1st Security Center is a powerful security utility that allows you to restrict access to Windows important resources. This easy-to-use utility helps you to keep your computer in order. It enables you to impose a variety of access restrictions to protect your privacy. You can deny access to each individual component of several Control Panel applets, including Display, Network, Passwords, Printers, and System. You can disable your boot keys, DOS programs, Registry editing and network access. You have got an ability to hide your desktop icons, individual drives, Start menu items and the taskbar features, it enables you to stop others from tampering with your desktop. If you set up the special list of allowed applications nobody will run unwanted programs. 1st Security Center supports Internet Explorer security that enables you to customize many aspects of the Internet Explorer Web browser. It lets you disable individual menu items, prevent others from editing your Favorites, disable individual tabs in the Internet Options dialog, restrict access to the IE browser options. The administrator password prevents anybody to run the program and change settings and uninstall the program. The "Import/Export" function helps you set up the same settings on several computers very easy.

Security restrictions can be applied universally or just to specific users because 1st Security Center has got the multiuser intuitional interface.

The professional version "1st Security Center Pro" has got more security functions :

1. "Folders Guard" - helps you keep your files protected, you can choose who gets access to what files on your computer ;
2. "User Working Time" - allows you to limit working time for your children , office colleagues , students and so on ;
3. "Log User Activity" - you can log WHO and WHEN uses your computer to the special log file.

Download 1st Security Center Pro

1st Security Software Center

See also :

License
Quick Start
How to install
How to protect my PC more securely

Software Requirements:

- - Windows 95 or Windows 98 or Windows ME or Windows NT or Windows 2000 or Windows XP
- - Software for install is required: any zip-archive extractor like WinZip.

Hardware Requirements:

- - 486 CPU or higher
- - 16 Mb of RAM or more
- - 2 MB free disk space
- - VGA Video

See also :

License
Quick Start
How to install
How to protect my PC more securely

1st Security Center (R)

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT "LICENSE" CAREFULLY BEFORE INSTALLING THE SOFTWARE. BY INSTALLING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, YOU ARE NOT AUTHORIZED TO INSTALL THIS SOFTWARE.

1. License.

The software and any images accompanying this License whether on disk, in read only memory, or on any other media are licensed, not sold, to you by AUTHOR. YOU OWN THE MEDIA ON WHICH THE SOFTWARE IS RECORDED BUT AUTHOR RETAIN TITLE TO THE SOFTWARE. Software in this package and any copies that this License authorizes you to make are subject to this License.

2. Permitted Uses and Restrictions.

This License allows you to install and use the unregistered version of Software for a reasonable period of time for the purpose of determining whether Software is suitable for your needs. The use of full version of Software requires registration.

Except as permitted by applicable law and this License, you may not decompile, reverse engineer, disassemble, modify, rent, lease, loan, distribute, create derivative works from the Software or its component or transmit the Software over a networks.

A limited license is granted to all registered and unregistered users, webmasters, owners of distribution systems, BBS etc to copy and distribute unregistered Software only for the trial use of others, subject to the above limitations, and also the following:

Software and all of its release files must be copied in unmodified form, complete with the file containing this license information.

Your rights under this License will terminate automatically without notice from AUTHOR if you fail to comply with any term(s) of this License.

3. Limited warranty.

AUTHOR warrants that the SOFTWARE will perform in substantial compliance with the description supplied with the software product. If a significant defect in the product is found, there is possibility of a refund. In no event will such a refund exceed the purchase price of the product.

4. Disclaimer of Warranty on AUTHOR.

AUTHOR DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PRODUCT. SHOULD THE SOFTWARE PROVE DEFECTIVE, THE PURCHASER ASSUMES THE RISK OF PAYING THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION AND ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES. IN NO EVENT WILL AUTHOR BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING

WITHOUT LIMITATION DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION AND THE LIKE) ARISING OUT OF THE USE OR THE INABILITY TO USE THIS PRODUCT EVEN IF AUTHOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. Complete Agreement.

This License constitutes the entire agreement between the parties with respect to the use of the Software and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by AUTHOR.

1st Security Software Center

http://www.1securitycenter.com
E-mail: support@1securitycenter.com

See also :
Quick Start
How to install
How to protect my PC more securely

- Unpack the compressed archive file named like **1sc.zip** to the temporary folder and execute the setup.exe file.

See also :
License
Quick Start
How to protect my PC more securely

Use the following steps to uninstall 1st Security Center.

- Choose Settings ->Control Panel from the Start menu
- Open "Add/Remove" applet
- Select 1st Security Center item and click "Add/Remove" button.

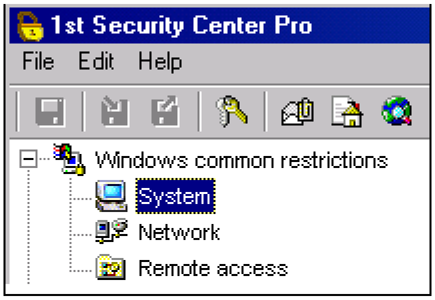
or

- Choose Programs -> 1st Security Center -> Uninstall 1st Security Center from the Start menu
- Follow the uninstall instructions.

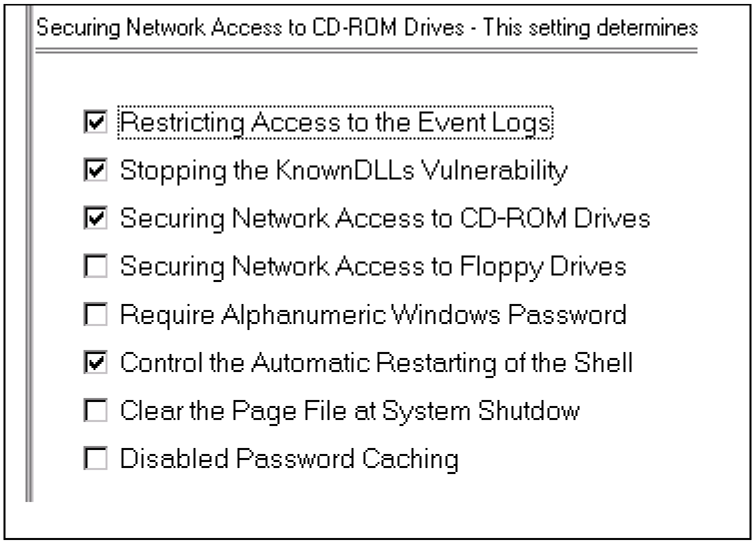
1. There are two kinds of restrictions : Windows common restrictions (these restrictions will affect all users of the computer) and Users Restrictions (you should select some user to set up restrictions).

2. Set up Windows common restrictions :

choose some item of Windows common restrictions



mark some check box to set up some restrictions



Securing Network Access to CD-ROM Drives - This setting determines

☑ Restricting Access to the Event Logs

☑ Stopping the KnownDLLs Vulnerability

☑ Securing Network Access to CD-ROM Drives

☐ Securing Network Access to Floppy Drives

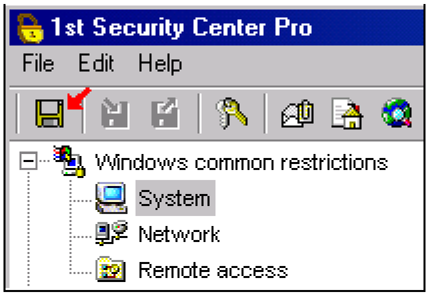
☐ Require Alphanumeric Windows Password

☑ Control the Automatic Restarting of the Shell

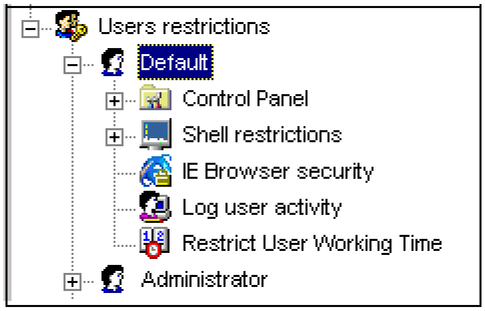
☐ Clear the Page File at System Shutdow

☐ Disabled Password Caching

save modifications



3. You should reboot computer to force modifications .
4. To set up Users Restrictions you should select some user , next select some restrictions item , set up restrictions, save modifications and reboot computer.



- Users restrictions
  - Default
    - Control Panel
    - Shell restrictions
    - IE Browser security
    - Log user activity
    - Restrict User Working Time
  - Administrator

See also :
License
Main menu - File
Administrator's password
How to protect my PC more securely

There are items : *Save,Import,Export* and *Exit*.

Save - use the "Save" menu item to apply modifications after you have set some restrictions or modify some settings ;

Import ... - use this function load user restriction settings from an external file ;

Export ... - use this function to save user restriction settings to an external file ;

Exit - use the "Exit" menu item to close the program.

See also :
Quick Start
Administrator's password

There is menu item : *Administrator's password .*

Administrator's password - use this menu item to define the administrator password. The administrator password prohibit users to run 1st Security Center and modify settings. Also the password doesn't allow to un-install program.
It's highly recommended to set the administrator password.

See also :
Quick Start
Main menu - File

There are menu items : *Help, IE Security Web page, Support e-mail* and *About...* .

Help - use this menu item to run and read this help file.

1st Security Center Web page - use this menu item to go to 1st Security Center Web page.

Support e-mail - use this menu item to run your default mailer program and send a letter to the support team. You may ask any questions, give us any suggestions and inform us about troubles and bugs. Please give us detailed information about problems and bugs.

Security Links - try another security tools from SSS Lab. Inc.

Windows Explorer add-ons - try new utility Magic Basket - it allows you to run only one instance of Windows explorer and see files in different folders at the same time.

About... - use this menu item to show information about 1st Security Center program.

See also :
Quick Start
Main menu - File
Administrator's password

These all system restrictions work for Windows NT/2000/XP only. These system restrictions will affect all users of the computer.

Restricting Access to the Event Logs - The Windows NT event log contains records documenting application, security and system events taking place on the machine. This tweak allows you to restrict access to administrators and system accounts only.

Stopping the KnownDLLs Vulnerability - In Windows NT, core operating system DLLs are kept in virtual memory and shared between the programs running on the system. This has exposed a vulnerability thatcould allow a user to gain administrative privileges on the computer the user is interactively logged onto.

Securing Network Access to CD-ROM Drives - This setting determines whether data in the CD-ROM drive is accessible to other users. This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media.

Securing Network Access to Floppy Drives - This setting determines whether data in the floppy disk drive is accessible to other users. This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media.

Require Alphanumeric Windows Password - Windows by default will accept anything as a password, including nothing. This setting controls whether Windows will require a alphanumeric password, i.e. a password made from a combination of alpha (A, B, C...) and numeric (1, 2 ,3 ...) characters.

Control the Automatic Restarting of the Shell - By default if the Windows NT user interface or one of its components fails, the interface is restarted automatically, the can be changed so that you must restart the interface by logging off and logging on again manually.

Clear the Page File at System Shutdown - Windows normally does not not clear or recreate the page file. On a heavy used system this can be both a security threat and performance drop. Enabling this setting will cause Windows to clear the page file whenever the system is shutdown.

Disabled Password Caching - Normally Windows caches a copy of the users password on the local system to allow for additional automation, this leads to a possible security threat on some systems. Disabling caching means the users passwords are not cached locally. This setting also removes the second Windows password screen and also remove the possibility of networks passwords to get out of sync.

See also :
Quick Start
Main menu - File
Administrator's password

Here are the network related restrictions. These network restrictions will affect all users of the computer.

Disable File and Printer Sharing - When "File and Printer sharing..." is installed it allows users to make services available to other users on a network, this functionality can be disabled by changing this setting. For Windows 9.x/ME/NT/2000/XP

Hide Share Passwords with Asterisks - This setting controls whether the password typed when accessing a file share is shown in clear text or as asterisks. For Windows 9.x/ME/NT/2000/XP

Disable Caching of Domain Password - Enabling this setting, disables the caching of the NT domain password, and therefore it will need to be re-entered to access additional domain resources. For Windows 9.x/ME/NT/2000/XP

Automatic Hidden Shares - This key controls whether the administration shares are created ie. c$ and d$. Set this option to disable admin shares for a server and for a workstation. For Windows NT/2000/XP

Disabling Save Password option in Dial-Up Networking - When you dial a phonebook entry in Dial-Up Networking (DUN), you can use the "Save Password" option so that your DUN password is cached and you will not need to enter it on successive dial attempts. This key disables that option. For Windows NT/2000/XP

Do not Display Last User Name - Enabling this key will blank the username box on the logon screen. Preventing people that are logging on from knowing the last user on the system. For Windows NT/2000/XP

Hiding Servers from the Browser List - If you have a secure server or workstation you wish to hide from the general browser list, use this option. For Windows NT/2000/XP

Restricting Information Available to Anonymous Logon Users - Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who want enhanced security have requested the ability to optionally restrict this functionality. For Windows NT/2000/XP

Disabled Password Caching - Normally Windows caches a copy of the users password on the local system to allow for additional automation, this leads to a possible security threat on some systems. Disabling caching means the users passwords are not cached locally. This setting also removes the second Windows password screen and also remove the possibility of networks passwords to get out of sync. For Windows 9.x/ME

Require Alphanumeric Windows Password - Windows by default will accept anything as a password, including nothing. This setting controls whether Windows will require a alphanumeric password, i.e. a password made from a combination of alpha (A, B, C...) and numeric (1, 2 ,3 ...) characters. For Windows 9.x/ME

See also :
Quick Start
Main menu - File
Administrator's password

Remote Access Security Settings will affect all users of the computer.

Disable Dial-In Access - It is possible for users to setup a modem on a Windows machine, and by using Dial-up Networking allow callers to connect to the internal network. Especially in a corporate environment this can cause a major security risk. For Windows 9.x/ME/NT/2000/XP

Disable "Automatically Use Dial-Up Networking to Logon" - There is an option that is available on the logon dialog box and allows you to dial into your logon server for authentication of your user account, this can be enabled by default. For Windows NT/2000/XP

Maximum Number of Remote Access Authentication Attempts - This setting controls the number of authentication retries before the remote access connection is terminated. For Windows NT/2000/XP

Maximum Time Limit for Authentication - A time limit can be enforced on the length of time given to logon via Remote Access. For Windows NT/2000/XP

Automatically Disconnect Remote Access Callers - Specifies the amount of idle time in minutes to wait before disconnecting the RAS client. For Windows NT/2000/XP

Define the length of time before callback is initiated - When callback is required or requested this setting defines how long to wait before initiating the callback connection. For Windows NT/2000/XP

See also :
Quick Start
Main menu - File
Administrator's password

For better security protection you need to modify some options in the system file MSDOS.SYS, since the program can't start in Safe Mode. These boot settings are available for Windows 9.x/ME only .

Set the following options to add these settings or to change existing settings in the section [Option] of MSDOS.SYS:

Disables interruption keys - sets BootKeys=0

By default Windows 9x enables the function keys on boot, these allow you to control the boot process. For example pressing F5 while the "Starting Windows 95..." message is displayed will boot Windows in Safe Mode. This option allows you to disable the F5, F6 and F8 keys. This option will affect all users of the computer.

Disables boot menu - sets BootMenu=0

If you installed an upgrade version of Windows 9x, you can normally press F4 to boot your previous version of Windows. This option can be disabled. This option will affect all users of the computer.

Disables the Safe Mode startup warning - sets BootWarn=0

Enabling the setting suppresses the safe mode warning message when booting up, and bypasses the Startup menu. This option will affect all users of the computer.

Require Validation by Network for Windows Access - By default Windows doesn't require a valid user name and password combination for a user to create and use a local Windows machine. This functionality can be changed to require this validation.

If your computer is connected to a network, make sure that the network is available and works properly, because validation of users will be done through the network. If the network is unavailable then you will not be able to access your computer. If you have a notebook computer, which you often disconnect from your corporate network, you should set the "Microsoft Family Logon" as a default way of logon in the network configuration. It will allow you to access to your computer outside the corporate network.

If your computer is not connected to a network then you need to create at least one user profile, and to assign a password for it. Make sure that the "Microsoft Family Logon" is enabled in the NetWork configuration and set as a current way of logon. To create a user profile, use the item "Users" in the "Control Panel". The "Microsoft Family Logon" will be automatically installed and enabled after creating the first user profile. If the "Microsoft Family Logon" is still not enabled, use the "Network" item in the "Control Panel" and install it by itself.

The "Microsoft Family Logon" is a network client, which is intended to emulate multi user access on a computer, when it is not connected to a real network.

WARNING: You should be carefully using the option "Require Validation by Network for Windows Access"

NOTE : You need to reboot the computer for these restrictions to come into force.

IMPORTANT: For the highest possible level of security in addition to the above settings it is necessary to make a change to the CMOS of your computer system. The Boot Order needs to be changed from A:then C:\ to C:then A:\. This prevents booting the system from a floppy boot disk unless the C:\ drive is non-functional. Use CMOS password protection to prevent unauthorized changes to this and other settings. Check the documentation that came with your computer for directions how to change your CMOS settings.

See also :
Quick Start
Main menu - File
Administrator's password

Display restrictions are available for Windows 9.x/ME/2000/XP

Disable display Control panel - This option disables the display settings control panel icon, and stops users from accessing any display settings.

Hide Background page - This option hides the background page, stopping users from changing any background display settings.

Hide Screen Saver page - This option hides the screen saver page from the display settings control, which stops users having access to change screen saver settings.

Hide Appearance page - This setting, once enabled, hides the display settings appearance page.

Hide Settings page - This option hides the Settings page from the display properties control.

See also :
Quick Start
Main menu - File
Administrator's password

Network restrictions are available for Windows 9.x/ME

Disable Network Control panel - Enabling this option disables access to the Network Control Panel icon.

Hide Identification page - The Network Identification page include options to set the Computer Name, Workgroup and Description, enabling this option disables access to the Network ID page.

Hide Access Control page - The Access Control Page, defines whether the computer support User-Level access or Share-Level access, enabling this option removes access to the Access Control Page.

See also :
Quick Start
Main menu - File
Administrator's password

Passwords restrictions are available for Windows 9.x/ME

Disable Passwords Control panel - This options disables access to the Passwords icon on the control panel, therefore stops users from changing security related settings.

Hide Change Passwords page - When this setting is enabled, users are no longer able to access the Change Passwords page.

Hide Remote Administration page - Hides the Remote Administration properties of Passwords in Control Panel.

Hide User Profiles page - the user profile page controls whether all users share or have separate user profiles, access to this page can be disabled by enabling this setting.

See also :
Quick Start
Main menu - File
Administrator's password

Printers restrictions are available for Windows 9.x/ME/2000/XP

Hide General and Details pages - This option hides the printer details and general printer information pages. Once enabled this option stops users from changing specific printer settings.

Disable Deletion of Printers - Printers can be deleted simply by any user pressing the delete key, enabling this setting stops users from being able to delete printers.

Disable Addition of Printers - Any user can add a new printer to their system, this option once enabled disables the addition of new printers to the computer.

See also :
Quick Start
Main menu - File
Administrator's password

System restrictions are available for Windows 9.x/ME

Hide Device Manager page - This setting controls whether the Device Manager, under Control Panel / System is visible.

Hide Hardware Profiles page - The settings when enabled hides the Hardware Profiles page from the System icon on the Control Panel.

Hide File System button - This option hides the File System button from the System icon on the Control Panel.

Hide Virtual Memory button - This option hides the Virtual Memory button from the System icon on the Control Panel.

See also :
Quick Start
Main menu - File
Administrator's password

This section enables you of choosing between 6 tabs used in Internet Options dialog and disable any of these tabs .

Hide General Tab - Hides General tab of Internet Options. See General tab of Internet Options. Option affects selected user, see the status bar. Applicable to Windows 9.x/ME/NT/2000/XP.

Hide Security Tab - Hides Security tab of Internet Options. See Security tab of Internet Options. Option affects selected user, see the status bar. Applicable to Windows 9.x/ME/NT/2000/XP.

Hide Content Tab - Hides Content tab of Internet Options. See Content tab of Internet Options. Option affects selected user, see the status bar. Applicable to Windows 9.x/ME/NT/2000/XP.

Hide Connections Tab - Hides Connections Tab of Internet Options. See Connections tab of Internet Options. Option affects selected user, see the status bar. Applicable to Windows 9.x/ME/NT/2000/XP.

Hide Programs Tab - Hides Programs tab in Internet Options. See Programs tab of Internet Options. Option affects selected user, see the status bar. Applicable to Windows 9.x/ME/NT/2000/XP.

Hide Advanced Tab - Hides Advanced tab of Internet Options. See Advanced tab of Internet Options. Option affects selected user, see the status bar. Applicable to Windows 9.x/ME/NT/2000/XP.

To get more security functions for IE Browser you should use the "Internet Explorer Security Pro" utility. Go to http://www.mybestsoft.com/iesec/index.html to get more info.

See also :
Quick Start
Main menu - File
Administrator's password
How to protect my PC more securely

Start Menu restrictions applicable to Windows 9.x/ME/NT/2000/XP

Remove the Run Command from the Start Menu - disallows the user to start applications or processes from the Start menu by removing the option completely.

Remove the Find/Search Command From the Start Menu - when enabled, this setting removes the "Find/Search"command from the Start Menu.

Remove the Favorites Folder from the Start Menu - removes the Favorites folder from the Start menu.

Remove the Recent Documents Folder from the Start Menu - removes the Recent Documents folder from the Start Menu.

Remove Common Program Groups from Start menu - disables the display of common groups when the user selects Programs from the Start menu. It also hides Open All Users and Explore All Users items in Start Menu context menu.

Hide Start Menu subfolders - set this when you use a custom Programs folder. Otherwise, two Programs entries will appear on the user's Start menu.

Remove "Folders Options" from Settings on Start Menu – removes the Folder Options option from Settings on the Start Menu, therefore stopping users from changing folder options.

Remove "Windows Update" from Settings on Start Menu – removes the Windows Update option from Settings on the Start Menu, therefore stopping users from unwanted updating your Windows.

Remove Folders from Settings on Start Menu – removes folders such as Control Panel, Printers and Faxes, and Network Connections from the Settings menu. These folders will disappear from My Computer as well.

Remove Taskbar and Start Menu from Settings on the Start Menu - removes the Taskbar and Start Menu option from Settings on the Start Menu, and stops users from changing the taskbar properties.

No Start Menu Context Menu - removes context menu from Start Menu. While this restriction is turned on, a user can not open Start Menu context menu using right mouse button for an item of the menu.

Disable LogOff command - this option allows you to stop users from being able to logging off the computer, by disabling the LogOff command.; displays explanation in a dialog box.

Disable Shut Down command - This option allows you to stop users from being able to shutdown the computer, by disabling the shut down command.; displays explanation in a dialog box.

Hide the Control Panel - this setting allows you to hide the Control Panel options from the Start Menu and deny access to it.

Hide Network and Dial-up Connections on Start Menu - this option allows you to hide the Network and Dial-up Connections option on the Start Menu and in Control Panel.

See also :
Quick Start
Main menu - File
Administrator's password

Desktop and TaskBar restrictions applicable to Windows 9.x/ME/NT/2000/XP

Hide All Items on the Desktop - this options hides all the items and programs on the Windows desktop.

Set Classic Shell - this option sets the classic view of Windows shell like the Windows 95 Desktop.

Disable Active Desktop - this option disables the use of the Active Desktop feature.

Don't Allow to Change Wallpaper - this option allows you to stop users from being able to change wallpaper.

Hide Desktop Context Menu - removes context menus from Desktop and Windows Explorer. While this restriction is turned on, a user can not open context menus for any items of Desktop and Windows Explorer using right mouse button or any other way.

Hide TaskBar Context Menu - removes context menu from Task Bar and System Tray Bar. While this restriction is turned on, a user can not open Task Bar and System Tray Bar context menu using right mouse button or any other way.

Remove File menu from Explorer - this option removes the File option from Explorer's toolbar.

See also :
Quick Start
Main menu - File
Administrator's password

Here you can customize Desktop, Favorites, Recent Documents, My Documents, Start Menu, Programs, Startup, Network Neighborhood and other Windows Shell Folders. Applicable to Windows 95/98/ME/NT/2000/XP.

Custom Programs Folder - These are the shortcuts that appear in the Programs group on the Start menu. This option customizes the contents of the Programs directory. Double click to select a path for the directory containing complete files or LNK files that define the Programs directory items.

Custom Desktop Icons - These are the shortcuts that appear on the desktop. This option customizes desktop icons. Double click to select a path for the directory containing complete files or LNK files that define the desktop shortcuts.

Custom Startup Folder - These are the programs or batch files that appear in the Startup group on the Start menu. This option customizes the contents of the Startup directory. Double click to select a path for the directory containing complete files or LNK files that define the Startup directory items.

Custom Network Neighborhood - These are the shortcuts to resources that appear in Network Neighborhood, including shortcuts to shared printers and files and to Dial-Up Networking connections. Customizes the contents of Network Neighborhood. Double click to select a path for the directory containing complete files or LNK files that define the Network Neighborhood items.

Custom Start Menu - These are the shortcuts and other options that appear on the Start menu, as defined by using the Taskbar Properties dialog box. This option customizes what is listed on the Start menu. Double click to select a path for the directory containing complete files or LNK files that define the Start menu items.

Custom Favorites - These are the shortcuts that appear in the Favorites group on the Start menu and in the Favorites of Internet Explorer. This option customizes the contents of the Favorites directory. Enter a path for the directory containing complete files or LNK files that define the Favorites directory items.

Custom Recent Documents - These are the shortcuts that appear in the Documents group on the Start menu. This option customizes the contents of the Recent directory. Enter a path for the directory containing complete files or LNK files that define the Recent directory items.

Custom My Documents - These are the shortcuts that appear in the My Documents folder. This option customizes the contents of the My Documents directory. Enter a path for the directory containing complete files or LNK files that define the My Documents directory items.

See also :
Quick Start
Main menu - File
Administrator's password

Hide the Network Neighborhood Icon from the Desktop - The Network Neighborhood/My Network Places icon is shown on the Windows desktop whenever Windows networking is installed, by enabling this setting the icon will be hidden. For Windows 95/98/ME/NT/2000/XP.

Remove Entire Network from Network Neighborhood - Entire Network is an option under Network Neighborhood that allows users to see all the Workgroup and Domains on the network. Entire Network can be disabled, so users are confined to their own Workgroup or Domain. For Windows 95/98/ME/NT/2000/XP.

Hide Workgroup Content from Network Neighborhood - this option hides all Workgroup content from being displayed in Network Neighborhood. For Windows 95/98/ME/NT/2000/XP.

Remove the Map and Disconnect Network Drive Options - Prevents users from making additional network connections by removing the Map Network Drive and Disconnect Network Drive buttons from the toolbar in Explorer and also removing the menu items from the Context menu of My Computer and the Tools menu of Explorer. For Windows 95/98/ME/NT/2000/XP.

Hide Computers Near Me in Network Places - this setting allows you to show or hide the computers listed Near Me in My Network Places. For Windows 2000/XP.

See also :
Quick Start
Main menu - File
Administrator's password

Disable registry editing tools - this setting disables user's ability to run Regedit.exe or Regedt32.exe to modify the registry. Be careful with this setting and make sure you don't lock yourself out of the registry. For Windows 95/98/ME/NT/2000/XP.

Disable the Autorun feature on all drives - determines whether the Autorun feature is enabled on each drive connected to the system. When Autorun is enabled, media is started automatically when it is inserted in the drive. For Windows 95/98/ME/NT/2000/XP.

Disable Task Manager - enables or disables the user's ability to start Task Manager to view processes, applications running, and make changes to the priority or state of the individual processes. For Windows NT/2000/XP.

Disable the Lock Workstation Button - this setting stops unauthorized users from locking machines from the Windows NT Security dialog box. For Windows NT/2000/XP.

Disable the Change Password Button - this setting disables the "Change Password" button on the Windows NT Security dialog box. For Windows NT/2000/XP.

Don't save settings at exit - Normally when Windows exits it saves the desktop configuration, including icon location, appearance etc. This setting disables these changes from being saved, this is useful in both a secure environment and when you don't want people to change the appearance of your desktop once you have it setup the way you like it. This option is enabled in Win95 only.

No System Key Combinations - this restriction prohibits users from using the system key combinations Ctl-Alt-Del, Alt-Tab, Ctrl-Esc. For Windows 9.x/ME .

See also :
Quick Start
Main menu - File
Administrator's password

You can prevent users from running any Windows-based applications except those that are listed. Use the "Add" and "Delete" buttons to add/remove applications to/from the list. Be carefully with this powerfull feature , because you might disable some useful system applications. Also remember that Windows will check up file names only.

See also :
Quick Start
Main menu - File
Administrator's password

Disable MS-DOS prompt - This setting allows you to disable the use of the MS-DOS command prompt in Windows. After setting this restriction up all applications, which use the command prompt will be disabled. For Windows 9.x

Disable single-mode MS-DOS applications - This setting allows you to disable the use of real mode DOS applications from within the Windows shell. For Windows 9.x

See also :
Quick Start
Main menu - File
Administrator's password

Here you can disable many Internet Explorer browser functions.

Disable "Add-Favorite dialog" - No Favorites menu, adding to favorites, or organizing favorites.

Disallow users to download files from Internet by using the option **"Disable Files Downloading"**.

The "Disable Context Menu - Disable right-click menu" option enables you to hide the HTML context menu.

Disable Form Autocomplete - Disables AutoComplete for forms.

Disable Password Autocomplete - Prevents Prompt me to save password from being displayed.

Disable Toolbar Customization - Disables the function to customize toolbar in Internet Explorer.

Disable the "Open" item of the "File-menu" - Disables Open command on File menu, CTRL+O, and CTRL+L.

Disable the "New" item of the "File-menu" - Disables CTRL+N

Disable the "Save As" item of the "File-menu" - Disables Save and Save As on the File menu.

Disable the "Close" item of the "File-menu" - Disables ALT+F4.

Disable the "View Source" item of the "View-menu" - prevents viewing the context of web pages.

Disable the "Internet Options" item of "Tools-menu" - Disables Internet Options on the Tools menu (disables changing browser settings).

Disable the "Windows update" item of "Tools-menu" - Disables an ability to update Windows from Internet.

To get more security functions for IE Browser you should use the "Internet Explorer Security Pro" utility. Go to http://www.mybestsoft.com/iesec/index.html to get more info.

See also :
Quick Start
Main menu - File
Administrator's password
How to protect my PC more securely

If you are a registered user of **1st Security Center Pro** you may upgrade at no charge to any newer release. Just download the latest shareware release of **1st Security Center Pro** and install it without uninstalling the previous version (don't forget close previous version of **1st Security Center Pro** if running). This will preserve your registration. If the registration code is no longer present on your system just re-enter it like the first time and restart the program.
You can download the latest shareware release of **1st Security Center Pro** from downloads page

We always value your input. Please send us your suggetions and feedbacks.
You can reach us at following:

- E-Mail:

  Technical support: support@1securitycenter.com

- Internet

  Main website:
  http://www.1securitycenter.com

  Technical support:
  http://www.1securitycenter.com/mainsup.html

  On-line Registration:
  http://www.1securitycenter.com/sc/order.html

For normal usage with optimal security you should register the copy of **1st Security Center Pro**. You may use the unregistered copy of **1st Security Center Pro** for 30 days only. After that testing period, you have to register or uninstall the program.

For registering your copy of **1st Security Center Pro** you should go to :

http://www.1securitycenter.com/sc/order.html

and choose one of the several methods for registration:

Online ordering
Phone & fax orders
Paying by Check via Postal Mail

Download security utilities

1st Security Center Pro - to really protect your computer you have to use the professional version. It has got more useful security functions. The powerful feature "User Working Time" allows you to limit working time for your children , office colleagues , students and so on. You can define several time intervals and time durations to manage users working time very easy.
New feature "Folders Guard" can help you keep your files protected. You can choose who gets access to what files on your computer. This program provides two levels of protection to suit any user : "Hidden" and "Read Only". It works with Network folders and fully supports protection of removable media (such as floppies, CD Roms, DVD, ZIP and some SCSI and RAID drives).
Try also more additional features.
It works with any Windows platforms : 9.x / ME / NT / 2000 / XP .

You should try another security utilities from **Security Software Solutions Laboratory** too :

Download security utilities

Internet Explorer Security Pro - Internet Explorer Security is an utility that customizes many aspects of the Internet Explorer Web browser. It's a snap to use and provides the tools you need to retain and manage your Web browser settings. It lets you disable individual menu items and prevent others from editing your Favorites. It also allows you to disable individual tabs in the Internet Options dialog, as well as specific settings from each tab. Still other settings let you change the title caption, toolbar background, and animated icon; change default folders; and replace standard error information pages. It allows you to manage security zones very easy. The powerful "Web Spy" feature enables you control web sites which users may view. Multiuser support and password protection are also offered.
It works with any Windows platforms : 9.x / ME / NT / 2000 / XP .

Download security utilities

Dark Files can help you keep your files protected. You can choose who gets access to what files on your computer. This program provides three levels of protection to suit any user : "Hidden", "Read Only", "Full Control". It works with any Windows platforms : 9.x / ME / NT / 2000 / XP . Dark Files can work with Network folders and fully supports protection of removable media (such as floppies, CD Roms, DVD, ZIP and some SCSI and RAID drives) on all platforms.

This easy-to-use program allows you to protect your files and folders (including subdirectories) in various ways. You can hide them or prevent others from deleting, renaming, executing, or modifying your files in any way. The Wildcard feature allows you to specify which files you want to protect (for example, all EXE or DLL files). The file system protection works independently of the program , so if you even close the program the file protection will still work.

Built-in support for multiple user interface allows you to use Dark Files without any change on multi user systems. You can define own settings for each user separately or just define settings for the "Guests group" . If your computer is configured for using by multiple users you can define the list of protected folders separately for each user. If some user has not got own settings the program will apply settings of the "Guests group" to that user.

If you are looking for a solid file protection program, look no further.

Download security utilities

Security Department is a resident file system protector for Windows 95 and Windows 98. It provides several levels of protection for different folders and files. You can prevent various actions for folders and files: copying, moving, deleting, renaming and so on. In addition to the two standard protection levels

"Read Only" and "Full protection", there is the Custom Protection level that allows you to fine tune the access of specific folders and files. Access to various folders and files can also be set differently for each user on a single PC. By employing Security Department a computer is provided with an additional level of protection from virus and internet hacker attacks. Security Department makes EXE and COM files truly Read-Only. There is not a single virus that can overcome this kind of protection. Young children deleting your files, emails, or important documents? Is your office computer vulnerable to others reading your mail or industrial espionage? Put a stop to all this right now! You can resolve these and other access problems by using Security Department.

Download security utilities

Before you contact us, please do the following:
1. Look at the help file and FAQ: it may already contain an answer to your question. A lot of people ask us something like "how do I...", even though the complete information is there.
2. Visit our downloads page. There is a good chance that you'll find the newest version of program there. If the serious bug has been found in the program, but the new version is not ready yet, we will make the hot fix for it.
But if you still have a problem with program and nothing else helps, please contact our technical support.

All users (registered and unregistered) can get technical support at any time. But registered users will have the advantage of a quicker response.
We welcome your suggestions and notices about problems. You may contact us via the following e-mail address:

support@1securitycenter.com

Ask for Eugene Mihailov .

Please let us know the following information :

· What Windows version do you use ?
· What version of the program do you use ?
· Have you installed any service packs?
· Network configuration (What network clients are available and how is the default logon set).
· What user restrictions and program options are set up ?
· Description of your problem (with as many details as possible).

Related Topics: FAQ's

Q1: Can I copy 1st Security Center settings to more than one computer?
A1: You should use the "Export/Import" functions under the "File" menu item .

Q2: What should I do if I have locked myself out ?
A2: You should contact the support team to get instructions how to unlock the computer .

Q3: Are there any education discounts?
A3: Yes. Discounts for education organizations there are. Please contact us to get addition info.

Q4: Are there any localizations of the program in other languages?
A4: Now not. You can translate pragram interface to your language and receive a **free registration**!

We welcome your questions and suggestions. Some of questions, tips and tricks we will put to the FAQ section.
Thanks.

See also :
Quick Start
Main menu - File
Administrator's password
How to protect my PC more securely