VISUAL AUTOMATION

Product Manual

Secure Utilities
Version 11
Visual Automation, Inc.
PO Box 502
Grand Ledge, Michigan 48837 USA

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

Last Updated October, 2022

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

Secure Desktop 10 utilities versus Secure Utilities 11

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 11.

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 11. Here, you can find utility examples, help, and the new interface to system registry settings. sKey On Screen Keyboard, sImage Viewer and sMenu Start Menu have also been added.

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, such as file attribute manipulation and Internet Explorer registry settings are deprecated.

We are very excited about Secure Utilities 11. The utilities are easy to use, better looking, and the best user experience yet.

Secure Utilities 11 is a 32-bit application but is also 64-bit aware. We tested Secure Utilities 11 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 11 on Microsoft Surface Pro and Microsoft Surface Laptop Studio computers. If you are using Windows 10/11 in a mission-critical setting, please consider using the Enterprise LTSB Edition. Secure Utilities 11 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 11 are 32-bit and is therefore compatible with Windows 10 on ARM and Windows 11 on ARM using emulation. We tested Secure Utilities 11 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 has 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 somewhat fragile environment in that the wrong setting somewhere 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 get 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 provide 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. There is a companion executable named suAdmin.exe, which 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 right now, named sUtility.pdf.

sExplore File Explorer

This program is a replacement for File Explorer that is restricted to a particular folder and file wild card based on command-line parameters. The user can not navigate above the base folder in the file folder hierarchy. File and folder editing is not possible, but the user 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 can not navigate above the base folders in the file folder hierarchy. File and folder editing is not possible. The file name for sCopy File is sCopy.exe.

sRun Program

This 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.

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 card based on command-line parameters. The user can not navigate 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.

sMenu Start Menu

This program provides a way to access all file shortcuts normally found in the Start Menu and Desktop.. The file name for sMenu Start Menu is sMenu.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 is met. This file is named sLogOff.SCR, located in the Windows System folder.

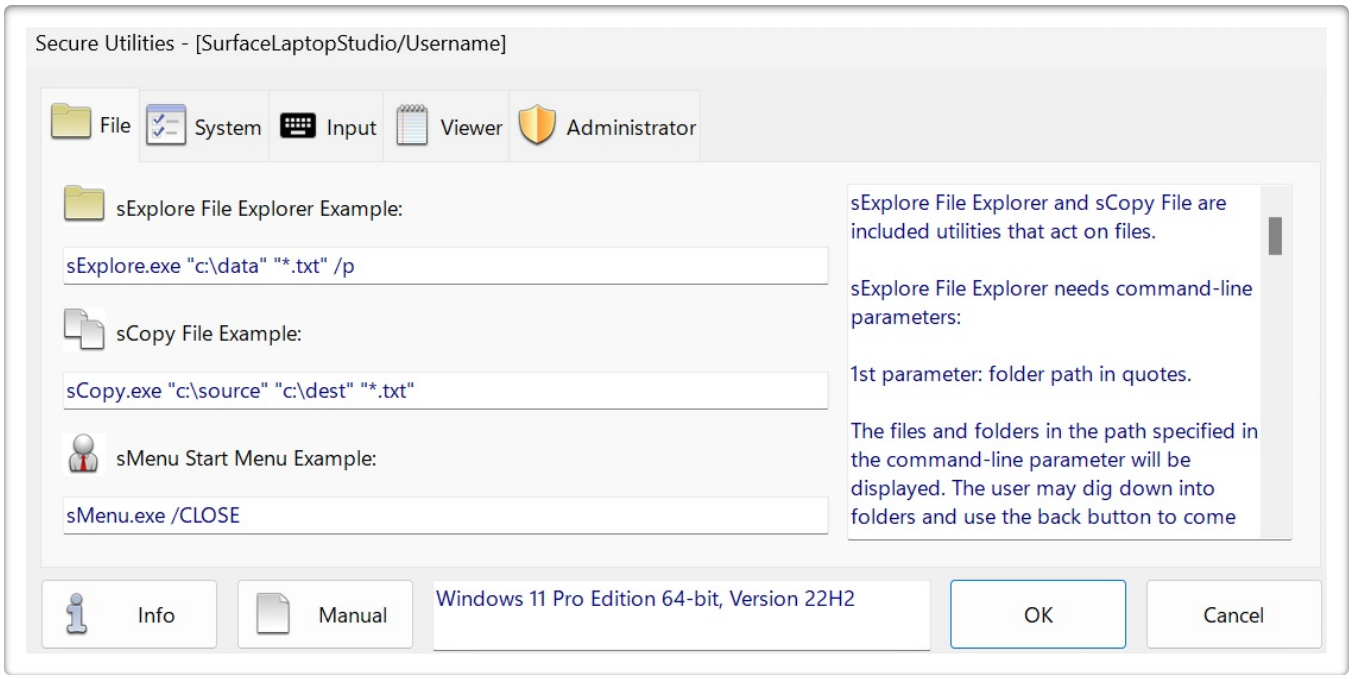
sUtilman

Secure Utilities includes a file named sUtilman.exe that is needed for the registry setting to disable Ease of Access, located in the Windows System folder.

Setup Program

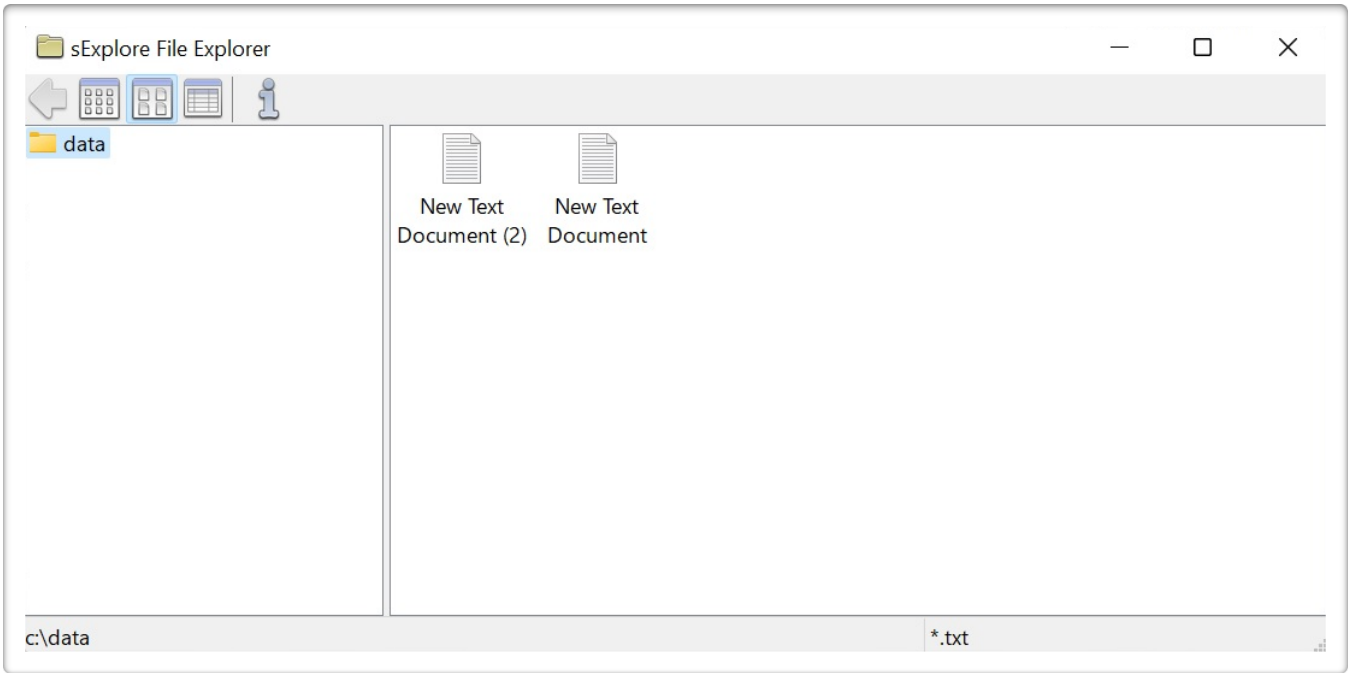
Secure Utilities 11 uses Inno Setup for its installation software.

Secure Utilities | File tab



sExplore File Explorer, sCopy File, and sMenu Start Menu are included utilities that act on files.

sExplore File Explorer



sExplore File Explorer needs command-line parameters:

1st parameter: folder path in quotes.

The files and folders in the path specified in the command-line parameter will be displayed. The user may dig down into folders and use the back button to come back up. But they can not go higher than 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.

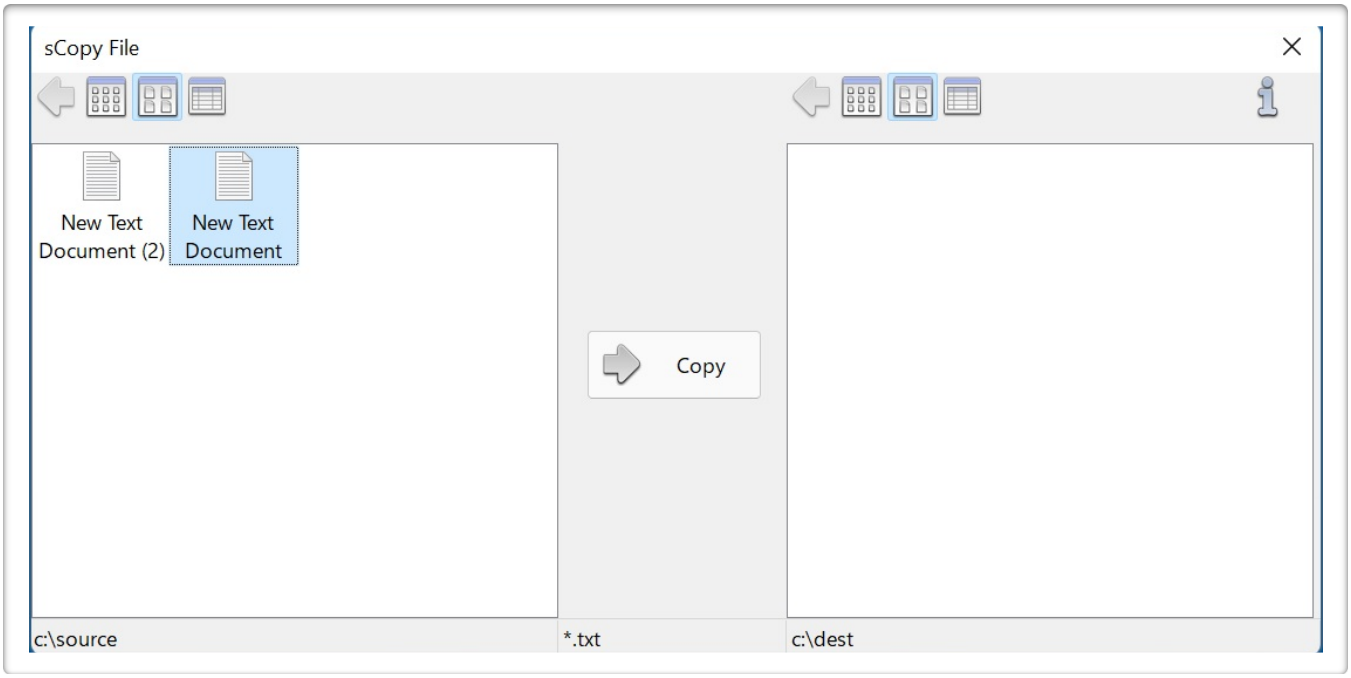
Only files matching the wildcard file filter will be displayed, along with any folders inside of the specified folder.

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

When the user has one or more document files selected and clicks Print, 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.

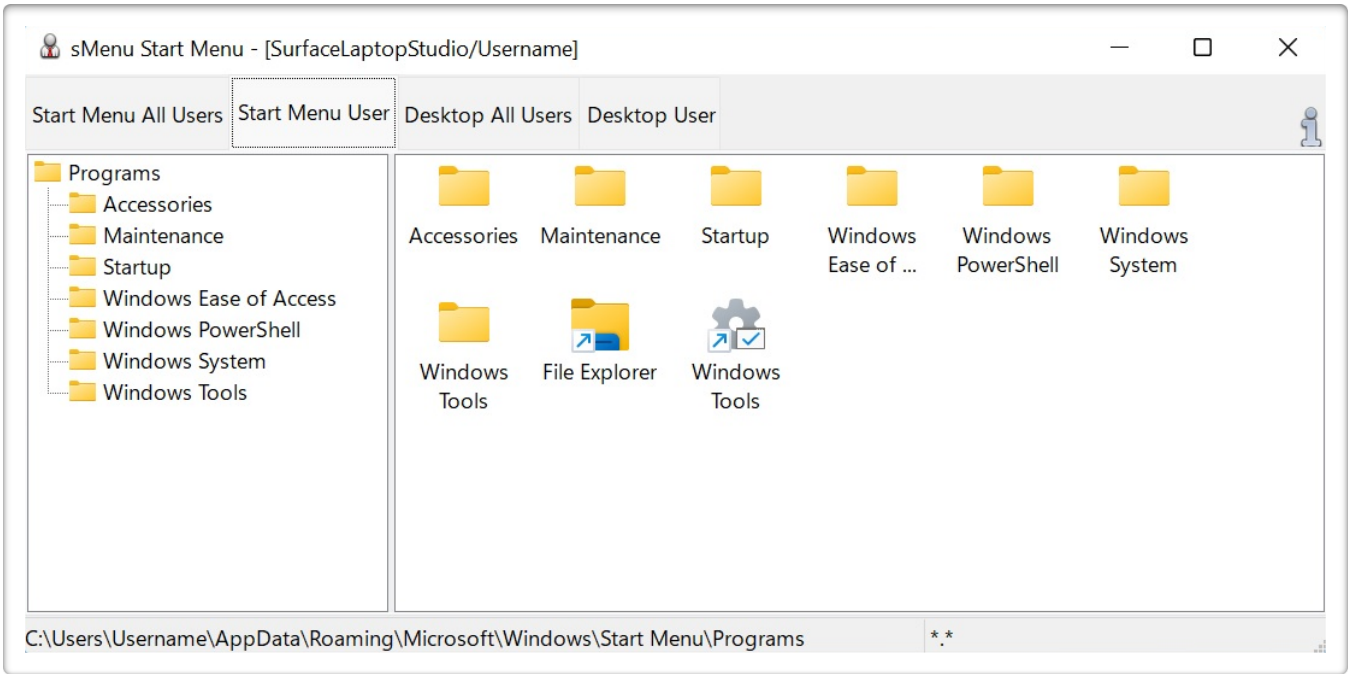
Example: sCopy.exe "c:\source" "c:\dest" "*.txt"

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 not go higher than the folder specified in the command-line. Selecting a file in the left pane and clicking on the Copy button will copy the file, and 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” are visible, along with any folders inside of the specified folder.

sMenu Start Menu



sMenu Start Menu is an included utility to provide access to file shortcuts that correspond to the file shortcuts found in the Start Menu and the Desktop.

sMenu Start Menu does not need command-line parameters.

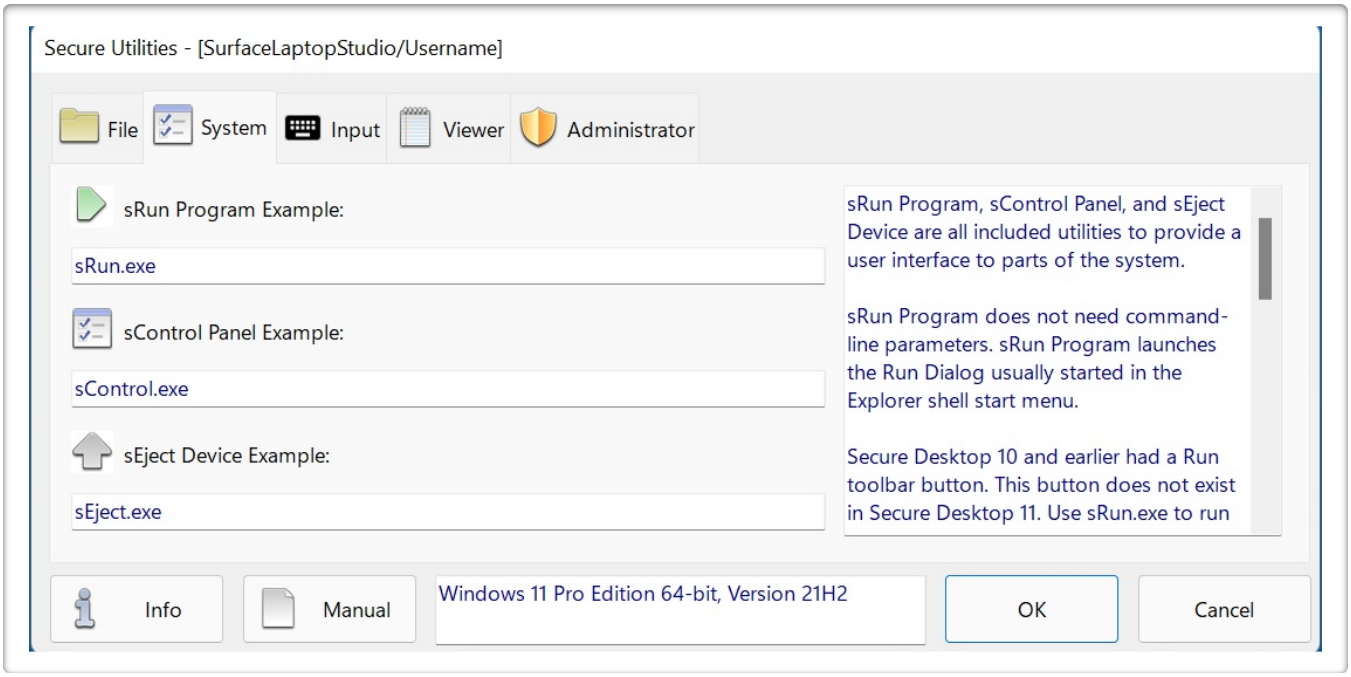
1st parameter (optional): /CLOSE will immediately close sMenu Start Menu after launching an icon.

sMenu Start Menu displays the files (file shortcuts) for the Start Menu, 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 normally availablle to the currently logged in user with the Explorer shell.

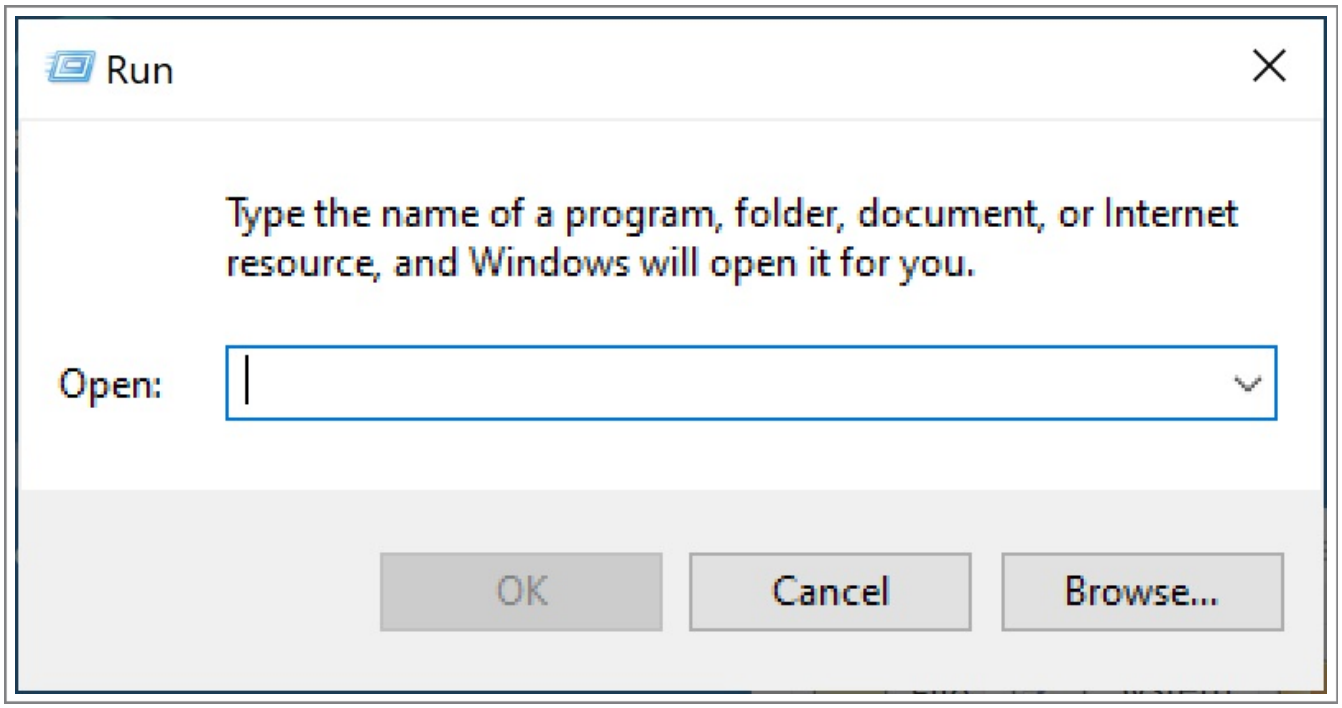
Secure Utilities installation will install a 32-bit or 64-bit version of sMenu as required by the 32-bit or 64-bit version of Windows.

Secure Utilities | System tab



sRun Program, sControl Panel, and sEject Device are all included utilities to provide a user interface to parts of the system.

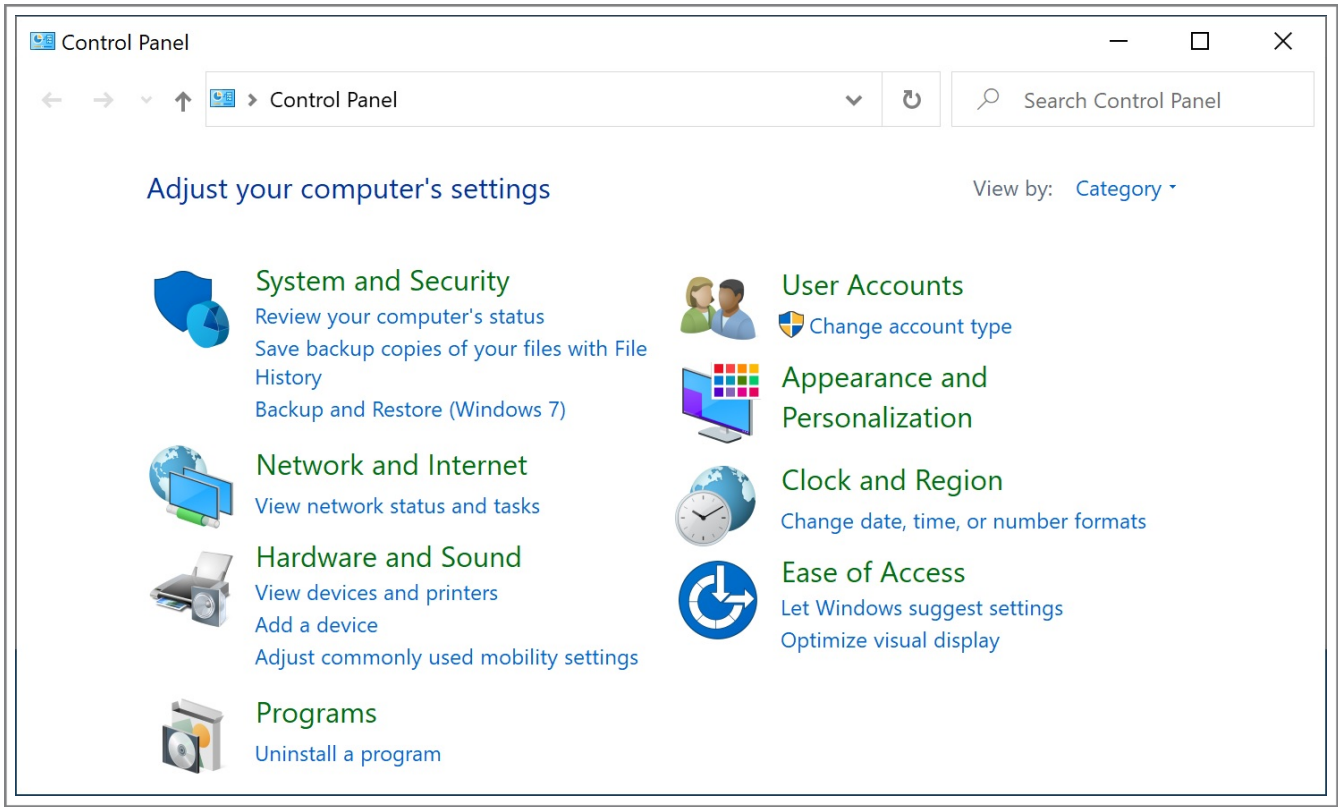
sRun Program



sRun Program does not need command-line parameters. sRun Program launches the Run Dialog usually started in the Explorer shell start menu.

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

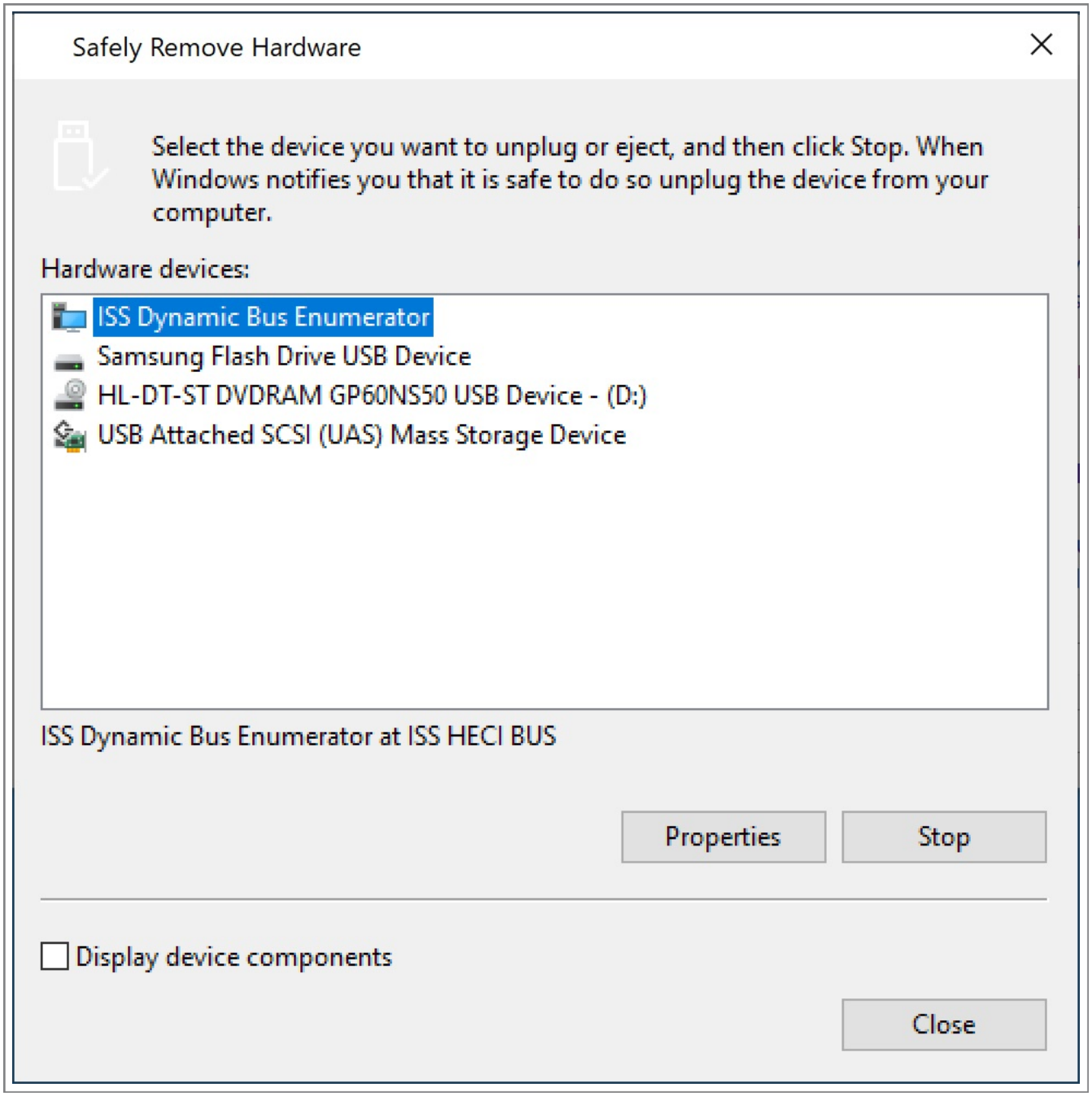
sControl Panel



sControl Panel does not need command-line parameters. sControl Panel launches the Windows Control Panel usually started in the Explorer shell start menu.

Secure Desktop 10 and earlier had a Control Panel toolbar button. This button does not exist in Secure Desktop 11. Use sControl.exe to launch the control panel as an icon in Secure Desktop 11. 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.

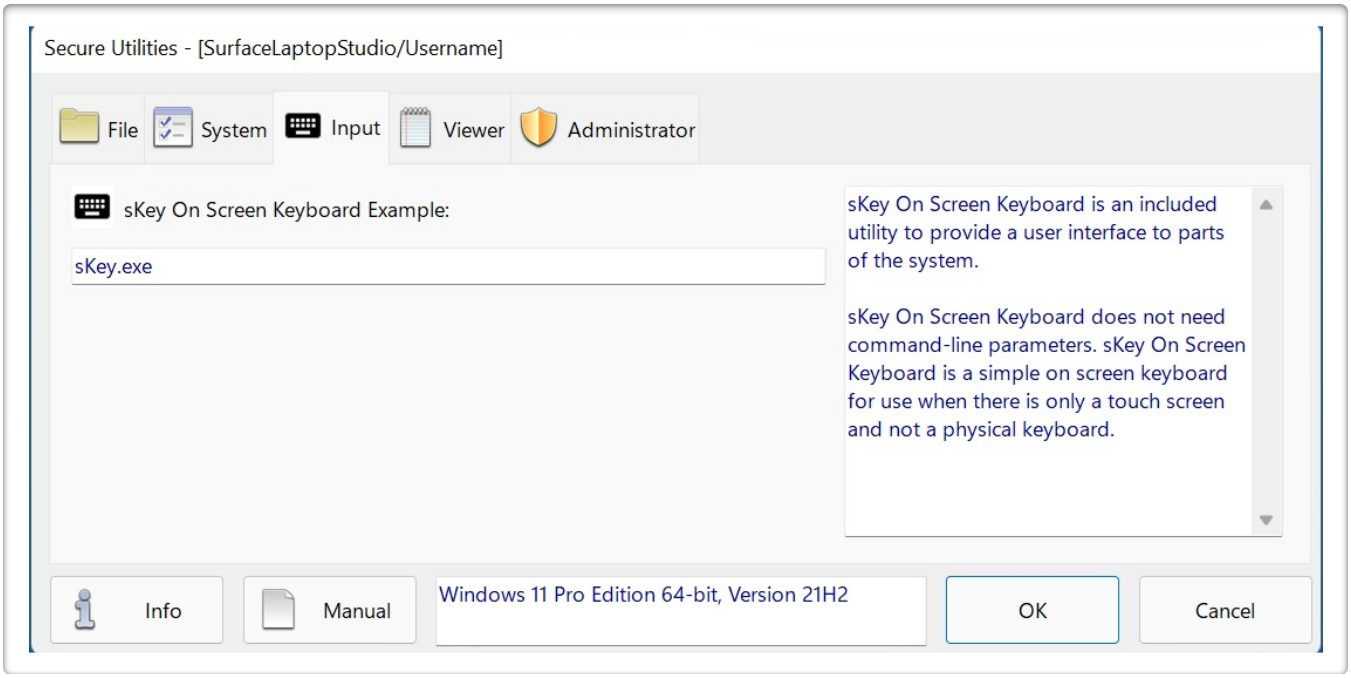
sEject Device



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

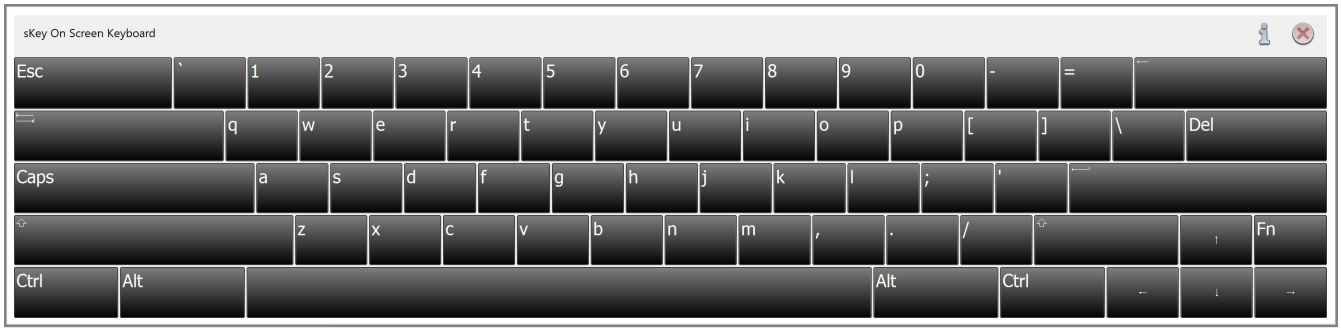
Secure Desktop 10 and earlier had an Eject Device toolbar button. This button does not exist in Secure Desktop 11. Use sEject.exe to launch the Safely Remove Hardware dialog as an icon in Secure Desktop 11.

Secure Utilities | Input tab

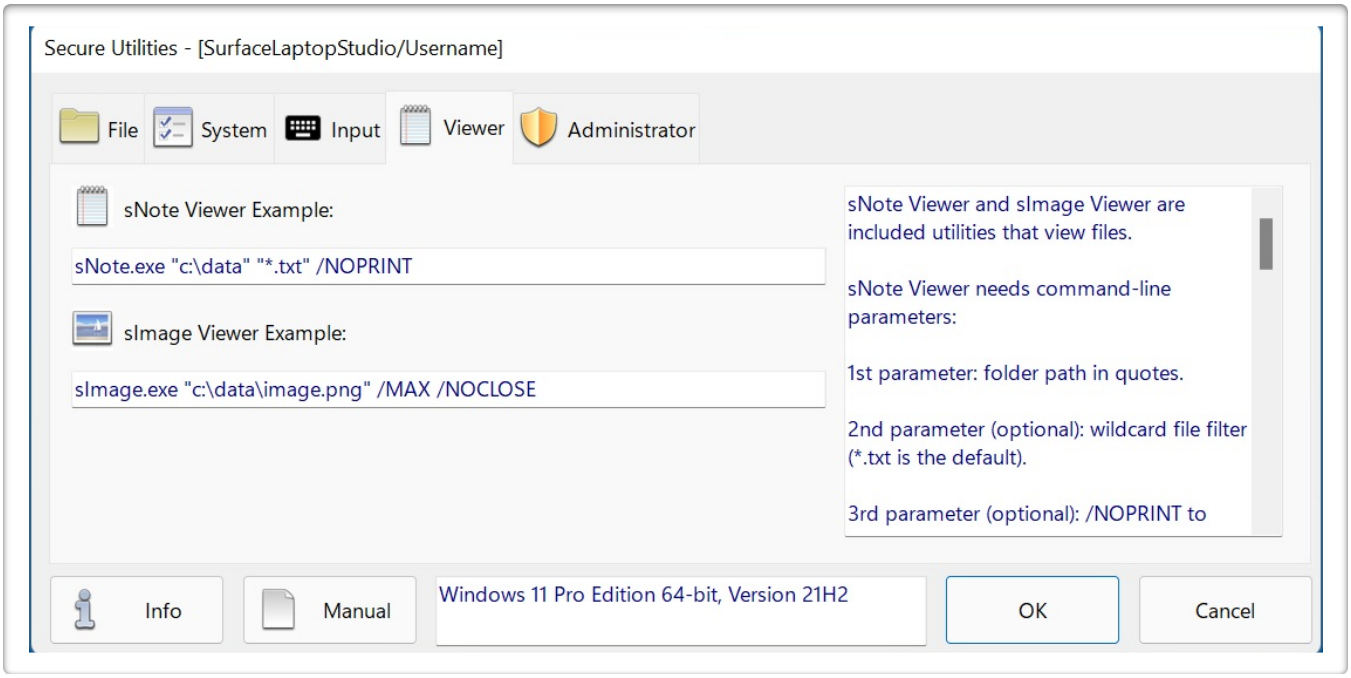


sKey On Screen Keyboard is an included utility to provide a user interface to parts of the system.

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



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

sNote Viewer

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 not go higher than 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” are visible, along with any folders inside of the specified folder. 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 name of the printer 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.

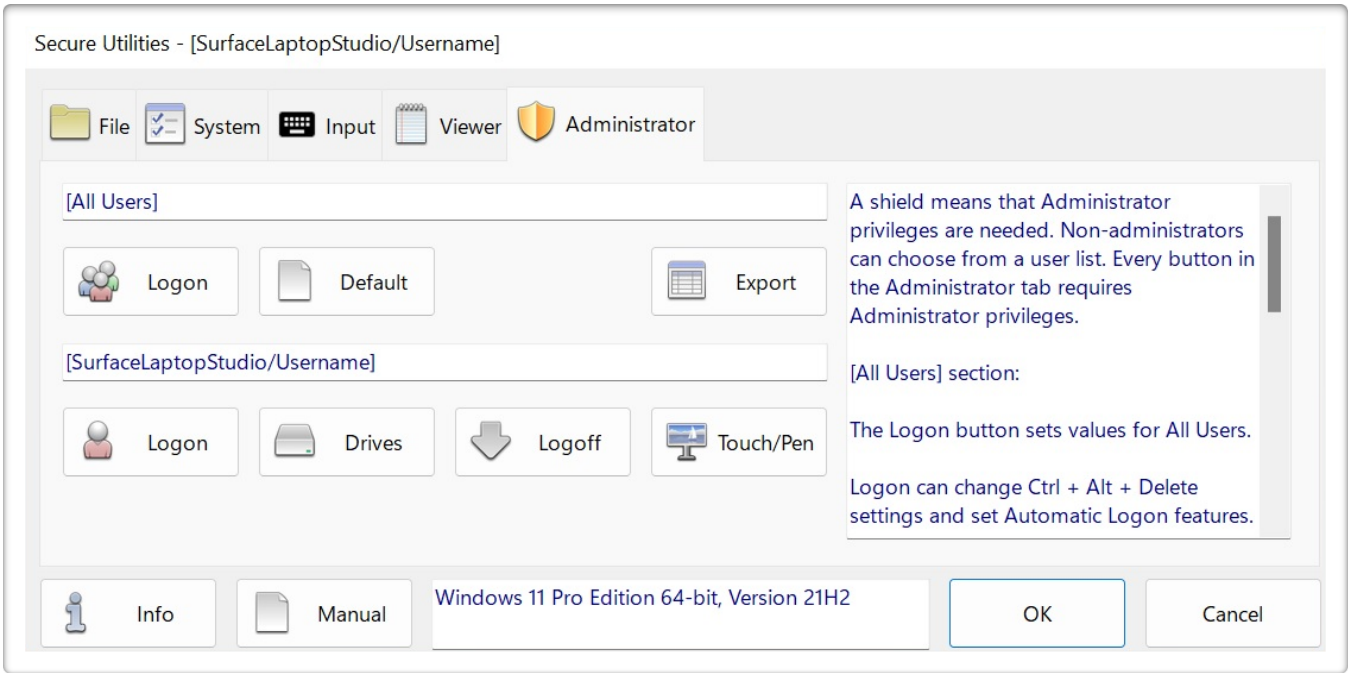
2nd parameter (optional): /MAX makes the image window open maximized.

3rd parameter (optional): /NOCLOSE disables the close button to prevent exiting the application.

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

The file path is displayed in the status bar.

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.

Default sets a registry value to remove a dialog to choose the default program to use for a file type.

The Export button displays automatically exported registry setting information.

[Computer/User Name] section:

The Logon, Drives, and Logoff buttons apply to the user logged in.

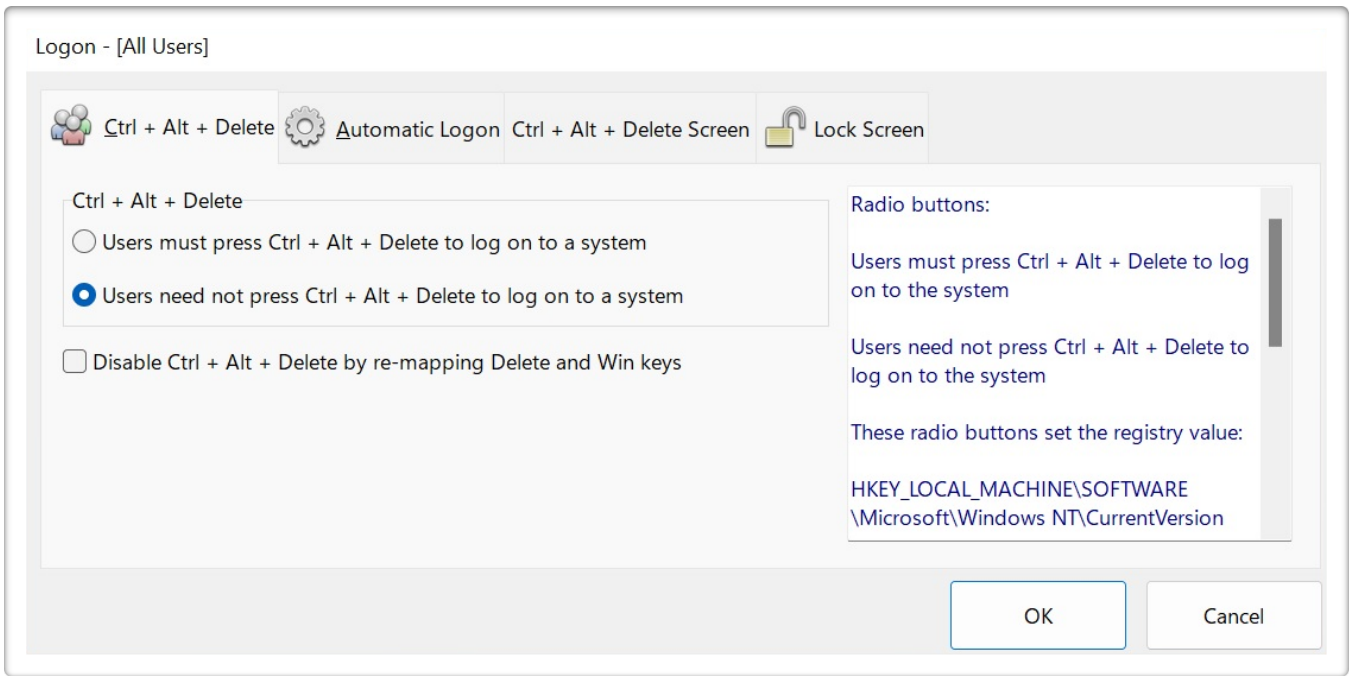
Logon will set restrictions in the Ctrl-Alt-Delete dialog.

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.

Touch/Pen provides a way to 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



Radio buttons:

Users must press Ctrl-Alt-Delete to log on to the system

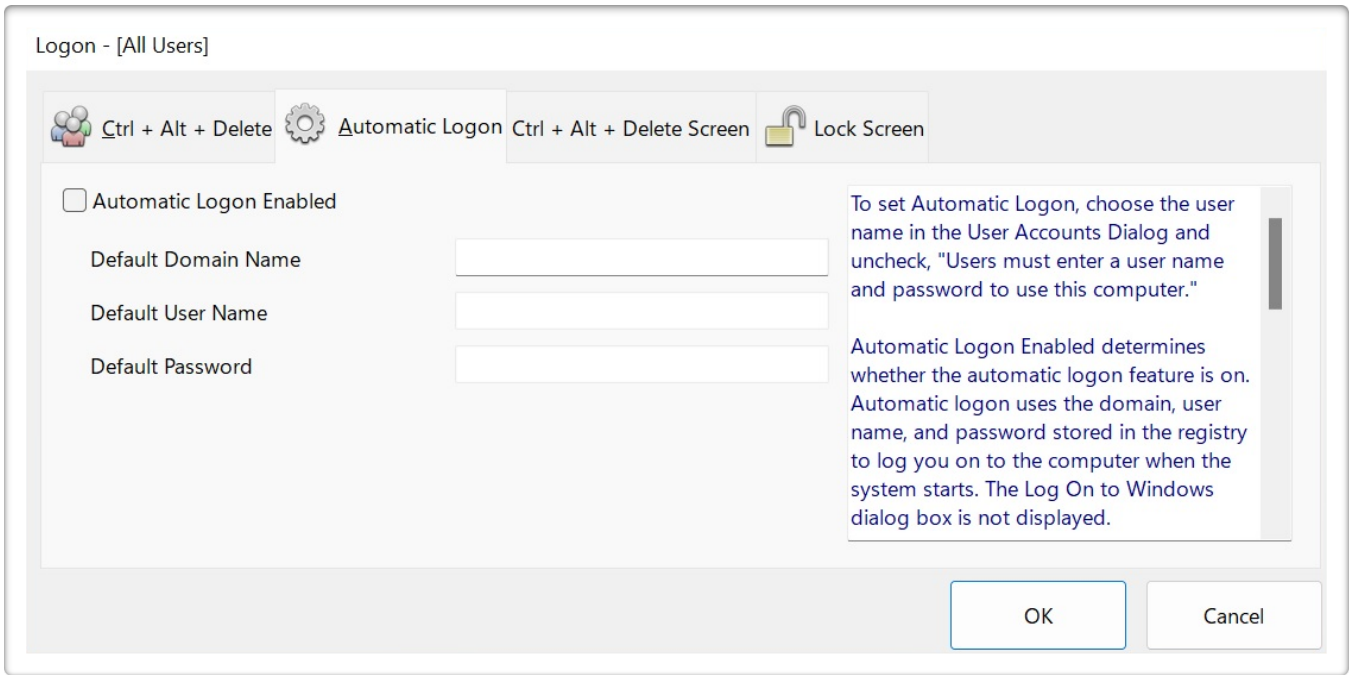
Users need not press Ctrl-Alt-Delete to log on to the system.

These radio buttons set the registry value:

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

This registry value is 0 for "must press" and set to 1 for "need not press".

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.

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

CAUTION:

Automatic logon allows other users to start your computer and log on using your account. Because 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:

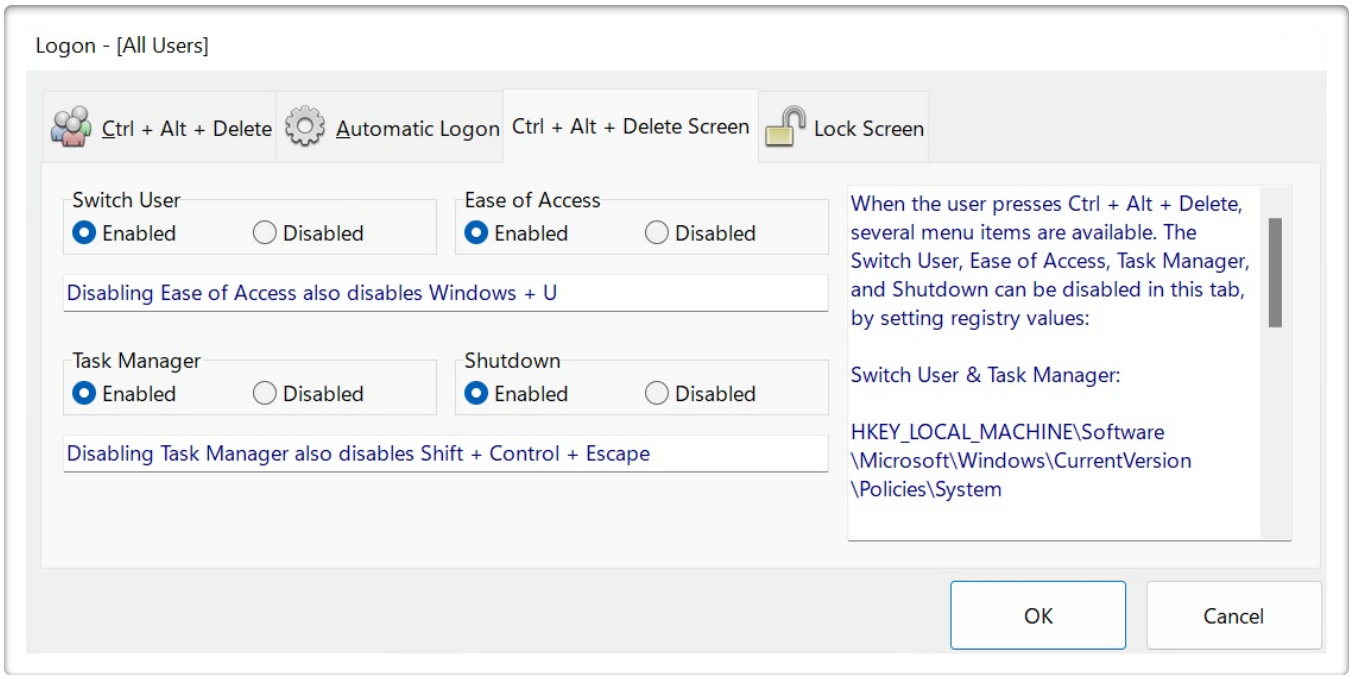
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

AutoAdminLogon

DefaultDomainName

DefaultUserName

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



When the user presses Ctrl-Alt-Delete, several menu items are available. The Switch User, Ease of Access, Task Manager, and Shutdown can be disabled in this tab, by setting registry values:

Switch User & Task Manager:

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

HideFastUserSwitching

DisableTaskMgr

Shutdown:

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

NoClose

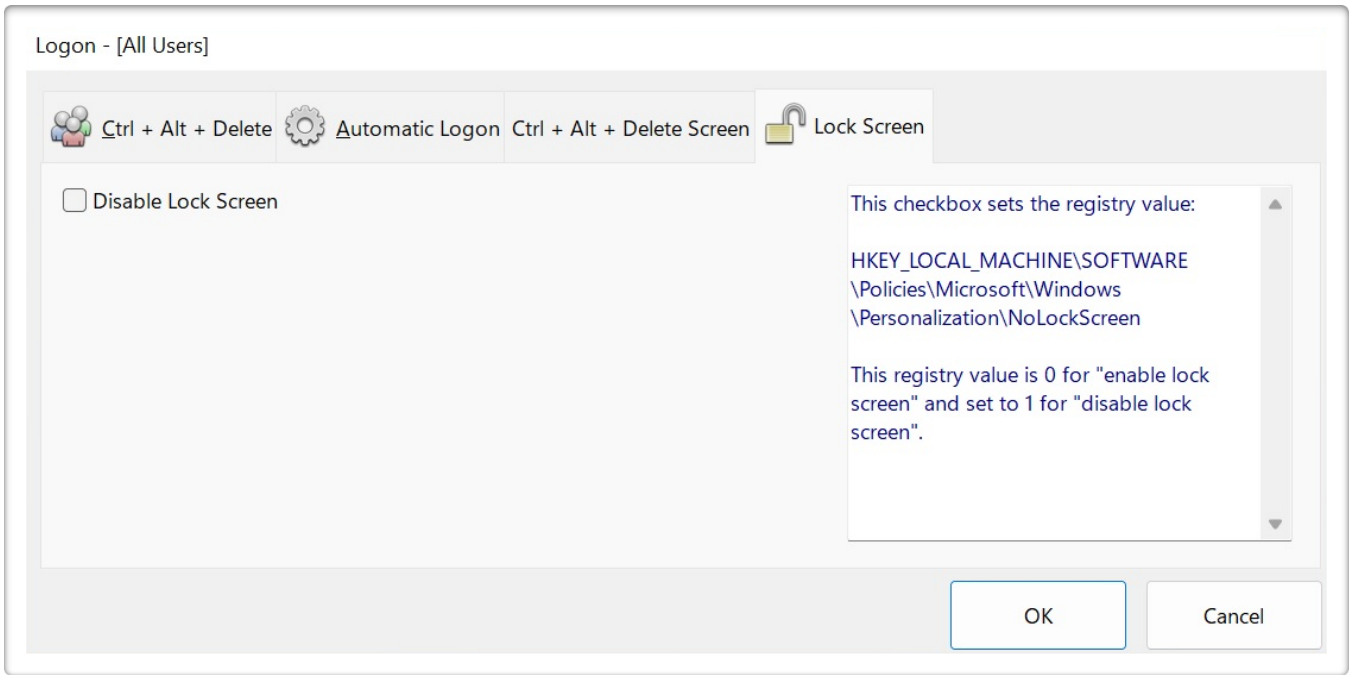
Ease of Access:

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

debugger

We use the file sUtilman.exe for this registry setting.

Secure Utilities | Administrator tab | [All Users] section | Logon button | Lock Screen tab

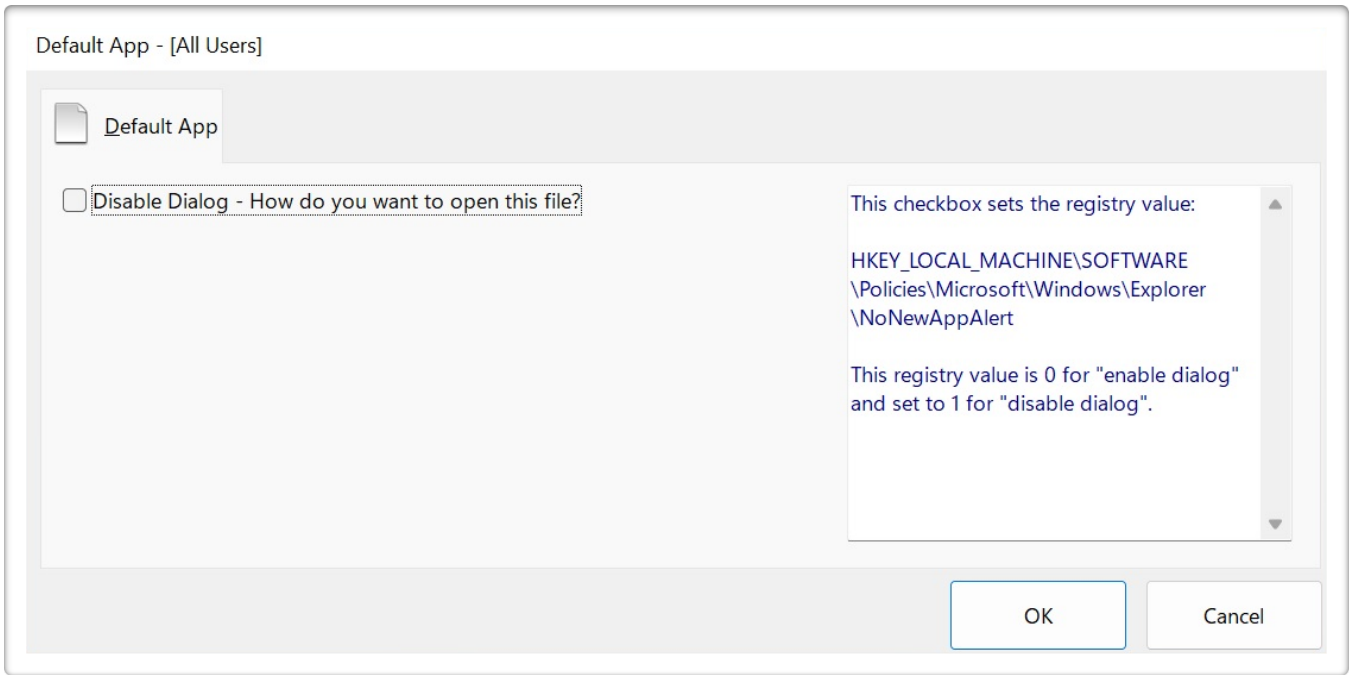


This checkbox sets the registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization\NoLockScreen

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

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



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

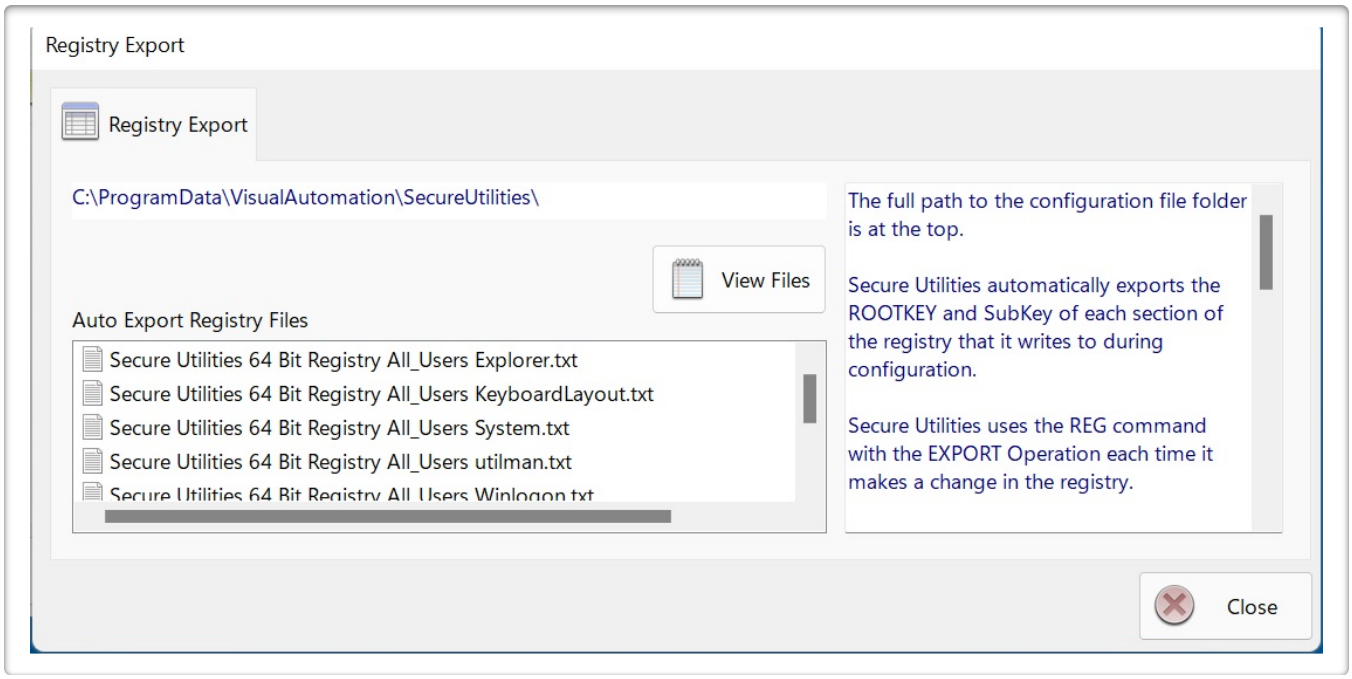
This registry setting disables this behavior.

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 | 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 section of the registry that it writes to during configuration.

Secure Utilities uses the REG command with the EXPORT Operation each time it makes a change in the registry.

The Secure Utilities Registry*.txt file name contains either the HostName.DomainName_UserName for HKEY_CURRENT_USER registry settings or All_Users for HKEY_LOCAL_MACHINE settings.

Secure Utilities creates the Secure Utilities Registry*.txt files primarily for documentation purposes.

However, 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 actually a merge of data.

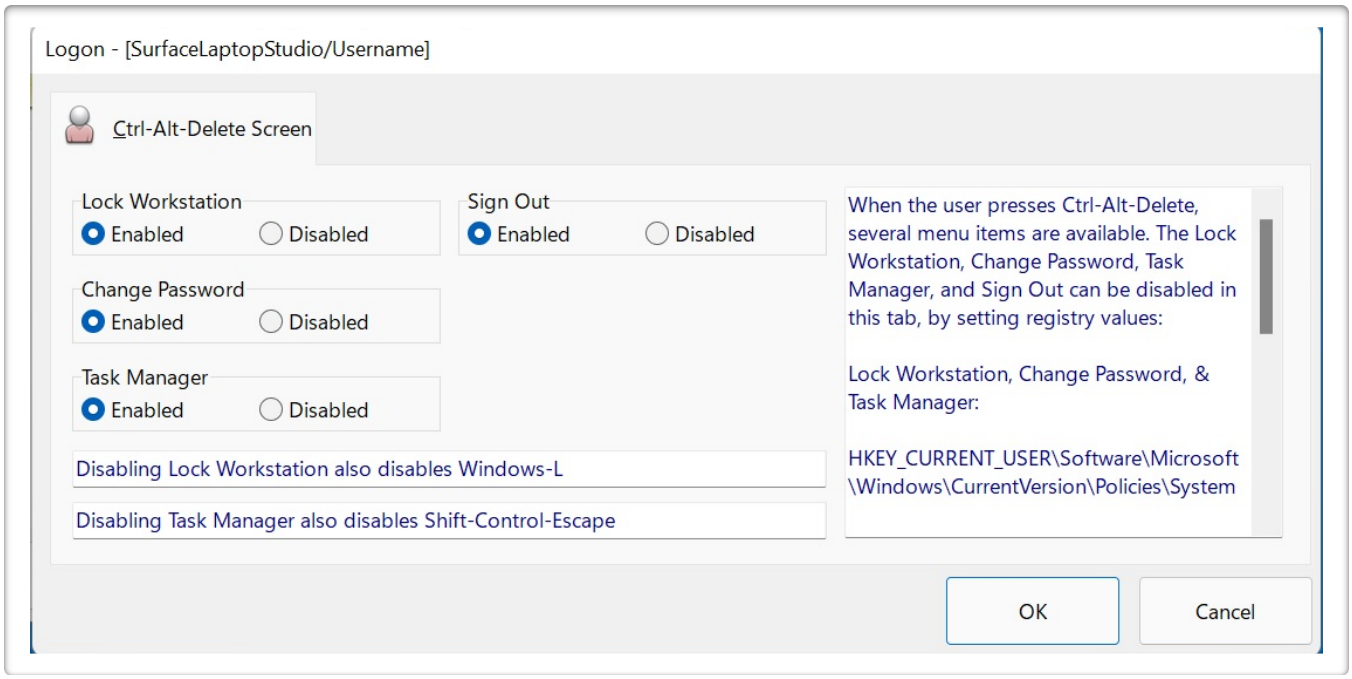
REG IMPORT may be useful for the configuration of other users or other identical computers, but we do not recommend this.

Some of the registry settings have corresponding Windows API calls or file renaming to achieve their purpose.

The View Files button will launch the sNote.exe program to view the exported Registry text files.

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



When the user presses Ctrl-Alt-Delete, several menu items are available. The Lock Workstation, Change Password, Task Manager, and Sign Out can be disabled 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

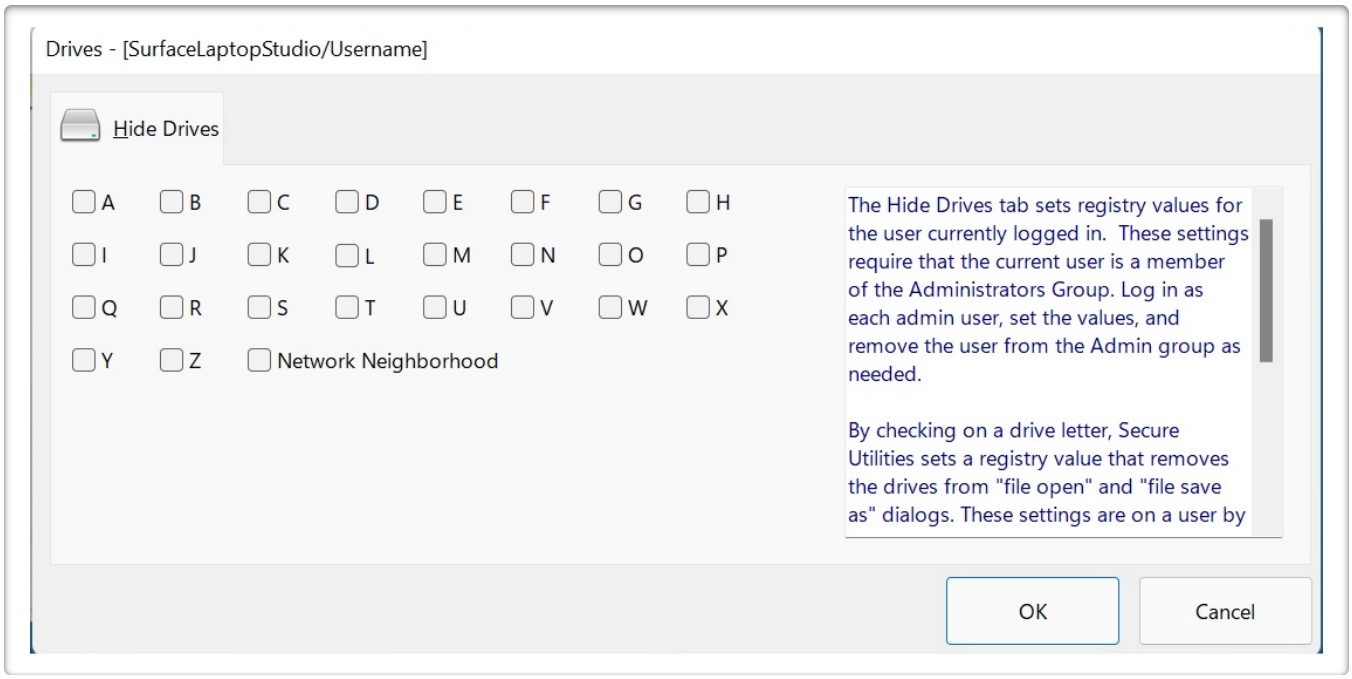
Sign Out:

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

NoLogoff

Windows shutdown can not be disabled 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.

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

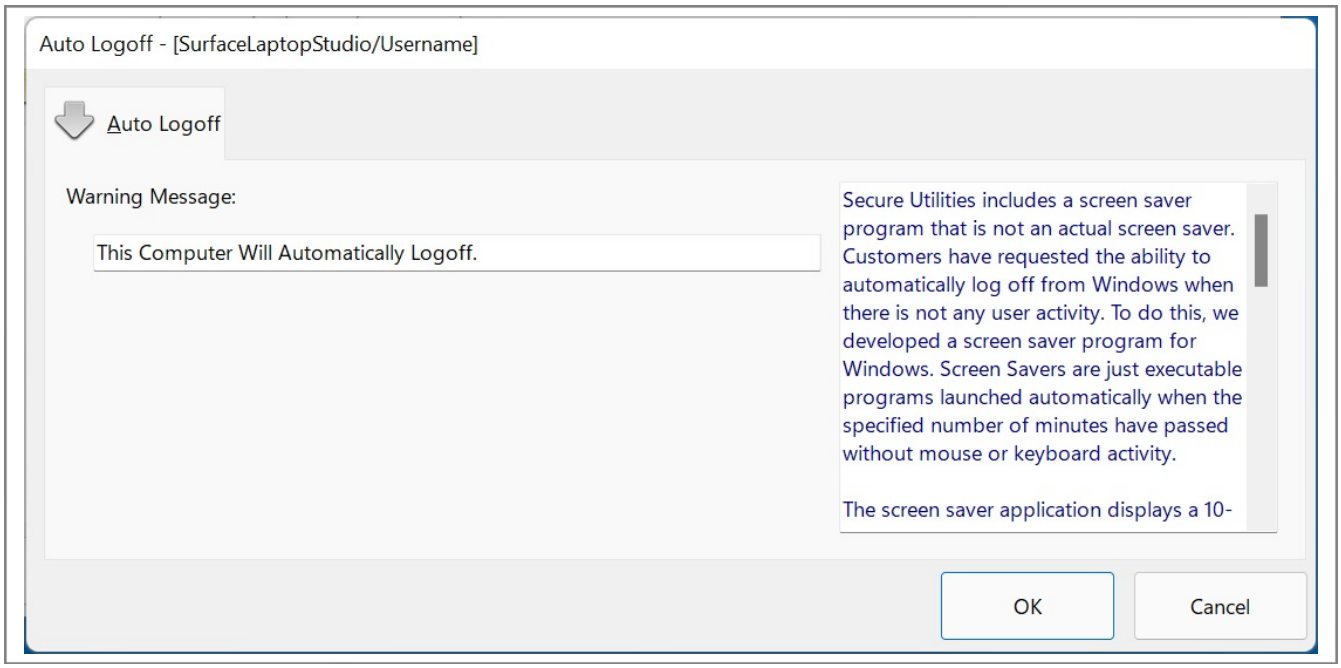
The registry set is:

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

NODRIVES

NoNetHood

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



Secure Utilities includes a screen saver program that is not an actual screen saver. Customers have requested the ability to automatically logoff from Windows when there is not any user activity. To do this, we developed a screen saver program for Windows. Screen Savers are just 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 count down dialog with a cancel button; then, it will perform a forced logoff. Any unsaved work within an editor (Notepad, Word, Excel, etc.) is lost. Note that any services that you may be running will continue to run after a log off operation. The screen saver application doe 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 logoff of the computer.

There are no settings for the screen saver other than the Warning Message and the number of minutes before starting after 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:

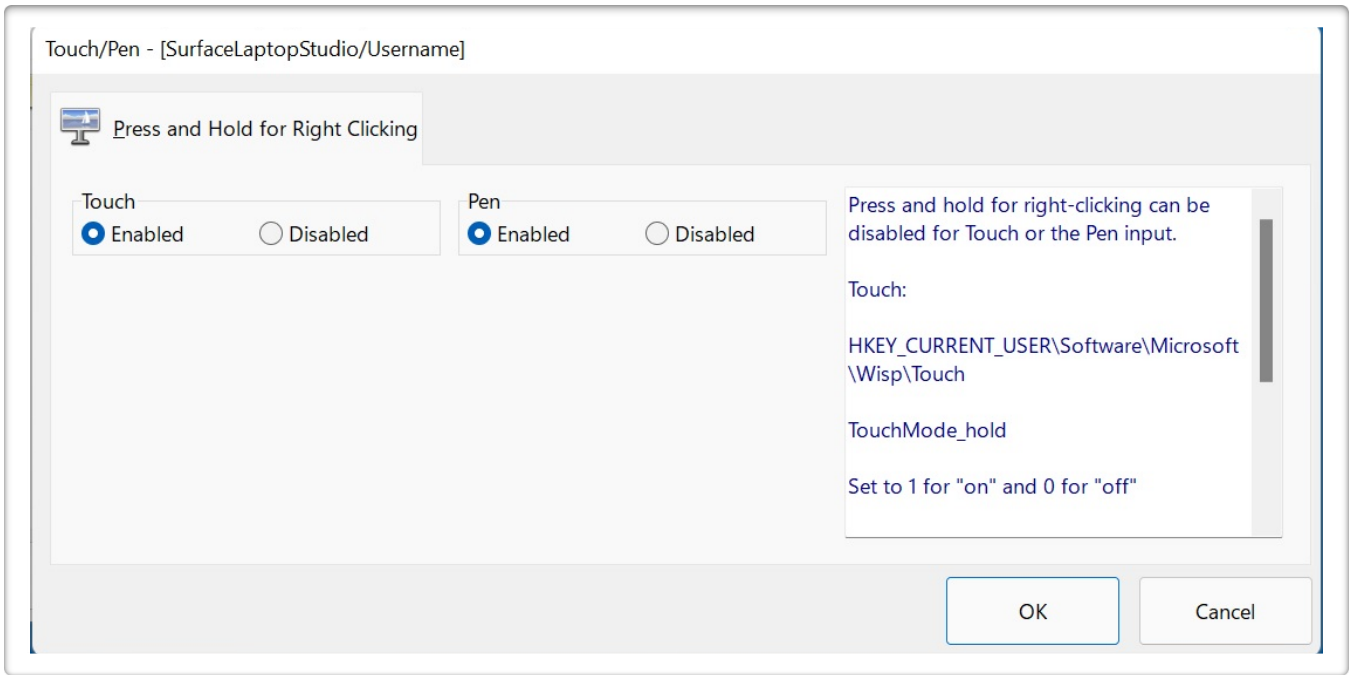
HKEY_CURRENT_USER\Software\Visual Automation\Secure Utilities\Auto Logoff

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"

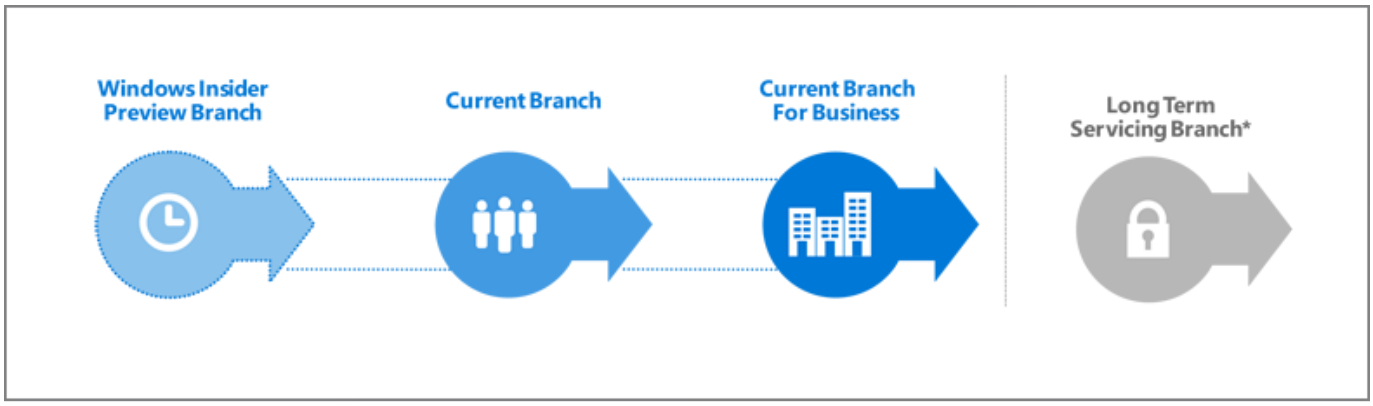
Windows Registry

If you need to modify Secure Utilities 11 registry settings manually, you will need to run RegEdit.exe.

USE CAUTION: This is a database containing essential information about how your Windows system operates; modifying the wrong parameter could lead to unintended results.

Secure Utilities 11 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 up to date. With this in mind, quality updates are still immediately available to Windows 10 Enterprise LTSB clients, but 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 web site that can appear to the user like a traditional application.

The Windows Explorer shell and the Secure Desktop shell both provide the ability to 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, Chrome, Firefox, and Opera. Other Win32 browsers will run “as is” or could be controlled slightly using the Windows Wizard.

Secure Desktop can not launch UWP browsers such as 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 will be retired and go out of support on June 15th, 2022.

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 10 is 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 what Edition of Windows 10 or Windows 11 you choose, Secure Desktop can not run UWP or PWA apps. Based on our research, we believe 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 not compatible with Windows 10S, Windows 10 in S Mode, Windows 11S or Windows 11 in S Mode. Secure Desktop 11 will work on Windows 10 on ARM in emulation mode, but Secure Desktop 10 will not. Secure Desktop 11 has not been specifically tested on Windows 11 on ARM at the time of this writing, but we believe it is fully compatible in 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. Now, Windows 10 Pro and Enterprise may be installed on the Surface Hub 2. Please read more from Microsoft here: techcommunity.microsoft.com

Secure Desktop 10, Secure Desktop 11, Secure Utilities 11 and ColdKey 10 should all work in the environment of Windows 10 Pro and Enterprise on Surface Hub 2. Secure Desktop 11 and Secure Utilities 11 should work in the environment of Windows 11 Pro and Enterprise on Surface Hub 2. We have not tested in these environments, but we believe that Secure Desktop is 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

As we grow, we plan to expand our service based on feedback from you. 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

http://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. To find the serial number, click on the info button or consult your e-mail message.

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.

Exact wording of any error messages and screenshots.