Faronics
WINSELECT™
STANDARD

DYNAMIC Preference Control

User Guide

This page has been left blank intentionally

Technical Support

Every effort has been made to design this software for ease of use and to be problem free. If problems are encountered, contact Technical Support:

Technical Support:	www.faronics.com/support
Web:	www.faronics.com

About Faronics

Faronics delivers market-leading solutions that help manage, simplify, and secure complex IT environments. Our products ensure 100% workstation availability, and have dramatically impacted the day-to-day lives of thousands of information technology professionals. Fueled by a customer-centric focus, Faronics' technology innovations benefit educational institutions, healthcare facilities, libraries, government organizations and corporations.

Last Modified: October 2018

This page has been left blank intentionally

Contents

This page has been left blank intentionally

WINSelect Program Overview

Controlling user activity on public use and kiosk computers is a problem that IT personnel continually face. IT administrators want a solution that allows them to easily manage user access to certain applications, web sites, and menu options so that they can influence how a workstation is used. Faronics WINSelect protects a computer's purpose by empowering administrators with full control over a workstation's abilities. Windows operating system features, Start menu functionality, Internet Explorer capabilities, and Windows Explorer options can all be heavily customized to suit organizational needs.

WINSelect Editions

Standard

- WINSelect Standard Edition runs on a standalone workstation.

Enterprise

- WINSelect Enterprise Edition provides centralized installation, deployment, administration, and control for multiple workstations on your network.

Program Requirements

Software

- Windows XP Professional SP3 (32-bit or 64-bit), Windows 7 (32-bit or 64-bit), Windows 8.1 (32-bit or 64-bit), or Windows 10 version 1803 (32-bit or 64-bit)

Supported Programs

- Microsoft Office XP, 2003, 2007, 2010 and 2013
- Internet Explorer 10 and above
- Mozilla Firefox (upto version 62.0)

Installing WINSelect

Prior to installing WINSelect, the Fast User Switching options for Windows XP and Windows 7 must be disabled. Refer to http://support.microsoft.com/kb/279765 *for more information.*

WINSelect must be disabled during the creation of a new User Profile. As part of WINSelect protection, the registry editing tools will be disabled. The administrator will have to disable WINSelect to use these tools.

If a removable drive is connected during the WINSelect install, it is assigned a drive letter. It is recommended that removable drives be disconnected during installation to avoid unintentionally applying WINSelect settings.

If Windows Group Policies are set on a workstation and WINSelect sets the same policy, WINSelect will take precedence. If WINSelect does not duplicate the Group Policy setting, the Group Policy will not be affected.

To install WINSelect, complete the following steps:

1. Insert the CD-ROM from the media package into the CD-ROM drive. If WINSelect has been downloaded via the Internet, double-click the application file named *WINSelect_Standard_ Installer32.exe.*

    The Installation Wizard appears.

2. The *End User License Agreement* appears. Select *I accept the terms in the License Agreement* followed by *Next.*

3. Enter the *User Name*, *Organization* and *License Key*. If you do not have a License Key, select the *Use Evaluation* check box. The evaluation version will stop functioning after 30 days. If you have already purchased WINSelect, you can get the License Key by logging into www. faronicslabs.com.

4. The application is installed by default to *C:\Program Files\Faronics\WINSelect.*

    Click *Browse* to choose a different location. If choosing to install to a different location other than Program files, be sure to remember this new location.

5. Click *Next.*

    Specify the *WINSelect Administrator Password*. Click *Next.*

6. Click *Install.* Once the installation is complete, click *Finish.*

7. A dialog appears stating that the system must be restarted for the configuration changes to take effect. Click *Yes* to restart or *No* to restart later.

Passwords cannot be retrieved by Faronics. The password must be recorded and guarded with care.

WINSelect Licensing

If no License Key is available, use the evaluation version of WINSelect. The evaluation version is valid for 30 days. To upgrade to the full version of WINSelect, enter a valid *Licence Key* in the dialog box launched when you click the *Set* button in the *About* node.

If no Key is entered after 30 days, WINSelect is disabled.

Uninstalling WINSelect

⚠️ *To perform a WINSelect uninstall, click on the Administrator node and ensure the Enable box is not selected.*

1. Launch the WINSelect installer *WINSelect_Standard_Installer32.exe*. The uninstall wizard appears, asking for confirmation of the uninstall.
2. Restart the workstation to complete the uninstall.

⚠️ *The administrator must log out of Windows and log back in at least once to complete the uninstall.*

Launching WINSelect Following Installation

To launch WINSelect, use one of the two following options:

- Use hotkey *Ctrl + Alt + Shift + F8*
- *Shift* + double-click the WINSelect System Tray icon

The WINSelect Login window appears:
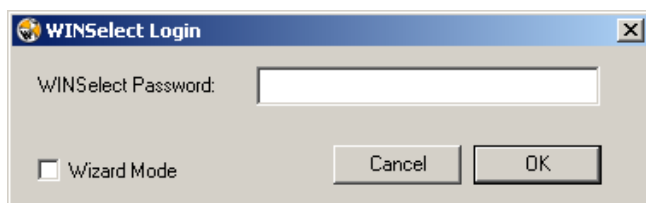
Enter the administrator password set during the WINSelect install. There are two options available from the Login window:

- To access the WINSelect Administrative Console click *OK* to log in. The Control Panel allows administrators to customize a workstation's abilities and operating features to a high level of detail.
- To access the Wizard Mode, select the *Wizard Mode* check box and click *OK*. The Wizard mode is used to quickly create a Kiosk and has a limited set of guided configuration options.

The first time the Login window appears, the option to access the Wizard Mode is enabled. The option to access the Administrative Console will appear following the completion of Wizard Mode steps.

The WINSelect icon in the System Tray ![icon] indicates if WINSelect is enabled. When WINSelect is disabled the icon is covered by a red X: ![icon].

WINSelect Layout

WINSelect is comprised of a series of *nodes* that appear in the left pane of the Administrative Console. Clicking on a node displays a set of options in the right pane of the Administrative Console. Nodes that contain more than one sub-node can be expanded by clicking on the icon next to the node name in the left pane of the Administrative Console.

Administrative Console

To access the Administrative Console, *Shift* + double-click the WINSelect icon located in the Windows System Tray or use the *Ctrl + Alt + Shift + F8* hotkey. Enter an active password and ensure the *Wizard Mode* check box is not selected. If the Wizard Mode is used before the Administrative Console is accessed, all configuration choices made in the Wizard are carried over.

The *About* node of the Administrative Console appears as below:
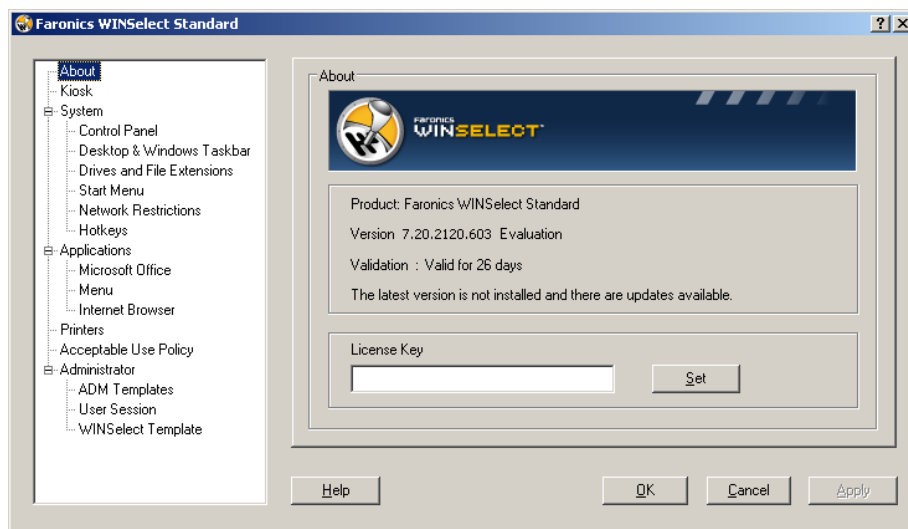
The Administrative Console is comprised of a series of nodes grouped by common function which allow the administrator to customize the Windows environment and functionality.

The *Kiosk* node allows administrators to create a workstation with limited Windows functionality and enable key WINSelect features in only a few short steps.

The *System* node contains options which protect the computer and prevent unauthorized access to key Windows settings. Here, the administrator can prevent changes to system-wide Windows components.

The *Applications* node allows the administrator to customize the software found on the WINSelect workstation. Use the Applications node to permit and restrict access to applications like Microsoft Office and various Internet browsers.

The *Printer* node allows administrators to disable local and network printers.

The *Acceptable Use Policy* node allows administrators to set Acceptable User Policy and display it to workstation users.

The *Administrator* node allows users to enable and disable WINSelect, customize WINSelect settings such as the creation of user sessions, and add or change password. WINSelect templates can also be created.

Click on any node to configure the workstation.

System

The System node allows configuring the system-wide options.
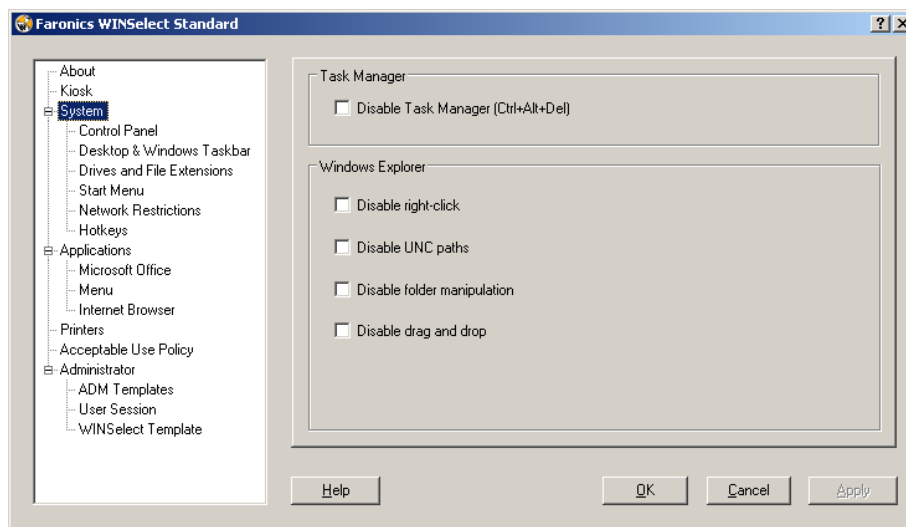
To disable the Task Manager, select *Disable Task Manager.* This prevents the user from accessing the Task Manager and ensures currently running tasks and processes cannot be ended by an unauthorized user.

Select *Disable Right Click* to prevent users from accessing commands such as *View, Paste, Copy,* and *Properties* in Windows Explorer.

Select *Disable UNC* (Uniform/Universal Naming Convention) *Paths* to prevent users from accessing shared network resources.

Select *Disable Folder Manipulation* to prevent the renaming, moving, or deleting folders. This will prevent users from being able to rename or change the location of folders through Windows Explorer.

Select *Disable Drag-and-Drop* to prohibit users from moving files and folders to different locations. This option also disables selecting text and images by dragging the mouse pointer in all applications.

⚠️ *The Disable Task Manager and UNC paths options are automatically enabled and cannot be configured when Kiosk mode is enabled.*

Control Panel

The Control Panel node provides options for restricting the display of Windows Control Panel applets. Windows Control Panel can be accessed but the icons may be selectively hidden.
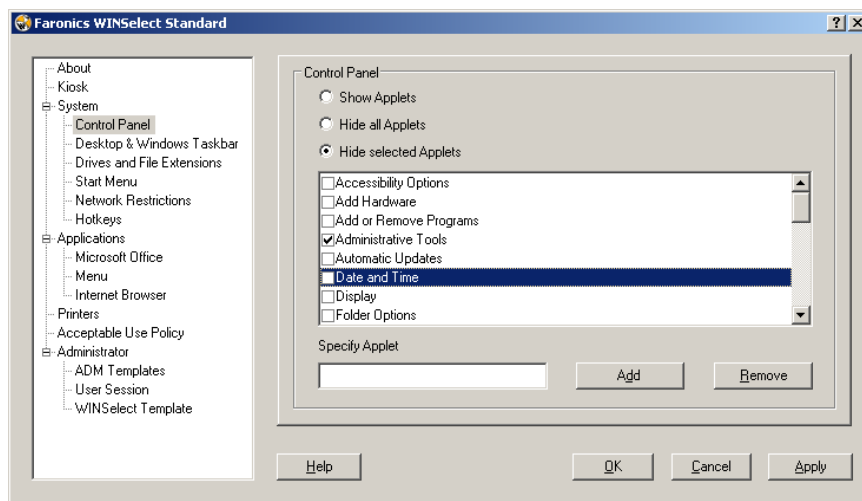
Some Control Panel settings can still be accessed and changed via a command line or the Run dialog.

To permit access to the entire Control Panel, select *Show Applets*. This displays each applet found in the workstation's Control Panel. To prevent access to every Control Panel applet select *Hide all Applets*. *Show Applets* and *Hide all Applets* do not allow for specific applets to be allowed or restricted.

To specify specific applets click *Hide selected Applets* and select the check box next to the applet to be restricted. A cleared check box next to the applet signifies a displayed and accessible applet.

To add an applet to the list, enter the applet name in the *Specify Applet* field and click *Add*.

To delete an applet, highlight it in the list and click *Remove*. A deleted applet still appears in Control Panel. It has only been removed from WINSelect's list of Control Panel applets.

Desktop & Windows Taskbar

The Desktop & Windows Taskbar node provides options for restricting the use of the workstation desktop and Windows Taskbar.
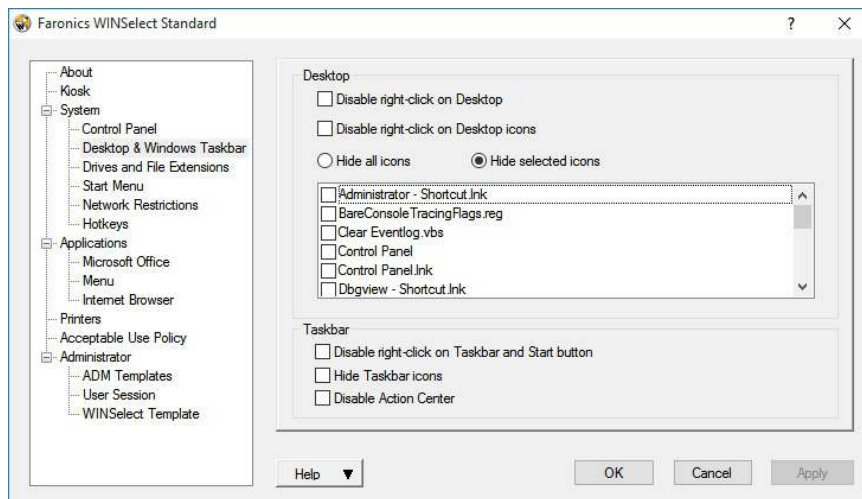
Disable Right-click on desktop prevents the user from right-clicking on the desktop. They will not be able to access the right-click menu and commands such as *New* and *Properties*.

Disable Right-click on Desktop Icons prevents the user from right-clicking on desktop icons. They will not be able to access commands such as *Open*.

The two radio buttons *Hide all Icons* and *Hide selected Icons* dictate the desktop icons that can be hidden. WINSelect recognizes the desktop icons on the workstation and lists them. Hide selected by selecting the *Hide selected Icons* radio button and selecting the check box for each icon to be hidden.

> **If Kiosk mode is enabled, changes to this node are not possible.**
>
> **Disabling right-click in the System node also disables the two Disable Right-click options in the Desktop & Windows Taskbar node.**

Drives and File Extensions

The Drives and File Extensions node provides options for restricting access to drives and specified file extensions for each application installed on the workstation.
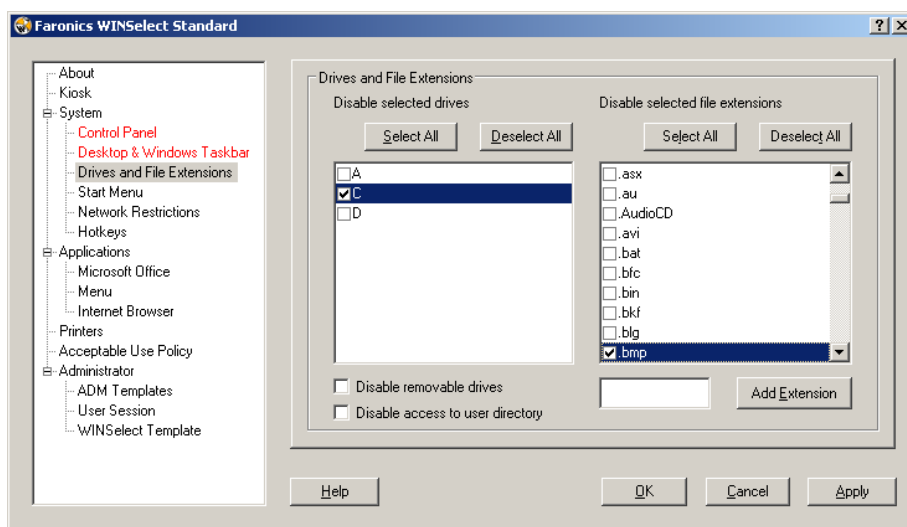
Choose which of the available drives and file extensions will be disabled by selecting the check box next to each one. Use the *Select All* or *Deselect All* options if required.

Files and directory structures are not visible once this feature is enabled. As an example, if all drives are selected, exploring the directories contained within is not permitted.

If there is no drive selected but a file extension is selected then the file extension will be disabled across all drives.

If the system drive is disabled, access to the user's directory is not disabled by default. Select *Disable access to user directory* to prevent access. As an example, if *C:* is listed as the system drive, selecting the check box next to *C* makes the *Disable access to user directory* check box available. The administrator can now choose to restrict the user to access the directory *C:\Documents and Settings\User* folder by selecting the check box. The user will be able to access only the *Desktop*. This option is only made available when the system drive letter is selected. Clear the check box to allow the user to save and create files within their own directory.

To prevent access to removable drives, select the *Disable removable drives* check box. This feature prevents the user from seeing any removable drives connected during a user session.

To disable file extensions from being used, select the desired extension. To add another file extension to the list, enter the extension in the field provided and click *Add Extension*. Once enabled, this feature prevents access to or creation of files with the specified extension.

⚠️ *If a removable drive is connected during the WINSelect install and configuration, it is assigned a drive letter. It is recommended that removable drives be disconnected during installation and configuration to avoid inadvertently applying WINSelect settings to the removable drive.*

Start Menu

The Start Menu node provides options for restricting access to the workstation's Start menu. Customize access to the Start menu by selecting one or more options.
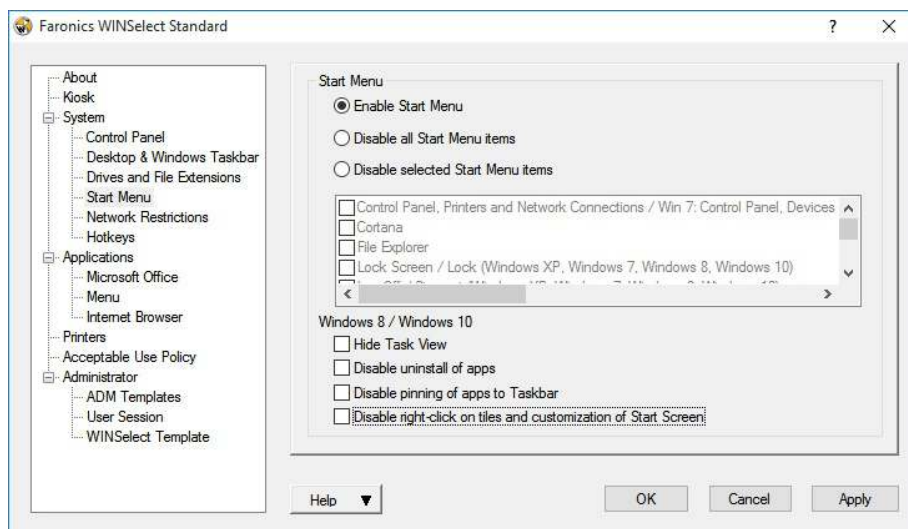
Enable Start Menu - select this option to allow access to the Start Menu.

Disable all Start Menu items - select this option to disable Start Menu completely.

Disable selected Start Menu items - select this option to disable the selected Start Menu items. Select the check box for the specific items/operating system version you want to disable.

Disable right-click Start Menu item - select this option to disable right-click for the Start Menu and prevent the user from accessing the secondary menu. This option is not available for Windows 8.1.

Enable Classic Style Start Menu - select this option to enable the Classic Style Start Menu. This option is available on Windows 7 and below.

Windows 8.1/Windows 10 version 1803

Select the following options if Windows 8.1 is installed on the managed computers:
Always boot to Desktop (Windows 8.1 Only) - select this option if you want the computers to always boot into Desktop mode. If you do not select this option, the computers running Windows 8.1 will boot into the Start Screen by default.

Hide Task View (Windows 10 version 1803 Only) - select the check box to disable Task View on Windows 10 version 1803. The Task View allows you to switch between programs currently running on the computer.

Disable uninstall of apps - select this option to disable uninstalling Windows 8.1 apps by the user.

Disable pinning of apps to taskbar - select this option to disable pinning the Windows 8.1 apps to the taskbar by the user.

Disable right-click on tiles and customization of start screen - select this option to disable the ability to right-click tiles on the start screen and also disable the customization of the start screen by the user.

Network Restrictions

The Network Restrictions node provides network restriction options. Administrators can limit access to specific web sites with these options.
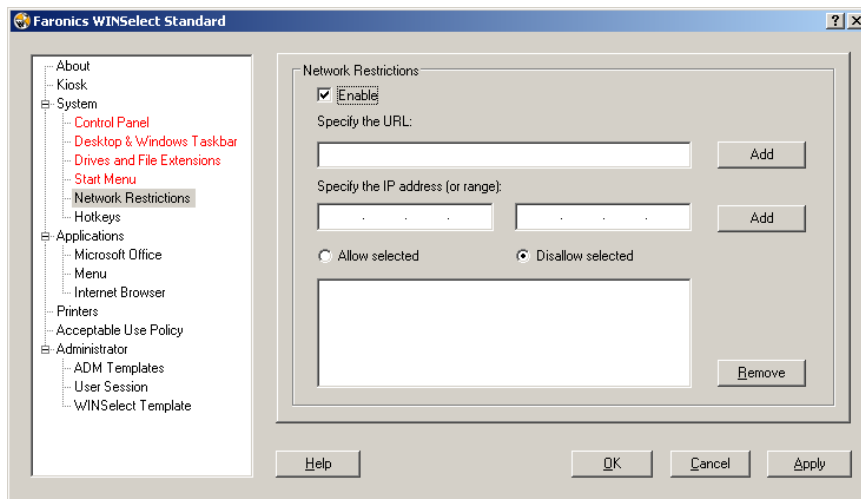

To apply network restrictions on the workstation, select *Enable*.

To restrict a specific domain name, enter it in the field labelled *Specify the URL* and click *Add*. The name appears in the list box.

To restrict an IP address or a range of IP addresses, enter the addresses in the field(s) provided and click *Add*. The addresses appear in the listbox.

If a range of addresses is specified, each individual address within the range is either restricted or allowed depending on the radio button selected (*Allow selected* or *Disallow selected*).

Select the *Allow selected* or *Disallow selected* radio buttons to specify the list box behavior. Restrict or permit selected ranges or domain names based on which entries are selected. If *Allow selected* is selected, the list entry selected will be allowed. If *Disallow selected* is selected then each list entry that is selected will not be allowed. To remove an item from the listbox, select the item and click *Remove*.
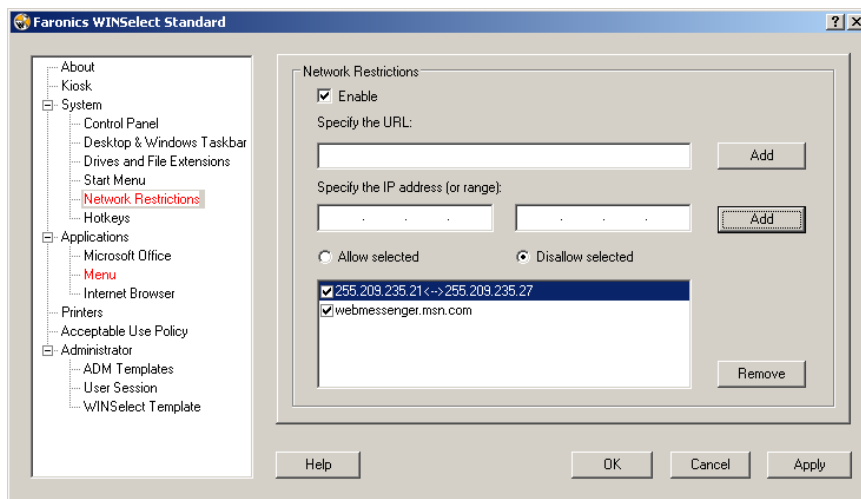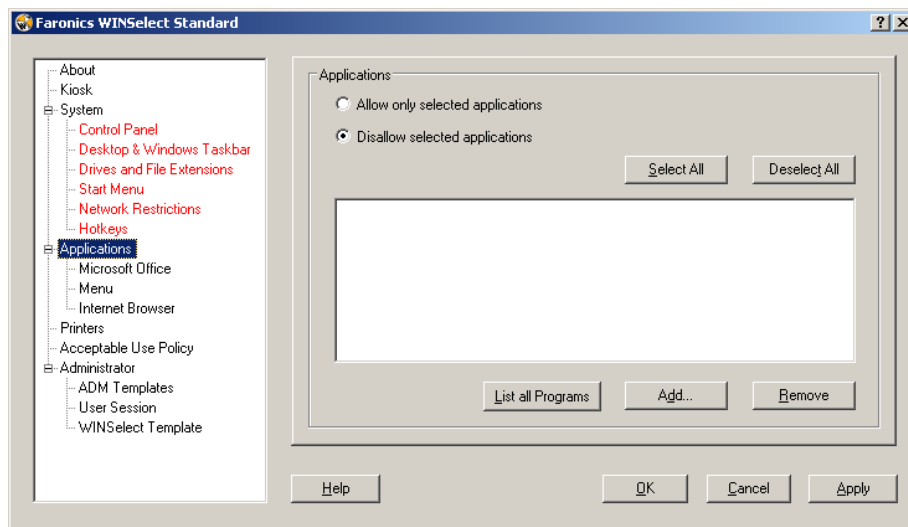
Applications

The Applications node allows for further customizing of applications.

This option is unavailable when Kiosk mode is enabled. If administrators wish to create a Windows environment featuring only specific available applications, but do not wish to create a WINSelect Kiosk, they can specify the applications on this node.

To populate the list with all available *.exe* files found within the Program Files folder, select *List All Programs.* Use the *Select All* or *Deselect All* buttons to select or deselect all programs. Click *Add* or *Remove* to add or remove programs from the list.

To add an individual application, click the *Add* button. Browse to the desired application's *.exe* file and click *Open.*

Allow only specific applications to run or to prevent specific applications from running. Each application must have its corresponding check box selected to dictate the list behavior. If an allowed application opens a second application, the second application must also be listed.

A disallowed application is recognized by name, not location. If an application is specified as disallowed, then moved to a different folder, WINSelect will still prevent it from being opened.

⚠ *Selecting Applications from the Windows system folder can cause system instability.*

To remove an application, select the application from the list and click the *Remove* button.

Microsoft Office

The Microsoft Office node provides options for restricting access to Microsoft Office menu items. The administrative features of Microsoft Office are listed to allow the administrator to prevent users from unauthorized manipulation of these settings.
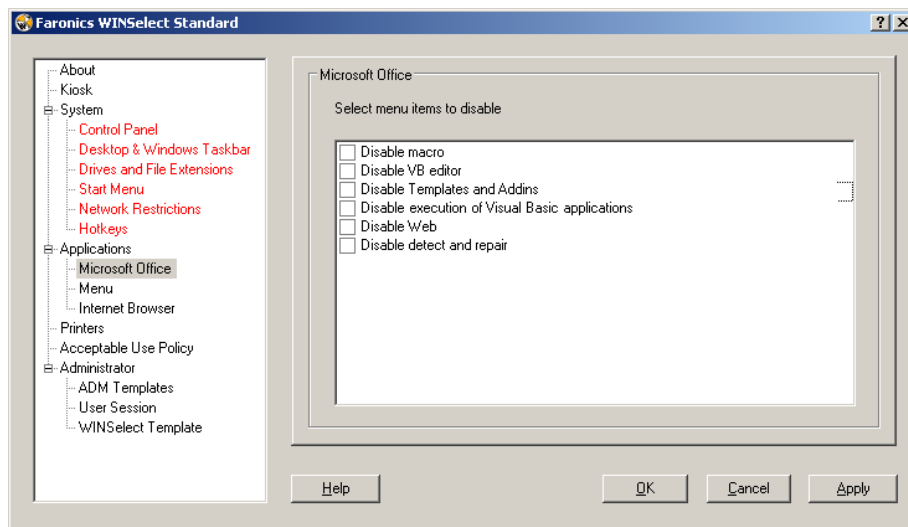
Select the menu items from the list that will restrict menu items of Microsoft Office applications on the workstation. Select the menu items from the list and click *Apply.*

The following Microsoft Office programs can be disabled by selecting the check box next to it:

Disable macro disables macros and the shortcut keys displayed.

Disable VB Editor disables the macros, Visual Basic editor and the shortcut keys displayed.

*Disable Templates and Addins* disables the Templates and Addins for Microsoft Office.

Disable execution of Visual Basic Applications disables the execution of Visual Basic programs.

Disable Web disables the Web toolbar in Microsoft Office.

Disable Detect and Repair disables the Detect and Repair option in the Help menu.
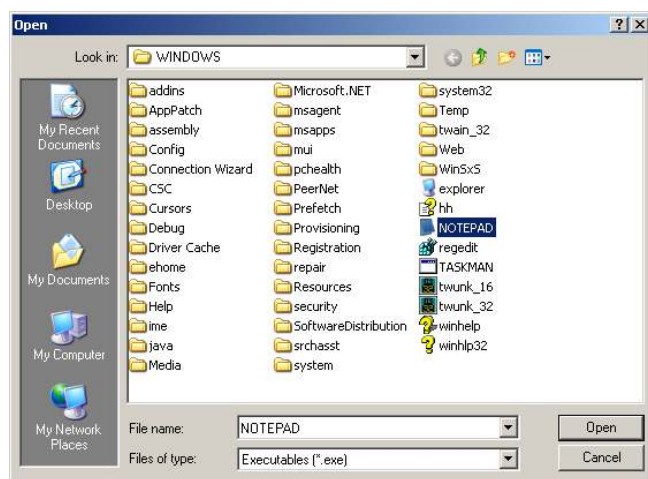
Menu

The Menu node provides options for restricting access to specific menu items within selected applications.
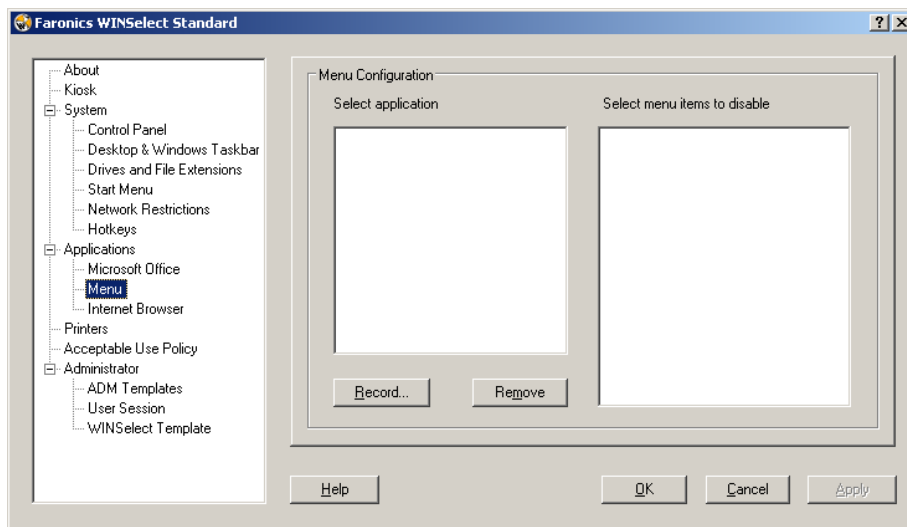

> ⚠ *WINSelect will record the menu only for products that adhere to Microsoft's menu structure. Menus of products having a different menu structure will not be recorded properly.*

To record a menu to be restricted:

1. Select a specific application by clicking *Record* and browse to the executable file (*.exe*). In the example below, the *Notepad* application is selected.

2. Open the menus to be restricted one at a time. The WINSelect Menu Recorder records the selected menu.

3. Close the application.
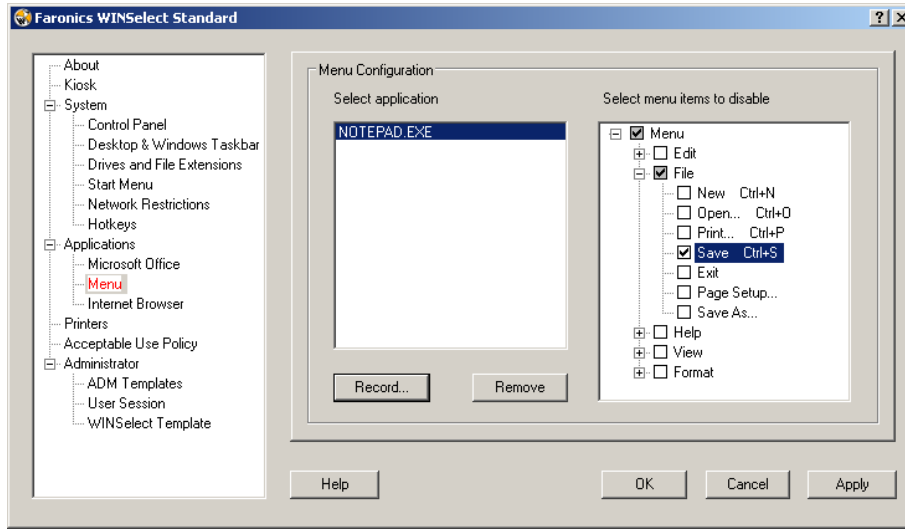
WINSelect now displays the *.exe* file selected on the left and the menu items the administrator opened on the right. Click on specific menu commands within the tree structure to restrict individual commands within those menus.

Once enabled, the user will be able to access the commands within the application but will not be able to use them.

> *Changes cannot be made to a set of menu commands once they have been selected. The .exe file must be deleted from the menu list and the process repeated.*
>
> *Menu commands for Microsoft Office cannot be recorded.*

Internet Browser

The Internet Browser node provides options for restricting access to Internet browser functions and menus. Enable these features when users are required to access the Internet, but are not permitted to save locations, print pages, access the favorites menu, etc.
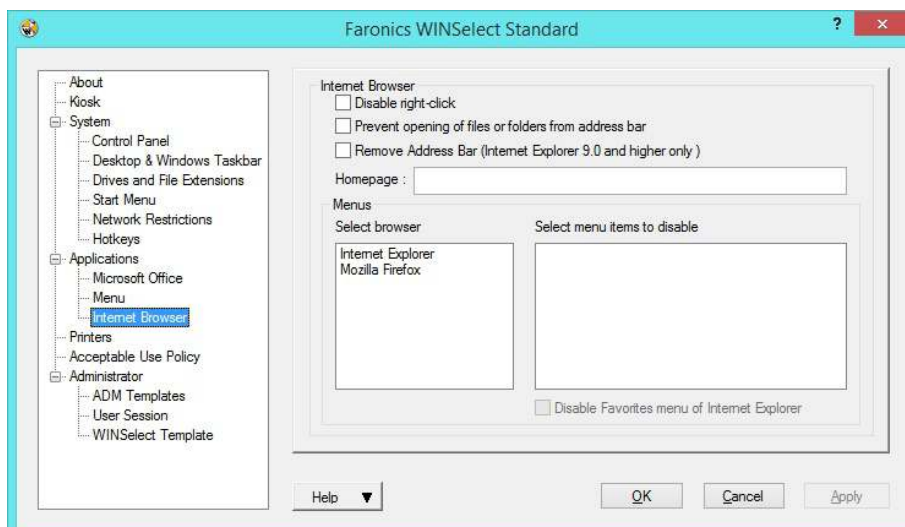
Disable right-click functionality by selecting the *Disable Right click* check box. This prevents the user from accessing right-click menus and prevents the saving of links or the copying of addresses.

To prevent access to material stored on a network, choose *Prevent opening of files or folders from address bar*. This prevents the user from opening documents on local drives or directory locations on the Internet.

Specify the workstation's browser home page in the space provided. This is the web page displayed each time the browser is opened. This overrides the home page specified within the Internet browser.

Select a browser from the list and select the menu items that will be disabled in that browser. Menus such as *File*, *View,* and *Favorites* can be selected, which prevents the user from accessing them.

Entire menus can be disabled along with individual commands within menus. Select the check box next to the top level to disable an entire menu, or click to expand the menu and check the individual boxes to disable the commands found within.

Select the *Disable Favorites menu of Internet Explorer* box to disable the saved list of frequently visited web sites. The user will not be able to view the Favorites list and bookmark new favorite web pages.

⚠️ *The Disable right-click, Disable Menu (or sub-menu items), and Disable Context Menu (or sub-menu items) will gray out the menu or the sub-menu items as selected. The menu or the context-menu will still be visible, but options cannot be selected once disabled.*

Hotkeys

The Hotkeys node provides options for restricting the use of specified hotkeys at the system level. Key combinations that work in multiple applications can be disabled regardless of which application is enabled on the workstation.
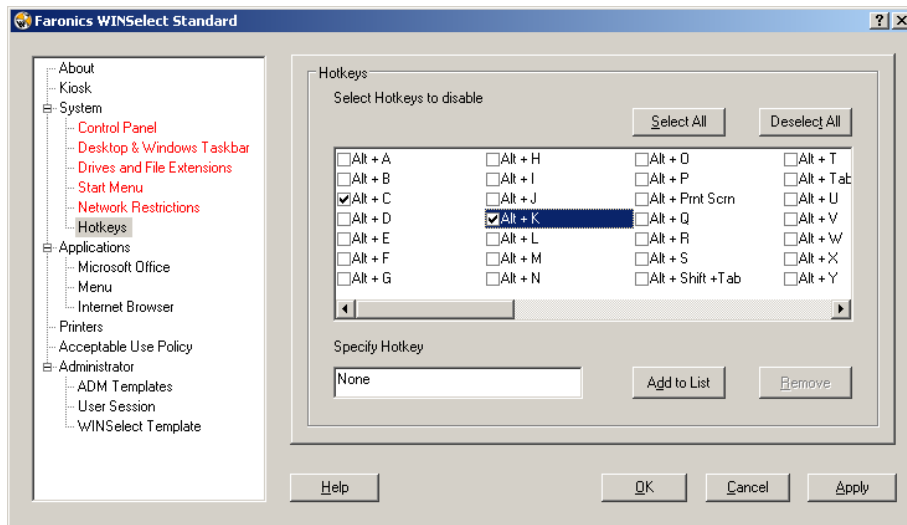
Select the hotkeys on the list that will be disabled on the workstation. Use the *Select All* or *Deselect All* buttons to select or deselect all hotkeys.

Hotkeys not listed can be added by entering the key combination and clicking the *Add to List Button.*

The *Remove* option only removes custom key combinations added by an administrator.
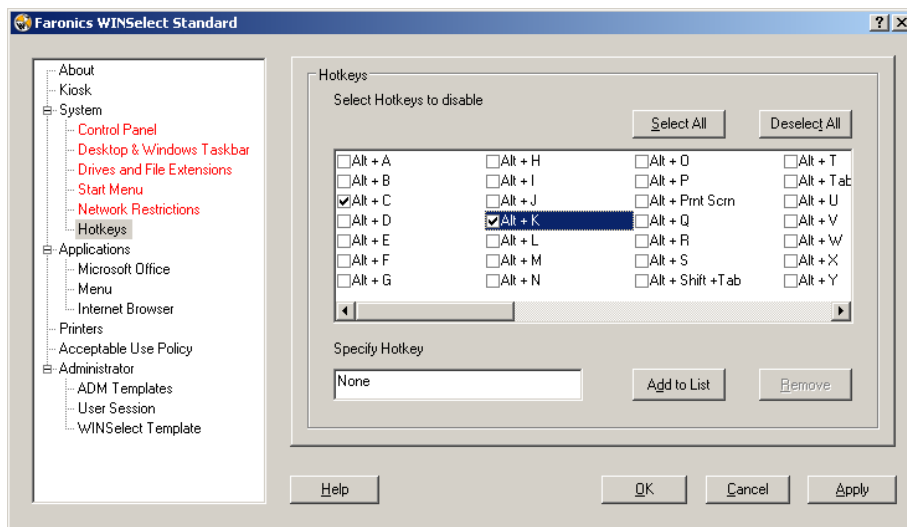
Printers

The Printers node provides options for restricting access to any available printers connected to the workstation. Use this feature to restrict printers entirely, or to permit users to print a specific amount of material on one or more selected printers.

Access to offline printers can be restricted. This is useful to remember since offline printers can still receive printing jobs.
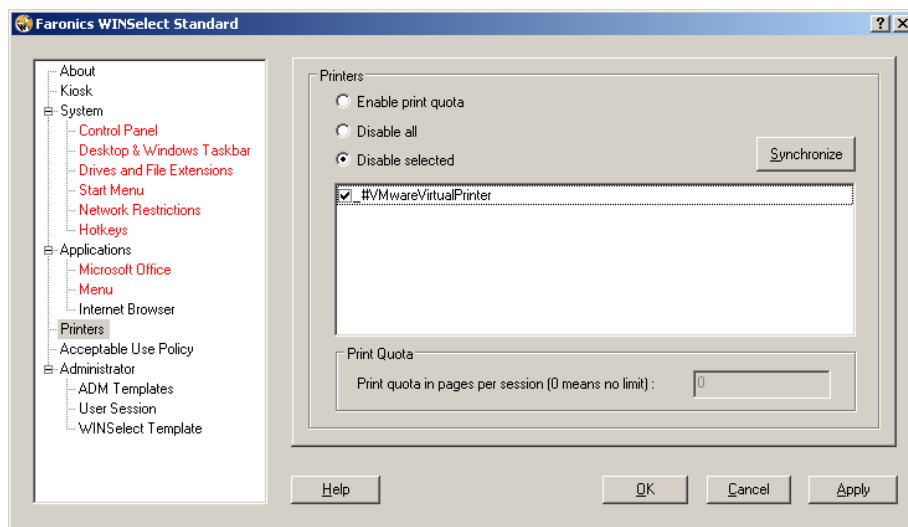
Select one of the three options available for configuring printer access. *Enable print quota* does not disable any printing capabilities. It only places a restriction on the amount of pages a user can print from the workstation. If choosing to specify a printing quota enter the number of pages per session in the box provided. Entering 0 (zero) denotes no limit.

Disable all restricts printing from each printer that has been added to the workstation. If choosing to disable selected printers only, select the specific printers on the list and select *Disable Selected.*

For more information on adding and connecting printers, refer to your Windows documentation.

To refresh the list of available printers click the *Synchronize* button This is useful if a printer has been recently connected to the workstation while WINSelect is enabled.

Acceptable Use Policy

The Acceptable Use Policy node allows for display of an Acceptable Use Policy (AUP) at the start up of the workstation. This feature allows the administrator to specify the conditions of use each time a user logs into a workstation. The user must accept this policy before using the workstation.

There is no file size restriction and only files with the *.rtf* extension can be imported.
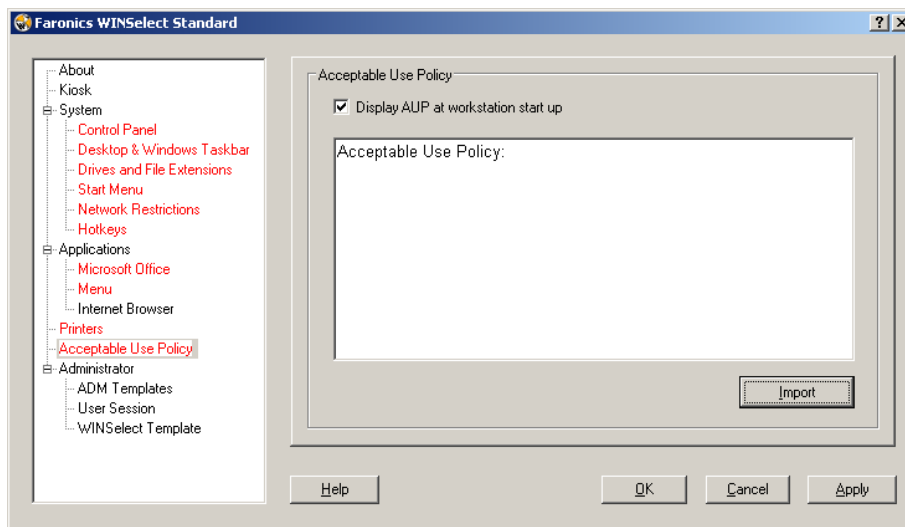
To enable this feature, select *Display AUP at workstation start up*. Once this setting is enabled, the user will not be able to access the workstation without accepting the policy.

Click *Import* and browse to the location of an *.rtf* file that has the AUP text.
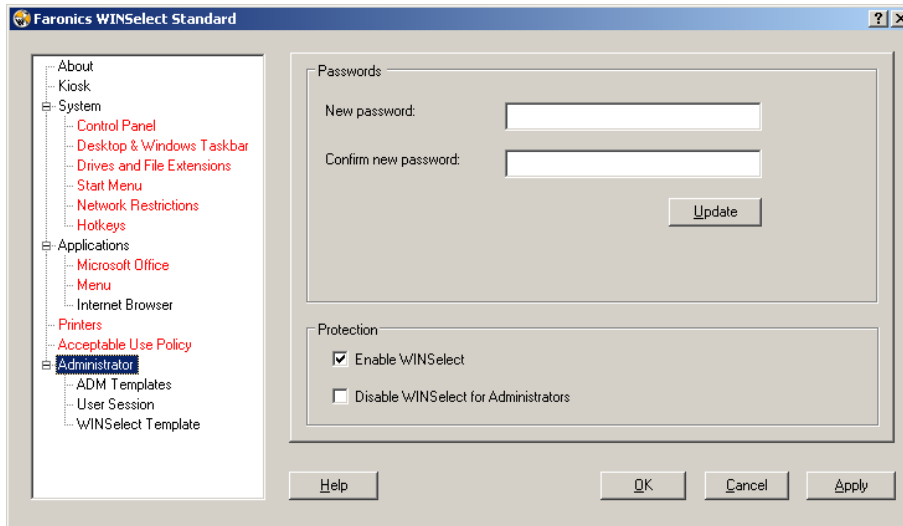
⚠️   *WINSelect does not enforce statements made in imported Acceptable Use Policy.*

Administrator

The Administrator node is used to change passwords required by administrators, and to enable or disable WINSelect.

Passwords

To set a new password, type the new password in the *New password* field. Enter and confirm the new password. Click *Update* to update the new password. The password initially set following the WINSelect install is replaced by the new one. Only one administrator password can be set.

Protection

Choose if WINSelect is enabled on the workstation, and if WINSelect is disabled for administrators.

If *Disable WINSelect for Administrators* is selected, the restrictions specified in WINSelect will not apply to users who log in as Windows administrator.

ADM Templates

The Active Directory Management (ADM) Template node provides the option to import and configure *.adm* templates. Since WINSelect provides administrators with an interface to edit Group Policy settings, administrators can create their own *.adm* templates to supplement WINSelect's features.

For more information consult the Microsoft support article regarding Active Directory Management.
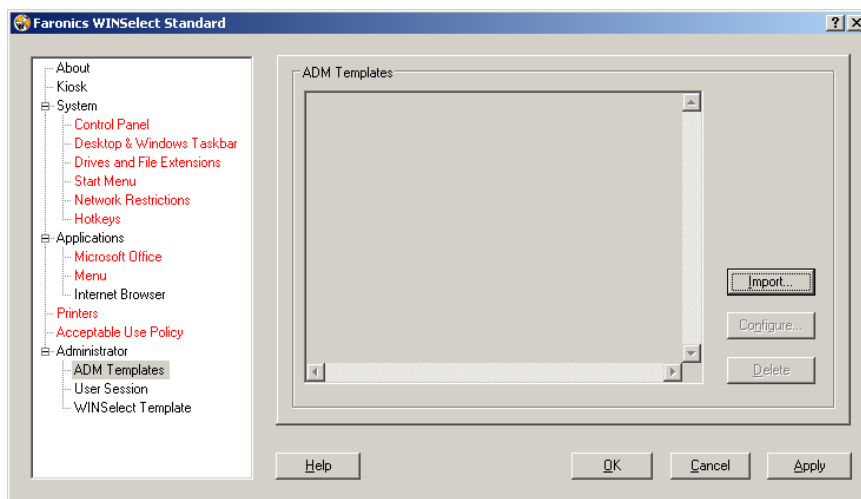
Select *Import* to add an *.adm* file. Importing an *.adm* template creates a *WINSelect.adm* file located in *C:\WINDOWS\inf.*

Once an *.adm* file has been opened, select *Configure* to open the Group Policy Editor where changes can be made.

Delete the ADM template by clicking the *Delete* button. Deleting the ADM template does not remove the applied settings. It only removes the template from the WINSelect Control Panel. Changes must be made by selecting *Configure* or through the Windows Registry Editor.
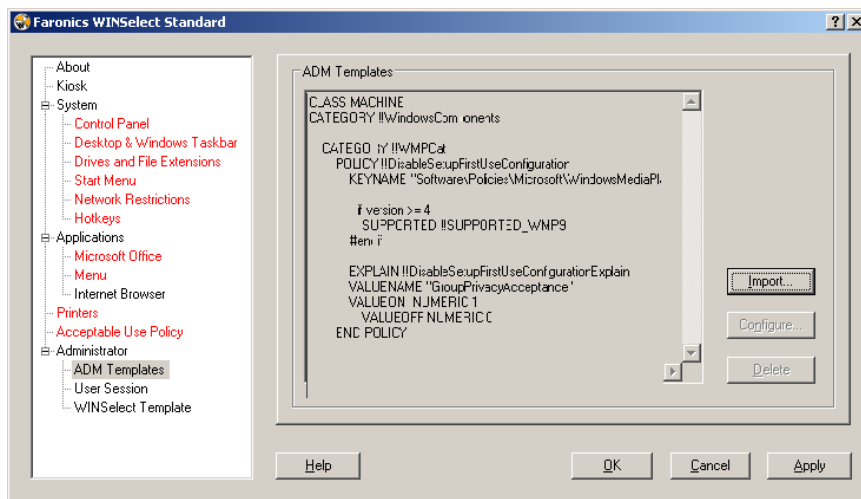
⚠️ *Only one ADM template can be active at a time.*

User Session

The User Session node provides the option to create user sessions that are limited in duration. This allows the administrator to specify the amount of time a user can spend logged into a workstation.
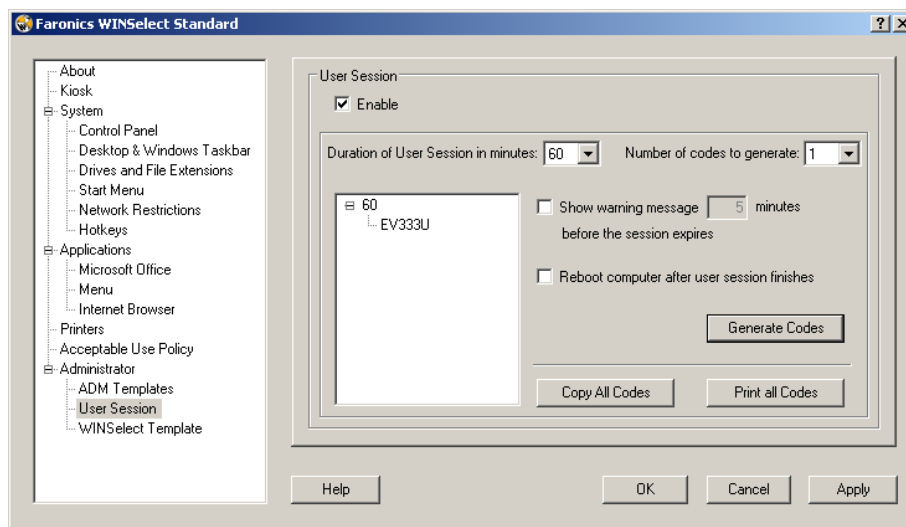

To enable the User Session feature, ensure *Enable* is selected and perform the following steps:

1. Choose the *Duration of User Session in minutes* for the session from the drop-down. Time values range from 5 minutes to 1440 minutes.

2. Choose how many session codes to be created from the *Number of codes to generate* drop-down. Count values range from 1 to 1000.

3. To display a warning select the *Show warning message x minutes before the session expires* check box. Specify a value for *x* between 1 and the *lowest user session -1.* For example, if you have selected three sets of user sessions with duration 15, 30, and 60 minutes, the warning must be between 1 and 14.

4. To reboot the computer after the user session, select the *Reboot computer after user session finishes* check box.

5. Click *Generate Codes.*

6   Click *OK.*

⚠️ *WINSelect Protection has to be Enabled for the User Session settings to be applied. If WINSelect Protection has not been enabled, select the Enable WIN Select check box in the Administrator node.*

After the Windows logoff (to apply the new settings) the next user to use the workstation is prompted to enter a generated code at the beginning of the user session.
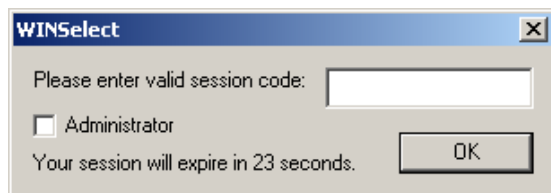
If you are the administrator, you can select the *Administrator* check box. The WINSelect login screen is displayed. You can enter the administrator password to launch WINSelect in Administrator mode. If you are logged in as the workstation user, and the session reaches its allotted time, a dialog will appear asking for a new code to be entered. The user will not be able to use the workstation until the new code has been entered. If a new code is not entered, the session will expire. Once a code has been used, it is automatically removed from all workstations on the network. If you login as an administrator, the user session never expires.

After logging on to the computer using the code, the following status bar is displayed at the top of the screen.

If the *Show warning message x minutes before the session expires* check box is selected in the User Session node, a warning is displayed x minutes before the expiry of the session.
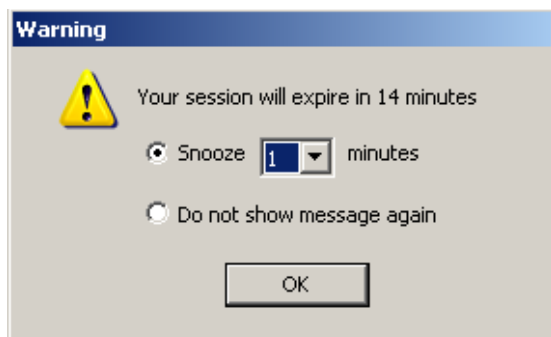
Click *Snooze* and select the number of minutes from the drop-down. Click *OK*. The warning will be displayed again after the selected duration.

If you do not want the warning to appear again, click *Do not show message again* and click *OK*.

Administrators can create multiple codes for multiple session lengths within this node. These codes can then be given to users to logon to this workstation. If only one code needs to be printed, right-click the code and select *Print*.

To remove an individual code, right-click on it and select *Remove*. To remove a group of codes, right-click the first node in the list and select *Remove*.

Click *Copy all Codes* to copy all the generated codes to the clipboard. You can launch the program of your choice and paste the codes.

Click *Print all Codes* to print all the generated codes using the default printer.

WINSelect Templates

The WINSelect Templates node provides the option to export all configured WINSelect settings as a WINSelect template. This template can then be deployed to any number of workstations protected by WINSelect.

It is saved in a proprietary file format and can only be opened by WINSelect.
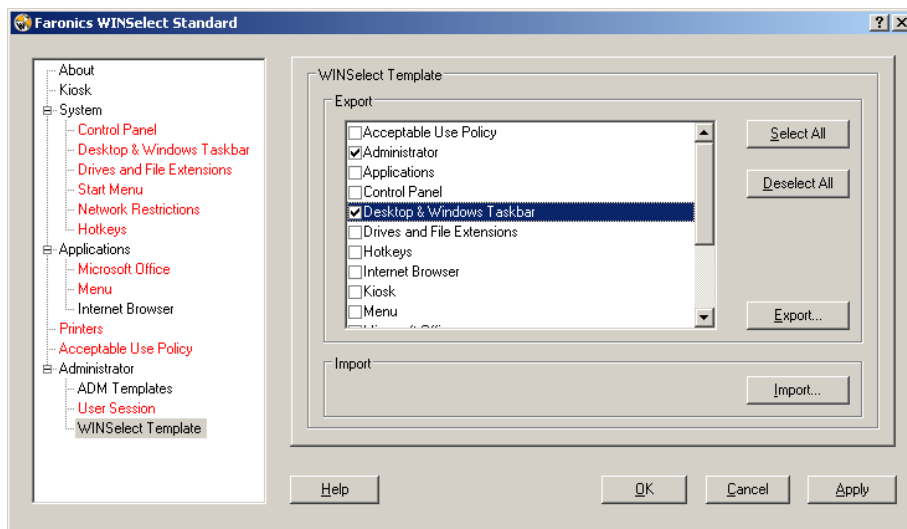
To create a WINSelect template, select all the settings that are to be part of the template in the list of WINSelect nodes. Use the *Select All* or *Deselect All* options as required. Click *Export*, browse to a location to save the template, and save it with a unique name.

To import a WINSelect template, click *Import* and browse to the location of the preferred template. Select the template and click *Open*.
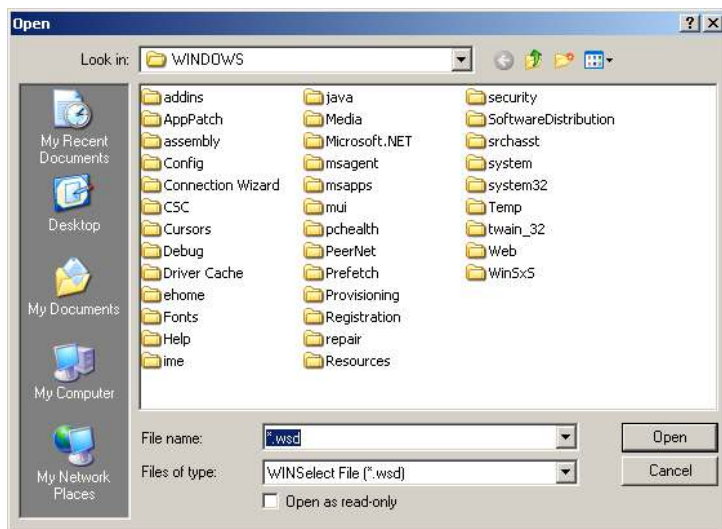
Using the WINSelect Kiosk Mode

This setting allows administrators to create a kiosk type workstation where only specified executables can be run. It also disables access to the Start button and Windows Taskbar. To access the Kiosk mode, click on the Kiosk node in the left pane of the Administrative Console.
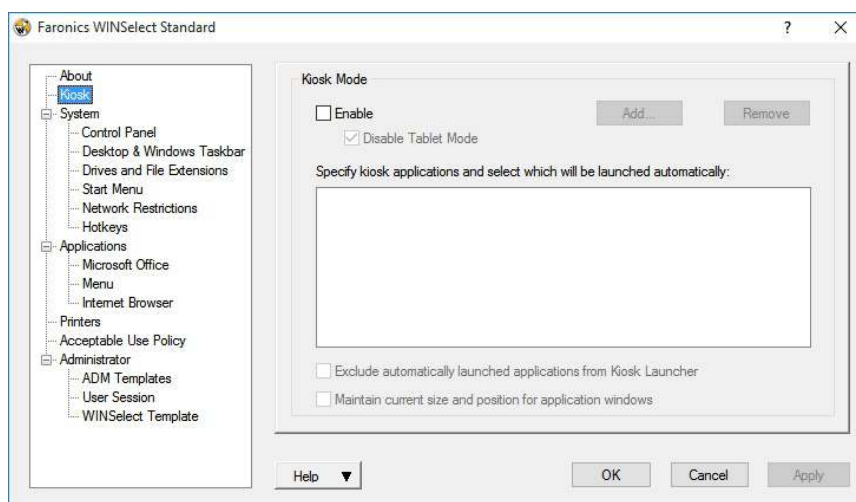
To create a Kiosk workstation, select *Enable* in the WINSelect Kiosk Panel. Select *Disable Tablet Mode* to disable launching in Tablet Mode.

To add an application, click *Add* and enter any executables that are active on the workstation. Once added to the list, these applications are available to the workstation user. Any application with a selected check box next to it will appear maximized on screen following a restart. Applications that are not selected will still be available and can be accessed through the WINSelect Kiosk Panel. The applications added to the Kiosk Panel should remain open till the settings are applied in WINSelect.

Use the *Maintain current size and position check box for application windows* to specify the window size and desktop placement for enabled applications. If this option is selected, the applications will open immediately and the administrator can set the size and position by clicking and dragging window frame edges.

> ⚠️ **Desktop shortcuts cannot be added to the list of applications; the executable itself must be added.**

There are three ways which a WINSelect Kiosk can function:

- One or more maximized applications: These can be selected using the Windows Taskbar. Enable these by selecting a series of applications using the *Add* button and select the check box next to each added application.

- Applications selected but not maximized: Applications can be accessed from the WINSelect Kiosk Panel. Configure by selecting a series of applications using the *Add* button and leaving the check boxes cleared. The user will switch between these applications using the WINSelect Kiosk Panel.

- Applications selected, size specified, and placed by the administrator: Configure by selecting a series of applications and selecting the *Maintain current size and position for application windows* check box for application windows.

The Kiosk panel is minimized to the Taskbar upon startup.

To remove an executable from the Kiosk list, select it and click *Remove*.

When Kiosk Mode is enabled the following settings are automatically applied and cannot be disabled:

- Task manager is disabled
- Right-click is disabled on Taskbar and Start Menu
- Taskbar icons are hidden (System Tray, clock)
- Start button is completely disabled
- Applications are disabled
- All UNC (Universal Naming Convention) paths are disabled
- Printing is blocked on Internet Explorer and Firefox

Click *Apply* to save the changes and create the Kiosk settings. A logoff is required for changes to take effect.

WINSelect Kiosk Panel

When the WINSelect Kiosk is active on a workstation, the selected applications appear in the WINSelect Kiosk Panel. By default, this panel is minimized to the Taskbar on startup. Click on the Taskbar to maximize the WINSelect Kiosk panel.

Using the WINSelect Wizard Mode

The Login window offers the option to enter *Wizard Mode*. The Wizard is a condensed version of the Administrative Console offering limited options to lock down a workstation.

The Wizard is best used when an administrator wishes to quickly create a Kiosk or when an administrator wants to restrict access to Windows features such as the Start menu, Task Manager, and Windows Explorer.

The first screen of the Wizard appears as below:
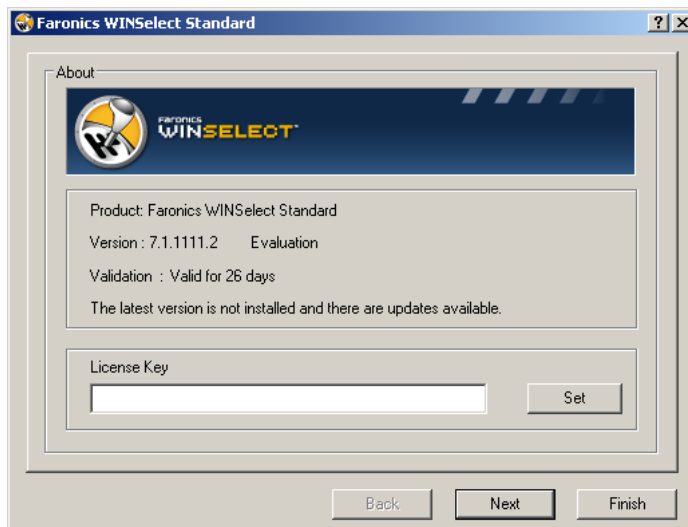
The *Kiosk Mode* screen appears. To skip this step, leave the *Enable* box blank and click *Next*.
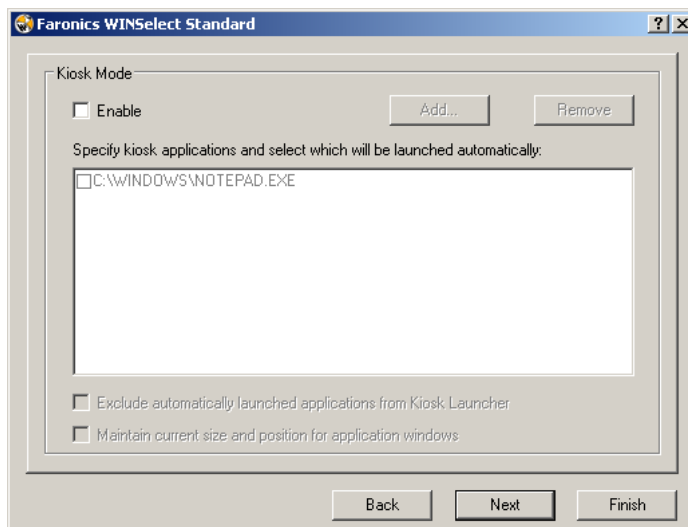
1. Select *Enable* to create a Kiosk.

2. If *Enable* is selected, click *Add* to list any executables that can be added to Kiosk mode.

   Customize the desktop view by selecting the *Maintain current size and position for application windows* check box. This feature immediately opens selected Kiosk applications which the administrator can then size and place. These cannot be moved and resized later by the user.

   Once enabled, the size and location of the window can not be changed without returning to WINSelect.

3. Click *Next*.

   The *Start Menu* screen appears.
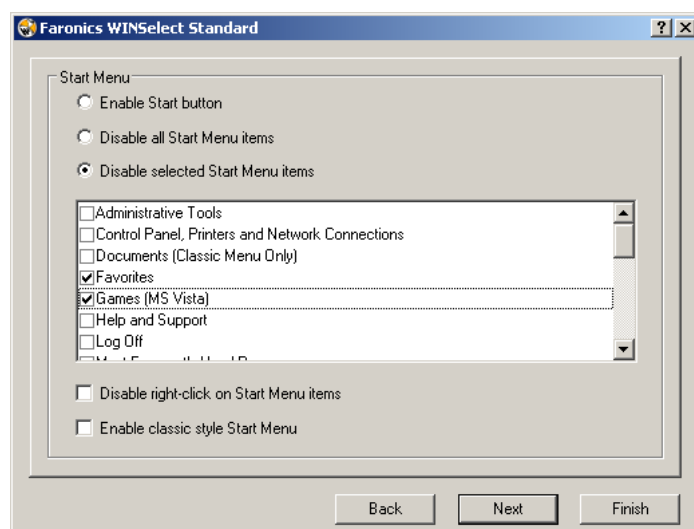
4. Select one of the three options available for configuring the Start menu. The Start menu can be displayed completely with each feature found within.

   If users are permitted to access features such as *Search*, *Run*, and *Set Program Access and Defaults* etc, those can be selected from the list.

   To prevent access to the Start Menu entirely, select *Disable all Start Menu items*.

5. Choose if the right-click on the Start menu option will be disabled. This prevents users from exploring and searching the Windows system.

   Selecting the *Enable classic style Start menu* option enables the classic style Start menu with the look and feature-limited behavior of the Windows 2000 Start menu.

⚠️ *If Kiosk mode is enabled changes to this node are not possible.*

6. Click *Next*.

The *Task Manager/Windows Explorer* screen appears. These options can also be found in the System node of the Administrative Console.
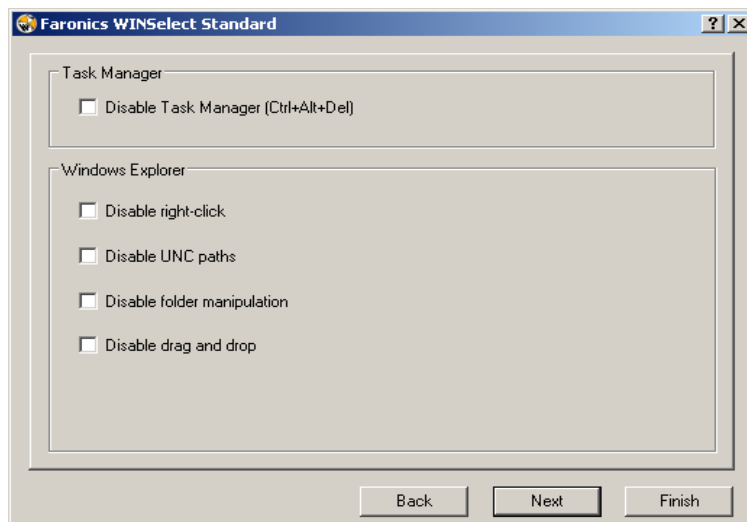
7. Choose the options to be disabled in the Task Manager and Windows Explorer.

Selecting the *Disable Task Manager (Ctrl+Alt+Delete)* check box disables the *Ctrl+Alt+Delete* hotkey which prevents the user from accessing the Task Manager or restarting the machine.
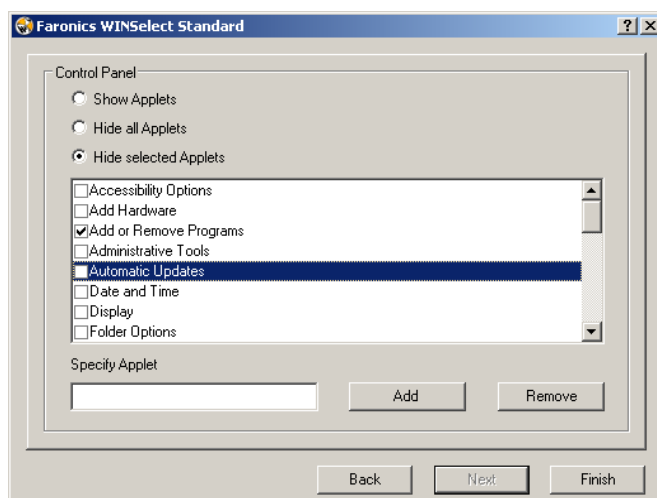
Selecting the *Disable Right click* check box prevents the user from exploring the workstation's directories.

> ⚠ ***If Kiosk mode is enabled, Disable Task Manager and Disable UNC paths are unavailable***

8. Click *Next*.

The *Control Panel* screen appears. These options can also be found in the Control Panel node in the Administrative Console.

9.   Select one of the three available options for configuring Control Panel. If you choose to disable selected applets only, select the specific applets to be disabled from the list.

10.   To add an applet to the list, enter the name in the *Specify Applet* field and click *Add*.

      To delete an applet, select it from the list and click *Delete*.

11.   Click *Finish*. The following dialog is displayed. Click *Yes* to launch the Administrative Console.

      Since the Wizard offers only typical configuration options, the Administrative Console can then be launched to configure all options.
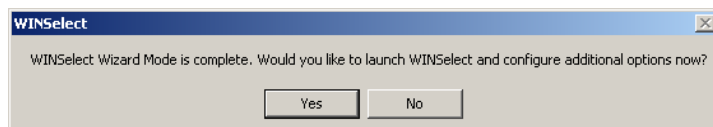
      All options that have been configured in the Wizard are carried over to the Administrative Console but can still be edited.

Appendix A: User Scenarios

The following two user scenarios outline possible WINSelect configurations according to the tasks the workstation will be used to accomplish. Other scenarios are possible as well.

User 1—Library System Administrator

Workstation Functionality	Suggested Configuration
Users are allowed to access the Internet, the library card catalog, and limited word processing capabilities.	Enable Kiosk mode with the following applications: Internet Explorer (IEXPLORE.EXE). Microsoft Word (WINWORD.EXE).
Users are prevented from using chat or email applications.	Set Internet Explorer as the default, maximized application upon start up.
An existing content filter is in place to block inappropriate web sites and other web based games or applications.	Apply an Acceptable Use Policy message indicating what is allowed on the workstation.
Users are limited to 30 minutes of computer time per session.	Enable User Sessions with a generated set of access codes.
Users can print only a specified number of pages per session.	Enable printer restrictions and set a specific limit on the pages printed.

User 2—Corporate IT Administrator

Workstation Functionality	Suggested Configuration
Users require access to Microsoft Office suite.	Configure *System* node to prevent access to the Task Manager, and to disable UNC path.
Users require access to email and their network folder to save information to. Users need to be prevented from saving to, or accessing any location on the C:\ drive, including their own profile.	Configure the *Applications* and *Internet Browser* nodes to prevent opening of files or folders from the address bar.
Users should not have any games installed on the workstation.	In the *Applications* node configure to block any applications that should not be run (games).
Internet access should be unfiltered.	Configure drives and file extensions to prevent access to C:\
	Configure Start menu to use classic layout and disable any applications that are not required for day to day operation.
	Configure Control Panel to hide all applets.
	Hide all desktop icons.