VISUAL AUTOMATION

Product Manual

Secure Utilities
Version 12
Visual Automation, Inc.
PO Box 502
Grand Ledge, Michigan 48837 USA

sales@visualautomation.com
support@visualautomation.com
https://visualautomation.com

The information contained in this document is subject to change without notice.

Visual Automation makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Visual Automation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishings, performance, or use of this material.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another program language without the prior written consent of Visual Automation, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

Secure Desktop 10 utilities versus Secure Utilities

Over several years of Secure Desktop development, we created many small utilities. These utilities are generally stand-alone. These programs are sExplore File Explorer, sCopy File, sNote Viewer, sUtilman, and the sLogOff screen saver. All of these are slightly improved and are now part of Secure Utilities.

New utilities named sRun Program, sControl Panel, and sEject Device replace Secure Desktop 10 and earlier functionality. These functions were part of Secure Desktop, whereas now they are stand-alone programs.

Also new is sUtility, the parent application of Secure Utilities. Here, you can find utility examples, help, and the new interface to system registry settings. We have also added sMenu Start Menu, sArchive File, sRes Resolutions, sLock Workstation, sKey On-Screen Keyboard, sImage Viewer, sCSV Viewer, and sZIP Viewer.

Secure Desktop 7 through 10 had an Administrator tab in Secure Desktop Tools. This tab and associated functionality is now part of sUtility. Included are registry settings for Logon and Drive hiding. Other functions like file attribute manipulation and Internet Explorer registry settings are deprecated.

We are very excited about Secure Utilities. The utilities are easy to use, look better, and have the best user experience.

Secure Utilities is a 32-bit application but is also 64-bit aware. We tested Secure Utilities in Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022. If you need legacy Windows version support, please consider purchasing Secure Desktop 10. We tested Secure Utilities on Microsoft Surface Pro and Microsoft Surface Laptop Studio computers. If you use Windows 10/11 in a mission-critical setting, please consider using the Enterprise LTSB Edition. Secure Utilities is not in the Windows Store and, therefore, will not run in Windows 10 S. Windows 10 S is upgradeable to Windows 10 Pro.

All modules of Secure Utilities are 32-bit and are therefore compatible with Windows 10 on ARM and Windows 11 on ARM using emulation. We tested Secure Utilities on Microsoft Surface Pro X.

Secure Utilities - An Introduction

A guide to Secure Utilities and an illustration of main concepts

Why Windows needs additional security

The design of Microsoft Windows is for a typical desktop environment, with one person using their computer. What if several people in an open environment use a PC that anyone can access? What if you want the computer user to have access to only specific programs? Secure Desktop and Secure Utilities provide this security. Windows is a fragile environment in that the wrong setting may cause the system not to function as it once did. The best remedy to secure this computer is to provide the user with access to only the items they need to achieve the goal of the machine. Secure Desktop and Secure Utilities offer this capability.

In Program Files or Program Files (x86) Folder:

Secure Utilities

Secure Utilities provides many applications for the desktop environment. The Secure Utilities parent application file name is sUtility.exe. Here, you can find utility examples, help, and the new interface to system registry settings. A companion executable named suAdmin.exe should not be called individually (it's called from sUtility.exe as needed).

Secure Utilities Manual

The manual for Secure Utilities is the file you are browsing, named sUtility.pdf.

sExplore File Explorer

Use sExplore in place of File Explorer. sExplore is restricted to a particular folder and file wild card based on command-line parameters. The user is prohibited to browse above the base folder in the file folder hierarchy. File and folder editing is prohibited, but users can launch a program or document file. The file name for sExplore File Explorer is sExplore.exe.

sCopy File

This program provides a way to copy files restricted to a particular source folder, destination folder, and file wild card based on command-line parameters. The user is prohibited to browse above the base folder in the file folder hierarchy. File and folder editing is not possible. The file name for sCopy File is sCopy.exe.

sMenu Start Menu

This program allows access to all Start Menu and Desktop file shortcuts for win32 applications. The file name for sMenu Start Menu is sMenu.exe.

sArchive File

This program provides a way to archive files restricted to a particular source folder, destination folder, and file wild card based on command-line parameters. The user is prohibited to browse above the base folder in the file folder hierarchy. File and folder editing is not possible. The file name for sArchive File is sArchive.exe.

sRun Program

sRun Program launches the same Run dialog started from the Start menu. The file name for sRun Program is sRun.exe.

sControl Panel

This program launches the Control Panel dialog started from the Start menu. The file name for the sControl Panel is sControl.exe.

sEject Device

This program launches the Eject Device dialog. The file name for the sEject Device is sEject.exe.

sRes Resolution

This program sets the display resolution. The file name for the sRes Resolution is sRes.exe.

sLock Workstation

This program locks the workstation. The file name for the sLock Workstation is sLock.exe.

sKey On-Screen Keyboard

This program launches an On-Screen Keyboard. The file name for sKey On Screen Keyboard is sKey.exe.

sNote Viewer

This program provides a way to view text files restricted to a particular folder and file wild cards based on command-line parameters. The user is prohibited to browse above the base folder in the file folder hierarchy. File and folder editing is not possible. The file name for sNote Viewer is sNote.exe.

sImage Viewer

This program provides a way to view an image file. The file name for sImage Viewer is sImage.exe.

sCSV Viewer

This program provides a way to view CSV files restricted to a particular folder and file wild cards based on command-line parameters. The user is prohibited to browse above the base folder in the file folder hierarchy. File and folder editing is not possible. The file name for sCSV Viewer is sCSV.exe.

sZIP Viewer

This program provides a way to view CSV files restricted to a particular folder and file wild cards based on command-line parameters. The user is prohibited to browse above the base folder in the file folder hierarchy. File and folder editing is not possible. The file name for sCSV Viewer is sCSV.exe.

Secure Utilities Version Information

This text file will show you the latest changes for the newest version you have installed. This file is named sVersion.txt.

In the Windows System Folder:

sLogOff Screen Saver

Secure Utilities includes a screen saver program that is not a screen saver. sLogOff automatically logs off the user after the designated period of inactivity. This file is named sLogOff.scr, located in the Windows System folder.

sUtilman

Secure Utilities includes a file named sUtilman.exe in the Windows System folder. This file is necessary for the registry setting to disable Ease of Access.

Setup Program

Secure Utilities uses Inno Setup for its installation software.

Secure Utilities | File tab

Secure Utilities - VA\User Name

| File | System | Input | Viewer | Administrator |

sExplore File Explorer Example:

sExplore.exe "c:\data" "*.txt" /p

sCopy File Example:

sCopy.exe "c:\src" "c:\dst" "*.txt"

sMenu Start Menu Example:

sMenu.exe /CLOSE

sArchive File Example:

sArchive.exe "c:\src" "c:\dst" *.txt /READONLY /NOREPLACE

| Info | Manual | Windows 11 Pro Edition 64-bit, Version 24H2 (LTSC) | Help | Close |
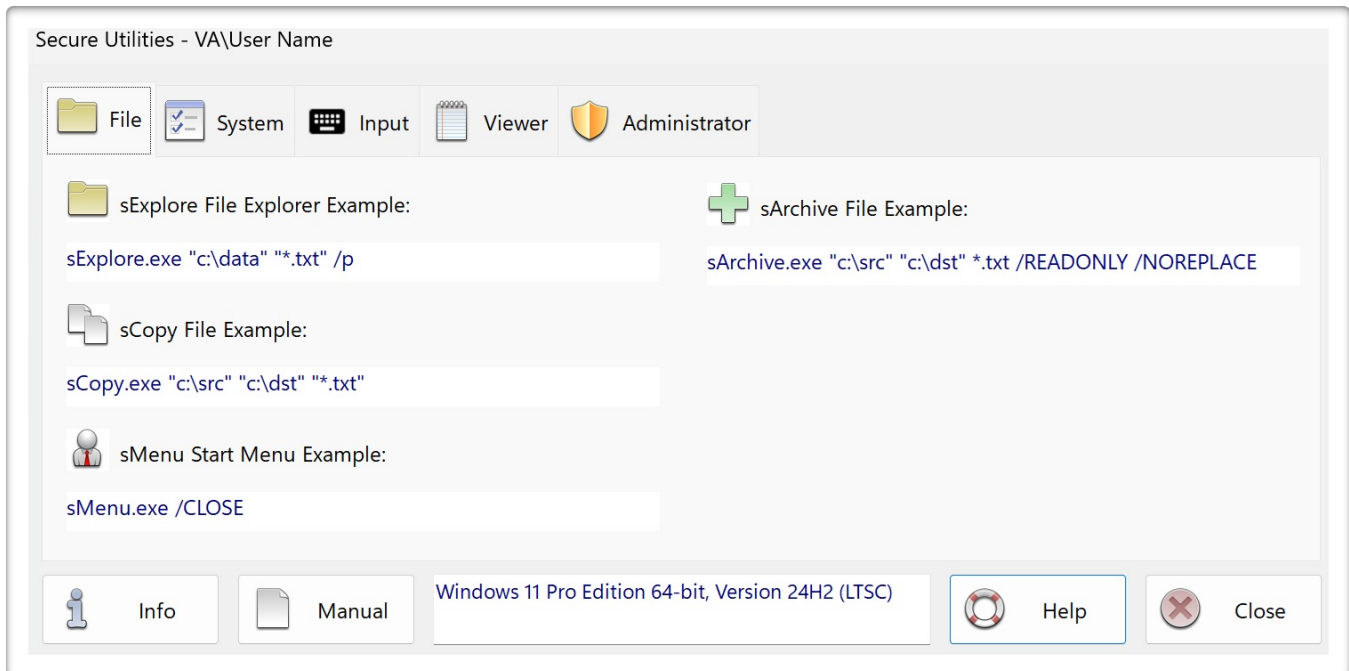
sExplore File Explorer, sCopy File, sMenu Start Menu, and sArchive File are included utilities that act on files.

sExplore File Explorer
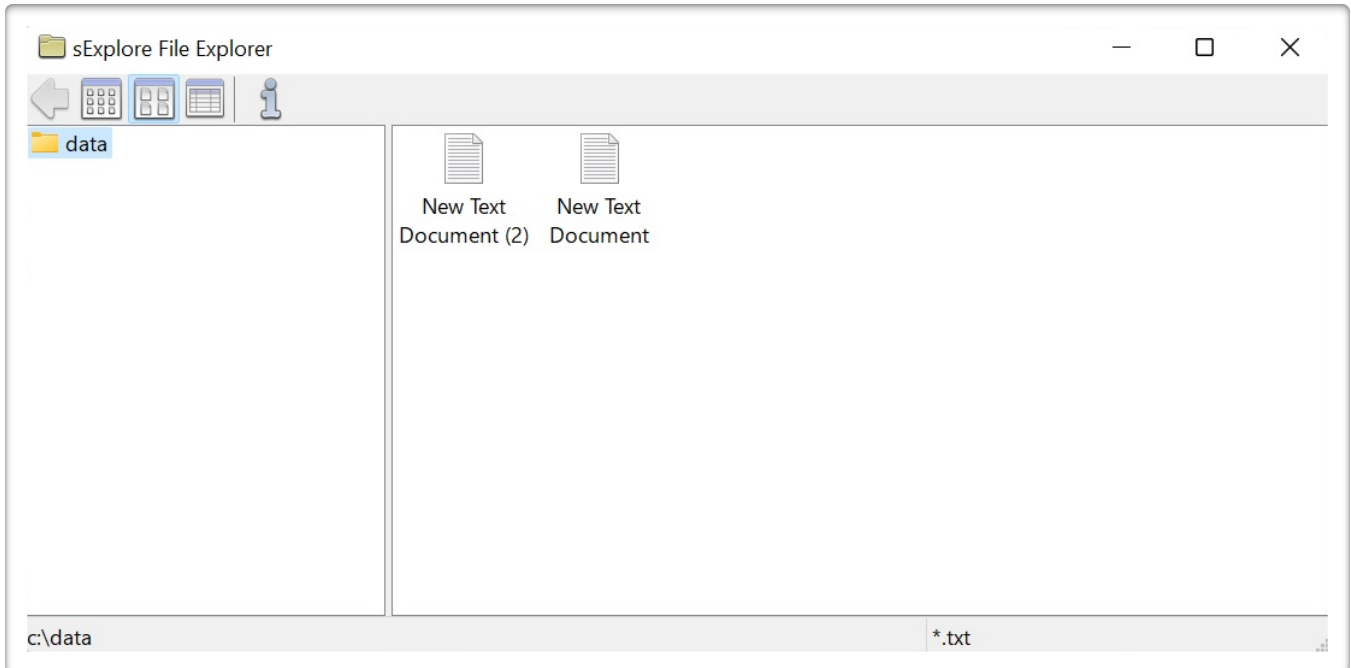
sExplore File Explorer needs command-line parameters:

1st parameter: folder path in quotes

sExplore displays the files and folders in the path specified in the command line parameter. The user may dig down into folders and use the back button to come back up. But they can only go as high as the folder specified in the command line. Double-clicking or hitting enter on a document or executable file will launch that program. The right mouse and other file editing functions are not active.

2nd parameter (optional): wildcard file filter

Only document files matching the wildcard file filter and any folders inside the specified folder are visible.

3rd parameter (optional): /p makes the Print button visible

When the user selects one or more document files and clicks the Print button, the documents print to the default printer via the registered applications associated with the document files.

Example: sExplore.exe "c:\data" "*.txt" /p
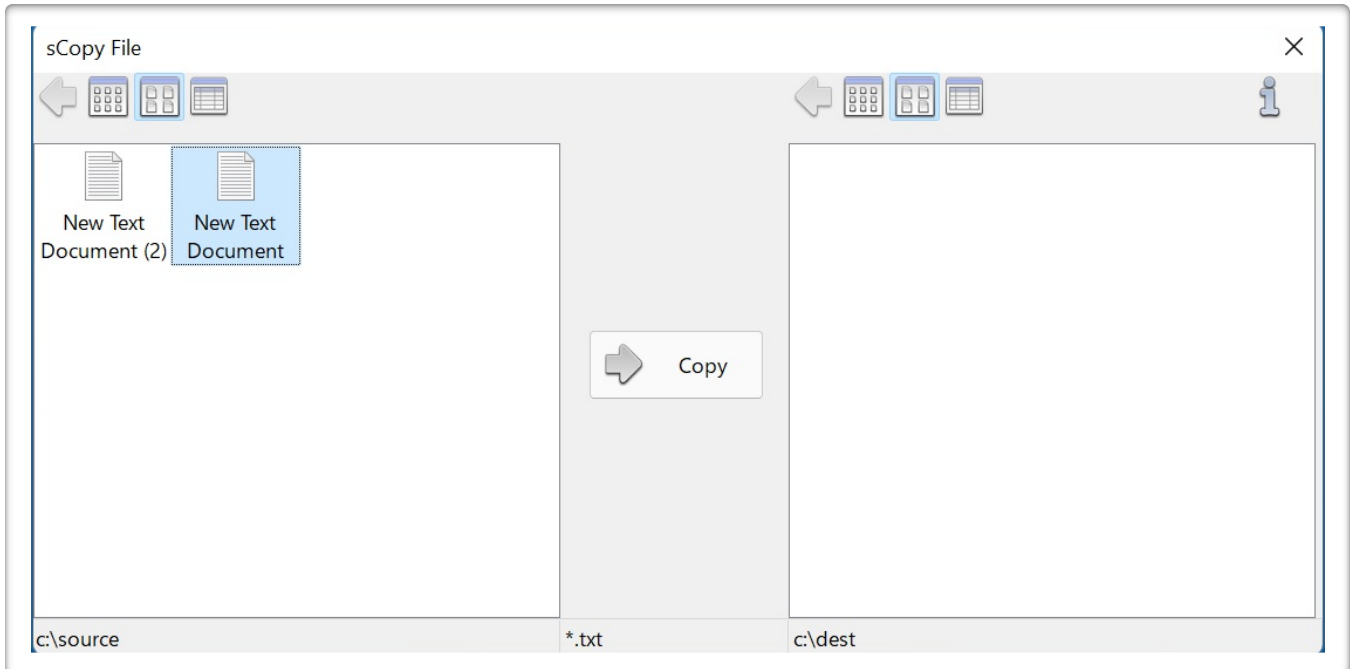
sCopy File

sCopy File needs command-line parameters:

1st parameter: source folder path in quotes

2nd parameter: destination folder path in quotes

3rd parameter: wildcard file filter in quotes

Example: sCopy.exe "c:\source" "c:\dest" "*.txt"

The files and folders in the source and destination paths specified in the command-line parameters are visible in the left and right panes. The user may dig down into folders and use the back button to come back up. But they can only go as high as the folder specified in the command line. Selecting a file in the left pane and clicking the Copy button will copy the file, then shown in the right pane for verification. The right mouse and other file editing functions are not active.

In the example above, only document files ending in "txt" and any folders inside the specified folder are visible.

 sMenu Start Menu
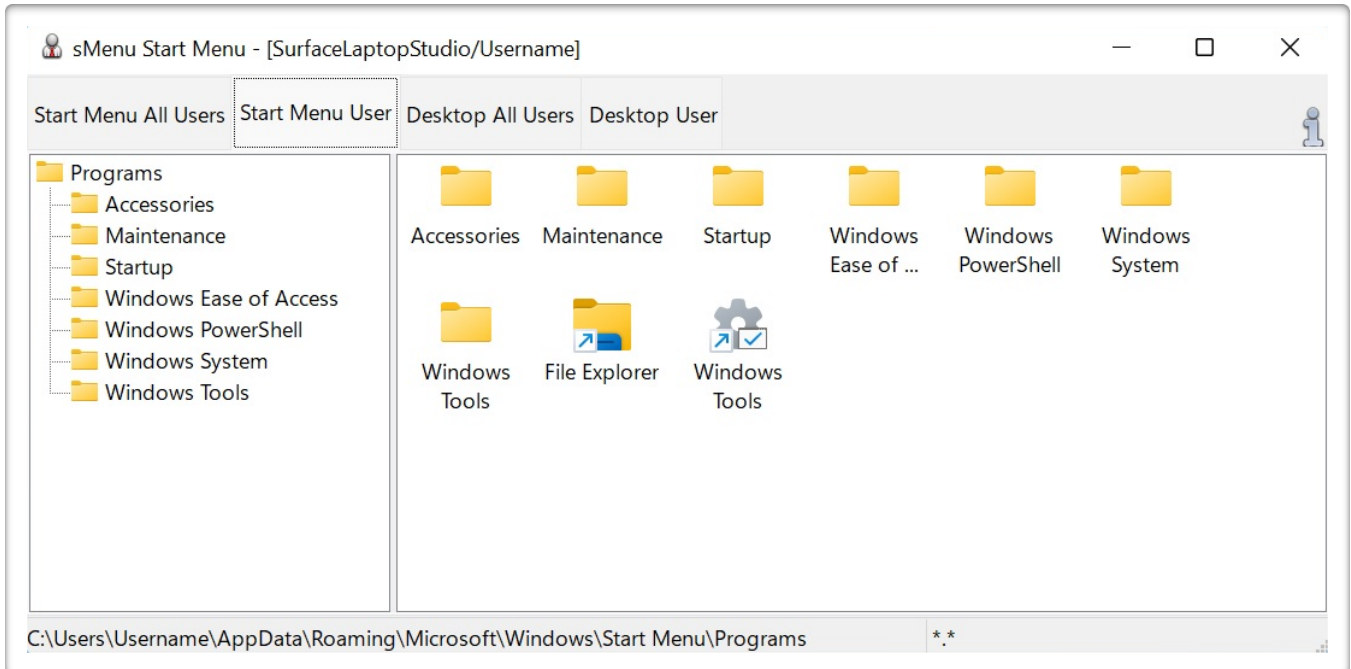
sMenu Start Menu does not need command-line parameters.

1st parameter (optional): /CLOSE will close the sMenu Start Menu application after launching an icon.

sMenu Start Menu displays the files (file shortcuts) for the Start Menu, the Start Menu for the currently logged-in user, the Desktop, and the Desktop for the currently logged-in user.

sMenu Start Menu provides access to most or all Win32 programs installed that are typically available to the currently logged-in user with the Explorer shell.

Secure Utilities installation will install a 32-bit or 64-bit version of sMenu as required by the 32-bit or 64-bit version of Windows.

sArchive File
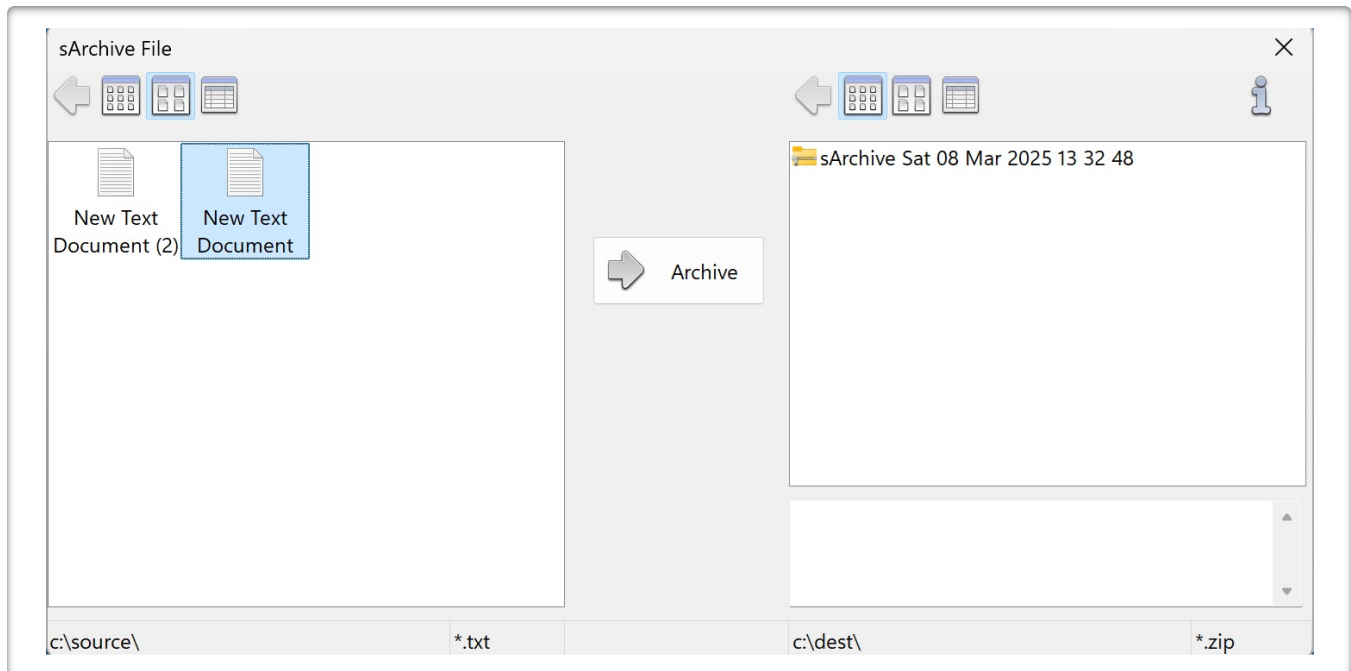
sArchive File needs command-line parameters:

1st parameter: source folder path in quotes

2nd parameter: destination folder path in quotes

3rd parameter: wildcard file filter in quotes

4th parameter (optional): /READONLY to set the zip file attribute to read only

5th parameter (optional): /NOREPLACE to not replace the contents of an existing zip file

Example: sArchive.exe "c:\src" "c:\dst" "*.txt" /READONLY /NOREPLACE

The files and folders in the source and destination paths specified in the command-line parameters are visible in the left and right panes. The user may dig down into folders and use the back button to come back up. But they can only go as high as the folder specified in the command line. Selecting a file in the left pane and clicking the Archive button will copy the file to a zip file, then shown in the right pane for verification. The right mouse and other file editing functions are not active.

In the example above, only document files ending in "txt" and any folders inside the specified folder are visible.

Secure Utilities | System tab

Secure Utilities - VA\User Name

| File | System | Input | Viewer | Administrator |

sRun Program Example:

sRun.exe

sControl Panel Example:

sControl.exe

sEject Device Example:

sEject.exe

sRes Resolution Example:

sRes.exe 0 800 600 /UPDATEREGISTRY /NO_OK

sLock Workstation Example:

sLock.exe

| Info | Manual | Windows 11 Pro Edition 64-bit, Version 24H2 (LTSC) | Help | Close |
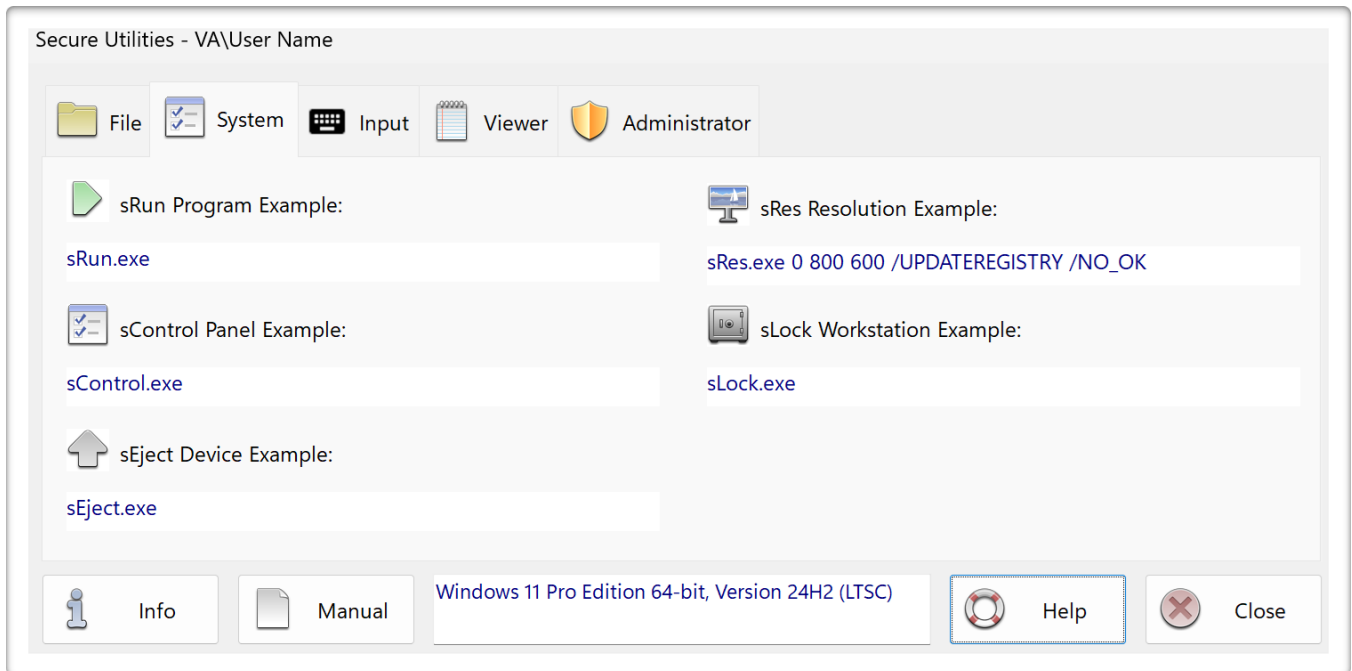
sRun Program, sControl Panel, sEject Device, sRes Resolution, and sLock Workstation are all included utilities to provide a user interface to parts of the system.

sRun Program
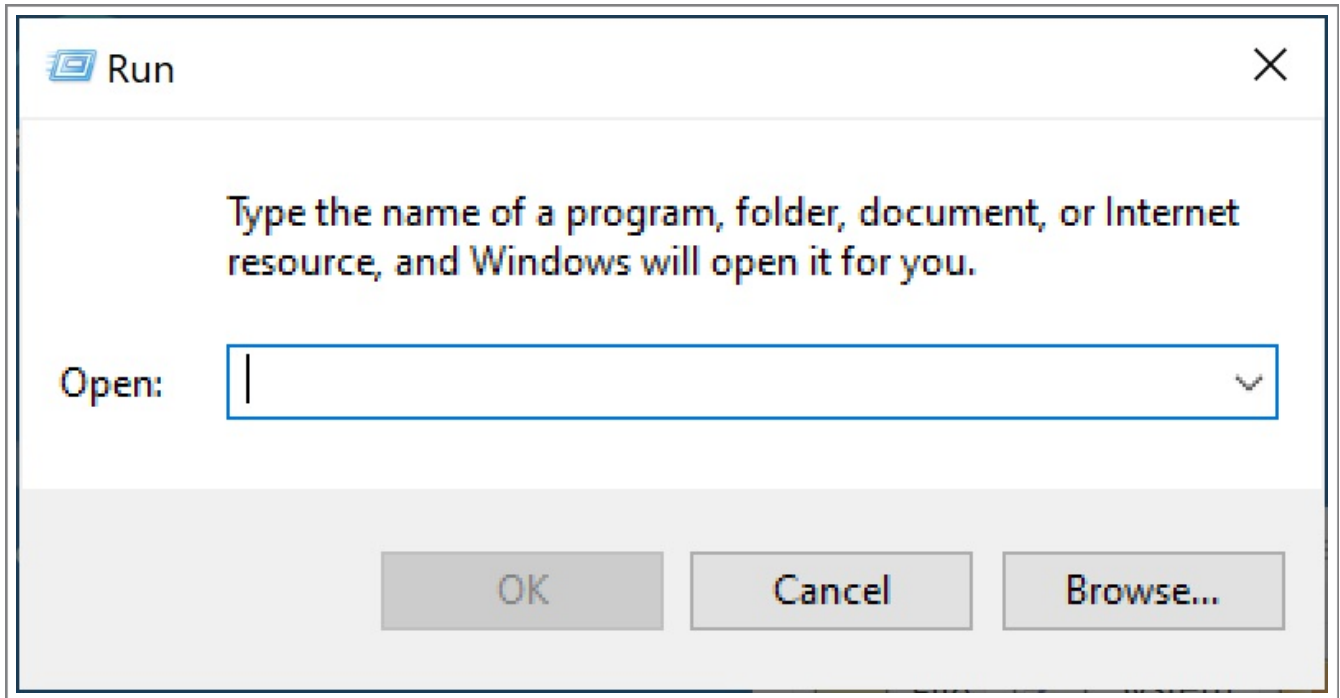
sRun Program does not need command-line parameters. sRun Program launches the Run Dialog.

Secure Desktop 10 and earlier had a Run toolbar button. This button does not exist in Secure Desktop 11 or 12. Use sRun.exe to run any program as an icon in Secure Desktop 11 or 12.
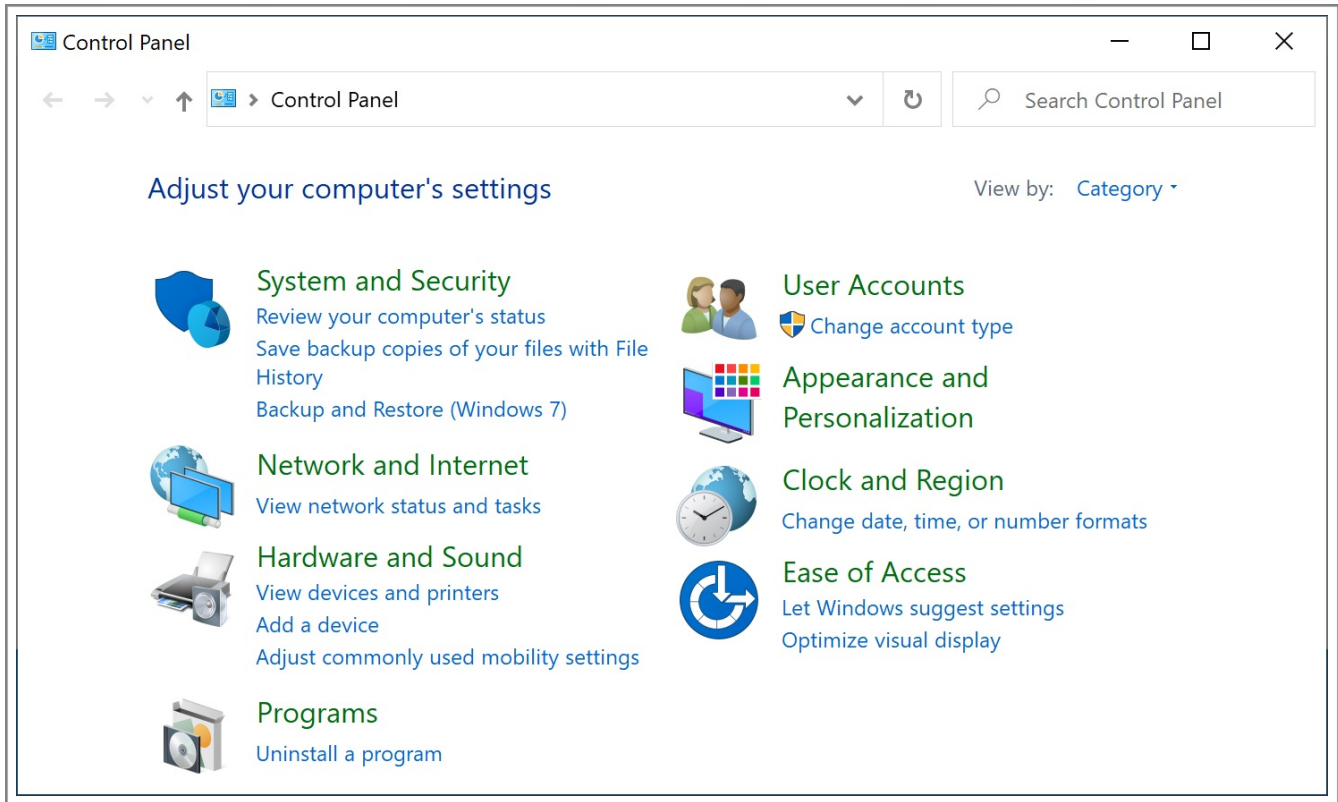
sControl Panel

sControl Panel does not need command-line parameters. sControl Panel launches the Windows Control Panel.

Secure Desktop 10 and earlier had a Control Panel toolbar button. This button does not exist in Secure Desktop 11 or 12. Use sControl.exe as an icon in Secure Desktop 11 or 12 to launch the control panel. The sControl.exe file included with Secure Desktop 10 and earlier attempted to display all control panel applets within a created window—the new sControl.exe launches the actual Windows Control Panel.

sEject Device

Safely Remove Hardware   ✕

Select the device you want to unplug or eject, and then click Stop. When Windows notifies you that it is safe to do so unplug the device from your computer.

Hardware devices:

ISS Dynamic Bus Enumerator
Samsung Flash Drive USB Device
HL-DT-ST DVDRAM GP60NS50 USB Device - (D:)
USB Attached SCSI (UAS) Mass Storage Device

ISS Dynamic Bus Enumerator at ISS HECI BUS

Properties   Stop

☐ Display device components

Close

sEject Device does not need command-line parameters. sEject Device launches the Safely Remove Hardware dialog.

Secure Desktop 10 and earlier had an Eject Device toolbar button. This button does not exist in Secure Desktop 11 or 12. Use sEject.exe to launch the Safely Remove Hardware dialog as an icon in Secure Desktop 11 or 12.

sRes Resolution

sRes Resolution needs command-line parameters:

1st parameter: Display Index (first display is zero)

If you only have one display, the index is zero. If there are two displays, then the primary display is zero and the other is one. If you specify a display index that doesn't exist, you will receive an error message and the resolution will not be changed.

2nd parameter: Pixel Width

3rd parameter: Pixel Height

The Pixel Width and Height have to be valid. In other words, 800 x 600 will probably work, but 801 x 601 will not. The width and height need to be valid for the video hardware on your system, otherwise an error will be displayed and the resolution will not be changed.

4th parameter (optional): /UPDATEREGISTRY

The graphics mode for the current screen will be changed dynamically and the graphics mode will be updated in the registry. The mode information is stored in the USER profile. Otherwise, the resolution change reverts when the user logs out and logs back in.

5th parameter (optional): /NO_OK

No OK message if resolution change succeeded. If error, message will be displayed.
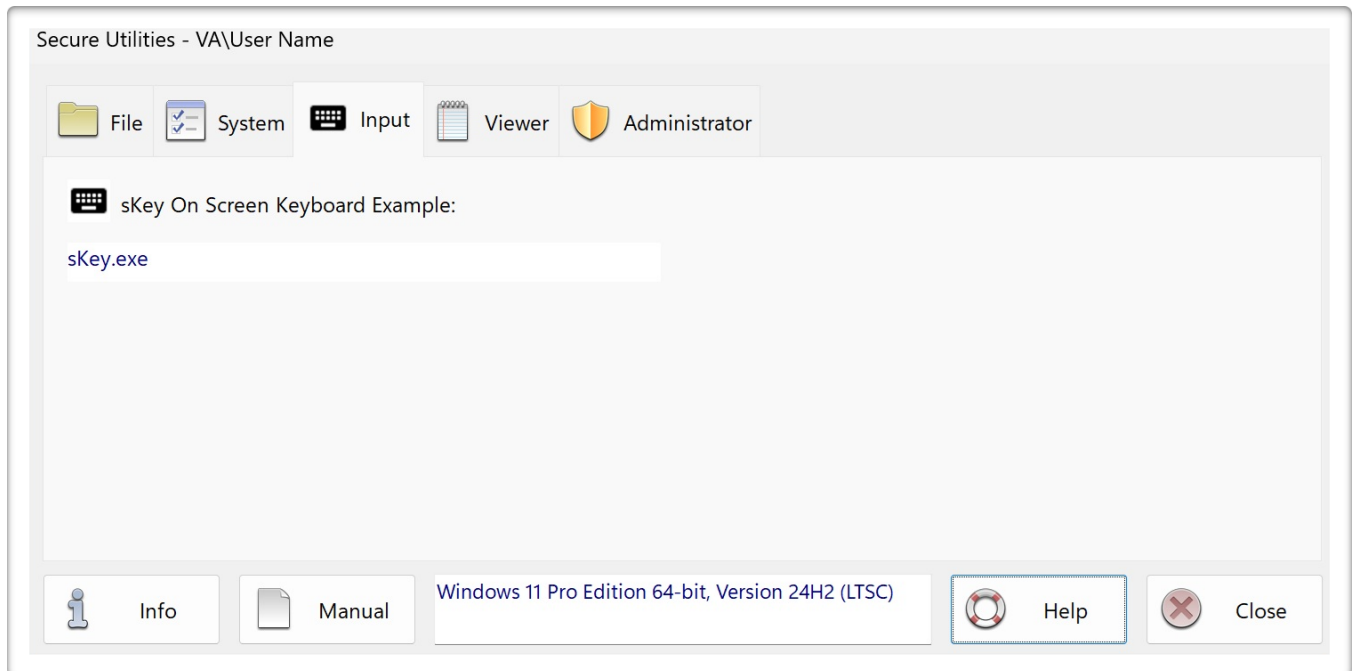
Example: sRes.exe 0 800 600 /UPDATEREGISTRY /NO_OK

sLock Workstation

sLock Workstation does not need command-line parameters. sLock Workstation locks the workstation's display. Locking a workstation protects it from unauthorized use.
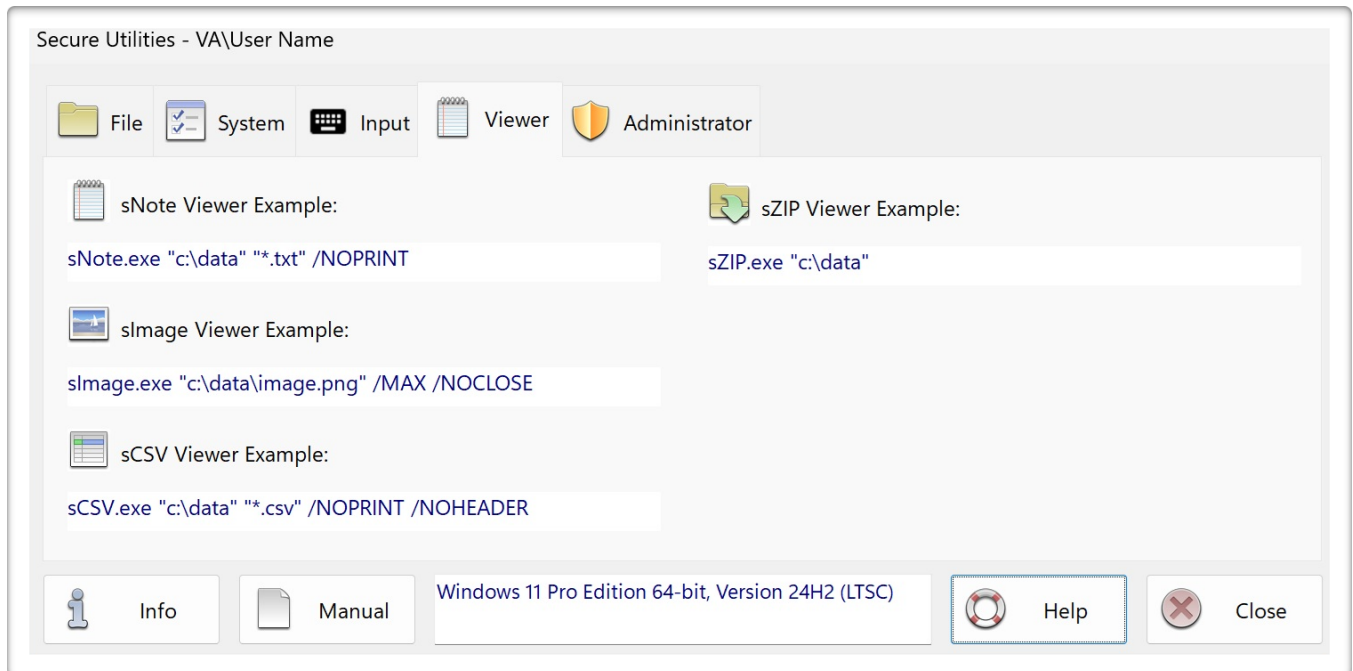
 Secure Utilities | Input tab

sKey On-Screen Keyboard is an included utility to provide a user interface to parts of the system.

sKey On Screen Keyboard does not need command-line parameters. sKey On-Screen Keyboard is a simple on-screen keyboard for use when there is only a touch screen and not a physical keyboard.

Secure Utilities | Viewer tab

Secure Utilities - VA\User Name

File   System   Input   **Viewer**   Administrator

sNote Viewer Example:

sNote.exe "c:\data" "*.txt" /NOPRINT

sImage Viewer Example:

sImage.exe "c:\data\image.png" /MAX /NOCLOSE

sCSV Viewer Example:

sCSV.exe "c:\data" "*.csv" /NOPRINT /NOHEADER

sZIP Viewer Example:

sZIP.exe "c:\data"

Info   Manual   Windows 11 Pro Edition 64-bit, Version 24H2 (LTSC)   Help   Close

sNote Viewer, sImage Viewer, sCSV Viewer, and sZIP Viewer are included utilities that view file contents.

 sNote Viewer

sNote Viewer and sImage Viewer are included utilities that view files.

sNote Viewer needs command-line parameters:

1st parameter: folder path in quotes.

2nd parameter (optional): wildcard file filter (*.txt is the default).

3rd parameter (optional): /NOPRINT to remove the print button or <printername> to specify the printer.

Example: sNote.exe "c:\data" "*.txt" /NOPRINT

The files and folders in the path specified in the command-line parameter are visible in the left pane. The user may dig down into folders and use the back button to come back up. But they can only go as high as the folder specified in the command line. Selecting a text file will display the text from that text file in the right pane. The right mouse and other file editing functions are not active.

In the example above, only document files ending in "txt" and any folders inside the specified folder are visible. The print button is not visible.

The default function of the print button is to print to the default printer. sNote Viewer uses the Notepad.exe application with appropriate command line parameters to send the text file to the default printer.

An alternate optional third command-line parameter is to specify the printer's name for the print button. Again, sNote Viewer uses the Notepad.exe application with appropriate command line parameters to print the text file to the designated printer name.

sImage Viewer
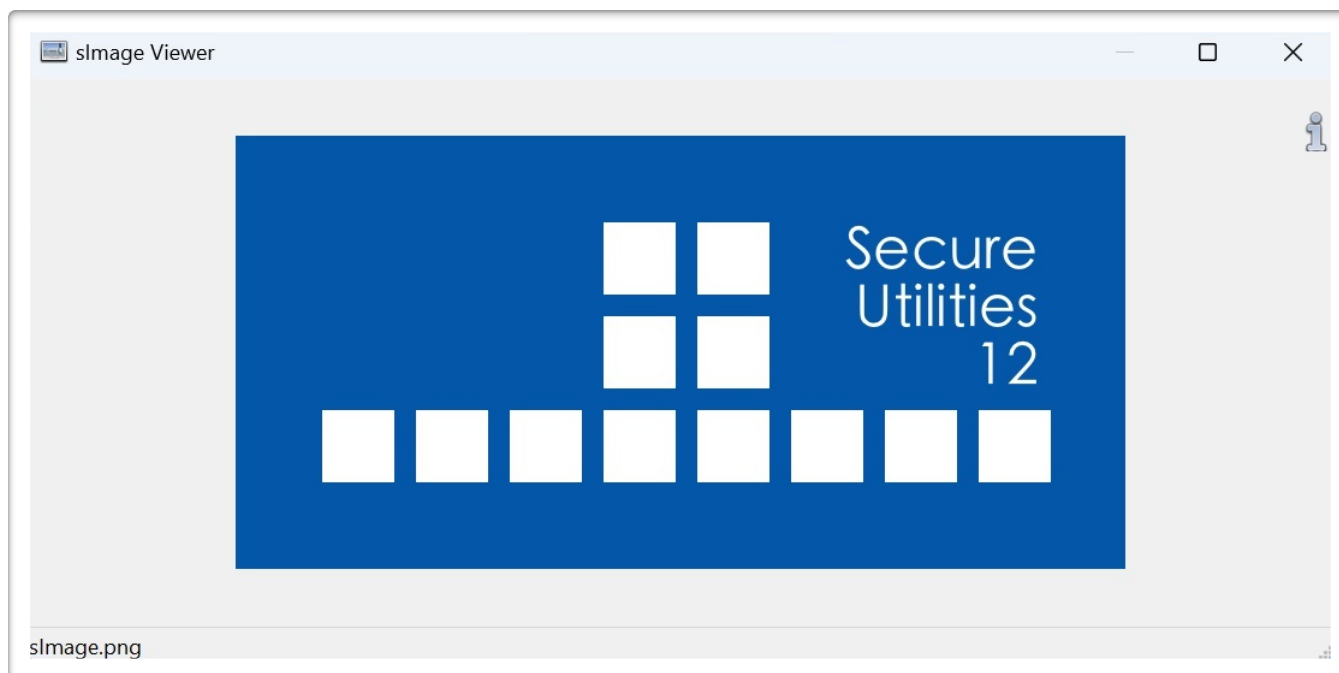
sImage Viewer needs command-line parameters:

1st parameter: file path in quotes

Most common image file types are supported.

2nd parameter (optional): /MAX makes the image window open maximized.

3rd parameter (optional): /NOCLOSE disables the close button to prevent exiting the application.
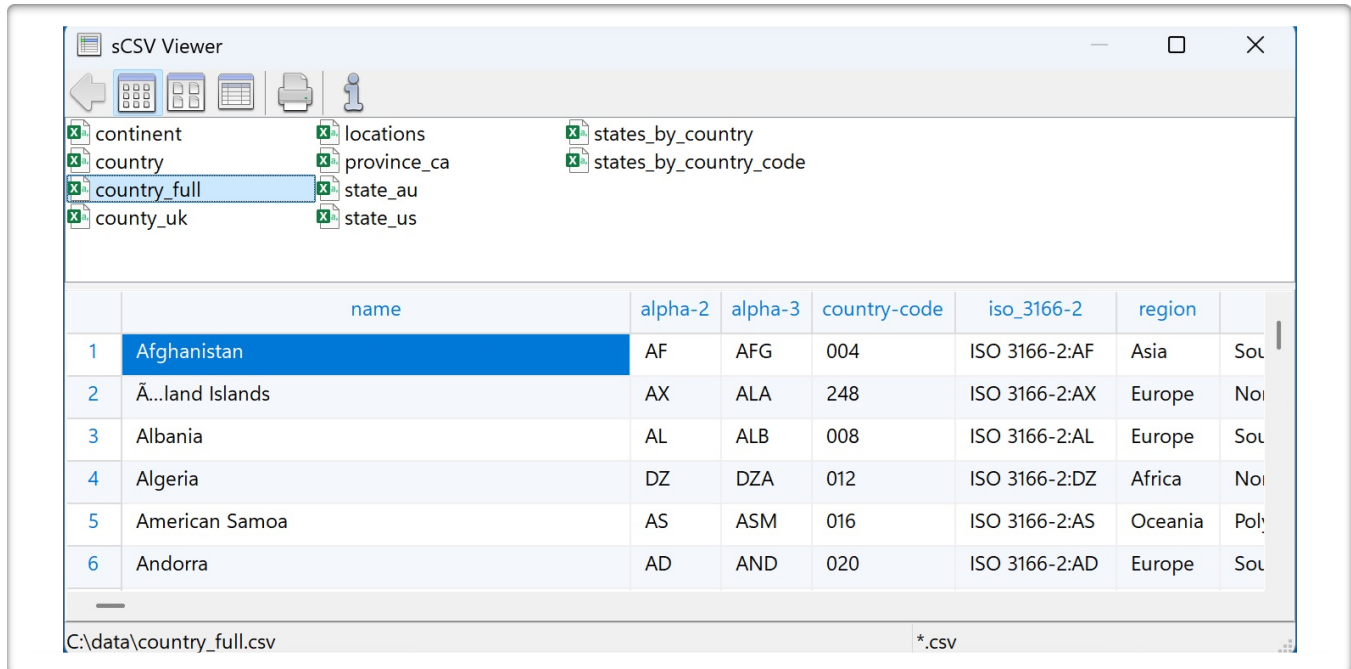
Example: sImage.exe "c:\data\image.png"/MAX /NOCLOSE

The status bar displays the file path.

 sCSV Viewer

sCSV Viewer needs command-line parameters:

1st parameter: folder path in quotes.

2nd parameter (optional): wildcard file filter (*.csv is the default).

3rd parameter (optional): /NOPRINT to remove the print button or <printername> to specify the printer.

Example: sCSV.exe "c:\data" "*.csv" /NOPRINT /NOHEADER

The files and folders in the path specified in the command-line parameter are visible in the top pane. The user may dig down into folders and use the back button to come back up. But they can only go as high as the
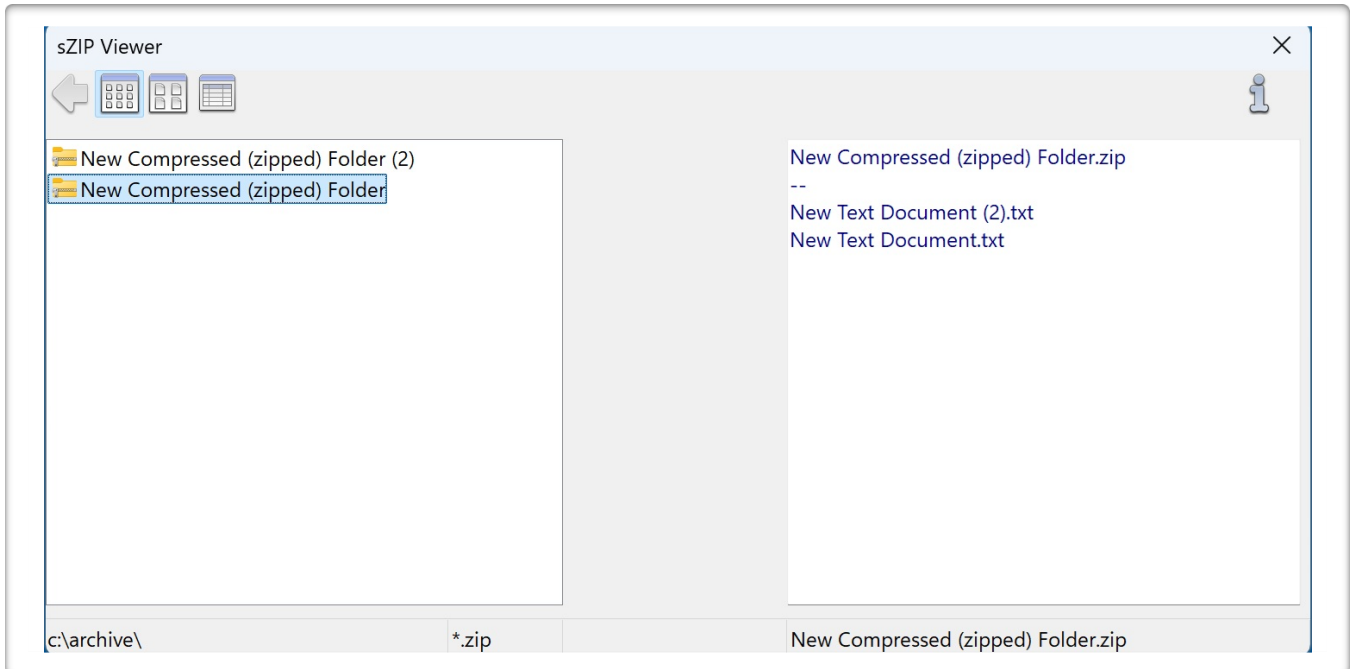
folder specified in the command line. Selecting a csv file will display the text from that csv file in the bottom pane. The right mouse and other file editing functions are not active.

In the example above, only document files ending in "csv" and any folders inside the specified folder are visible. The print button is not visible.

The default function of the print button is to print to the default printer. sCSV Viewer uses the Notepad.exe application with appropriate command line parameters to send the csv file to the default printer.

An alternate optional third command-line parameter is to specify the printer's name for the print button. Again,

sCSV Viewer uses the Notepad.exe application with appropriate command line parameters to print the text file to the designated printer name.

The /NOHEADER optional parameter should be used if the first line of the csv file does not contain header information.

sZIP Viewer

sZIP Viewer needs one command-line parameter:

1st parameter: folder path in quotes.

Example: sZIP.exe "c:\archive"

The files and folders in the path specified in the command-line parameter are visible in the left pane. The user may dig down into the folders and use the back button to come back up. But they can only go as high as the folder specified in the command line. Selecting a ZIP file will display the files within that ZIP file in the right pane. The right mouse and other file editing functions are not active.

Secure Utilities | Administrator tab
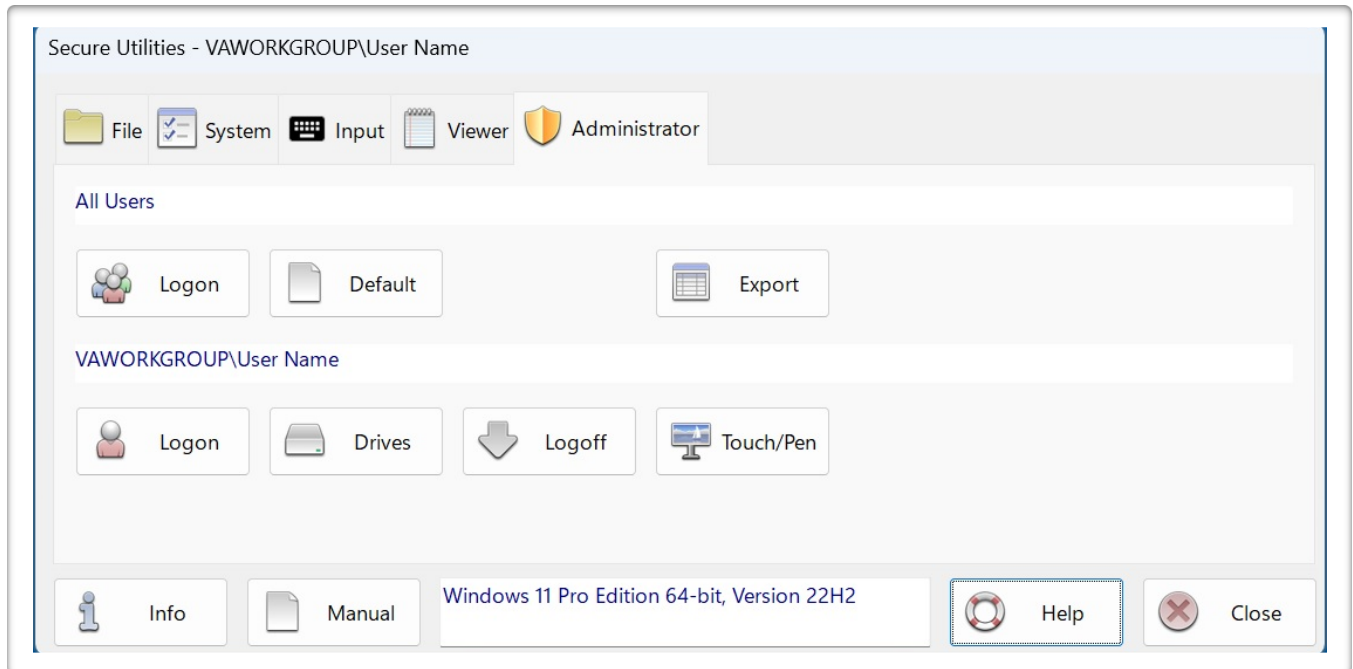
A shield means that Administrator privileges are needed. Non-administrators can choose from a user list. Every button in the Administrator tab requires Administrator privileges.

All Users section:

The Logon button sets values for All Users.

Logon can change Ctrl + Alt + Delete settings and set Automatic Logon features.

The Default button provides a setting to disable "How do you want to open this file?" dialogs.

The Export button displays automatically exported registry setting information.

User Name section:

The Logon, Drives, Logoff, and Touch/Pen buttons apply to the logged-in user.

Logon will set restrictions in the Ctrl + Alt + Delete dialog.

Drives will set registry values for the currently logged-in user to hide drive letters and other features from standard file open/save as dialogs.
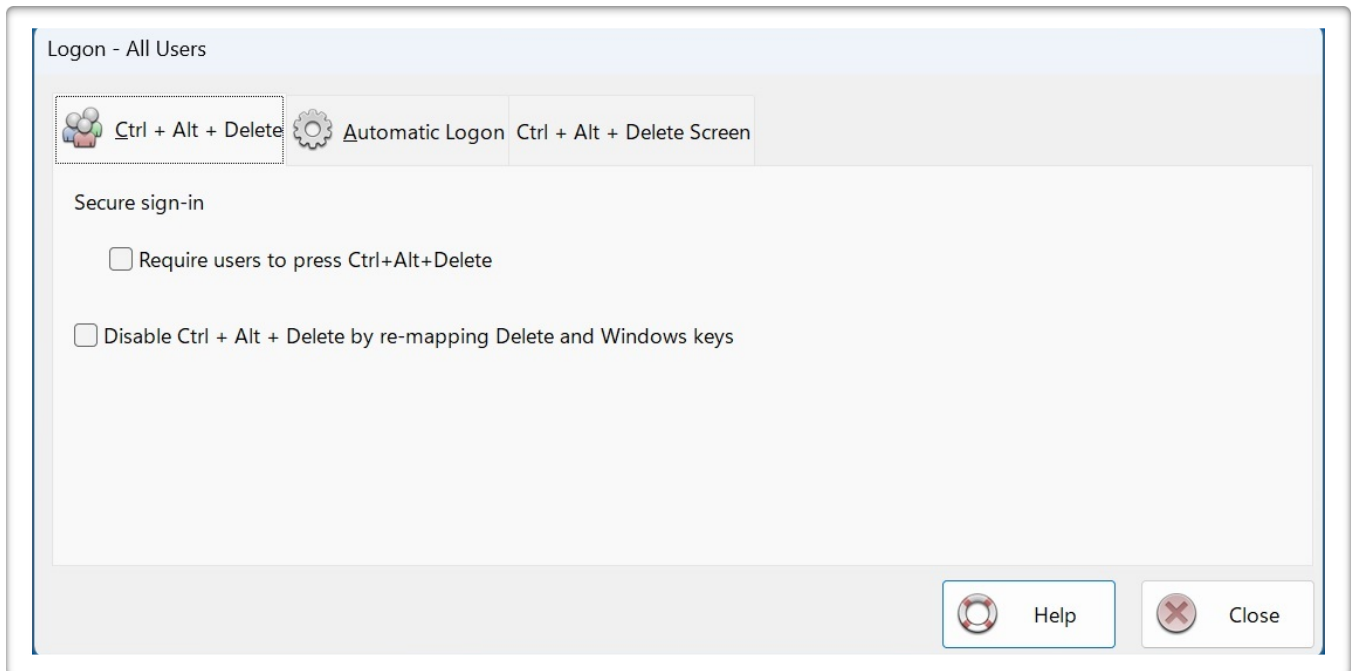
Logoff provides help for the Auto Logoff Screen Saver, and the ability to edit the Warning Message within the Auto Logoff Screen Saver.

Touch/Pen can disable the Touch and Hold Right Mouse Click function for touch and pen input.

 Secure Utilities | Administrator tab | All Users section | Logon button | Ctrl + Alt + Delete tab

Require users to press Ctrl+Alt+Delete checkbox:

This checkbox sets the registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DisableCAD

If you check the checkbox, this registry value is 0; otherwise, it is 1.

Disable Ctrl + Alt + Delete by re-mapping Delete and Windows keys checkbox:

To disable Ctrl + Alt + Delete, we re-map Delete with the Windows key for all users, even during login.

This checkbox sets the registry value:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout\Scancode Map

Secure Utilities | Administrator tab | All Users section | Logon button | Automatic Logon tab

To set Automatic Logon, choose the user name in the User Accounts Dialog and uncheck "Users must enter a user name and password to use this computer."

Automatic Logon Enabled determines whether the automatic logon feature is on. Automatic logon uses the domain, user name, and password stored in the registry to log you on to the computer when the system starts. The Log On to Windows dialog box is not displayed.

After setting these text fields, click on the Save button.

If you disable Automatic Logon, uncheck the Automatic Logon Enabled checkbox and click the Save button.

You must log off of Windows, shut down the computer, and start it again before changes to this entry take effect.

CAUTION:

Automatic logon lets other users start your computer and log on using your account. Because an automatic logon proceeds in a different order than an authenticated logon, it can cause timing conflicts.

The values entered on this tab set the following registry values:
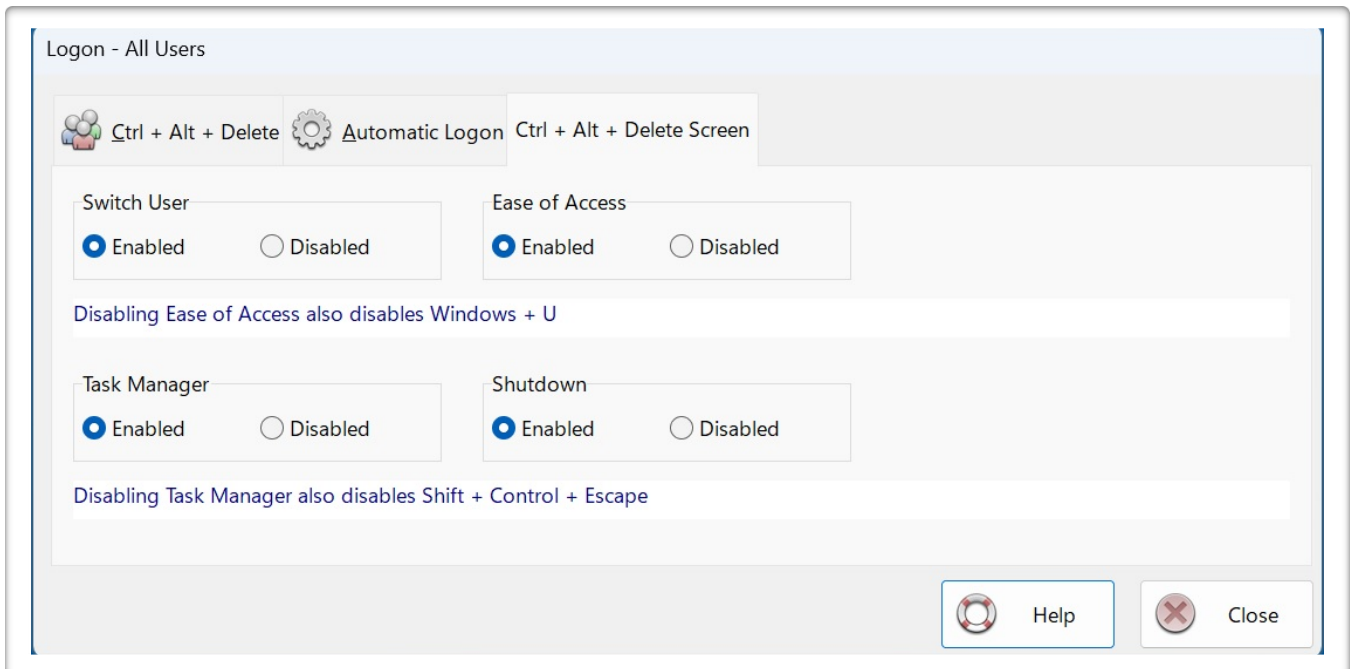
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

AutoAdminLogon

DefaultDomainName

DefaultUserName

Secure Utilities | Administrator tab | All Users section |

Logon button | Ctrl + Alt + Delete Screen tab

Several menu items are available when the user presses Ctrl + Alt + Delete. You can disable the Switch User, Ease of Access, Task Manager, and Shutdown in this tab by setting registry values:

Switch User & Task Manager:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

HideFastUserSwitching

DisableTaskMgr

Ease of Access:

HKEY_LOCAL_MACHINESoftware\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe

debugger

Shutdown:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

NoClose

Secure Utilities | Administrator tab | All Users section | Default button | Default App tab

When you install a new app that can open a file type with a default app association, a dialog will be displayed named "How do you want to open this file?" when launching the file.

This registry setting disables this behavior.
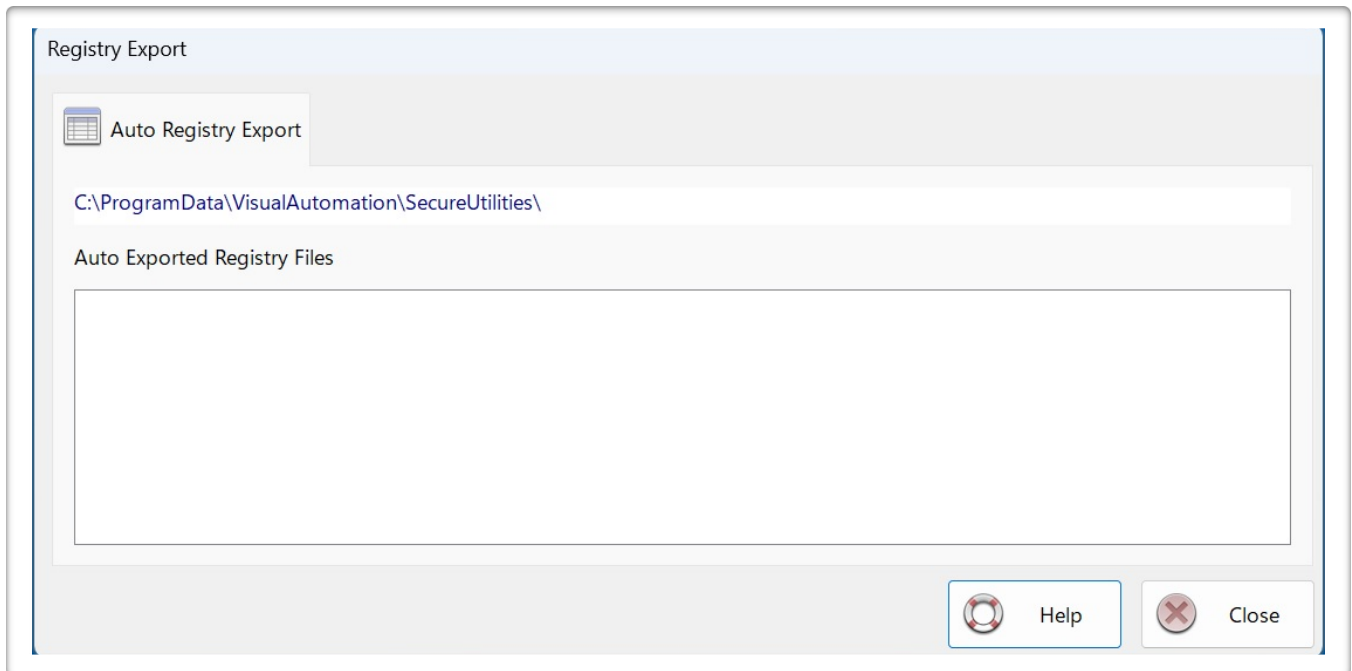
This checkbox sets the registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer\NoNewAppAlert

This registry value is 0 for "enable dialog" and set to 1 for "disable dialog."

Secure Utilities | Administrator tab | All Users section | Export button | Auto Registry Export tab

The full path to the configuration file folder is at the top.

Secure Utilities automatically exports the ROOTKEY and SubKey of each registry section it writes to during configuration.

Secure Utilities uses the REG command with the EXPORT Operation each time it changes the registry.

The Secure Utilities Auto Reg Export*.txt filename contains the UserName and HKLM or HKCU for HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER, respectfully.

Secure Utilities creates the Secure Utilities Auto Reg Export*.txt files primarily for documentation purposes. However, you could also use them to audit these setting changes.

Because Secure Utilities generates these files using REG EXPORT, they can also be IMPORTed using the REG command. Please keep in mind that the IMPORT is a merge of data.

REG IMPORT may be helpful in the configuration of other users or other identical computers, but we do not recommend this. Execute a REG IMPORT with caution.

To learn more about REG, open a command prompt and start REG /? for command-line help information.

Secure Utilities | Administrator tab | UserName section | Logon button | Ctrl + Alt + Delete Screen tab

Logon - VAWORKGROUP\User Name

Ctrl-Alt-Delete Screen

Lock Workstation
◉ Enabled   ○ Disabled

Sign Out
◉ Enabled   ○ Disabled

Disabling Lock Workstation also disables Windows-L

Change Password
◉ Enabled   ○ Disabled

Task Manager
◉ Enabled   ○ Disabled

Disabling Task Manager also disables Shift-Control-Escape

Help   Close

When the user presses Ctrl-Alt-Delete, several menu items are available. You can disable the Lock Workstation, Change Password, Task Manager, and Sign Out in this tab by setting registry values:

Lock Workstation, Change Password, & Task Manager:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

DisableLockWorkstation

DisableChangePassword

DisableTaskMgr

Sign Out:

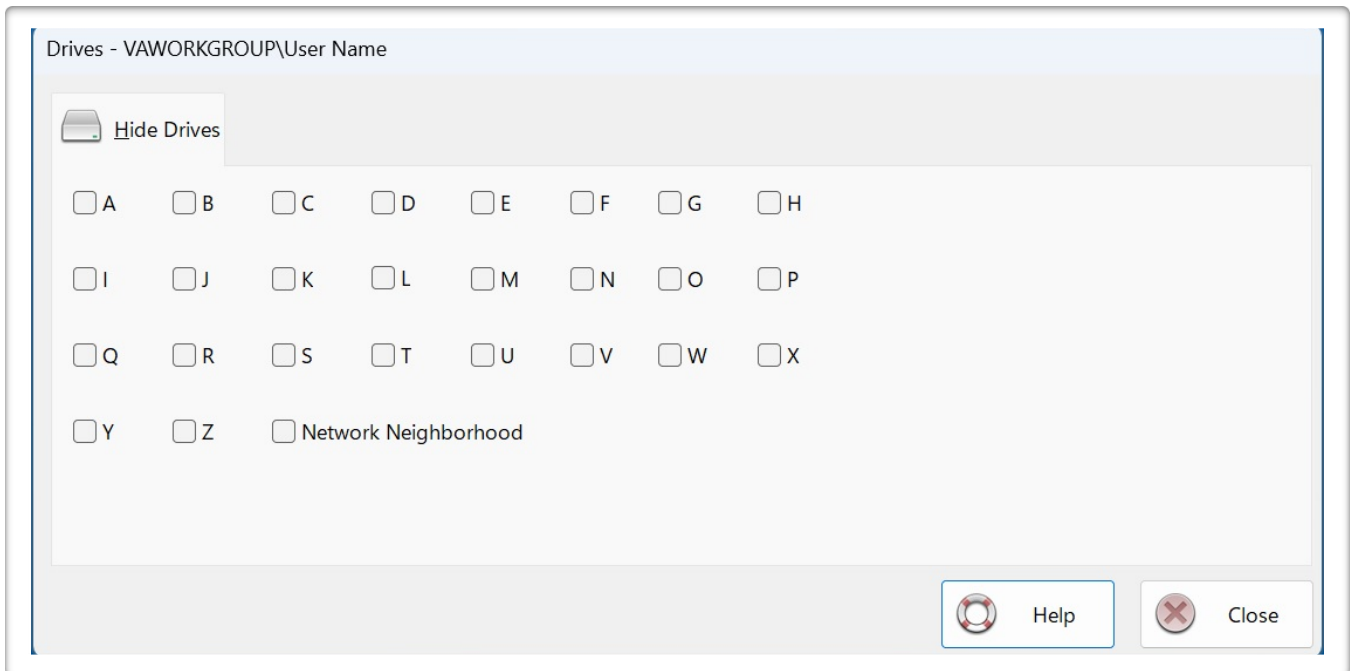HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

NoLogoff

You can not disable Windows shutdown here, but you can disable it in the All Users section | Logon button | Ctrl-Alt-Delete Screen tab.

Secure Utilities | Administrator tab | UserName section | Drives button | Hide Drives tab

The Hide Drives tab sets registry values for the user currently logged in. These settings require that the current user is a member of the Administrators Group. Log in as each admin user. Set the values and remove the user from the Admin group as needed.

Secure Utilities sets a registry value by checking on a drive letter that removes the drives from "file open" and "file save as" dialogs. These settings are on a user-by-user basis.

The registry set is:

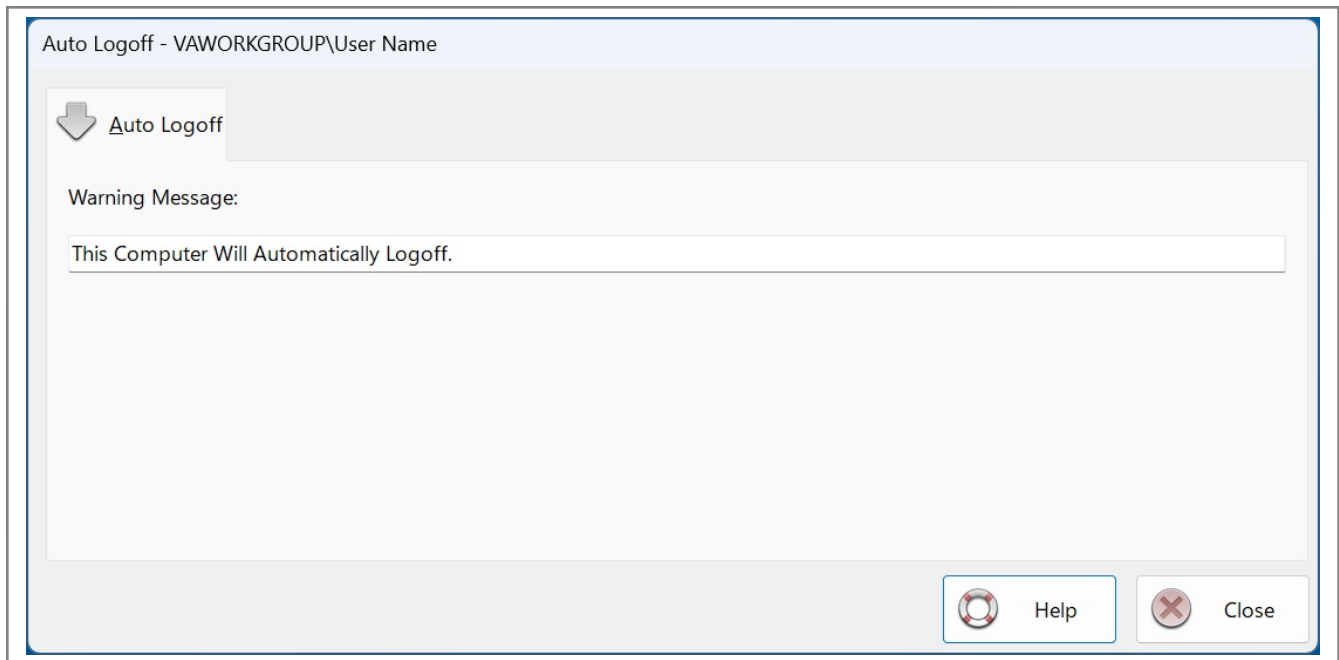HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

NODRIVES

NoNetHood

Secure Utilities | Administrator tab | UserName section | Logoff button | Auto Logoff tab

Auto Logoff - VAWORKGROUP\User Name

Auto Logoff

Warning Message:

This Computer Will Automatically Logoff.

Help   Close

Secure Utilities includes a screen saver program that is not an actual screen saver. Customers have requested the ability to automatically log off from Windows after no user activity for a period of time. To do this, we developed a screen-saver program for Windows. Screen Savers are executable programs launched automatically when the specified number of minutes have passed without mouse or keyboard activity.

The screen saver application displays a 10-second countdown dialog with a cancel button; then, it will perform a forced log-off. Any unsaved work within an editor (Notepad, Word, Excel, or other editor) is lost. Note that any services you may be running will continue after a log-off operation. The screen saver application does not use the password feature.

This feature is for customers who want to be sure that the logged-in user is the person using the computer. In an open environment, if a user walks away from the machine without logging off, the screen saver application will automatically log off the computer.

There are no settings for the screen saver other than the Warning Message and the number of minutes before starting after the activity. Choose the screen saver as you would any other. Note that you will need to set the screen saver for each user.

The registry location for the Warning Message is:

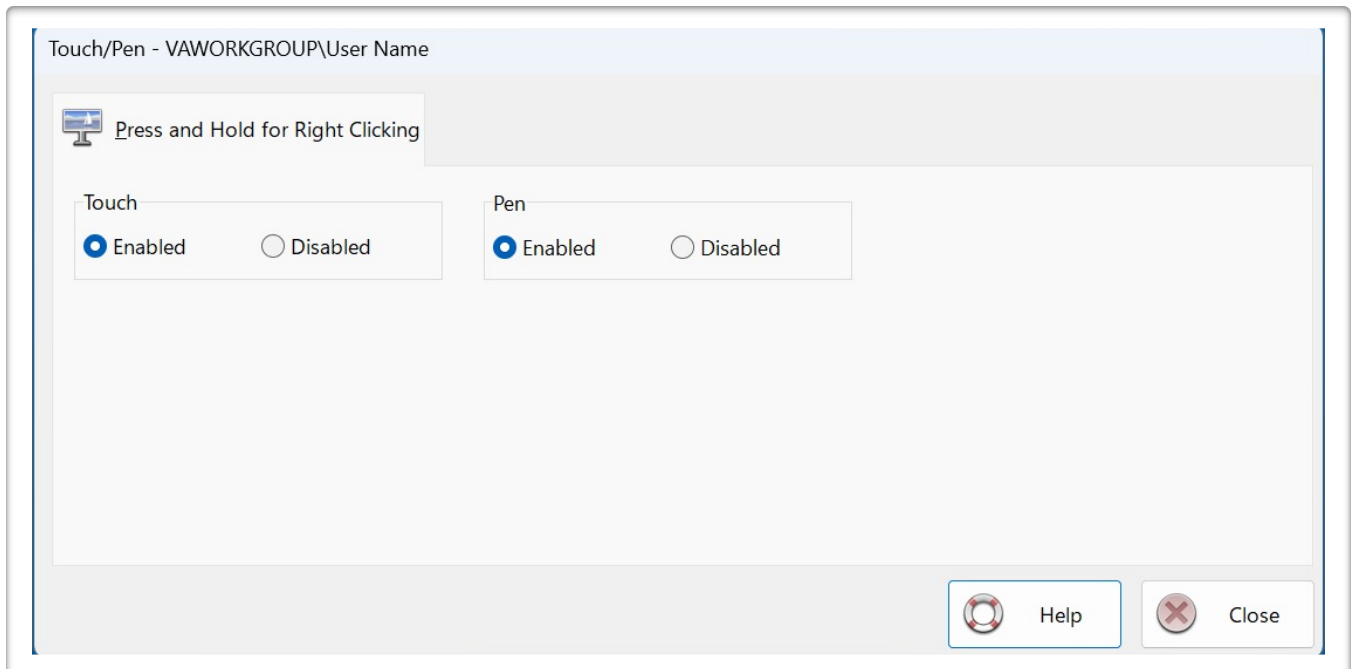HKEY_CURRENT_USER\Software\Visual Automation\Secure Utilities\Auto Logoff

WarningMessage

The default Warning Message is:

"This Computer Will Automatically Log Off."

Secure Utilities | Administrator tab | UserName section | Touch/Pen button | Press and Hold for Right Clicking tab

Press and hold for right-clicking can be disabled for Touch or the Pen input.

Touch:

HKEY_CURRENT_USER\Software\Microsoft\Wisp\Touch

TouchMode_hold

Set to 1 for "on" and 0 for "off"

Pen:

HKEY_CURRENT_USER\Software\Microsoft\Wisp\Pen\SysEventParameters

HoldMode

Set to 1 for "on" and 3 for "off"

Windows Registry

If you need to modify Secure Utilities registry settings manually, you must run RegEdit.exe.

Use caution: This database contains essential information about your Windows system's operation; modifying the wrong parameter could lead to unintended results.

Secure Utilities automatically exports registry settings to TXT files. Please see the section in this manual labeled Secure Utilities | Administrator tab | Export button | Registry Export tab

Windows 10 & 11 Editions
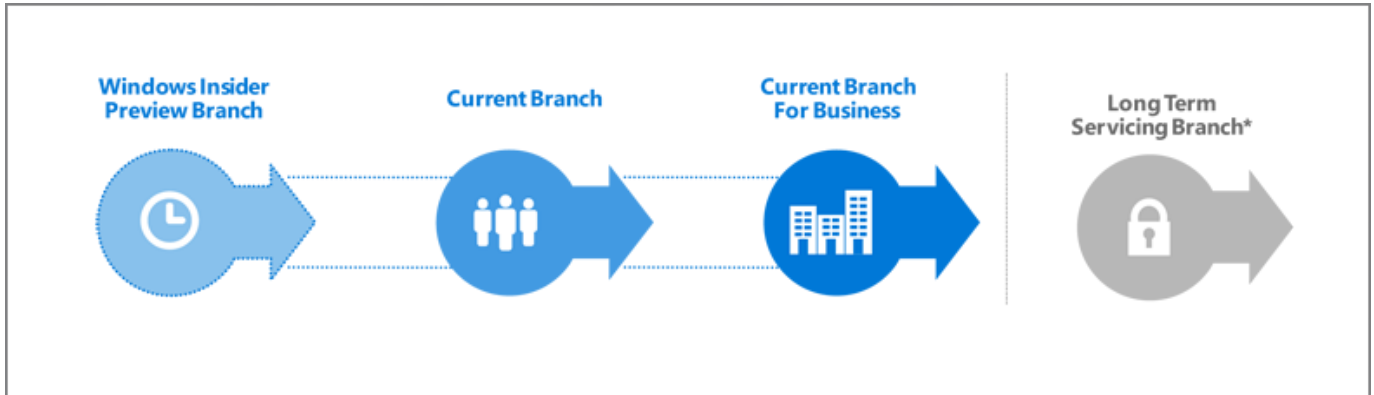
Windows 10. Windows as a Service (WaaS)

Windows 10 is very different from previous versions of Windows. Windows 10 will make regular incremental improvements to the operating system. Some of these changes might not be desirable in a mission-critical system. Because of this, the Windows 10 Enterprise Long-Term Servicing Branch (LTSB) Edition is worth consideration.

Windows 10 Enterprise Long-Term Servicing Branch (LTSB) Edition

"Specialized systems—such as devices that control medical equipment, point-of-sale systems, and ATMs—often require a longer servicing option because of their purpose. These devices typically perform a single important task and don't need feature updates as frequently as other devices in the organization. It's more important that these devices be kept as stable and secure as possible than up to date with user interface changes. The LTSC servicing model prevents Windows 10 Enterprise LTSB devices from receiving the usual feature updates and provides only quality updates to ensure that device security stays current. With this in mind, quality updates are still immediately available to Windows 10 Enterprise LTSB clients. However, customers can choose to defer them by using one of the servicing tools mentioned in the section Servicing tools."

Quoted from the following article:

https://technet.microsoft.com/en-us/itpro/windows/plan/windows-10-servicing-options

As the Microsoft TechNet article explains, Microsoft recommends the Windows 10 Enterprise LTSB Edition for a mission-critical system using Windows 10 in Retail, Manufacturing, and Pharmaceutical. We designed Secure Desktop for these same industries.

Win32 Windows application and the Universal Windows Program (UWP) app

We designed Secure Desktop for Win32 programs (e.g., COM, Win32, WPF, WinForms, etc.).

A Universal Windows Program (UWP) app is a new kind of app designed for Windows 10 and Windows 11. A Progressive Web App (PWA) is a website that can appear to the user like a traditional application.

The Windows Explorer and Secure Desktop shell can run Win32 programs.

In Windows 10 and Windows 11, UWP and PWA apps need the Windows Explorer shell. The Windows Explorer shell has to be running to launch and run a UWP or PWA app. This design is an unfortunate architectural choice.

Secure Desktop provides security by replacing the Windows Explorer shell. When setting the Secure Desktop program to be the Windows shell, the Explorer shell is not running. Because the Explorer shell is not running, Secure Desktop can not run UWP or PWA apps in any Edition of Windows 10 or Windows 11.

Browsers

Secure Desktop has always been able to launch Win32 browsers such as Internet Explorer, Brave, Chrome, Firefox, and Opera.

Secure Desktop can not launch UWP browsers like the original Microsoft Edge browser. The new Microsoft Edge browser is a Win32 app and, therefore, is compatible with Secure Desktop. We do not recommend using Internet Explorer. Internet Explorer 11 is retired and out of support.

If you are currently using Internet Explorer, please read the following Microsoft document about Internet Explorer and the Microsoft Edge Browser:

https://docs.microsoft.com/en-us/deployedge/edge-learnmore-neededge

If you are using the new Microsoft Edge browser, please read the following Microsoft document about the new Microsoft Edge browser policies:

https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies

Our Windows 10 Recommendation

Although Secure Desktop 11 and 12 are compatible with many editions of Windows 10 and Windows 11, we strongly recommend consideration of the Windows 10 Enterprise LTSC Edition before making a final decision. Regardless of the Edition of Windows 10 or 11 you choose, Secure Desktop can not run UWP or PWA apps. Our research shows that Windows 10 Enterprise LTSC Edition may be the most secure and stable in a mission-critical system.

https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise

Other Windows 10 & Windows 11 Versions

Secure Desktop is incompatible with Windows 10S, Windows 10 in S Mode, Windows 11S, or Windows 11 in S Mode. Secure Desktop 11 & 12 will work on Windows 10 on ARM in emulation mode, but Secure Desktop 10 will not. Secure Desktop 11 & 12 was not explicitly tested on Windows 11 on ARM at the time of this writing. However, it should be fully compatible with emulation mode.

Announcing the availability of Windows 10 Pro and Enterprise on Surface Hub 2

The Microsoft Surface Hub 2S has always shipped with Windows 10 Team, which runs Microsoft Store apps only. You can now install Windows 10 Pro and Enterprise on the Surface Hub 2. Please read more from Microsoft here: techcommunity.microsoft.com

Secure Desktop 10, Secure Desktop 11, Secure Desktop 12, Secure Utilities 11, and Secure Utilities 12 should all work in the environment of Windows 10 Pro and Enterprise on Surface Hub 2. Secure Desktop 11 & 12 and Secure Utilities 11 & 12 should work in the environment of Windows 11 Pro and Enterprise on Surface Hub 2. We have not tested these environments, but Secure Desktop should be fully compatible.

Windows 11

Secure Desktop 10 is not specifically designed or tested in Windows Server 2022 or Windows 11.

Secure Desktop 11 is specifically designed and tested for Windows Server 2022 and Windows 11.

Commenting on Visual Automation Products and Services

We plan to expand our service as we grow based on your feedback. If you have suggestions, comments, or feedback about a Visual Automation product or service, please write to:

Visual Automation, Inc.

PO Box 502

Grand Ledge, Michigan 48837 USA

sales@visualautomation.com e-mail sales

support@visualautomation.com e-mail support

https://visualautomation.com web page

Technical Support Options

Technical support is available via e-mail at support@visualautomation.com.

We can help you more quickly if you are at your computer, Secure Utilities is running, your Secure Utilities documentation is close by, and you have the following information on hand:

Product serial number. Click the info button or consult your e-mail message to find the serial number.

Product version number. To find the version number, click on the info button.

Computer make and model.

Microsoft Windows version.

Other applicable hardware and software.

Also, please include the exact wording of any error messages and screenshots.