Paws Studio – Beginner's Guide

Multiple Award Winning Security Software

Version 4.14 (Paws Studio 3.2.6)
Published May 2019

Titania Limited
Security
House
Barbourne Road
Worcester
WR1 1RS

Telephone: (+44)1905 888 785
Technical Support: Support@titania.com
Licensing: Enquiries@titania.com
Nipper Studio Support: https://www.titania.com/support/paws-studio

Contents

Overview

Paws Studio enables you to produce comprehensive security & compliance reports for your workstations and servers. A report can consist of a single or multiple audits, with many audit types included.

Paws Studio is highly configurable, allowing you to modify or build upon the already included report types using the Policy Editor, harnessing the power of the Paws Studio Check Library.

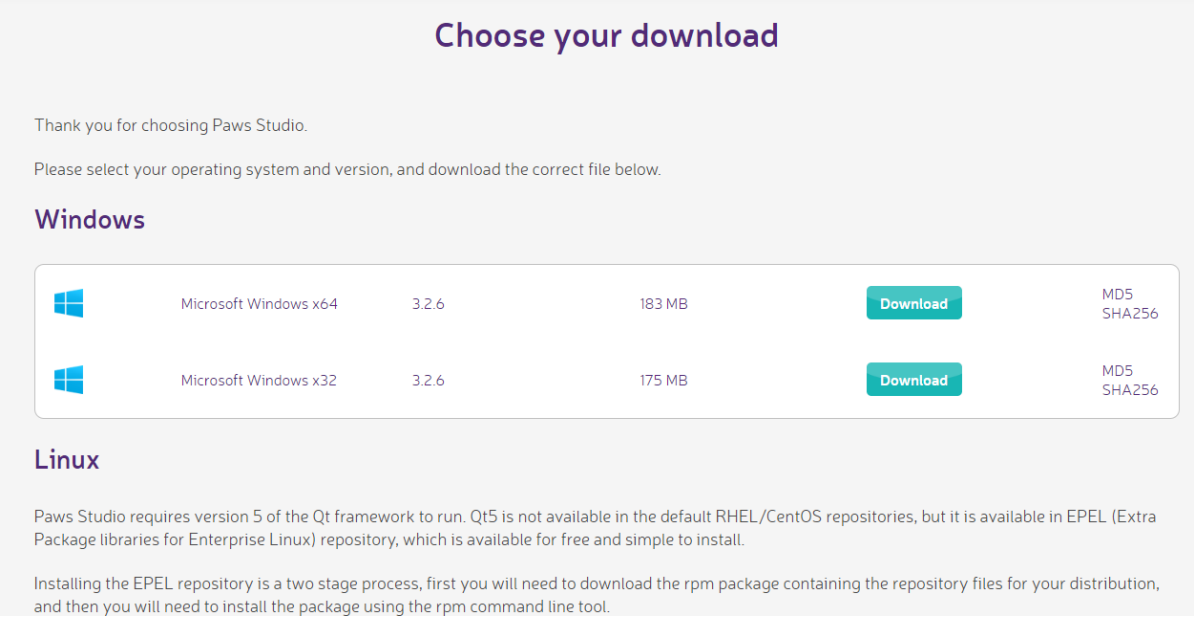
Paws Studio will significantly aid you in auditing your devices, checking compliance against published standards, or ensuring compliance with your own benchmarks.

Downloading Paws Studio

Navigate to https://www.titania.com/download/paws-studio and click Log In (create an account if you do not have one already).

Your Product Licenses page will be displayed showing the license details and a download button for your purchased products.

You will be taken to the download page for Paws Studio where you are presented with several download choices depending on the operating system you wish to install Paws Studio on (ie. Windows or Linux).

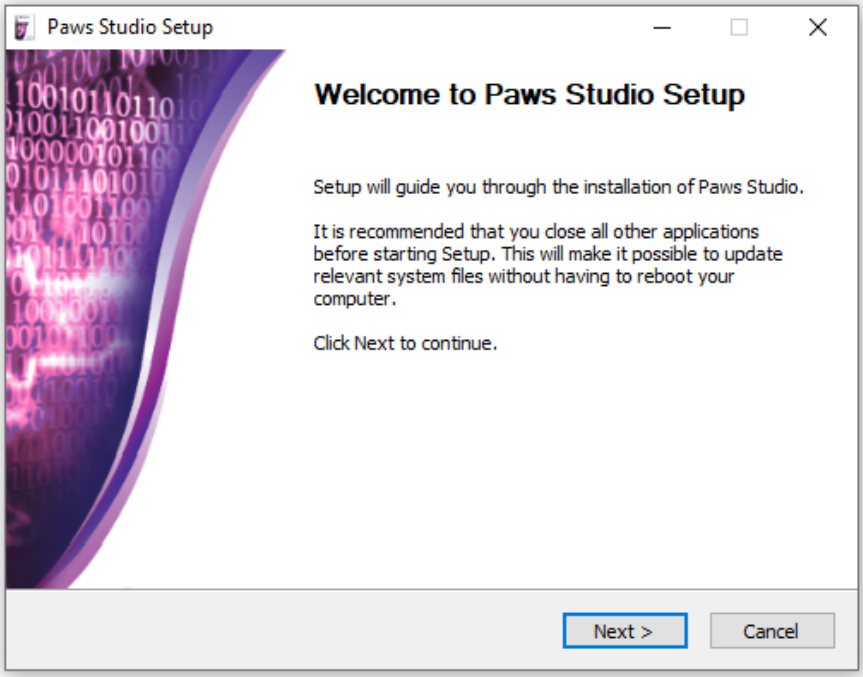


Clicking on the download button for your chosen version will begin the download of the Paws Studio installer.

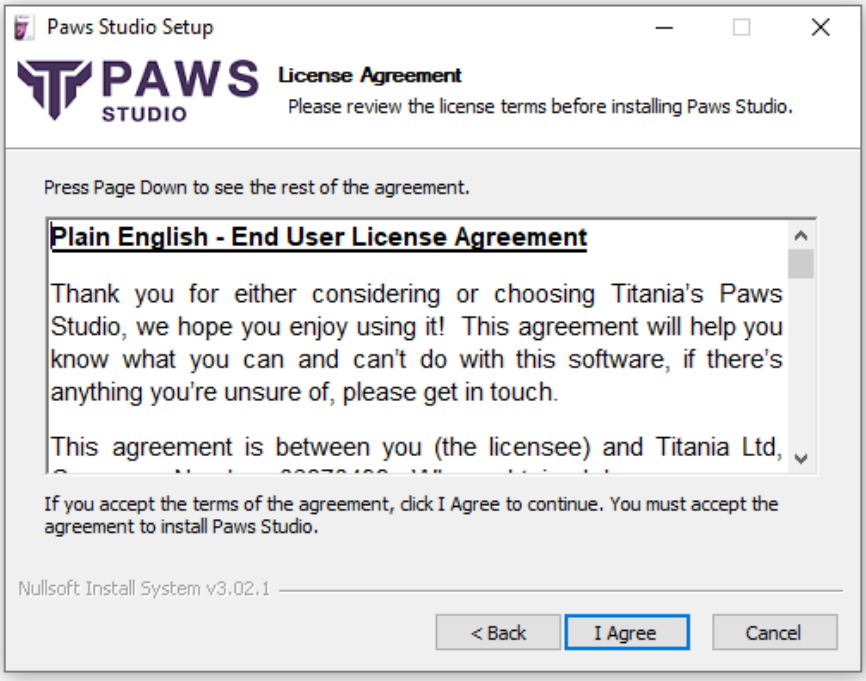
Installing Paws Studio on Windows Operating Systems

Once downloaded, navigate to the download location and run or double click the Paws Studio executable.

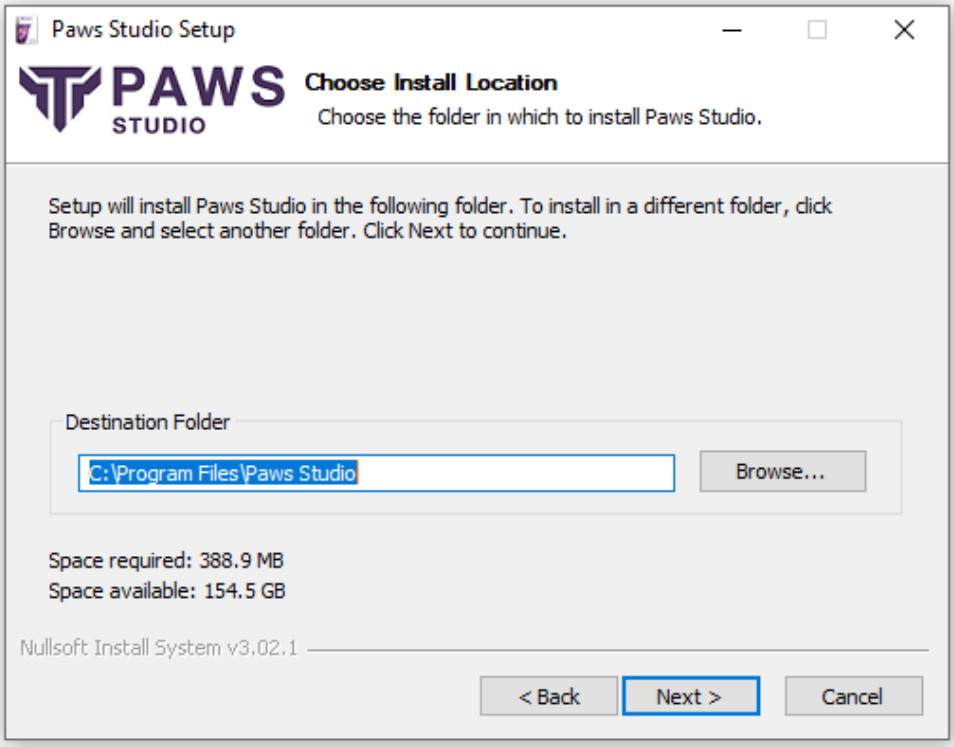
On the Welcome screen click Next.



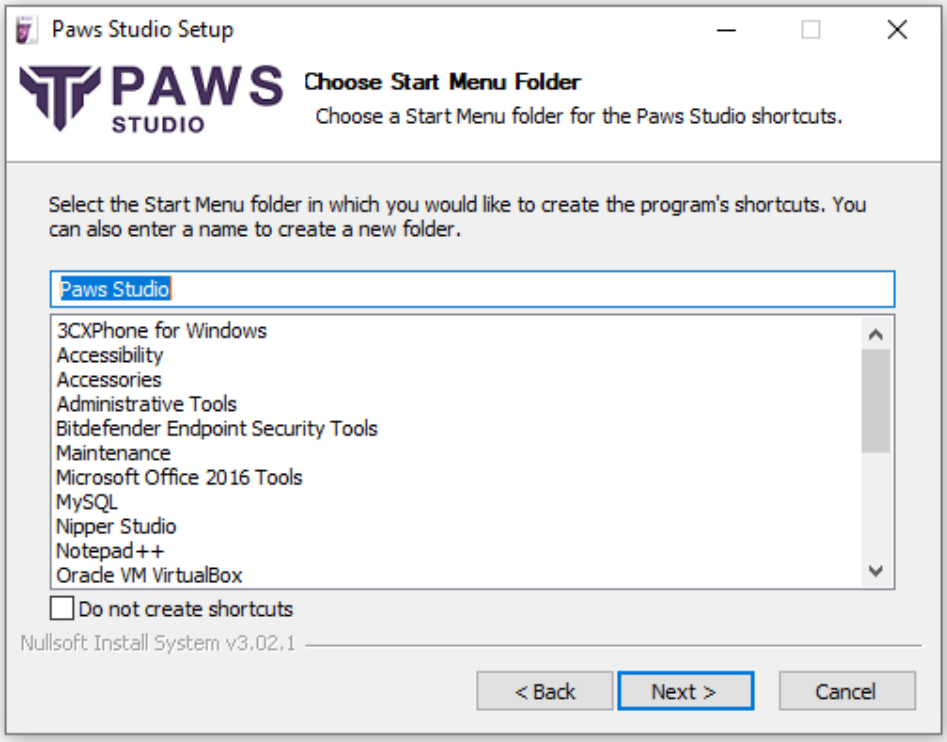
Read and agree to the end user license agreement to continue.



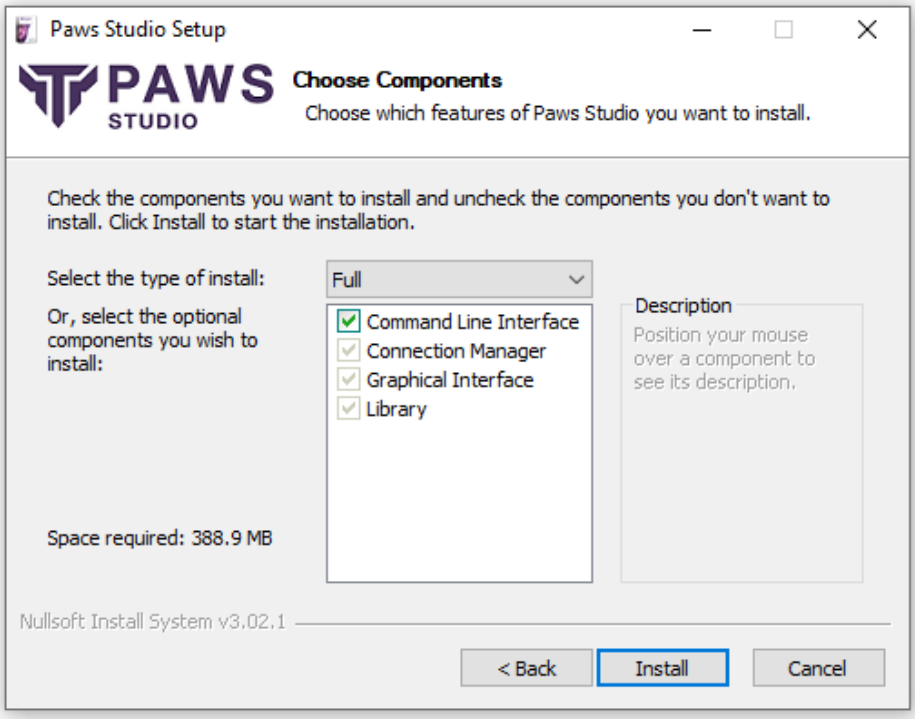
Paws Studio will suggest a default location to install. If you wish to amend this click Browse and navigate to your chosen installation location. Click Next to continue.



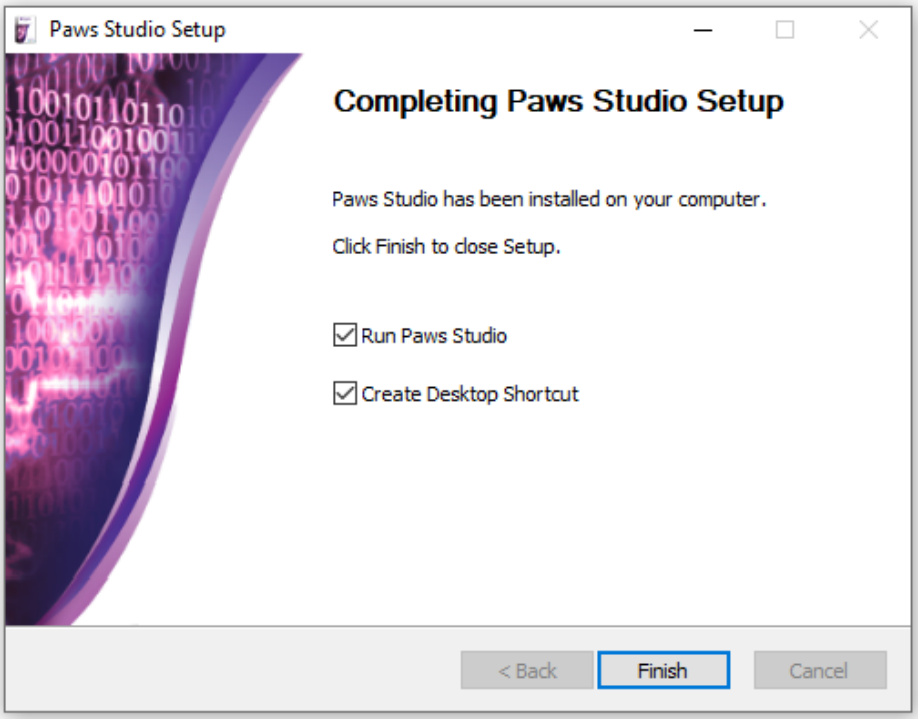
The install wizard will suggest a new Start Menu folder by default. You may rename this as required. Click Next to continue.



Choose the type of install. Full is recommended. The installation wizard will confirm how much space is required. Click Install when you are happy to proceed.



Paws Studio will now install. When complete you have the option of creating a desktop shortcut and launching Paws Studio. Click Finish to complete the installation process.



Installing Paws Studio on Linux Operating Systems

Installation Pre-requisites

Paws Studio requires version 5 of the Qt framework to run. Qt5 is not available in the default RHEL/CentOS repositories, but it is available in EPEL (Extra Package libraries for Enterprise Linux) repository, which is available for free and simple to install.

Installing the EPEL repository is a two stage process, first you will need to download the rpm package containing the repository files for your distribution, and then you will need to install the package using the rpm command line tool.

You can copy and run the commands for your Linux distribution before attempting to install Paws Studio, and the Qt5 dependencies should be resolved for you.

CentOS 7 (x64)

The new repository for epel's that CentOS 7 requires to run Paws Studio can be found here: http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-11.noarch.rpm

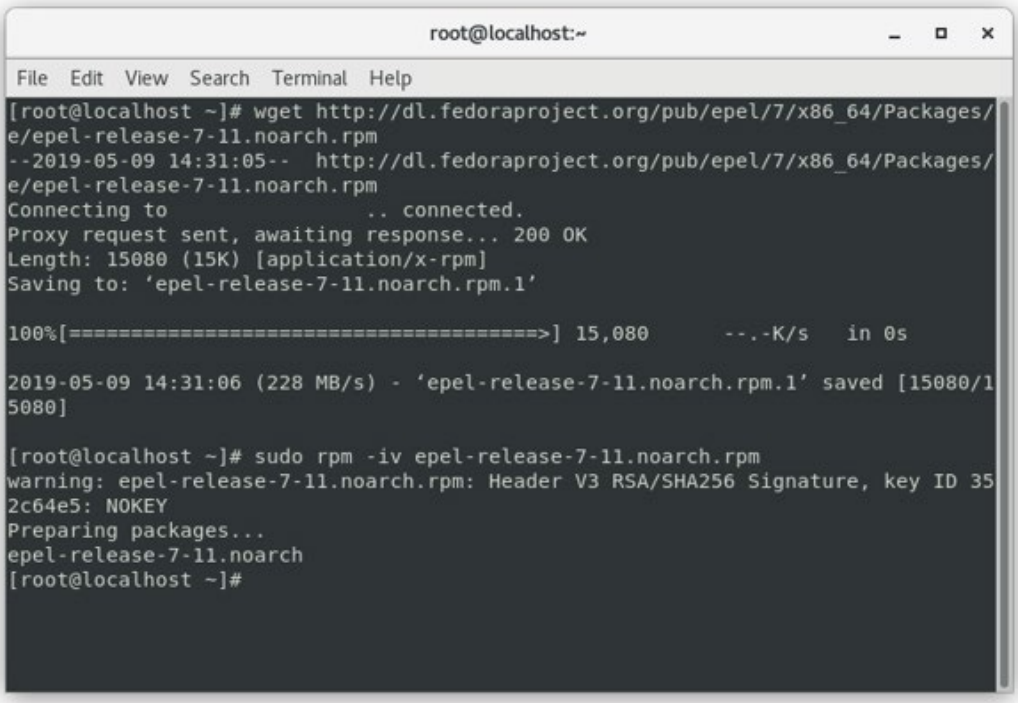
Once downloaded run the following command to remove the old repository:

"rpm –e epel-release-[version-number].noarch".

In order to install the new repository onto your machine, run the command:

“rpm –iv epel-release-7-11.noarch.rpm”

If you still encounter issues running Paws Studio on CentOS 7, try editing the repository file in: /etc/yum.repos.d/epel.repo

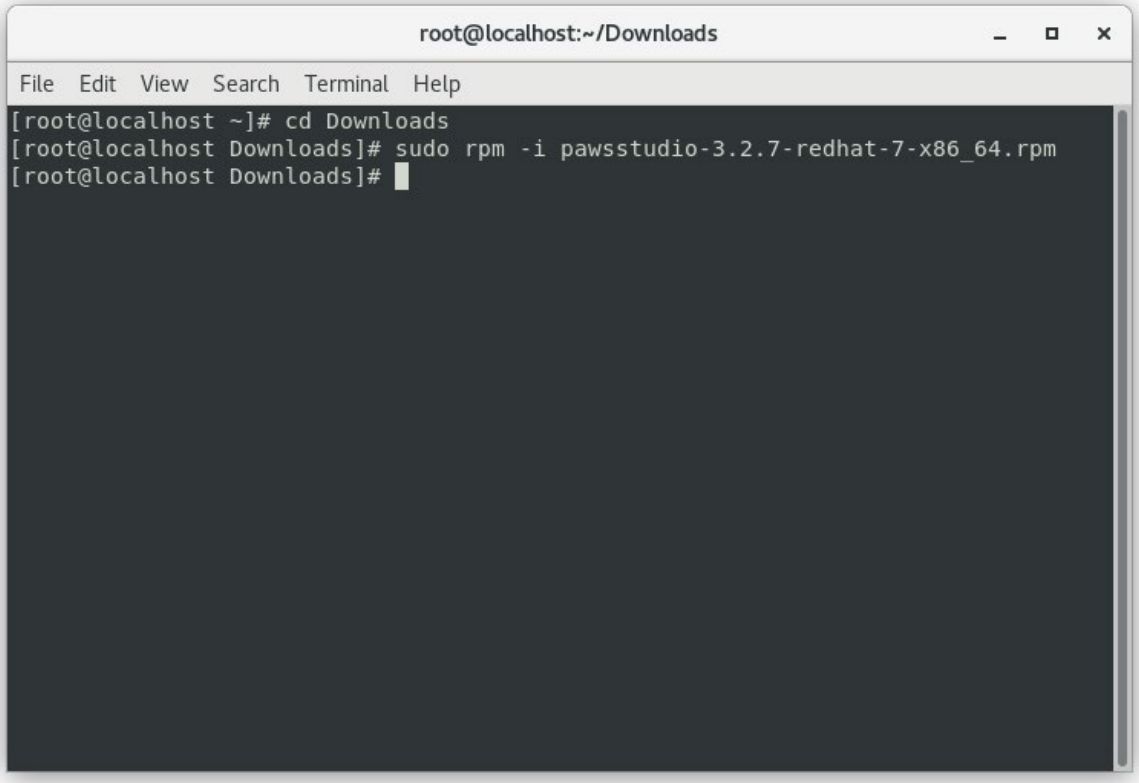


Installing Paws Studio on CentOS and RedHat Operating Systems

Within the terminal change directory to the location you have downloaded the installer to using **cd [download location]**

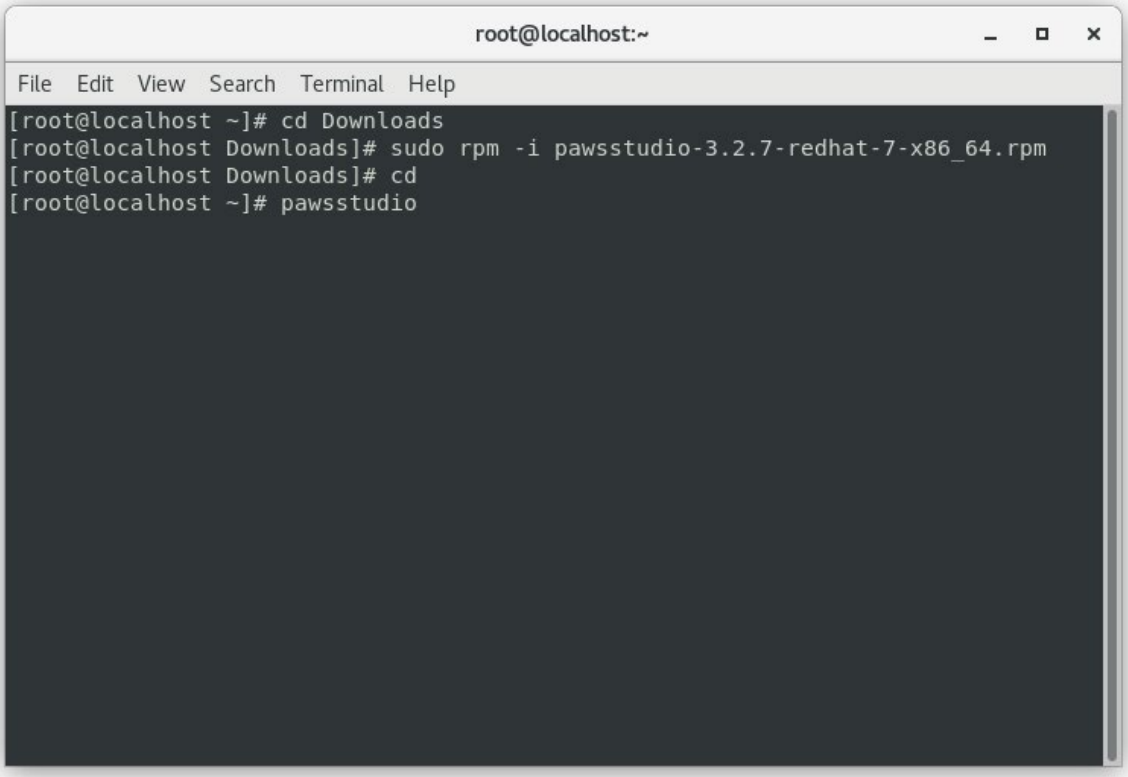
Run installation command:

sudo rpm –i pawsstudio-x.x.x-redhat-7-x86_64.rpm (where x.x.x is the Paws studio version downloaded ie. 3.2.7) – replacing redhat-7 with CentOS as required.



If successful the terminal will show no errors and return to a prompt. Type **cd** to return to the root.

You are now able to run Paws Studio using the command **pawsstudio**



Create a New Report

The **Create a New Report** option provides a simple interface to create your own audit report. This can be done by clicking **Create a New Report** from the shortcuts bar, going to **File> New Report** or by pressing **Ctrl+N**.

Create Report

Select Audit Reports

The audit selection screen allows you to select which audit types you wish to include in your report. You can include any combination of audits, however, some audits are only available on certain operating systems. Paws Studio will filter these as much as possible.

This screen will display all available audits, including the pre-build selection and any custom audits created using the Policy Editor.

If Paws Studio data files (.paws extension) have been manually retrieved using the **Data Collector**, you can include this information in your audit using the **Add Manual Files** option or you can scan a directory for the Paws Studio data files using **Scan Directory**.

Select Devices

Paws Studio allows you to audit your local device, to do so, simply add the device by selecting **Add Local Device**. Paws Studio will attempt to auto-detect your operating system and device name.

It is also possible to audit a device which can be connected to, over a local network connection. Adding network devices is done using the **Add Network Device** option, simply provide the IP address or machine name of the device, along with an *Administrative* username and password and operating system for that device.

Note: The data collection process requires admin access, so Administrator (or root for Linux devices) credentials are required.

To remotely audit a **Windows** machine, the target machine needs *File and Printer sharing* to be **enabled**. In addition, if the target machine is running a Windows version later than XP, it may require editing the registry to enable sharing administrative-access with a remote device. To do this:

- Open the *Registry Editor* on the target machine.

- Navigate in the tree to *H_KEY_LOCAL_MACHINE_SOFTWARE\MicrosoftWindows\CurrentVersion\Policies\system*
- Right click, hover over **New** and click **DWORD (32bit) value**. Edit the name to be **LocalAccountTokenFilterPolicy** and set the value to **1**.
- The target machine must then be rebooted for the change to take effect.

In order to remotely audit a **Windows XP** device from a **Windows** Machine, an additional compatibility step is required. *Samba version 1.0* must be enabled on the source machine to ensure that a connection to **Windows XP** is successful.
To do this:

- Click **Start** and perform a search for *Turn Windows Features ON or OFF*
- **Enable** the *SMB 1.0/CIFS File Sharing Support* node.

Paws Studio also provides some handy tools to auto-detect network devices: these are **Network Scan** and **Scan IP Range**.

An alternative method of adding network devices is through the *Network CSV Options > Import Network CSV* option. This allows you to select a CSV file containing the details of a network device on each row. The format for each row of a CSV file must be:

IP Address, Operating System, Username(Optional), Password(Optional)

It is also possible to export the contents of the device list to a CSV file for use at a later time through the *Network CSV Options > Export Network Devices as CSV* option.

You can include any combination of these devices in your audit.

Note: Self Certification Reports, such as DCPP CSM, do not require devices to be included in the report.

Report Generation

Once all devices and audits have been included, Paws Studio will begin creating your report. Using various mechanisms, Paws Studio collects required information from the device in real-time to allow a report to be produced.

Once this process is completed, your results are displayed, including how long generation took and also any issues the process may have encountered along with possible solutions.

Your Audit Report

Your audit report will be displayed to you in an easy to read format. The report includes a summary of your audit report which can be navigated through by clicking different sections with an easy to see contents bar which can be turned on/off by going to **View> Contents**.

Your report contains a few main sections:

- **Summary**

  Describes the devices and audit reports conducted on the device(s), these devices had their configurations assessed and are interactive; clicking on an audit report will take you to the results of the audit.

- **Contents**

  Provides links to key sections of your report. This can be toggled in View> Contents.

- **Audits**

  Audit reports are listed and can be viewed by clicking on the image or name of the audit report.

  Result Control & Comments

  Paws Studio allows users to manage the results of their compliance. If you wish to override the result of a compliance check, simply select **Change** next to the result icon. This new result is then reflected across your whole report.

  Paws Studio also provides a comments area to leave notes and important information which can be later referred to.

  Rerunning Results

  Paws Studio can quickly recheck the result of a compliance check by selecting the **Re-Run**button from the check screen. This will in real-time, reassess the scope against that single check and reassess all results.

  Save & Load

  Paws Studio allows you to save and load reports so work can be continued at a later point. Simply select **File> Save** or **Ctrl+S**, you will then be asked where you would like to save your report.

To open a save report, select **File> Open** or **Ctrl+O** and select your report.

Export Report

Paws Studio allows you to save/export your report in the following formats:

- Web Browser
  - This allows for printing through your default web browser.
- HTML
- PDF
- CSV(s) to directory
- XML
- ASCII

By default, exporting a report will export the complete report. If you wish to just export a single page navigate to **File> Export> Export Single Page** and select an option.

Audits

Paws Studio creates reports against audits. Within Paws Studio are pre-built report types you can include in your reports:

- **Configuration Report**
- **Compliance Reports**
  - **STIG** Security Technical Implementation Guide
  - **CIS Benchmarks** Center for Internet Security Benchmarks
  - **OVAL** Compliance System Assessments
  - **USGCB** United States Government Configuration Baseline
  - **Cyber Essentials**
  - **PCI DSS** Payment Card Industry Data Security Standard Compliance Report
- **Database Compliance Reports**
  - **MS SQL Server 2014** Database Security Technical Implementation Guide

- **Legacy Compliance Reports**
  - **Cyber Essentials** (Pre-March 2017)
  - **SANS** Institute Computer Security Policy Report
  - **NSA 2013** Guidelines
  - **NERC CIP 007-4** Systems Security Management
- **Self Certification Reports**
  - **DCPP** Defense Cyber Protection Partnership

Additionally you can create and use your own using the Policy Editor.

Note: Depending on your license, some of these audits may be unavailable.

Policy Editor

The Policy Editor is a tool to allow you to create your own policies. Policies can be created from scratch, or use a current policy as a template to modify.

The Policy Editor provides tools to add and remove sections of your policy. The tree structure allows you to quickly navigate through your policy.

Once selecting a section, the information bar or the right, displays details about that section. These can be modified as required.

Once you have finished creating and saved your policy, it will be available on the **Select Audits** page so reports can be generated against it.

Custom Policy Management

Your policies can be managed through the Settings dialog, under **Policies** > **Custom Policies**. Here you can see all of your custom policies, remove them, or *Import* new ones.

Import a Policy

If you have created a policy outside of the Policy Editor, or have been shared a policy, it can be imported using the **Import** option from the *Custom Policies* tab under *Policies* in the settings dialog.

From this option, just select the policy file with *Paws Studio* selected as the type, fill any other options and click **Save**. The policy is then embedded in Paws Studio and ready to be used.

SCAP

Paws Studio also supports **SCAP** language when importing policies. Simply select *SCAP* from the type drop-down menu when importing a policy, choose your SCAP files (*OVAL*, *XCCDF*) and fill the options listed.

Paws Studio will then convert these SCAP files into a Paws Studio Policy and integrate it into the software. The policy is then an option when creating a new report.

Check Library

The Check Library is the list of checks that can be performed by Paws Studio. Combinations of these checks are included in compliance audits.

Any of these checks can also be included in your own policies created through the Policy Editor.

- Anti Virus
  - Installed
  - Enabled
  - Up To Date
- Anti Spyware
  - Installed
  - Enabled
  - Up To Date
- Audit Policy
- Console Command
- File
  - Exists
  - Content
- Firewall

- Installed
- Enabled
- Microsoft Products Updates
- Operating System Lifecycle
- Password Policy
  - Forced Logoff Time
  - Max Password Age
  - Min Password Age
  - Min Password Length
  - Password Complexity
  - Password History
  - Password Lockout Counter
  - Password Lockout Duration
  - Password Lockout Threshold
- Password Warnings
  - Expired Passwords
  - No Password Expiry
  - No Password Required
  - Password Not Changeable
  - Unencrypted Passwords
  - User Max Password Age
- Permissions
  - File
  - Registry
- Registry
- Screensaver

- Software
  - Installed
  - Versions
  - Unauthorized
- Startup Items
- System Updates
- User Policy
  - Allow Unused Accounts
  - Bad Password Count
  - Inactivity Period
  - Max Password Age
- User Rights
- WMI Query

Export Data Collector

Paws Studio uses a Data Collector tool to pull in required information from devices so that reports can be created. It produces a data file with the .paws extension, which can be interpreted by Paws Studio and provides enough information to create a report.

After selecting **Export Data Collector** you will be provided with a menu to select which audit report types you would like to export for the audit. Once selected you will be asked where to save this and a folder will appear named **Data Collector**, within which a **Collector** directory can be found. Within this directory you will find:

- a **Data Collector Windows** folder, containing all the necessary files and dependencies for the Windows Data Collector.
- an **ExportedPolicies** folder, containing the policies specified for export from within Paws Studio.
- a **Run Windows Collector.bat** batch file, used to start the Windows Data Collector.

Note: The Data Collector requires running as an administrative (root) user.

Windows Data Collector

When auditing Windows devices, the Data Collector is a small executable that requires minimal dependencies. These dependencies come ready packed within the **Data Collector Windows** directory.

The Windows Data Collector tool will require policy files bundled with it, so only required information is collected. This bundling process is automated when exporting the Data Collector, and the specified policy files can be located in the **ExportedPolicies** folder.

The Data Collector can be run as a GUI application, or from the CLI.

GUI

To run the Windows Data Collector as a GUI application, run the **Run Windows Collector.bat**batch file. The simple GUI provides a checklist of the exported policies, a tab to run the collector on the **Local** machine, tabs for different target **Remote** operating systems and **Collect**/**Cancel** Buttons along with a **Progress** bar, an Import policy button and a settings button. You will be notified when collection finishes and the **collected.paws** data file is created in the same directory as the Data Collector by default.

For custom made policies, simply click the **Import** button and select the custom policy file from the system, this should make the custom policy selectable from within the checklist of policies.

Clicking the **Settings** button allows for various customisations for the Windows Data Collector, located across several tabs:

- Collection
  - **Policy Output Path** To specify the file location for the resultant **.paws** data file upon collection finish.
  - **User Collection Limit** To specify the maximum amount of users to collect data on from the target device.
  - **User Group Collection Limit** To specify the maximum amount of user groups to collect data on from the target device.
  - **Timeout** To specify the maximum amount of time to spend attemping data collection for the target device, in seconds.
- **Logging**

- **Debug Mode** Toggles debug mode. When on the actions of the Windows Data Collector are written to the specified debug log file.
- **Debug Log File** Specifies the location of the file to write the debug log to.

- **Connection**

- **Online Mode** Toggles Online mode, enabling the Windows Data Collector the capability to go online to collect data where necessary.
- **Drive Share Location** To specify a different Drive Share location for target remote Windows based devices, defaults to the volume C administrative share, **C$**.

CLI

To run the Windows Data Collector as a CLI application, navigate to: "<Paws Studio Installation Path>/Data Collector/Collector/Data Collector Windows/"
and run `RemoteDataCollector_cli.exe --help` to see a list of supported commands.
Please note that running `RemoteDataCollector_cli` with the absence of arguments will trigger the application as a GUI instead.

Red Hat Enterprise Linux 7 Data Collector

Paws Studio allows you to run SCAP policies on Red Hat Enterprise Linux 7. To do so, select **Tools>Export Data Collector**, alternatively you can select **Export Data Collector** from the **Shortcuts** menu or by pressing **Ctrl+D**.

You must select **Security Technical Implementation Guide** from the policy list and click **Export**. This will prompt you to choose a directory to export the data collector to.

Next, you have to copy the **Data Collector\Collector\DataCollectorLinux.tar** to a location on the Red Hat Enterprise Linux 7 device.

This **DataCollectorLinux.tar** can be extracted with the following command, using the **Terminal** application: `tar -xf`
After extracting the **DataCollectorLinux** folder from the **DataCollectorLinux.tar** file, you must first set the file permissions by typing in the following command, using the **Terminal**application, onto the extracted folder: `sudo chmod -R 755 DataCollectorLinux`. This will give you the correct file permissions to execute the data collector script.

To audit this machine, you must open the **Terminal** application, navigate to the extracted folder (DataCollectorLinux) and call the following command: `./RunLinuxDataCollector.sh`.

Once the process has been completed, a file with the extension **.tgz** should be generated; This file contains the data which was obtained from auditing the Red Hat Enterprise Linux 7 device.

To create a report using the data collected from the Red Hat Enterprise Linux 7 device, you must select **New Report** and then select **Add Manual Files**. Select **Add Manual** on the drop down menu and then select the **.tgz** file.

Once the file has been loaded you must click **next** which will take you the report menu, clicking **next** once more will generate the **report** which was created by your Red Hat Enterprise Linux 7 device.

Manual Auditing

When producing reports for local or network devices, the data collection process is automated. However, if you wish to audit a device which cannot be connected to over a network, you can manually collect this information by running the Data Collector tool on the device.

If you can manually place the Data Collector tool (USB Drive, Shared Drive, Email, FTP etc.) on the device, it can be run to produce a data file, which can then be transferred back to the auditing device to produce the report.

Paws Studio provides an easy way to export the Data Collector, this produces auditing methods for all supported operating systems.

Exporting

Exporting the Data Collector can be accessed from the shortcuts or Tools> **Export Data Collector**.

The simple interface prompts you to select which audits you wish to include when exporting. When finalized, the export process will ask where to export the Data Collector to.

This will create a directory containing both the Windows and Linux versions of the Data Collector ready to use on a device.

Network Auditing Protocols

When performing an audit against a network device, Paws Studio uses various protocols to perform the data collection process depending on the operating system of the host and target device.

The network auditing process follows a series of actions, differing between protocols, to copy the Data Collector onto the target machine, run commands to create the data file, copy this data file back to the host machine and then cleanup any resources left over.

SSH

When auditing Linux devices over a network, the SSH protocol is used.

To ensure a successful connection, the target device must allow SSH connections.

To test if an SSH connection can be made, run the following command from a terminal.

```
ssh -l root <ip-address>
```

You will be prompted for the root user password if a successful connection can be made.

SMB

Paws Studio uses `smbclient` & `scp` when auditing Windows devices from Unix based devices.

SMB version 1.0 is required for successful remote auditing of Windows devices. SMB version 1.0 is enabled by default on Windows systems, but can enabled using the following command in a **PowerShell** console with administrative privileges.

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

Note: SMB 1.0 should be disabled when not being used, as it is a vulnerable service.

Windows API

When auditing a Windows device from another Windows device, the Windows Networking API is used.

To ensure a successful connection, the host & target machine must both have **File & Printer Sharing** switched on. This is the default for Windows installations.

Note: When connecting to a Windows XP machine, SMB version 1.0 is required, see above for enabling this.

Settings & Customization

Paws Studio is highly configurable and customizable. There are many settings which allow you to change not only the look and feel of your report, but also the content.

Settings are available from both the homepage and the tool bar. Each setting provides a tool-tip describing what each setting does.

Command Line Interface

Paws Studio allows you to create reports, manage licenses and much more using the CLI.

To view help on how to use the Paws Studio CLI, simply run:

```
pawsstudio-cli --help
```

Mac OS X

To access the Paws Studio CLI on Apple Mac OS X systems, you must first select **Install Command Line Tools** from the **Tools** menu.

Licensing

Paws Studio licensing works on a per-device basis (physical or virtual).

1. Licenses are subscription based with all updates included during your subscription period.
2. Licenses include a device count corresponding to the number of devices you can audit during your subscription period.

3. The same device can be audited multiple times during your subscription period.

   Note: If you have a multi-year license, you can audit a different set of devices each year.

   Paws Studio allows you to manage your licenses by viewing usage, license and licensee information, adding and removing licenses etc. This is available from both the homepage and the menu bar.

Adding a License

Selecting **Add License** from the Manage Licenses page, allows you to add a new license to Paws Studio. All you need is the serial number and activation code available from titania.com on your account page.

Adding a license is easy, just follow the informative wizard and your license will be confirmed and added by the Titania servers.

If your machine is unable to connect to Titania's servers to add your license, we provide methods to add your license offline. These are accessible by selecting the **Show Options**checkbox.

System Wide Licensing

System Wide Licensing allows multiple users with administration access to use the same license for running audits.

Setup

To enable system wide licensing

- Start Paws Studio as an administrator.
- Enter settings/advanced/maintenance and check the box next to "system wide licensing"
- To activate this a restart of Paws Studio is required.
- On restart License details will need entering for the license you wish to use system wide.

Usage

- To enable system wide licenses for a second user.
- The user needs to start Paws Studio with administrator permissions.

- The user needs to navigate to settings/advanced/maintenance and enable "system wide licensing".
- Restart Paws Studio which will switch the user from the license they were using to the one previously added.

SQL Auditing

Using Paws Studio SQL Auditing

SQL Auditing on Paws is currently supported for Microsoft SQL Server using the "MS SQL Server 2014 Database Security Technical Implementation Guide". To use this policy create a new report in Paws Studio (Ctrl + N, or File > New Report) and from the list select the policy titled "MS SQL Server 2014 Database Security Technical Implementation Guide".

On the following device selection screen, add a new network device using the "Add Network Device > Add Network Device" button. Change the "Device Type" to "Microsoft SQL Server" and the following options will be presented:

- **IP Address:** The IP address (or machine name) of the target SQL Server.
- **Username:** The username to use for auditing, this must be a user with admin rights for the audit to succeed.
- **Password:** The matching password for the username.
- **Database Name:** The name of the database to be audited.
- **Port:** The port the SQL server being audited can be reached on (the default for MS SQL Server is 1433).
- **Windows Authentication:**
  - If checked, Paws Studio will connect with the MSSQL Server via Active Directory, with Authentication being done by the Domain and Authorization being handled by the SQL Server. **Note:** With this option, both the Username and Password fields are ignored.
  - If unchecked, Paws Studio will connect via the given Username and Password, with the SQL Server both Authenticating and Authorizing via a connection string over TCP/IP.

For more information please refer to the Microsoft Documentation.

Limitations

For the majority of checks, Paws Studio is only able to provide supplementary information to help you determine if the targeted database meets the criteria. Each check has the steps listed to meet the compliance criteria detailed within, this text is pulled directly from the official MS SQL Server 2014 Database Security Technical Implementation Guide XCCDF files. Some of these checks reference supplementary files to be used for auditing purposes, these files are supplied with Paws Studio and can be found in your installation directory at:
"<Paws Studio Installation Path>/rm/Policies/stig/sql-supplementary".

Some of the checks in the policy audit Trace and Audit records for server audit specifications. There is currently planned development to allow a user auditing a database to enter the server audit specification name so the supplementary information for these checks can be pulled as part of the Paws audit, leaving less work for the user.