admin group for that session duration, and administrator can easily perform admin activities without using any kind of passwords.
4. Every session can be monitored and logs of session are maintained.
5. RDPS allows to transfer files between admin machine and Windows endpoint machines. The RDPS supports Android and Windows devices.

9.1 RDPS Dashboard

The RDPS dashboard displays user information and support session logs as shown on the screen below:



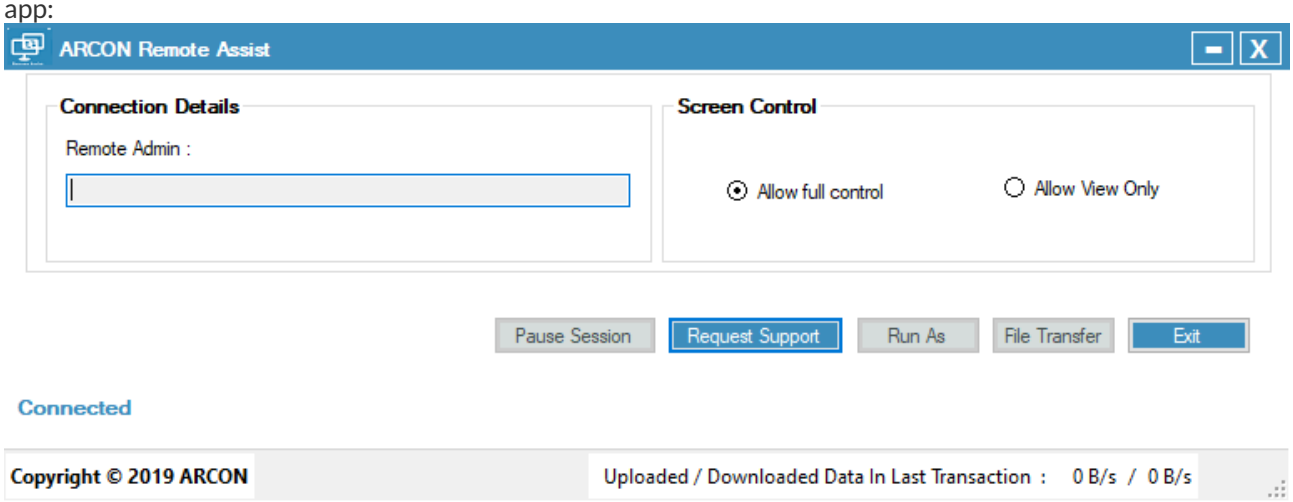
Refer to the following table to understand each of the fields in the RDPS dashboard's first section:

Field	Description
Active Sessions	This field displays the number of active sessions of the user support requests
Declined Sessions	This field displays the number of declined sessions of the user support requests
Uploaded Files	This field displays the number of uploaded files for the user
Users	This field displays the number of RDPS Portal users

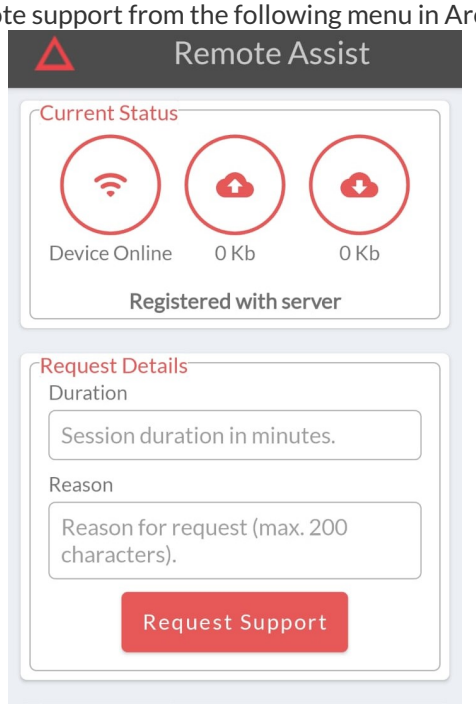
9.1.1 New Sessions

The New Sessions section displays the new requests initiated by users.

Windows users can crate new request for the support from the following Remote Assist menu in remote assist app:



Android users can request for remote support from the following menu in Arcon Remote assist app:



9.1.2 Dropped Sessions

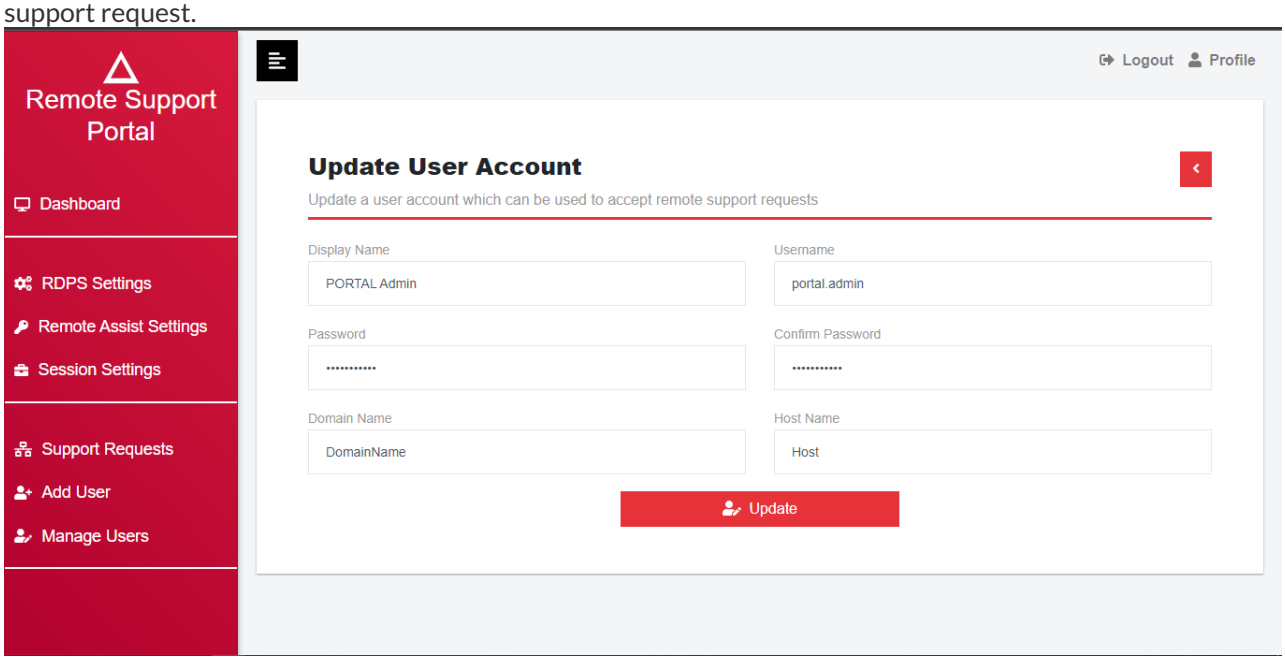
Refer to the following table to understand the data displayed in each column in the Dropped Sessions section:

Field	Description
View Details	This field displays requester and the request details in the view details

Field	Description
Requester Name	This field displays the requester name (user)
Reason	This field displays the reason of the request
Status	This field displays the status of raised request
Durations (minutes)	This field displays the turn around time to complete the action
Requested On	This field displays the request raised time and date
Client	This field displays the client details
Action	 Click on this icon to accept the request

9.2 Profile

This RDPS Profile module allows you to update the user account fields, which can be used to accept the remote support request.



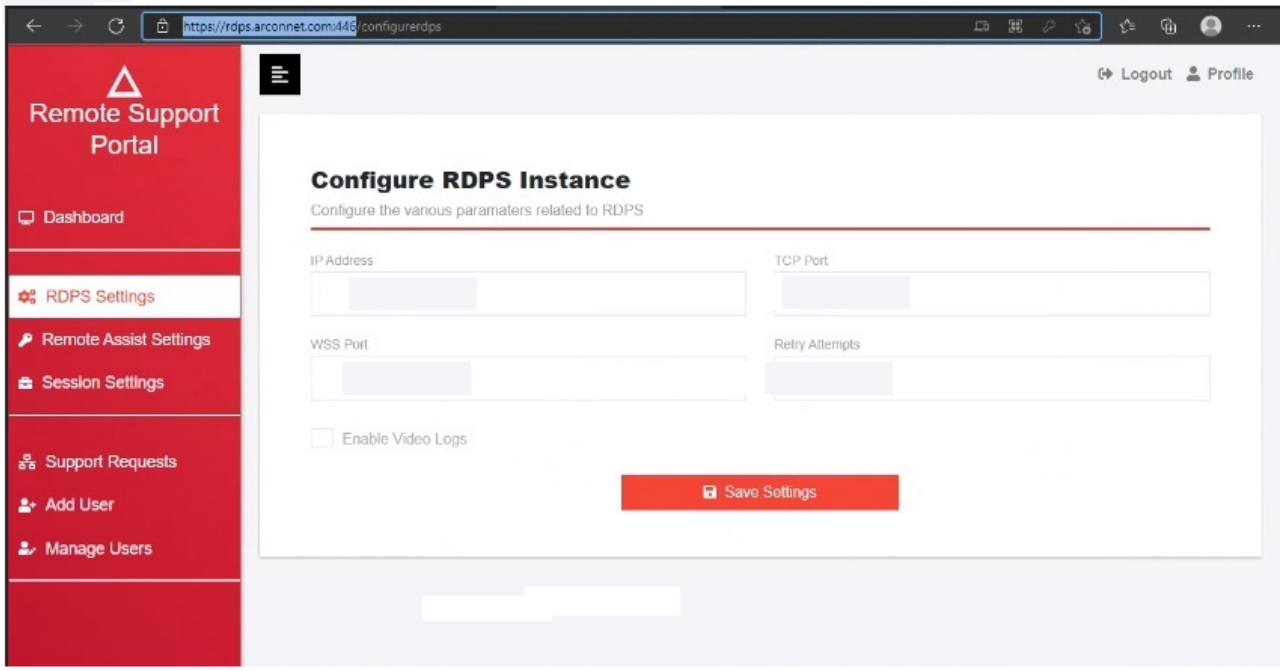
The Profile has the following fields:

Fields	Description
Display Name	This field is for common display name of user
Username	This field is for user name

Fields	Description
Password	This field is to input new password
Confirm Password	This field is to confirm new password
Domain Name	This field is for domain name of user
Host Name	This field is for host name of user

9.3 RDPS Setting

Through RDPS Setting, various parameters related to RDPS can be configured. RDPS Service is a supporting service used by RDPS portal on server side.



Refer to the following table to understand each of the fields in the Configure RDPS Instance:

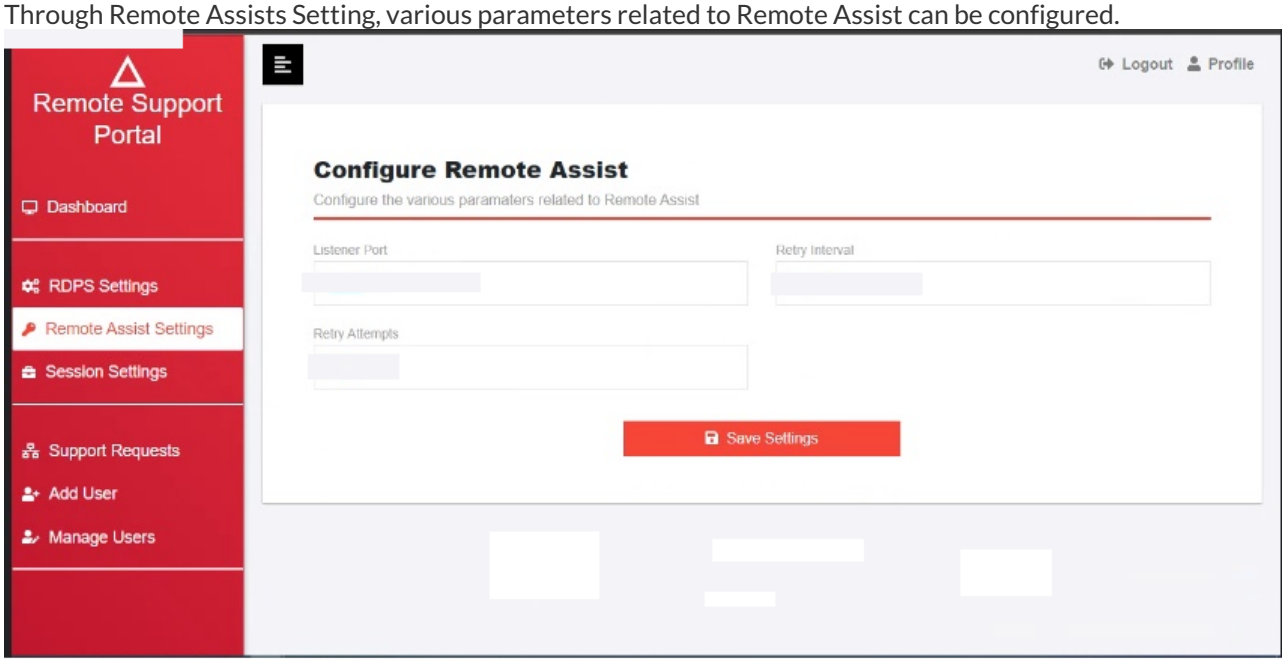
Field	Description
IP Address	This field displays the configured IP address of RDPS Portal
TCP Port	This field displays the TCP port number used by RDPS Service
WSS Port	This field displays the WSS port number used by RDPS Service
Retry Attempts	This field displays the number of retry attempts performed by RDPS service

Field	Description
Enable Video Logs	Enable the video logs button to record the remote session
Save Settings	Click on the save button to save the settings

9.4 Remote Assists Setting

Remote Assist refer to a connection that is intended to provide technical support from a distance. In this mode, a user can invite a technician to remotely access his/her computer and assist from a distant location. It is an application that is an add on to ARCON | EPM app on Windows endpoint which can be used to initiate the support request.

Through Remote Assists Setting, various parameters related to Remote Assist can be configured.

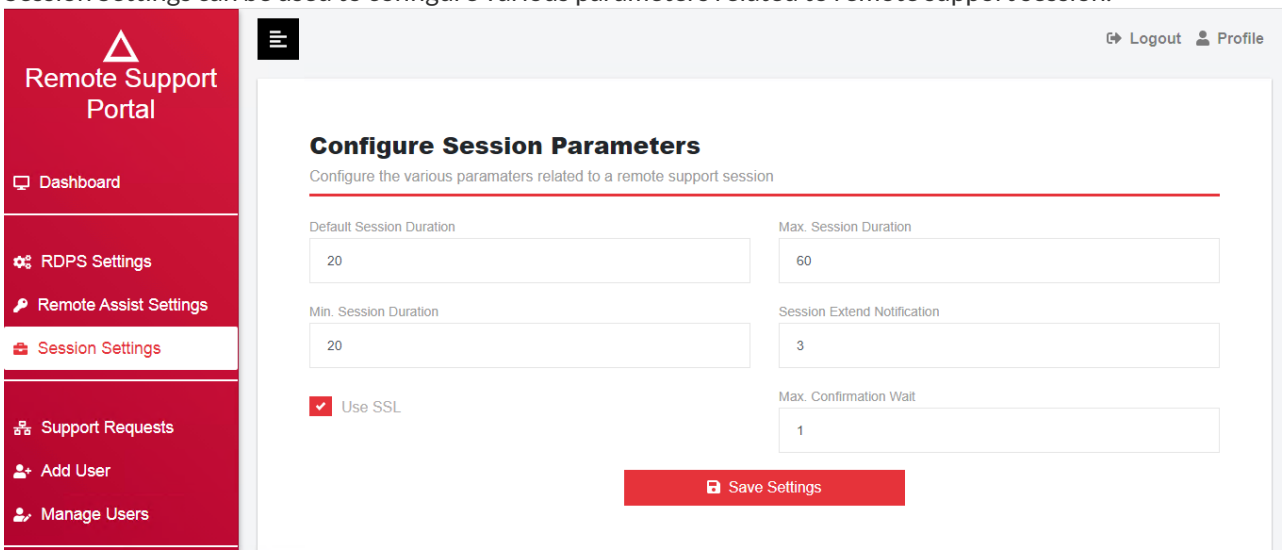


Refer to the following table to understand each of the fields in the Configure Remote Assists:

Field	Description
Listener Port	This field displays the Listener port address in the remote assist settings
Retry Intervals	This field is for retry intervals by remote assist
Retry Attempts	This field is for retry attempts performed by remote assist for the RDP connection.
Save Settings	Click on the save button to save the settings

9.5 Session Settings

Session Settings can be used to configure various parameters related to remote support session.

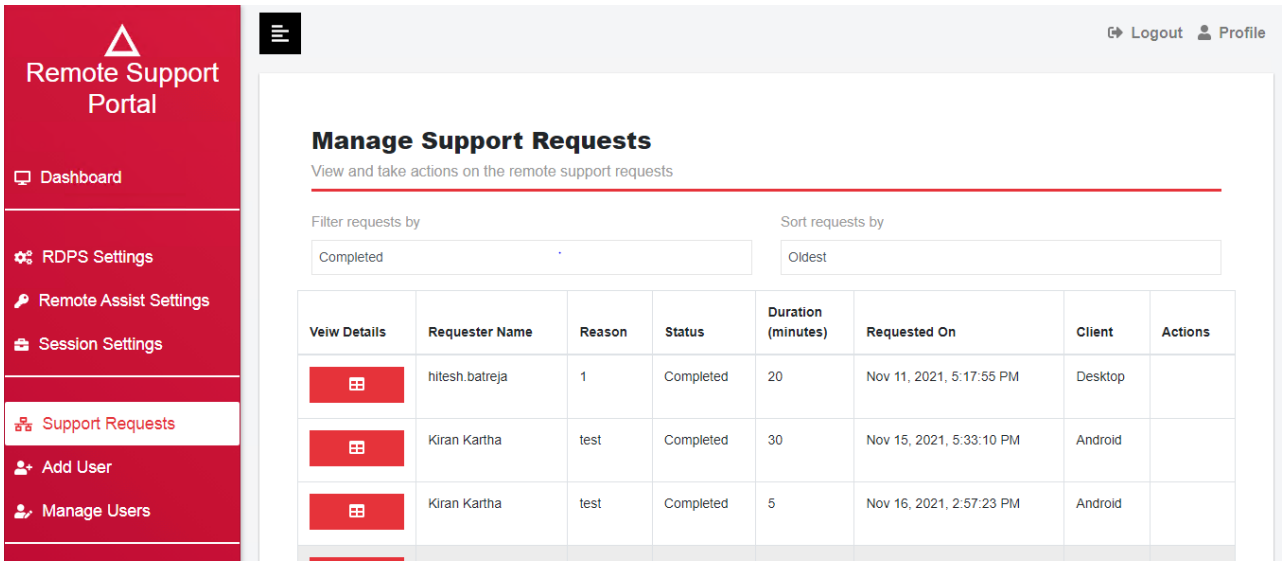


Refer to the following table to understand each of the fields in the Session Settings:

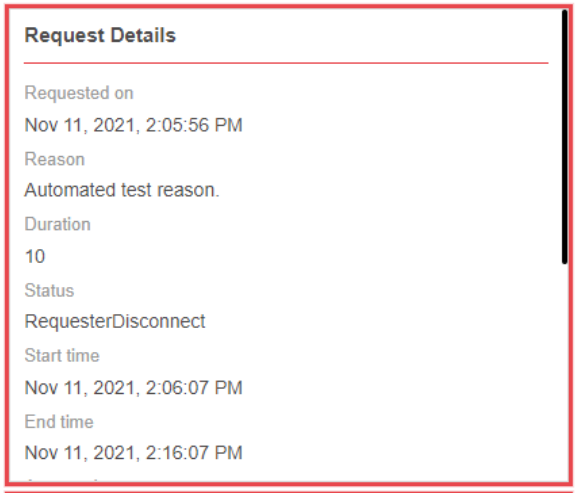
Field	Description
Default Session Duration	This field displays the default duration for remote support session.
Max. Session Duration	This field is to set maximum duration of remote support session.
Min. Session Duration	This field is to set minimum duration of remote support session.
Session Extended Notification	This field displays the time in minutes for session extended notification
Use SSL	This field can be checked to use SSL for RDPS Connection
Max. Confirmation Wait	This field displays maximum time in minutes for confirmation of support request.
Save Settings	This button is used to save updated settings.

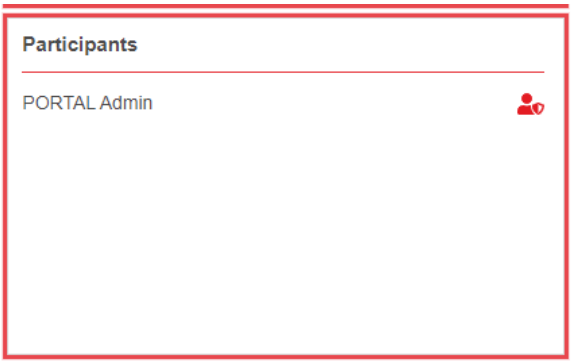
9.6 Support Request

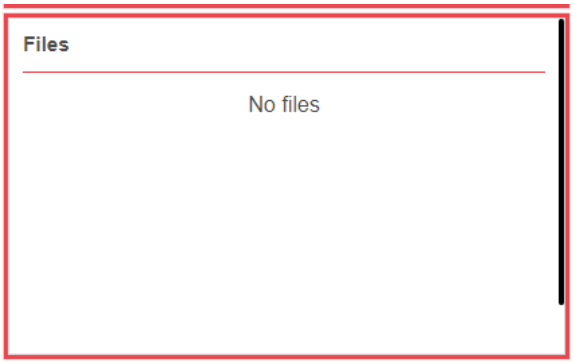
Support Request allows retrieving of support session information and and administrator can manage the requests. If the session has been disconnected or interrupted due to network issues administrator can retake the same session using actions.



Administrator can view details of support session which will be like following:





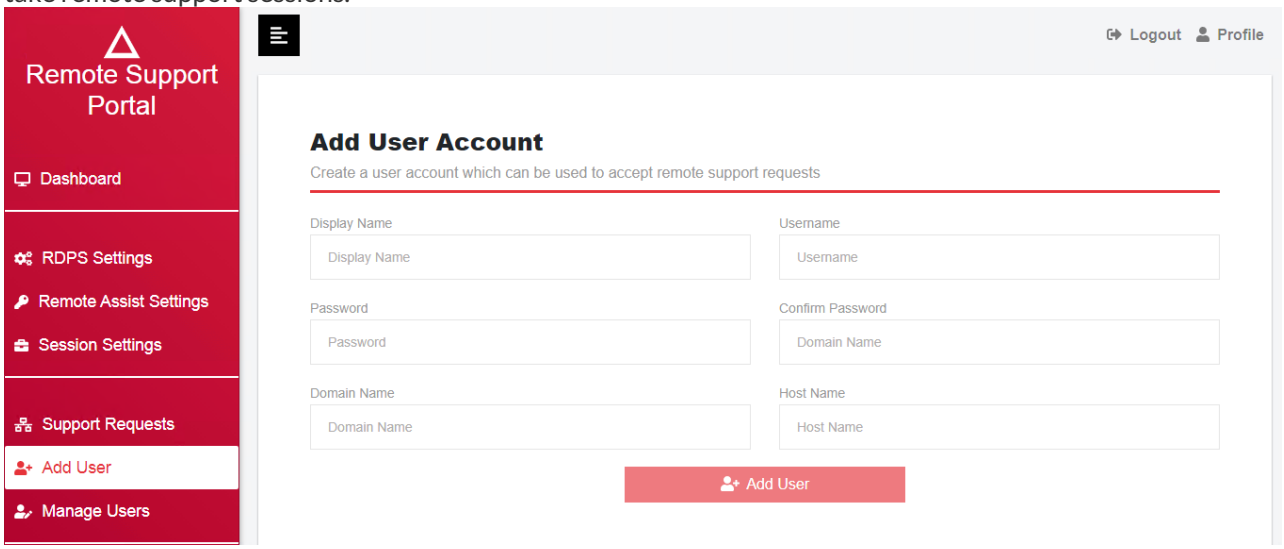


Detail Type	Description
Request Details	Provides the details of requested support session

Detail Type	Description
Requestor details	Provides the details of endpoint user and end point device
Participants	Provides the details of admins which accepted the support requests and took the remote support session.
Files	It displays the files which have been transferred to and from endpoint machine and RDPS Admin

9.7 Add User

Add User allows you to create a user account for RDPS Portal. These users can accept the support requests and take remote support sessions.



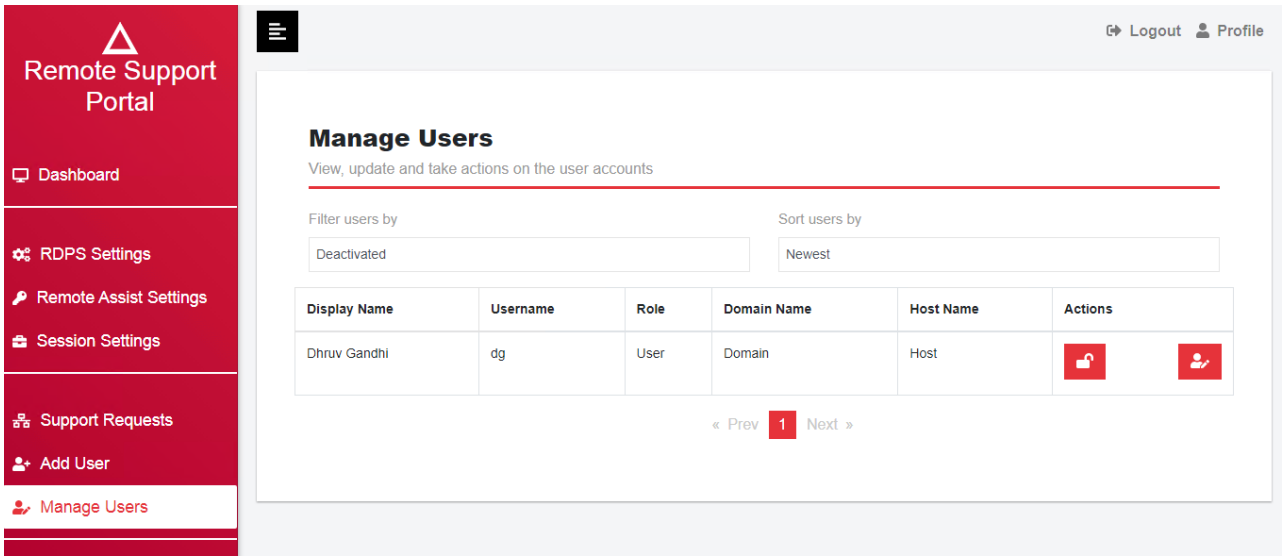
Refer to the following table to understand each of the fields in the Add User Account:

Field	Description
Display Name	This field is for the display name
User Name	This field is for the the user name
Password	This field for the new password
Confirm Password	This field is to confirm new password
Domain Name	This field for domain name of user
Host Name	This field for host name of user

9.8 Manage Users

Manage Users module allows RDPS portal administrators to view/update and take action on the user account.

Users can be filtered by their active status and administrator can take actions like activate or deactivate user and edit user details.

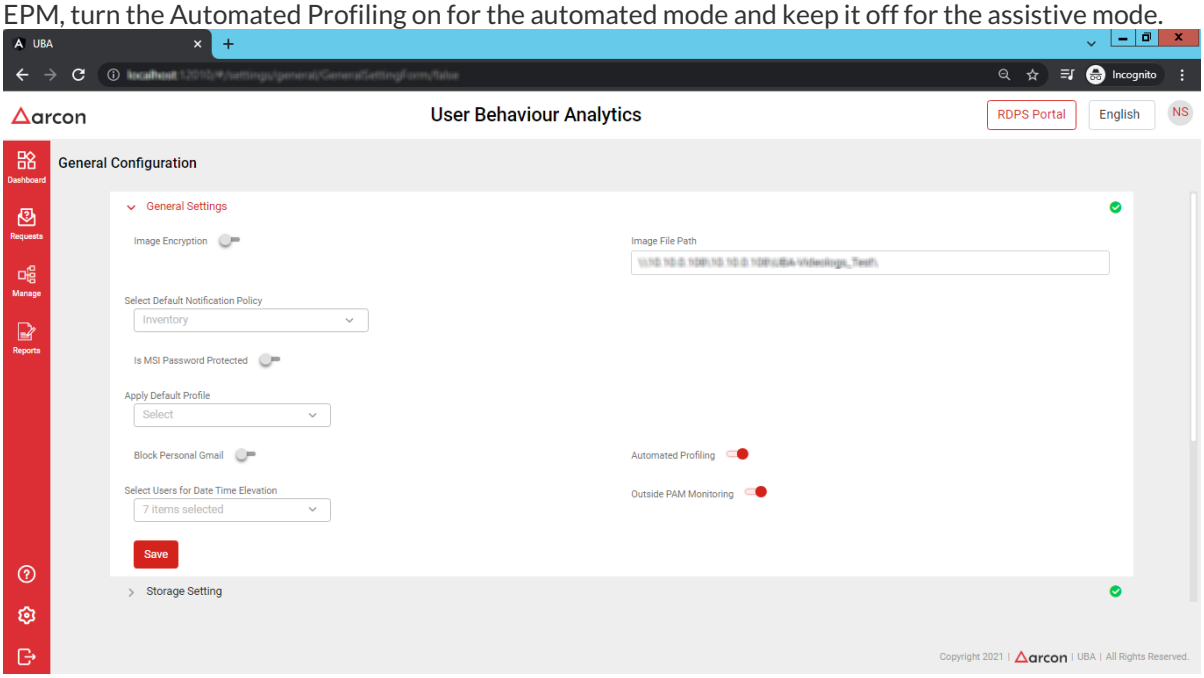

Remote Support Portal
Dashboard
RDPS Settings
Remote Assist Settings
Session Settings
Support Requests
Add User
Manage Users
Logout
Profile
Manage Users
View, update and take actions on the user accounts
Filter users by
Deactivated
Sort users by
Newest
Display Name
Username
Role
Domain Name
Host Name
Actions
Dhruv Gandhi
dg
User
Domain
Host
« Prev
1
Next »

10 Automated Profiling

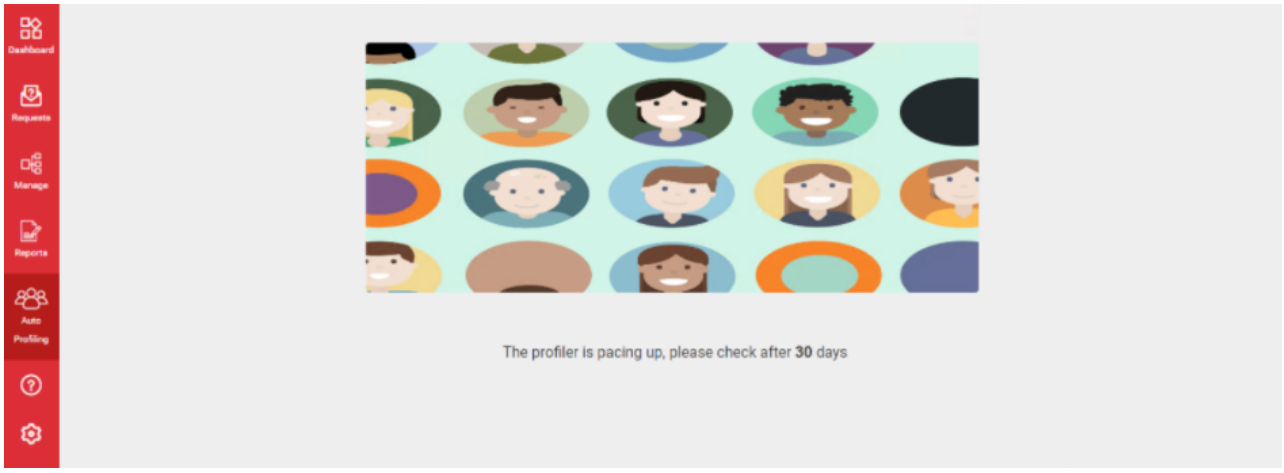
Automated Profiling automates the entire process of applying rules to the users. It groups the users based on their usage history and then assigns the processes that are most frequently used by that group.

Step Wise Configuration :

- Automated profiling is divided into two types : automated and assistive. In the global configuration of EPM, turn the Automated Profiling on for the automated mode and keep it off for the assistive mode.

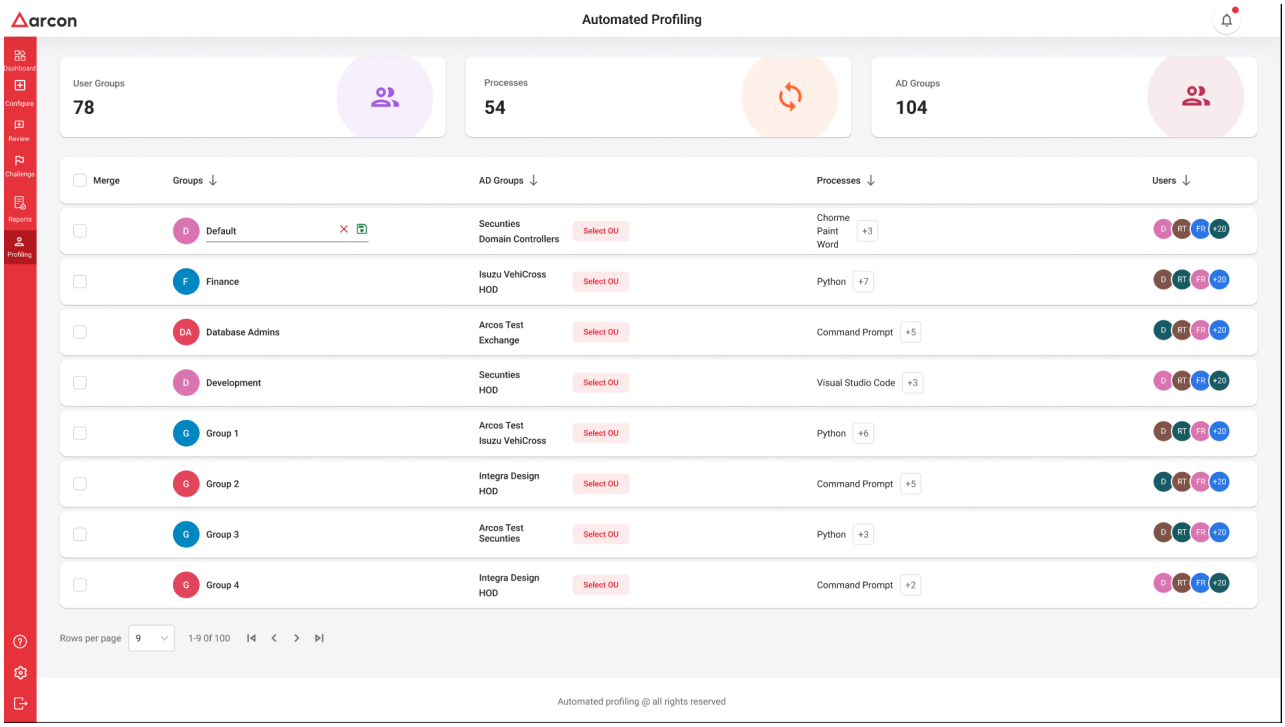


- For the first thirty days (configurable), the EPM runs normally while Automated Profiling is gathering the data and determining the profiles. No restriction is applied during this time.

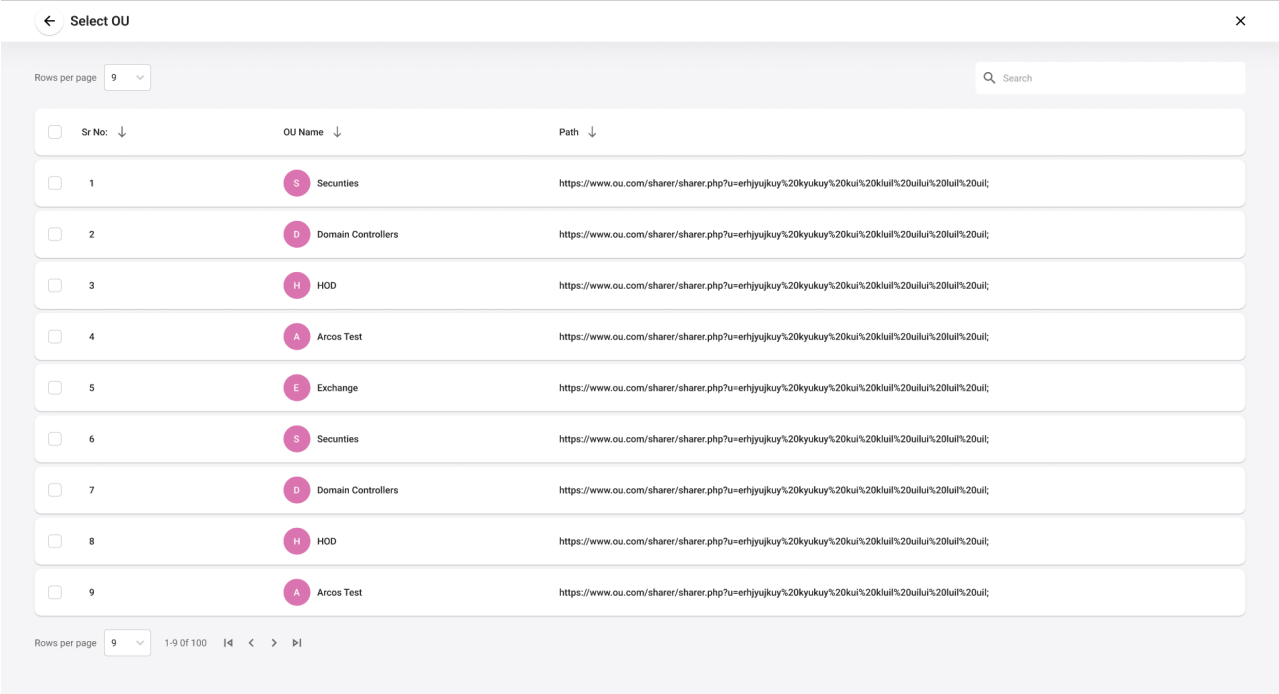


- After thirty days, the AP has determined the profiles based on the usage patterns of the user and has segregated the users into user groups.

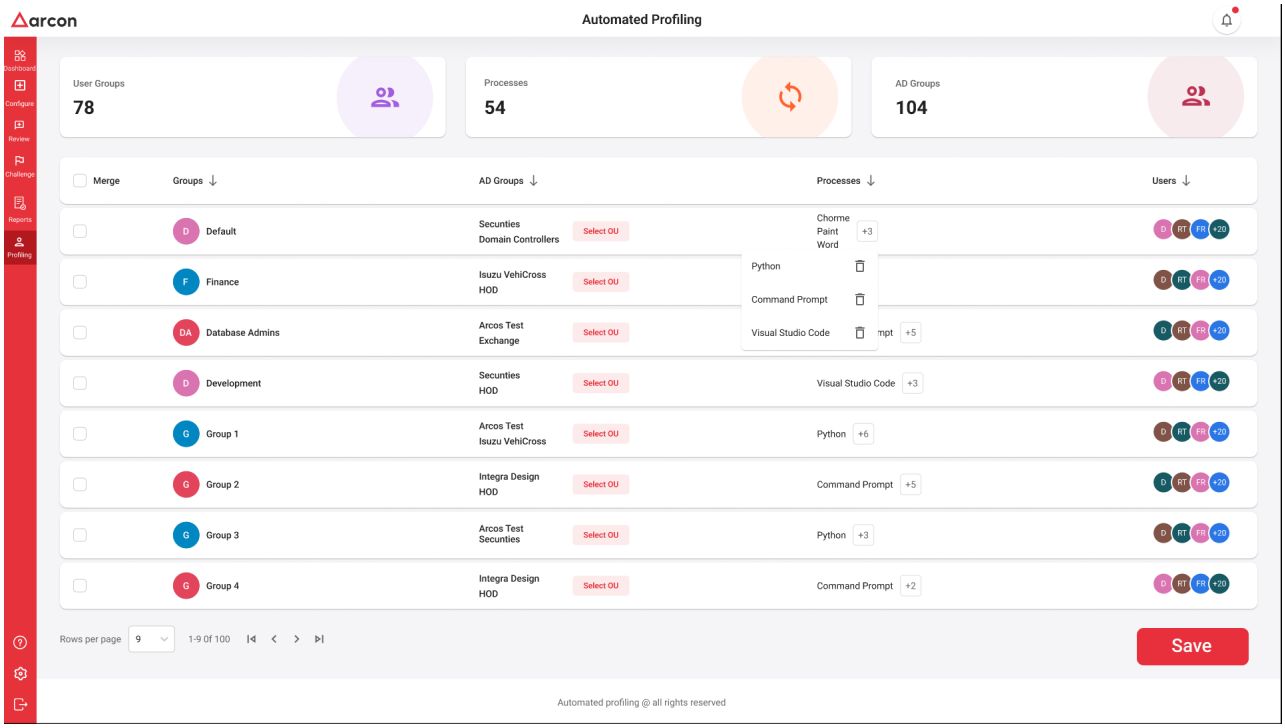
- Click on the profiling option in the main menu of EPM, it opens up the Automated Profiling page.



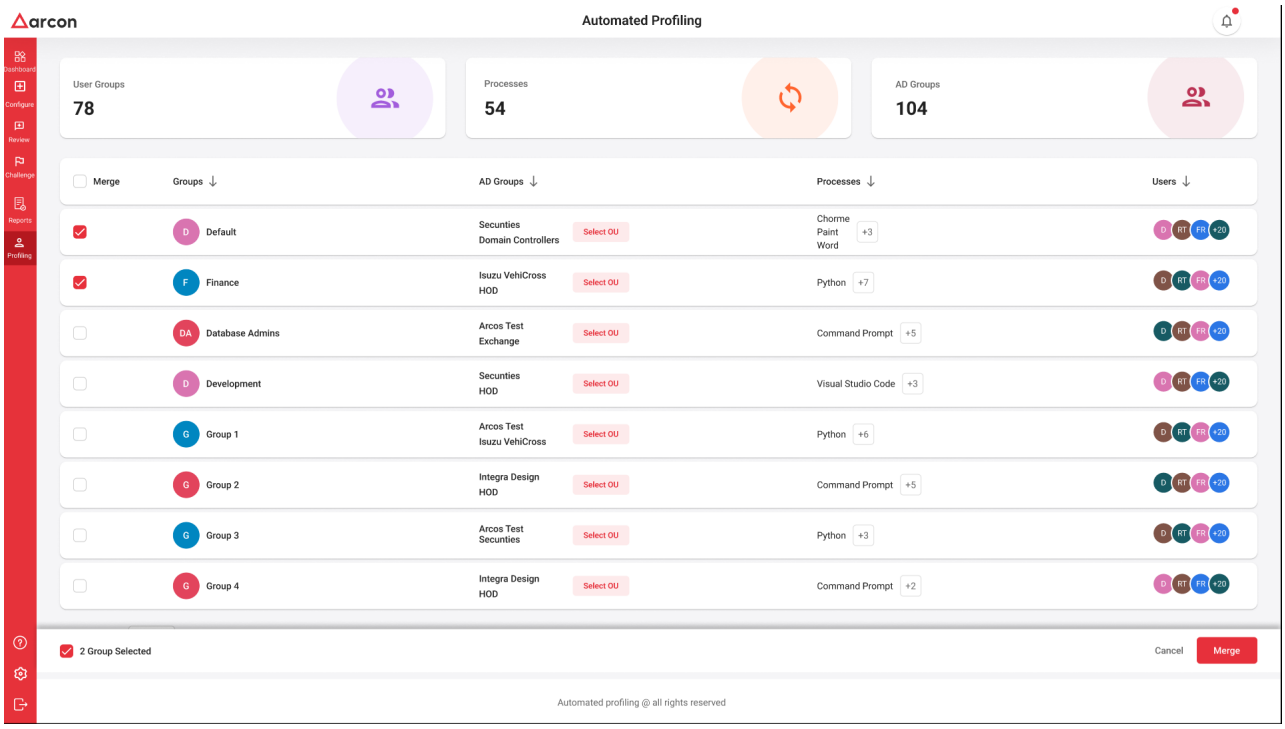
- The page is an interactive dashboard and it has the following contents:
  - User groups : Groups that are created automatically by the AP based on their process usage history, it has a default group which has a set of processes that are applied to every user. The user group names are editable fields.
  - AD groups : Active directory groups which are already present in the organization can be mapped to the generated User Group. This will help in auto assigning policy when a user is onboarded in the system from AD. One or more AD groups can be assigned to a generated user group. The AD group list is pulled from the domain configured in the global configuration of EPM. Click on select OU of the column and it opens a pop up to map the OU to Auto generated Group.



- Processes : This column has the processes that are most used by the users of the corresponding group. The processes that are listed here will be whitelisted for that group. The administrator can add/delete processes from the list.

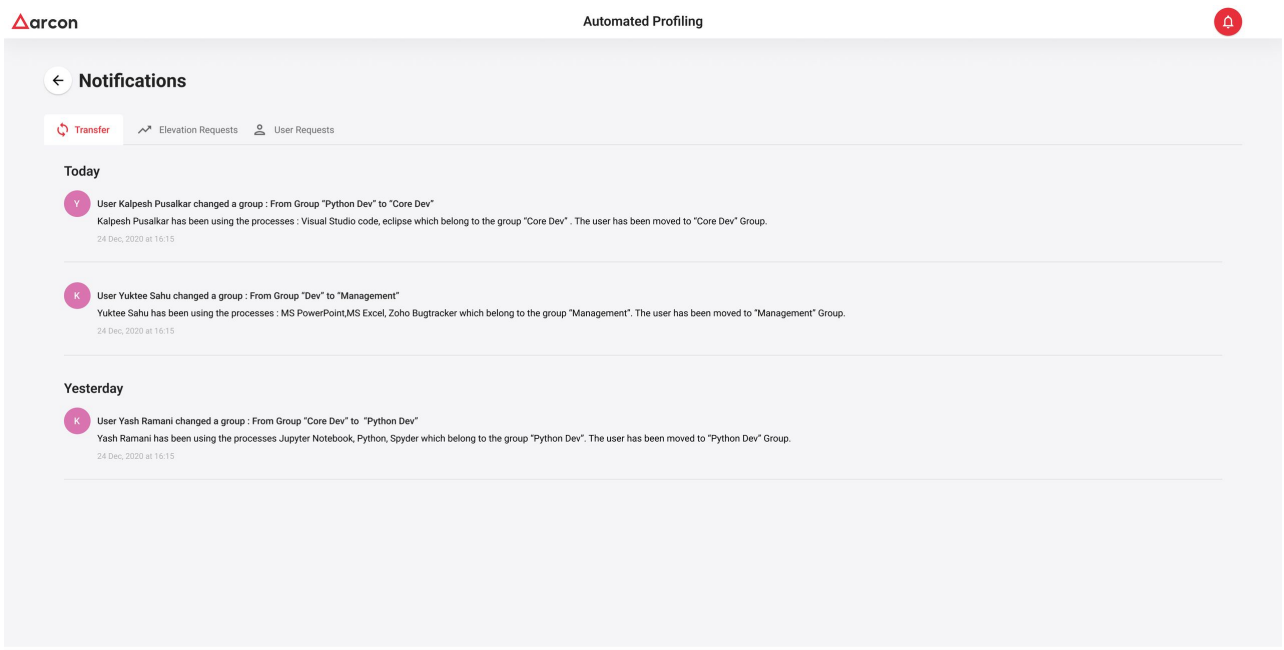


- Users : This column lists the users that have been identified to be part of the group. The Admin can also remove/add a user from the group.
- Additionally, using the “merge” option, the admin can also merge two or more groups into one.

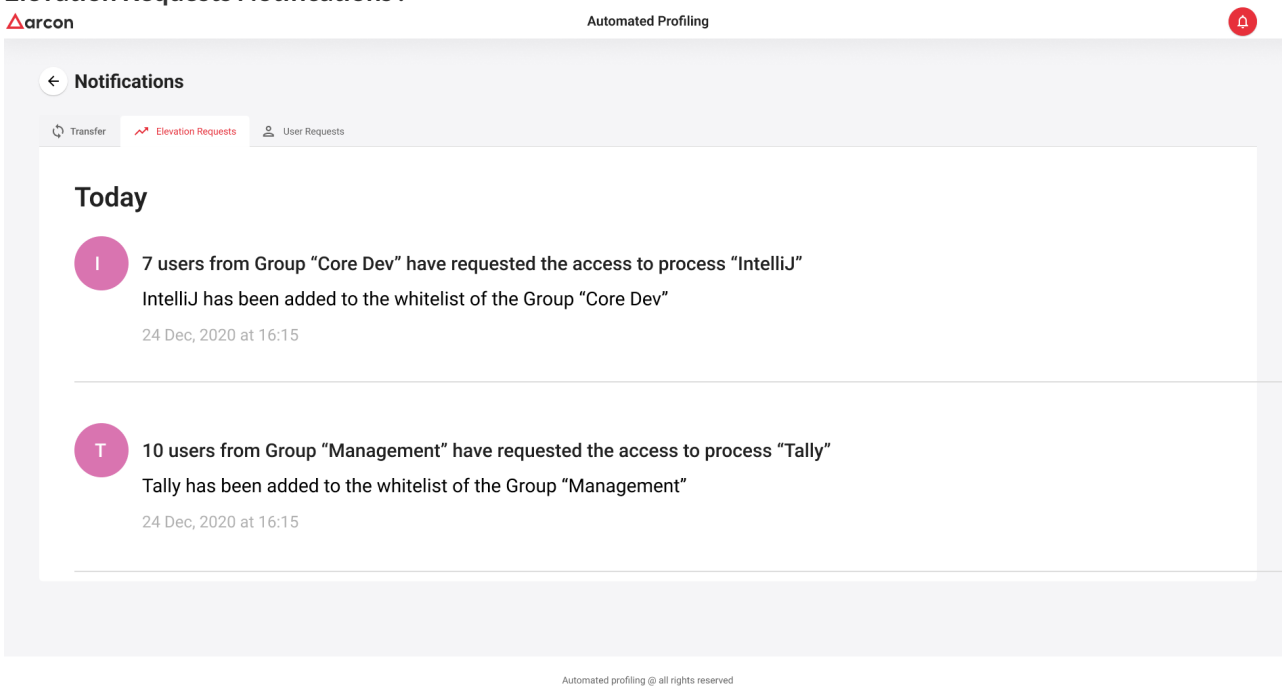


- There is a notification icon in the page, where there are three types of actions/notifications available.
    - Elevation Request: This notification indicates if a certain process which is not aligned to the group has been requested for elevation from more than 50 percent of the users of the group. Admin can add that process to the group or choose to not add it.
    - New User : The system notifies the admin if a new user is signed up in the organization. It initially assigns the default group to the user or if the AD group is specified then based on the rule written.
    - Group change : If the system detects a change in the usage pattern of the user, it notifies the admin for the same and the admin has an option to shift the user to another group.

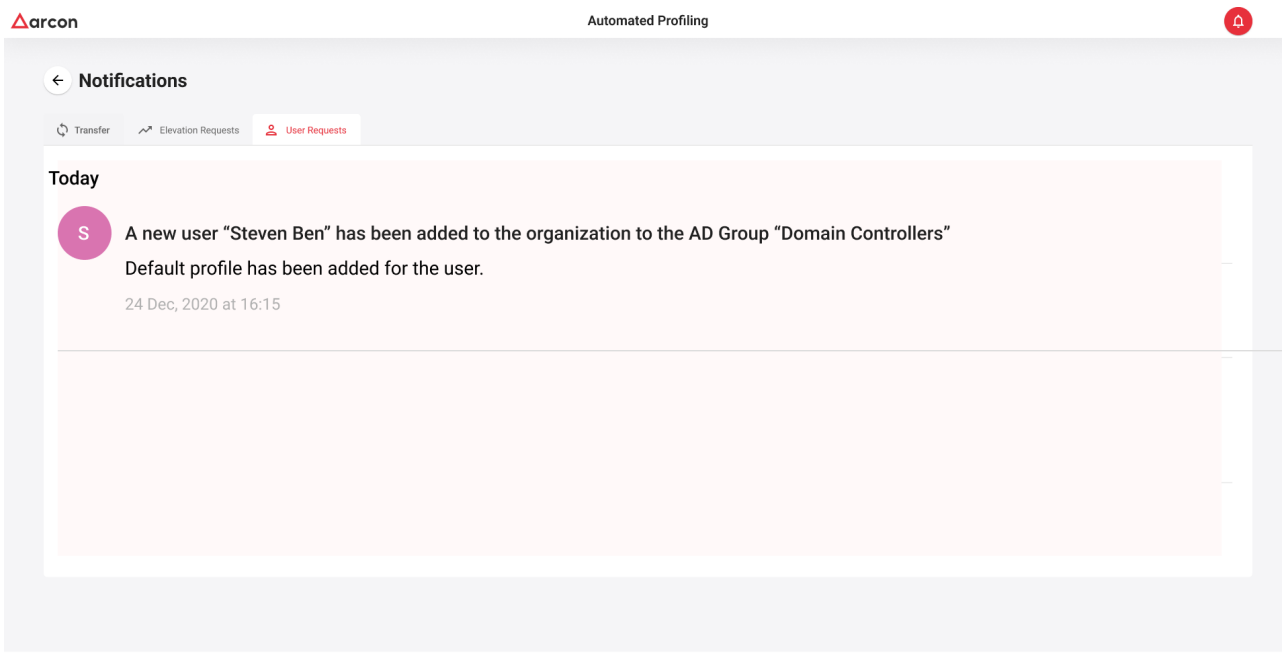
Group Transfer Notifications :



Elevation Requests Notifications :



New User Discovery Notification :


arcon
Automated Profiling
Notifications
Transfer
Elevation Requests
User Requests
Today
S
A new user “Steven Ben” has been added to the organization to the AD Group “Domain Controllers”
Default profile has been added for the user.
24 Dec, 2020 at 16:15
Automated profiling @ all rights reserved

11 Data Intellect

Need for Data Intellect

In recent times, we have gone past the stage of how oil used to be the most valued asset but Data at our fingertips is more powerful, important and obviously here to stay. Data is associated with every organization. As data evolves across different areas of business, it gives the organization endless opportunities to connect the missing dots and go for higher growth. The challenge for any organization is to get tangible benefits from the data (ex: financial, retail, sales data). Data organization is the practice of categorizing data to make it more usable. It is similar to arranging the data in the most logical and orderly fashion so that anyone who accesses it can easily find what they're looking for. Once identified as sensitive / important documents, the company administrator needs to restrict, control and monitor access. When looking at the mountain of data present in the organization, it becomes complex to pay attention to the crucial points like data categorization, its sensitivity, accessibility management, exposure analysis etc.

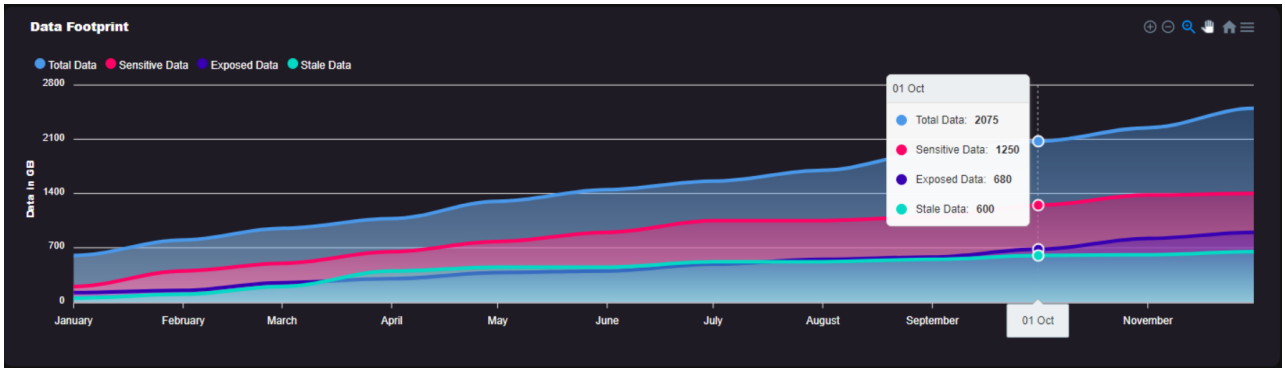
This is where the Data Intellect tool comes in. It categorizes the documents and amplifies data privacy, control and security. Each organization has its own particular relationship with its data, as well as specific needs for organizing and controlling access. Data Intellect, develops an active learning process from the documents present in the network.

The Data Intellect Solution

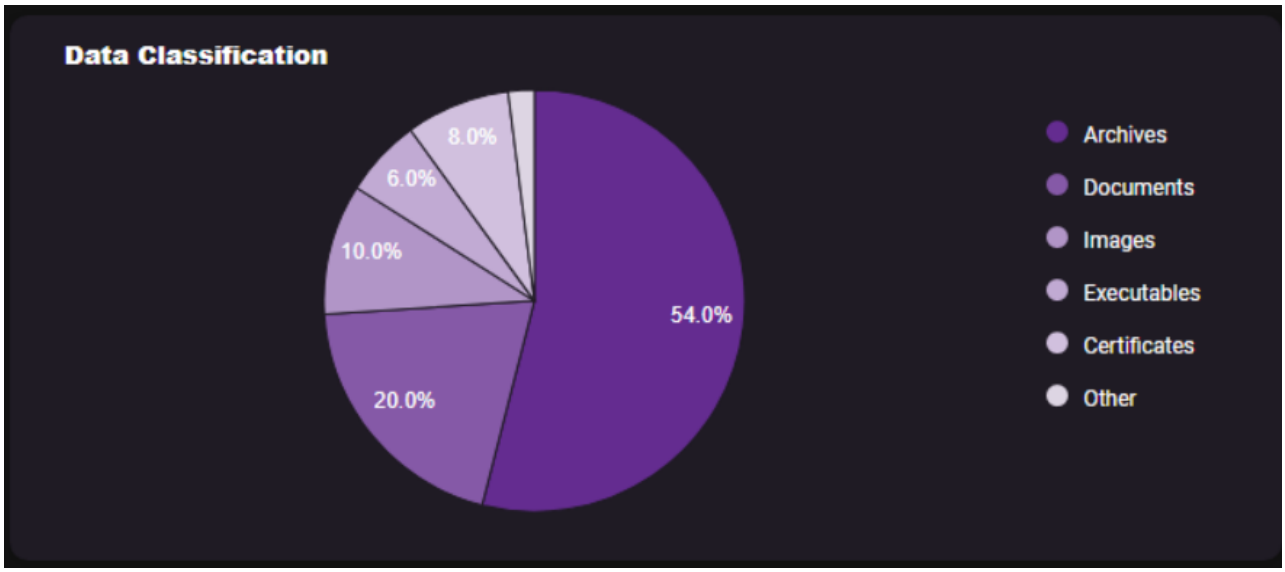
Data Intellect is an interactive analytical system, which uses state of the art Data Analysis techniques to provide deep insights into the magnanimous data of an organization. Data Intellect helps in visualizing the following:

- Global Data Summary: The tool scans through all the data and displays the count of documents and sensitive documents and their respective volumes across the organization.

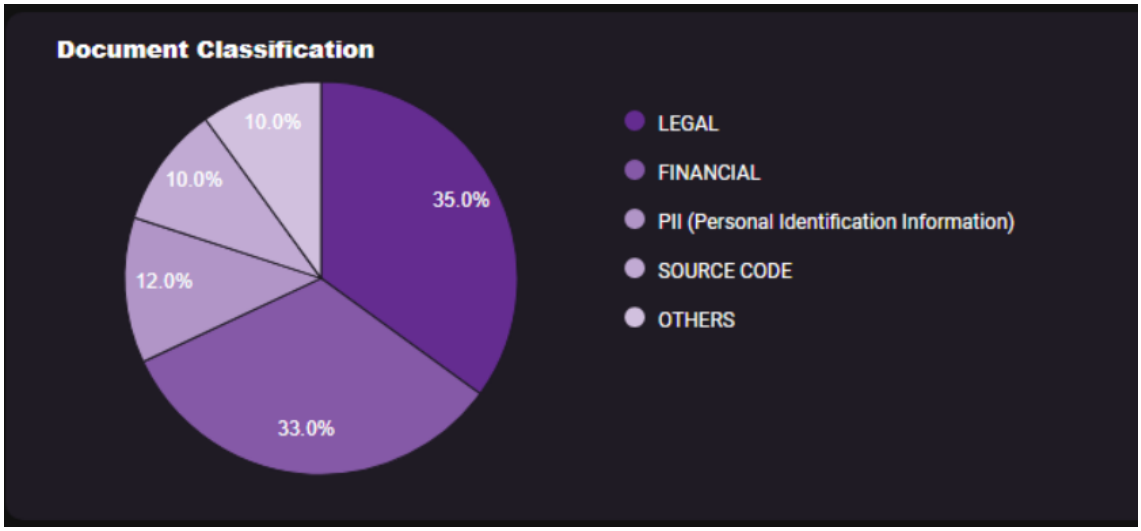
- Data Footprint : An overview is generated for the past 12 months, giving an insight of the total data size with respect to multiple datapoints such as:
    - Sensitive : The sensitivity of data is uniquely identified for an organization.
    - Exposed : Files shared by the users to other users increases the risk of data being exposed.
    - Stale : Stale data is expensive and unnecessary to store and manage.



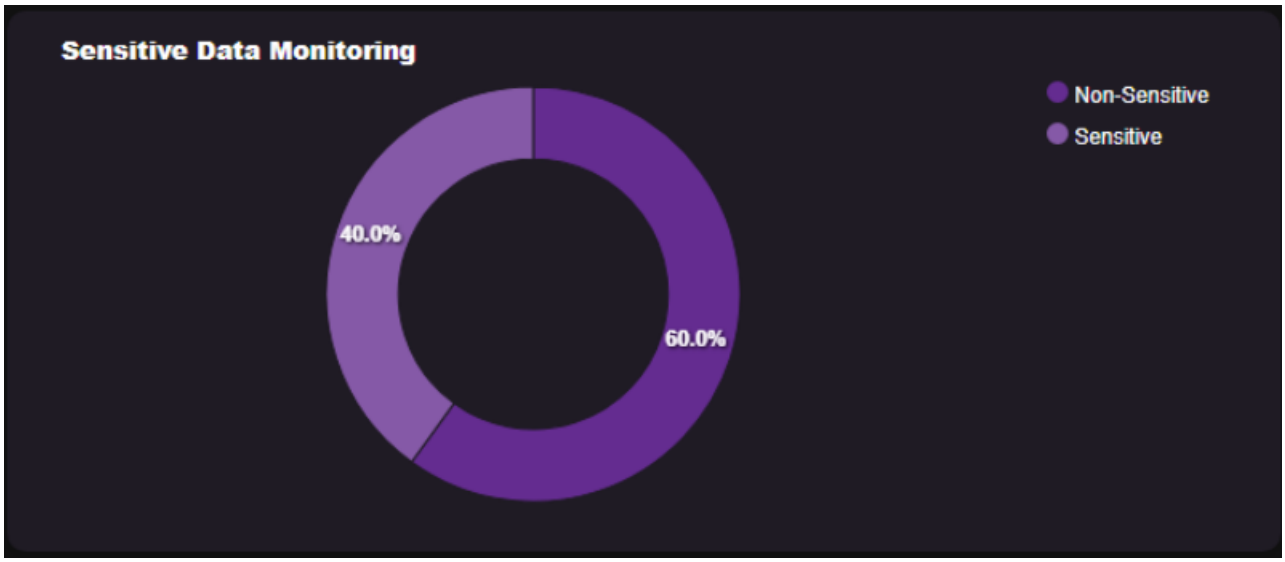
- Data Categorization : All the data is segregated into archives, documents, images, executables, certificates and others.



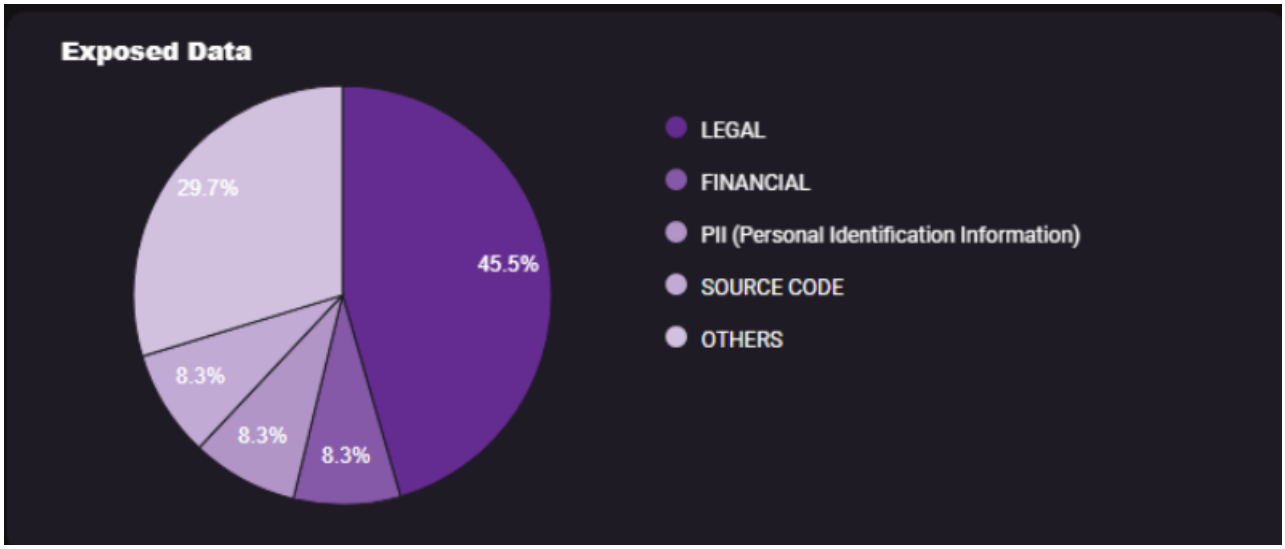
- Document Classification : The tool scans through documents in the organization and then classifies them into intuitive groups/classes like Legal, Financial, Personal Information Identifier, etc. These classes are pre defined as the Data Intellect Groups. This classification is done both on organizational and individual user levels.



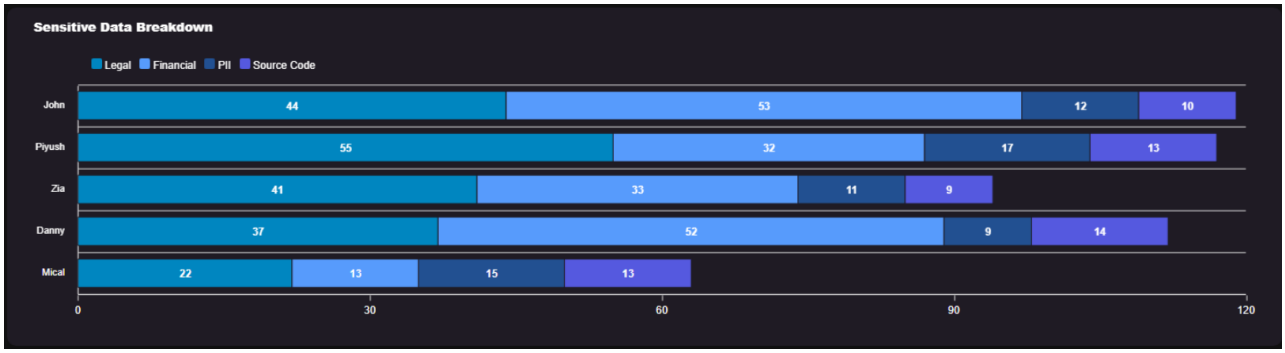
- Sensitive Data Monitoring : Sensitive data often contains the most private information about the organization as well as the user like personal data, credit card information, IP, emails and more.Sensitive data that is open to global groups presents a significant risk to the business and needs to be tracked. The system scans, classifies and monitors the sensitive data. The sensitive data is also marked into the Data Intellect Groups.



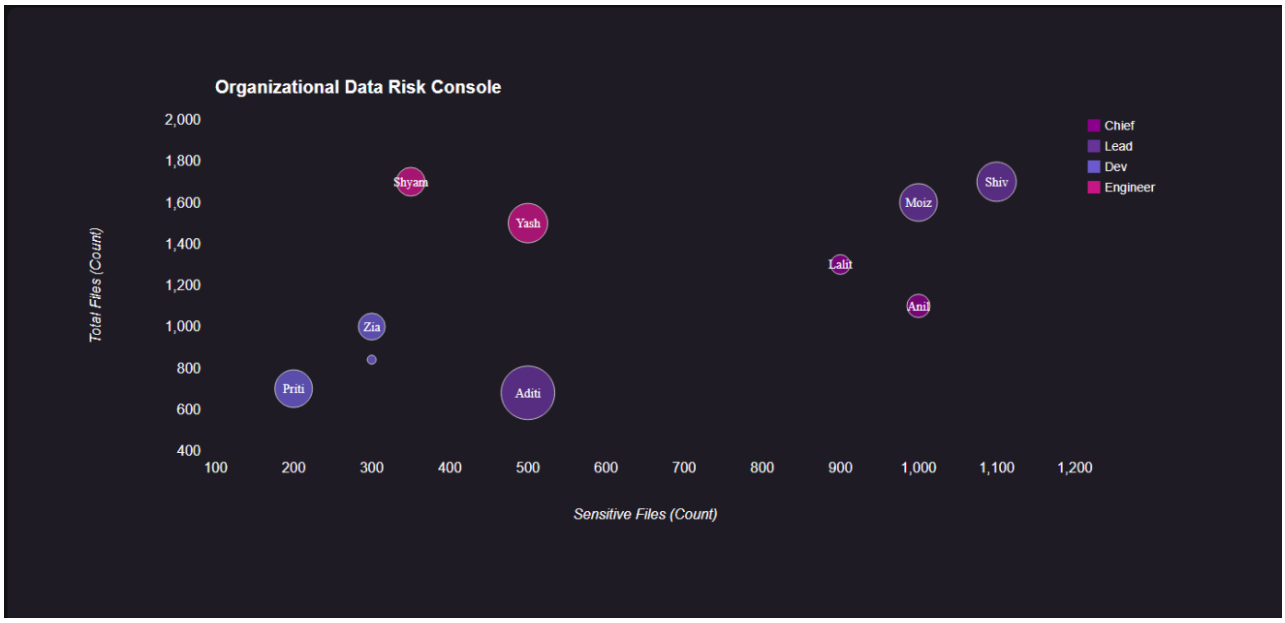
- Exposed Documents : The tool analyzes the exposure risk and categorizes w.r.t the Data Intellect Groups. Any document which is shared between multiple users is considered exposed.



- Sensitive Data Breakdown: A breakdown of total documents w.r.t the Data Intellect Groups for the top users having majority of sensitive data.



- Organizational Data Risk Console : A mapping of count of total files, sensitive files, percentage of exposed Data and the organization defined teams with respect to to each user in the organization. This console gives a broader perspective of all the data present in the organization in a simplistic graphical manner.



Future Roadmap.

1. Timeline Monitoring Capability for Documents : The system will be able to track the entire history and the flow of the individual document and will alert the administrator if any suspicious activity takes place.
2. User-Wise Analysis: User-Wise graphs for Exposure, Staleness, Sensitivity and distribution of documents with respect to Data Intellect Groups.
3. Giving administrators flexibility to define their own groups, sensitiveness, accessibility and privacy.
4. Data Footprint Reduction: In big organizations, there is a lot of overhead of storing the data and we end up storing redundant data which can impact the throughput and performance of the servers. Moreover, it can also represent a compliance violation. This feature will recognize redundant data across the organization and check if it's safe to remove or archive the same.
5. Data Compliance: Every organization has to meet the compliance requirements. With this tool you can ensure penalties are avoided. The tool helps us to identify and eliminate important but old data which is no longer useful for everyday work but might be a security liability.
6. User Data Usage Analysis: Monitoring the user's pattern of data usage w.r.t Data Intellect Groups will help in understanding the productivity of the user.

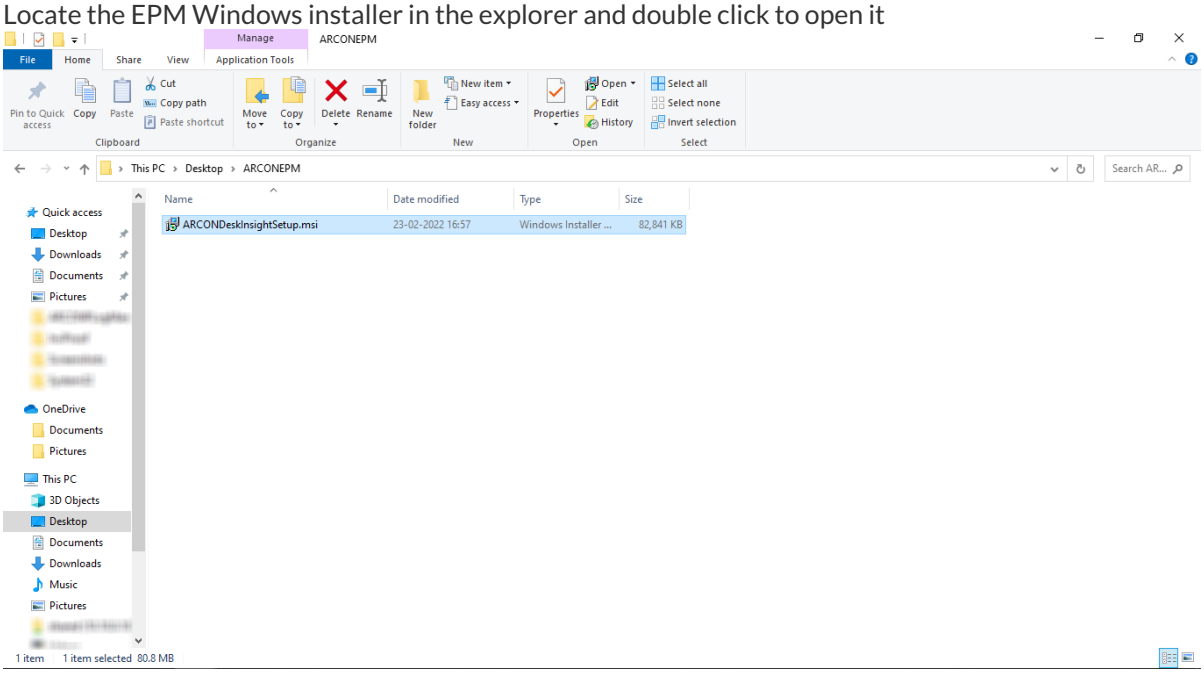
12 Endpoint Application

12.1 EPM Windows

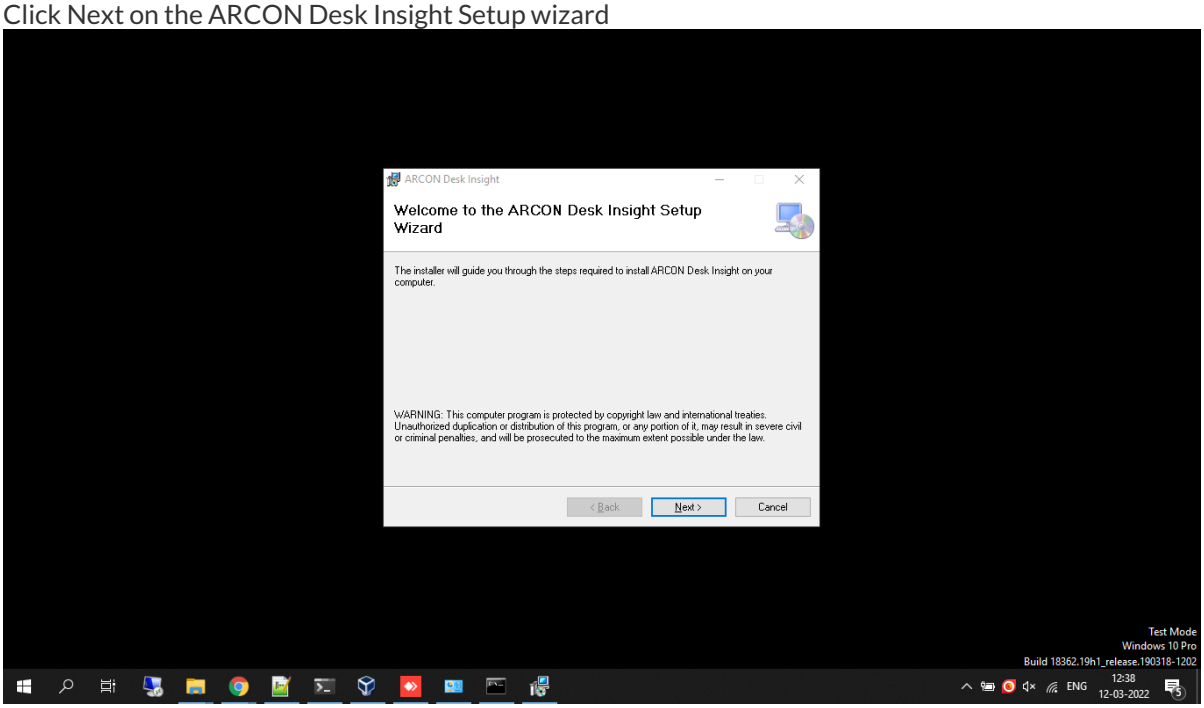
12.1.1 Installer

This section describes how to install the ARCON | EPM endpoint application on a windows endpoint

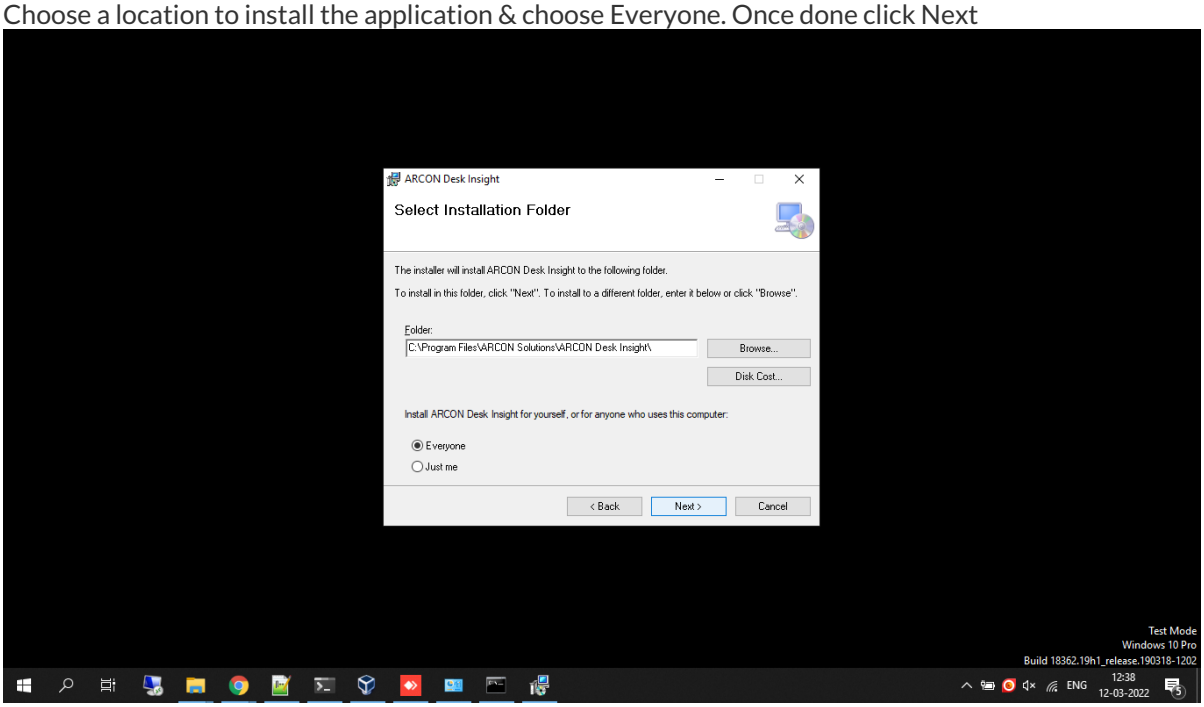
- Locate the EPM Windows installer in the explorer and double click to open it



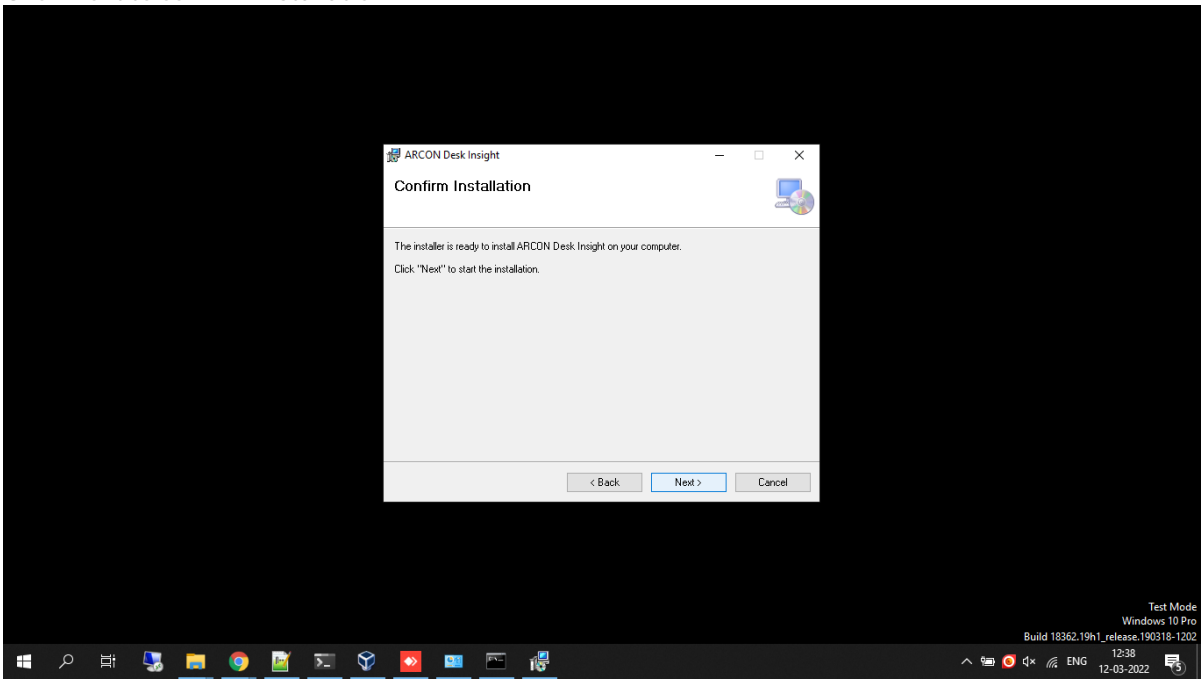
- Click Next on the ARCON Desk Insight Setup wizard



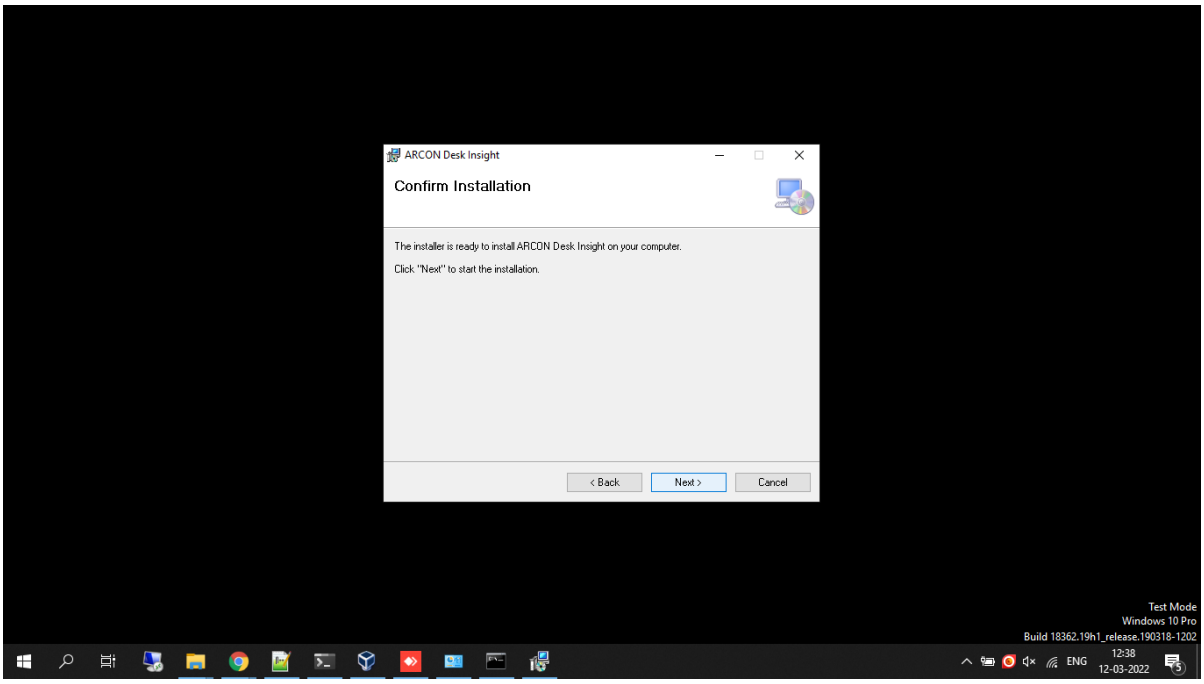
- Choose a location to install the application & choose Everyone. Once done click Next



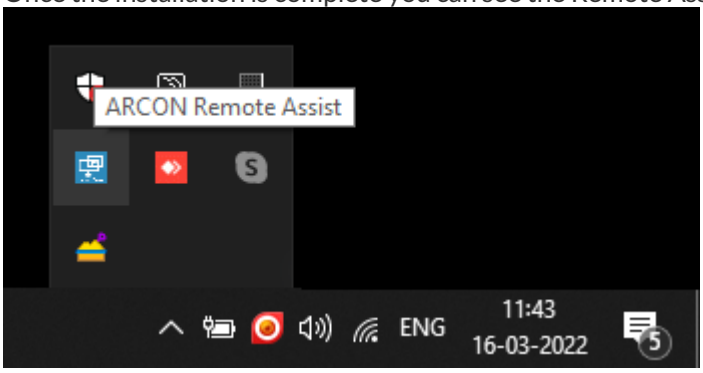
- Click Next to confirm Installation



- Click Close once the installation is complete to exit the installer



- Once the installation is complete you can see the Remote Assist icon in the system tray



12.1.2 Application Elevation (EPM Windows)

Application Elevation policy is a management method that assures that users have no access to any of the applications unless such access has been explicitly granted.

It enables the configuration of privileges so that users can request privilege elevation at specific times, for a duration of time, and on certain endpoints for required applications.

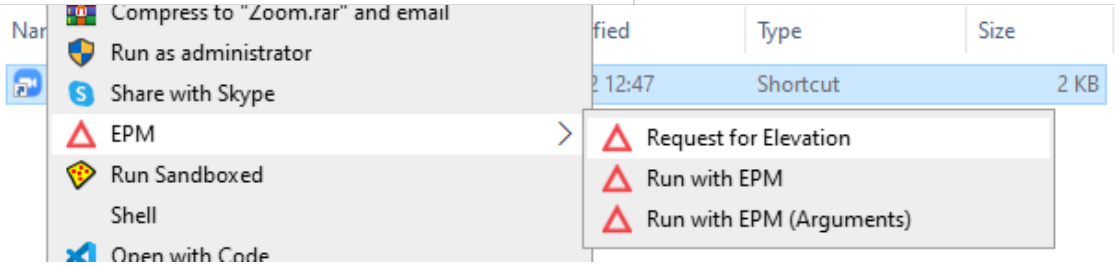
ARCON | EPM admin has full right to limit the time duration for which approvals are valid.

Enduser/Endpoint: When a user wants to elevate an application to the endpoint. They can right-click on the application and raise an elevation request EPM → Request for Elevation.

Once done a pop-up appears with a message **EPM: Raise Elevation request**.

Refer to the following table and specify fields in the pop-up to submit an elevation request:

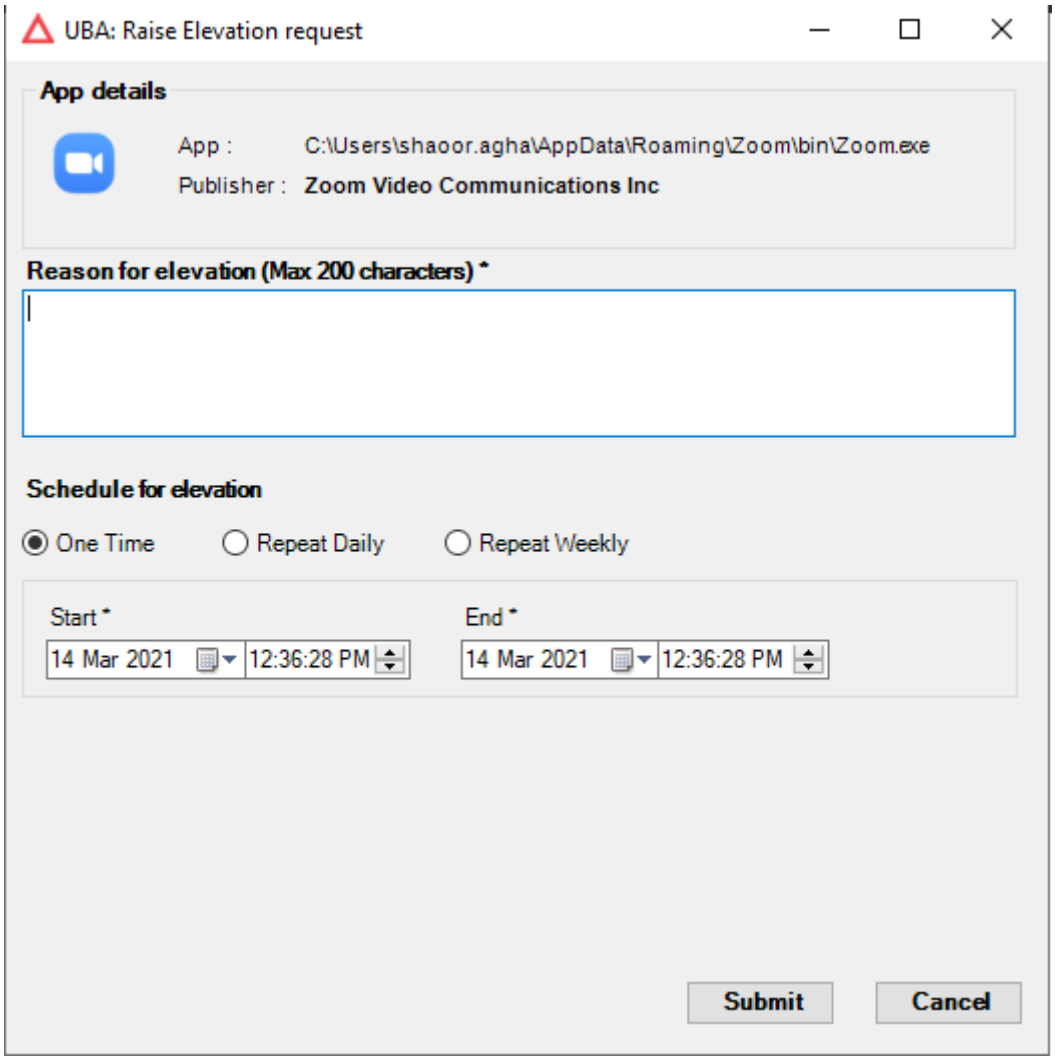
Field	Description
App	This field displays the application path
Publisher	This field displays the publisher's name
Reason for elevation(Max 200 characters)	Fill out a **reason** for the **elevation**



Schedule for elevation

Refer to the following table to understand each of the fields in the Schedule for elevation section:

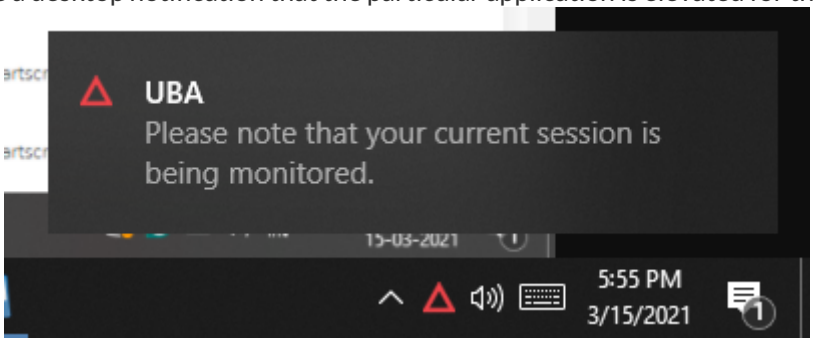
Field	Description
Once Time	If you Select this radio button , the request will be raised for one time **Start** *: Enter the Start Date / Time **End***: Enter the End Date/ Time
Repeat Daily	If you Select this radio button, the request will be raised for daily on a particular day of the week Start *: Enter the Start Date / Time End*: Enter the End Date/ Time Check the day of the week from the weekday picker
Repeat Weekly	If you Select this radio button, the request will be raised for weekly for the selected days of the week Start Time*: Specify the Start Time End Time*: Specify the End Time Check the day of the week from the weekday picker
Submit	Click the Submit button to submit the request
Cancel	Click the Cancel button to cancel the request

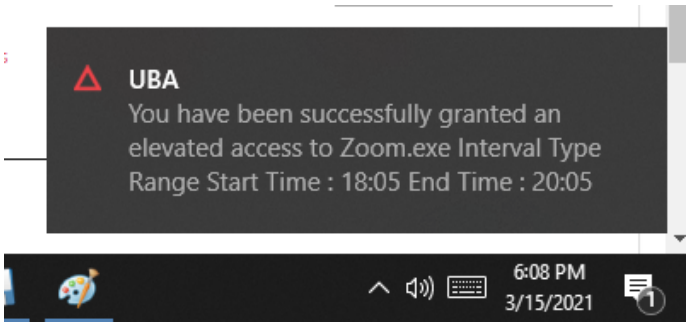


12.1.3 Endpoint Notification Centre

The endpoint notification center alerts end-user that they are being monitored every time they start the system. When an end-user raises an elevation request for accessing a particular application. And when it is approved from the EPM console.

End-user will receive a desktop notification that the particular application is elevated for the user.





Troubleshooting Policies with EPM Windows

ARCON | EPM allows the Administrator to run the solution in Debug mode for Windows. It also provides the privilege to the Administrator to set different levels of debugging policies in the EPM solution such as information, errors, warnings, alerts and so on.

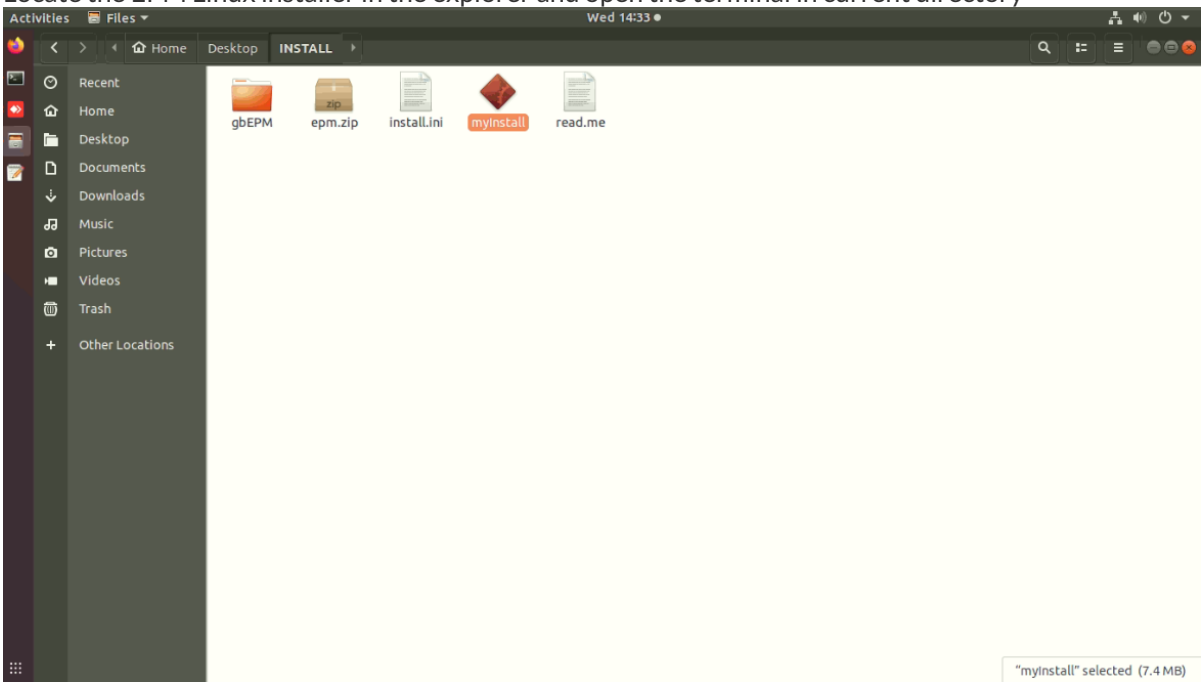
While running in the Debug mode, The ARCON EPM solution will capture each and every action of the policies and place the log data on a trace file (.txt). These trace files are created on target machines. However, these are generally useful where command manipulation is used and not ACLs (access control list).

12.2 EPM Linux

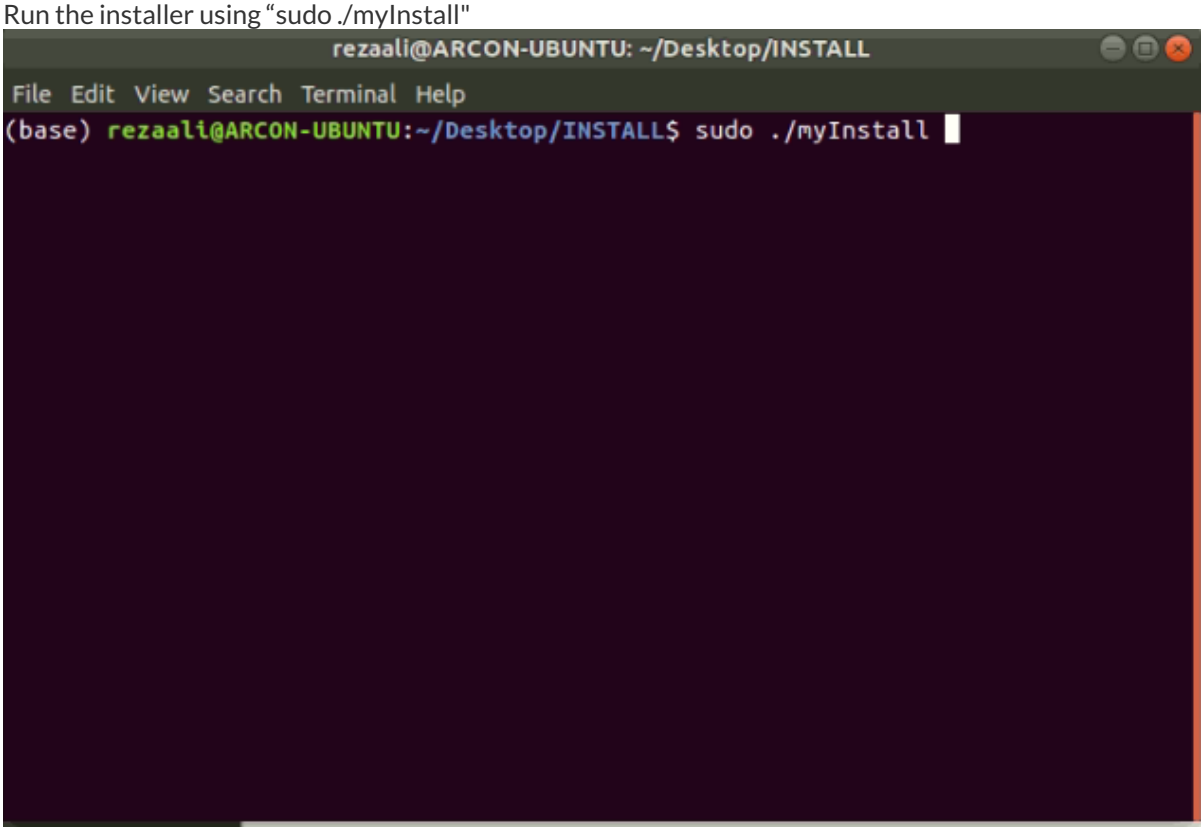
12.2.1 Installer

This section describes how to install the ARCON | EPM endpoint application on a linux endpoint

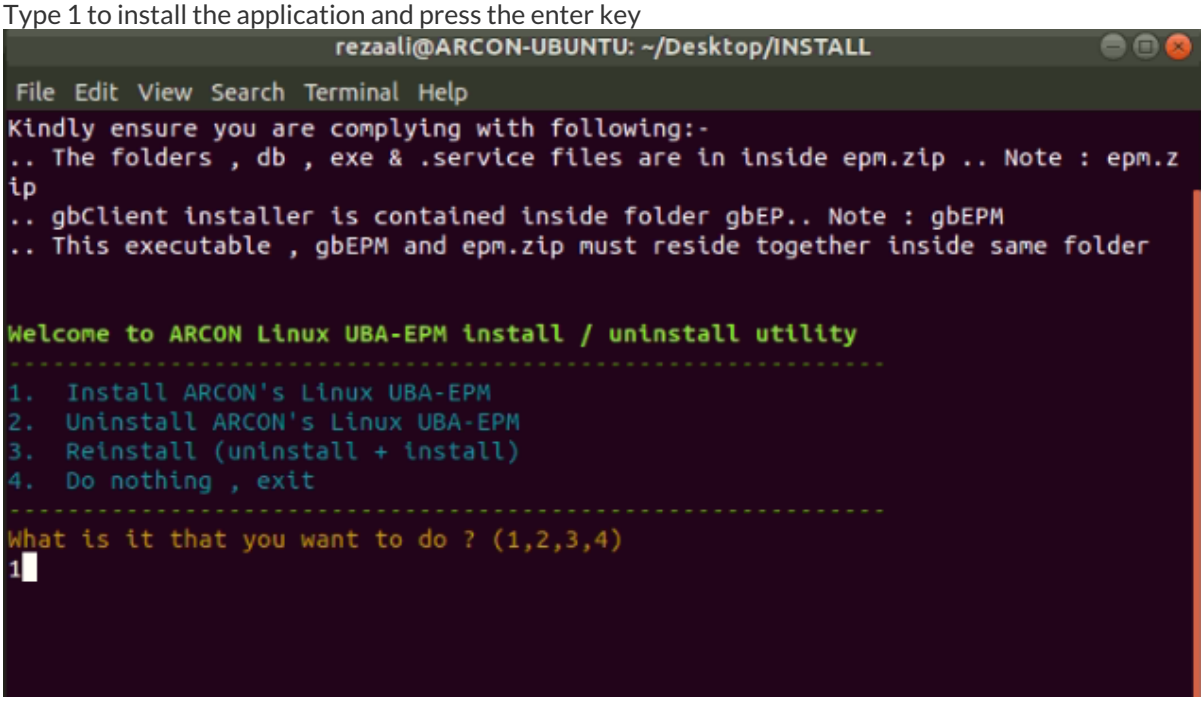
- Locate the EPM Linux installer in the explorer and open the terminal in current directory



- Run the installer using “sudo ./myInstall"



- Type 1 to install the application and press the enter key



- You will see the screen below stating the installation is completed

```
setting up database
shifting service files
        Making /usr/bin/epm/daemonCLI executable
        Copying /usr/bin/epm/daemonCLI.service to /etc/systemd/system/daemonCLI.
service
        Enabling  /etc/systemd/system/daemonCLI.service
        Starting /etc/systemd/system/daemonCLI.service
        Making /usr/bin/epm/daemonSRV executable
        Copying /usr/bin/epm/daemonSRV.service to /etc/systemd/system/daemonSRV.
service
        Enabling  /etc/systemd/system/daemonSRV.service
        Starting /etc/systemd/system/daemonSRV.service
(base) rezaali@ARCON-UBUNTU:~/Desktop/INSTALL$
```

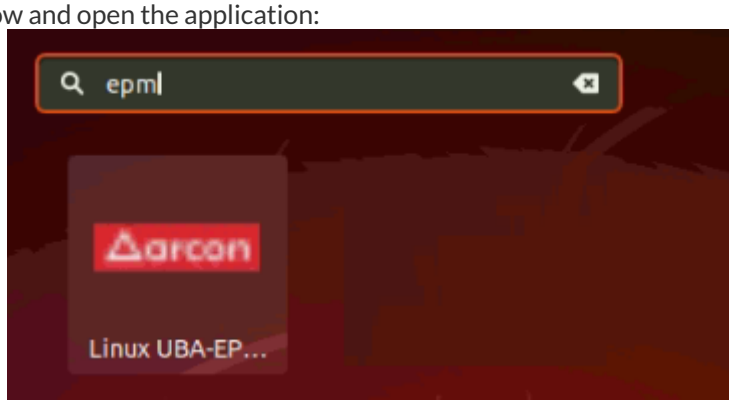
12.2.2 Application Elevation (EPM Linux)

Elevation using GUI

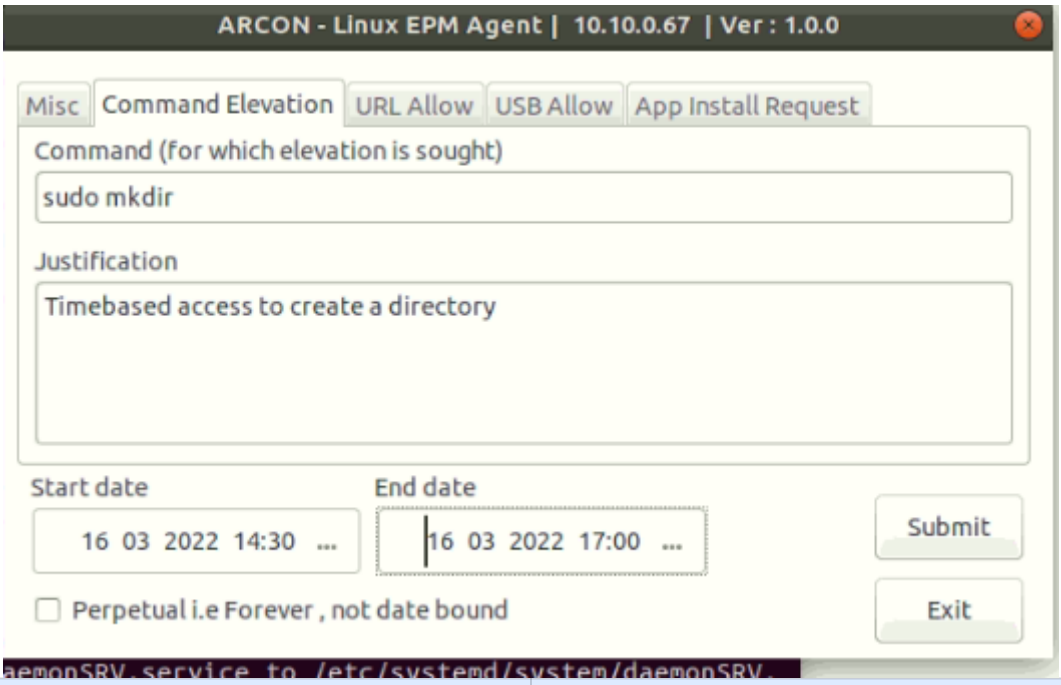
End-user can raise an elevation request for an application or command using GUI or CLI

To raise a request using the GUI go to programs by clicking on the following icon:

Search for epm like below and open the application:



Select Command elevation tab and fill in the required details:



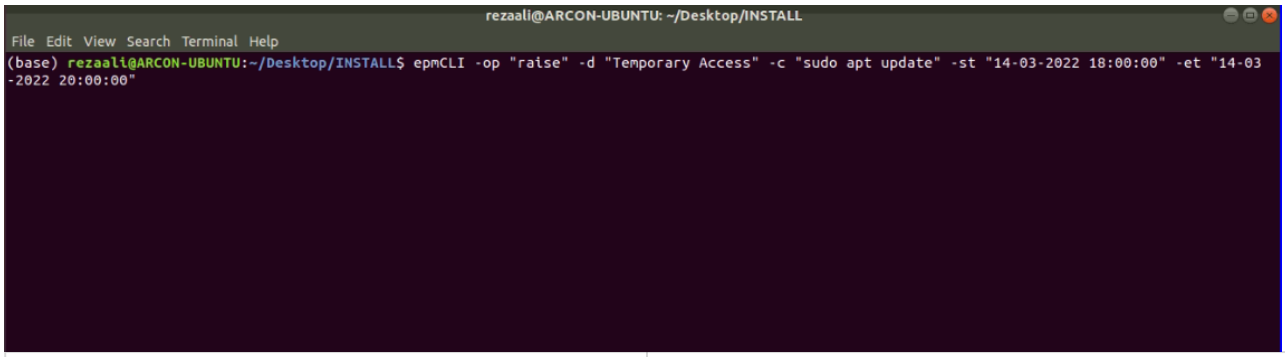
Field	Description
Command	Enter the sudo command for elevation
Justification	This field displays the publisher's name
Justification	Fill out a **reason** for the **elevation**
Start date	Select start date and time
End date	Select end date and time
Perpetual	Select perpetual if you need a permanent access

Once the request is raised you will get a confirmation saying request submitted

Elevation using CLI

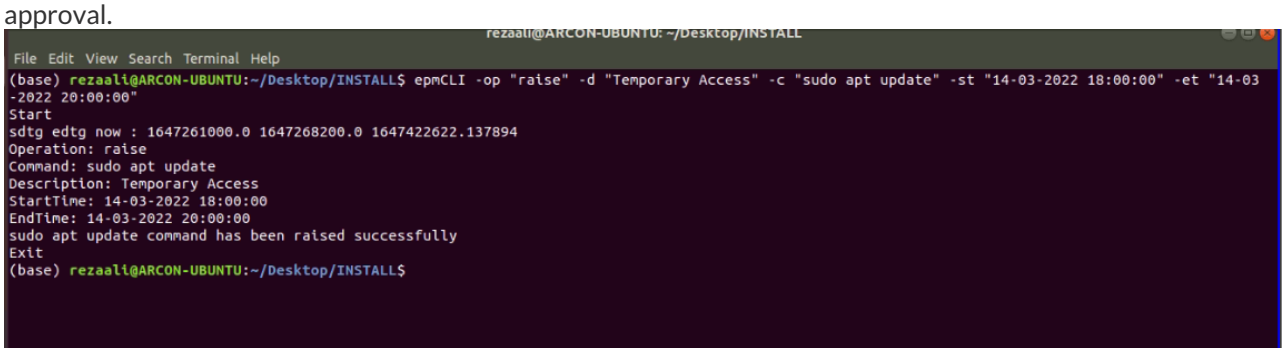
If the user wants to raise a request using the CLI he can type the below command:

```
epmCLI -op "raise" -d "Temporary Access" -c "sudo apt update" -st "14-03-2022
18:00:00" -et "14-03-2022 20:00:00"
```



Field	Description
-op	Enter “raise” if you want to raise a request
-d	Fill out a **reason** for the **elevation**
-c	Enter the command to be elevated
-st (Optional)	Enter the start date and time. Exclude if permanent
-et (Optional)	Enter the end time. Exclude if permanent

Once the request is raised a below screen will be shown and the request will be submitted in the workflow for approval.



Once the request is approved the user will be able to run the requested command with sudo privileges for the specific time or permanently as applicable.

Troubleshooting Policies with EPM Linux

ARCON | EPM allows the Administrator to run the solution in Debug mode for Linux. It also provides the privilege to the Administrator to set different levels of debugging policies in the EPM solution such as information, errors, warnings, alerts and so on.

While running in the Debug mode, The ARCON EPM solution will capture each and every action of the policies and place the log data on a trace file (.txt). These trace files are created on target machines. However, these are generally useful where command manipulation is used and not ACLs (access control list).

12.3 EPM MAC

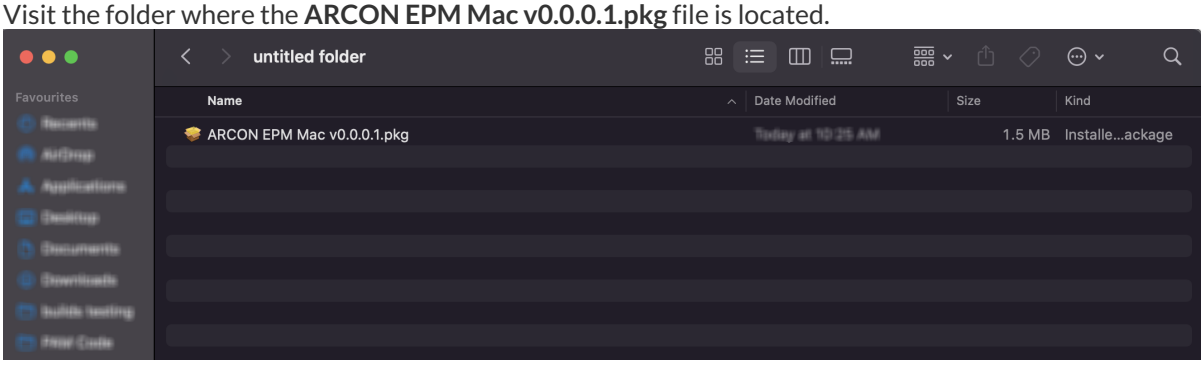
In this document, the step-by-step installation of EPM Package (version v0.0.0.1) for MAC OS will be covered.

Generic Functions for Installation:

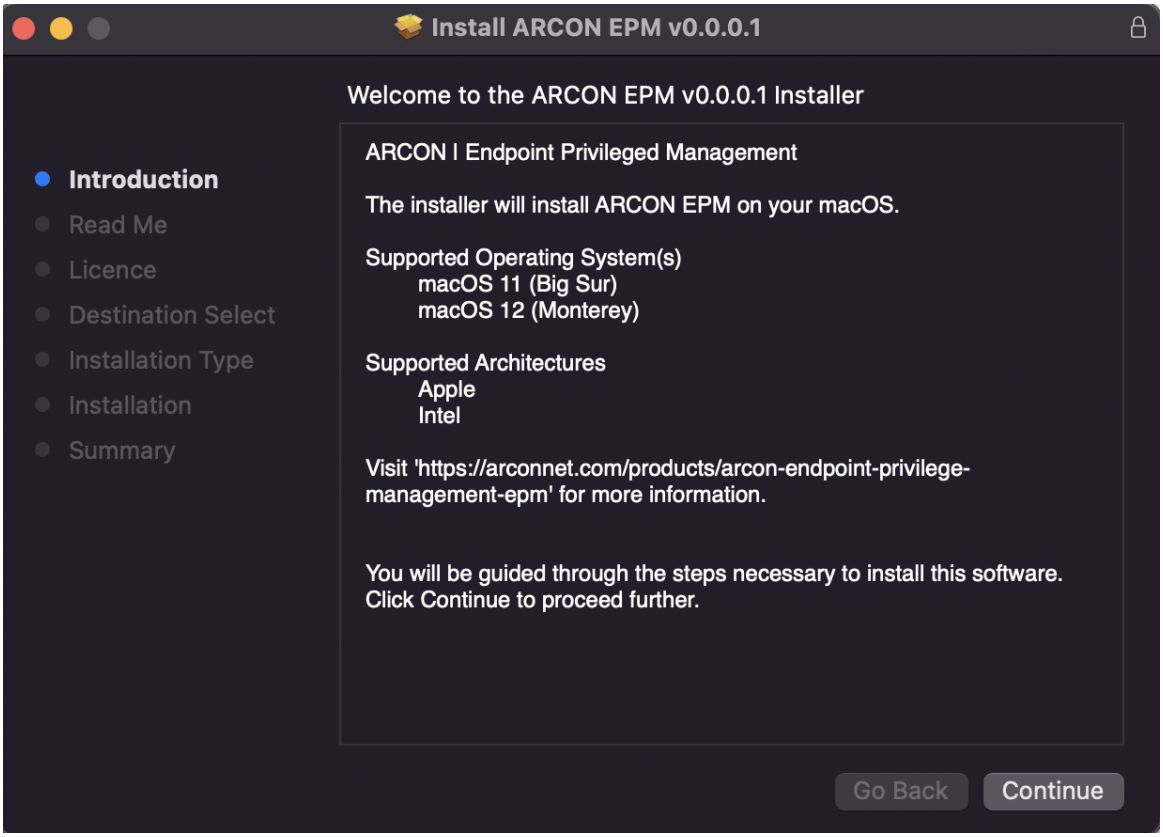
- **Print**: By clicking on this button, user will be able to print the information displayed on the installer window.
- **Save**: By clicking on this button, user will be able to save the information displayed on the installer window.
- **Go Back**: By clicking on this button, user will be able to go back to the previous stage of the installation process.

To install the EPM Package, user will need to perform the following steps:

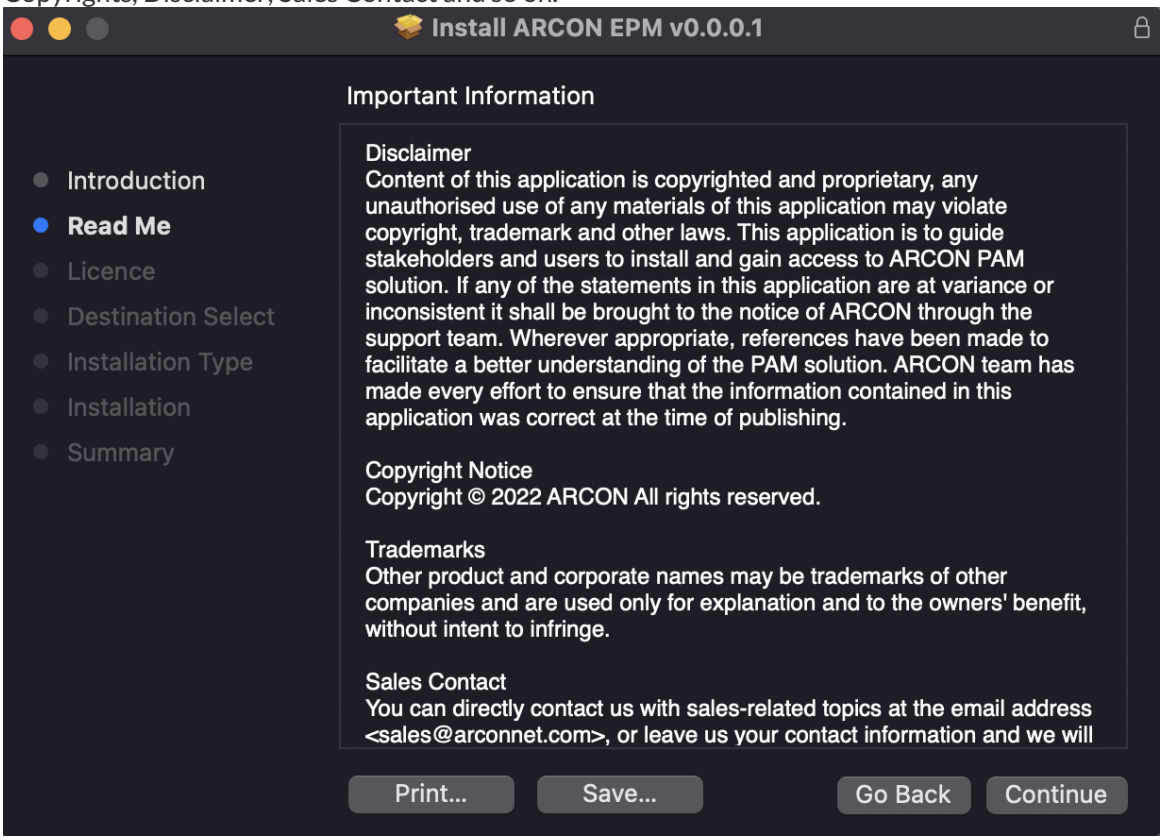
1. Visit the folder where the **ARCON EPM Mac v0.0.0.1.pkg** file is located.



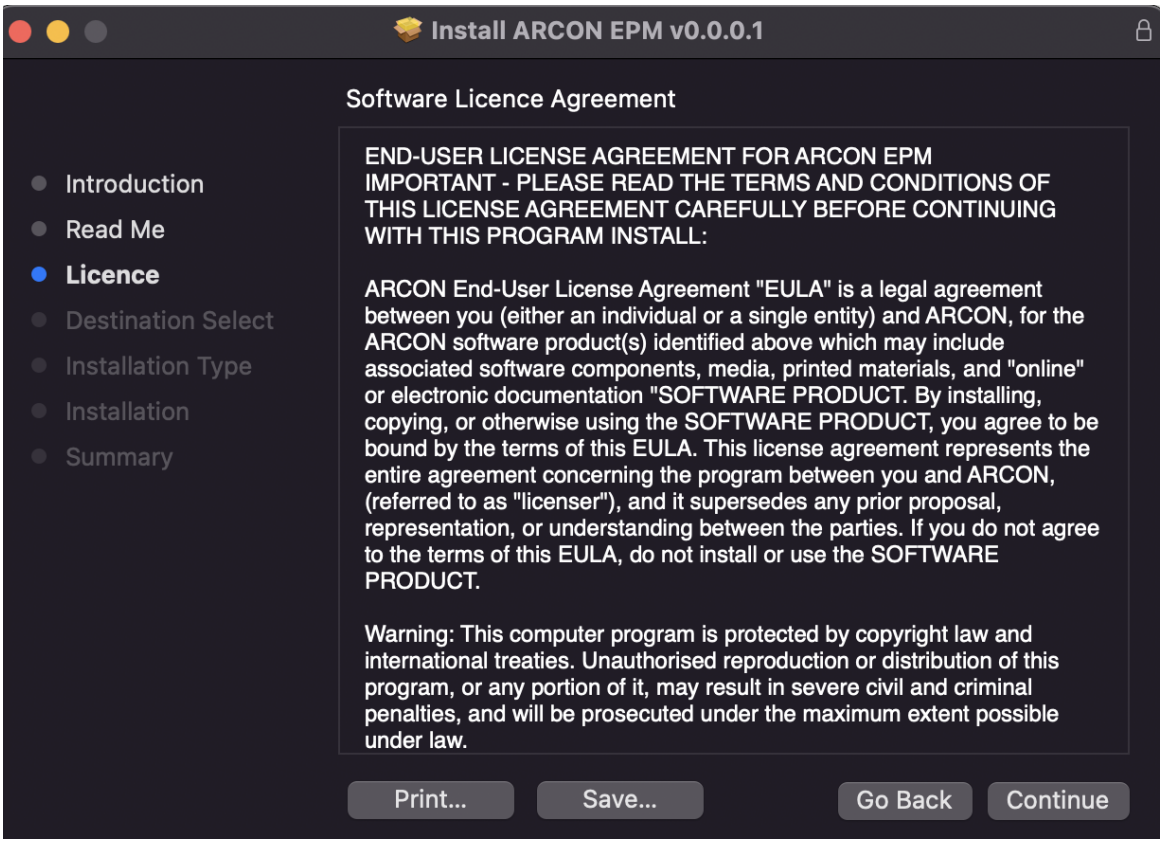
2. Double-click on the file. The Installer pop-up would be displayed stating the details of supported MAC OS and Architecture:



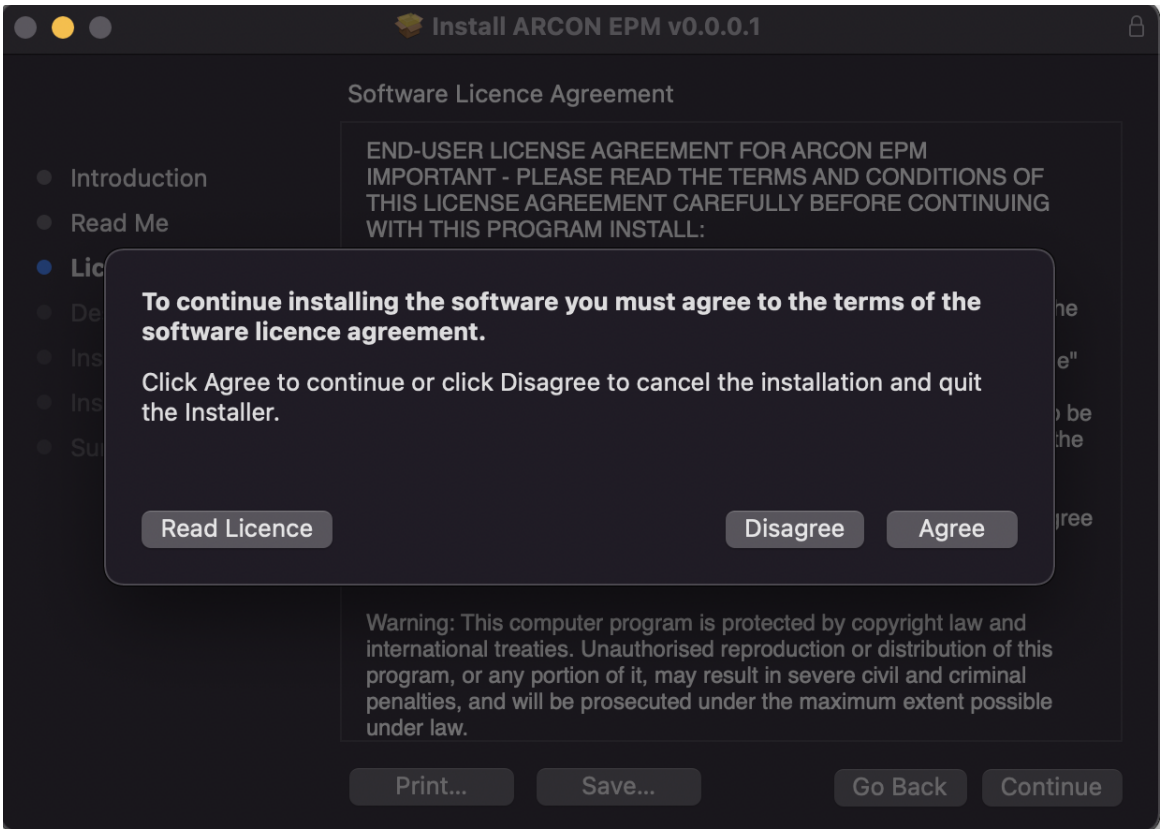
3. Click on **Continue**. The Important Information section will be displayed stating the ARCON EPM Copyrights, Disclaimer, Sales Contact and so on.



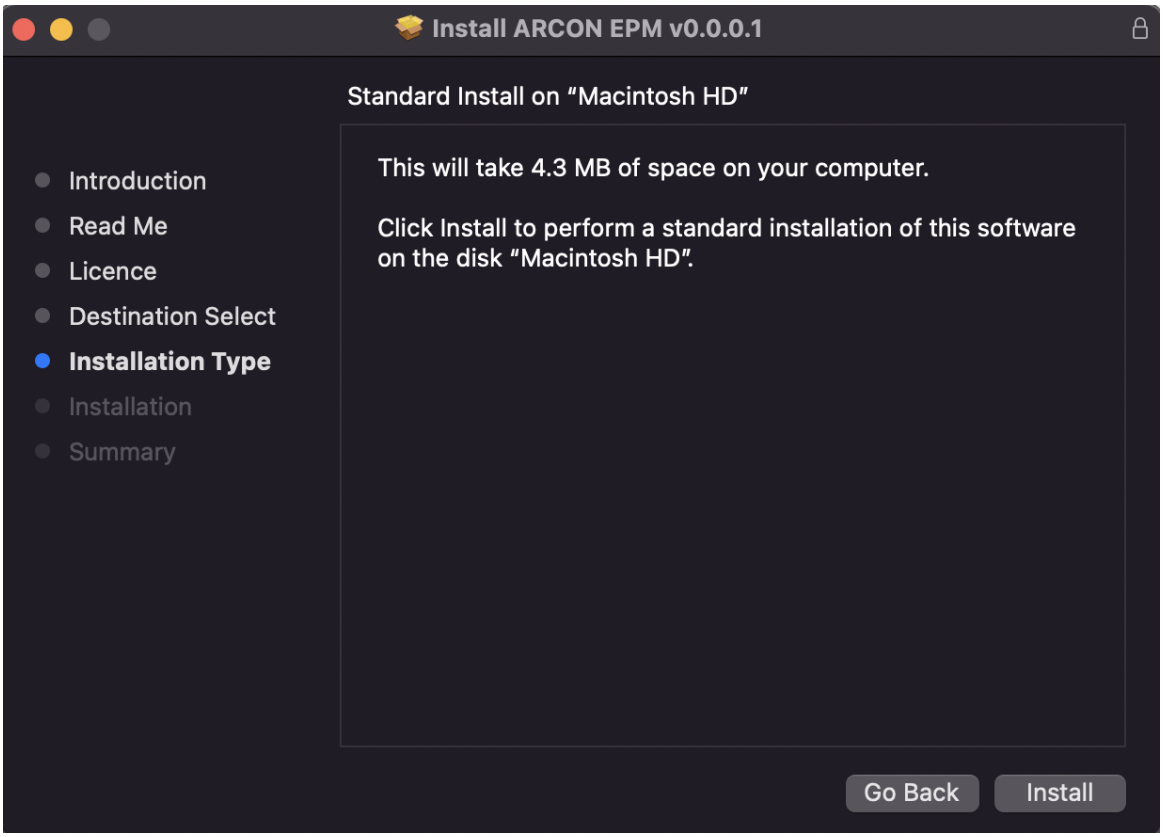
4. Click on **Continue**. The Software Licence Agreement details will be displayed.



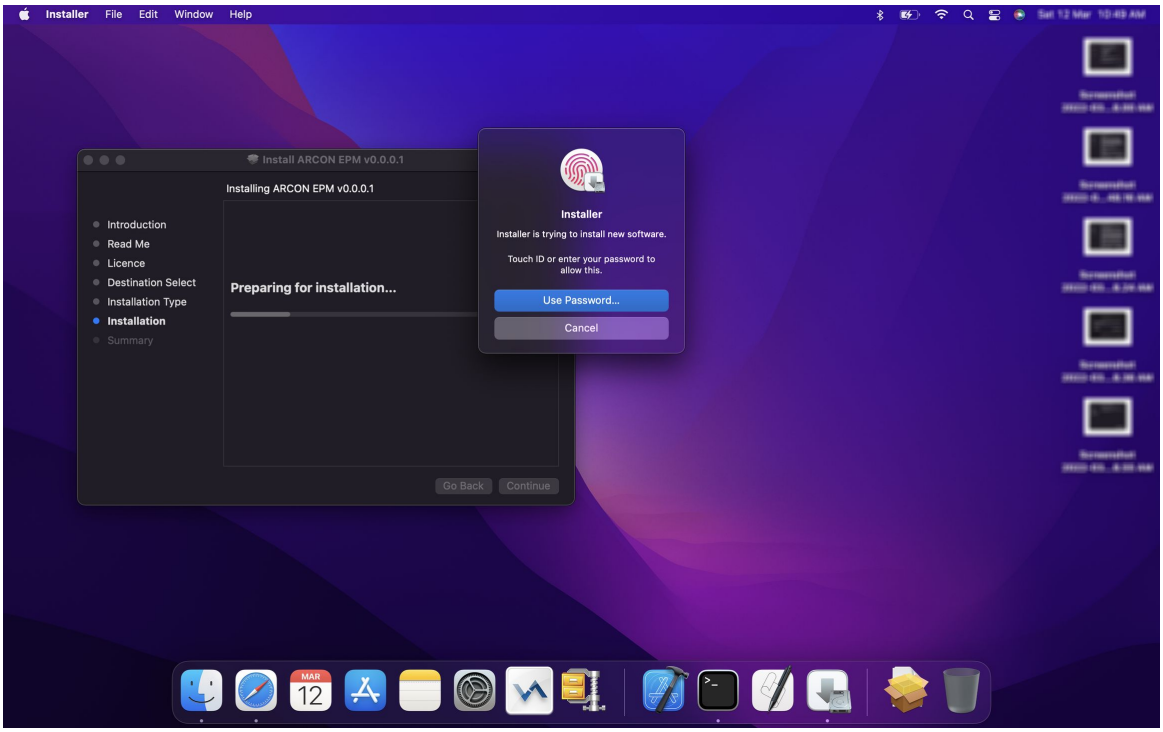
5. Click on **Continue**. The **Software Licence Agreement** pop-up will be displayed stating the following information:



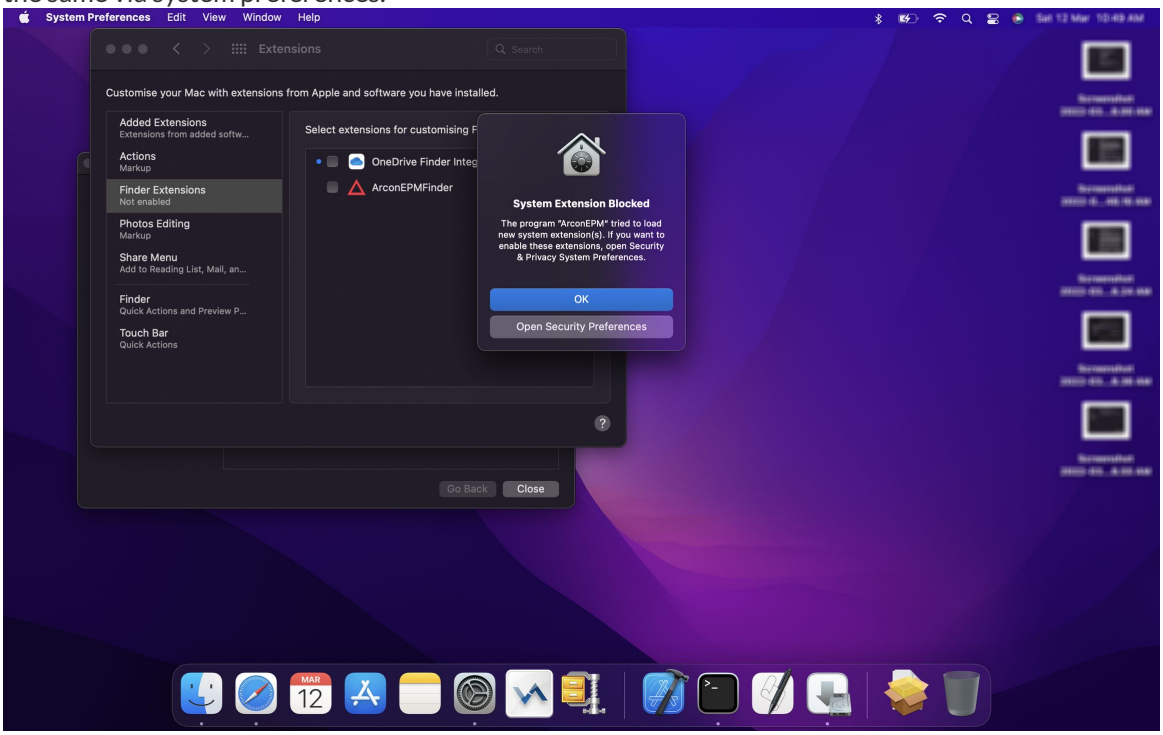
6. User can click on the **Read Licence** button to review the terms & conditions. Once it has been reviewed, user can click on **Agree** button. The **Installation Type** stage will be displayed:



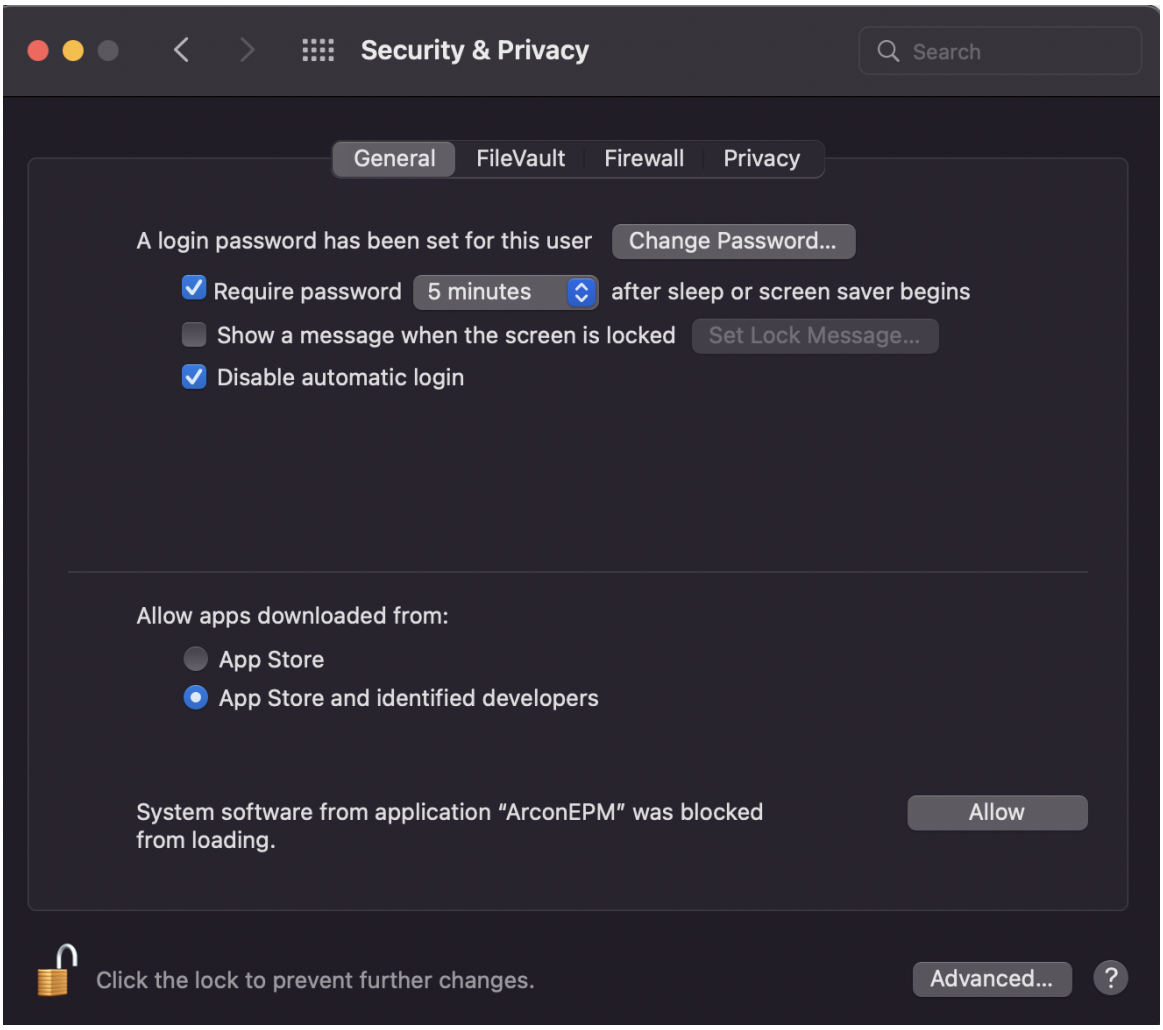
7. Click on **Install**. The Installer pop-up will be displayed asking the Administrator authentication to allow the installation process. This is the first step of installation where ARCON EPM will ask the user for privileges as it will require admin access for some of the files to be placed and all components to work as expected. The Administrator can either use the thumb impression (if it is already configured in the system) or can use the password to authenticate.



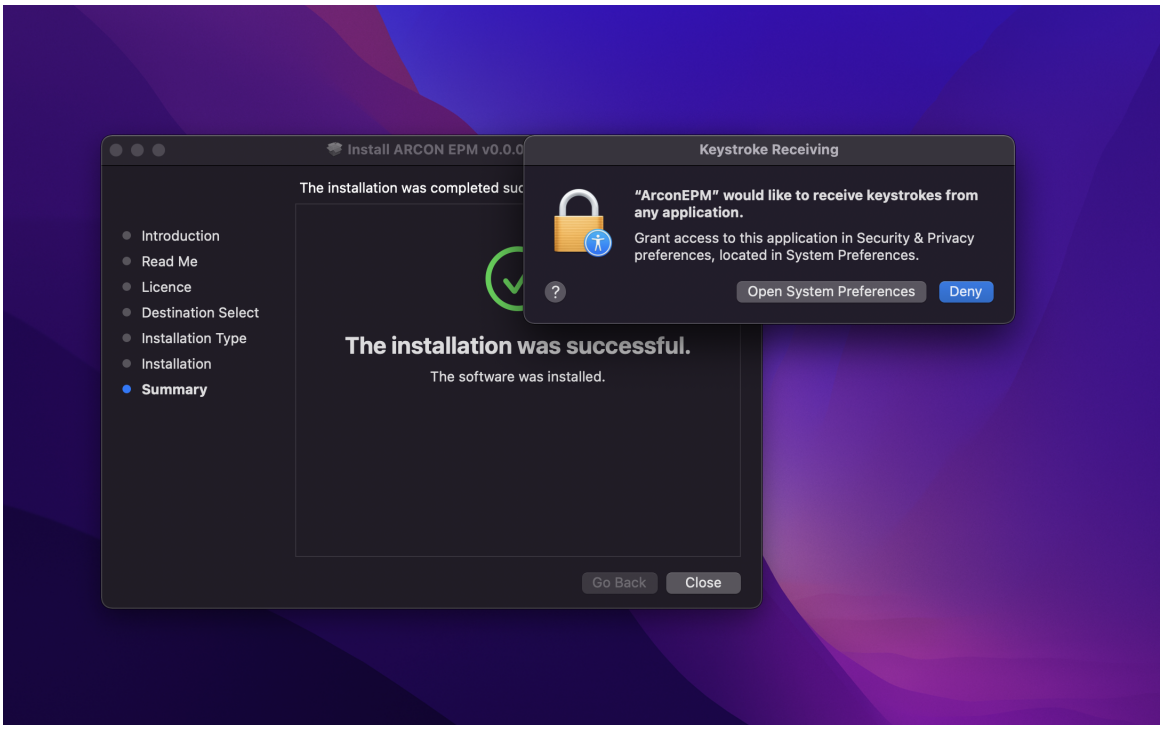
8. Once the Administrator access is authenticated, a **System Extension Blocked** pop-up will be displayed. This is the gatekeeper prompt that blocks any new system extensions to start till the user does not allow the same via system preferences.



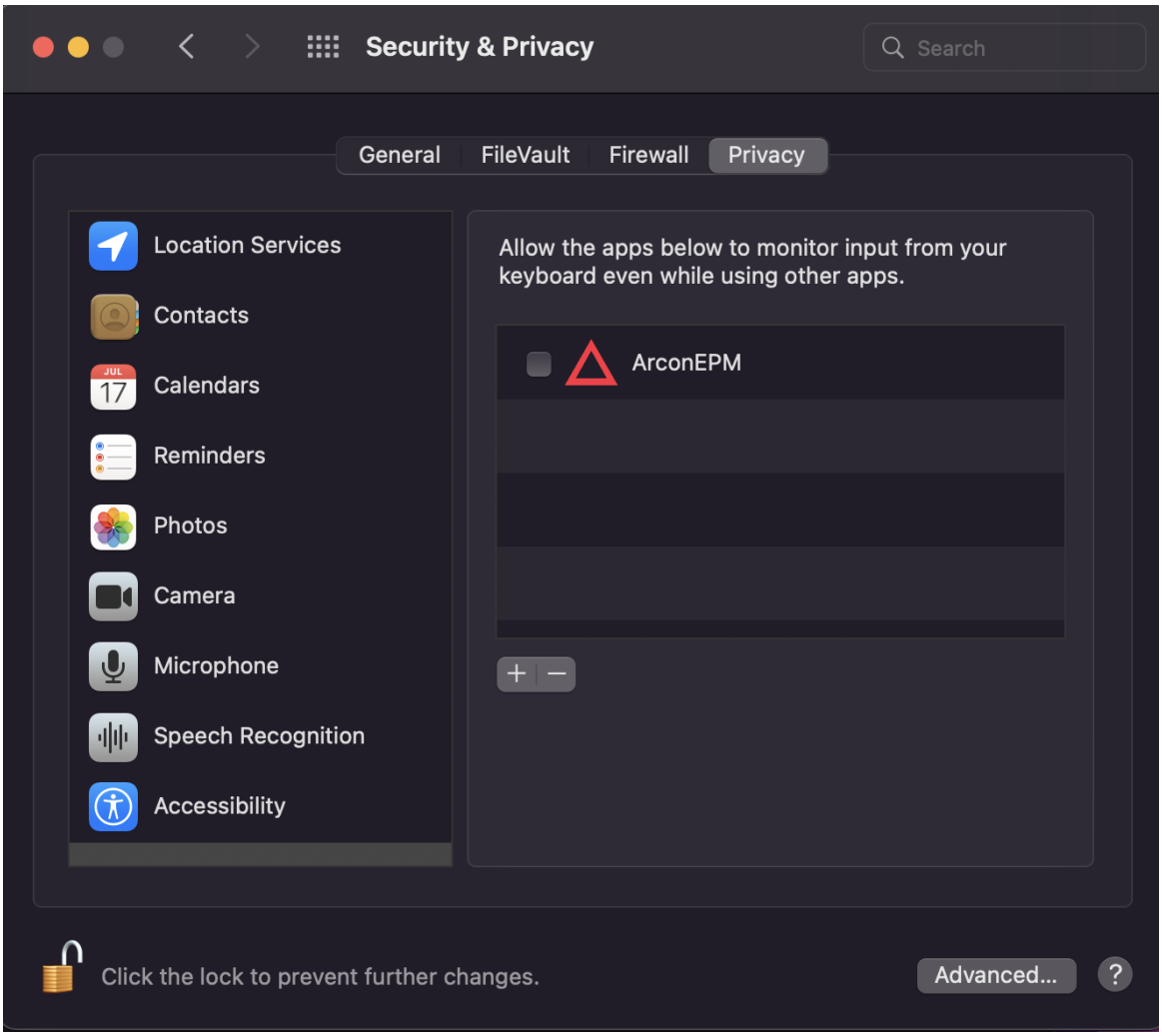
9. Click on **Open Security Preferences**. The user will be redirected to the following screen:



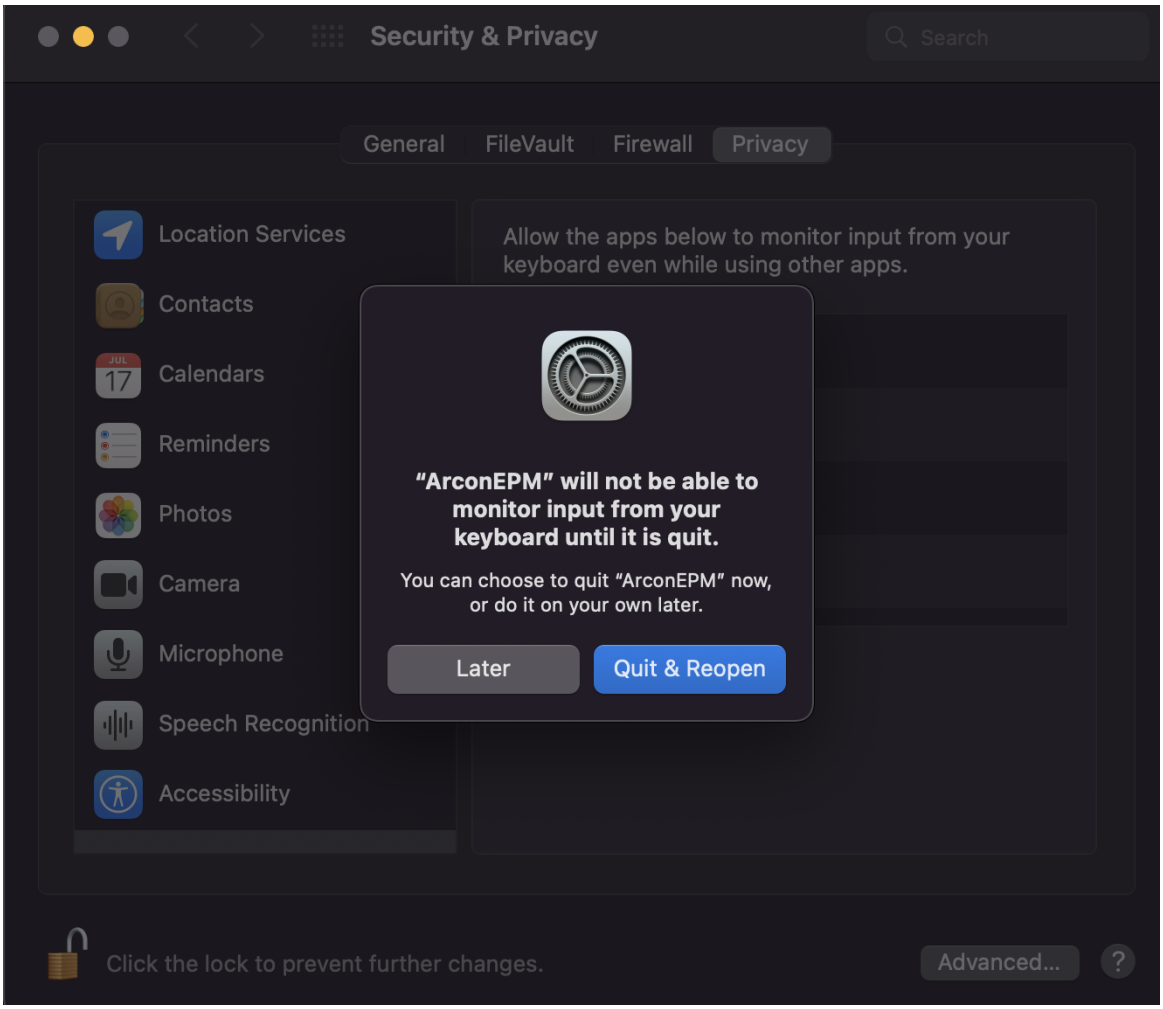
10. Click on **Allow**. The Keystroke Receiving permission pop-up will be displayed. Similar to System Extensions, there are some more accessibility permissions that needs to be provided for ARCON EPM:



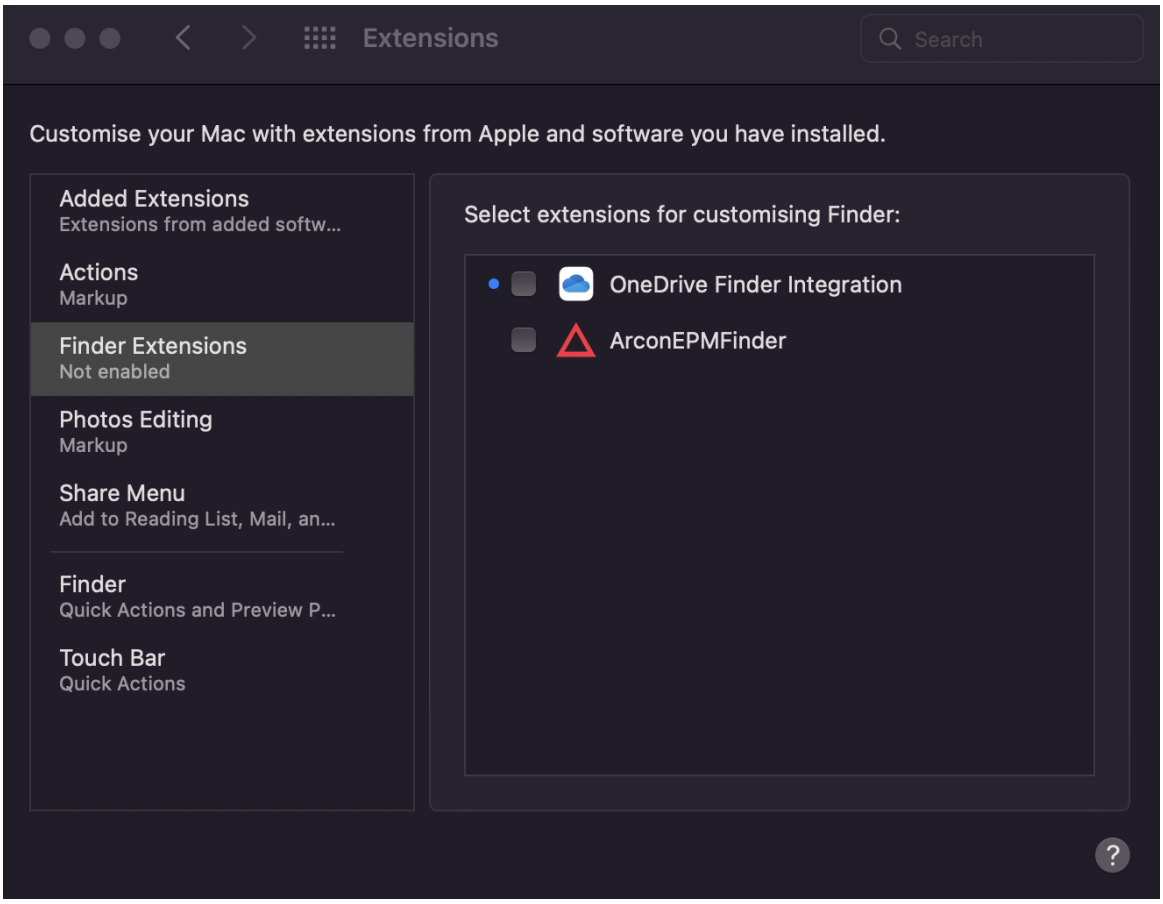
11. Click on the **Open System Preferences** button. The following screen will be displayed:



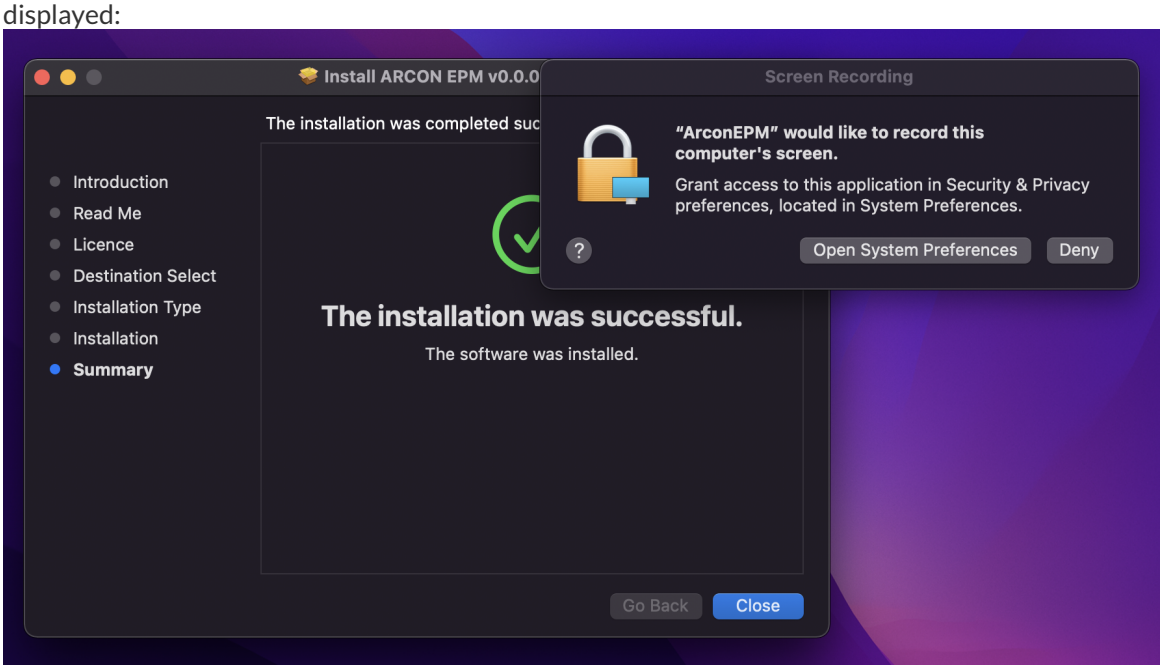
12. Select the checkbox against **ArconEPM** icon. The pop-up will be displayed stating to quit & reopen:



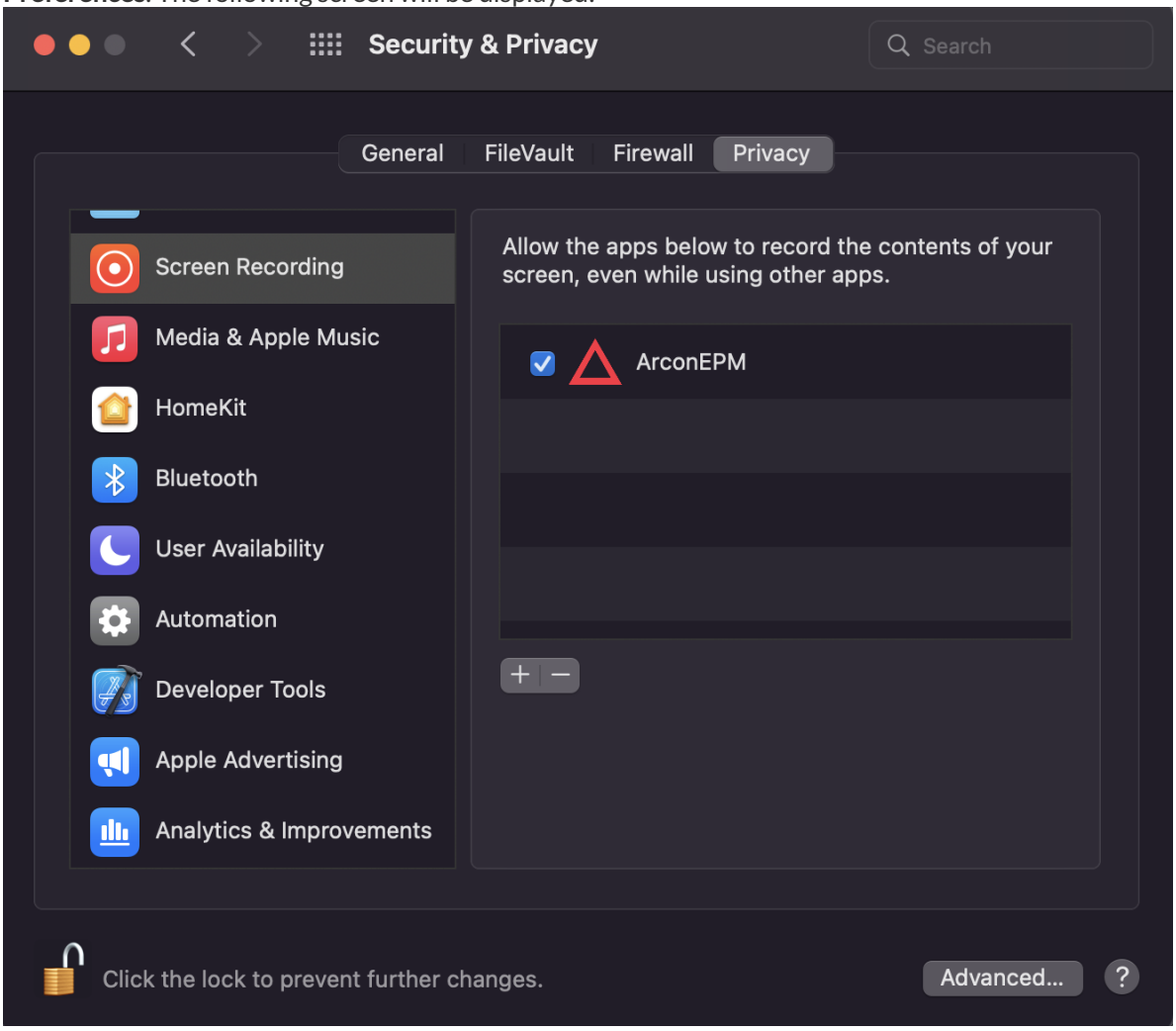
13. Click on Quit & Reopen. The Extensions window will be shown. This is the accessibility permission is for Finder Extensions by which, the ARCON EPM will be displayed in the Context Menu of Files and Applications.



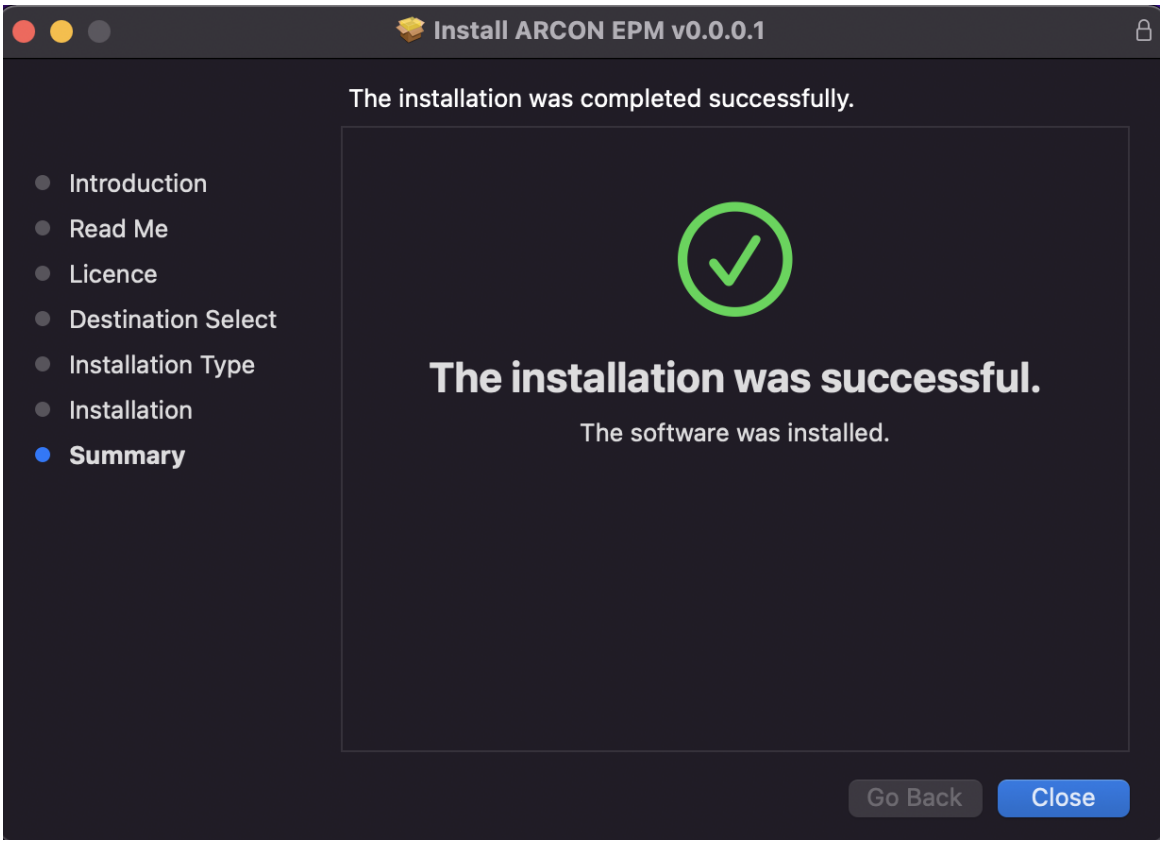
14. Select the checkbox against the **ArconEPMFinder** icon. The Screen Recording permission pop-up will be displayed:



15. This permission is required for screen Capture feature to work on EPM. Click on **Open System Preferences**. The following screen will be displayed:



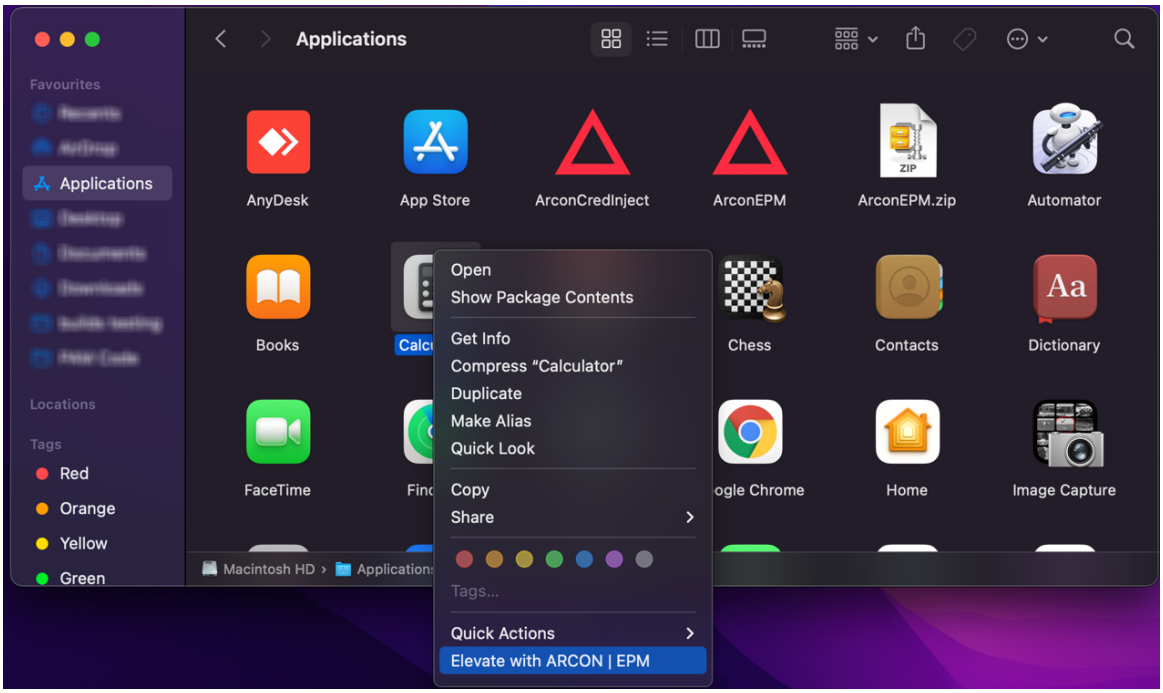
16. Select the checkbox against **ArconEPM**. The installation process will be completed. and the confirmation message window will be displayed:



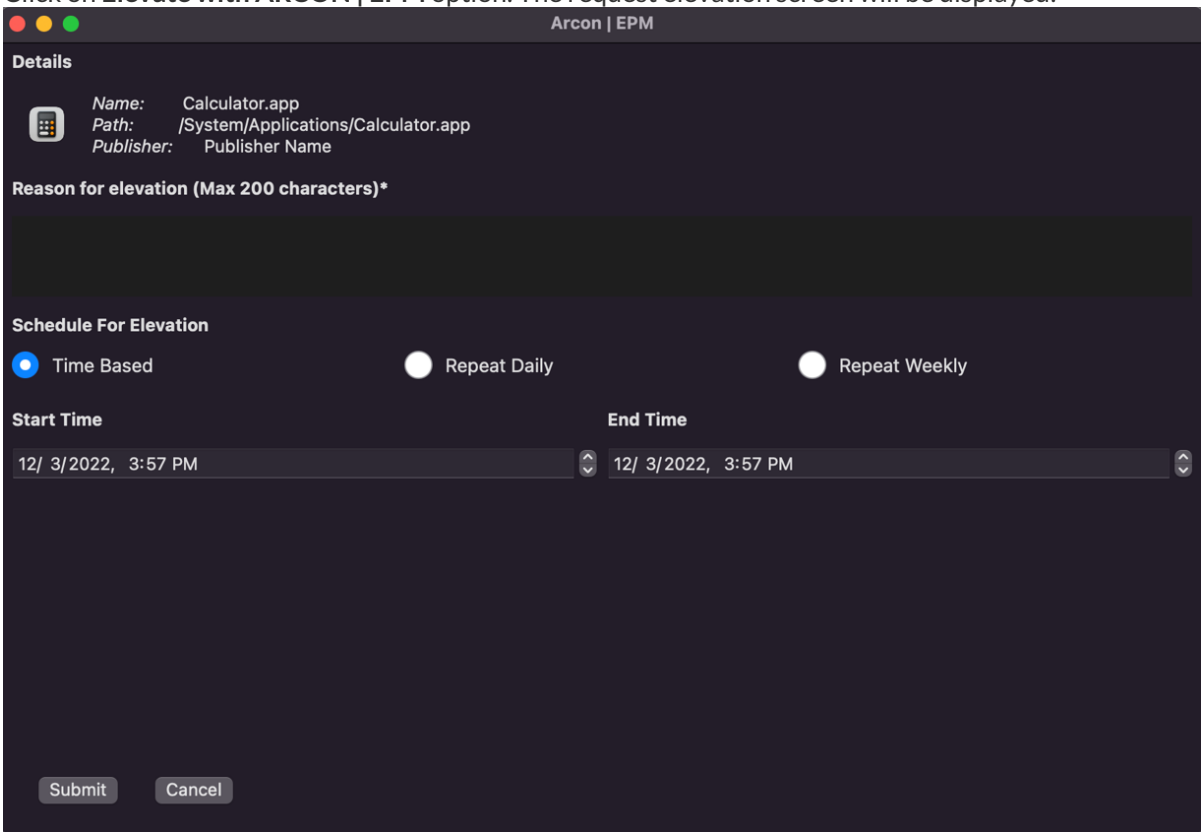
12.3.1 Requesting Elevation

Considering the ARCON EPM is installed in the system, user can now raise a request for elevation. To do the same, user will need to perform the following steps:

1. From the **Applications** folder, right-click on the application on which, the elevation needs to be raised:



2. Click on **Elevate with ARCON | EPM** option. The request elevation screen will be displayed:



Refer to the following table to understand the field level description shown in the preceding screen:

Field Name	Description
Reason for elevation	User will need to specify the reason for elevation. This is the mandatory field and the maximum limit for the characters will be 200.
Schedule For Elevation	In this section, user will need to define the schedule time for which, the elevation needs to be provided: • **Time Based**: In this option, user can specify the start & end time till which, the elevation will be active. • **Repeat Daily**: In this option, user can specify the start & end time for the elevation, which will be repeated on daily basis. • **Repeat Weekly**: In this option, user can specify the start & date time along with the specified days for which, the elevation needs to be raised.

3. Once all the required details are entered, click on **Submit**. The request will get submitted to the workflow for approval.

4. Once the request for elevation is approved, the user can double-click on the application for which, the elevation was raised. The respective application shall be open-to-use for the user for the specified amount of time.

Troubleshooting Policies with EPM MAC

ARCON | EPM allows the Administrator to run the solution in Debug mode for MAC. It also provides the privilege to the Administrator to set different levels of debugging policies in the EPM solution such as information, errors, warnings, alerts and so on.

While running in the Debug mode, The ARCON EPM solution will capture each and every action of the policies and place the log data on a trace file (.txt). These trace files are created on target machines. However, these are generally useful where command manipulation is used and not ACLs (access control list).

13 Hash Builder

Hash Builder is a utility whose task is to compare two folders (Ex: old built and present built) and after comparing provides only the Files\Folder which are modified or newly created.

Problem Definition

Previously we used to modify the older built and create a new package. The modifications performed was stored in same package and whole package supposed to be shared to the client which took a lot of time to upload the package and was difficult for client to add and delete the previous package and install the whole new package.

Scope of Project

The purpose behind building this utility is to make the task easy for Client as well as DevOps team(providing the package).

Step :1

Goes into loop only for folders not mentioned in the Array list.

If the folder does not exists then create a new folder.

```
static public void CopyFolder(string sourceFolder, string destFolder, string compFolder)
{

    //Goes into the loop only for folders not mentioned in the ArrayList(ignoreFolderList) i.e. folders which are not ignored.
    if (!CheckFolderName(sourceFolder))
    {
        // Step 1: If the folder does not exists then create a new folder
        if (!Directory.Exists(destFolder))
            Directory.CreateDirectory(destFolder);
```

Step :2

Get List Of Files in the folder.

Dictionary to store path of the file as key and also filename as value.

```
// Step 2: Get List of files in the folder.
//dictionary to store path of the file as key and also filename as value
Dictionary<string, string> filesInSFolder = new Dictionary<string, string>();
Dictionary<string, string> filesInCFolder = new Dictionary<string, string>();

string[] files = Directory.GetFiles(sourceFolder);
foreach (string file in files)
{
    // Use the Path.Combine method to safely append the file name to the path.
    string name = Path.GetFileName(file);
    string dest = Path.Combine(sourceFolder, name);
    filesInSFolder.Add(dest, name);
}
try
{
    files = Directory.GetFiles(compFolder);
}
catch (Exception e)
{; }
foreach (string file in files)
{
    string name = Path.GetFileName(file);
    string dest = Path.Combine(compFolder, name);

    filesInCFolder.Add(dest, name);
}
```

Step :3

Compare Files and their hash Code

1. **If the file does not exist in source folder, copy the file.**
2. **if the File are old than 4 days or they are third party files, it will ignore.**
3. **We have used File hasher utility program.**
4. **Copying the file if the hash code does not match.**

```
// Step 3: Compare Files and their hash coded
foreach (var item in filesInSFolder)
{
    // Step i : if the file dose not exisit in source folder , copy the file .
    // Use the Path.Combine method to safely append the file name to the path.
    // Will overwrite if the destination file already exists.
    if (!filesInCFolder.ContainsValue(item.Value)) {
        File.Copy(item.Key, destFolder + "\\" + item.Value, true);
        Console.WriteLine("ADDING New File:" + item.Key );
        log.Debug(" ADDING New File:" + item.Key + "\n");
    }
    else
    {
        var keyValue = item.Key.Replace("B22", "B21");
        var compKey = filesInCFolder.FirstOrDefault(x => x.Key == keyValue).Key;
        // Step ii : if the file are old than 4 days or they are third party files , please ignore .
        if (!CompFileTimeStamp(item.Key, compKey))
        {
            if (!CheckFileName(item.Value))
            {
                try
                {

                    //using hashCalculator from FileHasher Utlility Program
                    var hashSource = new HashCalculator(item.Key).CalculateFileHash();
                    var hashComp = new HashCalculator(compKey).CalculateFileHash();

                    //modified files
                    Console.WriteLine(" ADDING Modified File:" + item.Key );
                    log.Debug(" ADDING Modified File:" + item.Key + "\n");


                    //copying files if the hash code does not match else does not copies (using md51 cryptography method to generate hash
                      value
                    if (!hashSource.Equals(hashComp))
                    {
                        File.Copy(item.Key, destFolder + "\\" + item.Value, true);
                        log.Debug("Actual Copied files into Diff folder: " + destFolder + "\\" + item.Value + "\n");
                    }
```

Step : 4

If the files come under catch block it will force copy files.

```
                catch (Exception e)
                {
                    File.Copy(item.Key, destFolder + "\\" + item.Value, true);
                    Console.WriteLine("Forced Copied File Name:" + destFolder + "\\" + item.Value);
                    log.Warn("Forced Copied File Name:" + destFolder + "\\" + item.Value + "\n");
                    ;
                }
            }
        }
    }


}
```

Step : 5

This will check all folders recursively.

```
            }
            // Step 5 : Final Step to check all folders recurseively .
            string[] folders = Directory.GetDirectories(sourceFolder);
            foreach (string folder in folders)
            {
                string name = Path.GetFileName(folder);
                string dest = Path.Combine(destFolder, name);
                string comp = Path.Combine(compFolder, name);
                CopyFolder(folder, dest, comp);
            }
        }
    }
```

Privileged Access Management Suite