Secure Web Solo – User Guide

Version 26.1

PNQ Software

Introduction

In modern digital workplaces, the browser is increasingly becoming the primary access point to applications and information. At the same time, this creates a tension between user freedom and the need for control, security, and predictability.

Secure Web Solo was developed specifically to address this tension. Instead of a traditional browser that allows everything, it provides controlled and purpose-driven access to web applications. Users are presented with a clear, well-defined environment without distractions, while IT retains full control over functionality and behavior.

This makes Secure Web Solo particularly well suited for environments such as VDI, kiosk solutions, healthcare institutions, and other scenarios where reliability and simplicity are essential. The KioskPlus mode, in particular, combines a fully locked-down workspace with the flexibility to make exactly the required functionality available.

Secure Web Solo is therefore not a standard browser, but a controlled gateway to the digital workplace.

1. Architecture & Operation

Secure Web Solo consists of three main components:

1.1 Runtime browser engine

Based on WebView2:

- No DevTools
- No context menu
- No autofill or password storage
- No new windows (everything remains within the same view)

1.2 Configuration via INI

All behavior is defined through the sws.ini file. On first launch, this file is automatically generated if it does not exist.

Key sections:

- [Settings] → mode and language
- [URL] → navigation
- [Visible] → UI controls
- [Menu] → labels
- [Refresh] → automatic refresh
- [Delay] → startup delay

1.3 Application modes

Secure Web Solo supports three modes:

- Browser – Minimal browser without restrictions
- Kiosk – Fullscreen without UI
- KioskPlus – Fullscreen with configurable UI

The mode is defined via:

[Settings]

Mode = KioskPlus, Browser, Kiosk

or via command line:

sws.exe -kp, sws.exe -k, sws.exe -b

2. KioskPlus Mode (Core Feature)

KioskPlus mode represents the most powerful variant of Secure Web Solo, combining a fully locked-down kiosk environment with controlled flexibility. Unlike traditional kiosk solutions—where users cannot adjust anything—KioskPlus enables precise configuration of both interface and functionality. This includes options such as showing or hiding navigation controls, audio settings, restart options, or specific buttons.

The result is a controlled workspace that is secure and predictable, while still aligning exactly with the practical needs of the user. KioskPlus delivers the ideal balance between maximum IT control and end-user usability.

2.1 What Makes KioskPlus Unique

KioskPlus combines:

- A fully fullscreen kiosk
- With a configurable top bar

This makes the product:

- Usable for end users
- Fully manageable by IT

2.2 UI configuration

The entire UI can be defined via the INI file:

[Visible]

- Back = Yes
- Forward = Yes
- Home = Yes
- Refresh = Yes
- AddressBar = No
- Workplace = No
- AudioSelect = Yes
- Admin = No
- Volume = Yes
- Restart = Yes
- Shutdown = Yes

Each element is dynamically shown or hidden at runtime.

2.3 Menu Customization

[Menu]

Workplace = My Workplace

- Maximum of 15 characters
- Automatically truncated if necessary

2.4 Functionalities in KioskPlus

Depending on configuration:

- Navigation (Back / Forward / Home)
- Refresh (manual + scheduled)
- Volume control + mute
- Audio device selection (Audio Control Center)
- Restart / Shutdown
- Admin access (elevated PowerShell)

3. Navigation & Content

Within Secure Web Solo, navigation is fully focused on simplicity and control. Users are automatically directed to a predefined web environment, where only the allowed pages and functionalities are available. Depending on the configuration, elements such as a home button, back and forward navigation, or a refresh option can be provided—always within the boundaries defined by IT.

Content is central: web applications, dashboards, or portals are presented without distraction, with optional automatic refresh to keep information up to date. This creates a consistent and purpose-driven user experience, where the focus is entirely on the content rather than the browser itself.

3.1 URL Configuration

[URL]

Home = https://google.com

Workplace = https://intranet.company.com

Home = optional

Workplace = primary start page

Navigation is executed automatically at startup

3.2 Startup delay

[Delay]

StartupSeconds = 1

Use this for:

- Network initialization
- VDI login timing
- Backend dependencies

3.3 Automatic Refresh

[Refresh]

Time = 08:59

Repeat = 24

- First refresh at the specified time
- Then repeated at hourly intervals

4. Security & Control

Secure Web Solo is designed with security and manageability as its foundation. The browser is intentionally restricted to only the necessary functionality, preventing unwanted actions such as opening new windows, accessing developer tools, or storing data. Everything the user sees and can do is centrally controlled via configuration.

This approach ensures a predictable and controlled environment, minimizing risks and significantly reducing the likelihood of misuse. At the same time, IT retains full control over behavior, access, and settings—without relying on complex management solutions.

4.1 Restrictions

No new windows (forced redirect)

No DevTools

No context menu

No password storage

No script dialogs

4.2 Single instance

Only one instance can run:

- The application prevents duplicate launches
- An existing instance is brought to the foreground

4.3 Licensing & activation

Secure Web Solo uses a licensing system that verifies the presence of a valid license at startup. Without a valid license, the application will not start, ensuring controlled and compliant usage at all times.

At startup:

- Activation check
- License validation

The application only launches with a valid license.

5. Usage in VDI and Kiosk Environments

Secure Web Solo is ideally suited for VDI and kiosk environments where simplicity, security, and predictability are essential. Within VDI, it provides controlled access to web applications without relying on a full desktop experience. In kiosk setups, it delivers a fully locked-down workspace, where users are given direct access to the correct application—without distractions or escape possibilities. This results in a stable and manageable digital workplace.

5.1 Typical Use Cases

VDI / Citrix / AVD

- Secure access to SaaS
- Single-application workspace
- No local escape possibilities

Kiosk

- Reception terminals
- Healthcare terminals
- Self-service portals

Control rooms

- Dashboards with auto-refresh

6. Auto-login + Shell Replacement (Important)

Secure Web Solo can be deployed as a replacement for the standard Windows shell (Explorer), allowing users to enter the application directly after automatic login. In this configuration, the Windows desktop is not launched; instead, Secure Web Solo starts immediately, for example in KioskPlus mode. This creates a fully locked-down and controlled workspace, ideal for kiosk and VDI scenarios where users must not have access to the underlying operating system.

6.1 Objective

The goal of this configuration is to place the user directly into a controlled environment immediately after login, without any interaction with the Windows desktop. This completely restricts access to the operating system and ensures focus on a single specific application.

User logs in → immediately enters Secure Web Solo, without Windows Explorer

6.2 Operation

By replacing the default Windows shell per user, Explorer.exe is no longer started after login. Instead, Secure Web Solo is launched. This setting is applied at user level (HKCU), ensuring that only the intended user receives this environment, while administrative accounts remain unaffected.

In Windows:

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Modify:

Shell = "C:\Program Files\PNQ Software\Secure Web Solo\sws.exe -kp"

6.3 Result

The user is taken directly into a fullscreen application, with no visible Windows components. This eliminates distractions and prevents navigation outside the intended workspace.

After login:

- No Start menu
- No desktop
- No taskbar
- Only Secure Web Solo in fullscreen

➡️ This creates a true kiosk experience

6.4 Best practice

For an optimal and secure setup, it is recommended to use KioskPlus in combination with a minimal UI configuration. By disabling unnecessary elements, the environment remains clean, predictable, and fully controlled by IT.

For maximum security:

- KioskPlus mode
- AddressBar = No
- Admin = No

7. Audio Control Center

The Audio Control Center enables users to easily manage audio settings within the controlled environment of Secure Web Solo. It allows both input and output devices to be selected and adjusted, without requiring access to standard Windows settings. This makes it particularly suitable for VDI and kiosk environments where peripherals may change, but the user environment must remain locked down.

- Selection of input/output devices
- Change default Windows audio device
- Fully multilingual

➡️ Unique for kiosk browsers

8. Command Line Usage

Secure Web Solo supports command line parameters for flexible and rapid deployment across various scenarios. This allows the desired mode (Browser, Kiosk, or KioskPlus) to be defined at startup, with the option to pass a specific URL. It simplifies integration into scripts, shortcuts, or automated deployments, without relying on manual configuration.

For fast deployment:

sws.exe -kp https://portal.company.com

Or:

sws.exe -k, sws.exe -b

Capabilities:

- Define mode
- Inject URL
- Override configuration

9. Branding & Customization

Secure Web Solo provides extensive options to tailor the application both visually and functionally to the organization. This includes the use of a custom logo, color settings, and customized labels within the interface. Combined with configurable menu options, the user experience can be fully aligned with corporate branding and specific use cases—without requiring changes to the software itself.

Supported:

- Custom logo (via INI / file)
- BorderColor theming
- UI labels
- Multi-language UI (NL, EN, DE, FR, ES, IT, etc.)

10. Summary

Secure Web Solo delivers controlled and secure access to web applications, specifically designed for environments where simplicity, stability, and manageability are critical. By combining a minimalistic browser with extensive configuration options and support for kiosk and VDI scenarios, it creates a predictable and purpose-driven user experience.

With features such as KioskPlus, shell replacement, and centralized configuration via INI, Secure Web Solo is a powerful and flexible solution for organizations that want to maintain full control over their digital workplace.

Secure Web Solo offers:

🔒 Maximum control

⚙️ Full configuration via INI

🖥️ Perfect for VDI & kiosk

🎛️ Unique KioskPlus flexibility

🚀 Enterprise-ready deployment

11. Support

For assistance with using ScreenGenie, please contact your internal IT department or the designated support organization.

12. PNQ Software

For additional support, you can also contact PNQ Software. Please visit: https://pnqsoftware.com/support/

Contact details:

PNQ Software

De Nieuwe Erven 3

5431 NV Cuijk

Netherlands

Phone: +31 (0)85 060 4610E-mail: info@pnqsoftware.com