



NetSupport Protect User Guide

**All Rights Reserved
©2006 NetSupport Ltd**

Contents

Welcome to NetSupport Protect	3
Product Overview.....	4
Key Features at a Glance	5
System Requirements	6
The User Interface	7
Using NetSupport Protect.....	9
The Summary Dialog.....	9
Folders.....	10
System	12
Desktop	13
Applications	15
Network	16
Devices	18
Users	19
Settings	20
Save Configuration.....	21
Contact Us.....	22

Welcome to NetSupport Protect

NetSupport Protect is the number one choice of technology coordinators and teachers to protect Windows® operating systems and desktops from unwanted or malicious changes.

NetSupport Protect provides a secure, reliable and productive computer environment in the classroom. With its extensive list of security features and intuitive format, teachers and administrators can use NetSupport Protect to guarantee that students are getting the most beneficial use of their computer learning experience.

NetSupport Protect prevents users from deleting critical files and applications, making unauthorised changes to the desktop, saving unwanted programs and corrupting the operating system.

With NetSupport Protect, you can feel confident that unauthorised changes to a system, whether accidental or malicious, won't become an issue or impact on the productivity of your computer lab.

Product Overview

As schools continue to provide better access to computer hardware, networks, and web resources, district IT staff and classroom teachers face new challenges. IT staff must manage the challenges posed by computer labs and school networks as well as control software deployment and user issues.

Teachers need to manage students who are using computers in a lab or multi-desktop classroom to ensure that they are learning and spending time on their assigned tasks.

Children want to learn, and often the best way is to experiment. Unfortunately lab computers may be used four or five times a day for different classes, so you really can't afford for them to endure too much practical experimentation.
















NetSupport Protect provides a proactive, rather than reactive solution to the challenges faced. The philosophy of the product is to prevent changes to the desktop environment and avoid the need to rely on "repair" based solutions that are more costly and have a greater maintenance overhead.

Using NetSupport Protect, IT staff can create a secure desktop environment where system configuration and access from external sources are protected, where students can use available applications but are shielded from system resources and the temptation of investigating the workings of the desktop.

Key Features at a Glance

Simple to use, safe, and secure, NetSupport Protect is the ideal choice of technology coordinators and teachers. Presented in a simple and intuitive interface, system control can be configured in minutes and allows central control of settings.

Key feature highlights in NetSupport Protect are:

-  Hide folders and restrict creation of defined file types.
-  Restrict changes to the desktop, taskbar and system settings.
-  Restrict shutdown, logoff, lock and password changes.
-  Protect the operating system and computer settings.
-  Lock control panels, task manager, command prompt and registry.
-  Restrict user-defined applications from running.
-  Restrict available network drives, drive mappings and network neighborhood.
-  Prevent access to windows systems tools
-  Prevent web browsers from running.
-  Restrict changes to the system printers.
-  Control access to USB and CD/DVD drives.
-  Disable USB devices, allow read only or prevent application launch.
-  Prevent users from installing unauthorized software.
-  Apply policies to all users, or exclude specified accounts.
-  Share security configurations across a network.

System Requirements

IBM compatible Pentium III or higher with 256Mb RAM.

15Mb free disk space.

Windows 2000 or higher.

The User Interface

NetSupport Protect's easy to navigate interface means that the required level of system protection can be achieved in a matter of seconds.





Options are conveniently grouped into 6 main categories with the Summary option providing a colour-coded overview of the level of security currently applied to each. To access each category simply click the appropriate toolbar button or select the required group from the Summary dialog.

The Users option enables System Administrators to specify whether particular users are exempt from having protection applied. This is particularly useful where multiple users have access to the same PC.

In order to secure the configuration, ensuring that only appropriate personnel can edit the information, the Settings option provides two levels of password protection. Administrator level enables the user to load the NetSupport Protect Configuration, lock/unlock the system and amend the protection options. Manager level allows you to lock/unlock the system, in order to gain full access to programs etc but not change any of the protection options. The Status Bar indicates whether the system is currently locked or unlocked.

Unlocking the system provides administrators with a convenient method for temporarily lifting protection without physically changing any of the individual settings. This can be useful for testing the configuration while editing.

Click  to switch between locked and unlocked status.

Click  to refresh the configuration when changes have been made.

Note: If the Status Bar is 'greyed out' it means the NetSupport Protect service is not running.

Once the required settings are in place configurations can be saved to the local machine or to a network share for others to access.

Using NetSupport Protect

The Summary Dialog

A colour coding system provides a quick reference summary as to the current protection status of each category.



Red None of the options within this category are protected.

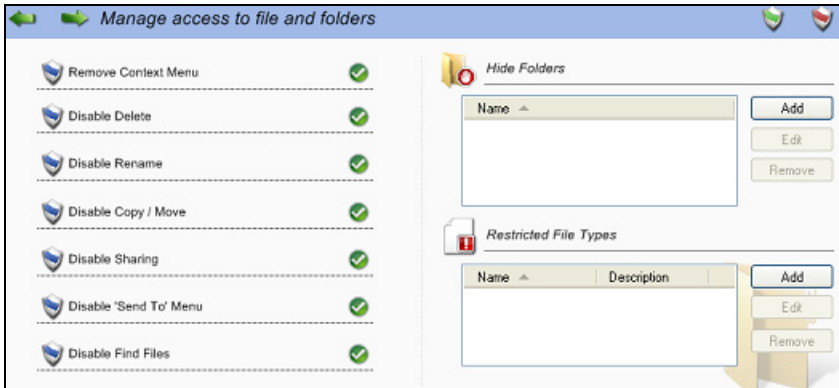
Amber Some of the options are protected.

Green All options are protected.

Click on the required category or select an icon on the toolbar to amend items.

Folders

These options enable you to manage the tasks that can be performed on files and folders stored on the PC. Potentially dangerous tasks can be disabled, specific folders can be hidden and access to certain file types can be blocked.



Remove Context Menu

The options normally available to users when right-clicking on a file or folder will be removed.

Disable Delete

Prevents users from being able to delete files and folders.

Disable Rename

Prevents users from being able to rename files and folders.

Disable Copy/Move

Prevents users from being able to copy or move files and folders.

Disable Sharing

Removes the ability to share folders.

Disable 'Send To' Menu

Disables the 'Send To' Mail Recipient, Disk etc facility.

Disable Find Files



Prevents the user from being able to search for files.

Hide Folders

Enables you to specify details of any folders that should be hidden from users. Click Add to specify the path for each folder.

Restricted File Types

Blocks access to certain types of file. Click Add to specify the file extension (exclude the .).

Clicking  or  turns protection on/off for all options.

System

Controls access to various system utilities.



Windows Update

Prevent users from running Windows Update.

Windows Installer

Prevent users from running Windows installers.

Shutdown

Prevent users from shutting down the system.

Log off


Prevent users from logging off.

Lock Workstation

Prevent users from locking the workstation.

Change Password

Prevent users from changing passwords.

Clicking  or  turns protection on/off for all options.

Desktop

Manage the access users have to the 'Start' menu or taskbar options.



Start Menu Options

Disable Properties

Prevents access to the Properties option from the 'Start' menu and the taskbar.

Disable Context Menu (not win2000)

Prevent modifications to 'Start' menu items.

Remove 'All Programs' (not win 2000)

Remove the 'All Programs' option from the 'Start' menu.

Remove 'Program Access and Defaults'

Prevents access to the 'Set Program Access and Defaults' option.

Remove 'Recent Documents'

Remove 'Documents' option from the 'Start' menu.

Remove 'Run'

Remove the 'Run' option.

Task Bar Options

Disable Context Menu

Remove the taskbar context menu when right-clicking.

Disable Unlock (not win2000)

Prevents the taskbar from being locked or unlocked.

General

Favourites Menu


Remove the 'Favourites' item from the 'Start' menu.

Change 'My Documents' Path

Prevent users from changing the path for the 'My Documents' folder.

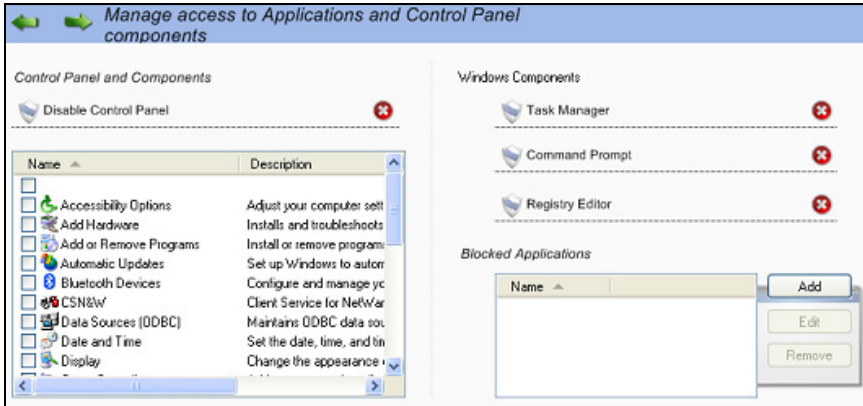
Create Shortcut

Prevent users from being able to create desktop shortcuts.

Clicking  or  turns protection on/off for all options.

Applications

Enables you to disable Control Panel and restrict access to applications and Windows components.



Control Panel and Components

Access to Control Panel can be completely disabled or you can remove individual components by checking the appropriate options in the list.

Windows Components

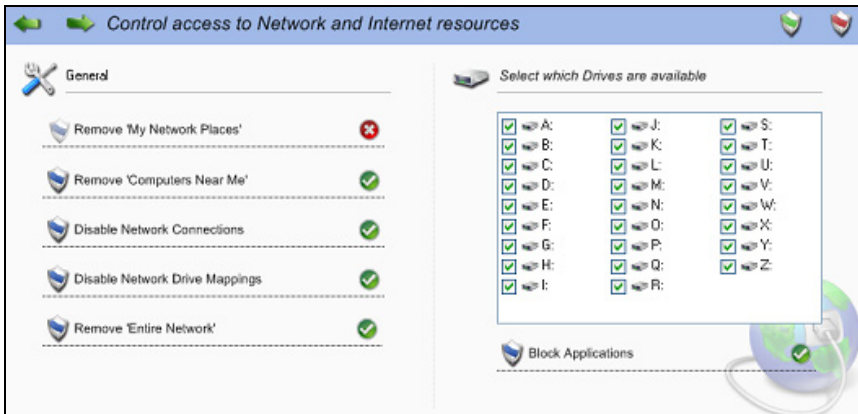
Remove access to Task Manager, the Command Prompt and Registry Editor.

Blocked Applications

Prevent users from accessing specific applications. Click Add to browse for the required exe files.

Network

Control access to network and internet resources.



Remove 'My Network Places'

Remove the 'My Network Places' icon from the desktop.

Remove 'Computers Near Me'

Removes the 'Computers Near Me' Icon and the icons representing the computers in the workgroup.

Disable Network Connections

Prevents users from accessing the 'Network Connections' option. Removes the option from Control Panel.

Disable Network Drive Mappings

Prevents users from being able to create or remove network drive mappings.

Remove 'Entire Network'


Remove access to computers outside the users workgroup or local domain.

Disable Network Drives

Determine which drives are available to the user. Uncheck those to be hidden.

Block Applications

Prevents the user running applications stored on a network share even if the Network Drive itself is available.

Clicking  or  turns protection on/off for all options.

Devices

Control the use of peripheral devices. Protect your systems against users trying to install damaging materials from memory sticks or CD.



Printers



Prevent users from adding and deleting local or network printers.

USB Mass Storage Access

You can block the use of external storage devices or prevent files being written to a device and block applications being run from the device.

CD/DVD Drive Access



Disable the CD/DVD drive or prevent applications being run from a disk.

Clicking  or  turns protection on/off for all options.

Users

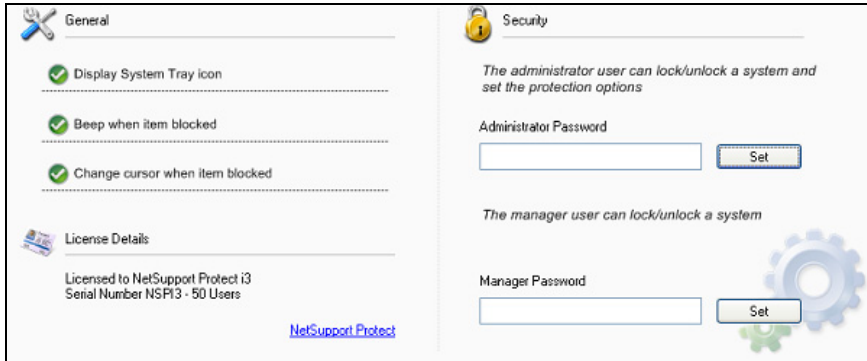
Create a list of users to whom protection does not apply. Click Add to enter the users login name.

These users will not have any protection applied when they log in

Name ▲	
 ABCDEF	<input type="button" value="Add"/>
 GHIJKL	<input type="button" value="Edit"/>

Settings

Enables you to set NetSupport Protect preferences.



General

Display System Tray Icon

If required, the NetSupport Protect tray icon can be hidden.

Beep when item blocked

An audible warning can be sounded if a user attempts to use an option that is blocked.

Change cursor when item blocked

To indicate to the user that a task is blocked you can display the NetSupport Protect shield logo.

License Details

Provides details of your NetSupport Protect license.

Security

Two levels of password can be assigned to users who need to access the NetSupport Protect Configuration:

Administrator - Enables the user to toggle between locked and unlocked status and change protection options.

Manager - Enables the user to toggle between locked and unlocked status in order to use the system without protection being in play but they do not have authority to change any of the protection options.

Save Configuration

Once all the relevant protection settings are in place, the configuration can be saved locally or to a network share for multiple users to access.

<p><input checked="" type="radio"/> Standalone</p> <hr/> <p>Save the configuration file locally for this computer to use</p> <p><input type="button" value="Save"/></p>	<p><input checked="" type="radio"/> Remote</p> <hr/> <p>Save the configuration file on a network share so that multiple computers can use it</p> <p>Path</p> <p><input type="text"/> <input type="button" value="Browse"/></p> <p>Security Credentials</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Confirm <input type="text"/></p> <p><input type="button" value="Save"/></p>
---	---

Contact Us

UK & International

www.netsupportsoftware.com

Technical Support: *support@netsupportsoftware.com*

Sales (UK & Eire): *sales@netsupportsoftware.co.uk*

Sales (International): *sales@netsupportsoftware.com*

North America

www.netsupport-inc.com

Technical Support: *support@netsupport-inc.com*

Sales: *sales@netsupport-inc.com*

Germany, Austria and Switzerland

www.pci-software.de

Technical Support: *support@pci-software.de*

Sales: *sales@pci-software.de*

Japan

www.pcip.co.jp

Technical Support: *support@pcip.co.jp*

Sales: *sales@pcip.co.jp*