Admin User Manual

This guide explains how admins can install, register, log in, and use key features on our endpoint security application. For instructions on the end-user app—covering installation, login, and usage please refer to the End-User Manual. You can request it from your organization's admin or the Vardaan sales team.

Admins are responsible for assigning licenses to end-users. Once assigned, the end-user's reports will be sent directly to the admin who assigned the license. Admins will also share the installation link with employees. Both admins and end-users install the app using the same link.

What's Inside This Guide

Getting Started

Installation, registration, and initial setup process for administrators

Admin Dashboard Features

Comprehensive overview of administrator control panel and key functionalities

USB Access Control

Managing and monitoring USB device access across your organization

Site Control

Configuration and management of site-wide security policies and restrictions

Audit and Blocked Reports

Detailed reporting on security events, blocked activities, and compliance tracking

License Management

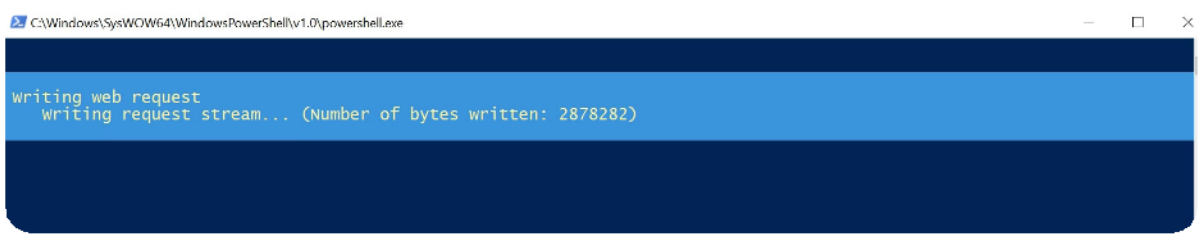
Assigning, tracking, and managing user licenses across your organization

Installation and Registration Guide

For the initial release of ViCTAA, we are offering two versions: a standard version and an advanced version with AI capabilities. The AI-enabled version is larger in size, and it is up to the administration to decide which option best suits the organisation and end users.

Step 1: Download and Install

- Click the installation link and download ViCTAA Lite or ViCTAA AI based on your requirement
  - If you encounter a message indicating an incomplete download, or if the downloaded file appears with a name like "Unconfirmed 530989.crdownload" and fails to complete, please refer to the troubleshooting instructions provided in the next section to resolve the issue.
  - If you encounter a "Virus detected" message during download, refer to the next section for troubleshooting steps.
  - Note: These exceptions are commonly encountered while installing software similar to ViCTAA
- After the download is complete, go to your **Downloads** folder.
- Locate the **ViCTAA.MSI** file (or ViCTAA_Lite.MSI)
- Double-click the file to begin installation
- If a "Windows protected your PC" dialog box appears, click More info, then select Run anyway to proceed
- If the dialog does not appear, proceed with the installation as usual
- Note: For ViCTAA_Lite, the installation proceeds as usual. For ViCTAA_AI, an additional file will be downloaded as part of the process. You will see the following download initiated(wait for it to complete):



Step 2: Launch with Administrator Privileges

- After installation, go to your Desktop and locate the ViCTAA application
- Alternatively, press the Windows button and search for ViCTAA.
- Right-click on the application and select Run as Administrator. Click Yes when prompted
- If the user cannot run the application as an administrator, they should follow the steps below.
  - "**Open Registry Editor:** Press the Windows key, type `regedit`, and press Enter.
  - **Navigate to the key:** Go to `HKEY_CLASSES_ROOT\Msi.Package\shell`.
  - **Add the "runas" key:** Right-click on the "shell" key, select "New", then "Key", and name the new key "runas".
  - **Add the "command" key:** Right-click on the "runas" key, select "New", then "Key", and name the new key "command".
  - **Set the default value of "command":** Select the "command" key, and in the right pane, double-click "Default". In the "Edit String" dialog, enter `msiexec /i "%1"` and click "OK".
  - **Test:** Close the Registry Editor and right-click on an .msi file. You should now see the "Run as administrator" option."
- Tip: To enable the application to run with admin privileges automatically from next time:
  - Right-click the application, select Properties
  - Go to the Compatibility tab
  - Check Run this program as an administrator, click Apply, then OK
- From the next scan onwards, you can launch it by simply double-clicking the app

Step 3: Register Your Account

- After installation, application will open automatically in your default web browser.
- Follow the on-screen prompts to create your account.
- Use your **admin email ID** to register.

Step 4: Log In

- After registration, you will be redirected to the login page.
- Enter your login credentials.
- Use the **OTP** sent to your registered email to complete the login.

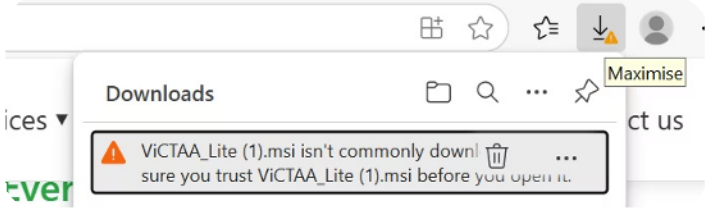
Note: To follows a hierarchical admin-user setup on Windows, we've included a step-by-step guide at the end of this document to help you configure the system appropriately. This is important for the effective implementation of ViCTAA: Polish this

Optional: You can configure the app to launch automatically at system startup. Instructions are provided at the end of this guide.

Troubleshooting

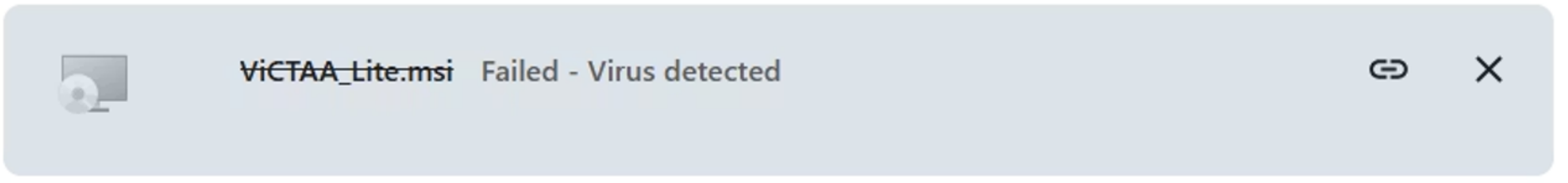
Resolving Incomplete Download: If you see a message indicating an incomplete download, and the file appears with the name "Unconfirmed 530989.crdownload", it means the download did not complete successfully. Follow the steps below to resolve this.

1. In your browser, click the download icon located near the top-right corner, next to your profile icon.

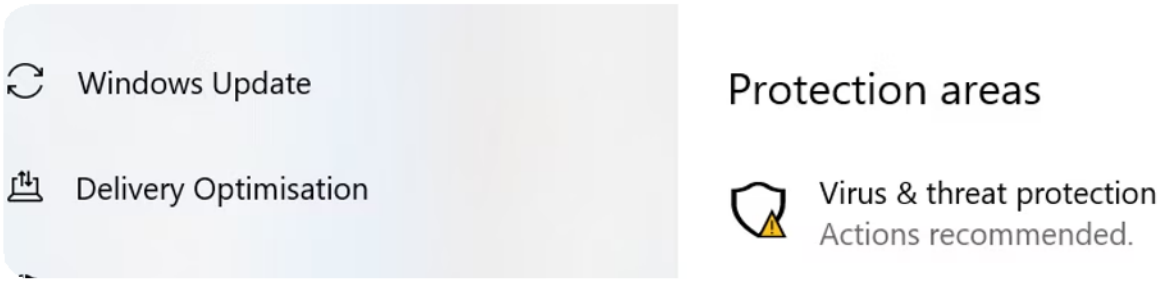


2. Hover over the warning message — a set of three dots will appear on the right side
3. Click on the three dots next to the Delete button
4. You will get the option to delete, keep, Report this file as safe, learn more, download link. Click on Keep
5. A dialog box will open with the message: “Make sure you trust ViCTAA_Lite (1).msi before you open it.” Click on “Show more” to reveal additional options.
6. Select “Keep anyway” to confirm.
7. The download will now complete successfully, and you can proceed with installation and use as outlined at the beginning of this manual.

Resolving Virus detected message



- Search for “Windows Security Settings” using the Start Menu search bar and click on the result.
- In the Windows Security window, select “Virus & Threat Protection” from the left-side panel or main dashboard.



- Under Virus & Threat Protection settings, click on "Manage settings".
- Toggle "Real-time protection" to Off. You can turn this back on once the installation is complete.

Admin Features

Upon successful login, admins are directed to the **Admin Dashboard**, where they can quickly view overall security reports at a glance.

1. Users and Reports

- The first section of the dashboard displays a list of all users associated with the admin.
- Admins can:
  - **View scan reports** for individual users.
  - **Select multiple users** using the checkboxes on the left to view combined reports.
  - **Check login status** for each user in real time.

☐	ID	Username	Actions	Login Status
☐	12	bhaskar	**View Report**	logged_in
☐	39	munisyam	**View Report**	logged_out
☐	45	test_for_license1	**View Report**	logged_out
☐	48	Prabhas	**View Report**	logged_out
☐	50	test_admin	**View Report**	logged_out
☐	51	tester	**View Report**	logged_out

Clicking View Report opens a new browser tab displaying the detailed scan report for the selected user. The report is organized into multiple sections, including AI-Predicted Threats and the following categories:

Detailed Scan Report Categories

System Information

- **CPU Information** - Detailed processor information including model, speed, and core count for performance monitoring
- **Memory Information** - Current memory usage, available memory, and optimization details
- **Disk Information** - Disk usage, health, capacity, and potential hardware failure identification
- **Battery Health** - Battery charge, capacity, and overall condition monitoring

Security & Threats

- **Threat Profile Summary** - Comprehensive summary of potential security threats with mitigation strategies
- **Service Accounts** - Active service accounts with usage tracking and permission management
- **Patch Updates** - System updates with latest patches to fix known vulnerabilities

Network & Connectivity

- **Network Information** - Real-time network interface monitoring, IP addresses, and bandwidth usage
- **Network Ports** - Open network ports monitoring for potential vulnerabilities
- **System Ports** - Active system ports verification for security
- **VPN Detections** - Active VPN connections for secure network traffic monitoring

USB & Device Management

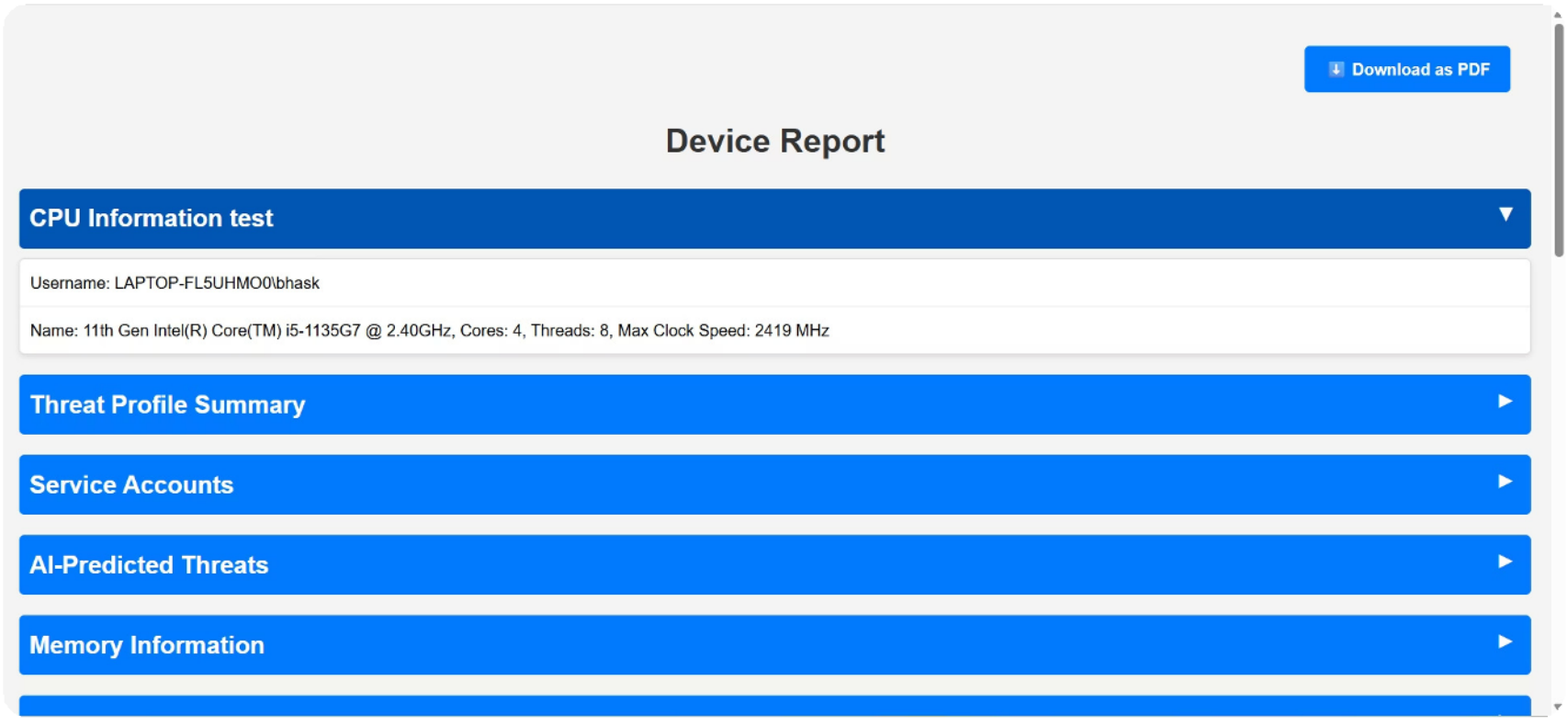
- **USB Ports Status** - Status of USB ports (active/disabled) for unauthorized access prevention
- **Detected USB Devices** - Currently connected USB devices listing
- **USB Activity History** - 10-day log of USB device activity tracking

Application & Usage Monitoring

- **Recently Used Applications** - Tracking of recently opened applications for usage analysis
- **Unused Applications** - Applications not used in the past 7 days for cleanup identification
- **VPN Usage History** - 24-hour VPN connection times and duration monitoring

Privacy & File Management

- **Cookies & Cache Files** - System cookies and cache management for privacy maintenance
- **Restricted Files** - Detection of restricted file types (e.g., .mp4, .mov, .mp3) to prevent unauthorized media transfer



2. Graphs and Insights

This section displays a consolidated summary of the **last seven scans** for the selected end-user. It includes key insights such as:

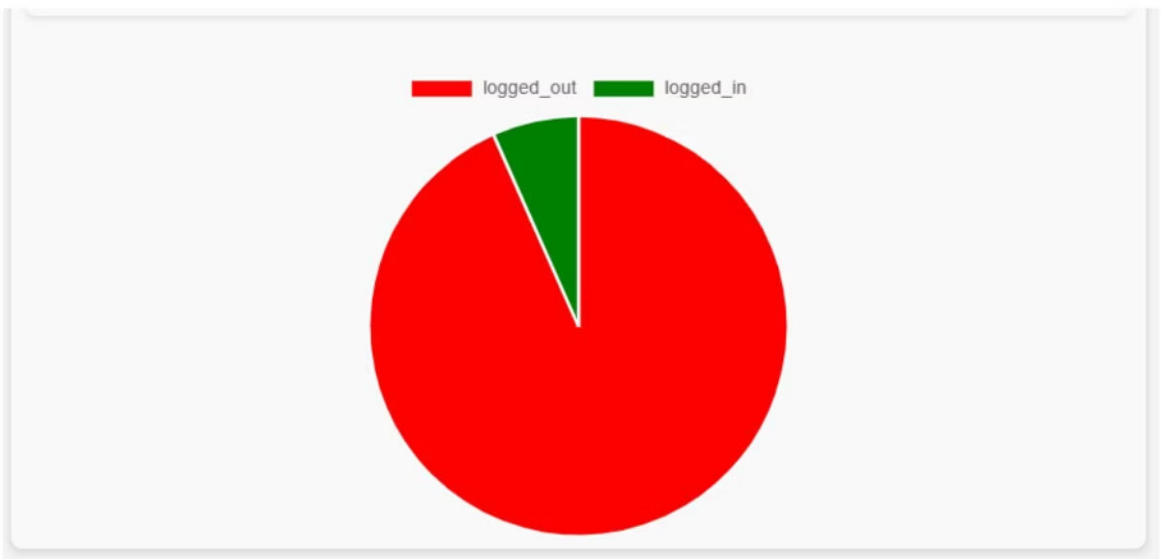
- Number of missing patches
- Detected vulnerabilities
- Installed software count
- Number of open and closed USB ports

To view the summary for different end-users, the admin must select the desired user from the dropdown located in the **top-right corner** of the dashboard.

3. Logged in VS Logged out users

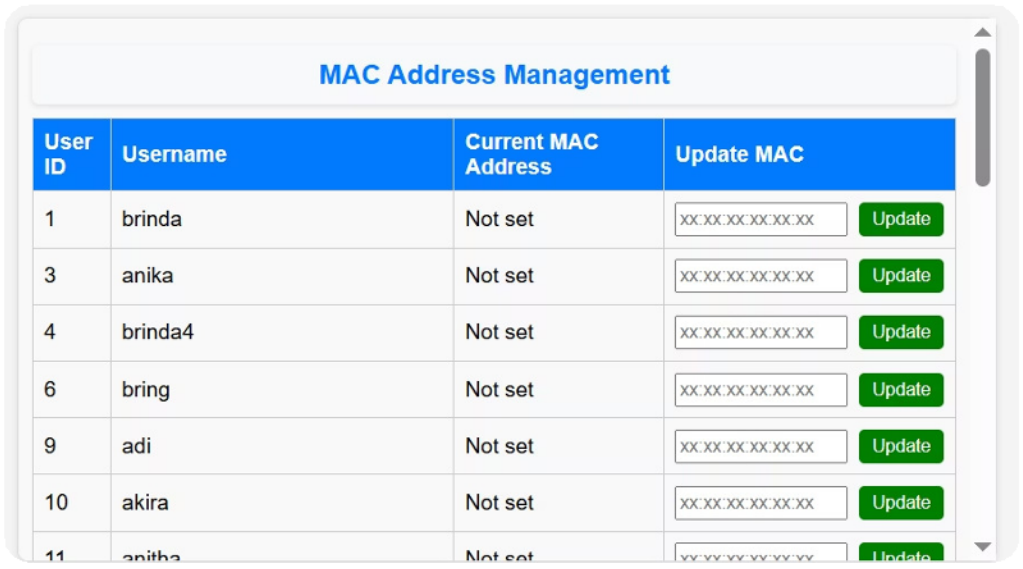
This section displays a **visual breakdown of logged-in vs. logged-out users**.

- Hovering over each section of the chart reveals the **total number** of users in that category.
- Clicking on any section lists the **user details**, including their email IDs, under each login status group.



4. Mac Address

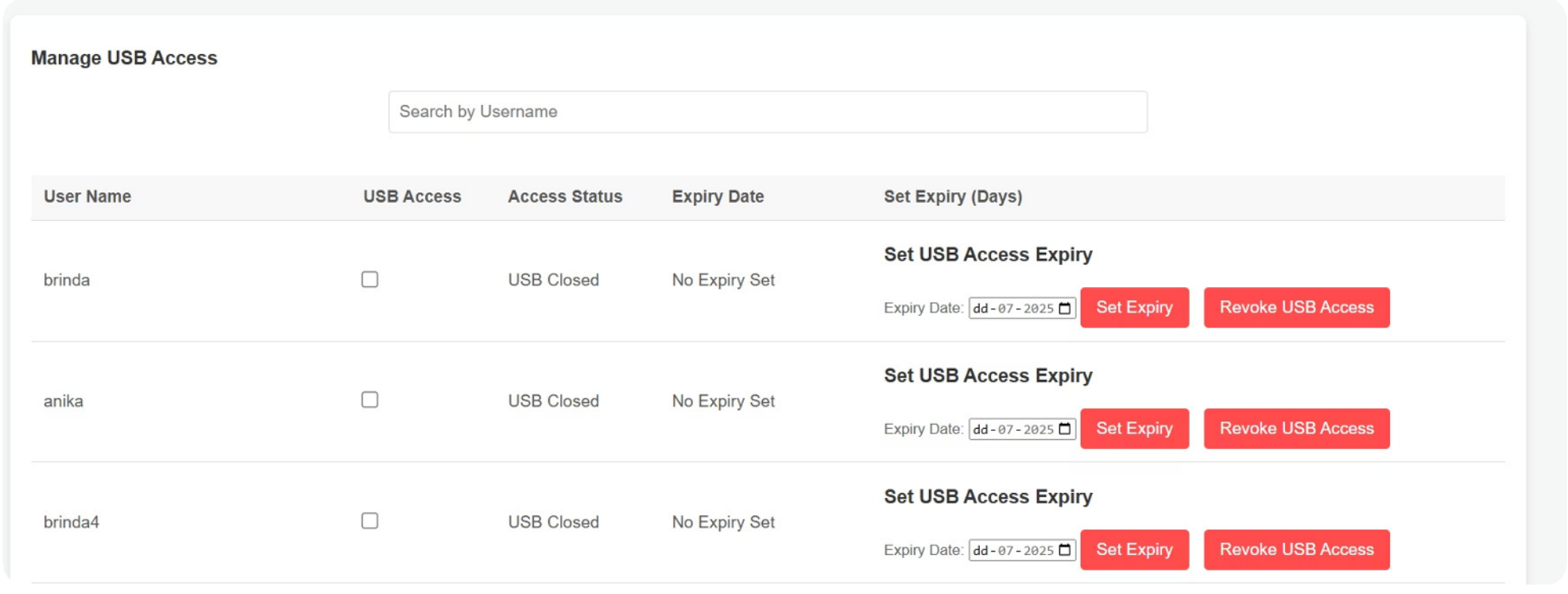
Admins can manually add or update a user's MAC address if it hasn't been auto-populated by the system.



USB Access Management System

To manage USB permissions, admins can navigate to the **USB Control** tab in the top navigation bar.

- To grant USB access to a specific user for a limited time, select the user, choose an **expiry date**, and click **Set Expiry**.
- To revoke USB access for any user, click the **Revoke USB Access** button next to their name

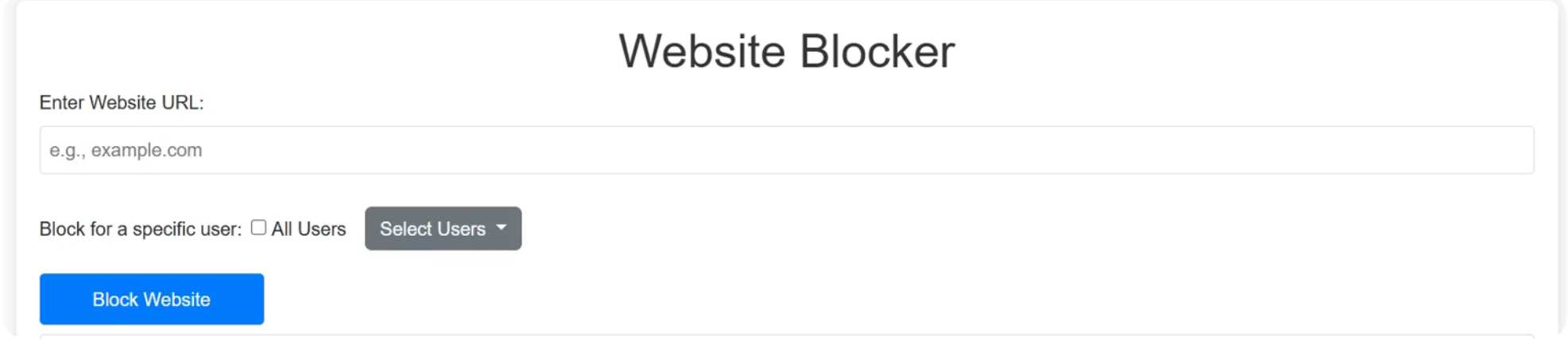


Site Control

The **Site Control** section allows admins to block or unblock websites for one or more users.

To block a website:

1. Click on the **Site Control** tab in the top navigation bar.
2. Enter the website URL in the input field.
3. Click **Select Users** to choose users individually, or use the **Select All Users** checkbox to apply the rule to all users.
4. Once the website and users are selected, click **Block Website** to apply the restriction.



Unblock Website

To unblock a website for specific users, the admin can use the search bar to locate the website from the list below. Once found, they can view the list of users it is blocked for and click the Unblock button next to each user to remove the restriction.

Search blocked websites

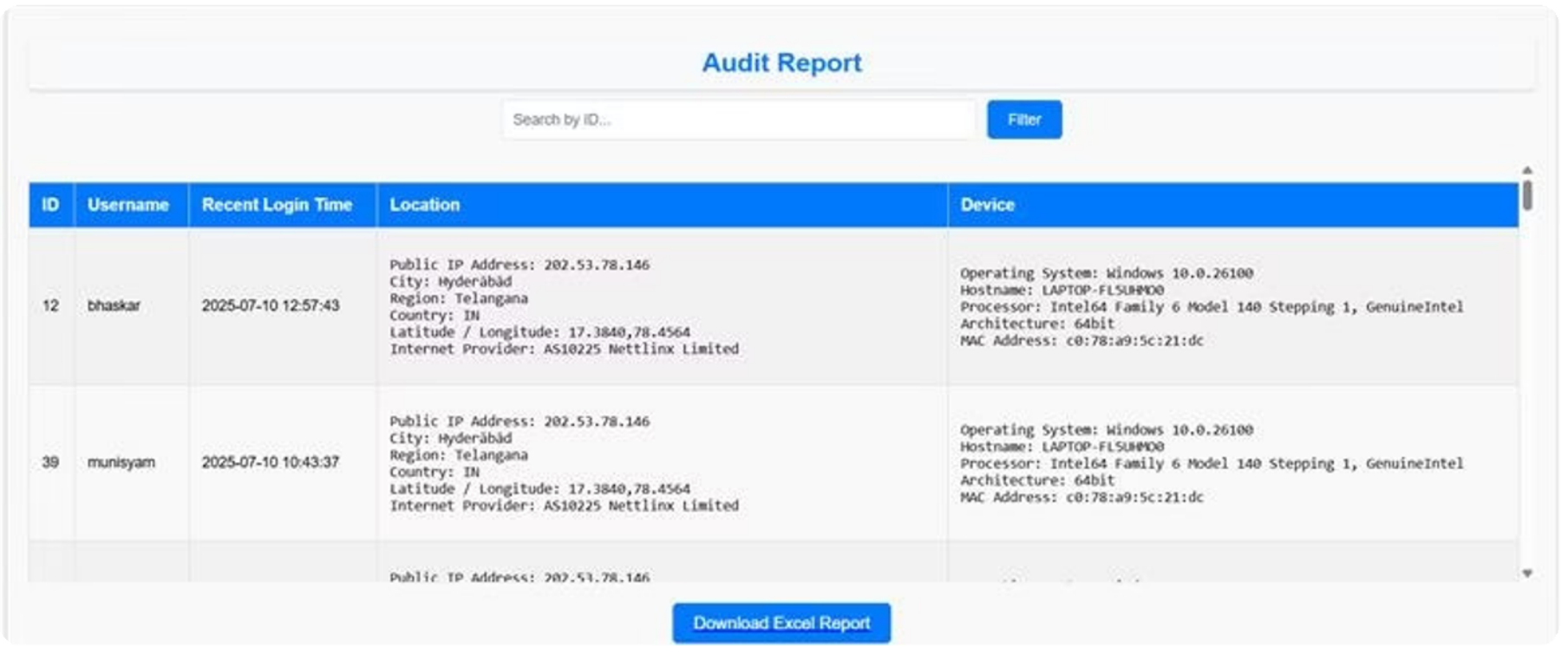
ID	Blocked Website	User ID	Username	Action
154	amazon.in	28	Vikas	**Unblock**
65	bookmyshow.com	20	Alice	**Unblock**
153	bookmyshow.com	27	Bob	**Unblock**
61	example.com	17	Praharshitha	**Unblock**
87	fed.com	26	Akhilesh	**Unblock**
71	friday.com	12	Bhaskar	**Unblock**

Audit Report

To access audit details, the admin clicks on the **Audit** tab and selects **Audit** from the dropdown. This section displays the following information for each user:

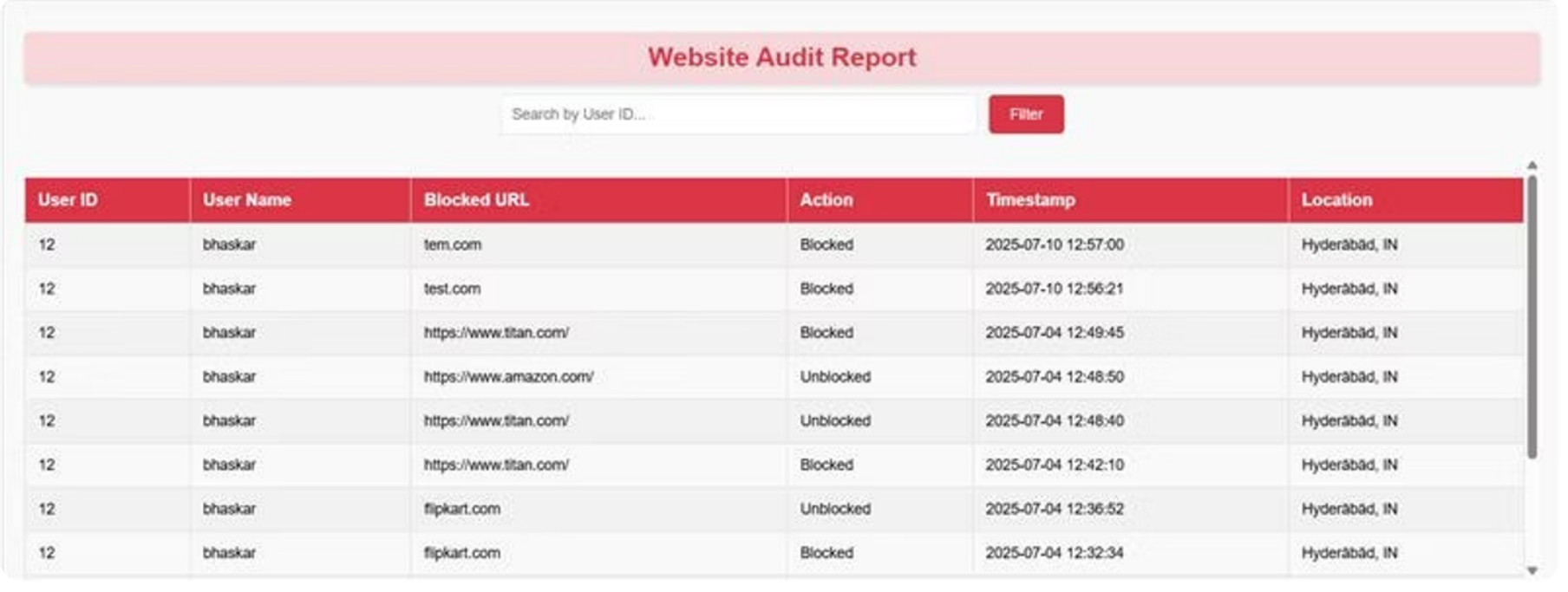
- Recent login time
- Location
- Device details

To download these records, click **Download Excel Report**. This will generate and save the report in Excel format for further analysis or documentation.



Blocked Report

This section displays a list of all websites blocked by the admin. To export the data, click the **Download Excel Report** button to download the list in Excel format.



Licensing

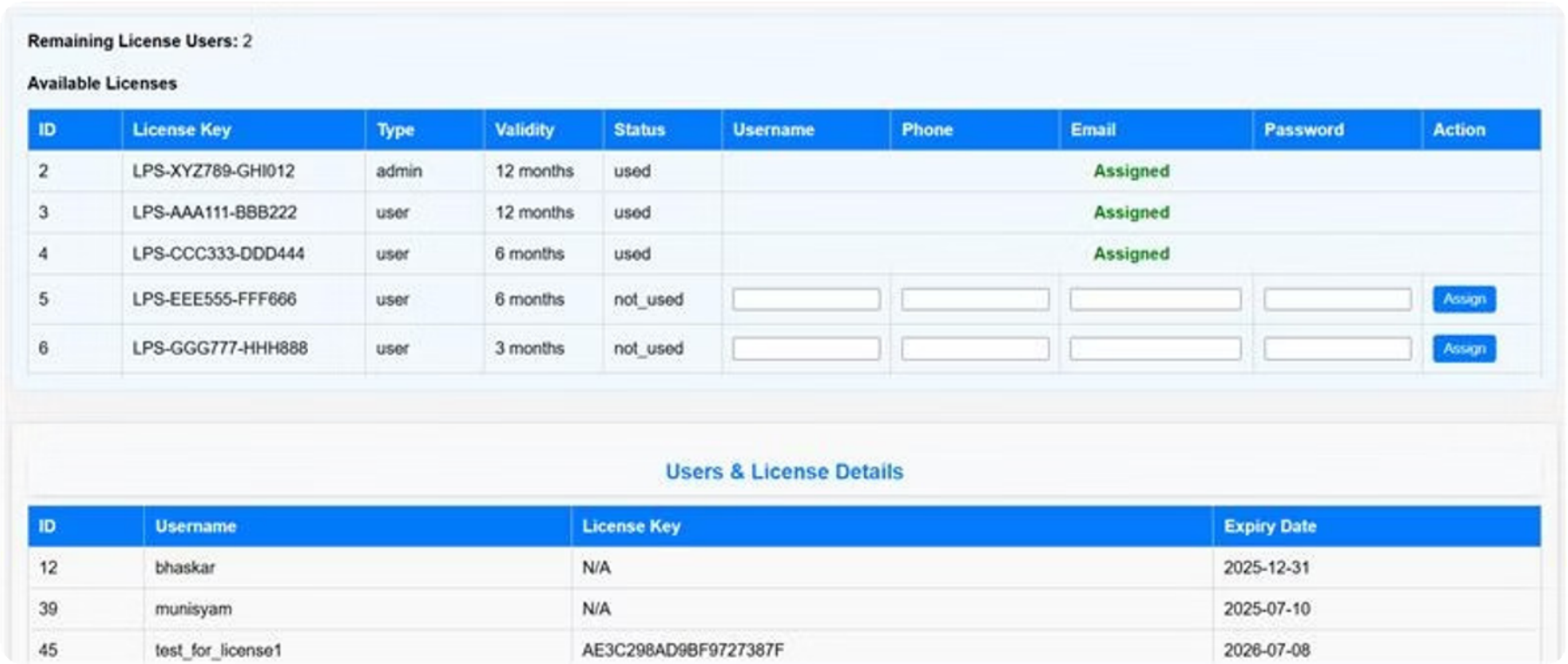
This section allows admins to assign licenses to users. Admins can view all purchased licenses and assign them by entering the required details, including:

- User's email address
- Phone number
- Temporary password (which the user can reset later)

After filling in the necessary information, click the **Assign** button. The assigned user will receive an email with login credentials linked to their email address.

> **Important:** Each license can be assigned to only one user, and each user can be linked to only one license.

To revoke or reassign a license, please contact the Vardaan admin or sales team.



Remaining License Users: 2

Available Licenses

ID	License Key	Type	Validity	Status	Username	Phone	Email	Password	Action
2	LPS-XYZ789-GHI012	admin	12 months	used			Assigned		
3	LPS-AAA111-BBB222	user	12 months	used			Assigned		
4	LPS-CCC333-DDD444	user	6 months	used			Assigned		
5	LPS-EEE555-FFF666	user	6 months	not_used					Assign
6	LPS-GGG777-HHH888	user	3 months	not_used					Assign

Users & License Details

ID	Username	License Key	Expiry Date
12	bhaskar	N/A	2025-12-31
39	munisyam	N/A	2025-07-10
45	test_for_license1	AE3C298AD9BF9727387F	2026-07-08

Implementation of Hierarchical Admin-User Setup in Windows.

Creating a hierarchical user account set-up as Admin and Users

Creating the New Administrative Account

1. Press Win + I to open the Windows Settings application and navigate to the Accounts section, then select Other users from the left sidebar menu.
2. Click on the Add account button to begin the process of creating a new user account for administrative purposes.
3. When prompted for sign-in information, select "I don't have this person's sign-in information" to create a local account rather than a Microsoft account.
4. Choose "Add a user without a Microsoft account" to proceed with local account creation, which provides better control over the account configuration.
5. Enter a username such as "SystemAdmin" or "Administrator" and create a strong password for this account, then click Next and Finish to complete the initial account creation

Elevating the New Account to Administrator Status

1. While still in the Accounts settings under Other users, locate the newly created account in the user list and click on it to access account options.
2. Select "Change account type" from the available options and change the account type from Standard User to Administrator using the dropdown menu.
3. Click OK to confirm the changes and grant full administrative privileges to the new account.

Converting Your Original Account to Standard User Status

1. Sign out of your current account completely and sign into the newly created administrative account using the credentials you established.
2. Once logged into the admin account, open Settings again and navigate to Accounts, then Other users to manage the existing accounts.
3. Locate your original account in the user list and click on it, then select "Change account type" to modify its privileges.
4. Change the account type from Administrator to Standard User, which will remove administrative privileges while preserving all existing data and settings.
5. Click OK to confirm this change, effectively creating the hierarchical structure with the new admin account having full control and your original account operating with restricted privileges.

Ensuring complete transfer of information and data to the existing User account

Verifying Data Preservation During Account Conversion

1. The conversion process from administrator to standard user automatically preserves all existing data, documents, settings, and personal files within your original account without any manual transfer required.
2. Log back into your original account, which is now a standard user account, to verify that all your documents, desktop files, downloads, pictures, and other personal data remain intact and accessible.
3. Check that all your personalized settings including desktop wallpaper, taskbar configuration, browser bookmarks, and application preferences have been preserved during the account type conversion.

Confirming Application and Settings Accessibility

1. Verify that previously installed applications that were installed for your user profile specifically remain functional and accessible from your standard user account.
2. Test access to your email accounts, cloud storage synchronization, and other personal services to ensure they continue working properly under the new account structure.
3. Confirm that any custom folder structures, file organization systems, and shortcuts you had established continue to function as expected in the standard user environment.

Setting up of rules and restrictions on Application installation and uninstallation on the user account

Configuring User Account Control Settings

1. From the administrative account, press Win + R and type "msconfig" to open the Microsoft System Configuration utility, then navigate to the Tools tab.
2. Select "Change UAC Settings" from the tools list and click Launch to access User Account Control configuration options.
3. Set the UAC slider to "Always notify" position to ensure maximum security and require administrator credentials for any system changes or application installations.
4. Click OK to apply these settings, which will prevent the standard user account from installing or uninstalling applications without explicit administrator approval.

Implementing Group Policy Restrictions for Enhanced Security

1. Press Win + R and type "gpedit.msc" to open the Local Group Policy Editor, which allows for granular control over system permissions and restrictions.
    a. If gpedit.msc is not available on your system, run the following commands in Command Prompt (as Administrator) to enable access to the Group Policy Editor.
    FOR %F IN ("%SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientTools-Package~*.mum") DO (DISM /Online /NoRestart /Add-Package:"%F")

    FOR %F IN ("%SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~*.mum") DO (DISM /Online /NoRestart /Add-Package:"%F")
2. Navigate to Computer Configuration, then Administrative Templates, followed by Windows Components, and finally Windows Installer to access installation-related policies.
3. Locate and enable the "Prohibit User Installs" policy to prevent standard users from initiating any installation processes without administrative intervention.
4. Configure the "Always install with elevated privileges" setting to ensure that when installations do occur, they are performed with full system privileges and affect all user accounts.

Establishing Software Restriction Policies

1. Press Win + R and type "secpol.msc" to open the Local Security Policy editor, then navigate to Software Restriction Policies in the left panel.
2. Right-click on Software Restriction Policies and select "Create Software Restriction Policy" to establish new restrictions on executable files and installations.
3. Configure path rules to prevent execution of installers and setup files from userwritable directories such as Downloads, Temp, and user profile folders.
4. Set the default security level to "Disallowed" for unsigned or unrecognized installation packages, requiring explicit administrator approval for all software installations

How to install an application on Admin system in order for it to also reflect on the user system

Proper Installation Methodology for System-Wide Application Access

1. Log into the administrative account and locate the application installer that you wish to install for system-wide access across all user accounts.
2. Right-click on the installer file and select "Run as administrator" to ensure the installation process has full system privileges and can modify system-wide settings.
3. During the installation process, carefully select "Install for all users" or "Install for everyone on this computer" when presented with installation scope options.
4. Choose installation paths within system directories such as C:\Program Files or C:\Program Files (x86) rather than user-specific directories to ensure accessibility across all accounts.
5. Complete the installation process while ensuring that all components, shortcuts, and registry entries are configured for system-wide access rather than user-specific access.

Configuring Post-Installation Settings for Multi-User Access

1. After installation completion, navigate to the Start Menu and verify that the application appears in the "All Programs" section rather than being limited to the administrator's personal programs.
2. Check the application's installation directory to confirm proper file permissions that allow standard users to read and execute the application files while preventing modification.
3. Test the application's functionality by logging into the standard user account and launching the application to ensure it operates correctly without administrative privileges.

Verifying Application Accessibility and Functionality

1. From the standard user account, attempt to launch the newly installed application to confirm it appears in the Start Menu and functions properly without requiring elevation.
2. Test all major features of the application while logged in as the standard user to ensure that the installation was configured correctly for multi-user access.
3. If the application requires specific permissions or registry access, return to the administrative account to configure these permissions appropriately without compromising system security.
4. Document any applications that require special configuration steps so that future installations can follow the same methodology for consistent multi-user accessibility

Optional: Configure to Run at Startup

To ensure the app launches automatically when the system starts, follow these steps:

Step 1: Open Task Scheduler

- Press **Win + R**, type **taskschd.msc**, and press **Enter** to open Task Scheduler.

Step 2: Locate the ViCTAA Task

- In the **Task Scheduler Library**, locate the ViCTAA task.

Step 3: Configure Triggers

- Right-click the ViCTAA task and select **Properties**.
- Go to the **Triggers** tab.
- Click **New**, then:
- Set **Begin the task** to **At startup**.
- Click **OK** to save the trigger.

Step 4: Configure Actions

- Go to the **Actions** tab.
- Click **Edit** (or **New** if no action exists).
- In the **Program/script** field, browse and select ViCTAA executable (e.g., **victaa.exe**).
- Click **OK** to save the action.

Step 5: Finalize and Save

- Click **OK** on the task properties window to apply all changes.

Note: The app will now automatically launch at system startup with administrative privileges, if configured accordingly.

Contact Us

For more information and guidance please contact us

📧**Email:** info@vardaanglobal.com

📞**Phone:** +91 40-35171118, +91 40-35171119

📍 **Address:**

Aurum, 1st Floor, Plot No 57, Jayabheri Enclave,

Gachibowli, Hyderabad – 500032, INDIA

🌐 **Website:** https://vardaands.com