



## User Guide

Version 3.4 (Paws Studio 3.0.0)

© Titania Limited 2015. All Rights Reserved

This document is intended to provide advice and assistance for the installation and running of Paws Studio. While Titania takes care to ensure that all the information included in this document is accurate and relevant, customers are advised to seek further assistance from our support team if required.

No part of this documentation may be copied or otherwise duplicated on any medium without prior written consent of Titania Limited, publisher of this work.

The use of Paws Studio software is subject to the acceptance of the license agreement.

## 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.



## Contents

User Guide .....	1
Overview .....	1
Create a New Report.....	3
Create Report .....	3
Select Devices .....	3
Report Generation .....	4
Your Audit Report.....	5
Result Control & Comments.....	5
Re-running Results .....	5
Save & Load .....	5
Export Report.....	6
Audits .....	7
Policy Editor .....	7
Check Library .....	8
Export Data Collector .....	10
Windows Data Collector .....	10
GUI .....	10
CLI .....	10
Linux Data Collector.....	11
Manual Auditing .....	11
Exporting.....	11
Network Auditing Protocols .....	13
SSH .....	13
SMB.....	13
Windows API.....	13
Settings & Customization .....	14
Command Line Interface .....	14
Mac OS X .....	14
Licensing .....	15
Adding a License .....	15



## 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 audit's 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. To remotely audit a Windows machine, the target machine needs File and Printer sharing to be **enabled**. Paws Studio also provides some handy tools to auto-detect network devices these are **Network Scan** and **Scan IP Range**.

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

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



Note: Self Certification Reports, such as Cyber Essentials & DCPD 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.

## Re-running 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:

- HTML
- PDF
- CSV(s) to directory
- XML
- ASCII

Exporting HTML, PDF or CSV(s) to directory will save the specific page you have open at the time. To save the entire audit report navigate to **File> Export> Export Complete Report** where the remainder of the save options are located.



## Audits

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

- Configuration Report
- Self Certification Reports
  - **DCPP** Defense Cyber Protection Partnership
- Compliance Reports
  - **SANS** Institute Computer Security Policy Report
  - **NERC CIP 007-4** Systems Security Management
  - **NSA 2013** Guidelines
  - **PCI DSS** Payment Card Industry Data Security Standard Compliance Report
  - **DISA STIG** Defense Information Systems Agency Security Technical Implementation Guide
  - **OVAL** Compliance
  - **USGCB** United States Government Configuration Baseline
  - **Cyber Essentials** 5 essential controls set out by the UK Government

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

## 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 on 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.



## 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



## Data Collector

Paws Studio uses a Data Collector tool to pull in required information from devices so that reports can be created. It produces an encrypted 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 three folders will appear **Windows**, **Linux** and **Mac OSX**

**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 no system dependencies.

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.

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

## GUI

The simple GUI provides a button for each pre-built audit, clicking the audit will start the collection process. You will be notified when finished and the data file is created in the same directory as the Data Collector by default.

For custom made policies, simply click the **Custom** button and select the custom policy file from the system.

## CLI

- **local** Informs the tool it is running a local audit.
- **config[=<filename>]** Create a configuration data file.
- **stig[=<filename>]** Create a DISA STIG data file.
- **pci[=<filename>]** Create a PCI DSS data file.
- **sans[=<filename>]** Create a SANS data file.
- **nsa[=<filename>]** Create a NSA 2013 data file.
- **nerc[=<filename>]** Create a NERC data file.
- **ovalvuln[=<filename>]** Create an OVAL Vulnerability data file.
- **ovalcomp[=<filename>]** Create an OVAL Compliance data file.



- **custom=<policy>|<filename>** Create a custom data file for the policy defined at <policy>.
- **-destination-folder=<dir>** Override the directory where the data file is created.
- **-xml-folder=<dir>** Override the directory where policy files are stored.
- **--user=<user>** Override the user running the tool.
- **--currentuser** Only audits the current user when collecting user information. Cannot be used with the --nodomain option.
- **--nodomain** Ignores domain users when collecting user information. Cannot be used with the --current user option.
- **--offline** Ensures the Data Collector does NOT use online services to collect information.
- **-timeout=<int>** Specify the number of seconds before a command times-out. By default, 5s.
- **-d** Debug Mode. Creates a debug file in working directory.

### Linux Data Collector

The Linux Data Collector tool is a bash script which, when run, produces the data file to include in Paws Studio.

Each Data Collector script can only create data for a single audit, so each audit will produce a different script which will need to be run individually.

```
sudo sh data-collector.sh
```

### 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 to use tool to export the Data Collector and all audit files for all 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.

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 be enabled using the following command in a **PowerShell** console with administrative privileges.

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

### 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.



## 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:

```
pawsstudiocli --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).

Licenses are subscription based with all updates included during your subscription period.

Licenses include a device count corresponding to the number of devices you can audit during your subscription period.

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.