Impero Client/Server Overview

October 2018

Introduction

Impero Education Pro is a Classroom Management, Network Management and Online Safety integrated software solution. The two main components of the software are referred to as Impero Client and Impero Server. This document covers these components and provides an overview of their relationship and responsibilities to each other.

Below is a link to our latest system requirements document

Impero Education Pro – Minimum System Requirments

Impero Client

Impero Client is the required end point software installed on all devices and facilitates the connection to Impero Server. It is available for 4 platforms (Windows, MacOS, ChromeOS , iOS) which can all simultaneously connect to the same Impero Server. The client is installed on all devices connected to the Impero Server regardless if they are a student, teacher or admin user.

Impero Client contains the Impero Console application (Windows and MacOS only) which is available to users based on access rights configured within Impero Server. Impero Console allows users to monitor and interact with connected devices. Levels of access and visibility of devices is configured within Impero Server. An Admin user might have access to all devices and can use all functionality within Impero Console. A teacher user might have restricted access so they can only view the devices they need to while being given access to only the functions on the product that they require in the classroom. Student users will have no access rights and thus cannot use Impero Console.

Impero Console has many features that perform actions on devices. Certain functionality is not available on certain platforms. The feature Matrix link below shows a break down of what actions can be performed on what devices.

Impero Education Pro – Feature Matrix

Impero Client logs user activity and relays that information back to Impero Server where it is added to a central database which can be viewed in Impero Console. Access to the database can be restricted via access rights on Impero Server. Certain platforms don't relay activity for all actions back to the the database. A breakdown of each platform and supported log data is below

Windows Client support – *Screen Captures, Window History, Applications used, websites visited, printed documents, deleted files and timeline*

MacOS Client support - *Screen Captures, Window History, Applications used, websites visited and timeline*

ChromeOS Client support - *Screen Captures, websites visited and timeline*

iOS Client support - *Screen Captures, websites visited and timeline*

Impero Server

Impero Server is used to authenticate client access while also being the storage location for all log data recorded from client devices. Specific configuration options are available on Impero Server and these will affect all connected clients. Impero Server also stores your Impero Configuration data which is housed in encrypted XML files. All clients connect to Impero Server and check for changes and updates to this configuration data with changes being sent to clients to ensure they have the correct information regarding settings, groups and policies. Impero Server can also deploy and update Impero Client on Windows and MacOS. Once configured, Impero Server will update to the latest version and then begin deploying the updated client to Windows and Mac devices. Client updates are handled on the fly and devices can still be used while Impero Client updates are installed, although it is highly recommended that a restart of the client is performed after updating to ensure full product functionality.

© 2018 Impero Solutions Ltd

Security

Impero Education Pro utilises the latest in data encryption and security to ensure no unauthorised users or software can access or manipulate devices connected via your Impero Network.

All communications between Impero Client (all platforms) and Impero Server are handled by TCP socket connections and are authenticated using a challenge-handshake protocol. Data is transmitted between Impero Server and Impero Client is done so using TLS encryption. Inter process communications within Education Pro are verified using authentication certificates.

Access to Impero Console is controlled by Console Access Rights on the Impero Server. These settings allow administrators to customise the functionality and access each console user has so that only the right people can see the right devices.

Additional Resources

Below are links to our data retention and data storage security guides

Impero Education Pro – Data Retention Guide

Impero Education Pro – Data Storage Security Guide

Additional links to useful guide resources can be found below

Impero Education Pro – Network Port Schema Guide

Impero Education Pro – Online Safety features Guide

info@imperosoftware.com

www.imperosoftware.co.uk

www.imperosoftware.com

+44 (0) 1509 611341 UK

877-883-4370 USA