



NetSupport Protect

Product Manual – Version 2.10

Manual COPYRIGHT (C) 2014 NetSupport Ltd. All rights reserved.

Information in this document is subject to change without notice. NetSupport Ltd reserves the right to revise this document and to make changes from time to time in the content hereof without obligation to notify any person or persons of such revisions or changes.

The software described in this document is supplied under a licence agreement and is protected by international copyright laws. You may copy it only for the purpose of backup and use it only as described in the Licence agreement.

Any implied warranties including any warranties of merchantability or fitness for a particular purpose are limited to the terms of the express warranties set out in the licence agreement.

Program COPYRIGHT (C) 1991-2014 NetSupport Ltd. All rights reserved.

Trademarks

NetSupport is a registered trademark of NetSupport Ltd.

Windows, Windows 2003/2008/XP/Vista, Windows 7 and 8 are trademarks of Microsoft Corporation.

Other products, trademarks or registered trademarks are the property of their respective owners.

Software Licence Agreement

Please read this agreement before using your copy of NetSupport Software. This is a legal agreement between you and NetSupport Ltd. If you do not wish to be bound by the terms of this licence agreement you must not load, activate or use the software.

TERM: Subject to termination under Termination Clause below the licence shall be perpetual.

GRANT OF LICENCE: Subject to the payment of the applicable licence fees, and subject to your abidance by the terms and conditions of this agreement, NetSupport Ltd hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the software which you have acquired.

USE: The software is licensed with volume use terms specified in the applicable order acknowledgement, product invoice, licence certificate or product packaging. You may make, install and use as many additional copies of the software on the number of devices as the terms specify. You must have a reasonable mechanism in place to ensure that the number of devices on which the software has been installed does not exceed the number of licenses you have obtained.

SERVER USE: To the extent that the applicable order acknowledgement, product invoice, product packaging or licence certificate sets forth, you may use the software on a device or on a Server within a multi-user or networked environment ("Server Use"). A separate licence is required for each device or "seat" that may connect to the software at any time, regardless of whether such licensed devices or seats are connected to the software concurrently, or are actually using the software at any particular time. Your use of software or hardware that reduces the number of devices or seats that connect to and use the software directly or simultaneously (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required. Specifically, you must have that number of licenses that would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of devices or seats that can connect to the software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the software does not exceed the use limits specified for the licence you have obtained.

COPYRIGHT: This software is protected by international copyright laws. You may copy it only for backup purposes. The software is licensed to you, but not sold to you.

RESTRICTIONS: Neither you nor any reseller may rent, lease, sell licensed copies [on approval], or otherwise transfer the right to use this software to another person, except that you may sell or give away your original copy, as long as you do not keep any copies. The software may not be modified, disassembled or reverse engineered except with the prior written consent of NetSupport Ltd.

LIMITED WARRANTY: NetSupport Ltd warrants that the software will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of purchase. NetSupport's entire liability and your exclusive remedy shall be either a) the replacement of the defective software or b) return of the price paid. This remedy shall be at NetSupport's option and subject to proof of purchase from an authorised source.

Any implied warranties including any warranties of quality or fitness for a particular purpose are limited to the terms of the express warranties. NetSupport Ltd. Shall not in any event be liable for loss of profits, data or information of any kind or for special, incidental, consequential, indirect or other similar damages arising from any breach of these warranties or use of the software even if they have been advised of the possibility of such damages. Some countries do not allow the limitation or exclusion of incidental or consequential damages, so the above limitation or exclusion may not apply to you. This warranty does not affect your statutory rights, and you may have other rights that vary from country to country. In any event NetSupport's maximum liability shall not exceed the price paid by the end-user / licensee.

TERMINATION: You may terminate this licence and this Agreement at any time by destroying the program and its documentation, together with any copies in any form.

NetSupport Ltd. may terminate this licence forthwith by notice in writing to you if you commit any serious breach of any term of this licence and (in the case of a breach capable of being remedied) shall have failed within 30 days after receipt of a request in writing from NetSupport Ltd. so to do, to remedy the breach (such request to contain a warning of NetSupport's intention to terminate). Upon termination you will destroy or return to NetSupport Ltd the original and all copies of the software and will confirm in writing to NetSupport Ltd that this has been done.

SUPPORT: If you have a problem with the installation of the software you should in the first instance contact your supplier. You can separately purchase support and maintenance which will also cover the supply of enhancements and upgrades.

GOVERNING LAW: This agreement shall be governed by the laws of England.

Contents

Welcome to NetSupport Protect	6
Product Overview	7
Key Features at a Glance	8
Installation	9
System Requirements	9
Starting the Installation	10
NetSupport Licence Agreement	10
Licence Information	10
Custom Setup	11
Completing the Installation	12
Existing Installation Detected	12
Upgrading NetSupport Protect	13
The User Interface	14
Using NetSupport Protect	16
The Summary Dialog	16
Folders	17
System	19
Desktop	21
Applications	23
Network	25
Devices	26
Recovery	27
Users	29
Settings	30
Save Configuration	32
Discovery and Deploy Tool	34
Deploy Setup Options	36
Contact Us	38

WELCOME TO NETSUPPORT PROTECT

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

NetSupport Protect provides a secure, reliable and productive computer environment. With its extensive list of security features and intuitive format, IT administrators can use NetSupport Protect to guarantee that users are getting the most beneficial use of their computer experience, while safeguarding both the configuration and content on their systems.

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

For added peace of mind, NetSupport Protect also offers integrated hard disk protection and recovery so, if an error should occur, you can perform a full system restore quickly and transparently.

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 office PCs or computer lab.

Product Overview

Education

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.

Corporate

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 users can utilise 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 IT administrators and technology coordinators. Presented in a simple and intuitive interface, system control can be configured in minutes and allows either individual or central control of security settings.

Key feature highlights in NetSupport Protect are:

- Disable access to the Windows Store.
- Prevent uninstall from Windows 8 Start Menu.
- Restrict user-defined apps for Windows 8 from running.
- Prevent copying, deletion and renaming of files and folders.
- 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 neighbourhood.
- Prevent access to windows systems tools
- Prevent web browsers or any other user defined applications from running.
- Restrict creation and deletion of system printers.
- Control access to USB and CD/DVD drives.
- Disable USB devices, allow read only or prevent application launch.
- Prevent users from installing unauthorised software.
- Apply policies to all users, or exclude specified accounts.
- Share security configurations across a network.
- A convenient Deploy utility enables multiple installations of NetSupport Protect onto remote machines.
- Instantly restore your hard disk to an earlier point in time.

Benefits

Using NetSupport Protect IT administrators can prevent unwanted changes to the OS, control the creation of content, restrict unwanted file downloads and control application usage. With easy to adopt end point security, administrators can avoid the introduction of harmful or unwanted content from external sources yet retain the flexibility to utilise existing technology.

Traditional "policy based" security provides for inflexible on/off lockdown, NetSupport Protect allows useful technologies, such as portable storage devices to still be utilised, but in a constructive manner with controls over functionality.

INSTALLATION

System Requirements

30 Mb free disk space.

Microsoft Windows 8 and 8.1 (32bit and 64bit), Windows Server 2012 (and R2), Windows 7 (32bit and 64bit), 2008 (32bit, 64bit and R2), Vista (32bit and 64bit), 2003, XP (Service Pack 3 and above).

Disk Recovery

For Disk Recovery to be installed, the following pre-requisites are required:

Windows 2003 Service Pack 2

Windows Vista Service Pack 1

Windows XP System Restore must be turned off

Windows Vista and above System Protection must be turned off

Windows Vista and above Windows update must be disabled

Windows Vista and above Bitlocker must be disabled.

Notes:

- When upgrading from a previous version of NetSupport Protect, your existing roll back recovery point will be removed. See Upgrading NetSupport Protect for further information.
 - Disk Recovery is not supported on Windows 2003 Server, Windows 2008 Server and Windows Server 2012.
 - It is not recommend that Protect Disk Recovery be used on more than one boot partitions on Dual Boot systems, Disk Recovery is not supported on RAID-based systems.
 - When you have an active NetSupport Protect Disk Recovery partition, you will be unable to use the Windows 8 Operating Recovery options.
-

Starting the Installation

Insert the NetSupport Protect installation CD into your computer and let it autorun. If it does not autorun, run the NETSUPMENU.exe command from the CD.

Alternatively, you can download your copy of NetSupport Protect from www.netsupportprotect.com/downloads.asp

Click the appropriate language from the menu and select the option to install NetSupport Protect.

The NetSupport Protect installation will start displaying a Welcome screen.

Click **Next** to continue.

NetSupport Licence Agreement

The NetSupport Licence Agreement will be displayed. Please read the Licence Agreement carefully and select 'I accept the terms in the Licence Agreement' and click **Next** to continue.

If you reject the Licence Agreement, ('I do not accept the terms in the Licence Agreement') click **Cancel**. NetSupport Protect will not be installed and you will be directed to exit from the install program.

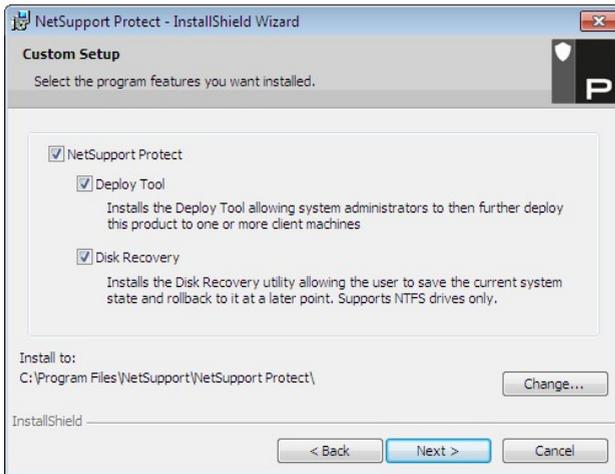
Licence Information

Select **Register** and enter the licence details you have been provided with.

If you are evaluating NetSupport, select **14 day evaluation** and click **Next**.

Custom Setup

Select the components to install.



NetSupport Protect

Deploy Tool

The Deploy Tool enables you to remotely deploy NetSupport Protect without the need to visit each individual workstation.

Disk Recovery

This component allows you to instantly restore the system to an earlier point in time.

Notes:

- To install disk recovery on Windows XP and Vista, the system restore/protection must be turned off.
 - Windows Vista and Windows 7 must have Windows Update disabled.
 - Disk Recovery is not supported on Windows 2003 Server, Windows 2008 Server and Windows Server 2012.
 - When upgrading from a previous version of NetSupport Protect your existing roll back recovery point will be removed. See Upgrading NetSupport Protect for further information.
-

Install to:

By default, NetSupport will be installed in the folder C:\Program Files\NetSupport\NetSupport Protect. If you want to install in a different folder, click **Change**.

Click **Next** when ready to continue.

Completing the Installation

Ready to Install the Program

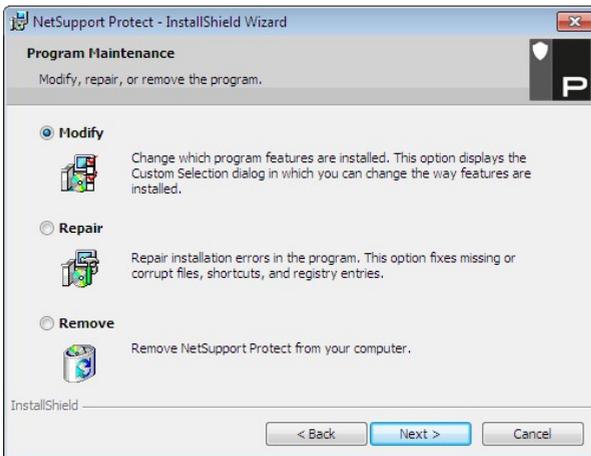
To start the installation, click **Install**. To change any of the previous selections, click **Back**. To quit the installation, click **Cancel**.

Installation Complete

Click **Finish** to exit the Setup program. Remove the CD and restart the workstation.

Existing Installation Detected

This screen will appear if a copy of NetSupport is already installed on the workstation.



You can choose to:

Modify

Change the program features that are installed.

Repair

Repair any installation errors in the program.

Remove

Remove NetSupport Protect from the computer.

Select the required option and click **Next**.

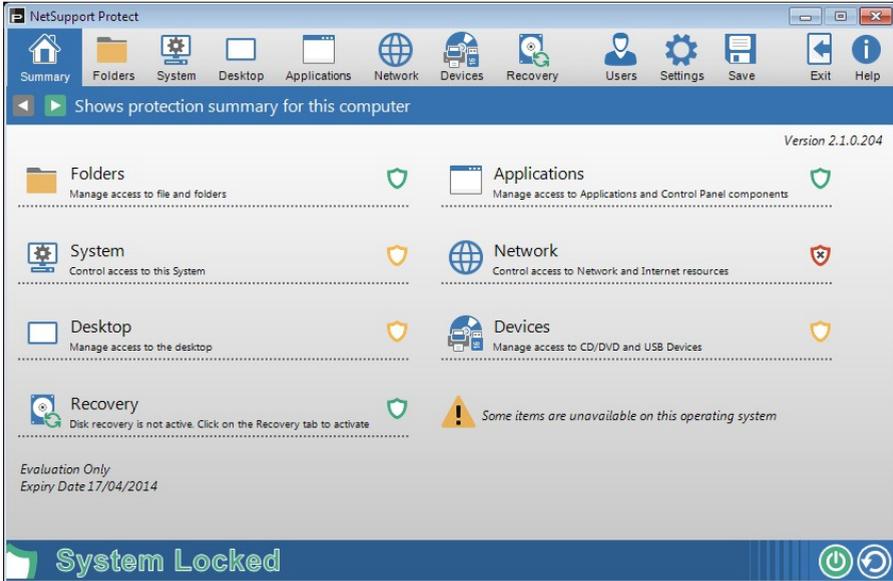
Upgrading NetSupport Protect

When upgrading from a previous version of NetSupport Protect your existing roll back recovery point will be removed. To ensure the computer is able to restore to the same state as your existing roll back point you may need to exit the installer and use your existing roll back point before completing the installation.

Once the installation for the upgrade is complete, a new roll back point can be created.

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 seven 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 Recovery option allows you to protect systems from unauthorised changes, the current Recovery status will be displayed.

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.

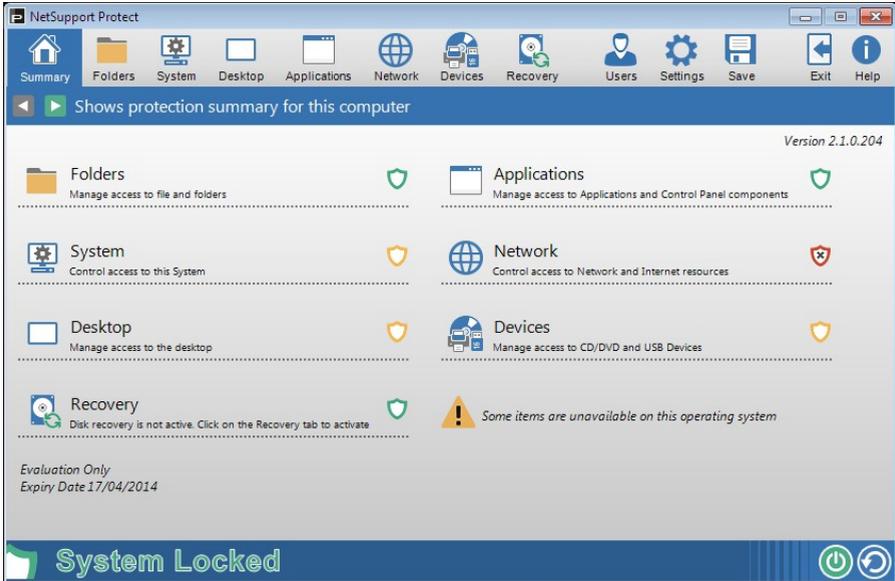
Note: If the Status bar is 'greyed out' it means the NetSupport Protect service is not running.

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.

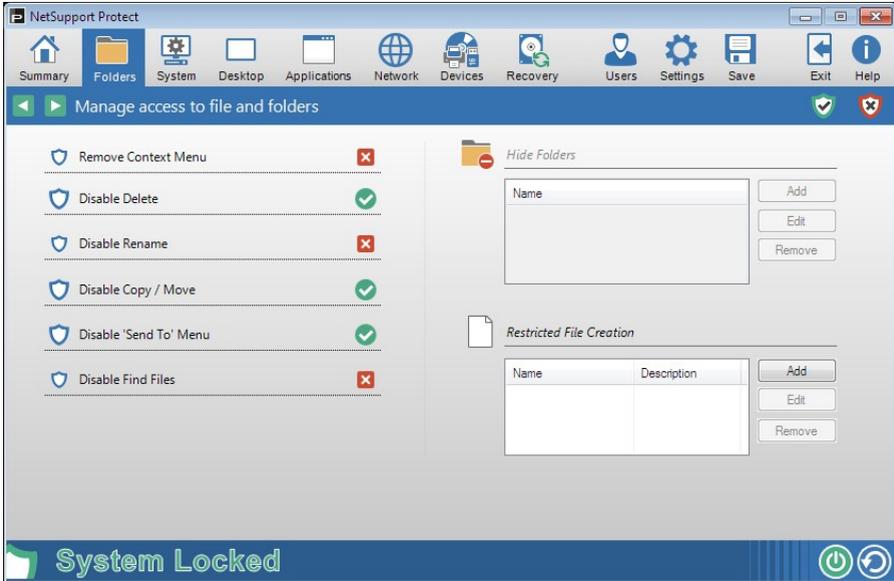


- Red None of the options within this category are protected.
- Amber Some of the options are protected.
- Green All options are protected.

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 '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 (Not supported on Windows Vista and above)

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 Creation

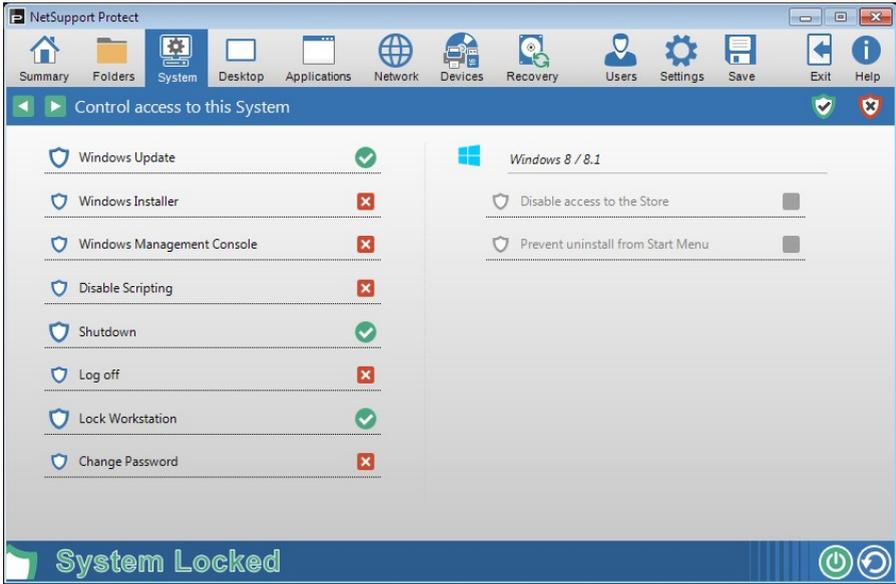
Blocks access to certain types of file. Click **Add** to specify the file extension (exclude the .).

Note: Enabling the **Copy**, **Delete** or **Rename** options on Windows Vista will disable the Organise menu in Windows Explorer.

Clicking  or  turns protection on/off for all options.

System

Controls access to various system utilities.



Windows Update

Prevent users from running Windows Updates.

Windows Installer

Prevent users from running Windows installers.

Windows Management Console

Prevent users from accessing the Windows Management Console.

Disable Scripting

Prevent Windows Script Host and Java Scripts from being created or executed.

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.

Windows 8/8.1

These options are only applicable to users running Windows 8 or 8.1.

Disable access to the Store

Prevent users from accessing the Windows Store.

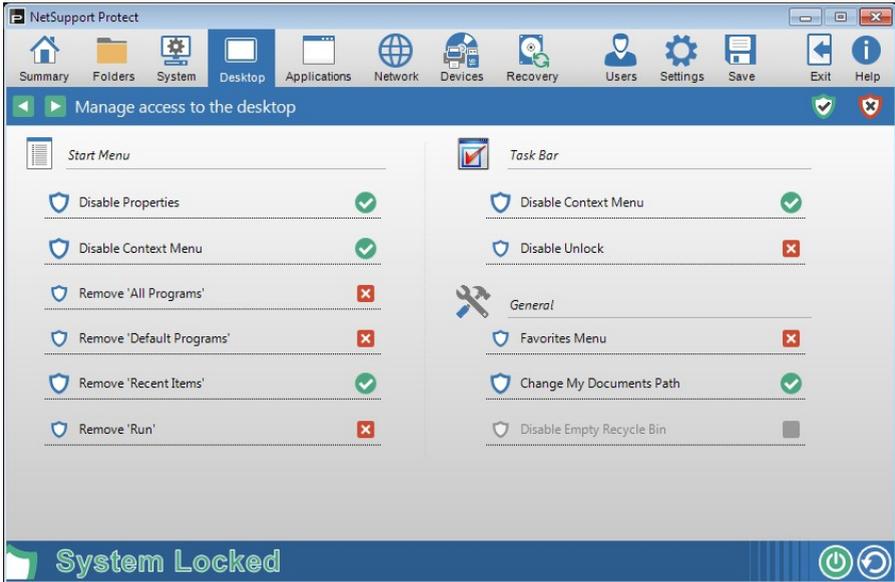
Prevent uninstall from Start Menu

Removes the uninstall option from the Start menu.

Clicking  or  turns protection on/off for all options.

Desktop

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



Start Menu

Disable Properties

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

Disable Context Menu

Prevent modifications to Start menu items.

Note: You can't disable the right-click context menu for the 'All Programs' option. However the right-click context menu will be disabled for the submenus from the 'All Programs' option.

Remove 'All Programs'

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

Remove 'Default Programs'

Prevent access to the Default Programs option from the Start menu.

Remove 'Recent Items'

Remove the Recent Items option from the Start menu.

Remove 'Run'

Remove the Run option.

Task Bar

Disable Context Menu

Remove the taskbar context menu when right-clicking.

Disable Unlock

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.

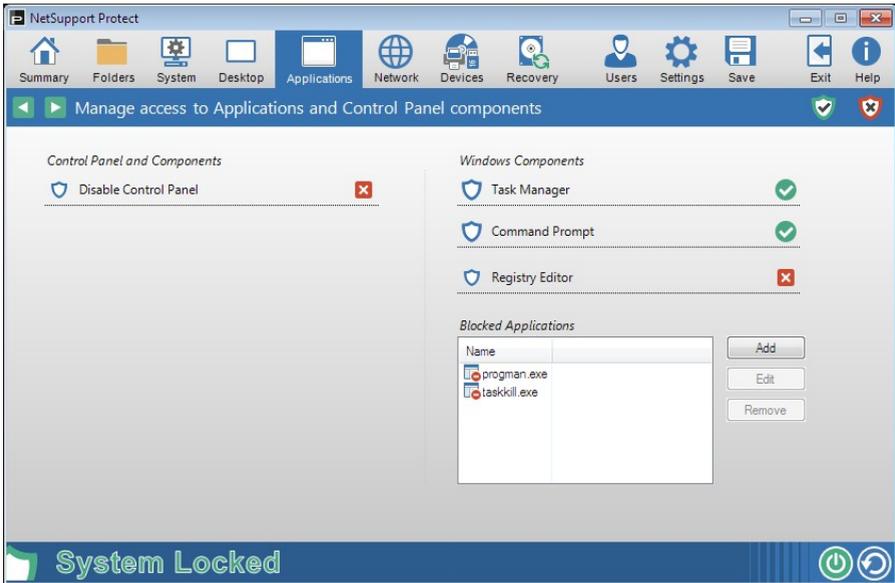
Disable Empty Recycle Bin (not supported on Windows Vista and above)

Prevent users from being able to empty the recycle bin.

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.

Note: Removing individual components is not supported on Windows Vista and above.

Windows Components

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

Blocked Applications

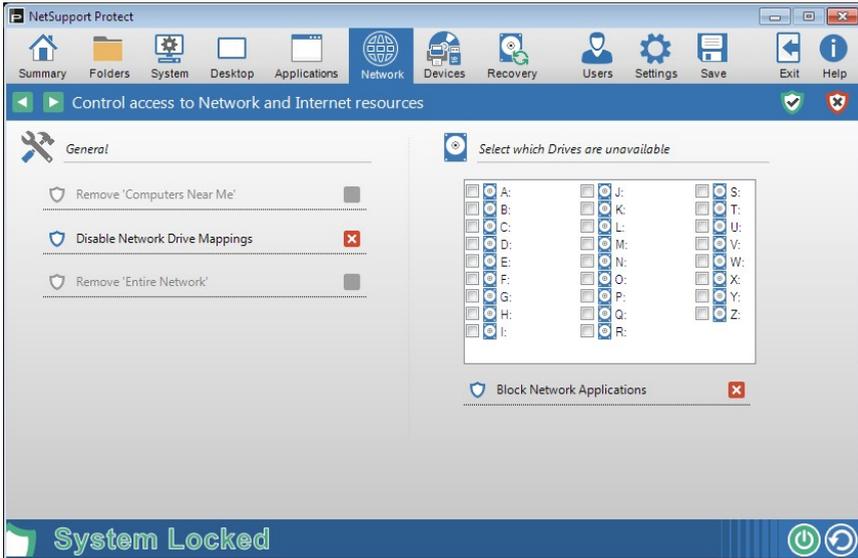
Prevent users from accessing specific applications. Click **Add** to browse for the required exe files.

Note: When adding applications on Windows 8 workstations two tabs will be displayed in the Application Properties dialog. The 'Desktop Application' tab allows you to add standard Windows applications. The 'Windows Store Application' tab lists Windows 8 applications. Select the required application and click **OK** to add to the blocked applications list.

Clicking  or  turns protection on/off for all options.

Network

Control access to network and internet resources.



Remove 'Computers Near Me' (not supported on Windows Vista and above)

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

Disable Network Drive Mappings

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

Remove 'Entire Network' (not supported on Windows Vista and above)

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

Disable Network Drives

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

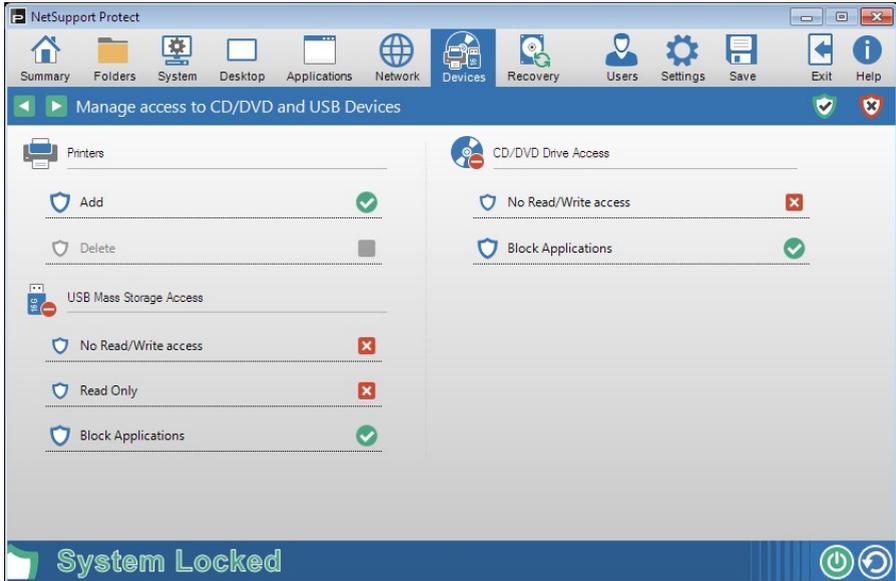
Block Network Applications

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.

Note: The delete printers option is not available on Windows Vista and above.

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.

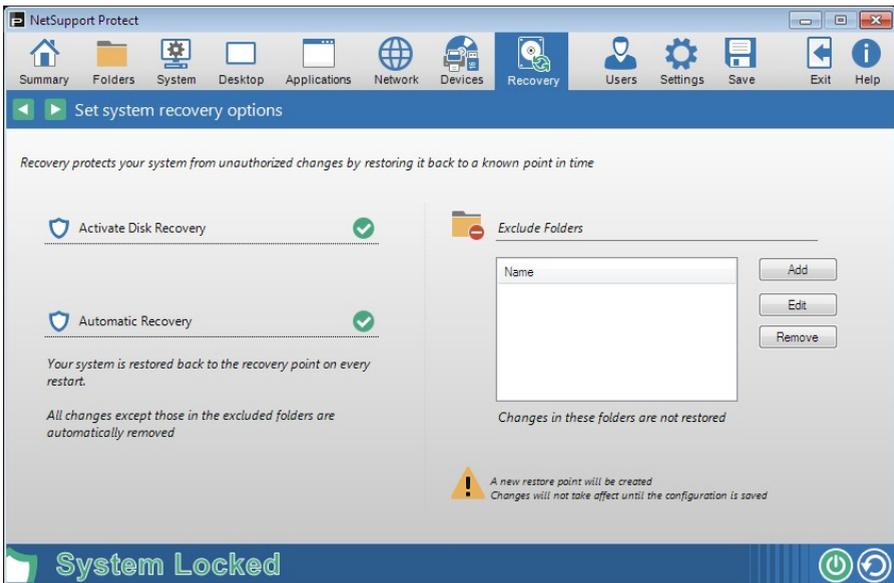
Recovery

NetSupport Protect disk recovery is ideally suited to training and classroom environments providing a quick and convenient facility to enable PCs to be recovered to a known state on a regular basis. This ensures that a consistent and clean environment is always provided for training purposes.

Once disk recovery is 'activated' NetSupport Protect monitors and records changes applied to the PC so that these changes can be quickly reversed in readiness for the next session.

The time taken to roll back a PC at the end of a training session is dependent on the level of activity since the roll back point was created or last used. A regular roll back cycle (for example daily) is therefore recommended to keep the recovery time to a minimum.

Major system changes applied through 'Service Packs' or 'Windows Updates' should not be attempted and cannot be recovered using NetSupport Protect disk recovery. Disk recovery needs to be de-activated prior to applying system updates. Once the system updates are complete disk recovery can be 'activated' again and a new roll back point created.



Notes:

- To install disk recovery on Windows XP and Vista the system restore/protection must be turned off.
 - Windows Vista and Windows 7 must have Windows Update disabled.
 - Disk Recovery is not supported on Windows 2003 Server, Windows 2008 Server and Windows Server 2012.
 - When you have an active NetSupport Protect Disk Recovery partition, you will be unable to use the Windows 8 Operating Recovery options.
-

These options allow you to restore the system on reboot:

Activate Disk Recovery

Allows you to switch the Disk Recovery option on/off.

The current recovery status is displayed. From here you can create or update a recovery point.

Automatic Recovery

Enables you to automatically restore systems back to the recovery point on every reboot.

Exclude Folders

Specify folders to be excluded when the system is restored. A new recovery point will be created when a folder is added.

Note: Sub folders are automatically excluded.

Users

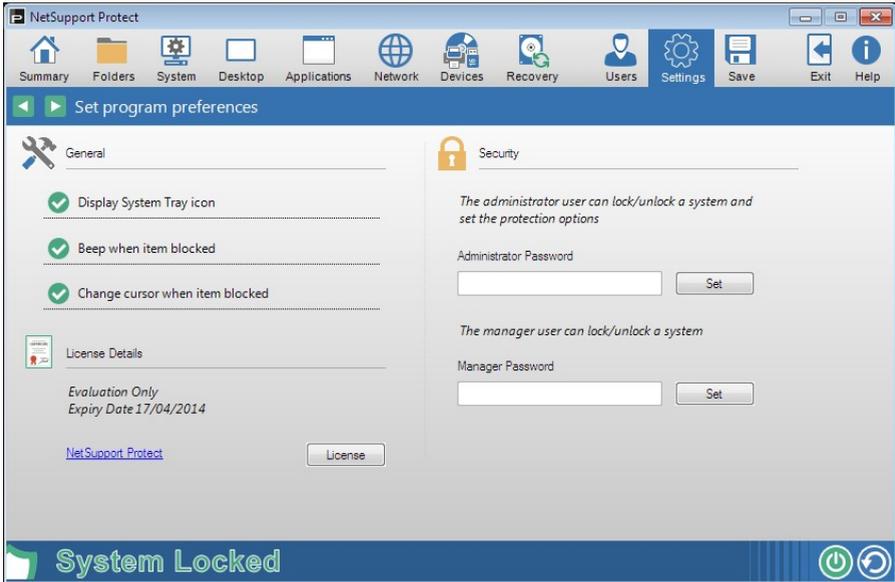
Create a list of users to whom protection does not apply. Click **Add** to enter the users login name.

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

Name	
 Administrator	<input type="button" value="Add"/>
	<input type="button" value="Edit"/>
	<input type="button" value="Remove"/>

Settings

Enables you to set preferences for NetSupport Protect.



General

Display System Tray icon

If required, the NetSupport Protect tray icon can be hidden. If displaying the NetSupport Protect tray icon, you may want to set an administrator/manager password to ensure that unauthorised users do not deactivate protection.

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 licence.

If converting from an evaluation to a sale copy, you will need to activate your product licence key. Click **License** to enter the details you have been supplied with.

To Install with a pre-activated License key, place the NSP.LIC file in the same directory as the NetSupport Protect installer.

Security

Two levels of security 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. 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.



Standalone

Once appropriate settings are in place click **Save** to store the configuration. If the 'Current Mode' is set to Remote, click **Use** in order to load the locally stored configuration file.

Remote

For ease of administration, NetSupport Protect can be set to load restrictions from a centrally stored configuration file (lockdown.dat) on a network share.

Click **Remote** to enable the following options.

Save Saves the current configuration and sets this PC to load it's restrictions from a network share. You will be required to enter a path and appropriate user credentials.

Load Sets this PC to Load its configuration from a network share. Browse for the required file and enter the appropriate user credentials.

Note: The user credentials must exist locally and on the Network and with rights to the specified share.

Installing with pre-configured restrictions

A stored configuration file, Lockdown.dat, can be applied to other installations.

Place the configuration file in the same directory as the installer to install and apply your pre-set configuration when using locally stored configuration files.

Silent Install

Setup /S /v/qn will perform a silent installation without displaying installer dialogs.

Setup /S /v/qb will not prompt for input but will display a progress bar during installation.

Remotely Deploy Configurations

The NetSupport Protect Deploy tool provides a convenient method for centrally deploying stored configurations to remote PCs.

Using Disk Recovery with Shared Configuration Files

When loading a remote configuration from a Network drive, there are certain considerations to be taken into account when using the Disk Recovery options.

Sufficient time needs to be allowed for the configuration file update to be detected, acted on and for the new recovery point to be generated.

If the restore point creation process is interrupted by logging off, re-booting etc this can lead to a corrupt restore point being generated.

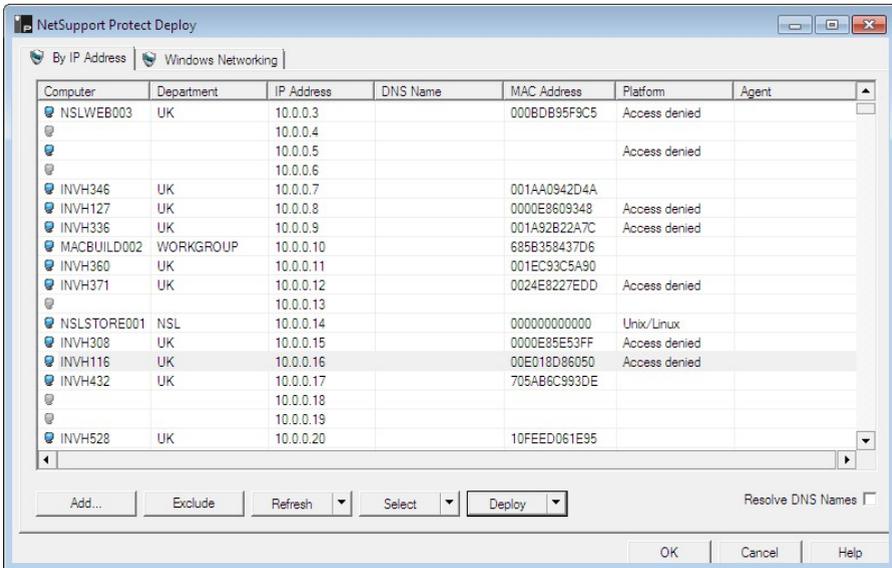
Creating/Updating Restore Points using Remote Configuration Files

1. Ensure all the PCs that are set to use the remote configuration file are logged off.
2. Use Protect to save the new settings to the remote configuration file (lockdown.dat) on the Network Drive.
3. Logon the PCs and wait for the new configuration to be detected and applied.
4. Wait for the dialog displayed on each PC during the recovery point generation to clear.

DISCOVERY AND DEPLOY TOOL

The Deploy Utility, launched from the NetSupport Protect program group, provides Network Administrators with the ability to install and configure NetSupport Protect on multiple workstations without the need to visit the machines individually.

You are provided with a view of your Network, allowing you to select the workstations you want to include and you can then choose to deploy the NetSupport Protect Setup package, a Configuration file or a License file. You can also remotely uninstall NetSupport Protect.



Find PCs

To determine which machines to include in the deployment firstly decide whether to search 'by IP Address' or 'Windows Network' by selecting the appropriate Tab.

Click **Add**.

If searching by IP Address enter the address range or select an existing range if present. Select the appropriate Network Groups if using Windows Networking.

Click **OK** to begin searching the network for matching machines.

Select PCs

To help identify the PCs to be included or excluded from the deployment the list can be sorted by clicking on any of the column headings. You can further refine the list by removing machines that you do not want to include in the deployment. Click **Select** and choose the appropriate task from the drop down list. Click **Exclude** to remove the highlighted items.

From the PCs that remain, select the ones to deploy to. To include all machines click Select – All Clients or highlight the PCs individually using Shift-Click, Ctrl-Click.

With the required PCs selected, click **Deploy**.

Select Type Of Deployment

Setup

Select this option if you want users at the remote machine to be able to access the NetSupport Protect Interface, change settings and create new configurations. At the same time as deploying the setup package you can optionally include a new License File and/or a specific Configuration file.

Uninstall

Enables you to remotely uninstall NetSupport Protect from the selected machines.

Configuration

Deploy a stored NetSupport Protect configuration (lockdown.dat file).

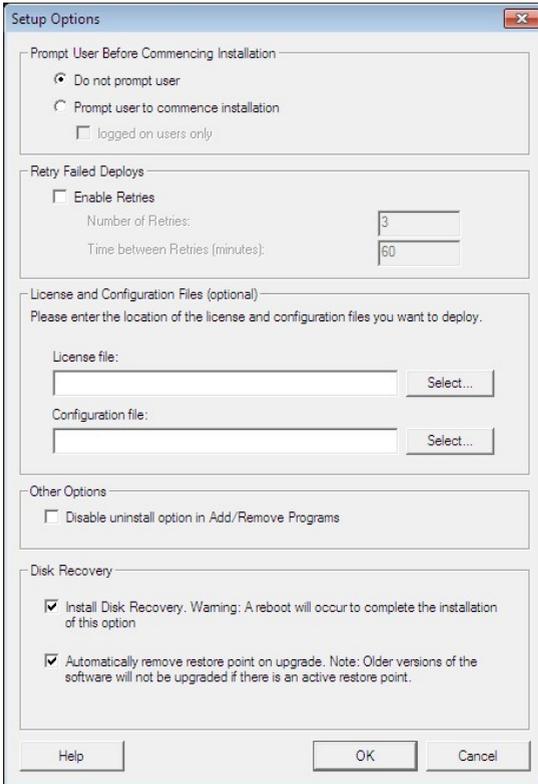
License

Deploy a NetSupport Protect License file. (nsp.lic)

Click **Start**. Depending on the type of deployment you will be prompted to provide additional information such as the location of license and configuration files, and the NetSupport Protect Admin password.

Deploy Setup Options

When deploying a NetSupport Protect Setup you will be prompted to provide additional information.



Prompt User Before Commencing Installation

If the target PCs are likely to be in use at the time of the deployment you can display a prompt at the machines before commencing. The user can then start the installation when ready. The message can be sent to Logged On machines only.

Retry Failed Deploys

Indicate if the deployment should be automatically retried in the event of a failure. Specify the number of retry attempts and the interval between.

(Optional) Deploy License and Configuration Files

At the same time as deploying the setup you can also include a specific License file (nsp.lic) and/or Configuration file (lockdown.dat). Click **Select** to browse for the appropriate files.

Other Options

Disables the uninstall option in Add/Remove Programs, ensuring the user is unable to remove the deployed items.

Disk Recovery

Install Disk Recovery

Installs the disk recovery feature, this is enabled by default. To complete the installation of this option the selected machines will be rebooted.

Automatically remove restore point on upgrade

This option allows you to remove an existing roll back point when performing an upgrade. If you are upgrading from a previous version of NetSupport Protect you will be unable to proceed with the upgrade if there is an active roll back point.

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.netsupportjapan.com

Technical Support: support@netsupportsoftware.com

Sales: sales@netsupportjapan.com