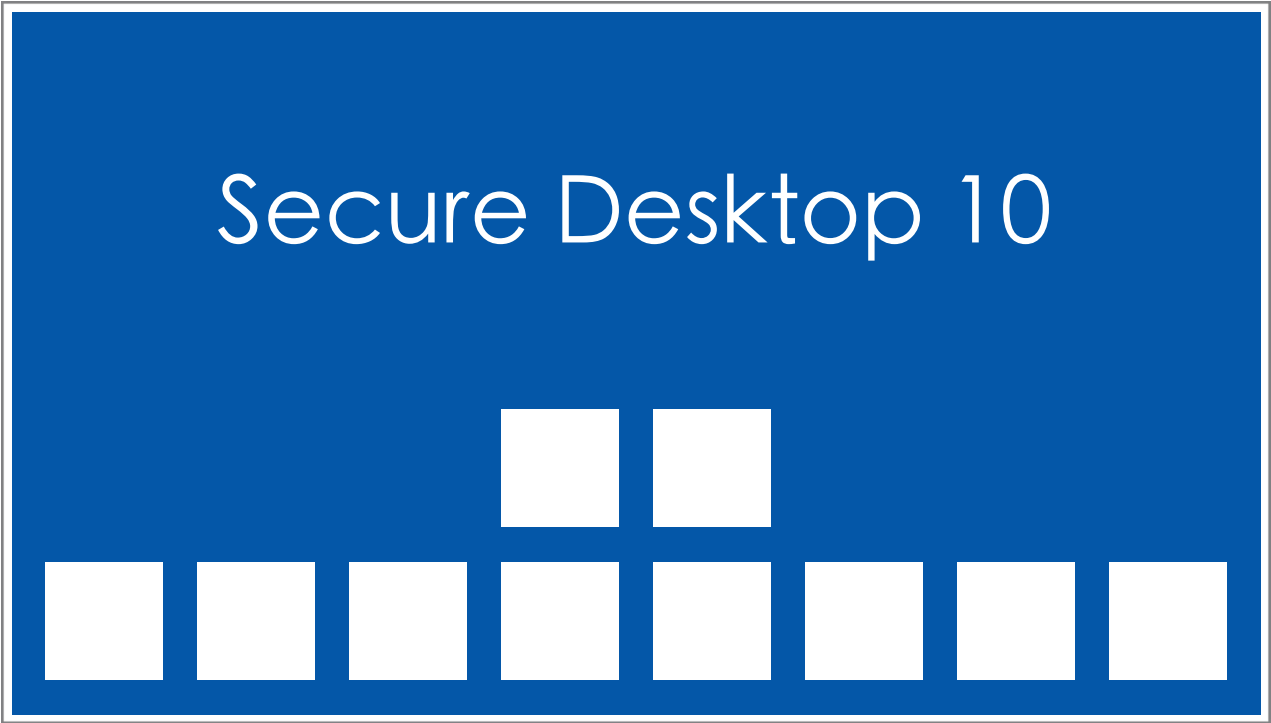


VISUAL AUTOMATION



VISUAL AUTOMATION

Product Manual

Secure Desktop

Version 10

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.

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.

© Visual Automation, Inc. 1994-2024 All Rights Reserved.

Last Updated January, 2024



TABLE OF CONTENTS

Comparison of version 6.85 versus Secure Desktop 10	6
Secure Desktop - An Introduction and description of included files and modules	7
Secure Desktop Tools – Secure Desktop Tab	11
Secure Desktop Tools – Windows Shell Tab	12
Secure Desktop Tools – Safe Mode Tab	13
Secure Desktop Tools – USB Tab	14
Secure Desktop Tools – Administrator Tab	16
Secure Desktop Shell	18
The 10 Minute Setup	19
Secure Desktop Icon Setup	23
Secure Desktop Icon - Import Button	24
Secure Desktop Icon - Icon Button	27
Secure Desktop Icon - Startup Tab	28
Secure Desktop Icon - Timed Tab	29
Secure Desktop Icon - Shutdown Tab	30
Secure Desktop Options – Password Tab	31
Secure Desktop Options – Icon Tab	33
Secure Desktop Options – Audit Tab	35
Secure Desktop Options – Key..Mouse Tab	36
Secure Desktop Options – F1..F12 Tab	39
Secure Desktop Options – A..Z 0..9 Tab	41
Secure Desktop Options – Key State Tab	43
Secure Desktop Options – Startup Tab	44

TABLE OF CONTENTS (CONTINUED)

Secure Desktop Options – Shutdown Tab	45
Secure Desktop Window Wizard – Step 1	46
Secure Desktop Window Wizard – Step 2	47
Secure Desktop Window Wizard – Step 3	48
Secure Desktop Window Wizard – Step 4	49
Secure Desktop Window Wizard – Step 5 – Manipulate a Window	50
Secure Desktop Window Wizard – Step 5 – Close a Program during Shutdown	52
Manage Users – Manage Users Tab	53
Manage Users – Edit User Tab	54
Manage Users – Edit User Tab – Edit UserName	55
Manage Users – Backup Tab	56
Manage Users – Restore Tab	57
Manage Users – Registry Tab	58
Setting - Setting Tab	60
Setting - Console Tab	61
Setting - File Explorer Tab	62
Setting - Task Manager Tab	63
Setting - Mobility Center Tab	64
Setting - Internet Explorer Tab	65
Dialog - File Open/Save As Tab	66
Dialog - Print Tab	68
Dialog - Run Tab	69
Dialog - Internet Options Tab	70

TABLE OF CONTENTS (CONTINUED)

Dialog - File Properties Tab	71
Dialog - Popup Menu Tab	72
Administrator - All Users - Supervisor - Supervisor Mode Tab	73
Administrator - All Users - Supervisor – When Logged In Tab	74
Administrator - All Users - Supervisor – Calculation Passwords Tab	75
Administrator - All Users - Files	77
Administrator - All Users - Logon - Ctrl-Alt-Delete Tab	78
Administrator - All Users - Logon – Automatic Logon Tab	79
Administrator - All Users - Logon – Ctrl-Alt-Delete Screen Tab	81
Administrator - User - Drives – Hide Drives Tab	81
Administrator - User - Logon – Ctrl-Alt-Delete Screen Tab	82
Administrator - User - Logon – Auto Logoff Tab	83
Administrator - User - Internet Explorer – Privacy Tab	84
Administrator - User - Internet Explorer – Behavior Tab	85
Administrator - User - Internet Explorer – Downloads Tab	86
Administrator - User - Internet Explorer – Approved Sites Tab	87
Secure Desktop's Configuration sdesktop.xml File	88
Windows Registry	88
Windows 10 Editions	89
Control Panel Tips	91
Explorer Tips	92

TABLE OF CONTENTS (CONTINUED)

File Open and File Save As Dialog Tips	93
Commenting on Visual Automation Products and Services	94
Technical Support Options	94

Secure Desktop 6.85 versus 10

Secure Desktop 7 represented the single biggest re-design, largely due to native support of Windows 7. It was necessary to change how we store the Secure Desktop configuration data, how registry modifications are made, and even how Secure Desktop help works. Because we had to make these necessary changes, we took the opportunity to re-design the user interface, re-name product files, change how Secure Desktop launches programs, and even drop features that are no longer relevant.

We are very excited about Secure Desktop 10. It's easier to use, better looking and the best user experience yet.

However, if you are an existing customer moving from version 6 or earlier of Secure Desktop to version 10, we strongly advise that you completely re-test your use of Secure Desktop. Secure Desktop 10 will automatically migrate your ini configuration files to the new sdesktop.xml file, making that part very easy. However, with so many changes, it's very important for you to re-test your configuration, especially in a mission-critical environment. Secure Desktop 7, Secure Desktop 8 and Secure Desktop 10 use the exact same sdesktop.xml file for configuration data.

Secure Desktop 10 is a 32-bit application, but is also 64-bit aware. Secure Desktop 10 has been tested in Windows XP, Windows Server 2003, Windows 7, Windows Server 2008, Windows 8.0, Windows 8.1, Windows Server 2012, Windows Server 2016 and Windows 10. Secure Desktop 10 is not designed or tested for Windows Server 2022 or Windows 11. Secure Desktop 10 was tested on Microsoft Surface Pro computers. If you are using Windows 10 in a mission-critical setting, please consider using the Windows 10 Enterprise LTSC Edition. Secure Desktop 10 is not in the Windows Store and therefore will not run in Windows 10 S. Windows 10 S may easily be upgraded to Windows 10 Pro.

Secure Desktop - An Introduction

A guide to Secure Desktop and an illustration of main concepts

Why Windows needs additional security

Microsoft Windows is designed for a typical desktop environment, with one person using their computer. What if a computer is used by several people in an open environment that anyone has access to? What if you want the computer user to have access to only certain programs? This is the security that Secure Desktop provides. Windows is a rather 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. Secure Desktop provides this capability.

In Program Files or Program Files (x86) Folder:



Secure Desktop Shell

Secure Desktop provides many applications for the desktop environment. In Secure Desktop 6, the Secure Desktop Shell was referred to as Secure Desktop (vaprgman.exe). The Secure Desktop Shell file name is now sDesktop.exe with accompanying dll named sDesktop.dll.



Secure Desktop Tools

The Secure Desktop Tools application provides the configuration interface for the Secure Desktop Shell and registry settings. In Secure Desktop 6 this was called Secure Setup (secure.exe). The Secure Desktop Tools file name is now sTools.exe found in the Program Files Folder. There is a companion executable named sAdmin.exe, which should not be called individually (it's called from sTools.exe and sDesktop.exe as needed).



Secure Desktop Manual

This is the file you are browsing right now, named sManual.pdf.



Secure Desktop Audit Viewer

This program is a viewer for the sAudit XML files that Secure Desktop logs. In Secure Desktop 6 this file was called sLog.exe. The Secure Desktop Audit Viewer is now named sAudit.exe.



Secure Desktop Control Panel

This program shows all of the control panel applets. You can also pass a command line switch of /p to only show Printer Control Panel program. The Secure Desktop Control Panel is named sControl.exe.

Secure Desktop Version Information

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



Secure Desktop Wallpaper

Turn on the wallpaper feature and set the jpg, jpeg, png or bmp file to use at Secure Desktop Tools | Secure Desktop tab | Options button | Startup tab. This program is named sWall.exe. sWall.png file is also installed, as the default wallpaper.



Secure Desktop File Explorer

Launch sExplore.exe with the first command-line parameter of the folder path you would like to display, in quotes. For example:

```
sExplore.exe "C:\Users\User Name\Documents"
```

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 that is specified in the command-line. Double-clicking or hitting enter on a document or executable file will launch that program. There is no right mouse support, or any other file editing functions.

An optional second command-line parameter is a wildcard file filter. For example:

```
sExplore.exe "C:\Users\User Name\Documents" "*.doc"
```

In the example above, only document files ending in "doc" would be displayed, along with any folders inside of the specified folder. sExplore.exe is found in the Program Files folder where Secure Desktop 10 was installed.

An optional third command-line parameter is "/p". This add a Print button to the sExplore window. When the user has one or more document files selected, and clicks Print, the documents will be printed to the Default printer via the registered applications associated with the document files.



Secure Desktop Note File Viewer

Launch sNote.exe with the first command-line parameter of the folder path you would like to display, in quotes. For example:

sNote.exe "C:\Users\User Name\Documents"

The files and folders in the path specified in the command-line parameter will be displayed 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 that is specified in the command-line. Selecting a text file will display the text from that text file in the right pane. By default, only *.txt files will be displayed. There is no right mouse support, or any other file editing functions.

An optional second command-line parameter is a wildcard file filter. For example:

sNote.exe "C:\Users\User Name\Documents" "*.bat"

In the example above, only document files ending in "bat" would be displayed, along with any folders inside of the specified folder. sNote.exe is found in the Program Files folder where Secure Desktop 10 was installed.

An optional third command-line parameter is /NOPRINT to remove the print button.

The print button by default prints to the Default printer. This is actually accomplished by using the system Notepad.exe application with appropriate command line parameters to print 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, this is accomplished by using the system Notepad.exe application with appropriate command line parameters to print the text file to the designated printer name.



Secure Desktop Copy Utility

Launch sCopy.exe with the first command-line parameter of the source folder path you would like to display, in quotes, the second command-line parameter of the destination folder path you would like to display, in quotes, and the third parameter as a wildcard file filter. For example:

```
sCopy.exe "C:\Source" "C:\Dest" "*.csv"
```

The files and folders in the source and destination paths specified in the command-line parameters will be displayed 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 that is specified in the command-line. Selecting a file in the left pane and clicking on the Copy button will copy the file and it will be immediately displayed in the right pane for verification. There is no right mouse support, or any other file editing functions.

In the example above, only document files ending in "csv" would be displayed, along with any folders inside of the specified folder. sCopy.exe is found in the Program Files folder where Secure Desktop 10 was installed.

In System32 Folder

If in Windows XP, SASGINA.DLL is there to disable Ctrl-Alt-Delete. sCmd.exe disables the Safe-Mode command line. sDesktop.rat is used to create a white list of web sites for Internet Explorer.

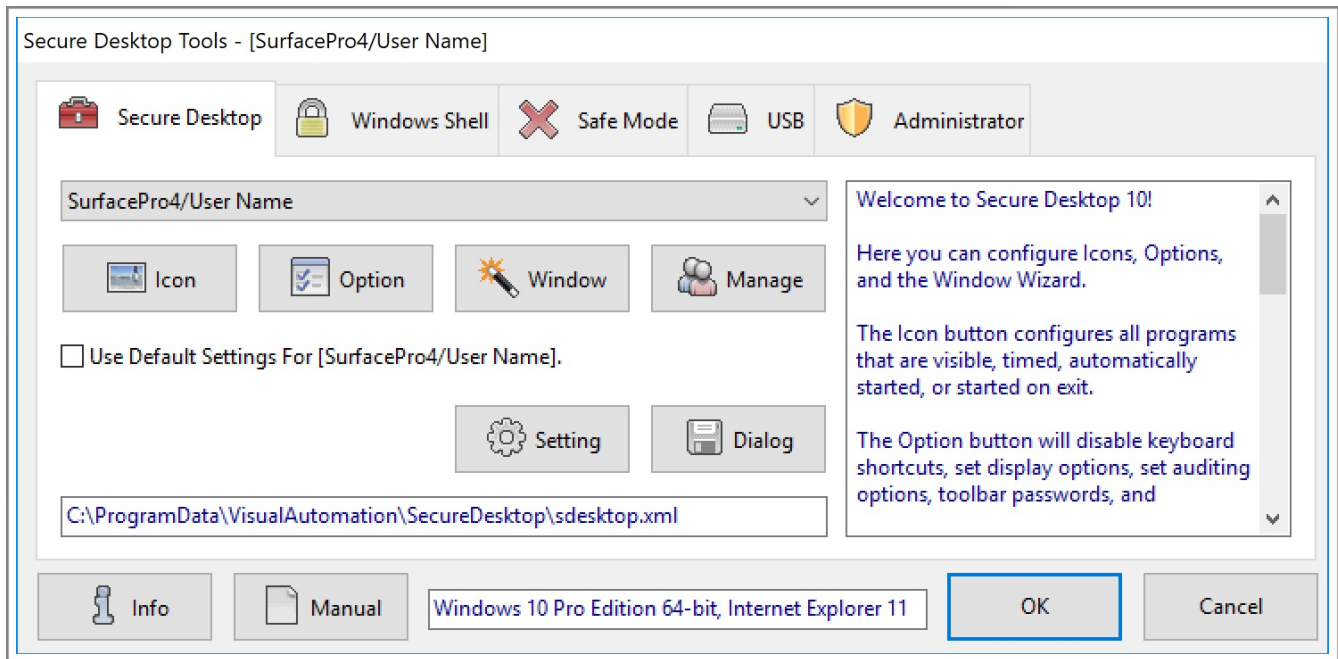
sLogoff.scr is a screen saver that forces a log off. sUtilMan.exe disables the Utility Manager (utilman.exe).

New Setup Program

Secure Desktop 10 now uses Inno Setup for it's installation software, rather than Wise. The setup exe file is now signed and the files are smaller.



Secure Desktop Tools – Secure Desktop Tab



Welcome to Secure Desktop 10!

Here you can configure Icons, Options, and the Window Wizard.

The Icon button configures all programs that are visible, timed, automatically started, or started on exit.

The Option button will disable keyboard shortcuts, set display options, set auditing options, toolbar passwords, and startup/shutdown options.

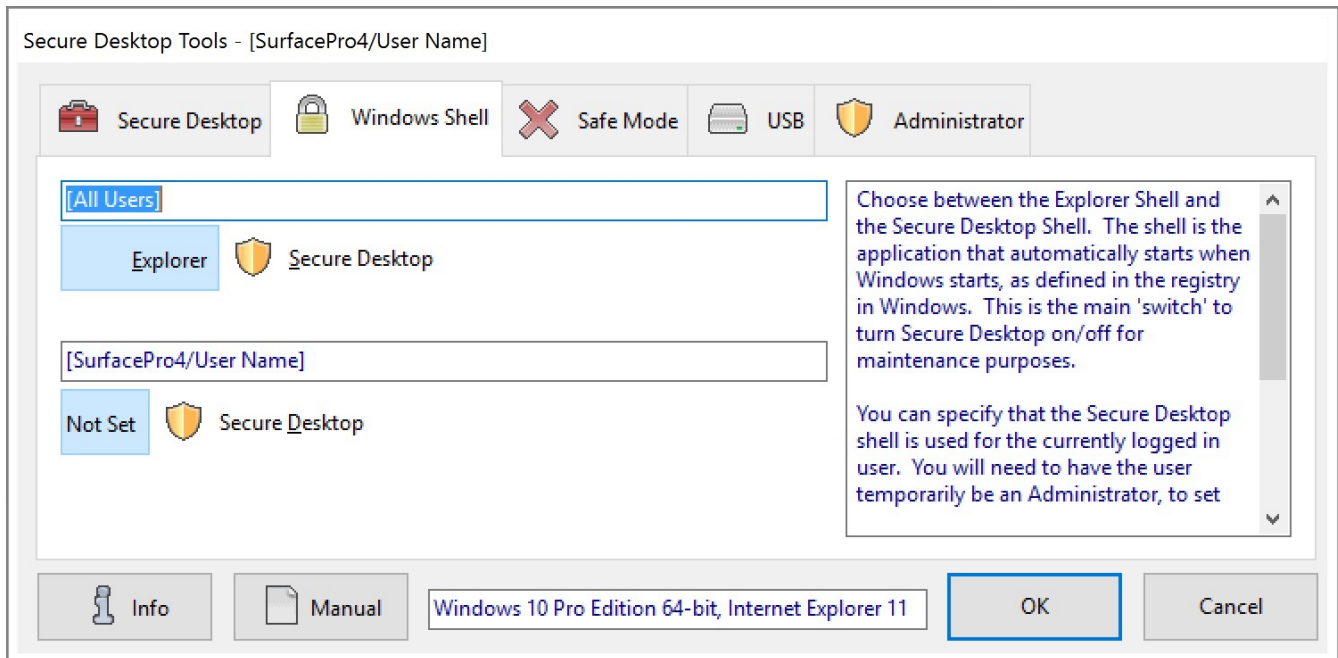
The Window button takes you to the Window Wizard and provides a way to act on other programs in the system, manipulating their windows.

Manage provides an easy way to copy settings from one user to another, edit user information, backup/restore the configuration XML file and examine the Registry export files.

Use Default Settings For This User - In the User List, you see one setting for "Default". Each User can have their own settings, or you can choose to use the Default settings for a user. If a user does not have settings, then the Default settings are used. The Setting button provides a method to immediately close many setting-related editing apps, should they be opened by any application. The Dialog button provides a method to immediately close dialogs such as File Open, File Save As, Print, Run and Internet Options.



Secure Desktop Tools – Windows Shell Tab



Choose between the Explorer Shell and the Secure Desktop Shell. The shell is the application that automatically starts when Windows starts, as defined in the registry in Windows. This is the main 'switch' to turn Secure Desktop on/off for maintenance purposes.

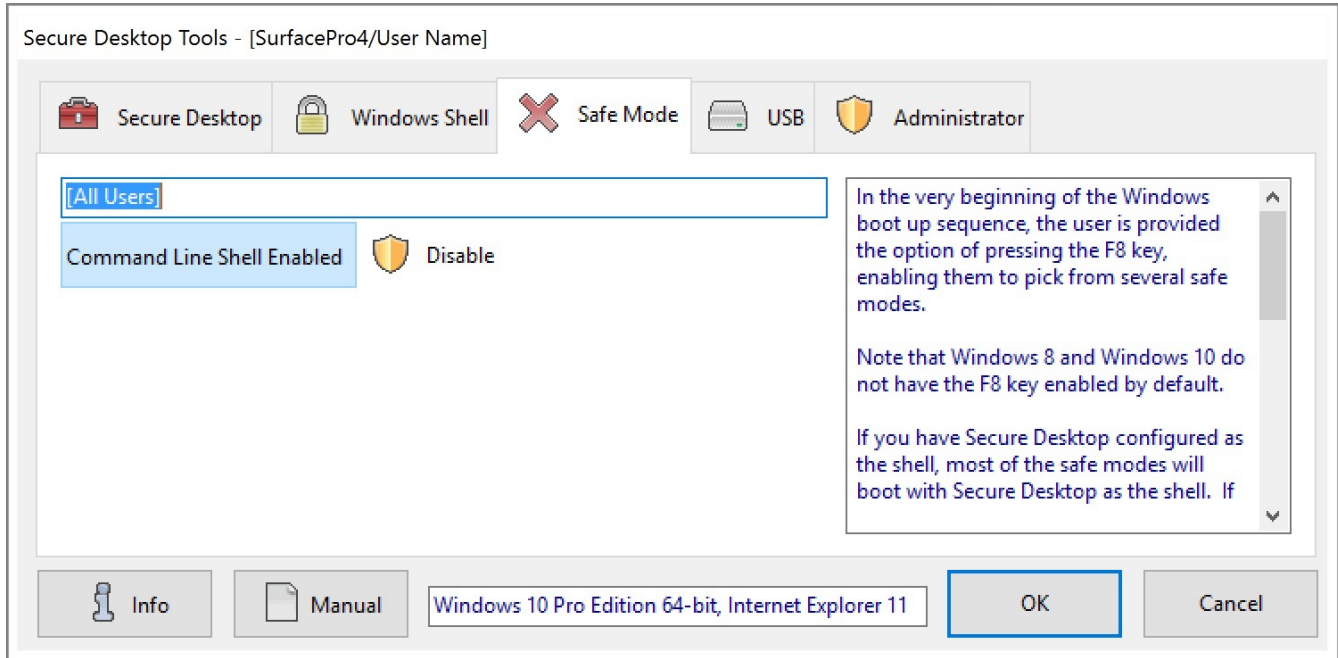
You can specify that the Secure Desktop shell is used for the currently logged in user. You will need to have the user temporarily be an Administrator, to set this registry value. Starting with version 10.99.10, if you're using Windows 10, a different registry value is set that does not require Admin rights for the user. Explorer would be the shell for all other users without this registry setting.



A shield means that Administrator privileges are needed. If you are not logged in as an Administrator, you can choose from a user list.



Secure Desktop Tools – Safe Mode Tab



In the very beginning of the Windows boot up sequence, the user is provided the option of pressing the F8 key, enabling them to pick from several safe modes.

If you have Secure Desktop configured as the shell, most of the safe modes will boot with Secure Desktop as the shell. If the user selects the Command Line Safe Mode, the shell is by default set to the Command Line interpreter.

To prevent this, disable using the button shown. If the user presses F8 and then selects the Command Line Safe Mode, they will get a gray screen telling them to press Ctrl-Alt-Delete to restart.

Note that Windows 8 and Windows 10 do not have the F8 key enabled by default. If F8 is not enabled, there is no need to disable the Command Line Shell.

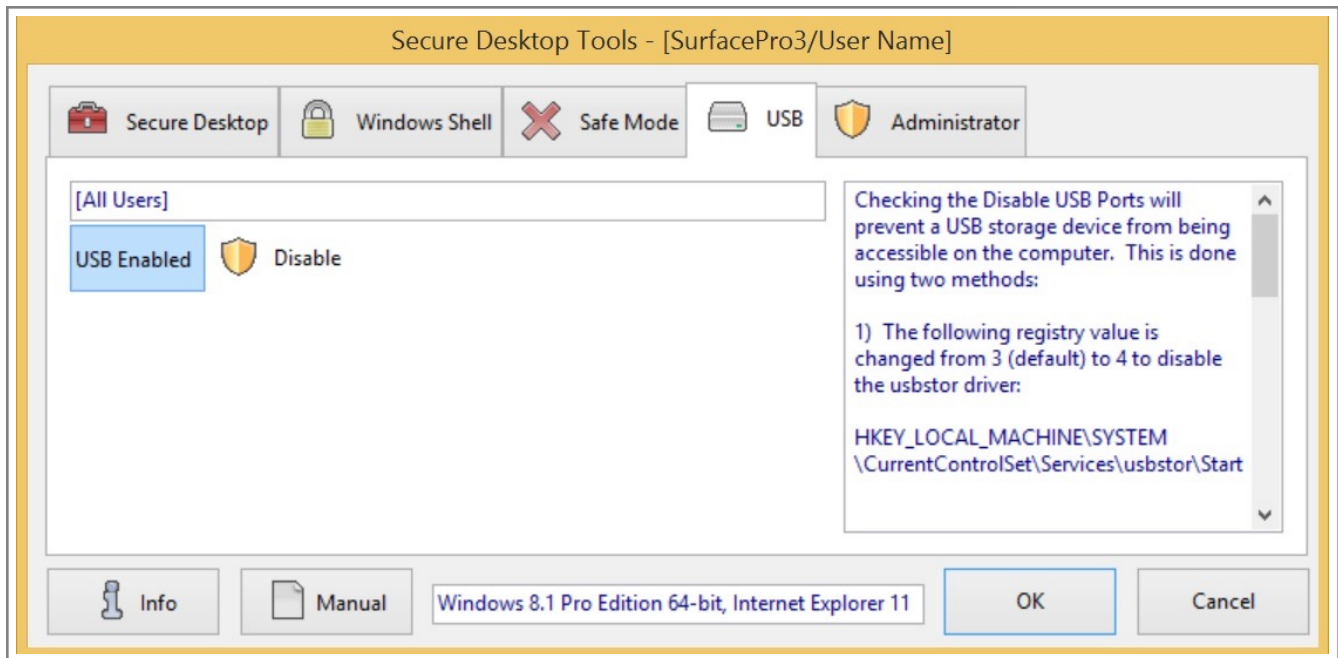
It is important to disable the Lock Workstation, Change Password, and Task Manager buttons in the Administrator tab, Logon button settings.



A shield means that Administrator privileges are needed. If you are not logged in as an Administrator, you can choose from a user list.



Secure Desktop Tools – USB Tab



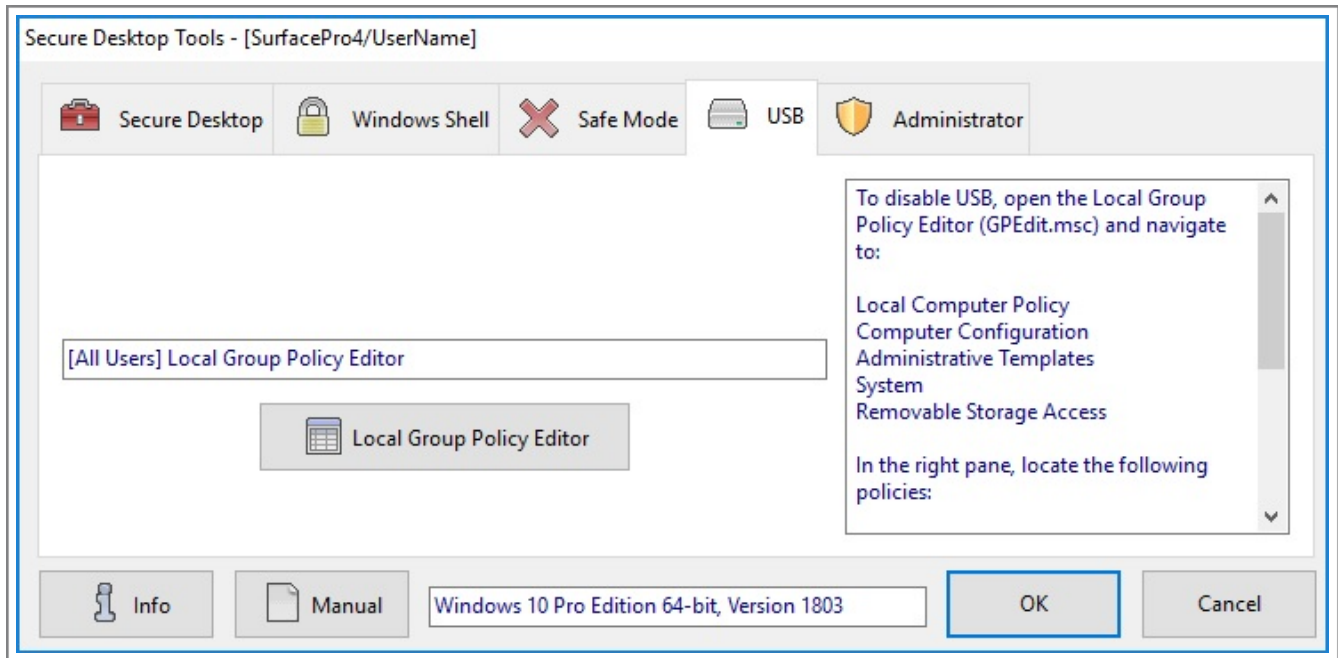
Checking the Disable USB Ports will prevent a USB storage device from being accessible on the computer. This is done using two methods:

- 1) The following registry value is changed from 3 (default) to 4 to disable the usbstor driver: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\usbstor\Start
- 2) In Windows\Inf we are renaming 2 files, usbstor.inf and usbstor.PNF to usbstov.ini and usbstov.PNF, when this checkbox is checked, and renamed back when unchecked. If the USB driver has never been loaded, this should prevent the driver from being loaded the first time. If it did load, it would reset the registry value above to 3, rather than 4.

Because the CD-ROM and Floppy drives are volumes, by default, they are shared as an administrative share on the network. If checked, the drives are allocated to the user as part of the interactive logon process and, therefore, only the current user can access it. This prevents administrators and remote users (and even the same user at a different computer) from accessing the drives while the current user is logged on. The drive is shared again when the current user logs off.



A shield means that Administrator privileges are needed. If you are not logged in as an Administrator, you can choose from a user list.



The method we use on the previous page of the manual does not work in Windows 10. Use the following method for Windows 10 (and Windows 7 or 8 also):

To disable USB, open the Local Group Policy Editor (GPEdit.msc) and navigate to:

Local Computer Policy

Computer Configuration

Administrative Templates

System

Removable Storage Access

In the right pane, locate the following policies:

Removable Disks: Deny execute access

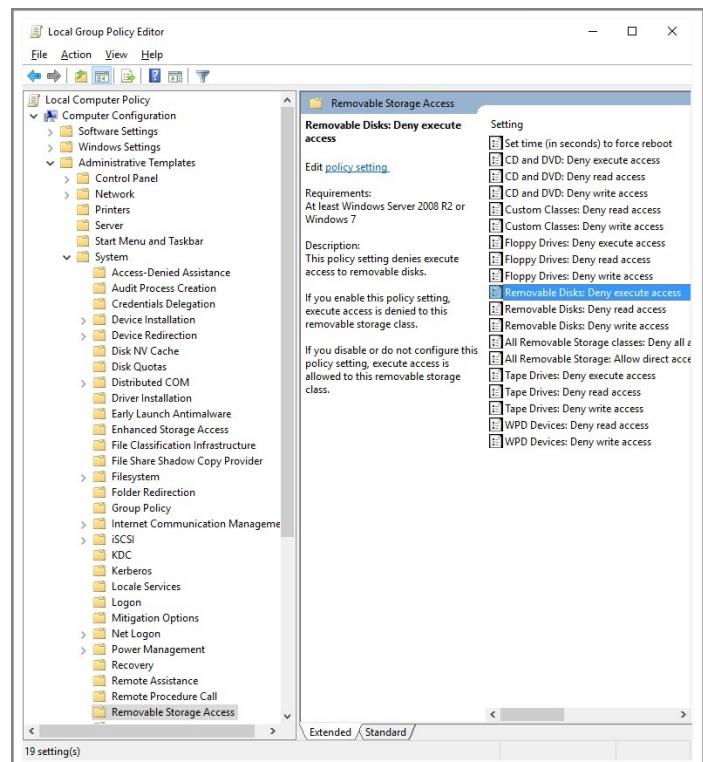
Removable Disks: Deny read access

Removable Disks: Deny write access

Set each of these policies to Enabled.

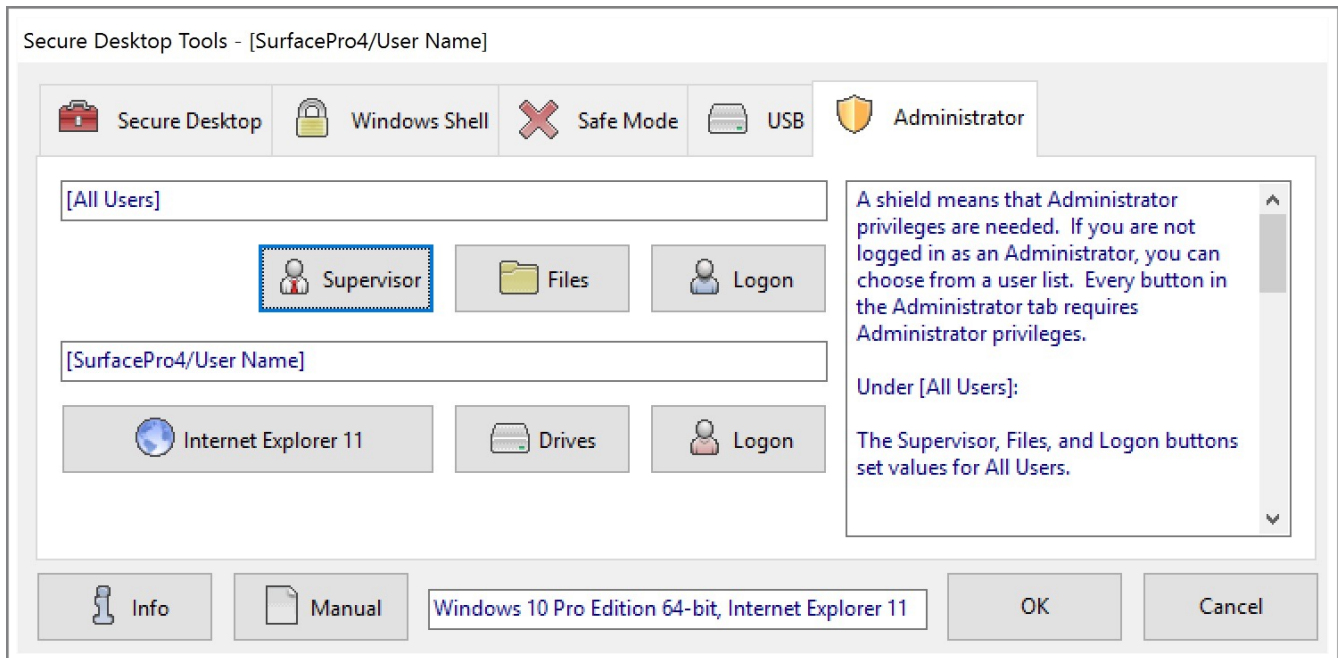
Restart the system for these policies to take effect.

Note: The Local Group Policy Editor is not available in Windows Home Edition.





Secure Desktop Tools – Administrator Tab



[All Users]

The Supervisor, Files, and Logon buttons set values for All Users.



Supervisor can turn on a supervisor toolbar button to temporarily un-lock the system, disabling passwords, re-enabling keyboard shortcuts, and setting calculation password features.



Files is simply a tool to set the hide and read-only attributes of a file or folder.



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

[HostName.DomainName/UserName]

The Internet Explorer, Drives and Logon buttons below apply to the user who is currently logged in.



Internet Explorer will set registry values for the currently logged in user to lock down Internet Explorer 11.



Drives will set registry values for the currently logged in user to hide drive letters.

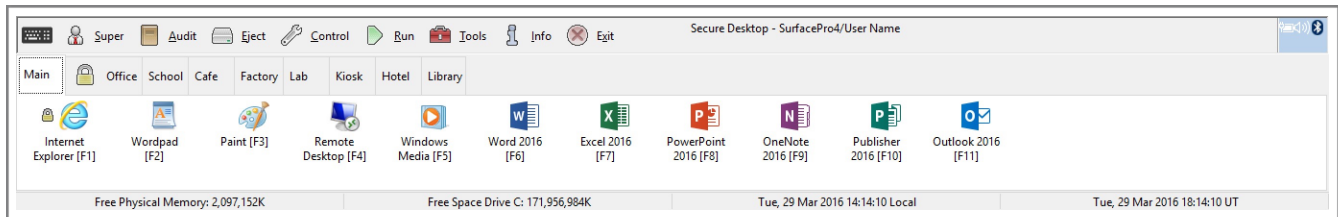


Logon will set restrictions in the Ctrl-Alt-Delete screen and provides help for the Auto Logoff Screen Saver.










Secure Desktop Shell

This is what a configured system looks like when the Windows system boots.



Toolbar Buttons

From left to right, these buttons are as follows; Keyboard,  Supervisor,  Audit Viewer,  Eject,  Control Panel,  Secure Desktop Tools,  Info, and  Exit. All toolbar buttons may be removed completely, except Info and Exit. All Toolbar buttons may be password protected, except for Keyboard and Info. Tooltip help is provided for each of these toolbar buttons.

Tab Definitions

You can define up to 10 different Icon tabs in the Secure Desktop Shell. Each tab has up to 12 visible icon applications. The Secure Desktop Shell also contains up to 18 startup applications, up to 12 timer applications, and up to 12 Shutdown applications. Startup, timer and shutdown applications are not visible to the user. Each tab, except for the main tab, may have a password associated with the user getting to that tab. The lock icon next to a tab name designates a password protected tab.

Icon Definition

Classic Windows applications are typically defined as EXE, COM, or BAT files. Shortcut files (*.LNK) can be imported, and document files can be started as well. A description can be typed in, indicating the name below the icon. A longer tooltip description can be typed in, which will be displayed as a tooltip when the icon is selected. The padlock displayed next to an icon indicates a password protected icon. Universal Windows apps are not supported.

Memory and Disk Space Monitoring, Date and Time

The Secure Desktop Shell monitors memory and disk space on the Windows drive. This can be disabled, and the status bar can be hidden. The Secure Desktop Shell displays date and time, locally and in Universal Time (UT) format. Date and Time information logged with the Audit features are stored in Universal Time (UT).



Using Secure Desktop

Step-by-step instructions to help you complete tasks

Getting Started with Secure Desktop

Once the software has been installed, the Secure Desktop 10 group is found under the Start menu, Programs (All Apps), Secure Desktop 10 menu. The main icon to focus on here is the Secure Desktop 10 Tools icon, providing the configuration information necessary for setting up your system. In the Windows 8 or 8.1 Start Screen, tap on the down arrow to show all apps, then scroll to the right and look for the Secure Desktop 10 Group.

The 10 Minute Setup

To quickly setup your system and get running, in approximately 10 minutes, follow these instructions:

Go to the Secure Desktop 10 group in the start menu and double-click on the Secure Desktop 10 Tools icon



After choosing Default from the list of users in the Secure Desktop Tools tab, click the Option button.

Choose any overall options you may want here and click OK. Be sure to leave the Enable Tools checked in the Password tab.

Secure Desktop Option - [SurfacePro4/User Name]

Lock	Password	Icon	Audit	Key..Mouse	F1..F12	A..Z 0..9	Key State	Startup	Shutdown
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="Audit Password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="Eject Device Password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="Control Panel Password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="Program Run Password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="Tools Password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="text" value="Exit Password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="text" value="Hot-Key = Ctrl-F12"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="text" value="Hot-Key Password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Each of the toolbar buttons listed may be enabled and password protected.

Audit - Launches the Secure Desktop Audit Viewer, sAudit.exe, to view the log files configured in the Audit tab.

Eject Device - Launches the Windows Eject Device dialog, to safely remove a USB or Firewire storage device.

OK Cancel



Click the Icon button

Secure Desktop Icon - [SurfacePro4/User Name]

Name	Internet Explorer	Name	Main
ToolTip	iexplore	<input checked="" type="checkbox"/> Enable Icon	<input checked="" type="checkbox"/> Icon Password <input type="password" value="••"/>
Command	C:\Program Files (x86)\Int	<input type="button" value="Import"/>	Normal <input type="button" value="v"/>
Directory	C:\Program Files (x86)\Int	<input type="checkbox"/> Run As Administrator	<input type="checkbox"/> Re-start If Closed
		<input type="checkbox"/> Single Instance Only	<input type="button" value="Help"/>

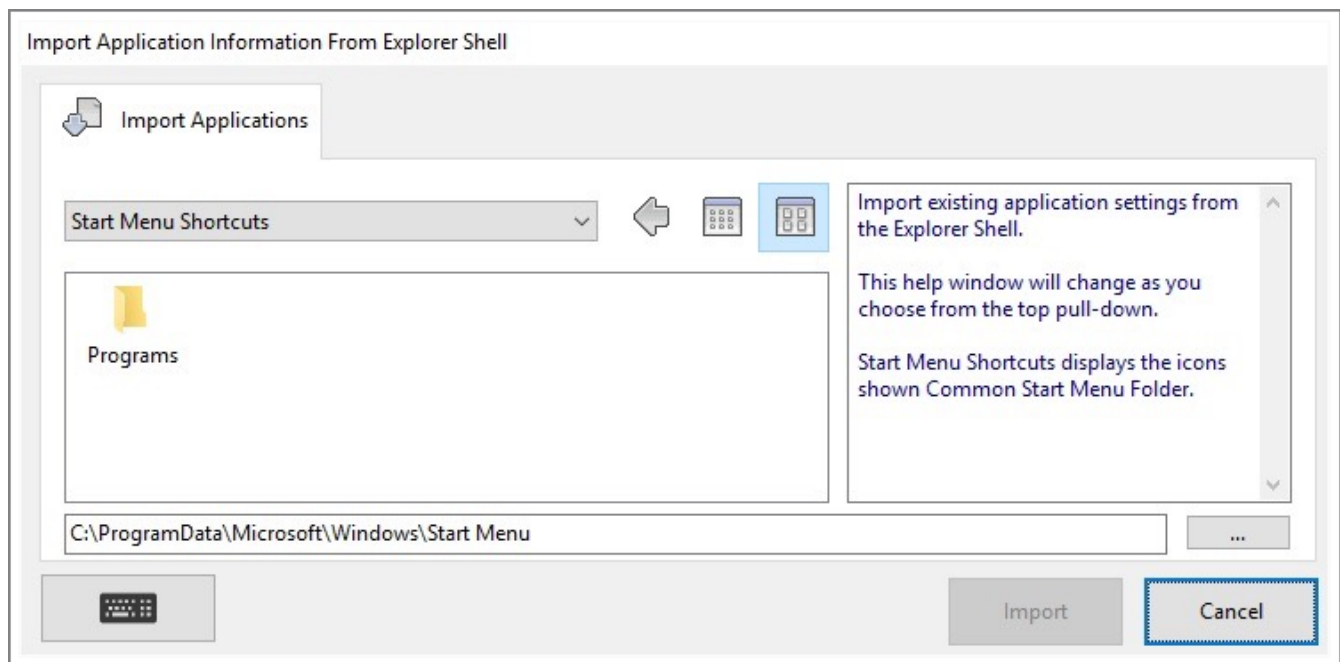
Main		Office	School	Cafe	Factory	Lab	Kiosk	Hotel	Library	Tab 9		Startup		Time
------	--	--------	--------	------	---------	-----	-------	-------	---------	-------	--	---------	--	------


Internet Explorer [F1]	Wordpad [F2]	Paint [F3]	Remote Desktop [F4]	Windows Media [F5]	Word 2016 [F6]	Excel 2016 [F7]

--	--	--	--	--	--	--

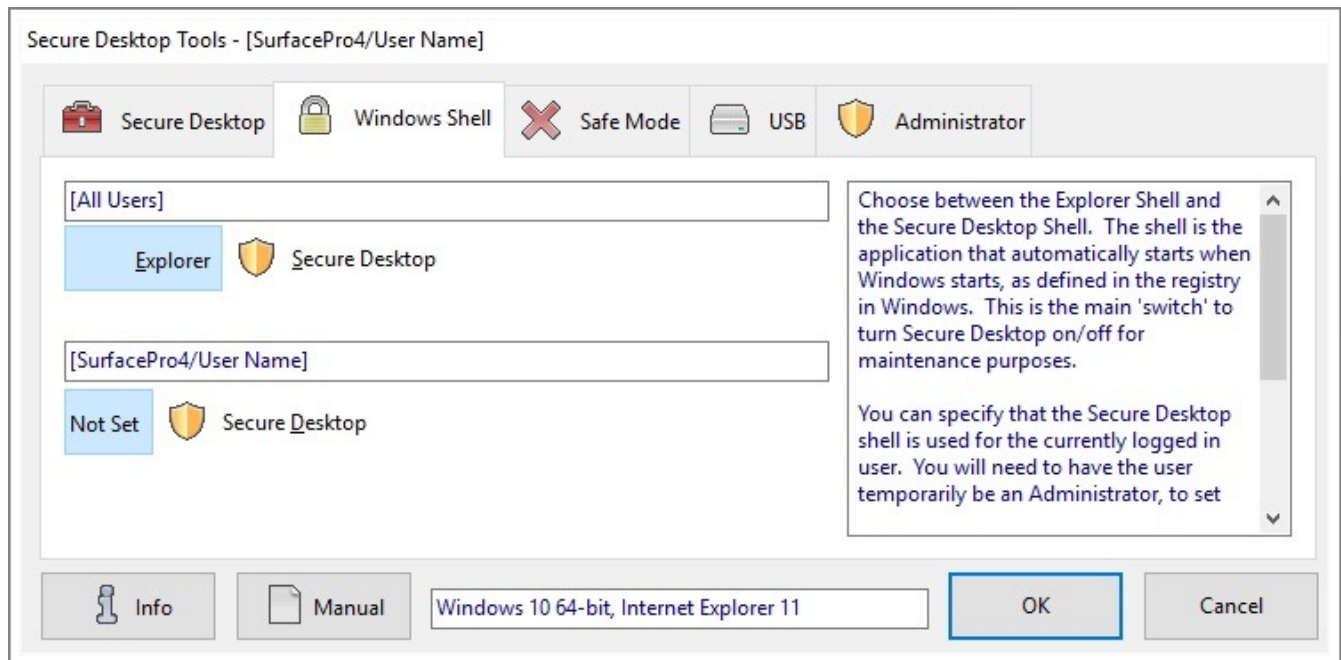


You will see Tab 0, Tab 1, Tab 2, and so-on. Choose one of those and press the Import button. This will import the icon shortcut to the highlighted Secure Desktop icon. You can now change various pieces of information about the icon, and apply a password to each of them if you want to.



You can test your settings right now by running the Secure Desktop Shell  from the Start Menu. Once you are satisfied with your configuration, you can set the shell to Secure Desktop. Please make sure that the Tools buttons is still available, so that you can get back into configuration.

Click Secure Desktop button in the Windows Shell Tab to set Secure Desktop as the shell for [All Users].



When you log off and log back on, you will not see the Explorer shell, only the Secure Desktop Shell.

That's all there is to it! (Did it take 10 minutes?)



Secure Desktop Icon Setup

Secure Desktop Icon - [SurfacePro4/User Name]

Name	Internet Explorer	Name	Main
ToolTip	ieexplore	<input checked="" type="checkbox"/> Enable Icon	<input checked="" type="checkbox"/> Icon Password <input type="password" value="••"/>
Command	C:\Program Files (x86)\Int	<input type="button" value="Import"/>	Normal <input type="button" value="v"/>
Directory	C:\Program Files (x86)\Int	<input type="checkbox"/> Run As Administrator	<input type="checkbox"/> Re-start If Closed
			<input type="checkbox"/> Single Instance Only
			<input type="button" value="Help"/>

Main		Office	School	Cafe	Factory	Lab	Kiosk	Hotel	Library	Tab 9		Startup		Time
Internet Explorer [F1]	Wordpad [F2]	Paint [F3]	Remote Desktop [F4]	Windows Media [F5]	Word 2016 [F6]	Excel 2016 [F7]								

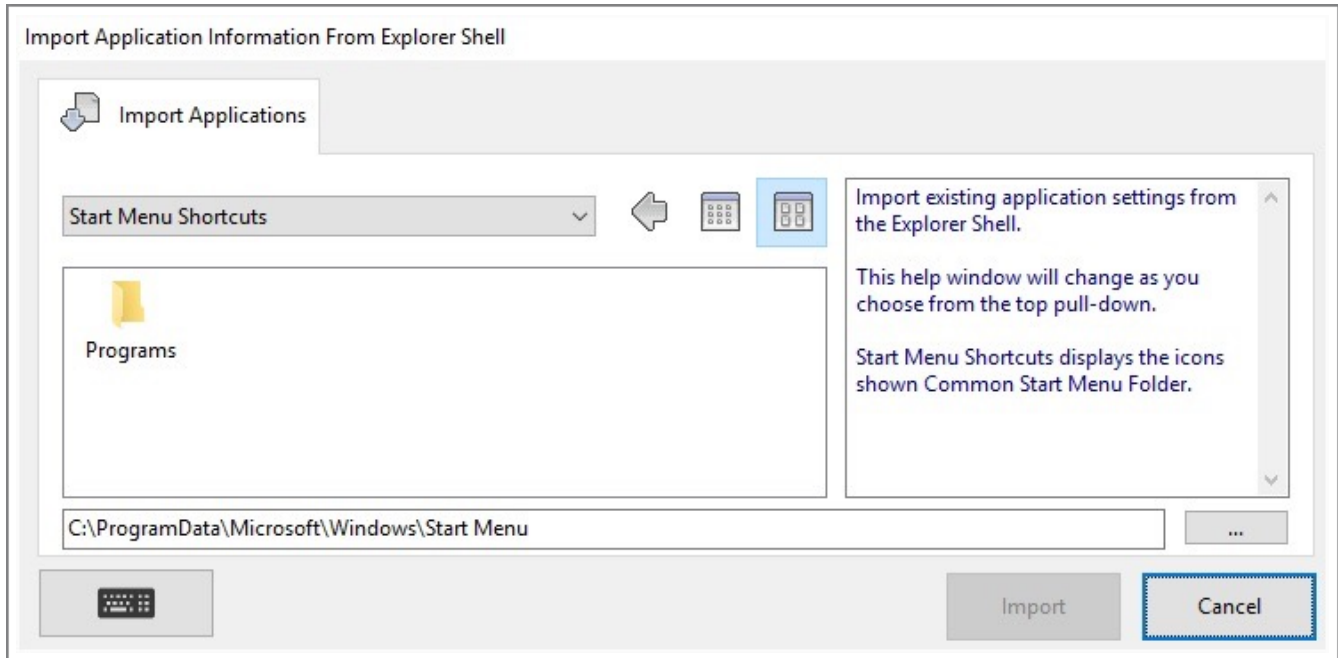
	More	Cut	Copy	Paste	Delete	Close



The Import button provides a way to import existing program settings from the Explorer Shell.



Secure Desktop Icon - Import Button



Start Menu Shortcuts displays the icons shown in the Explorer Start Menu.

Startup Group Shortcuts displays the icons in the Common Startup Folder. (available when Startup Tab selected)

Registry Startup displays the programs in the
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run registry location. (available when
Startup Tab selected)

Desktop Shortcuts displays the icons in the Common Desktop Folder.

Program Files displays the icons in the Program Files Folder.

My Computer displays the icons in the Drives Folder.

Simply select the icon that you wish to import and tap the Import Button.

When importing a shortcut file (*.LNK), Secure Desktop looks for an EXE and File Path information, and imports that data directly into the appropriate fields for a Secure Desktop Icon.



Secure Desktop Icon Setup (continued)



The More button will widen the dialog to the full width of your screen, so that you can see all icons and



tabs in one row. This button will change to Less, to bring it back to the normal size.

Icons F1 - F12 are setup very similar to icons in the Explorer shell.

Name - This is a short description that sits below the icon. This description defaults to the file name after browsing for an application or dropping a shortcut on to the command line area.

Tooltip - This description is displayed as a tooltip when the mouse passes over an icon. This can be a much longer description, and defaults to the directory and executable name when the browse button is used.

Command - This is the most important part of setting up an application icon. The command line represents the path and executable name with any additional command line parameters. The browse button on the right is useful for finding the application that you want to configure. Typical file extensions in the command line are EXE, COM, and BAT, but you can also bring in document files. Secure Desktop supports Classic Windows applications. Secure Desktop does not support Universal Windows apps.

Directory - This represents the path needed by the program defined in the command line. Most programs use their own path as the working directory, so this is the default when a program is browsed for. There are some programs that may require a different path to be entered here.

☐ **Enable Tab** - determines if this tab will be displayed in the Secure Desktop Shell.

☐ **Password** - determines if individual tab security is enabled.

Tab Name - name of the individual tab.

☐ **Enable Icon** - determines if this icon will be displayed in the Secure Desktop Shell.

☐ **Password** - determines if individual application security is enabled.

Icon Password Entry Field - determines the password to use if the Icon Password checkbox is enabled. When the user is prompted for the password, an on screen keyboard may be used for touchscreen systems.



Secure Desktop Icon Setup (continued)



Icon Button - Provides the ability to change to a different icon in the application, or to switch to an icon in another file, such as different EXE, DLL, or ICO file extension. This file and index are displayed in the center of the Icon Information group.

Window State - determines the initial size of the window for the application, Normal representing the last size, Minimized as an icon, Maximized as full screen, and Hidden. Hidden windows are not displayed anywhere in the system and are useful for communications programs that users do not need to interact with.

☐ Re-start If Closed - When checked, Secure Desktop will monitor a program to see if it has shut down for any reason. If it has shut down, it will re-start it with the exact same parameters specified. NOTE: This function works because Secure Desktop actually starts a new process. In the main timer loop, Secure Desktop checks to see if that process is still running. If it is not running, the program is re-launched. If the program that you start actually starts another program and then ends it's main process, you may have a loop situation where the program will continually start. We have witnessed this effect with various programs.

☐ Run As Administrator – Check to run the program in a different user security context. Note that disabled hot-keys or mouse buttons will not be disabled in applications in this different user security context.

☐ Single Instance Only – Check to allow one instance of a program only.



Cut,



Copy,



Paste,

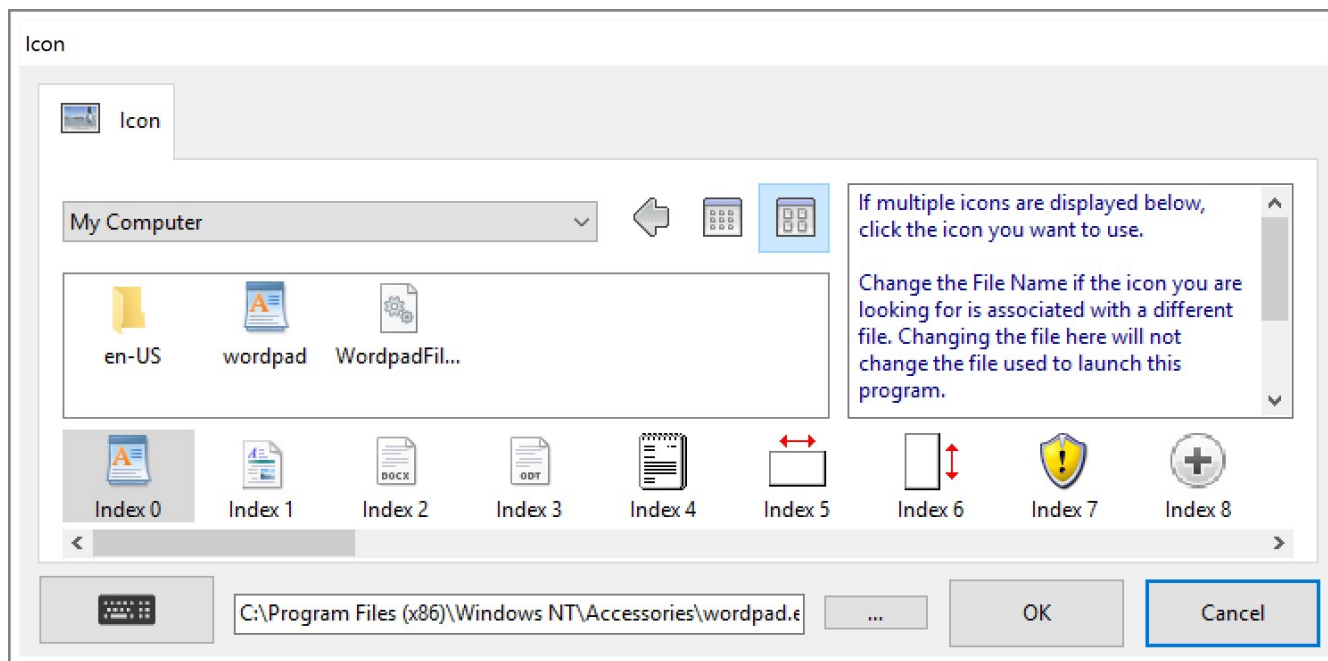


Delete Buttons - These are standard clipboard functions that

work with the entire collection of possible settings for a given application, providing a simple method of copying an application to a different place. Individual text strings may work with the clipboard via the Ctrl-X (Cut), Ctrl-C (Copy), Ctrl-V (Paste), or Del (Delete).



Secure Desktop Icon - Icon Button



If multiple icons are displayed below, click the icon you want to use.

Change the File Name if the icon you are looking for is associated with a different file. Changing the file here will not change the file used to launch this program.

Select the icon from the list below. Scroll through this list if you want to see more icons.



Secure Desktop Icon - Startup Tab

Secure Desktop Icon - [SurfacePro4/User Name]

☒ Enable Icon

Command Normal ☐ Re-start If Closed

Directory Delay Before ☐ Single Instance Only

Main Office School Cafe Factory Lab Kiosk Hotel Library Tab 9

[S1] [S2] [S3] [S4] [S5] [S6] [S7]

In the Startup tab, you will find 18 icons labeled [S1] – [S18]. These icons define up to 18 applications that will automatically start right after the Secure Desktop Shell has started.

Clicking on one of these icons, you'll find that many of the fields are hidden that are not needed. These icons never appear to the user as applications that can be started, they just start. Therefore, you only need the command string, the window state, and enable icon enabled for the main configuration.

Note the Delay Before setting. This is to specify the number of seconds to wait, before starting a particular application.

The Explorer shell may start many programs specified by either the Startup folder or Registry settings. The Secure Desktop shell, by design, only auto starts the programs found in the Startup tab.

To find a list of what the Explorer shell auto starts during system boot up or login, consider downloading a free utility from Microsoft named Autoruns. At the time of this writing, you should be able to download it here:

<https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx>

Autoruns will also give you information about auto-start services. The Secure Desktop shell does not start services, but the Explorer shell may start services that it needs. Simply set any service you need to Automatic.



Secure Desktop Icon - Timed Tab

Secure Desktop Icon - [SurfacePro4/User Name]

Time 1 Every Month 1st Day of the Month

☒ Enable Icon

Command Normal ☐ Re-start If Closed

Directory ☐ Single Instance Only

Office School Cafe Factory Lab Kiosk Hotel Library Tab 9 Startup Timed

[T1] [T2] [T3] [T4] [T5] [T6] [T7]

In the Timed tab, you will find 12 icons labeled [T1] - [T12]. These tabs define up to 12 applications that will automatically start based on the Timing Information settings at the top of the dialog.

Clicking on one of these icons, you'll find that many of the fields are hidden that are not needed. These applications never appear to the user as applications that can be started, they just start based on the time intervals. Therefore, you only need the command string, the window state, and enable icon for the main application definition.

Up to four times per a given day may be defined for automatic application start up. These four time settings may be executed every day, once per week, or once per month based on the settings specified.



Secure Desktop Icon - Shutdown Tab

Secure Desktop Icon - [SurfacePro4/User Name]

☒ Enable Icon

Command

Directory Delay After

School	Cafe	Factory	Lab	Kiosk	Hotel	Library	Tab 9	Startup	Timed	Shutdown

In the Shutdown tab, there are 12 icons labeled [SD1] – [SD12]. These icons define up to 12 applications that will be automatically started when Secure Desktop is closed.

Clicking on one of these icons, you'll find that many of the fields are hidden that are not needed. These icons never appear to the user as applications that can be started, they just start. Therefore, you only need the command string, the window state, and application start enabled for the main configuration.

Note the Delay After setting. This is to specify the number of seconds to wait after starting a particular application.



Secure Desktop Option – Password Tab

Secure Desktop Option - [SurfacePro4/User Name]

☒ Password
 ☒ Icon
 ☒ Audit
 ☒ Key..Mouse
 ☒ F1..F12
 ☒ A..Z
 ☒ 0..9
 ☒ Key State
 ☒ Startup
 ☒ Shutdown

☒ Enable Audit View
 ☒ Password:

☒ Enable Eject Device
 ☒ Password:

☒ Enable Control Panel
 ☒ Password:

☒ Enable Program Run
 ☒ Password:

☒ Enable Tools
 ☒ Password:

☒ Exit Password:
☒ When Shell Only

☒ Hot-Key = Ctrl-F12
 ☒ Password:



☒ Audit
 ☒ Eject
 ☒ Control
 ☒ Run
 ☒ Too

Each of the toolbar buttons listed may be enabled and password protected.


Audit - Launches the Secure Desktop Audit Viewer, sAudit.exe, to view the log files configured in the Audit tab.

Eject Device - Launches the Windows Eject Device dialog, to safely remove a USB or Firewire storage device.

Each of the toolbar buttons listed may be enabled and password protected.

☐ Audit View - Launches the Secure Desktop Audit Viewer,  sAudit.exe, to view the log files configured in the  Audit tab.

☐ Eject Device - Launches the Windows Eject Device dialog, to safely remove a USB storage device.

☐ Control Panel - Launches the Secure Desktop Control Panel program  sControl.exe. sControl.exe has a command-line switch of /p to show only the Printers and Faxes part of the Control Panel (need to run as an icon application to pass /p command line parameter).

☐ Program Run - Displays File Open Dialog for running any program.



☐ Tools - Launches Secure Desktop Tools, file name `sTools.exe`, for Secure Desktop Shell configuration.

☐ Exit - Ask for a password before displaying our Log Off, Restart, Exit Windows dialog. Optionally, only ask for a password if Secure Desktop is the shell.

Hot-Key to bring Secure Desktop to the Top - Defines a global keystroke for bringing Secure Desktop to the top of the window pile (top of the z-order).

Optionally, when the hot-key is pressed, a password dialog will appear. If the password is entered incorrectly, or if 60 seconds have passed, the window that previously had focus will come back to the top.



Secure Desktop Option – Icon Tab

Secure Desktop Option - [SurfacePro4/UserName]

Icons: Password, **Icon**, Audit, Key..Mouse, F1..F12, A..Z 0..9, Key State, Startup, Shutdown

Secure Desktop Position	Top of Screen	<p>Secure Desktop Position - Sets the initial position of the Secure Desktop toolbar on startup to Top or Bottom of the Screen.</p> <p>Secure Desktop Window - Sets the Z-Order to normal Window, Always On Top, or Always On Bottom. If Always On Top is selected, a maximized window will use Secure Desktop as it's top or bottom edge.</p> <p>Icon Mouse Click - You can choose to</p>
Secure Desktop Window	Normal	
Icon Mouse Click	Single Click	
Icon Background Color	<input type="checkbox"/> Window Background	
<input type="checkbox"/> Disable Keyboard Button for the on-screen Keyboard		
<input type="checkbox"/> Disable Keyboard Button on the Password Dialog		

More OK Cancel

Secure Desktop Position - Sets the initial position of the Secure Desktop toolbar on startup to Top or Bottom of the Screen.

Secure Desktop Window - Sets the Z-Order to normal Window, Always On Top, or Always On Bottom. If Always On Top is selected, a maximized window will use Secure Desktop as it's top or bottom edge.

Icon Mouse Click - You can choose to have single or double-click for starting applications with the mouse.

Icon Background Color - Background color used in Icon field.

- ☐ Disable Keyboard Button for the on-screen Keyboard - If disabled, the Keyboard button will not be visible on the main Secure Desktop Shell window. It will still be visible on a password window.
- ☐ Disable Keyboard Button on the Password Dialog - If disabled, the Keyboard button will not be visible on the Password dialog.
- ☐ Disable All Function Keys for Secure Desktop Icons - Icons are automatically assigned F1 - F12 function keys, check this to disable them.
- ☐ Set to First Tab After Icon in another Tab is clicked - If you password protect groups (or tabs), then you may want to use this. If a user is in a tab other than the first group (far left), then clicks on an icon, the tab will automatically switch back to the first tab, if this checkbox is checked.
- ☐ Hide the Tab Bar if only the First Tab is Enabled - To minimize Secure Desktop's height, you can turn off the tab bar if you are only using the first tab.
- ☐ Disable Mouse Click for 'Tray Icons' - This will disable both the left-mouse button and the right-mouse button for all icons in the Secure Desktop tray icon area.
- ☐ Show System Icons (Volume, Network, Power...) - This will start shell services. Please use with CAUTION, as Shell Services are sometimes compromised by malware.
- ☐ Hide Status Bar - To minimize Secure Desktop's height, you can turn off the status bar, which displays the Windows disk drive space, memory, and the date/time.
- ☐ Hide Universal Time on Status Bar - Normally both Local Time and Universal Time are displayed.
- ☐ Disable Screen Saver Continuously - Some customers have corporate-wide profile updates that set a screen saver. Check this option if you do not want any screen saver to be activated. Secure Desktop will actually clear the screen saver settings on a continuous basis.



Secure Desktop Option – Audit Tab

Secure Desktop Option - [SurfacePro4/User Name]

☐ Password
 ☐ Icon
 ☒ Audit
 ☐ Key..Mouse
 ☐ F1..F12
 ☐ A..Z 0..9
 ☐ Key State
 ☐ Startup
 ☒ Shutdown

☐ Audit Secure Desktop Events

☐ Disable Disk Monitor (Display and Audit File)

☐ Disable Memory Monitor (Display and Audit File)

☐ Audit Keystrokes, Window Titles, URLs, and User Name

C:\ProgramData\VisualAutomation\SecureDesktop\sAudit RSS Tuesday 01 March 2016 UT.xml

☐ Audit Secure Desktop Events - Start, stop, program start, tab click, and toolbar icon click can be saved in the sAudit xml files. These xml files are in the RSS 2.0 format, with the file name corresponding to the day of the log, one log file per day.

☐ Disable Disk Monitor and Disable Memory Monitor will disable the status bar display of that value as well as logging this data to the XML files.

☐ Audit Keystrokes, Window Titles, URLs, and User Name - The keystrokes are saved to the xml files either every 5 minutes or when the enter key is pressed. The top window title and Internet Explorer 11 (if running) are also stored as is the latest user who has logged in.

For security purposes, if a text field has the ES_PASSWORD flag (shows * for password characters) or if Internet Explorer 11 URLs are on HTTPS pages, then * (asterisk) will be logged to disk, rather than the keystroke.

Date and Time are logged in Universal Time format.



Secure Desktop Option – Key..Mouse Tab

Secure Desktop Option - [SurfacePro4/User Name]

☐ Password
 ☐ Icon
 ☐ Audit
 ☒ Key..Mouse
 ☐ F1..F12
 ☐ A..Z 0..9
 ☐ Key State
 ☐ Startup
 ☐ Shutdown

☐ Check/Clear Most
 ☐ Check/Clear Most

Disable Windows Hot-Keys

☐ Alt-Tab

☐ Ctrl-Tab

Disable Mouse Buttons

☐ Right

☐ Alt Right

Disable Windows Hot-Keys (keyboard shortcuts) and Disable Mouse Buttons - Check the appropriate checkbox to disable the keystroke.

Known keyboard shortcut help is available above when a specific keystroke is high-lighted.

Use the More Button for easier

Disable Windows Hot-Keys

- ☐ Alt-Tab: Switch between open windows. While holding the Alt key down, you can press Tab several times to navigate through the system display of each previously used window.
- ☐ Ctrl-Tab: Moves to next pane or palette.
- ☐ Ctrl-Shift-Tab: Moves to previous pane or palette.
- ☐ Alt-Shift-Tab: Similar to Alt-Tab, switch backward between open windows. You can switch between moving backward or forward by holding or releasing Shift key.
- ☐ Esc: Cancel the current task.
- ☐ Alt-Esc: Cycle the input focus through the windows in the order that they were opened; compare to Alt-Tab.
- ☐ Ctrl-Esc: Display or hide the Start menu (same as Windows Key).

- ☐ Shift-Esc: Used By Some Multimedia Programs To Exit.
- ☐ Ctrl-Shift-Esc: Launches Windows Task Manager.
- ☐ Ctrl-Alt-Esc: Cycle the input focus through the windows in the order that they were opened; same as Alt-Esc.
- ☐ Ctrl-Alt-Shift-Esc: Cycle the input focus through the windows in the order that they were opened; same as Alt-Esc.
- ☐ Alt-Shift-Esc: Similar to Alt-Esc, cycle focus backward through windows. You can switch between moving backward or forward by holding or releasing the Shift key.
- ☐ Windows: Display or hide the Start menu.
- ☐ Applications: Display the shortcut menu for the selected item.
- ☐ Alt: Activate the menu bar and enter menu mode.
- ☐ Print Screen: Copy an image of the screen.
- ☐ Ctrl-Print Screen: Copy an image of the screen.
- ☐ Alt-Print Screen: Copy an image of the current window.
- ☐ Ctrl-Break: May cause some programs to stop executing a script.
- ☐ Delete: Delete selected items.
- ☐ Shift-Delete: Delete selected item permanently without placing the item in the Recycle Bin.
- ☐ Alt-Home: Go to your Home page (browser).
- ☐ Ctrl-Page Up: Move backward through tabs (same as Ctrl-Shift-Tab).
- ☐ Ctrl-Page Down: Move forward through tabs (same as Ctrl-Tab).
- ☐ Alt-Up Arrow: Move selected item up in the Favorites list in the Organize Favorites dialog box (browser).
- ☐ Alt-Down Arrow: Move selected item down in the Favorites list in the Organize Favorites dialog box (browser).
- ☐ Alt-Left Arrow: Go to the previous page (browser).

- ☐ Alt-Right Arrow: Go to the next page (browser).
- ☐ Alt-Space: Display shortcut menu for the active window.
- ☐ Alt-Shift-Space: Same as Alt-Space, display shortcut menu for the active window.
- ☐ Alt-Enter: View properties for the selected item.
- ☐ Ctrl-Ins: Copy the selected item.
- ☐ Shift-Ins: Paste the selected item.

Disable Mouse Buttons

- ☐ Right: Displays context sensitive pop-up menu.
- ☐ Left: PLEASE USE CAUTION! The Left Mouse button is used for almost everything mouse related.
- ☐ Shift Left: Creates a new browser window when clicking on a link.
- ☐ X1: Go to the previous page (browser).
- ☐ X2: Go to the next page (browser).



Secure Desktop Option – F1..F12 Tab

Secure Desktop Option - [SurfacePro4/User Name]

Icons: Password, Icon, Audit, Key..Mouse, **F1..F12**, A..Z 0..9, Key State, Startup, Shutdown

☐ Check/Clear All

Auto-Close Help Windows

☐ HTML Help

☐ WinHelp

☐ 'Help' in Window Title

Disable Function Hot-Keys

☐ F1

☐ Ctrl-F1

Disable Function Hot-Keys (keyboard shortcuts) - Check the appropriate checkbox to disable the keystroke.

Known keyboard shortcut help is available above when a specific keystroke is high-lighted.

Use the More Button for easier configuration.

More OK Cancel

- ☐ F1: Displays Help.
- ☐ Ctrl-F1: Internet Explorer brings up the help with Ctrl-F1.
- ☐ Shift-F1: Internet Explorer brings up the help with Ctrl-F1.
- ☐ Ctrl-Shift-F1: Internet Explorer brings up the help with Ctrl-F1.
- ☐ Ctrl-Alt-Shift-F1: Internet Explorer brings up the help with Ctrl-F1.
- ☐ Alt-F4: Alt-F4 or Alt-Shift-F4 closes a window.
- ☐ Alt-Shift-F4: Alt-F4 or Alt-Shift-F4 closes a window.
- ☐ Ctrl-F4: This is used in some software packages to shut-down an application.

Auto-Close Help Windows

☐ HTML Help - Microsoft created a new help system that is HTML based and requires components that come with Internet Explorer. Secure Desktop disables this help by looking for windows that have a system menu with the menu item "Jump to URL..." within it. When it finds this kind of window, it closes it, regardless of what application may have brought up the window.

☐ WinHelp - Secure Desktop disables this traditional help by looking for and automatically closing the following 2 kinds of windows:

- 1) If the window has menu items File, Edit, Bookmark, Options, Help. Note that a help file may modify these menu items, so this is not a guarantee. If this is the case, you can use the Window Wizard to disable a special help window.
- 2) If the window has a caption that begins with "HELP TOPICS:". This window would be the table of contents for a WinHelp file.
- 3) 'Help' in Window Title - If the window has the word 'help' in it anywhere. Some programs have their own help windows.



Secure Desktop Option – A..Z 0..9 Tab

Secure Desktop Option - [SurfacePro4/User Name]

☐ Password
 ☐ Icon
 ☐ Audit
 ☐ Key..Mouse
 ☐ F1..F12
 A..Z 0..9
☐ Key State
 ☐ Startup
 ☐ Shutdown

☐ Check/Clear All
 ☐ Check/Clear All

Disable Letter

Hot-Keys

☐ Ctrl-A

☐ Ctrl-B

Disable Number

Hot-Keys

☐ Ctrl-[

☐ Ctrl-]

Disable Letter Hot-Keys (keyboard shortcuts) and Disable Number Hot-Keys - Check the appropriate checkbox to disable the keystroke.

Known keyboard shortcut help is available above when a specific keystroke is high-lighted.

Use the More Button for easier

- ☐ Ctrl-A: Select all.
- ☐ Ctrl-B: Open the Organize Favorites dialog box (browser).
- ☐ Ctrl-C: Copy selected items.
- ☐ Ctrl-D: Add the current page to your favorites (browser).
- ☐ Ctrl-E: Open Search in Explorer bar (browser).
- ☐ Ctrl-F: Opens the Find dialog box.
- ☐ Ctrl-H: Open History in Explorer bar (browser).
- ☐ Ctrl-I: Open Favorites in Explorer bar (browser).
- ☐ Ctrl-N: Opens a new blank document.
- ☐ Ctrl-O: Opens the Open dialog box.

- ☐ Ctrl-P: Opens the Print dialog box.
- ☐ Ctrl-S: Saves the document that currently has the input focus.
- ☐ Ctrl-V: Paste, cut or copied items.
- ☐ Ctrl-W: Close the current window (browser).
- ☐ Ctrl-X: Cut selected items.
- ☐ Ctrl-Y: Redo the last action.
- ☐ Ctrl-Z: Undo the last action.
- ☐ Ctrl-Shift-Q: Used By Some Multimedia Programs To Exit.



Secure Desktop Option – Key State Tab

Secure Desktop Option - [SurfacePro4/User Name]

Password
 Icon
 Audit
 Key..Mouse
 F1..F12
 A..Z 0..9
 Key State
 Startup
 Shut_down

Num Lock Key Do Nothing

Caps Lock Key Do Nothing

Scroll Lock Key Do Nothing

☐ Disable StickyKeys (Shift key 5 times)

☐ Disable FilterKeys (Hold down Right Shift key for 8 seconds)

☐ Disable ToggleKeys (Hold down Num Lock key for 5 seconds)

The Num Lock, Caps Lock, and Scroll Lock keys are special in that they have a "state" associated with them. Rather than just trap them like other keystrokes, we can actually force them to the on state or the off state, all of the time. If you have a program where passwords are case sensitive, be careful about forcing the caps lock, as you may not be able to enter the password. Secure Desktop passwords are not case sensitive. Windows passwords are case sensitive, however

More
 OK
Cancel

The Num Lock, Caps Lock, and Scroll Lock keys are special in that they have a "state" associated with them. Rather than just trap them like other keystrokes, we can actually force them to the on state or the off state, all of the time. If you have a program where passwords are case sensitive, be careful about forcing the caps lock, as you may not be able to enter the password. Secure Desktop passwords are not case sensitive. Windows passwords are case sensitive, however Secure Desktop is not actually running during the Windows Login, so this password would not be affected.

Accessibility Options Hot-Keys can be disabled. Although all of these hot-keys can be disabled via the Accessibility Options in Control Panel, we provide the ability within Secure Desktop for convenience. Note that when these hot-keys are disabled for a given user, Secure Desktop does not re-enable them unless explicitly set in this dialog.



Secure Desktop Option – Startup Tab

Secure Desktop Option - [SurfacePro4/User Name]

☐ Password
 ☐ Icon
 ☐ Audit
 ☐ Key..Mouse
 ☐ F1..F12
 ☐ A..Z 0..9
 ☐ Key State
 ☒ Startup
 ☐ Shutdown

☐ Start Explorer In Addition To Secure Desktop (Current User)

The current user needs to have adequate security to be able to write to the registry.

☐ Disable all Secure Desktop Startup applications

☐ Display Wallpaper when Secure Desktop is the Shell

C:\Program Files (x86)\Secure Desktop 10\sWall.png

Start Explorer In Addition To Secure Desktop (Current User) - When checked, the currently logged in user would get both Secure Desktop and the Explorer Desktop, primarily for administration purposes.

Note that the user needs to have the ability to write to this registry location, such as the administrator. Secure Desktop actually starts the Explorer shell, so if the administrator exits Windows

☐ Start Explorer In Addition To Secure Desktop (Current User) - When checked, the currently logged in user would get both Secure Desktop and the Explorer Desktop, primarily for administration purposes. This feature is not technically possible in Windows 10.

Note that the user needs to have the ability to write to this registry location, such as the administrator. Secure Desktop actually starts the Explorer shell, so if the administrator exits Windows using Explorer, the next user still gets Secure Desktop as the shell.

☐ Disable all Secure Desktop Startup applications - If you would like to temporarily disable startup applications, for debugging purposes.

☐ Display Wallpaper when Secure Desktop is the Shell - This launches a Secure Desktop application file named sWall.exe with the assigned picture file to run in the background, acting as the wallpaper. The picture file can be a jpg, jpeg, png or bmp file.



Secure Desktop Option – Shutdown Tab

Secure Desktop Option - [SurfacePro4/UserName]

Password
 Icon
 Audit
 Key..Mouse
 F1..F12
 A..Z 0..9
 Key State
 Startup
 Shutdown

Shutdown/Restart/Logoff Ask Permission Before Exit

Disable Options In Shut Down Dialog

☐ Shut Down
 ☐ Restart
 ☐ Log Off

Enable Option In Shut Down Dialog

☐ Set Shell to Explorer for [All Users] and Log Off

In Windows 7/8/10, the User Access Control will prompt for an Administrator logon if needed.

Shutdown/Restart/Logoff - Choose if you would like to force a shut down. If a program, such as Notepad, has an open document - and that document has not been saved, that data would be lost. This setting is not for a specific window, it is how the actual exit will work after any of the windows in the shutdown wizard have been closed.

Disable Options In Shut Down Dialog - In the shutdown dialog, there are normally 3 different options available to the user. Using these checkboxes, you can choose to disable the ☐ Shut down, ☐ Restart, and/or the ☐ Log Off portion of the dialog.

More
 OK
Cancel

Shutdown/Restart/Logoff - Choose if you would like to force a shut down. If a program, such as Notepad, has an open document – and that document has not been saved, that data would be lost. This setting is not for a specific window, it is how the actual exit will work after any of the windows in the shutdown wizard have been closed.

Disable Options In Shut Down Dialog - In the shutdown dialog, there are normally 3 different options available to the user. Using these checkboxes, you can choose to disable the ☐ Shut down, ☐ Restart, and/or the ☐ Log Off portion of the dialog.

Some computers will not "power off" when they are being shutdown, so you can disable the power off aspect of shutdown, which means that the computer will display a screen saying that it is safe to shut off the computer.

Enable Option in Shut Down Dialog - Optionally add an option to set the Shell to the Explorer Shell and Log Off. In Windows 7/8/10, the User Access Control will prompt for an Administrator logon if needed.



Secure Desktop Window Wizard – Step 1

Window Wizard - Step 1 of 5 - [SurfacePro4/User Name]

☒ Manipulate a Window

☐ Edit an Existing Window Manipulation

☐ Close A Program During Shutdown

☐ Edit an Existing Program Close

Manipulate or edit a Window Manipulation - Secure Desktop will continuously monitor the system for these windows, and will then hide the window, minimize the window, maximize the window, close the window, or manipulate the menus within the window.

Close A Program During Shutdown - Each window that you choose will be sent a "close" command in the order that you have selected. This feature has been added due to situations in which an application may not want to close due to

Back Next Start Close

☐ Manipulate or edit a Window Manipulation - Secure Desktop will continuously monitor the system for these windows, and will then hide the window, minimize the window, maximize the window, close the window, or manipulate the menus within the window.

☐ Close A Program During Shutdown - Each window that you choose will be sent a "close" command in the order that you have selected. This feature has been added due to situations in which an application may not want to close due to it's dependency on another application.

Start the application and bring up the window you wish to manipulate, then press the Next button.








Secure Desktop Window Wizard – Step 2

Window Wizard - Step 2 of 5 - [SurfacePro4/User Name]

Untitled - Notepad

Please Choose a Window from the List.

This is a list of Window titles that you may act on. This might be the main window of a program, or possibly a child window.

  Back  Next   Close

Please Choose a Window from the List.

This is a list of Window titles that you may act on. This might be the main window of a program, or possibly a child window.



Secure Desktop Window Wizard – Step 3

Window Wizard - Step 3 of 5 - [SurfacePro4/User Name]

Untitled - Notepad
&File &Edit F&ormat &View &Help

☒ Window Title After Dash (-)

☐ Window Title Before Dash (-)

☐ Exact Window Title

☐ Top Level Menu (File Edit ... Help)

☐ BOTH Top Level Menu AND Window Title After Dash (-)

☐ BOTH Top Level Menu AND Window Title Before Dash (-)

☐ BOTH Top Level Menu AND Exact Window Title

Please choose the best method to identify the window, by window title and/or by the top level menu.

Most window titles have a dash, where one side of the dash is the program title, and the other side is the document title.

If the window has a top level menu attached to the window, you can use that to identify the window also.

Back

Next

Start

Close

Please choose the best method to identify the window, by window title and/or by the top level menu.

Most window titles have a dash, where one side of the dash is the program title, and the other side is the document title.

If the window has a top level menu attached to the window, you can use that to identify the window also.

If the window does not have a top level menu attached to the window, top level menu options will not be displayed.



Secure Desktop Window Wizard – Step 4

Window Wizard - Step 4 of 5 - [SurfacePro4/User Name]

Untitled - Notepad
&File &Edit F&ormat &View &Help
Window Title After Dash (-)

☐ Hide Window

☐ Force Window to be Maximized

☐ Force Window to be Minimized

☐ Force Window to be Always-On-Top

☐ Close Window

☒ Disable Menus within Window

Please choose an action to perform on this window.

Hide Window will set the visible flag for a window to hidden.

Force Window to be Always-On-Top will make the chosen window stay on top of the Z-Order, regardless of which window has focus.

Close Window sends the same command to a window as pressing the X icon in the upper right corner.

Back

Next

Start

Close

Please choose an action to perform on this window.

Hide Window will set the visible flag for a window to hidden.

Force Window to be Always-On-Top will make the chosen window stay on top of the Z-Order, regardless of which window has focus.

Close Window sends the same command to a window as pressing the X icon in the upper right corner.

Disable Menus within Window provides a way to disable both System Menus and Menus attached to the window.

If the window does not have System Menus or Menus attached to the window, the Disable Menus option will not be displayed.



Secure Desktop Window Wizard – Step 5 – Manipulate a Window

Window Wizard - Step 5 of 5 - [SurfacePro4/User Name]

Untitled - Notepad
&File &Edit F&ormat &View &Help
Window Title After Dash (-)
Disable Menus within Window

System Menus
To Delete

- ☐ SYS 00 &Restore
- ☐ SYS 01 &Move
- ☐ SYS 02 &Size
- ☐ SYS 03 Mi&nimize
- ☐ SYS 04 Ma&ximize
- ☐ SYS 05 SEPERATOR
- ☒ SYS 06 &CloseAlt+F4

Name:

Main Menus
To Delete

- ☒ MAIN 00 &File
- ☐ SUB 00 00 &NewCtrl+N
- ☐ SUB 00 01 &Open...Ctrl+O
- ☐ SUB 00 02 &SaveCtrl+S
- ☐ SUB 00 03 Save &As...
- ☐ SUB 00 04 SEPERATOR
- ☐ SUB 00 05 Page Set&up...

Check the system menu item and main menu items that you wish to remove, then enter a name and click Save.

The system menu is from an icon in the upper left of a window. Removing minimize, maximize, or close will typically remove the associated icons in the upper right corner of a window.

The main menu represents the typical File, Edit, etc. if the menu is attached to the window.

Disable Menus

DISCLAIMER - This feature has been written based on customer requests. Although it should work with nearly all Classic Windows applications, it does not work with every one of them. This feature should be used with caution, as un-predictable results may happen if you delete a menu in an application, and that application tries to "do something" with that menu. Please spend time testing your menu modifications before implementing for an end user.

NOTE ABOUT MICROSOFT PRODUCTS - Microsoft Office, Internet Explorer, and other newer Microsoft products do not have a menu attached to the Window. With these products, the menu items (File, Edit, etc.) will "light up" with a rectangle around them. This new menu system is really a series of buttons in a cool bar. When you press one of these menu buttons, a popup menu appears. Due to this different menu architecture, Secure Desktop's menu disabling feature will not work. Please check out the Window Wizard's ability to automatically close a window, which may give you similar functionality.

Many customers have expressed the desire to "disable" the ability of exiting or closing an application, or possibly using an application such as WordPad as a file viewer with no saving capabilities. This disable menu feature provides this capability. You can delete any menu, whether system or regular, from the application that is launched.

When this step is first loaded, the application specified in the command line field is launched, listing all of the menus found in the System Menu and the Main Menu of the application. Simply check the box next to the menu that should be removed. The values that are important here are the menu type, and the co-ordinates of the menu. There are three types of menus, SYS, MAIN, and SUB. Co-ordinates start at zero for the first menu. For instance, the SUB 00 00 &NewCtrl+N found in the Main Menus To Delete list, represents a sub menu under the first menu in the Main Menu, in this case &File. The 00 represents the 1st menu item, including separators. Menu descriptions are displayed for visual reference, but are not used in the actual menu deletion operation. The type of menu and co-ordinates are the important part.



Secure Desktop Window Wizard – Step 5 – Close a Program During Shutdown

Window Wizard - Step 5 of 5 - [SurfacePro4/User Name]

Untitled - Notepad
&File &Edit F&ormat &View &Help
Window Title After Dash (-)
Close Window During Shutdown. Time Delay: 0 secs

Append


Insert

Save

Untitled - Notepad - 0 Seconds Delay


Choose to Append or Insert this Program Closing configuration. Remember, the programs are closed in the order listed.


If editing an existing configuration, simply press Save.



Back

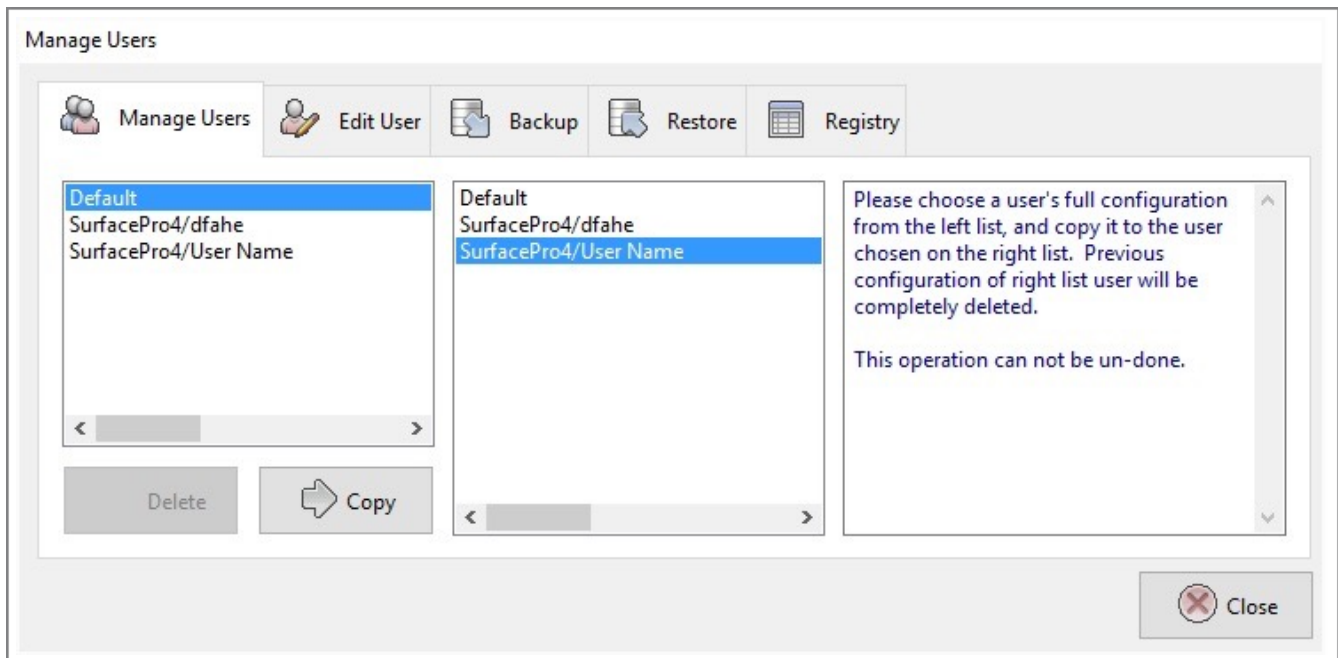
Next

 Start

 Close

When choosing to close a program during shutdown in step 1, step 5 will look like the window above, rather than the step 5 image on the previous page, for manipulating a window.

Step 4 provides the capability of specifying the number of seconds to delay after closing the program.

**Manage Users - Manage Users Tab**

Please choose a user's full configuration from the left list, and copy it to the user chosen on the right list. Previous configuration of right list user will be completely deleted.

You can not undo this operation.



Manage Users - Edit User Tab

Manage Users

Manage Users Edit User Backup Restore Registry

Default
SurfacePro4/User Name
SurfacePro4/dfahe

SurfacePro4

User Name

Edit UserName

[All Users]

☐ Ignore HostName.DomainName

Delete Duplicate

UserName Only for User Lookup

HostName.DomainName:

The fully qualified DNS name that uniquely identifies the computer. If the local computer is a node in a cluster, this field is the fully qualified DNS name of the local computer, not the name of the cluster virtual server.

The fully qualified DNS name is a combination of the DNS host name and the DNS domain name, using the form

Close

HostName.DomainName:

The fully qualified DNS name that uniquely identifies the computer. If the local computer is a node in a cluster, this field is the fully qualified DNS name of the local computer, not the name of the cluster virtual server.

The fully qualified DNS name is a combination of the DNS host name and the DNS domain name, using the form HostName.DomainName.

UserName:


The User's Logon Name.

Ignore HostName.DomainName checkbox: When checked, a user's configuration data read/write will be based on the UserName only. The HostName.DomainName stored in the sdesktop.xml file will be ignored.

If checked, the sdesktop.xml file will be much more portable for customers who copy the sdesktop.xml file to several identical computers.

**Manage Users - Edit User Tab - Edit UserName**

Edit UserName

 Edit UserName

SurfacePro4

Current UserName: User Name

New UserName:

Verify UserName:


UserName must be spelled exactly the same as the Logon UserName

Invalid UserName Characters / \ [] " ; | < > + = , ? * % @

The UserName has to match a Windows User Logon Name.

New Users are created via Control Panel | User Accounts or Settings, depending on Windows version.

When the Secure Desktop shell starts, it opens the sdesktop.xml file and looks up the user's configuration using the HostName.DomainName/UserName string.



The UserName has to match a Windows User Logon Name.

New Users are created via Control Panel | User Accounts or Settings, depending on Windows version.

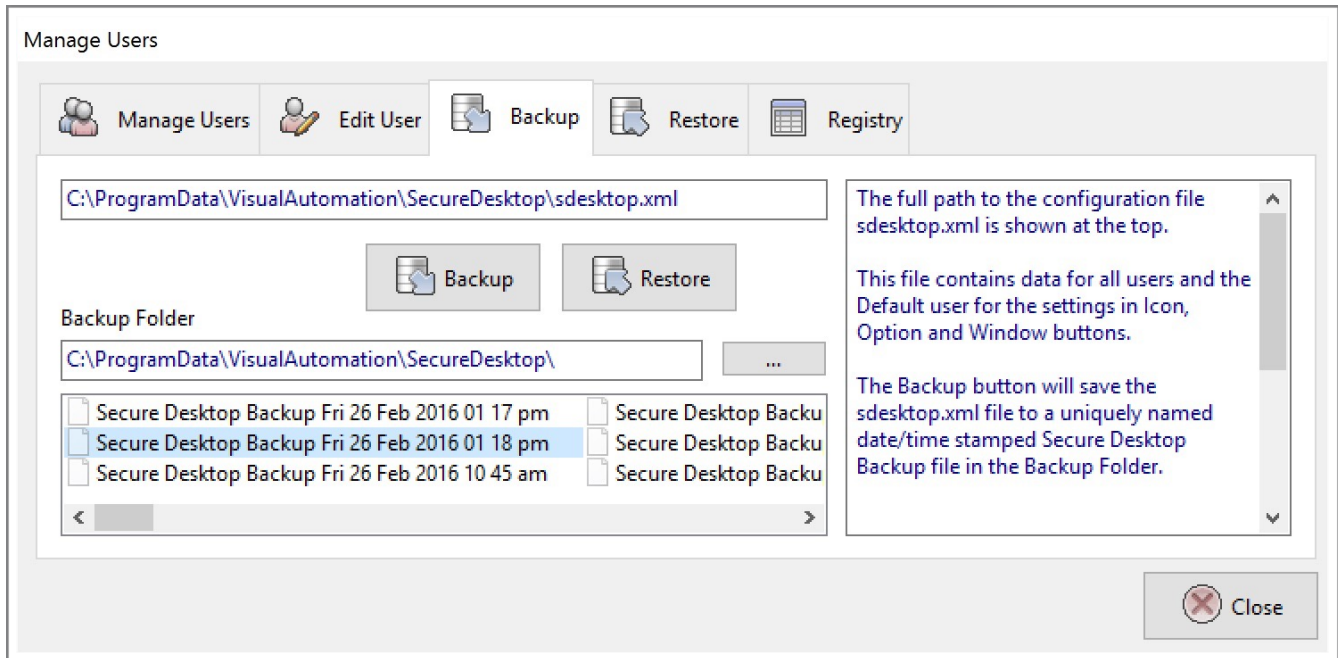
When the Secure Desktop shell starts, it opens the sdesktop.xml file and looks up the user's configuration using the HostName.DomainName/UserName string.

If it finds that configuration, it looks for the switch to determine if the User settings should be loaded or the Default settings.

If it does not find that configuration, the Default settings are loaded.



Manage Users - Backup Tab



The full path to the configuration file sdesktop.xml is shown at the top.

This file contains data for all users and the Default user for the settings in Icon, Option and Window buttons.

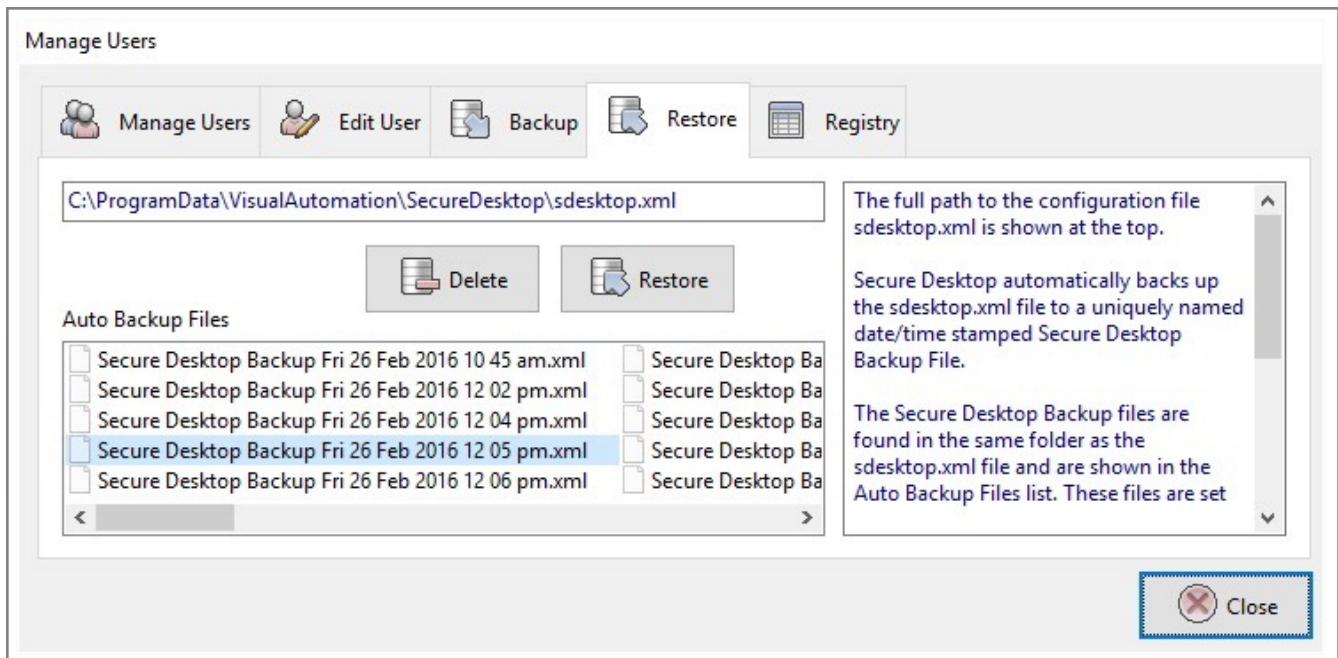
The Backup button will save the sdesktop.xml file to a uniquely named date/time stamped Secure Desktop Backup file in the Backup Folder specified.

The default Backup Folder is the folder where the sdesktop.xml is located, but any folder that the user has write-access to can be selected via the ... button.

The Restore button will restore any uniquely named date/time stamped Secure Desktop Backup file listed in the Backup Folder.



Manage Users - Restore Tab



The full path to the configuration file sdesktop.xml is shown at the top.

Secure Desktop automatically backs up the sdesktop.xml file to a uniquely named date/time stamped Secure Desktop Backup File.

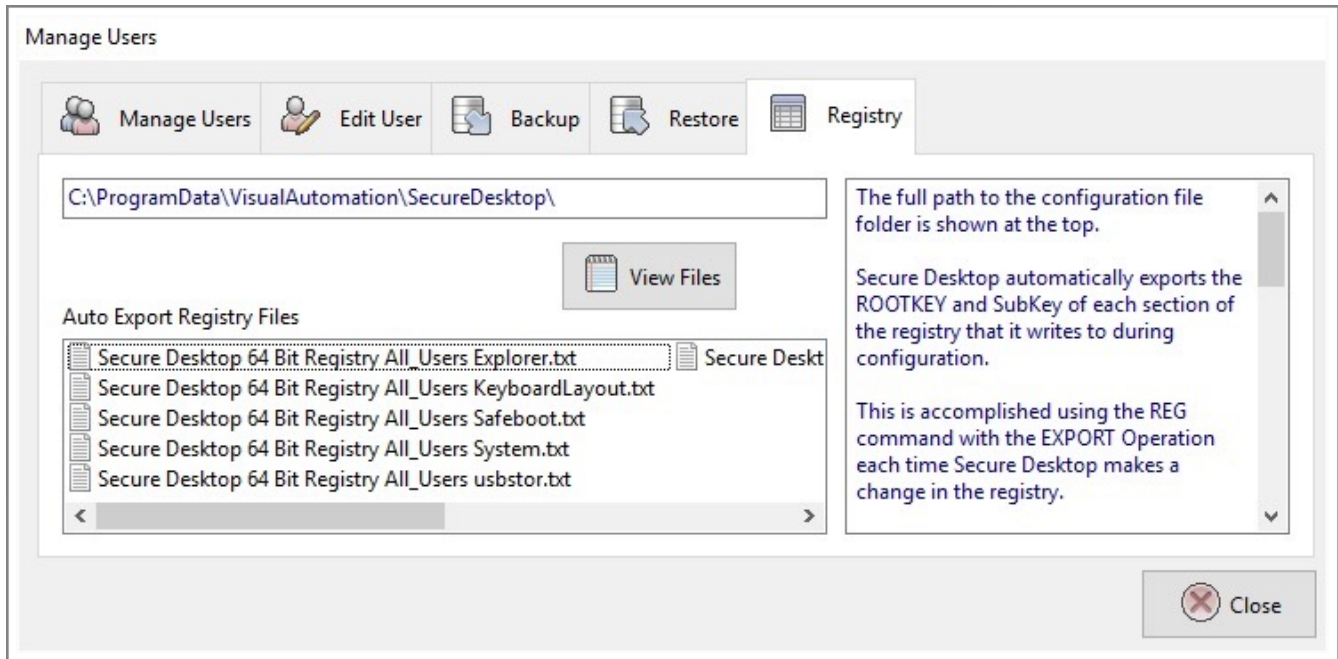
The Secure Desktop Backup files are found in the same folder as the sdesktop.xml file and are shown in the Auto Backup Files list. These files are set with the Read Only and Hidden file attributes.

The Restore button will restore any uniquely named date/time stamped Secure Desktop Backup file selected in the Auto Backup Files list.

The Delete button will delete the selected Secure Desktop Backup file shown in the Auto Backup Files list.



Manage Users - Registry Tab



This feature is only available in Windows 8 and Windows 10.

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

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

This is accomplished using the REG command with the EXPORT Operation each time Secure Desktop makes a change in the registry.

The Secure Desktop Registry*.txt file name contains either the HostName.DomainName_UserName for HKEY_CURRENT_USER registry settings or All_Users for HKEY_LOCAL_MACHINE settings. The file name will also indicate if it's referring to the 32-bit or 64-bit portion of the registry.

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

However, because they are EXPORTed using the REG command, they can also be IMPORTed using the REG command. Please keep in mind that the IMPORT is actually a merge of data.

This may be useful for the configuration of other users or other identical computers, but is not recommended.

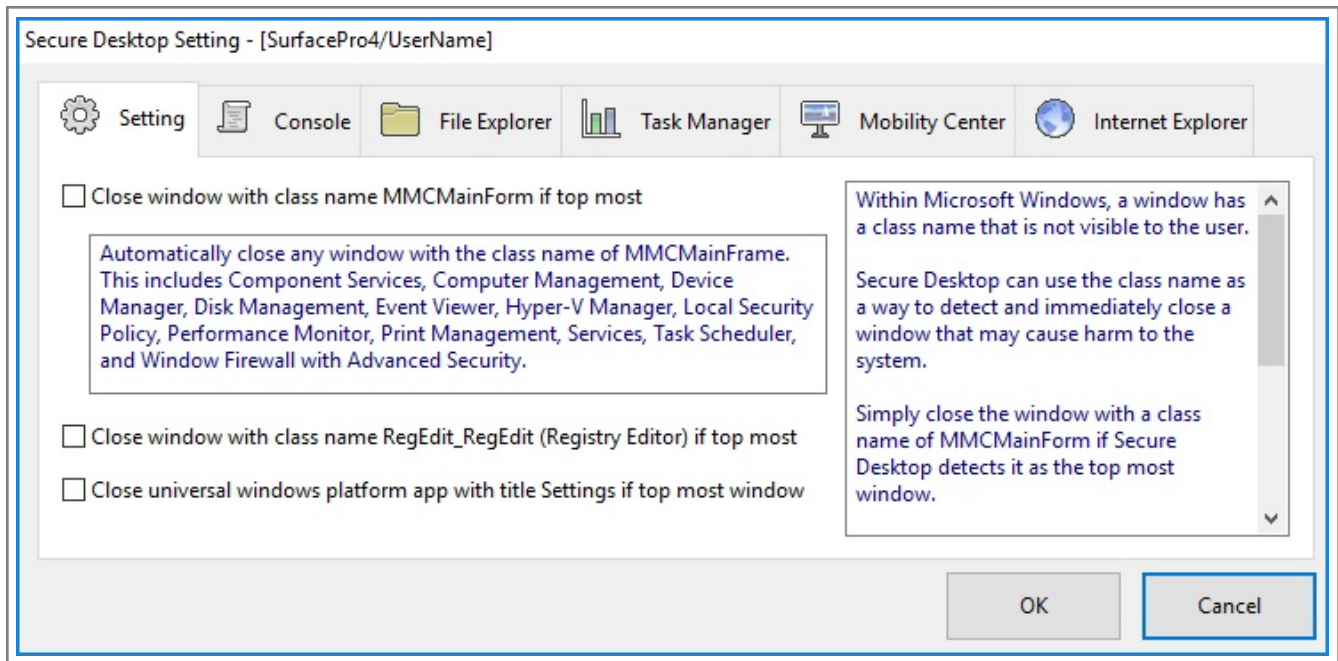
Some of the registry settings made by Secure Desktop have corresponding Windows API calls and/or file renaming to achieve their purpose.

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

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



Setting - Setting Tab



Automatically close any window with the class name of MMCMainFrame. This includes Component Services, Computer Management, Device Manager, Disk Management, Event Viewer, Hyper-V Manager, Local Security Policy, Performance Monitor, Print Management, Services, Task Scheduler, and Window Firewall with Advanced Security.

Within Microsoft Windows, a window has a class name that is not visible to the user.

Secure Desktop can use the class name as a way to detect and immediately close a window that may cause harm to the system.

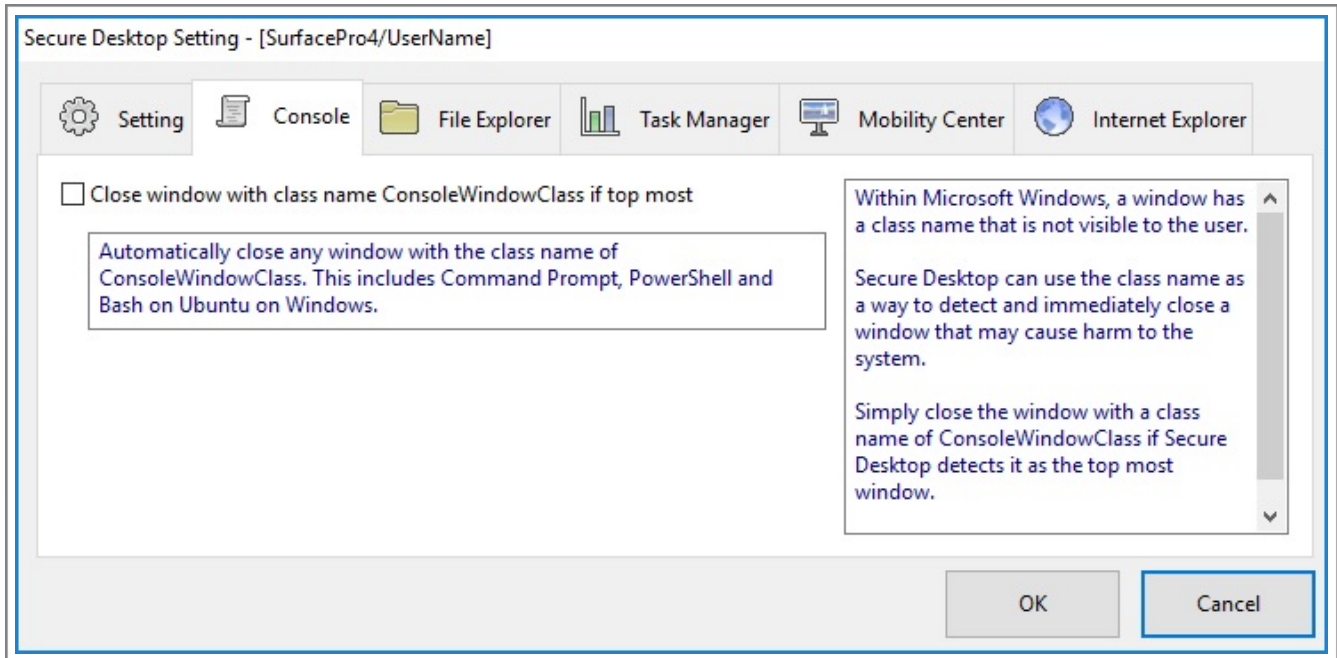
Simply close the window with a class name of MMCMainForm if Secure Desktop detects it as the top most window.

Simply close the window with a class name of RegEdit_RegEdit if Secure Desktop detects it as the top most window.

Simply close the Universal Windows Platform app with the title Settings if Secure Desktop detects it as the top most window.



Setting - Console Tab



Automatically close any window with the class name of ConsoleWindowClass. This includes Command Prompt, PowerShell and Bash on Ubuntu on Windows.

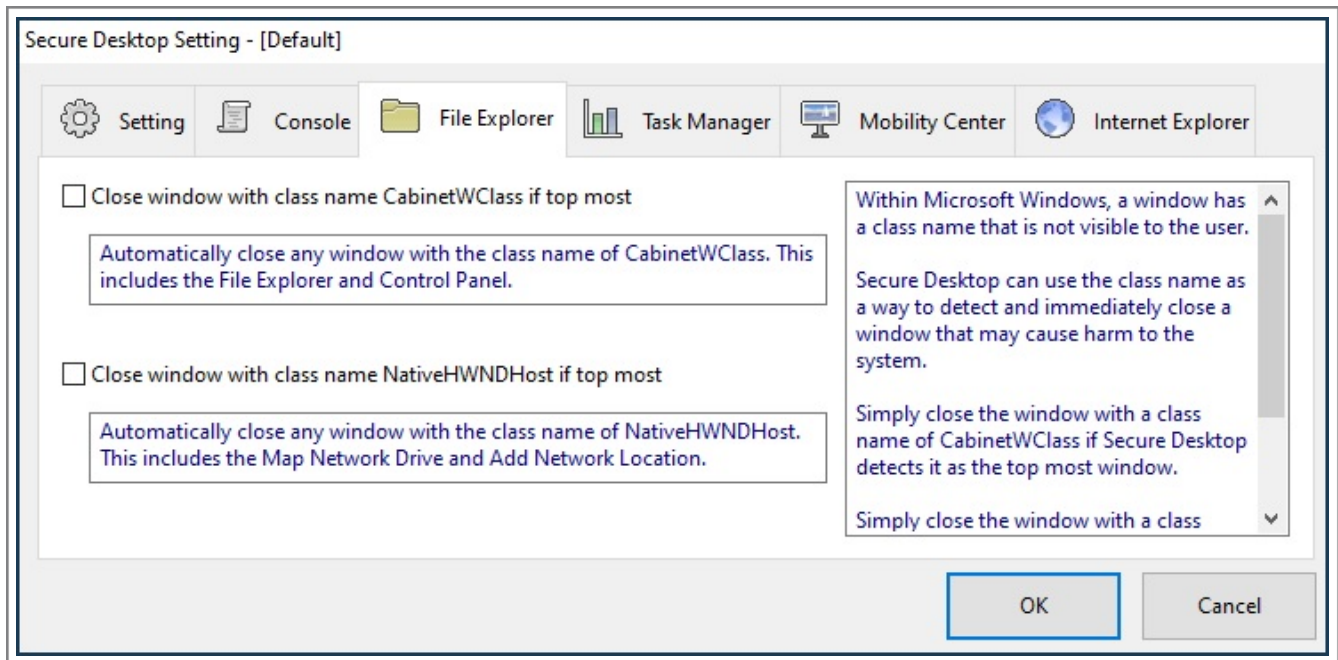
Within Microsoft Windows, a window has a class name that is not visible to the user.

Secure Desktop can use the class name as a way to detect and immediately close a window that may cause harm to the system.

Simply close the window with a class name of ConsoleWindowClass if Secure Desktop detects it as the top most window.



Setting - File Explorer Tab



Automatically close any window with the class name of CabinetWClass. This includes the File Explorer and Control Panel.

Automatically close any window with the class name of NativeHWNDHost. This includes the Map Network Drive and Add Network Location.

Within Microsoft Windows, a window has a class name that is not visible to the user.

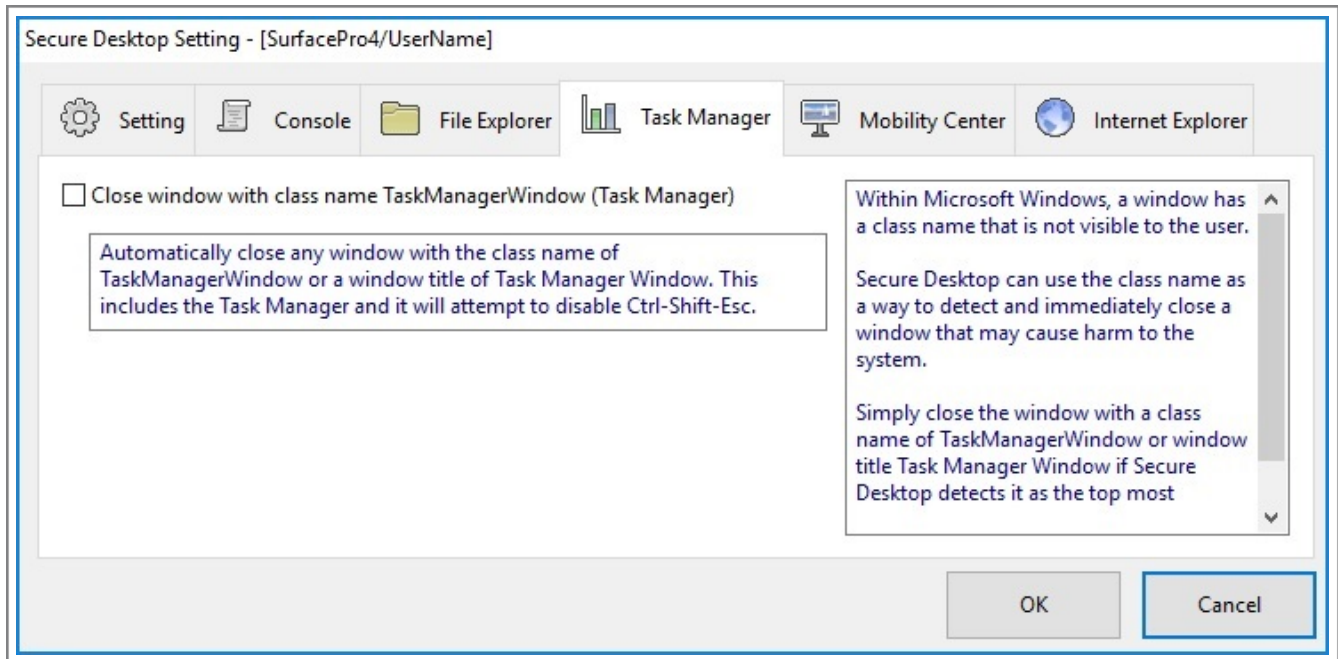
Secure Desktop can use the class name as a way to detect and immediately close a window that may cause harm to the system.

Simply close the window with a class name of CabinetWClass if Secure Desktop detects it as the top most window.

Simply close the window with a class name of NativeHWNDHost if Secure Desktop detects it as the top most window.



Setting - Task Manager Tab



Automatically close any window with the class name of TaskManagerWindow or a window title of Task Manager Window. This includes the Task Manager and it will attempt to disable Ctrl-Shift-Esc.

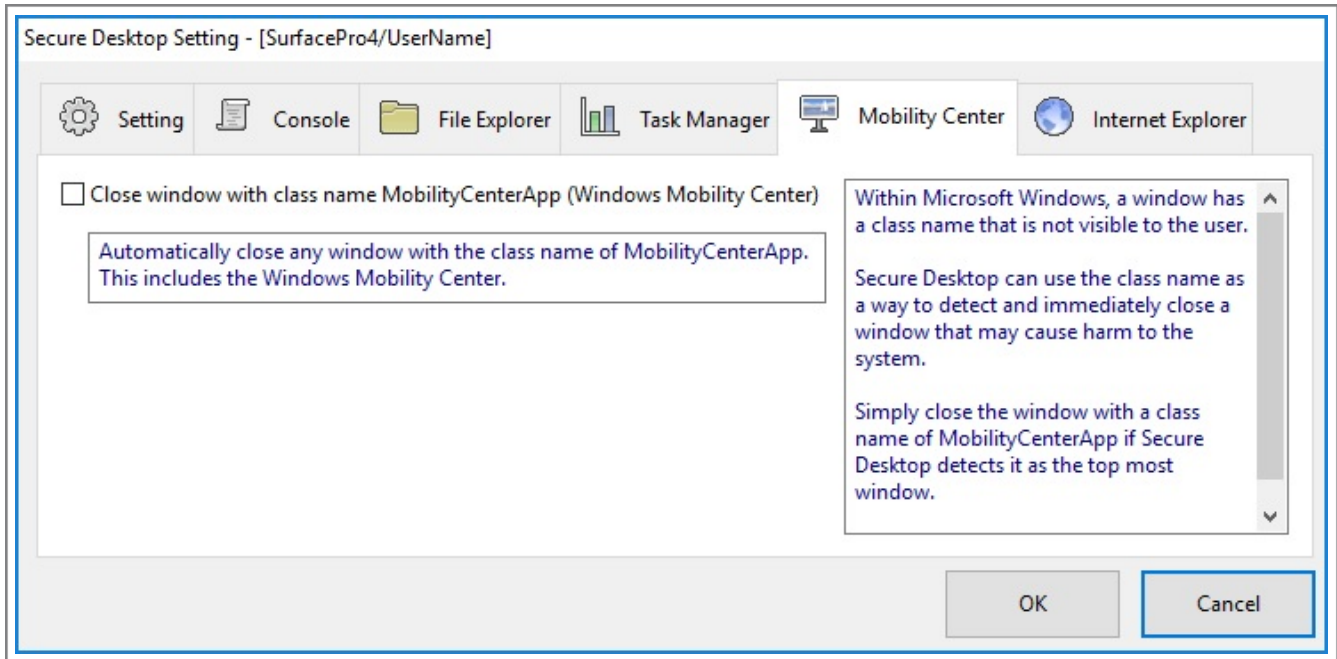
Within Microsoft Windows, a window has a class name that is not visible to the user.

Secure Desktop can use the class name as a way to detect and immediately close a window that may cause harm to the system.

Simply close the window with a class name of TaskManagerWindow or window title Task Manager Window if Secure Desktop detects it as the top most window.



Setting - Mobility Center Tab



Automatically close any window with the class name of MobilityCenterApp. This includes the Windows Mobility Center.

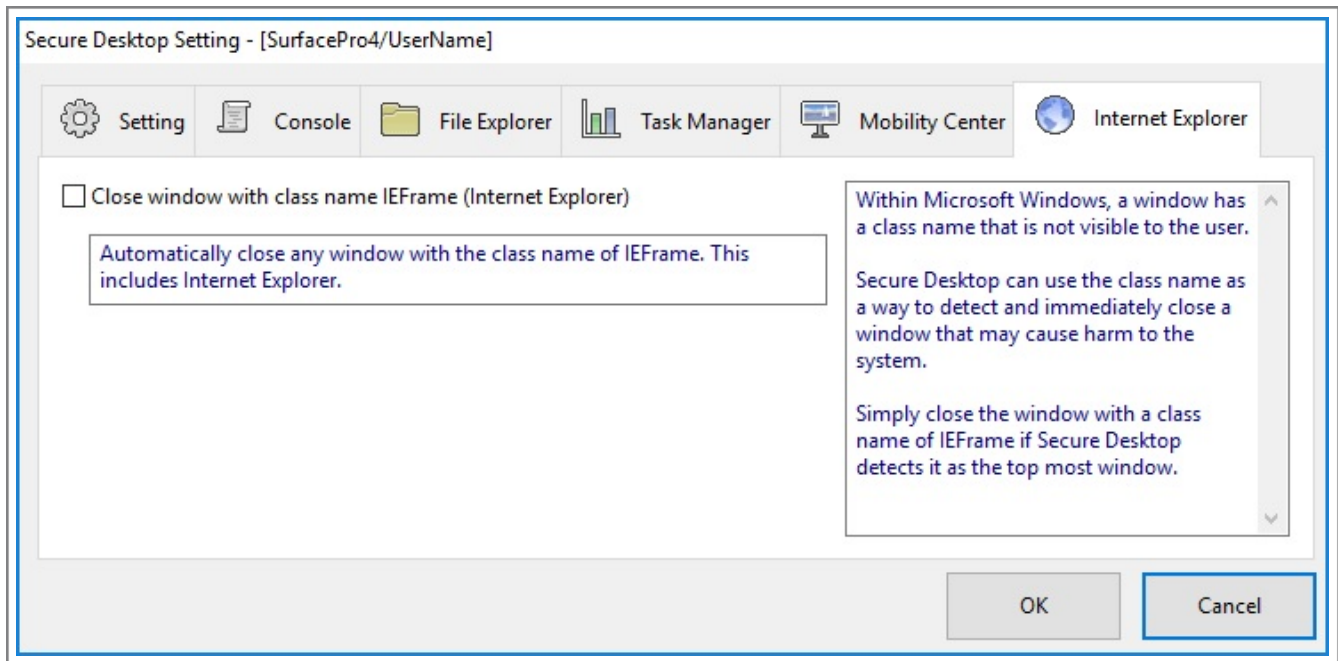
Within Microsoft Windows, a window has a class name that is not visible to the user.

Secure Desktop can use the class name as a way to detect and immediately close a window that may cause harm to the system.

Simply close the window with a class name of MobilityCenterApp if Secure Desktop detects it as the top most window.



Setting - Internet Explorer Tab



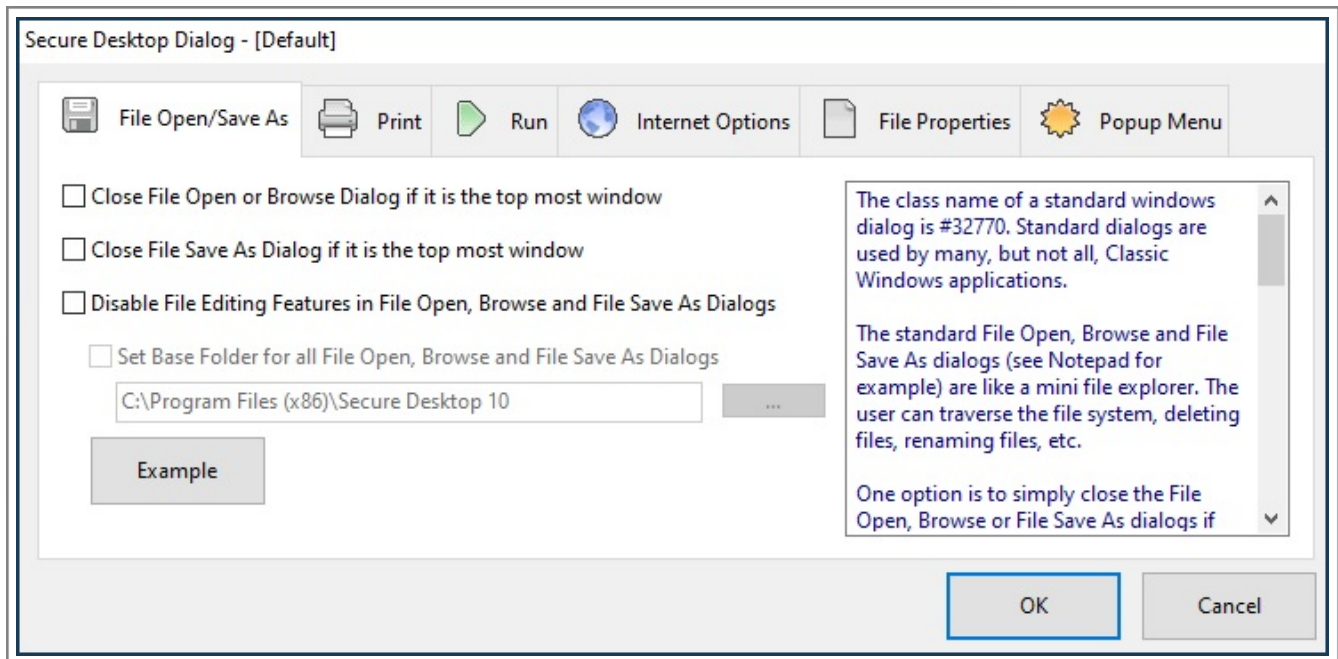
Within Microsoft Windows, a window has a class name that is not visible to the user.

Secure Desktop can use the class name as a way to detect and immediately close a window that may cause harm to the system.

Simply close the window with a class name of IEFram if Secure Desktop detects it as the top most window.



Dialog - File Open/Save As Tab



The class name of a standard windows dialog is #32770. Standard dialogs are used by many, but not all, Classic Windows applications.

The standard File Open, Browse and File Save As dialogs (see Notepad for example) are like a mini file explorer. The user can traverse the file system, deleting files, renaming files, etc.

One option is to simply close the File Open, Browse or File Save As dialogs if Secure Desktop detects it as the top most window. This may work well if the user does not need to open files after launching the program.

Another option is to disable the mouse and keyboard inputs to most of the user interface of the File Open, Browse and File Save As dialogs.

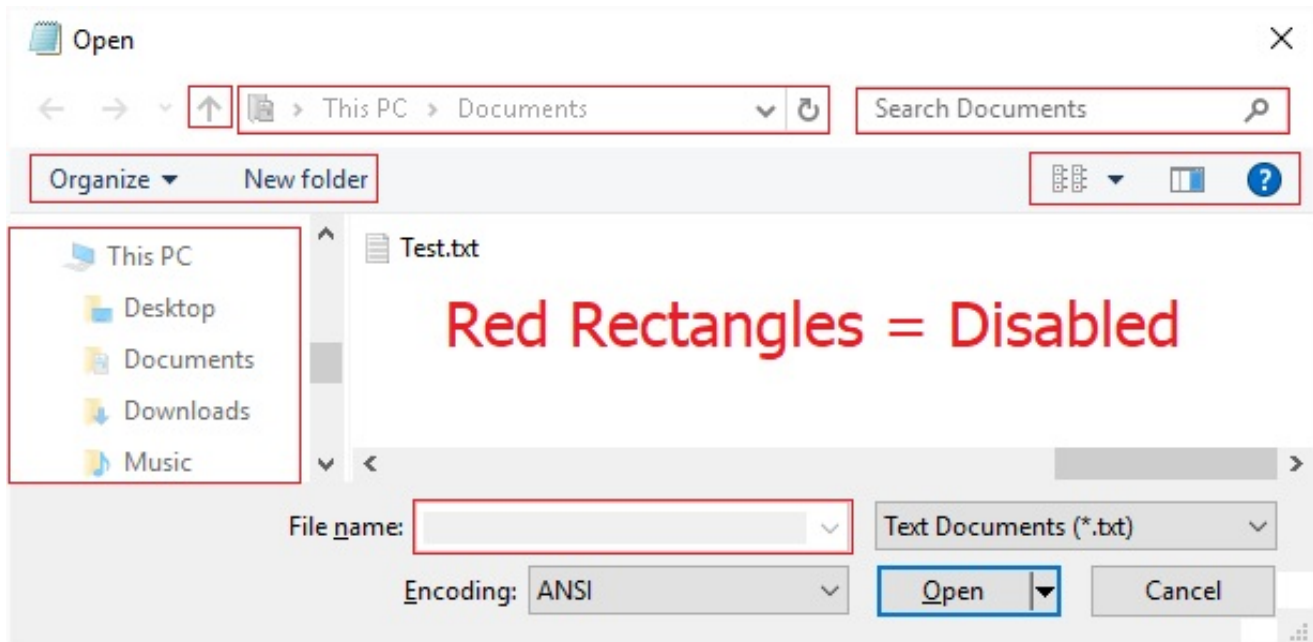
Disable toolbar, navigation, search, right mouse click, long left mouse click and " : ; \ | " keys.

Disable keyboard shortcuts F2, Alt-Enter, Ctrl-D, Ctrl-V, Shift-F10, Delete, Shift-Delete, Tab, Shift-Tab, Ctrl-Tab, Ctrl-Shift-Tab, Alt-Up, Alt-Down, Backspace.

If the Set Base Folder for all File Open, Browse and File Save As Dialogs checkbox is not checked, the user will not be able to change to another folder. The default File Open, Browse or File Save As folder for the program will not change.

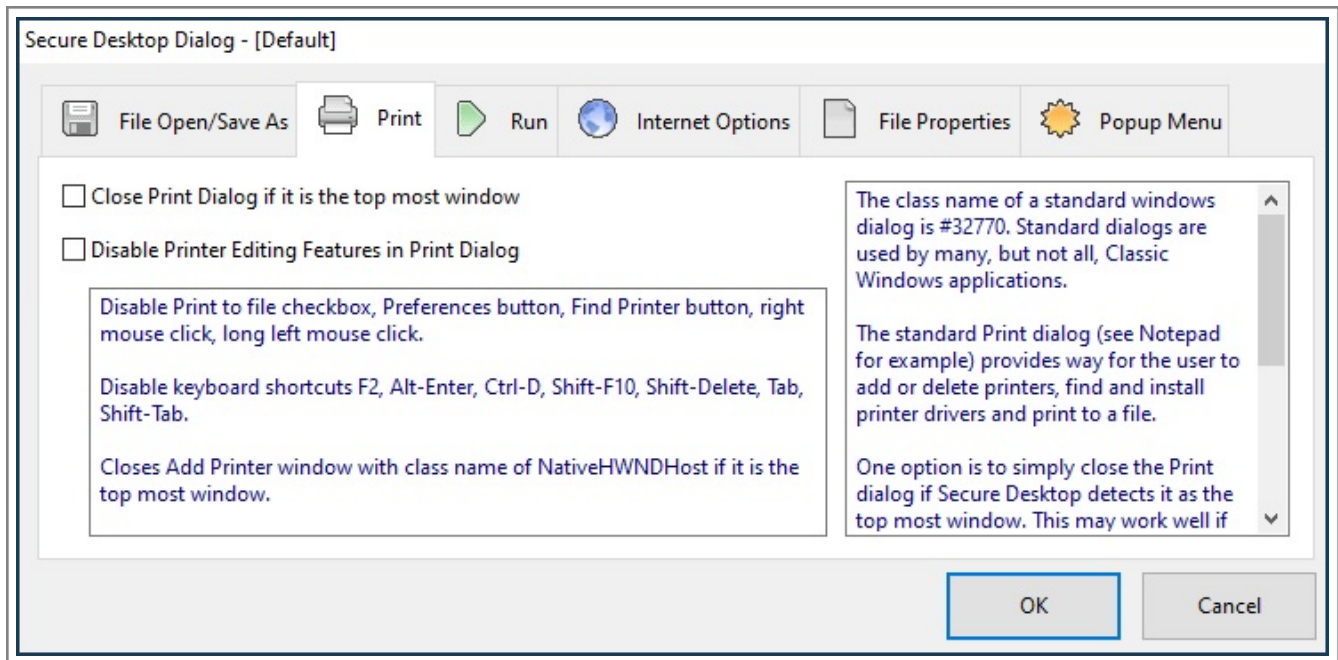
The end result is the user can pick a file to open from the default folder or save to that same folder.

In Windows 7, 8 or 10: if the Set Base Folder for all File Open, Browse and File Save As Dialogs checkbox is checked, the user can visit that base folder and any sub-folders only.





Dialog - Print Tab



Disable Print to file checkbox, Preferences button, Find Printer button, right mouse click, long left mouse click.

Disable keyboard shortcuts F2, Alt-Enter, Ctrl-D, Shift-F10, Shift-Delete, Tab, Shift-Tab.

Closes Add Printer window with class name of NativeHWNDHost if it is the top most window.

The class name of a standard windows dialog is #32770. Standard dialogs are used by many, but not all, Classic Windows applications.

The standard Print dialog (see Notepad for example) provides way for the user to add or delete printers, find and install printer drivers and print to a file.

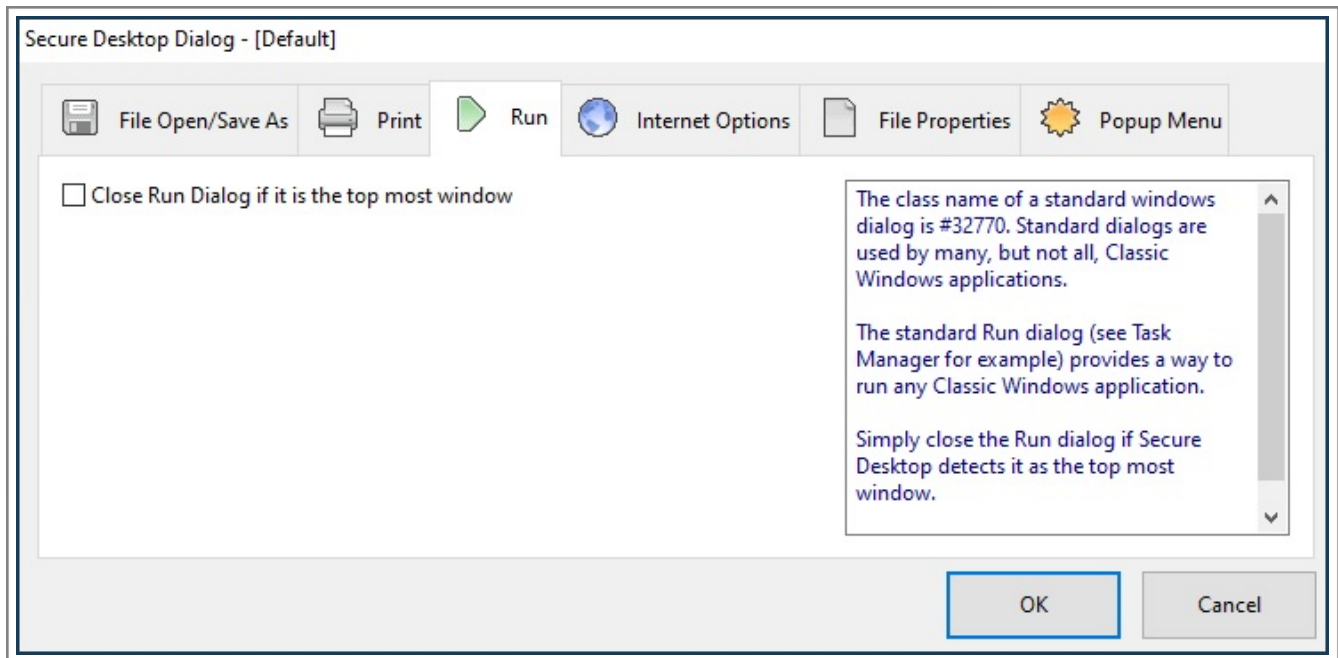
One option is to simply close the Print dialog if Secure Desktop detects it as the top most window. This may work well if the user does not need to print.

Another option is to disable the mouse and keyboard inputs to most of the user interface of the Print dialog.

The end result is that the user will not be able to add or delete printers or print to a file.



Dialog - Run Tab



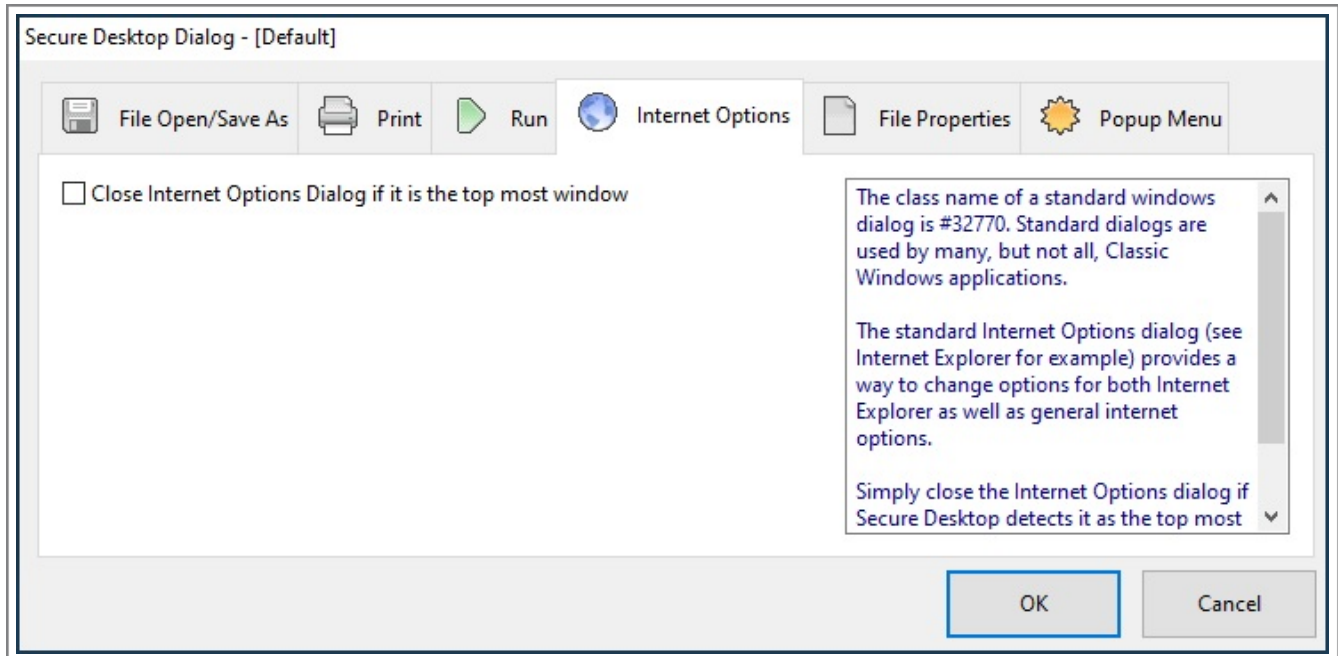
The class name of a standard windows dialog is #32770. Standard dialogs are used by many, but not all, Classic Windows applications.

The standard Run dialog (see Task Manager for example) provides a way to run any Classic Windows application.

Simply close the Run dialog if Secure Desktop detects it as the top most window.



Dialog - Internet Options Tab



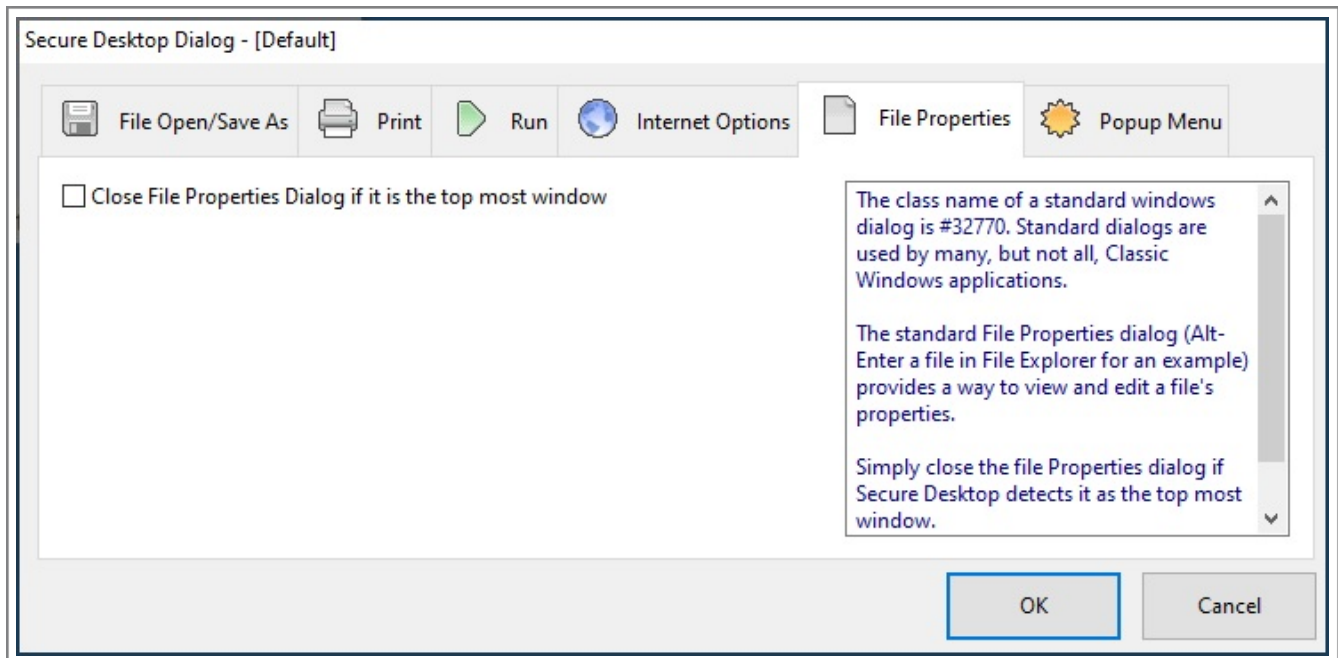
The class name of a standard windows dialog is #32770. Standard dialogs are used by many, but not all, Classic Windows applications.

The standard Internet Options dialog (see Internet Explorer for example) provides a way to change options for both Internet Explorer as well as general internet options.

Simply close the Internet Options dialog if Secure Desktop detects it as the top most window.



Dialog - File Properties Tab



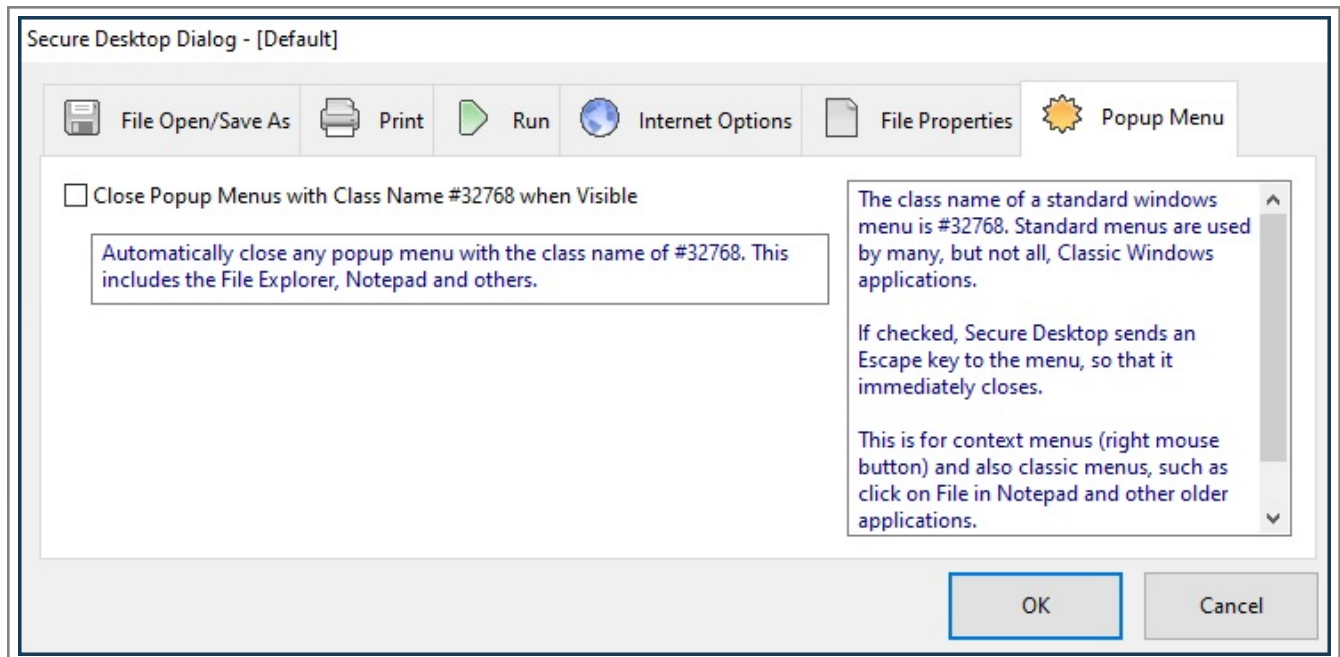
The class name of a standard windows dialog is #32770. Standard dialogs are used by many, but not all, Classic Windows applications.

The standard File Properties dialog (Alt-Enter a file in File Explorer for an example) provides a way to view and edit a file's properties.

Simply close the file Properties dialog if Secure Desktop detects it as the top most window.



Dialog - Popup Menu Tab



Automatically close any popup menu with the class name of #32768. This includes the File Explorer, Notepad and others.




The class name of a standard windows menu is #32768. Standard menus are used by many, but not all, Classic Windows applications.

If checked, Secure Desktop sends an Escape key to the menu, so that it immediately closes.

This is for context menus (right mouse button) and also classic menus, such as click on File in Notepad and other older applications.


**Administrator - All Users - Supervisor - Supervisor Mode**

Supervisor Setup - [All Users]

 **Supervisor Mode**  **When Logged In**  **Calculation Passwords**

☒ Enable Supervisor Toolbar Button


Supervisor Password

Icon Background Color  Yellow ▼

☐ Automatically Log Off after minutes

☐ Set to First Tab On Log Off

The Supervisor feature provides an easy way to 'login' with one password and have un-interrupted access to normally 'secure' items. If enabled, a new toolbar button appears in Secure Desktop that prompts for a password.



The Supervisor feature provides an easy way to 'login' with one password and have un-interrupted access to normally 'secure' items. If enabled, a new toolbar button appears in Secure Desktop that prompts for a password.

**Administrator - All Users - Supervisor – When Logged In Tab**

Supervisor Setup - [All Users]

Supervisor Mode **When Logged In** **Calculation Passwords**

<input type="checkbox"/> Enable Keystrokes/Mouse Buttons	<input type="checkbox"/> Enable Audit
<input type="checkbox"/> Enable Tray Icon Mouse Clicks	<input type="checkbox"/> Enable Eject Device
<input type="checkbox"/> Show Hidden Files/Folders	<input type="checkbox"/> Enable Control Panel
<input type="checkbox"/> Disable Window Wizard	<input type="checkbox"/> Enable Run
<input type="checkbox"/> Unlock All Tabs	<input type="checkbox"/> Enable Tools
<input type="checkbox"/> Unlock All Icons	<input type="checkbox"/> Unlock Exit

When the supervisor has successfully logged in, he/she may have access to any of the items checked in the When Logged In tab. Note that toolbar buttons that may not have been enabled under normal operation can be turned on temporarily in this manner. After login, the Supervisor button changes from a lock to an un-lock and the icon background is yellow (default) to remind the Supervisor to log off, which requires another click of the button. You can set a time for automatic

Clear All **Default** **OK** **Cancel**

When the supervisor has successfully logged in, he/she may have access to any of the items checked in the When Logged In tab. Note that toolbar buttons that may not have been enabled under normal operation can be turned on temporarily in this manner. After login, the Supervisor button changes from a lock to an un-lock and the icon background is yellow (default) to remind the Supervisor to log off, which requires another click of the button. You can set a time for automatic log off also, and you can choose to set back to the first tab on log off.



Administrator - All Users - Supervisor – Calculation Passwords Tab

Supervisor Setup - [All Users]

Supervisor Mode | When Logged In | **Calculation Passwords**

5 Digit PIN Save PIN To ☒ XML File ☐ Registry

Formula

Append Calculation To These Passwords

<input type="checkbox"/> Audit	<input type="checkbox"/> Tools	<input type="checkbox"/> All Tabs
<input type="checkbox"/> Eject Device	<input type="checkbox"/> Exit	<input type="checkbox"/> All Icons
<input type="checkbox"/> Control Panel	<input type="checkbox"/> Supervisor	
<input type="checkbox"/> Program Run		

You can use calculation passwords throughout Secure Desktop, where previously it was for the Supervisor Mode only.

There is a calculation based on a PIN number up to 5 digits, the day, the month, and the year using the Formula.

You have the choice of storing the PIN number in the sDesktop XML file or in the registry. The registry location is

You can use calculation passwords throughout Secure Desktop, where previously it was for the Supervisor Mode only.

There is a calculation based on a PIN number up to 5 digits, the day, the month, and the year using the Formula.

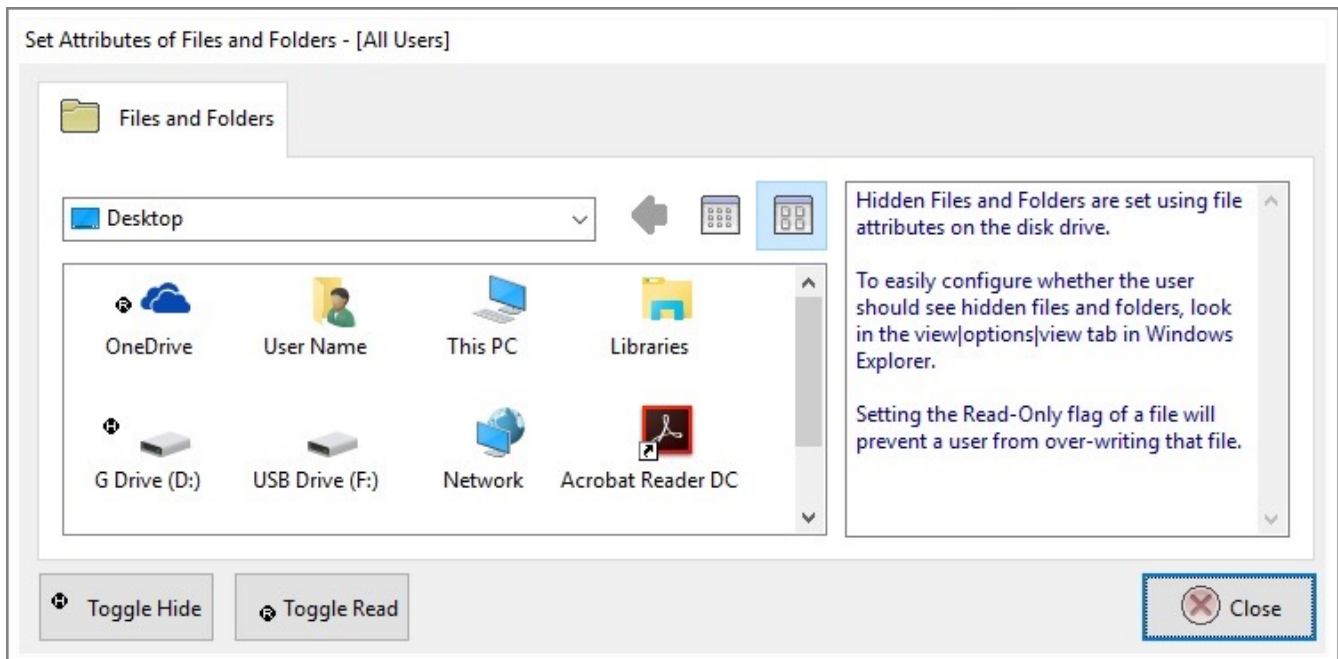
You have the choice of storing the PIN number in the INI file or in the registry. The registry location is

HKEY_LOCAL_MACHINE\SOFTWARE\Visual Automation\Secure Desktop\Version4.0\CalcNumber

For the items selected, the calculated password is appended to whatever text password is associated to that item.

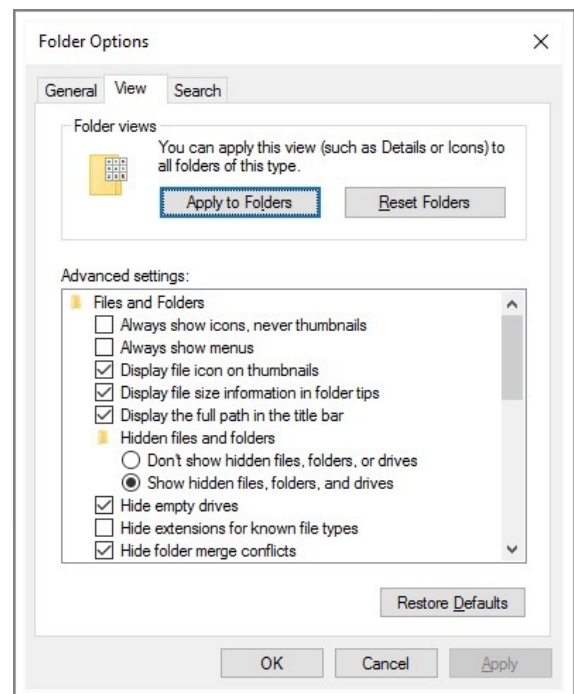
Example as follows:

- 1) Today is February 21, 2006.
- 2) My PIN number is 12345.
- 3) The Calculated number for this day would be $(2*21)+2+21+2006+12345$ which equals 14416.
- 4) If Supervisor was checked, and the text password was 'super', then when the user clicked on the Supervisor button, they would enter 'super14416'.
- 5) If Supervisor was not checked, they would just enter 'super'.
- 6) If All Tabs is checked, then every tab that has a password associated with it would have the 14416 number appended to the text configured with that tab.

**Administrator - All Users - Files**

Hidden Files and Folders are set using file attributes on the disk drive. To easily configure whether the user should see hidden files and folders, look in the Tools | Folder Options | View tab in Explorer.

Setting the Read-Only flag of a file will prevent a user from over-writing that file.



**Administrator - All Users - Logon – Ctrl-Alt-Delete Tab**

Logon - [All Users]

Ctrl-Alt-Delete **Automatic Logon** **Ctrl-Alt-Delete Screen**

Ctrl-Alt-Delete

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

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

☐ Disable Ctrl-Alt-Delete by re-mapping Delete and Win keys

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

Clear All **Default** **OK** **Cancel**

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

**Administrator – All Users – Logon – Automatic Logon Tab**

Logon - [All Users]

Ctrl-Alt-Delete **Automatic Logon** Ctrl-Alt-Delete Screen

☐ Automatic Logon Enabled

Default Domain Name:

Default User Name:

Default Password:

Automatic Logon Enabled determines whether the automatic logon feature is turned 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.

Automatic Logon Enabled determines whether the automatic logon feature is turned 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. If you are loading several network transport protocols, automatic logon might cause Windows 7/8/10 to attempt to connect to network resources before the protocols network transports are completely loaded.



Administrator – All Users – Logon – Ctrl-Alt-Delete Screen Tab

Logon - [All Users]

Ctrl-Alt-Delete Automatic Logon Ctrl-Alt-Delete Screen

Switch User ☒ Enabled ☐ Disabled Ease of Access ☒ Enabled ☐ Disabled

Disabling Ease of Access also disables Windows-U

Task Manager ☒ Enabled ☐ Disabled Shutdown ☒ Enabled ☐ Disabled

Disabling Task Manager also disables Shift-Control-Escape

Switch User can be disabled from Ctrl-Alt-Delete Dialog.
Utility Manager (XP/2003) or Ease of Access can be disabled from Ctrl-Alt-Delete Dialog.
The Task Manager menu item and the Shutdown menu item can be disabled.

OK Cancel

Ctrl-Alt-Delete Screen has two elements that can be disabled.


Disable Switch User. This setting is for all users, Switch User will no longer appear as an option if disabled.

Disable Ease of Access (Utility Manager in XP/2003). This will also disable the Windows-U keystroke combination.

The Task Manager menu item and the Shutdown menu item can be disabled.

**Administrator - User - Drives – Hide Drives Tab**

Drives - [SurfacePro4/User Name]

 **Hide Drives**

<input type="checkbox"/> A	<input type="checkbox"/> B	<input type="checkbox"/> C	<input type="checkbox"/> D	<input type="checkbox"/> E	<input type="checkbox"/> F	<input type="checkbox"/> G	<input type="checkbox"/> H
<input type="checkbox"/> I	<input type="checkbox"/> J	<input type="checkbox"/> K	<input type="checkbox"/> L	<input type="checkbox"/> M	<input type="checkbox"/> N	<input type="checkbox"/> O	<input type="checkbox"/> P
<input type="checkbox"/> Q	<input type="checkbox"/> R	<input type="checkbox"/> S	<input type="checkbox"/> T	<input type="checkbox"/> U	<input type="checkbox"/> V	<input type="checkbox"/> W	<input type="checkbox"/> X
<input type="checkbox"/> Y	<input type="checkbox"/> Z	<input type="checkbox"/> Network Neighborhood					

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. Login as each admin user, set the values, and remove the user from the Admin group as needed.

By checking on a drive letter, a registry value is set that removes the drives from file open and file save dialogs. These settings are on a user by user basis.

Clear All Default **OK** Cancel

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. Login as each admin user, set the values, and remove the user from the Admin group as needed.

By checking on a drive letter, a registry value is set that removes the drives from file open and file save dialogs. These settings are on a user by user basis.



Administrator - User - Logon – Ctrl-Alt-Delete Screen Tab

Logon - [SurfacePro4/User Name]

Ctrl-Alt-Delete Screen
 Auto Logoff

Lock Workstation
☒ Enabled ☐ Disabled

Change Password
☒ Enabled ☐ Disabled

Task Manager
☒ Enabled ☐ Disabled

Log Off
☒ Enabled ☐ Disabled

Shutdown
☒ Enabled ☐ Disabled

Disabling Lock Workstation also disables Windows-L

Disabling Task Manager also disables Shift-Control-Escape

The Windows Security dialog that comes up when you depress Ctrl-Alt-Delete has several buttons that you may want to disable.

The Task Manager, Change Password, Lock Workstation, Log Off, and Shutdown buttons can all be disabled.

You can disable Ctrl-Alt-Delete completely via the All Users Logon button in Windows XP/2003, but you may not be

Clear
 Default
 OK
 Cancel

The Windows Security dialog that comes up when you depress Ctrl-Alt-Delete has several buttons that you may want to disable.

The Task Manager, Change Password, Lock Workstation, Log Off, and Shutdown buttons can all be disabled.

Shutdown can not be disabled here in Windows 10, but you can disable it in the All Users section | Logon button | Ctrl-Alt-Delete Screen tab.

You can disable Ctrl-Alt-Delete completely via the All Users section | Logon button | Ctrl-Alt-Delete tab in Windows XP or Windows Server 2003, but you may not be able to due to conflicting GINA files. Even if you disable Ctrl-Alt-Delete, you may want to disable the 3 buttons, in case a user boots up in safe mode.



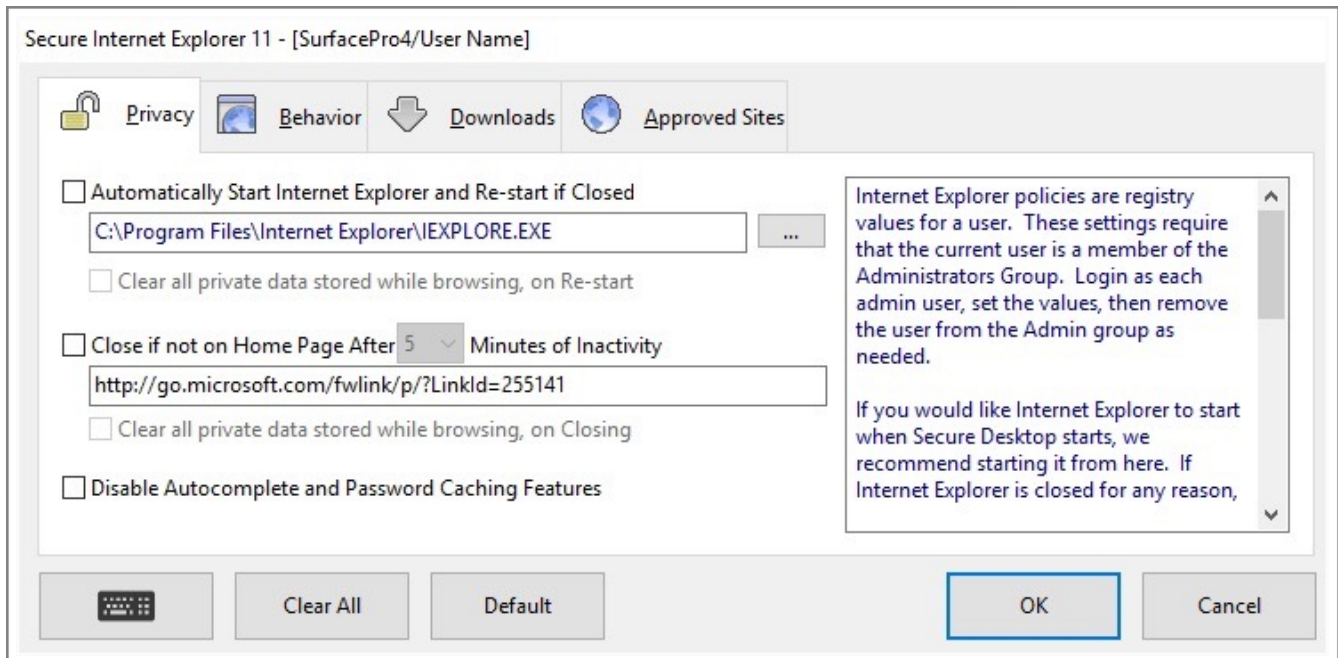
Administrator - User - Logon – Auto Logoff Tab

Secure Desktop includes a screen saver program that is not really a screen saver. Customers have requested the ability to automatically log off from Windows when there is not any user activity. To do this, we developed a screen saver program for Windows. Screen Savers are really just executable programs that are automatically launched when the specified number of minutes have passed without mouse or keyboard activity.

The Secure Desktop screen saver application simply displays a 10 second count down dialog with a cancel button, then it will perform a forced log off. This means that any un-saved work within an editor (Notepad, Word, Excel, etc.) will not be saved. Note that any services that you may be running will continue to run after a log off operation. The Secure Desktop screen saver application does not use the password feature.

This feature is primarily intended for customers who want to be sure that the logged in user is actually 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 number of minutes before starting after activity. Simply pick the screen saver as you would any other. Note that you will need to set the screen saver for each user.

**Administrator - User - Internet Explorer – Privacy Tab**

Internet Explorer policies are registry values for a user. These settings require that the current user is a member of the Administrators Group. Login as each admin user, set the values, then remove the user from the Admin group as needed.

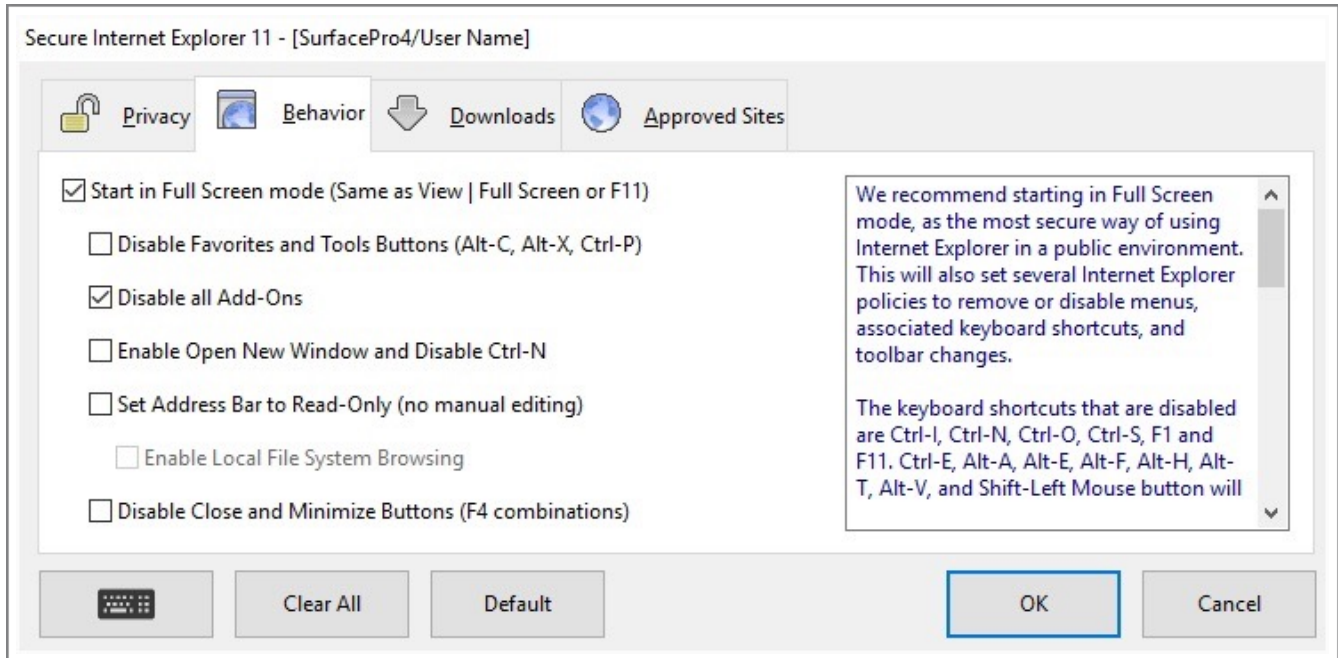
If you would like Internet Explorer to start when Secure Desktop starts, we recommend starting it from here. If Internet Explorer is closed for any reason, it will automatically re-start. Optionally, you can clear all private data when this happens, which includes internet address history, cookies, temporary internet files, and browser history.

If you are using 64-bit Windows, you can choose either the 32-bit or 64-bit version of Internet Explorer to run. The 32-bit version is in the Program Files (x86) folder.

You can automatically close all instances of Internet Explorer after a set number of minutes of inactivity when not on the home page. You can also clear all private data at that time. We recommend disabling all autocomplete and password caching features.



Administrator - User - Internet Explorer – Behavior Tab



We recommend starting in Full Screen mode, as the most secure way of using Internet Explorer in a public environment. This will also set several Internet Explorer policies to remove or disable menus, associated keyboard shortcuts, and toolbar changes.

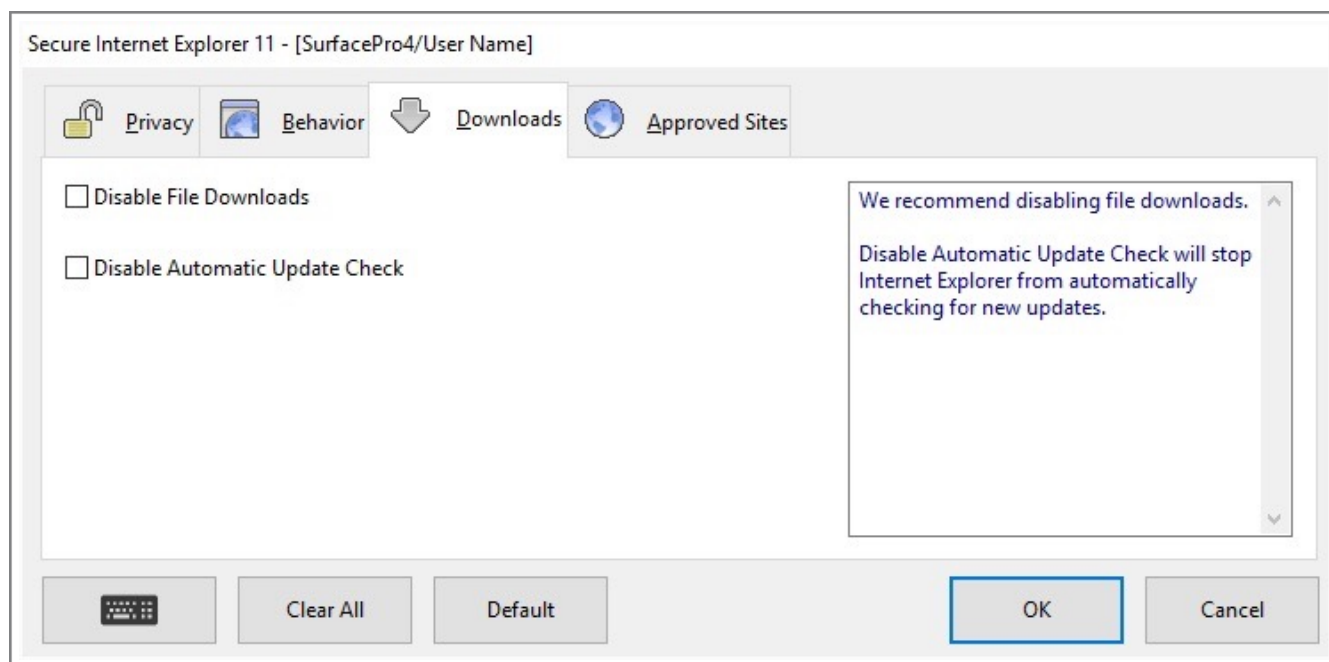
The keyboard shortcuts that are disabled are Ctrl-I, Ctrl-N, Ctrl-O, Ctrl-S, F1 and F11. Ctrl-E, Alt-A, Alt-E, Alt-F, Alt-H, Alt-T, Alt-V, and Shift-Left Mouse button will be disabled by Secure Desktop. Additional shortcuts disabled are Ctrl-D, F7, and F12. Disabling Favorites and Tools Buttons disables Alt-C, Alt-X and Ctrl-P. If Open New Window is enabled, allowing a web site to open a new window, then Ctrl-N is disabled.

Sometimes, you may want to use Internet Explorer for essentially one web site (the home page). If this is the case, you can choose to not display the internet address bar (URL) or set it to read-only. You can still view it, but no longer manually type into it. Local file browsing can be enabled if the URL is set for read-only.

The Close and Minimize buttons can be disabled. The Restore button is always disabled, to keep Internet Explorer in Full Screen mode. Alt-F4, Shift-Alt-F4, and Ctrl-F4 are disabled by Secure Desktop.



Administrator - User - Internet Explorer – Downloads Tab

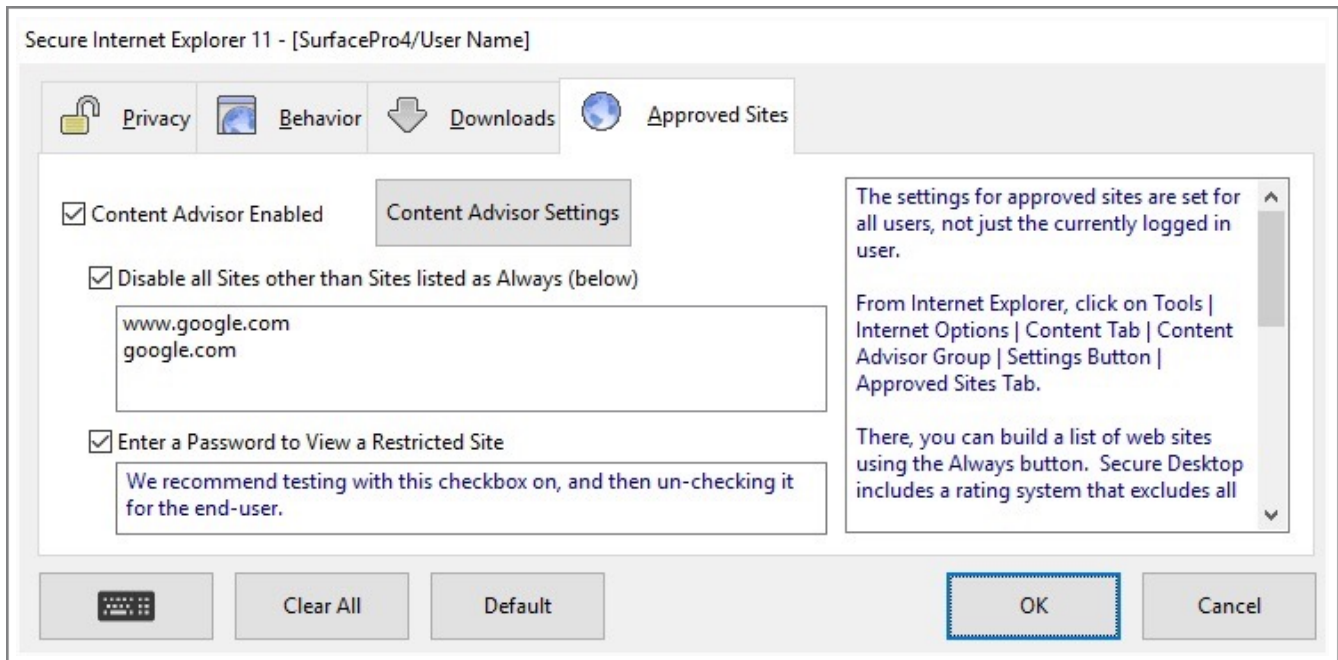


We recommend disabling file downloads.

Disable Automatic Update Check will stop Internet Explorer from automatically checking for new updates.



Administrator - User - Internet Explorer – Approved Sites Tab

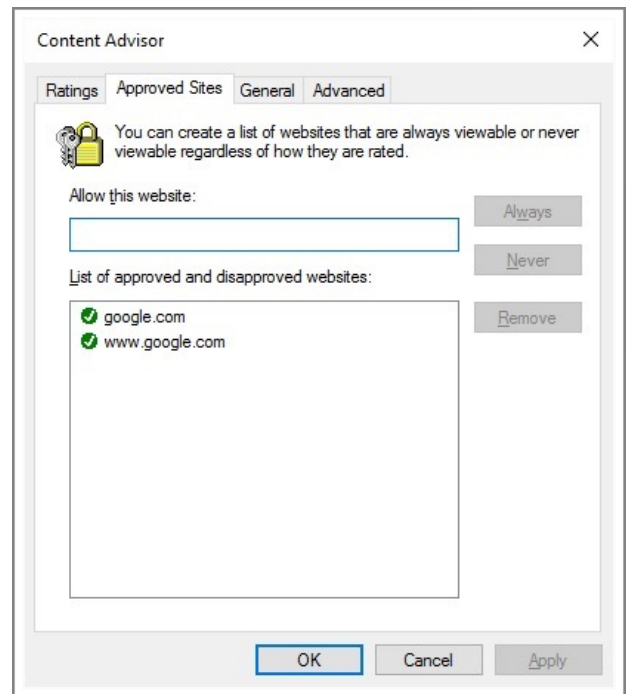


The settings for approved sites are set for all users, not just the currently logged in user.

Tap on the Content Advisor button to open the Internet Explorer Content Advisor, then tap on the Approved Sites Tab. There, you can build a list of web sites using the Always button. Secure Desktop includes a rating system that excludes all web sites other than those listed with the Always flag.

By checking the "Enter a Password to View a Restricted Site", you can build this list dynamically through testing. Then we recommend un-checking it, for the end user, to prevent password guessing.

Although this method of preventing web site use works most of the time, it does not work 100% of the time. Based on our testing, typing a URL or clicking on a normal <a href> kind of link in a web site should work fine. However, if a link is pushed from a script, it may not work. One example is a Google Advertisement.



Secure Desktop's Configuration sdesktop.xml File

All settings interfaced in the Secure Desktop system are saved in one XML file. This file would typically be found in:

Windows XP:

C:\Documents and Settings\All Users\Application Data\VisualAutomation\SecureDesktop\sdesktop.xml

Windows 7/8/10:

C:\ProgramData\VisualAutomation\SecureDesktop\sdesktop.xml

The XML file format is based on RSS 2.0. Audit files are also stored as XML/RSS 2.0 files, found in the same location, such as:

Windows XP:

C:\Documents and Settings\All Users\Application Data\VisualAutomation\SecureDesktop\sAudit RSS Monday 13 October 2008 UT.xml

Windows 7/8/10:

C:\ProgramData\VisualAutomation\SecureDesktop\sAudit RSS Monday 13 October 2008 UT.xml

The registry is modified for the system settings, to change the shell and other registry settings.

Windows Registry

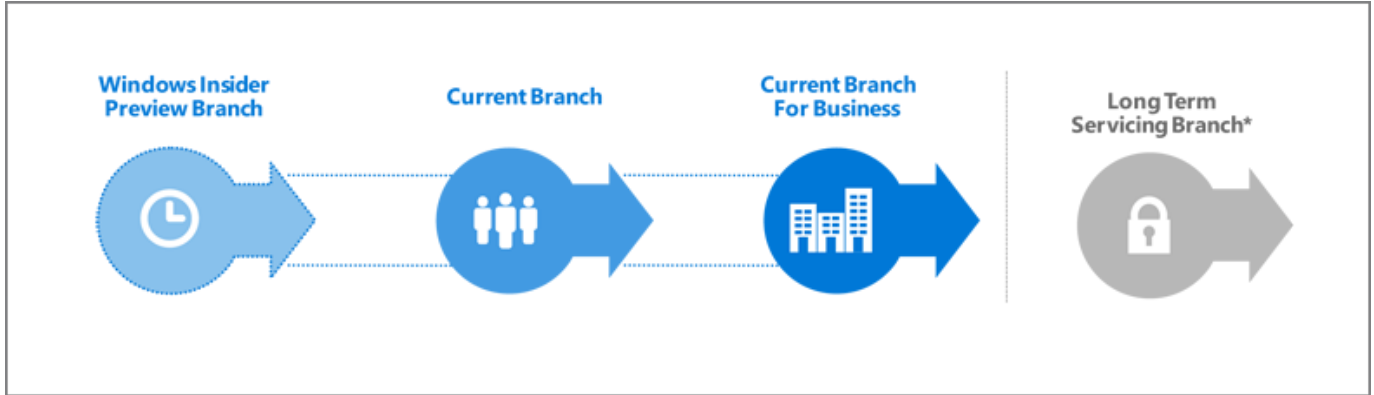
The registry contains the information necessary to change the shell application from Explorer.exe to sDesktop.exe. If you need to modify these settings manually, you will need to run RegEdit.exe. **USE CAUTION:** This is a database containing very important information about how your Windows system operates, modifying the wrong parameter could lead to nasty results. If you go to the key,

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

you will see the exe name of the shell. This will be either explorer.exe, vaprgman.exe (Secure Desktop 6), or sDesktop.exe (Secure Desktop 7/8/10).

Secure Desktop 10 automatically exports registry settings to *.TXT files in Windows 8 and Windows 10. Please see Manage Users - Registry Tab for more details.

Windows 10 Editions



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

“For critical or specialized devices (for example, operation of factory floor machinery, point-of-sale systems, automated teller machines), the Long-Term Servicing Branch (LTSB) provides a version of Windows 10 Enterprise that receives no new features, while continuing to be supported with security and other updates for a long time. (Note that the Long-Term Servicing Branch is a separate Windows 10 Enterprise image, with many in-box apps, including Microsoft Edge, Cortana, and Windows Store, removed.)” - Michael Niehaus, Microsoft

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

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

Classic Windows application and the Universal Windows app

Secure Desktop has always been designed for what is now called a Classic Windows application (CWA). These applications run on what is now called the Classic Windows Platform (CWP) (e.g., COM, Win32, WPF, WinForms, etc.).

A Universal Windows app (UWA) is a new kind of app for Windows 10 and is built to run on the Universal Windows Platform (UWP).

The Classic Windows Platform exists as a series of services, usually exe and dll files, that run independently of the Windows Explorer shell. The Windows Explorer shell and the Secure Desktop shell both provide the ability to run Classic Windows applications.

In Windows 10, the Universal Windows Platform is an integral part of the Windows Explorer shell. The Windows Explorer shell has to be running to launch and run a Universal Windows app. This is an unfortunate architectural choice.

Secure Desktop provides security by replacing the Windows Explorer shell. When Secure Desktop is set as the Windows shell, the Explorer shell is not running. Because the Explorer shell is not running, Secure Desktop can not run Universal Windows apps in any Edition of Windows 10.

Browsers

Secure Desktop has always been able to launch browsers that are designed as Classic Windows applications (CWA) such as Internet Explorer, Chrome, Firefox and Opera. We have specific features for Internet Explorer 11. Other CWA browsers will simply run "as is" or may be controlled slightly using the Windows Wizard.

Secure Desktop can not launch browsers that are designed as Universal Windows applications (UWA) such as Microsoft Edge.

Our Windows 10 Recommendation

Although Secure Desktop 10 may be used on any Edition of Windows 10, we strongly recommend consideration of the Windows 10 Enterprise LTSB Edition before making a final decision. Regardless of what Edition of Windows 10 you choose, Secure Desktop can not run Universal Windows apps. Based on our research we believe that Windows 10 Enterprise LTSB Edition may be the most secure and stable in a mission critical system.

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

Windows 11

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

Control Panel Tips

Although the Control Panel looks just like another group, it is really a parent application containing DLL calls to various Window's configuration functions. If you wish to execute just one of these icons within Control Panel, simply run the Control Panel followed by the icon name. For instance, to set the Date & Time, place the following in the Command Line:

```
C:\WINDOWS\CONTROL.EXE Date/Time
```

In some cases, this may not work. The *.CPL file can be specified on the command line also.

If you want to use the same icon, you can pull the icons from the different *.CPL files found in the Windows system directory. For example, the Date/Time icon is found in the MAIN.CPL file.

When you run an icon in this manner, nothing else is accessible in the Control Panel.

Secure Desktop includes a control panel program, called sControl.exe. With this program, you can run it with a /p to get the printers configuration only.

Explorer Tips

There may be a case where you want use Explorer type windows to display icons. You can display a "directory" or "folder" by specifying a command line of EXPLORER.EXE followed by the full directory path. This will allow the icons to be displayed in an explorer window, providing full access just like normal explorer mode, meaning icons and programs can be deleted, modified, etc. The following is a full definition of the explorer command line interface:

You can use the command-line switches for Windows Explorer in shortcut links or batch files, for example, to run Windows Explorer with a specified file selected.

Syntax

```
explorer [/n] [/e][,/root,object][[/select],subobject]
```

Parameters

/n - Always open a new window (even if the specified folder is already open).

/e - Use Windows Explorer view. The default is Open view.

/root,object

Specify the object in the normal namespace that will be used as the root of this Windows Explorer Folder. The default is to just use the normal namespace root (the desktop).

subobject - Specify the folder to receive the initial focus unless /select is used. The default is the root.

/select - Specifies that the parent folder is opened and the specified object is selected.

Windows Explorer Examples

To open a window rooted at \\myserver so you can easily browse the whole server, but nothing else:

```
explorer /e,/root,\\myserver
```

To open a folder window on C:\WINDOWS (or make an open window active) and select CALC.EXE, use:

```
explorer /select,c:\windows\calc.exe
```

sExplore.exe

Our sExplore.exe application is an alternative to using Explorer for file launching or document printing. Please see that section of the manual for more details.

File Open and File Save As Dialog Tips

It seems like nearly all programs running in Windows have a file open dialog and a corresponding file save as dialog. These dialogs are very helpful to the user in choosing files to open or where to save a file. In the course of making things easier, several features have been added to these dialogs that may cause a security breach.

Secure Desktop has several tools to try and prevent people from using these dialogs beyond the basic needs. The following features may help with this:

Secure Desktop Tools | Secure Desktop tab | Dialog button | File Open/Save As tab

Secure Desktop Tools | Administrator tab | [All Users] section | Files button | Files and Folders tab

Secure Desktop Tools | Administrator tab | [current user] section | Drives button | Hide Drives tab

Commenting on Visual Automation Products and Services

As we grow, we plan to expand our service on the basis of 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

(517)622-1850 sales/support

Technical Support Options

Calling technical support

Technical support is available via e-mail at support@visualautomation.com. You can also reach us by phone from Monday through Thursday, 9 am to 4 pm Eastern Standard Time, at (517)622-1850.

We can help you more quickly if you are at your computer, Secure Desktop is running, your Secure Desktop 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 original disk or e-mail.

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

Computer make and model.

Microsoft Windows version number (XP or Windows 7/8/10). Service Pack Number, if available. Internet Explorer version number, if appropriate.

Other hardware you are using.

Exact wording and number of error message (if applicable).