

THINSCALE

ThinScale ThinKiosk Profile Configuration Guide V 7.5





Table of Content

Table of Content	1
1. ThinKiosk Profile Overview:	5
2. Profile	6
Profile Details	6
3. ThinKiosk	7
ThinKiosk Mode:.....	7
Device Login Options:.....	8
General	8
4. Appearance	10
General Appearance:.....	10
Language:	11
Splash Screen.....	12
Appearance – Ribbon Bar.....	13
Ribbon and Status Bar Appearance:.....	13
Appearance - KioskBar	14
General Settings	15
Notification Area	17
Window Control	17
Application Exclusion:	18
Appearance – Display	19
5. Applications	21
Applications:.....	21
Tile Appearance:.....	23
Behaviour:	23
Applications – VDI Connectors	24
Add StoreFront / RDS / Horizon / WVD Connector	25
Secondary Broker	27
Connector List.....	28
Citrix Integration Options:.....	29
Microsoft RDS Integration Options	31
VMware Horizon Integration Options.....	32
Applications – Connector Login.....	33
Applications – Login Options	35



Legal Notice / MOTD	38
Applications – Workspace Control	39
End of Session Options:	40
Applications – LDAP Integration.....	41
Enable LDAP Password Change/Verification integration	41
Applications – Local Applications	43
Local Applications.....	44
Citrix, Microsoft RDS or VMware Horizon connections	45
6. Secure Browser	48
Secure Browser:	48
General Appearance:.....	49
General	50
VDI Controls:.....	52
Secure Browser - Web Sites	53
Adding / Editing a Site	53
Adding / Editing a Site	54
Secure Browser - URL Filtering	56
7. Access Policies.....	59
Network.....	59
Windows Update.....	60
8. Computer Settings.....	61
Local Device Restrictions	61
Ctrl+Alt+Del Screen:	62
Computer Settings – Startup Script.....	64
Startup Script.....	64
Computer Settings – Login Script	65
Login Script	65
Computer Settings – Logoff Script.....	66
Logoff Script	66
Computer Settings - Session Settings.....	67
Local Volume	67
Appearance:	68
Screen Saver:	68
Local Clean-up	68
Printers	68



- General 69
- Magic Filter:..... 70
- Magic Filter Delay Option:..... 71
- Computer Settings - Session Security..... 72
- Power Options:..... 72
- Computer Settings – Power Option 73
- Power Saving Options: 73
- Computer Settings - Additional Registry Values 75
- Additional Registry Values:..... 75
- Computer Settings - Proxy Server Settings 77
- Computer Settings - Privacy Settings (Win10) 78
- Computer Settings - Lock Screen..... 79
- Computer Settings – Authentication Helper 80
- 9. End Point Protection:82**
 - Windows Security Centre Detection 82
 - End Point Protection - Windows Security Centre Detection..... 82
 - End Point Protection - Windows Patch Management..... 84
 - End Point Protection - Windows Firewall Control..... 90
 - Windows Firewall Control 90
- 10. End Point Security93**
 - End Point Security - Wi-Fi Adapters 93
 - End Point Security - Virtual Machine Detection..... 94
 - End Point Security - USB Device Blocking..... 95
 - End Point Security – Temporary Storage 96
 - Enable Temporary Storage..... 96
 - End Point Security - Application Execution Prevention..... 98
 - Application Execution Prevention 98
 - End Point Security - Application Execution Prevention (Offline) 105
 - End Point Security - Service Execution Prevention 107
 - Service Execution Prevention..... 108
 - Service Execution Prevention - User Notifications..... 110
- 11. Administration..... 111**
 - Administrator Access:..... 111
 - Administrative Access: 112
 - Exclusions: 112



Inclusions:.....	112
Administration – Screen Capture	113
SMTP Settings:.....	113
Server Details:	113
SMTP User Credentials:.....	113
Default Values:	114
12. Software Package Installation	115
13. Client Paths	116
14. ThinScale Virtual Desktop Agent	117



1. ThinKiosk Profile Overview:

The ThinKiosk profile provides all the configurations required for the ThinKiosk client.

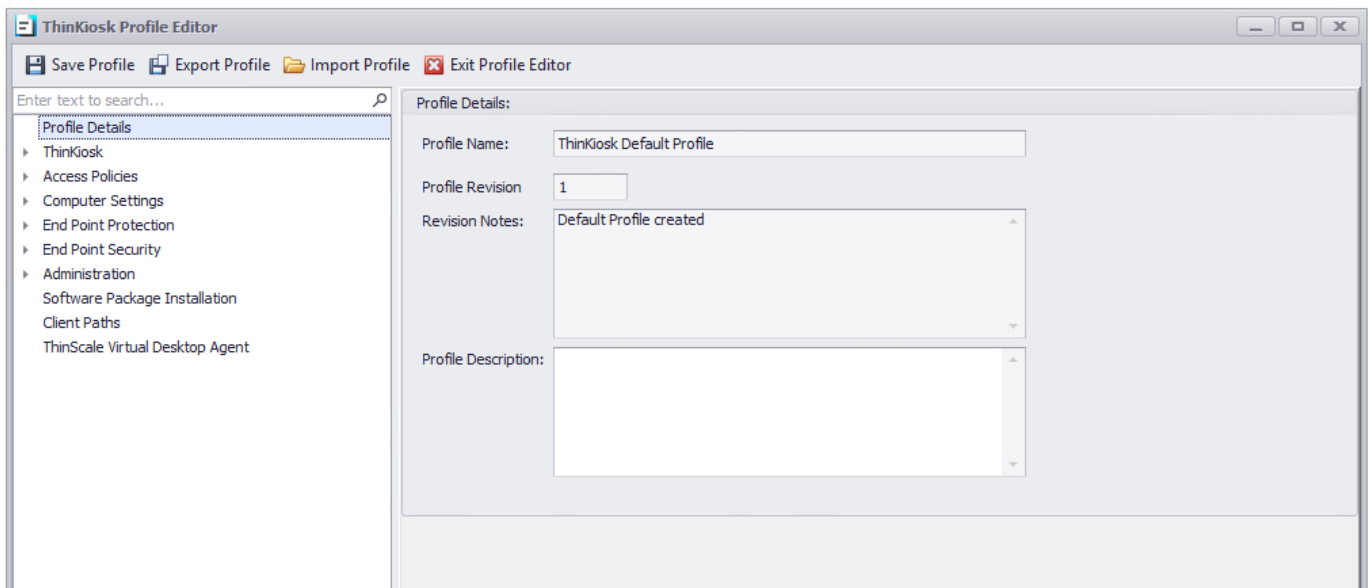
This profile is JSON based and very easy to modify with the new ThinKiosk Profile Editor.

The profile editor can be accessed in separate ways depending on the profile delivery method you have opted for.

- ThinScale Management Server - From the ThinScale Management Console, right-click your profile and select 'Edit Profile'
- Local Profile - From the ThinKiosk 'Admin' menu select 'Profile Editor'
- FTP – Using the Profile Editor the profile can be exported and then saved to the configured location on your FTP server.



2. Profile



Profile Details

Profile Name

Shows the profile's name.

Profile Revision

Shows the total amount of edits you made on the profile.

Revision Notes

Shows the comments you added when editing a profile.

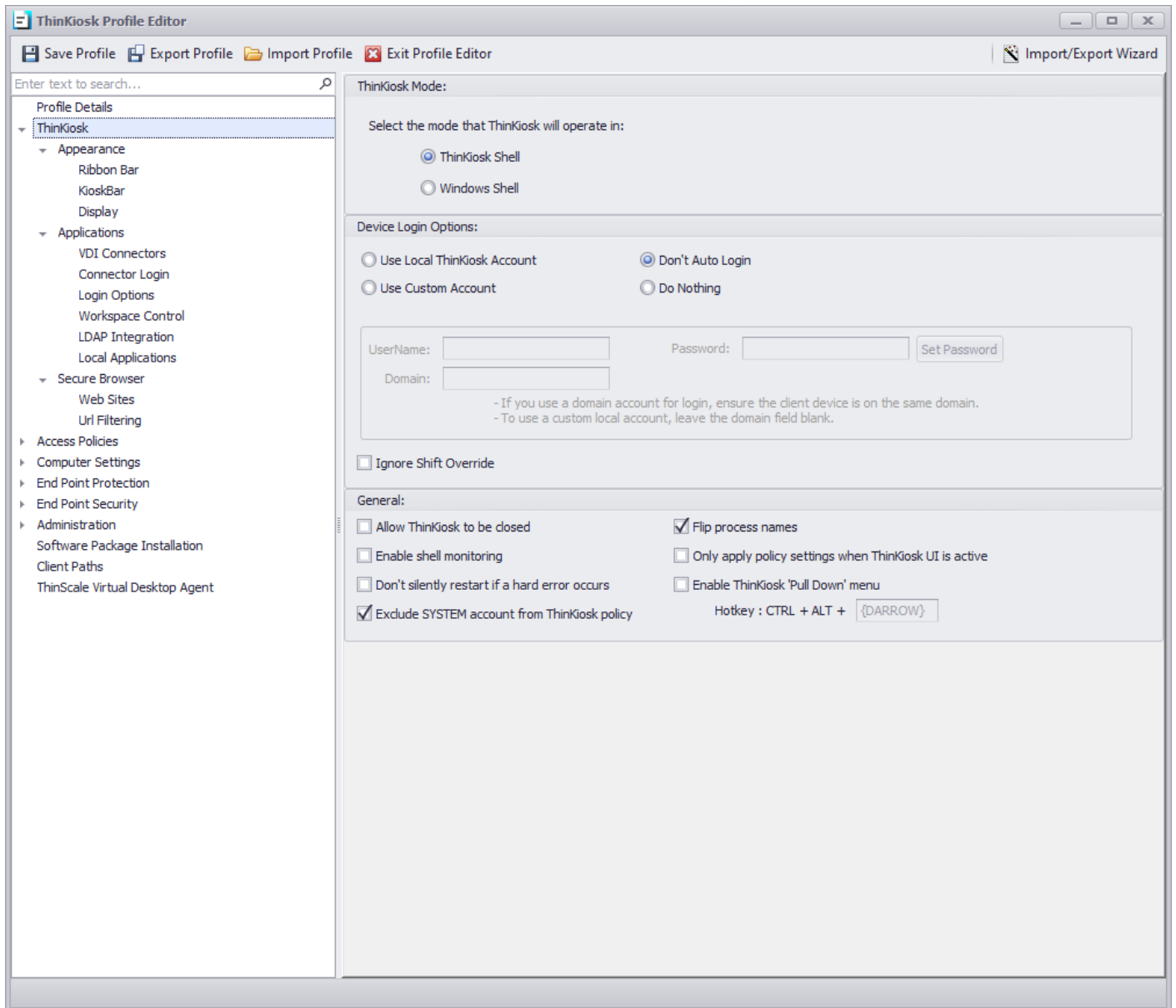
Profile Description

Brief description of the profile.

Note: based on the comments, you can track changes made on that profile and revert to a previous revision if desired.



3. ThinKiosk



ThinKiosk Mode:

ThinKiosk Shell

ThinKiosk UI is configured as the Windows shell and Windows Explorer will NOT run.

Windows Shell

Windows Explorer is used as the Windows shell application.



Device Login Options:

Use Local ThinKiosk Account

The device will auto-login using a local account 'ThinKioskUser' created by ThinKiosk. This user is a low privileged user account.

Use Custom Account

The device will auto-login using the credentials supplied in the Username / Password and Domain fields. This can be an alternate local account, or a domain account if the device is domain-joined.

Don't Auto Login

Disables any configured auto-login settings.

Do Nothing

ThinKiosk will not apply or remove any auto-login configuration. If the device already has auto-login configuration applied or this configuration is delivered by other means it will remain in place.

Ignore Shift Override

Prevents the left shift key from overriding the auto-login configuration.

General

Allow ThinKiosk to be closed

If enabled, users will be able to close the ThinKiosk UI.

Note: This is not recommended if ThinKiosk is configured as the shell.

Flip process names

The ThinKiosk UI ships as two executables: ThinKiosk.exe and iexplore.exe, these executables are identical.

By default, ThinKiosk uses the iexplore.exe as the shell process, unless the Flip process names option is enabled.

Enable shell monitoring

Enables ThinKiosk's shell monitoring application which can be accessed via the CTRL + ALT + BREAK hotkey combination.

Only apply policy settings when ThinKiosk UI is active

When enabled, ThinKiosk locks down policies will only apply when the ThinKiosk UI is active.

Don't silently restart if a hard error occurs

This option has been retired and is no longer available.

Enable ThinKiosk 'Pull Down' menu

This option enables the CTRL + ALT + DOWN ARROW hotkey combination to display the ThinKiosk 'Pull Down' menu.



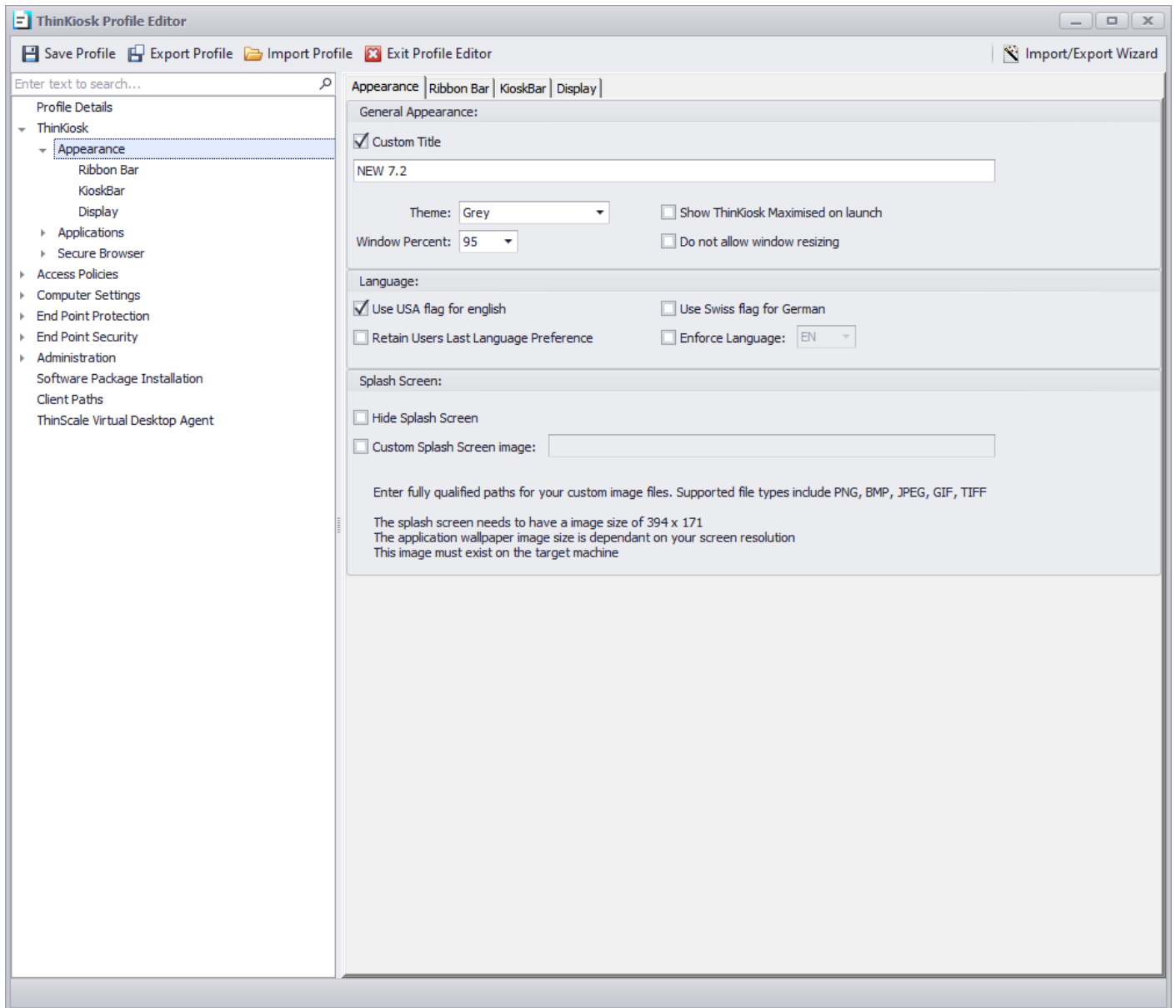
ThinKiosk's 'Pull Down' menu can be accessed even when connected to a full-screen remote session allow you access to options available on ThinKiosk's ribbon bar.

Exclude SYSTEM account from ThinKiosk policy

If enabled, an action performed under the SYSTEM account will be allowed to run. Useful when a write filter is installed on the machine.



4. Appearance



General Appearance:

Custom Title

Allows you to configure a customised title for the ThinKiosk UI. If no custom title is provided, ThinKiosk will use the title 'ThinKiosk' by default.

Theme

Sets the theme ThinKiosk UI will use.



Window Percent

Set's the size of the ThinKiosk UI.

Show ThinKiosk Maximised on launch

If enabled, the ThinKiosk UI will launch maximised and will override the *Window Percent* setting.

Do not allow window resizing

When enabled the ThinKiosk UI is fixed to the size it was launched at.

Language:



Use USA flag for English

Switches the USA flag icon in language selection for the English language.

Use Swiss flag for German

Switches the Swiss flag icon in language selection for the German language.

Retain Users Last Language Preference

ThinKiosk remembers the user's language selection and automatically switches to that language the next time it starts.

Enforce Language

Forces ThinKiosk to use the selected language.



Splash Screen

Hide Splash Screen:

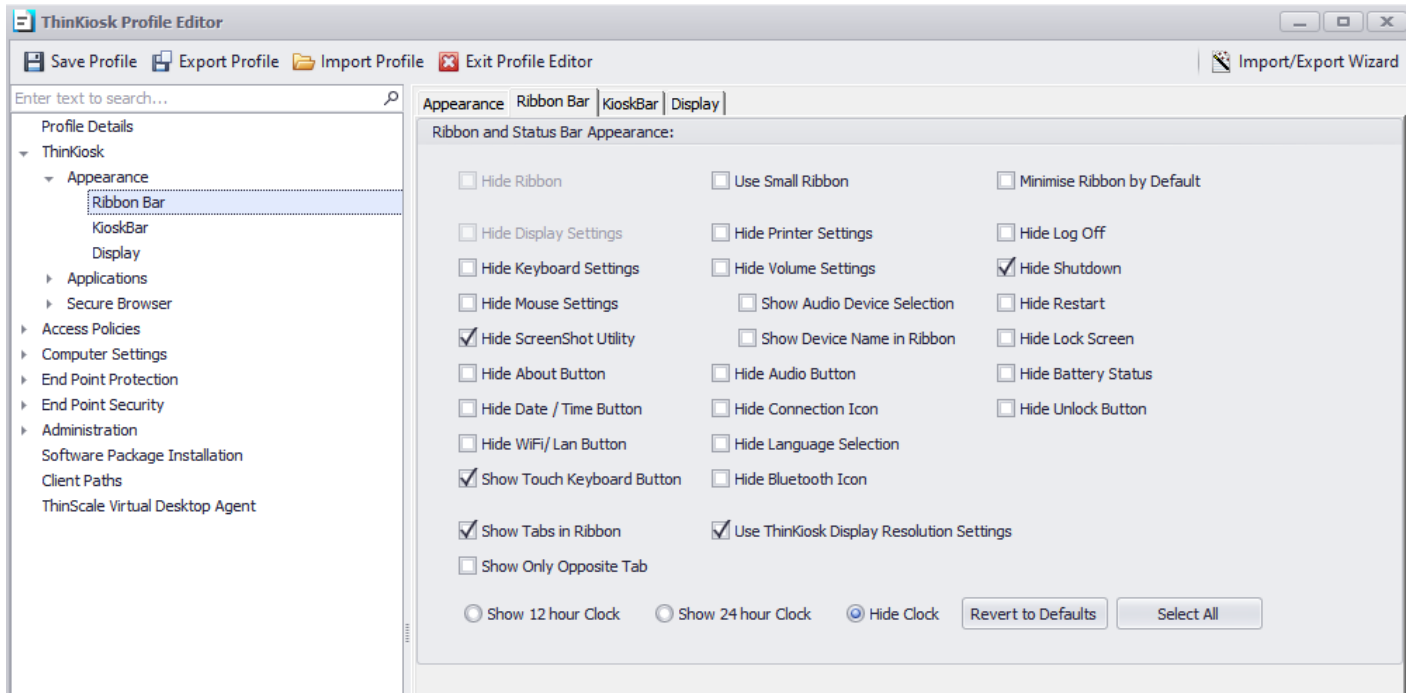
If enabled will hide the splash screen window.

Custom Splash Screen image:

Enter a fully qualified file name for the custom splash screen image. Supported file types include PNG, BMP, JPEG, GIF, TIFF. Image size 394x171.



Appearance – Ribbon Bar



Ribbon and Status Bar Appearance:

The distinct options in this section allow you to hide (if selected) the individual settings you do not require to be displayed on the ribbon bar, the status bar or the ThinKiosk Taskbar for the ThinKiosk client.

Use ThinkKiosk Display Resolution Settings

If enabled, ThinKiosk will use its display settings panel, not the built-in Windows Control Panel applet or Settings application, to allow users to change monitor resolutions.

Note: this option must be selected when ThinKiosk is the main shell or a timeout error will be shown.

Revert to Default:

If clicked will reset all the settings to the default one.

Select All:

If clicked will select all the options at once.



Appearance - KioskBar

ThinKiosk Profile Editor

Save Profile | Export Profile | Import Profile | Exit Profile Editor | Import/Export Wizard

Enter text to search...

Profile Details

- ThinKiosk
 - Appearance
 - Ribbon Bar
 - KioskBar**
 - Display
 - Applications
 - Secure Browser
 - Access Policies
 - Computer Settings
 - End Point Protection
 - End Point Security
 - Administration
 - Software Package Installation
 - Client Paths
 - ThinScale Virtual Desktop Agent

Appearance | Ribbon Bar | KioskBar | Display

General Settings:

- Show the ThinKiosk kioskbar
 - Delay startup by 0 seconds
- Show kioskbar on all displays
- Always keep kioskbar on top
- Apply background appearance to desktop
- Show time on kioskbar as 24 Hour Clock
- Show date on kioskbar as Short Date Format
- Block calendar pop-up access
- Enable diagnostic logging
- Group kioskbar buttons by application
- Combine buttons when more than 3 in group
- Expand groups on mouse click
- Expand groups on mouse hover
- Auto expand/combine groups as needed
- Prioritise buttons when moving from overflow
- Show window preview on mouse hover
- KioskBar mouse hover delay: (Normal)

Notifications Area:

- Show system notifications area
 - Block notification icon user interaction
 - Block notification balloon message pop-ups
 - Show input method selection notification icon
 - Limit the processes that can use the tray (* requires UWP support enabled)
 - Allow these processes
 - Prevent these processes

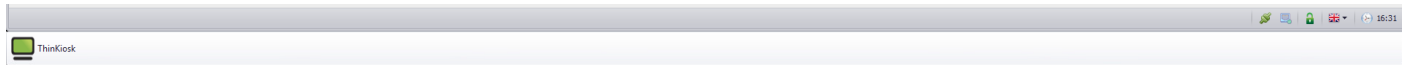
Window Control:

- Allow the user to minimize/restore application windows from the kioskbar
- Block control for application windows where the title bar contains the following text:

General Settings

Show the ThinKiosk Kioskbar

Enables the ThinKiosk taskbar. This is a replacement taskbar for the one provided by Windows Explorer, showing your currently running applications.



Delay startup by

If enabled, ThinKiosk start-up will be delayed by the number of seconds you specified in the numeric box, allowing you to wait for potential applications that need to start before ThinKiosk.

Show the KioskBar on all displays

If enabled, the ThinKiosk KioskBar will be visible to the user on all available displays.

Always keep KioskBar on top

If enabled, the Secure Remote Worker KioskBar will be always visible in the foreground of any window (VDI included)

Apply background appearance to desktop

If enabled, the wallpaper colour or customer wallpaper will be displayed on all desktops.

Show time on kioskbar as

If enabled, a 12 hour or 24-hour time will be displayed on the kioskbar.

Show date on kioskbar as

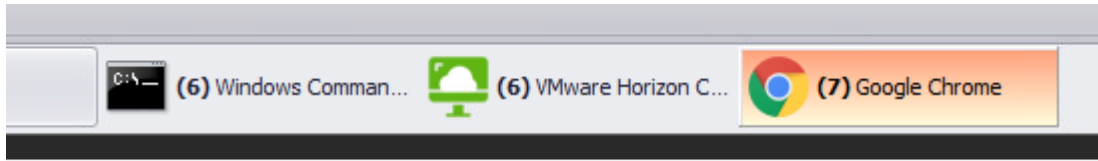
If enabled, a short or long date format will be displayed on the kioskbar.

Block calendar pop-up access

If enabled, the calendar pop-up will be denied

Group kioskbar button by application

If enabled, the new TK 7.5 will group applications together



Combine buttons when more than x

If enabled, applications will be grouped when the specified number of open windows is reached

Expand groups on mouse click

If enabled, groups will be expanded on mouse click

Expand groups on mouse hover

If enabled, groups will be expanded on mouse hover

Auto expand/combine groups as needed

If enabled, groups will be expanded based on the space left on the taskbar

Prioritise buttons when moving from the overflow

If enabled, when moving the button from the overflow to the main kioskbar area, applications clicked will move to the outer left.

Show window preview on mouse hover

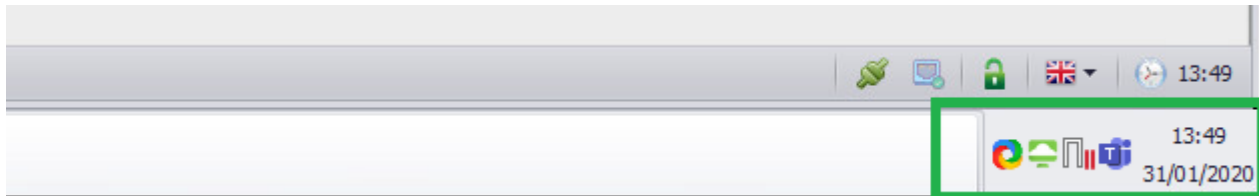
If enabled, applications preview will be displayed on mouse hover



Notification Area

Show system notification area

If enabled, a Windows systray style notification area will be visible to the users.



Block notification icon user interaction

If enabled, the right-click context menu on the notification area will be disabled.

Block notification balloon message pop-ups

If enabled, balloon tooltip messages on the notification area will be hidden.

Show input method selection notification icon

If enabled and multiple languages are installed on the system, user will be able to switch languages using the systray icon

Limit the process that can use the tray

If enabled, only the allow/ disallow process will be able to show the icon in the ThinScale systray.

Window Control

Allow the user to minimize/restore application windows from the kioskbar

If enabled, users will be able to minimize or restore any of the applications launched from the kioskbar

Block control for application windows where the title bar contains the following text

If enabled, any application added to the list will be blocked to minimize or restore using the kioskbar



Tip: Use * as a wildcard or %PRODUCT% for ThinkKiosk

--

Add

Remove

Application Exclusion:

Hide application windows where the title bar contains the following text

If enabled, any application added to the list will be hidden from the user

Tip: Use * as a wildcard or %PRODUCT% for ThinkKiosk

SelfServiceMain

Add

Remove

i.e.

Tip: Use * as a wildcard or %PRODUCT% for ThinkKiosk

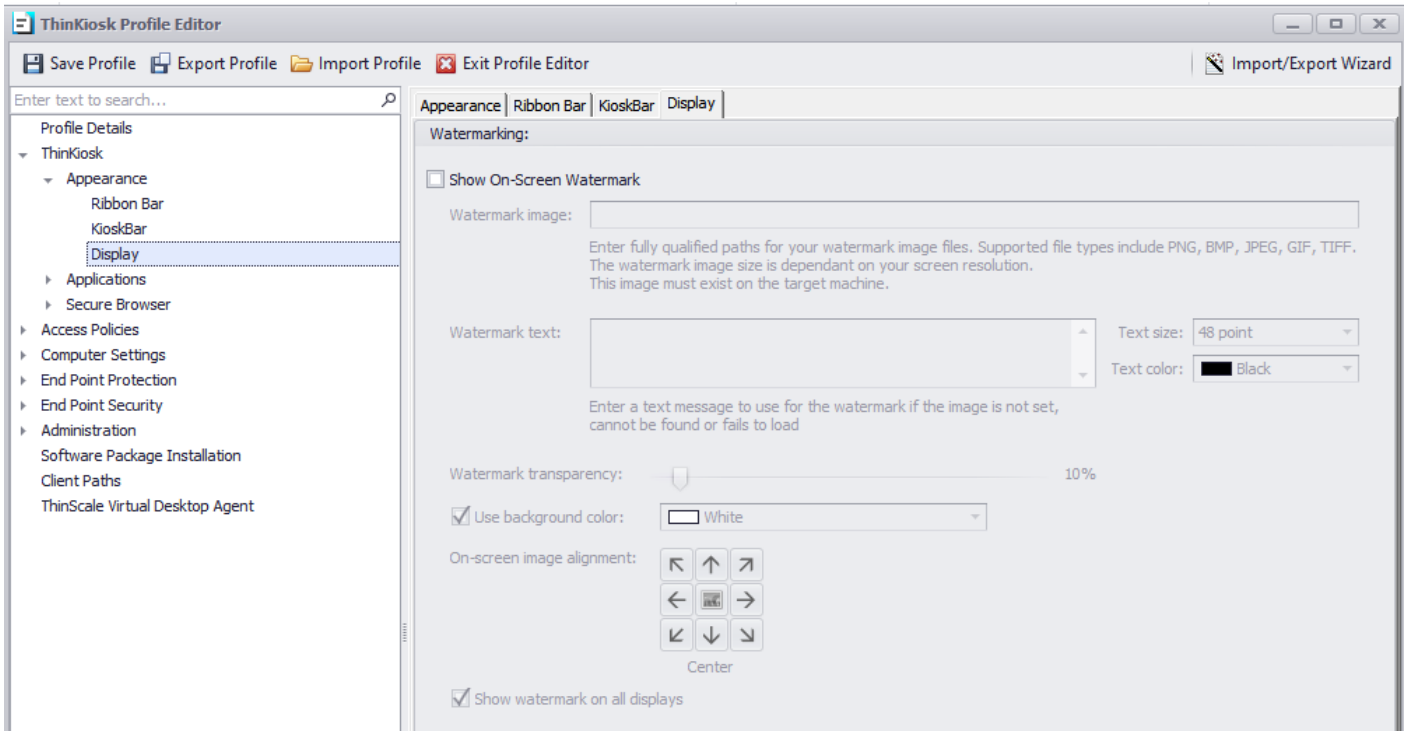
*notepad
%PRODUCT%

Add

Remove



Appearance - Display

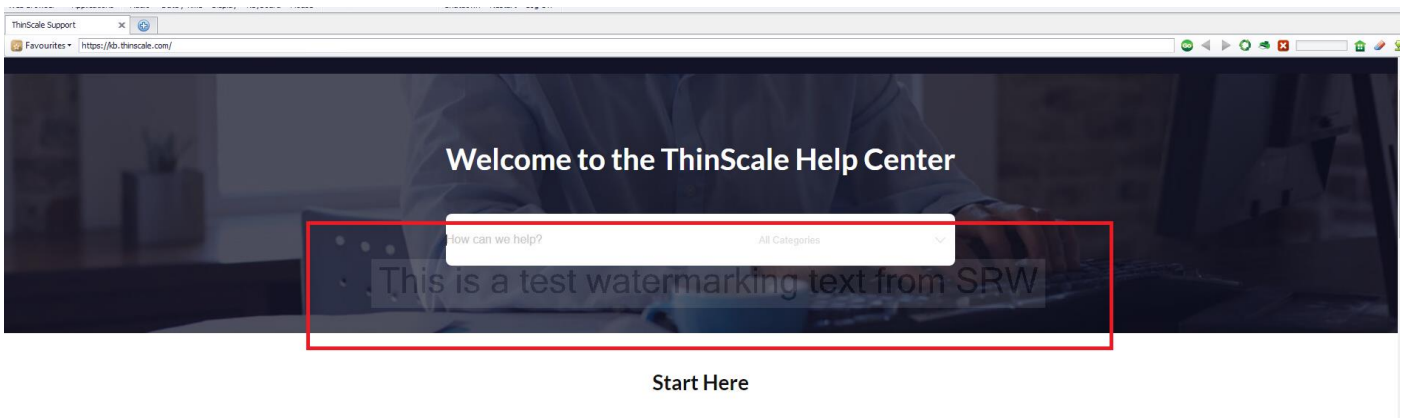


Watermark Image

The path where the overlay image must exist on the target machine.

Watermark text

If no image is found/used, you can show a personalized text on the screen as an overlay text





Watermark transparency

It is the transparency's value of the text/image displayed within the TK desktop.

Watermark transparency

It is the background colour that is displayed behind the text.

On-screen image alignment

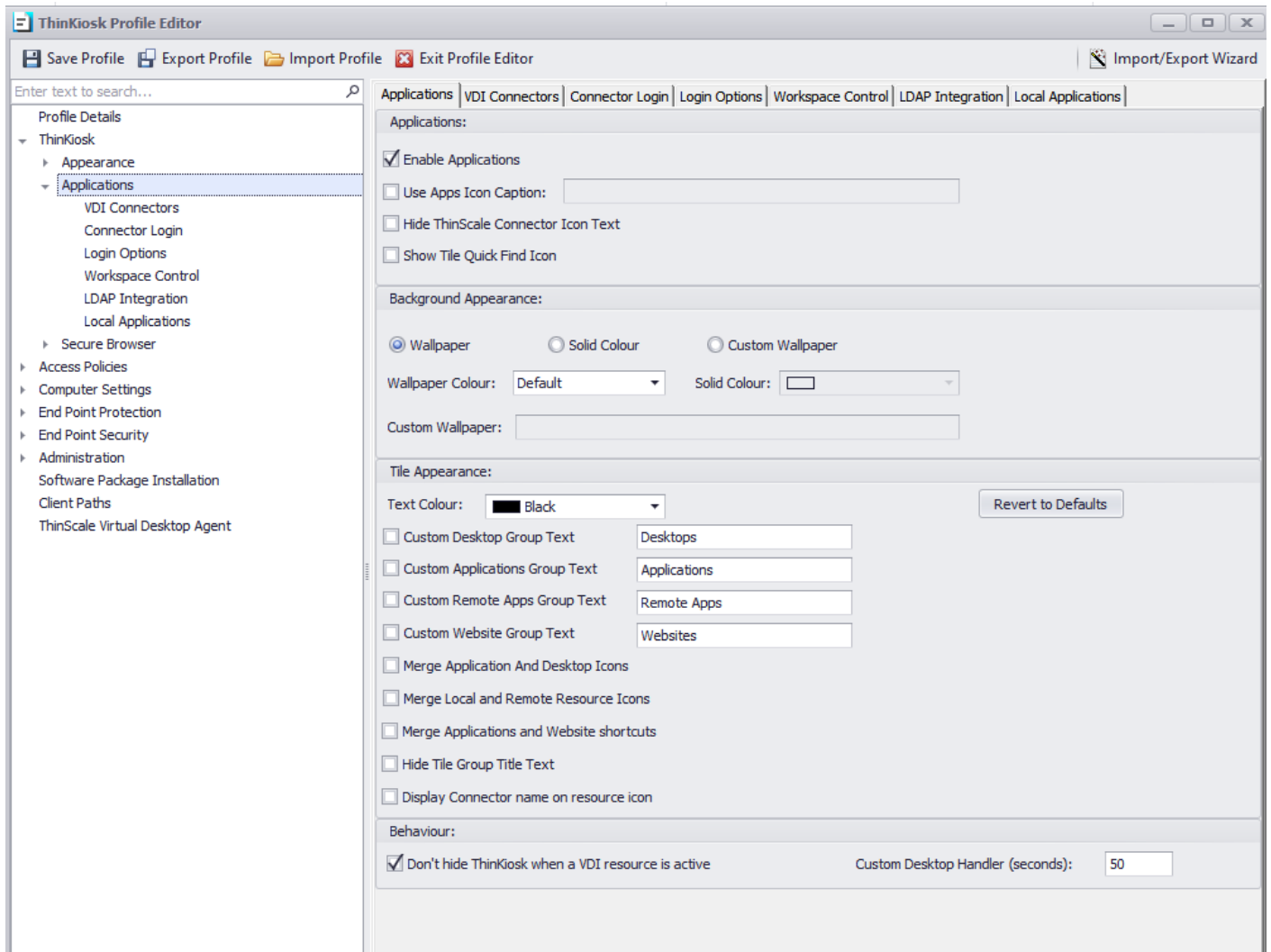
It is the position where the image or the text will be shown on the TK desktop.

Show watermark on all display

If enabled, the watermarking image/text overlay will be displayed to all monitors, otherwise only on the primary one.



5. Applications



Applications:

Enable Application

If enabled, the application tab inside ThinKiosk Desktop will be shown.

Use Apps icon caption

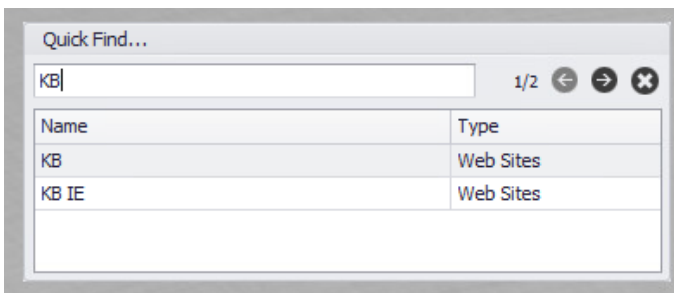
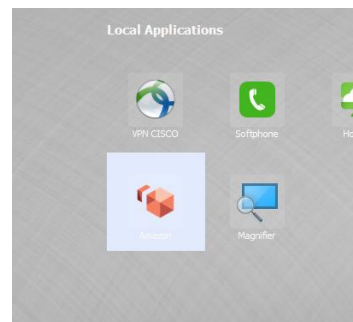
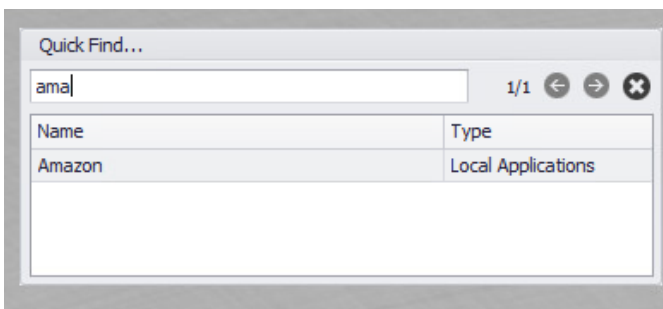
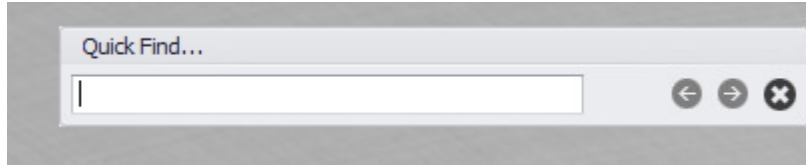
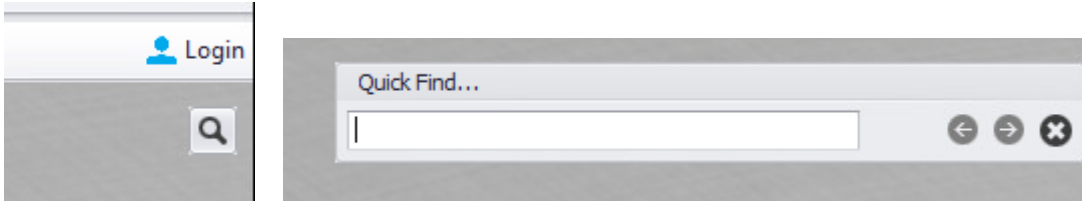
Provides a caption to use for the applications tab icon.

Hide ThinScale Connector icon text

If enabled, the 'ThinScale Connector' text that is displayed when a user is not logged on is hidden.

Show Tile quick Find icon

If enabled, the quick find icon will be shown inside the TK UI. You will be able to search local applications, VDI desktop, Remote Apps and Web sites.



Background Appearance:

Allows the configuration of either a built-in Wallpaper or a solid colour to be used as the background in the application tab within ThinkKiosk.



Tile Appearance:

Text Colour

The colour of the application's text name.

Custom Desktop, Application, Remote Apps Group Text

Allows for the customisation of the group headings in the applications tab.

Hide Tile Group Title Text

Hides the group headings in the applications tab.

Display Connector name on resource icon

The 'Connector Name' is displayed next to the resource icon.

Revert to Default

When clicked the default settings will be applied back.

Behaviour:

Don't hide Thinkiosk when a VDI resource is active

If enabled Thinkiosk will remain open in the background while in the foreground your VDI session is open.

Note: recommended if users want to switch between VDI session and Thinkiosk desktop.

Custom Desktop Handler

The number of seconds a remote session must be active for before Thinkiosk will treat it as an active session and perform End of Session options when it ends.



Applications – VDI Connectors

ThinKiosk Profile Editor

Save Profile | Export Profile | Import Profile | Exit Profile Editor | Import/Export Wizard

Enter text to search...

Applications | **VDI Connectors** | Connector Login | Login Options | Workspace Control | LDAP Integration | Local Applications

Profile Details

- ThinKiosk
 - Appearance
 - Applications
 - VDI Connectors**
 - Connector Login
 - Login Options
 - Workspace Control
 - LDAP Integration
 - Local Applications
 - Secure Browser
- Access Policies
- Computer Settings
- End Point Protection
- End Point Security
- Administration
- Software Package Installation
- Client Paths
- ThinScale Virtual Desktop Agent

Connector List:

Connector Name:	Connector Type:	Broker Address:	Enabled
Horizon	Horizon	https://tstlabvmwrbkr01.tstlab.local/broker/xml	No
StoreFront	StoreFront	http://cbxstf.tstlab.local/Citrix/tstlab	Yes

Add Connector | Edit Connector | Remove Connector

Enable TLS 1.1 support * Disable SSL 3.0 support * requires .NET Framework 4.5 to be installed on the client device
 Enable TLS 1.2 support * Disable TLS 1.0 support
 Display connector name on any error / warning messages

Citrix Integration Options:

Pre Launch Citrix Receiver (if available) Disable Citrix Desktop Viewer
 Enable Citrix Pass through authentication Use Citrix Desktop Viewer
 Don't auto accept Citrix prompts Enable Desktop Viewer Full Screen Startup
 Prompt when password is expiring Allow Desktop Restart
 Don't display errors after restart

Microsoft RDS Integration Options:

Don't disable certificate prompt Unpin the RDP Client Connection bar
 Disable remote computer identity checking Disable the RDP Client Connection bar
 Enable SSO for RD Gateway Connections

VMware Horizon Integration Options:

Disable certificate checking in Horizon Client Let the Horizon Client handle authentication
 Disable 'login as current user' option Disable the Horizon client shade menu bar
 Show Horizon View window always on top of ThinkGosk window

Automatically Connect USB on Startup Automatically Connect USB when Inserted

Enabled Enabled
 Disabled Disabled
 Allow user to decide Allow user to decide



Add StoreFront / RDS / Horizon / WVD Connector

Add StoreFront Connector [Close]

Connector Enabled

Primary Broker

Connector Name:

Broker Address:
e.g. https://storefront.domain.local

Use Local Credentials (SSO) Store Name:

Ignore SSL Errors Send username in UPN format

Display Desktop Resources Display Remote Applications

Filter Resources

(use a Regular Expression to determine which resources are displayed to users)

Secondary Broker

Enabled

Connector Name:

Broker Address:
e.g. https://netscaler.domain.com

Use Local Credentials (SSO) Store Name:

Ignore SSL Errors Send username in UPN format

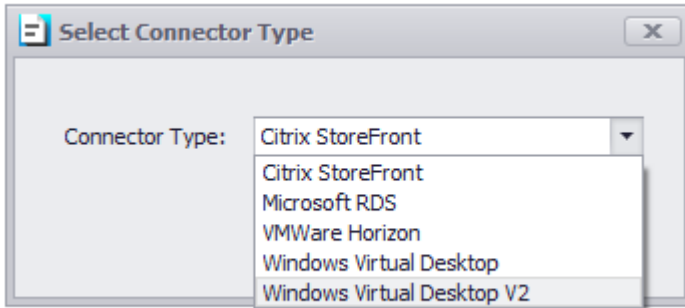
Display Desktop Resources Display Remote Applications

Filter Resources

(use a Regular Expression to determine which resources are displayed to users)

Use Secondary Broker if the following URL's are not contactable

(a semicolon delimited list of URL's to contact)



Connector Enabled

Enables the connector for resource enumeration.

Connector Name

The name of the Connector you are adding e.g. 'Production Store'.

Broker Address

URL for the broker. Examples are given on the associated add broker dialogs.

Note: WVD default connector URL is <https://wvd.microsoft.com>

Use Local Credentials (SSO)

The credentials of the currently logged Windows users are passed to the broker for authentication.

Note: This is only supported on StoreFront brokers.

Store Name

An optional Store name for StoreFront Connectors

Ignore SSL Errors

Any SSL errors are ignored during communication with the broker.

Send Username in UPN format

If enabled, the Username will be passed as User Principal Name with a format like user@domain



Display Desktop Applications

If enabled, the application created in the Application tab will be shown together with published application resources.

Display Remote Applications

If enabled, published application resources are returned along with desktop resources.

Note: RDS published RemoteApp applications require Windows Explorer to be running unless the client device is running Windows 10.

Filter Resources

You can use Regular Expression to show which resources are displayed to the users.

Secondary Broker

The secondary broker details will be used based on the network location of the device; beacons are used to determine the device location. Secondary brokers can be used when you have a separate internal and external connection URL.

Enabled

Enables the secondary broker for resource enumeration.

Connector Name

The name of the secondary connector.

Broker Address

URL for the secondary broker.

Use Local Credentials (SSO)

The credentials of the currently logged Windows users are passed to the broker for authentication. *(This is only supported on StoreFront brokers).*

Store Name

An optional Store name for StoreFront Connectors. (this is not currently used).



Ignore SSL Errors

Any SSL errors are ignored during communication with the broker.

Display Desktop Applications

If enabled, an application created in the Application tab will be shown together with published application resources.

Display Remote Applications

If enabled, published application resources are returned along with desktop resources.

Note: RDS published RemoteApp applications require Windows Explorer to be running unless the client device is running Windows 10.

Filter Resources

You can use Regular Expression to show which resources are displayed to the users.

Use Secondary Broker if the following URL's are not contactable

A semicolon-delimited list of URLs' ThinKiosk will try to contact. If any of the URL's in the list are not contactable then ThinKiosk will switch and use the secondary broker configuration details to enumerate your broker resources.

Connector List

Enable TLS 1.1 support

Enables support for the TLS 1.1 cryptographic protocol

(Note: Requires .NET Framework 4.5 or above).

Enable TLS 1.2 support

Enables support for the TLS 1.2 cryptographic protocol

(Note: Requires .NET Framework 4.5 or above).

Disable SSL 3.0 support

Disables the use of the SSL 3.0 cryptographic protocol.

Disable TLS 1.0 support

Disables the use of the TLS 1.0 cryptographic protocol.

Display Connector name on any error/warning messages

The 'Connector Name' as configured above is displayed next to the resource icon even after an error message occurred.

Citrix Integration Options:

Pre-Launch Citrix Receiver

If enabled, ThinKiosk will launch components of the Citrix Receiver such as the Connection Centre.

Enable Citrix Pass-through authentication

Enables pass-through authentication with the Citrix Receiver, this option is required if SSO is enabled in the StoreFront Connector configuration.

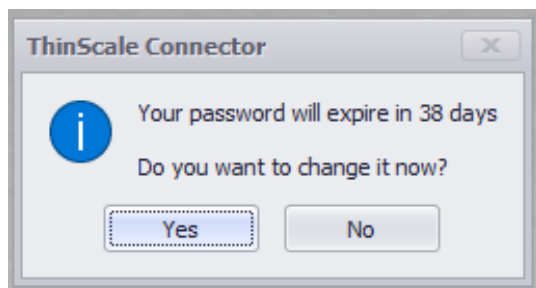
Note: Domain pass-through must be enabled in the "Manage Authentication Methods" in your StoreFront.

Don't auto accept Citrix prompts

If enabled, any pop-up prompts by the Receiver will need to be manually accepted.

Prompt when password is expiring

If enabled, during login, the end-user will be prompt with a password expiration reminder, with the option to change or continue.



Disable Citrix Desktop Viewer

Disables the use of the Citrix Desktop Viewer.

Use Citrix Desktop Viewer

Forces the use of the Citrix Desktop Viewer.

Enable Desktop Viewer Full Screen Start-up

Forces the Citrix Desktop Viewer to start desktop resources in full-screen mode.

Allow Desktop Restart

If enabled, user can restart their desktop while in TK using the new right-click option.



Don't display error after a restart

If enabled, during g server (usually multi-session) a timeout error could have been displayed. This option will hide it temporarily until the server is restarting.



Microsoft RDS Integration Options

Don't disable the certificate prompt

If enabled, any certificate warning prompts from the RDP client will be displayed.

Disable remote computer identity checking

Prevents the RDP client remote computer identity check. If the remote computer's identity cannot be verified it can cause additional security dialogs to be presented on connection.

Enable SSO for RD Gateway Connections

When enabled, user credentials will be automatically passed to RD Gateway providing a complete single sign-on experience.

Unpin the RDP Client Connection bar

When enabled, the RDP client will start with the connection bar unpinned.

Disable the RDP Client Connection bar

When enabled, the RDP client connection bar will be disabled.

VMware Horizon Integration Options

Disable certificate checking in the Horizon Client

If enabled, all certificate checking by the Horizon client will be disabled.

Disable 'login as current user' option

Disables the 'login as current user' Horizon Client feature.

Let the Horizon Client handle authentication

If enabled, authentication prompts will be handled by the Horizon client.

Disable the Horizon client share menu bar

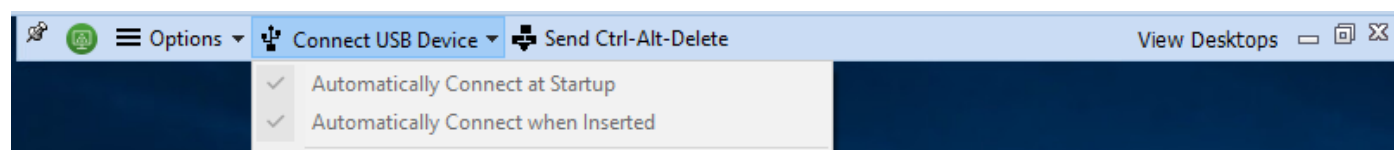
If enabled, ThinKiosk will disable Horizon's client 'shade menu bar'.

Show Horizon View window always on top of ThinKiosk window

If enabled, the Horizon View will always be opened on top of the ThinKiosk window.

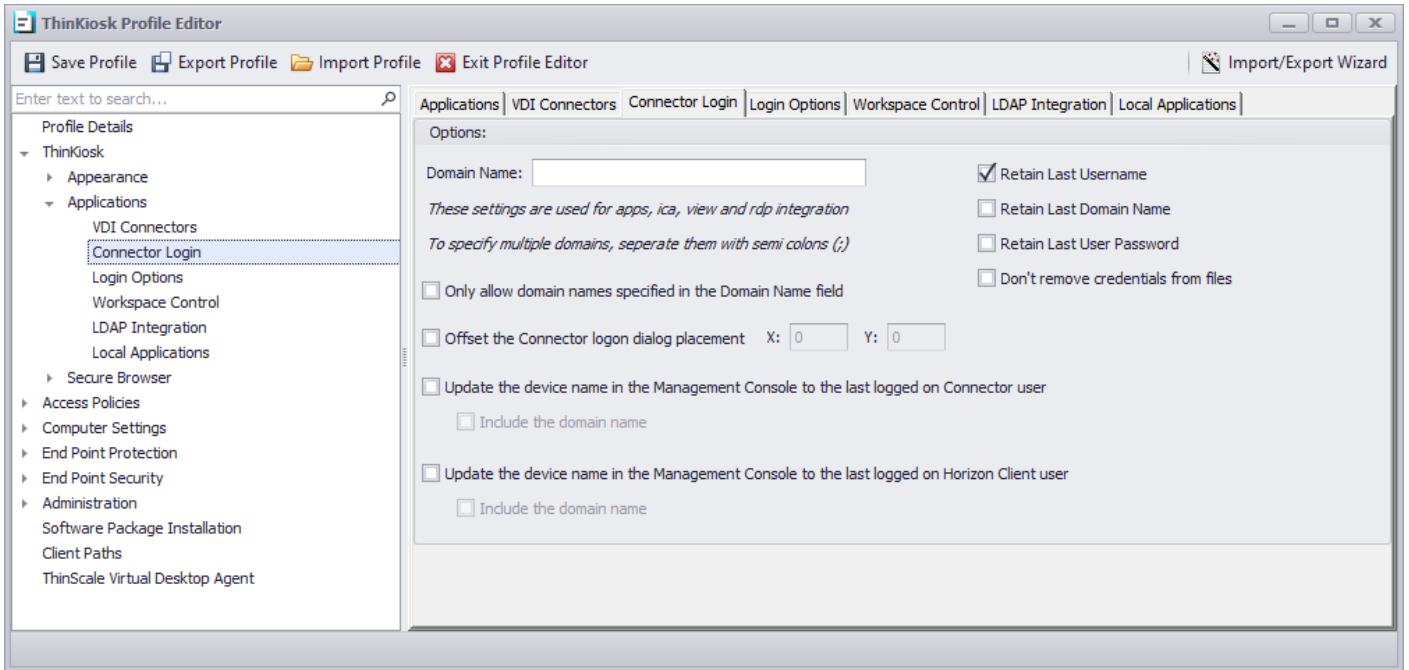
Automatically Connect USB on Startup/ when Inserted

Depending on the selected choice, the user will be able/won't be able to have access to the USB option inside the Horizon View



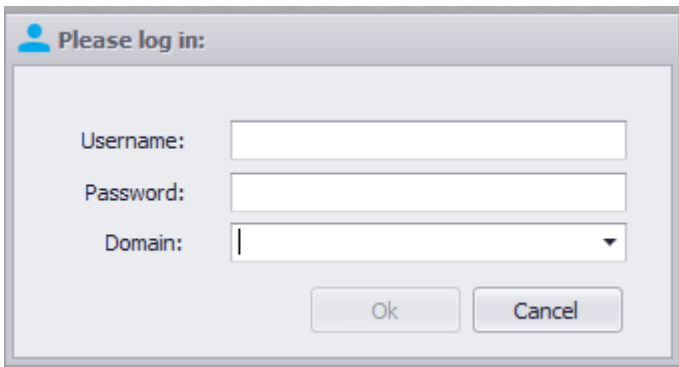


Applications – Connector Login



Domain Name:

A semicolon-delimited list of domains that are pre-populated in the ThinKiosk Login Dialog.



Retain the Last Username

The last username used during a successful logon will be retained and pre-populated for the next logon.

Retain Last Domain Name

The last domain used during a successful logon will be retained and pre-populated for the next logon.



Retain Last User Password

The last password used during a successful logon will be retained and pre-populated for the next logon.

Don't remove credentials from files

When using a Citrix, Microsoft RDS or VMware Horizon connection file, any embedded credentials will not be removed, and the logon prompt will not be displayed.

Only allow domain names specified in the Domain Name field

When enabled, the domain drop-down field in the Connector login dialog is read-only so users can only select a domain that is prepopulated in the ThinKiosk profile.

Offset the connector login dialog placement

Allows the on-screen Connector login dialog placement to be changed by specifying X and Y offset coordinates relative to the centre of the screen.

Positive values will move the dialog down and right

Negative values will move the dialog up and left

Update the device name in the Management console to the last logged on Connector User

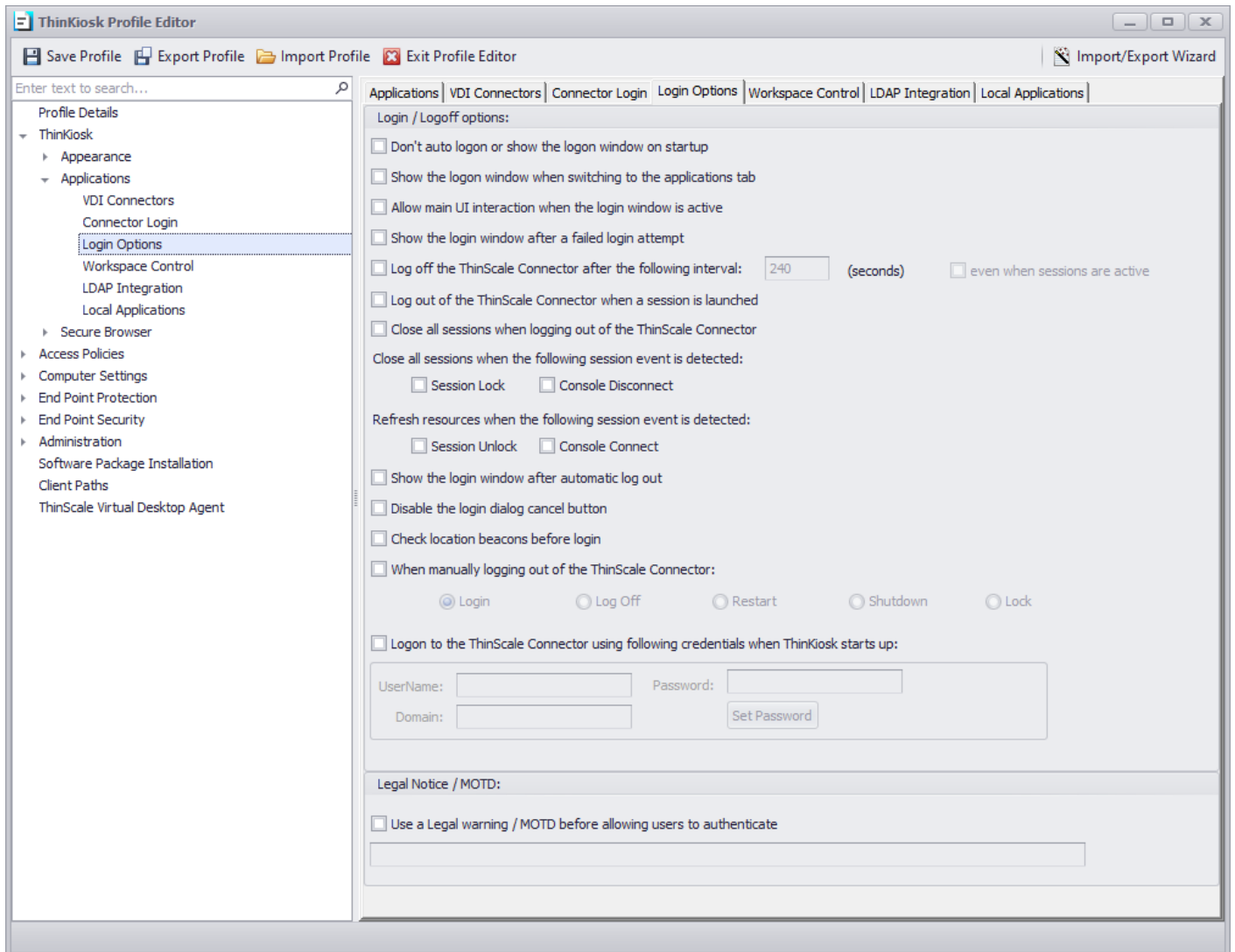
When enabled, the device name inside the Management Console will be renamed as the last connected user using the Thin Scale connector. **

Update the device name in the Management console to the last logged on Horizon Client User

When enabled, the device name inside the Management Console will be renamed as the last connected user after the Horizon client has been launched. **

**ThinKiosk 5.7 required

Applications – Login Options



Don't auto logon or show the login window on start-up

If enabled, ThinKiosk will not automatically show the ThinScale Connector Login dialog when ThinKiosk starts.

Show the logon window when switching to the applications tab

If enabled, ThinKiosk will launch the ThinScale Connector Login dialog when switching to the applications tab from the browser tab, if not already logged on to the connector.

Allow main UI interaction when the login window is active

When enabled, users can interact with the main ThinKiosk UI including the Ribbon Bar even when the Connector login dialog is active.



Show the login window after a failed login attempt

When enabled, the Connector login dialog will re-appear if the login attempt fails.

Log off the ThinScale Connector after the following interval

If enabled, ThinKiosk will automatically log out of the ThinScale Connector after the configured number of seconds.

Even when sessions are active

If enabled, the Connector login will occur even if there are active remote sessions.

Log out the ThinScale Connector when a session is launched

If enabled, ThinKiosk will automatically log out of the ThinScale Connector and the Citrix StoreFront / Web Interface website after launching a resource.

Close all sessions when the following event is detected:

When the Windows machine is Locked or the console is Disconnected ThinKiosk will close all the open sessions.

Refresh resources when the following event is detected:

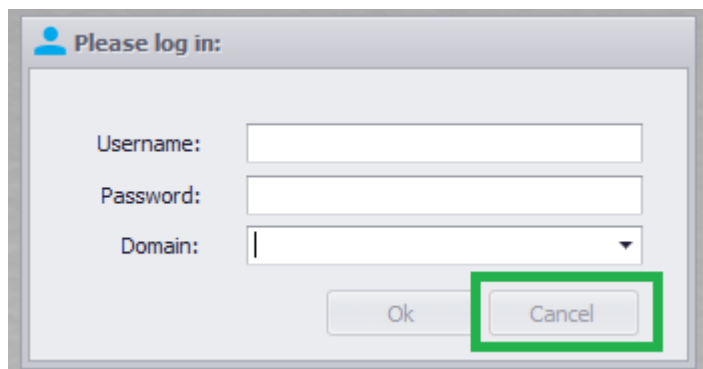
When the Windows machine is Unlocked, or the console is re Connected ThinKiosk will refresh all the open sessions.

Show the login windows after automatic log out

If enabled, the Connector login dialog will appear after the Connector has been automatically logged out.

Disable the login dialog cancel button

If enabled, the Connector login dialog's cancel button will be disabled.



A screenshot of a Windows-style login dialog box titled "Please log in:". It contains three input fields: "Username:", "Password:", and "Domain:". Below the fields are two buttons: "Ok" and "Cancel". The "Cancel" button is highlighted with a green rectangular border.

Check location beacons before login

When enabled, ThinKiosk will determine the location of the device before the Connector login dialog is displayed. Enable this option you if roam and do not restart ThinKiosk.

When manually logging out of the ThinScale Connector:

When users click the Connector's Log Off button the selected action will be performed.

Logon to the ThinScale Connector using the following credentials when ThinKiosk starts up:

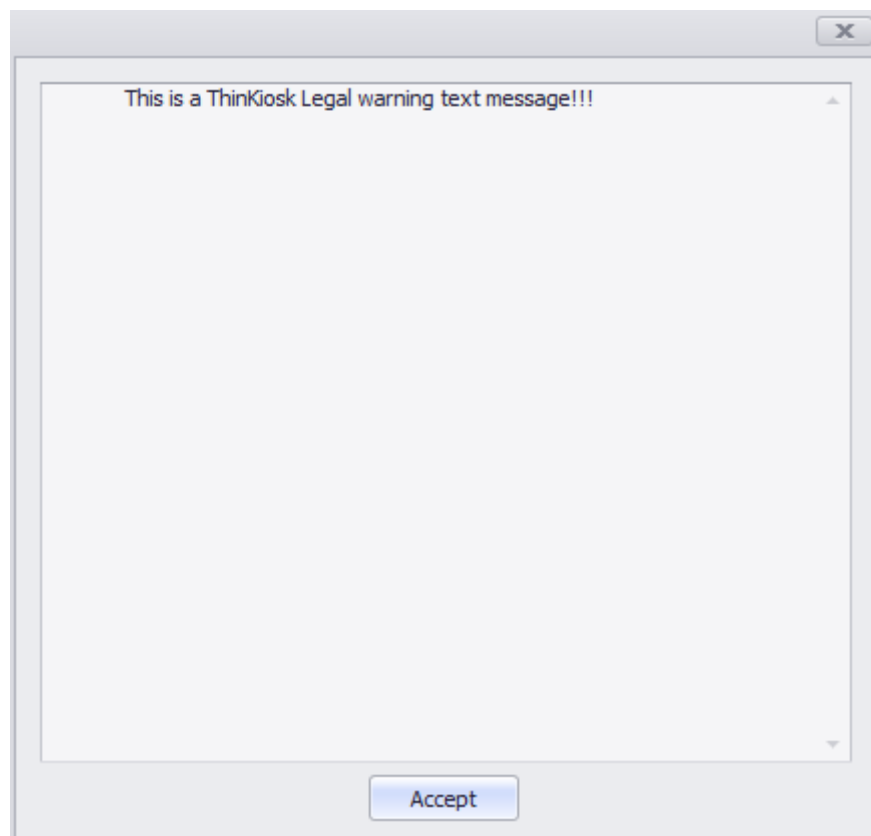
When enabled, ThinKiosk will use the supplied credentials to automatically log on to the Connector at startup.

Note: Not recommended if multiple users, log to the same machine.

Legal Notice / MOTD

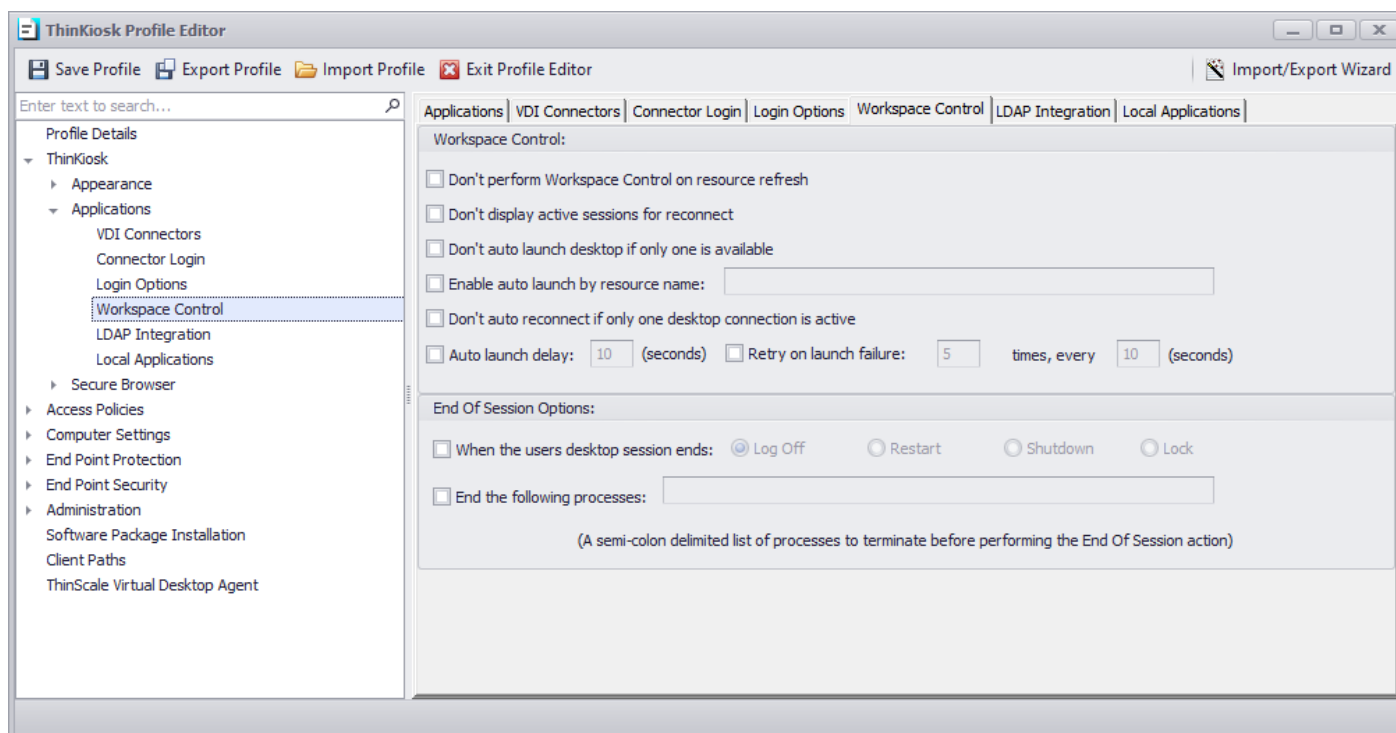
Use a Legal warning / MOTD before allowing users to authenticate

If enabled, the configured warning / MOTD is displayed to the user before they can log on to the ThinScale Connector.





Applications – Workspace Control



Don't perform Workspace Control on resource refresh

If enabled, Workspace control options will not be performed if a user's click the 'Refresh Resource' button. Workspace control will only be performed after the initial login.

Don't display active sessions to reconnect

If enabled any active sessions the user has available to reconnect to will not be presented.

Don't auto-launch desktop if only one is available

If enabled, ThinKiosk will not automatically connect to a desktop if it is the only resource available to the user.

Enable auto launch by resource name

If enabled, ThinKiosk will auto-launch any resource available to the user in the order they appear in the configured list.



Don't auto-reconnect if only one desktop connection is active

If the user only has one active session to reconnect to ThinKiosk will automatically connect to it unless this option is enabled in which case the desktop is displayed in the reconnection dialog.

Auto launch delay

If enabled, auto launching of any resource is delayed by the configured amount of time.

Retry on launch failure

If enabled, when ThinKiosk receives a launch error from the associated broker it will automatically retry the launch for the configured number of times every configured time interval.

End of Session Options:

When the user's desktop session ends

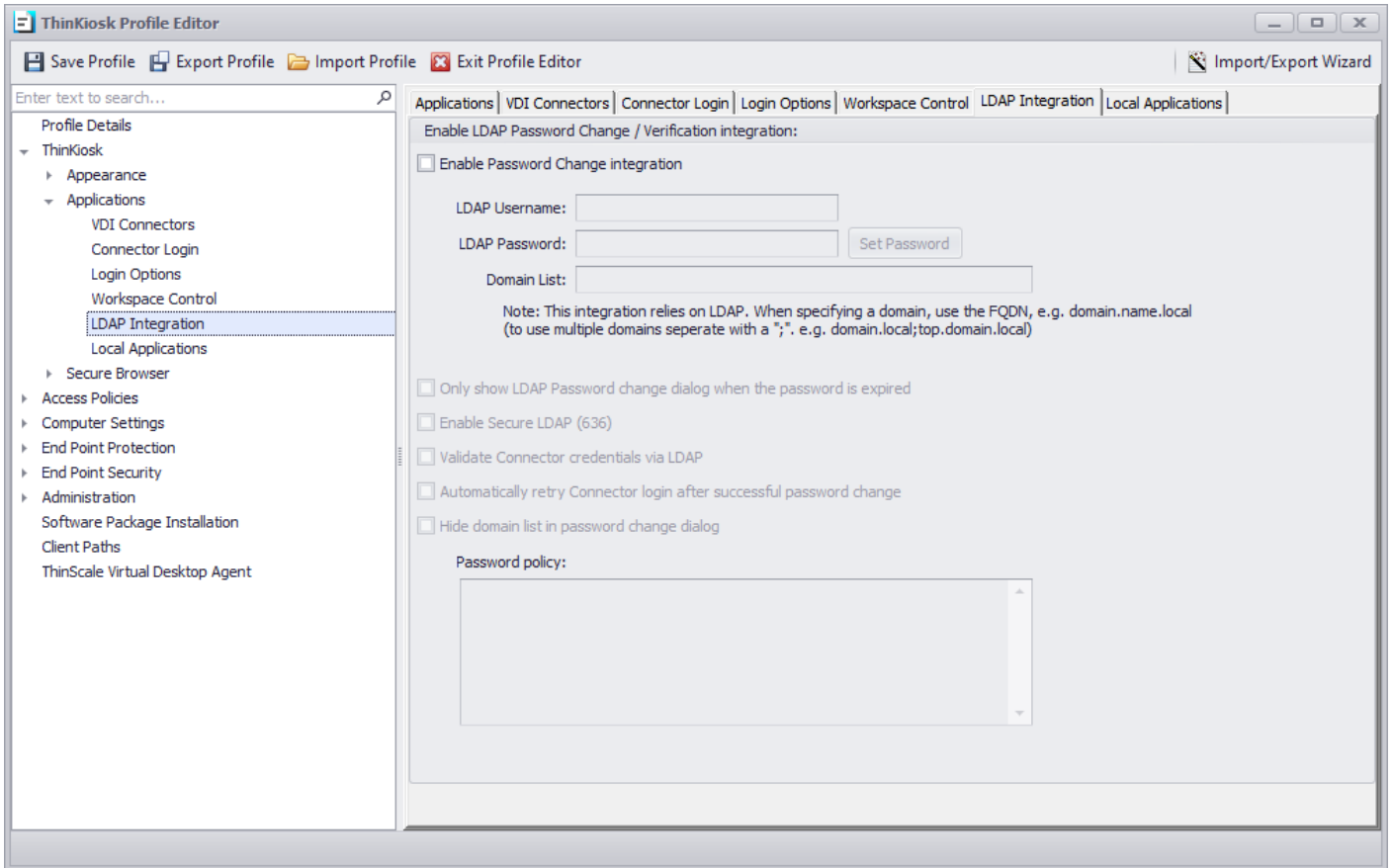
When ThinKiosk has detected that all remote sessions have ended it will perform the configured action on the client device.

End the following processes

A semi-colon delimited list of processes that ThinKiosk will terminate before performing the configured end of session action.



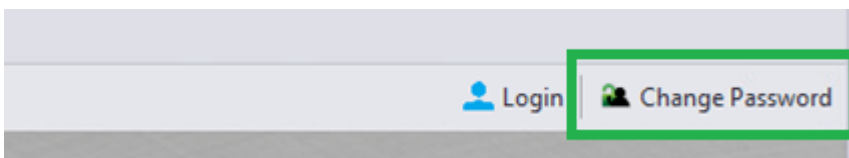
Applications – LDAP Integration



Enable LDAP Password Change/Verification integration

Enable Password Change integration

If enabled, users have the option to change their domain password before logging on to the ThinScale connector.



LDAP username

A domain username that has permission on the domains in the domain list to change user passwords.



LDAP password

The password of the account is specified in the LDAP username option.

Domain List

A semi-colon delimited list of FQDN's that users can change their password for.

Enable Secure LDAP (636)

If enabled, secure LDAP communications will be used.

Validate connector credentials via LDAP

If enabled, the user's credentials entered in the ThinScale Connector login dialog are validated by LDAP before being passed to the configured Connectors.

Automatically retry Connector login after successful password change

If the user is changing their password as the result of an expired password result from the ThinScale Connector. ThinKiosk will automatically retry the Connector login using changed credentials.

Hide domain list in password change dialog

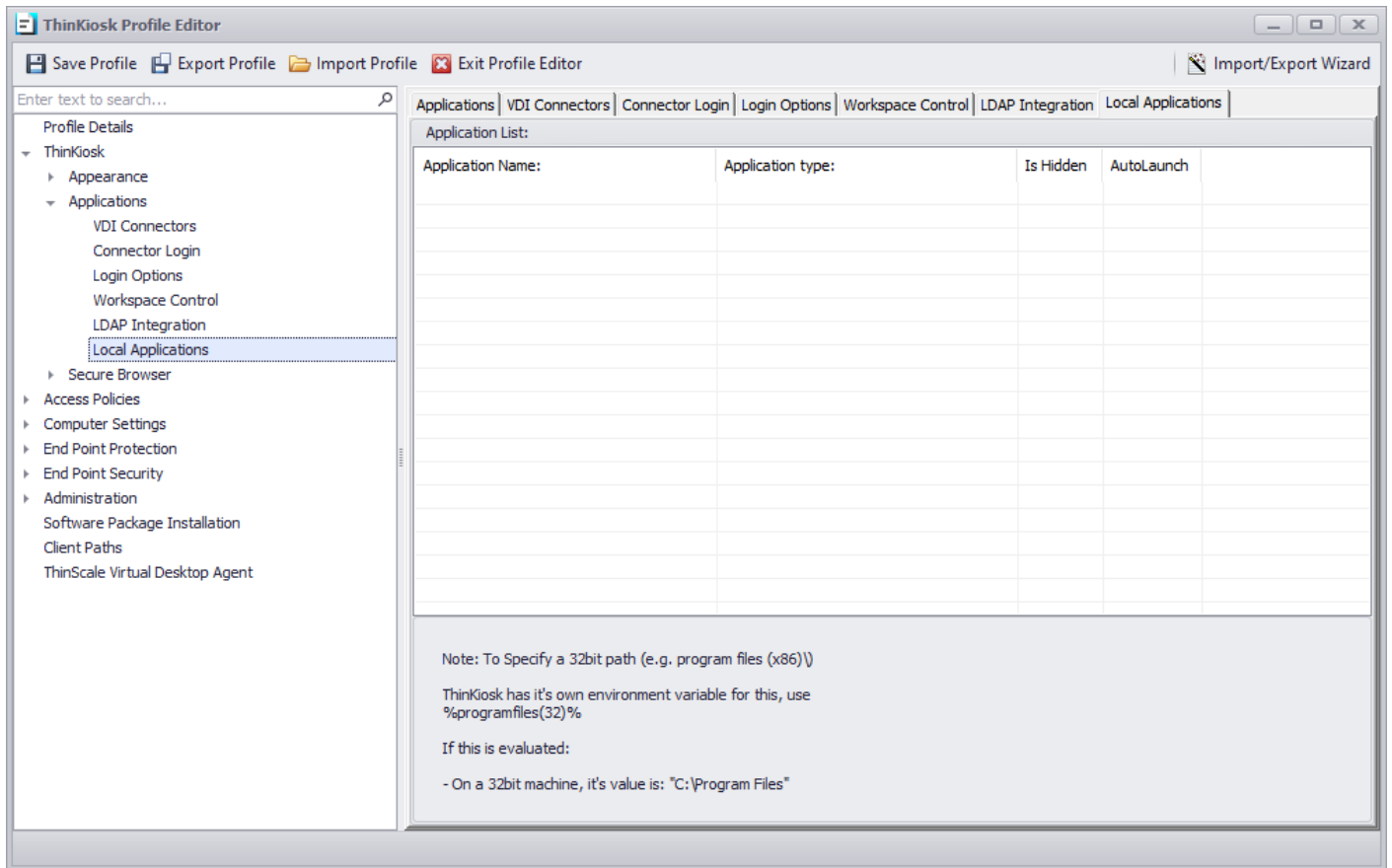
Hides the domain dropdown list in the change password dialog.

Password Policy

A free text entry field allows you to detail your company password policy. This information is displayed in the change password dialog.



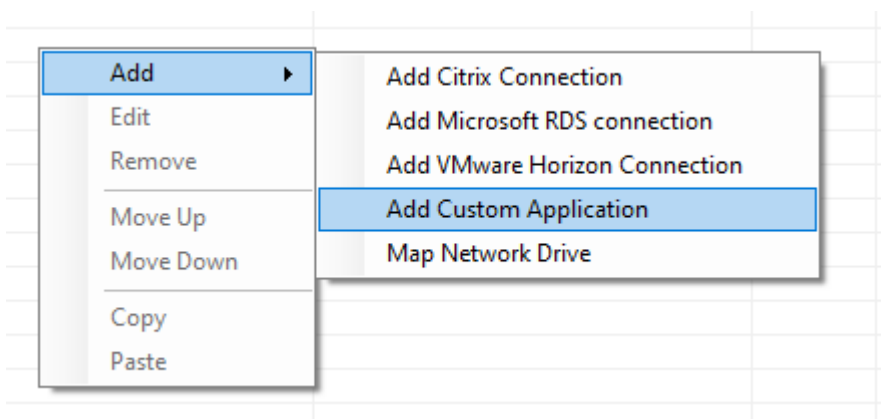
Applications – Local Applications



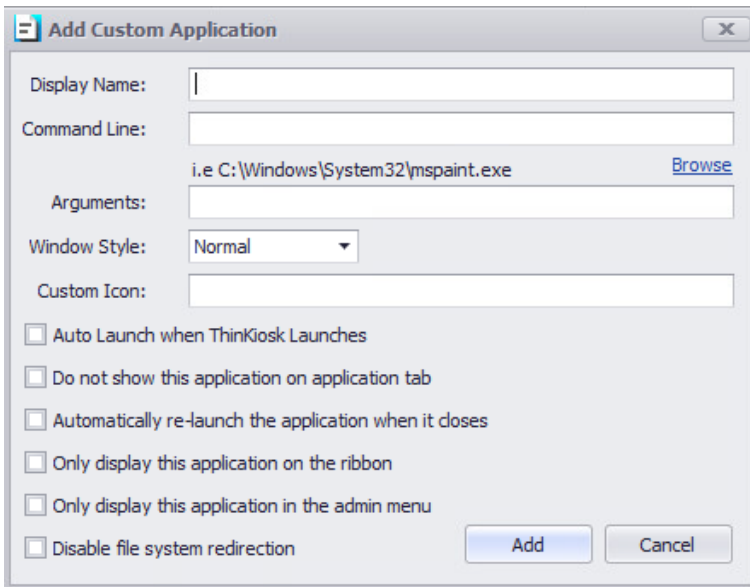
Application List

The list of local applications is available in the 'Applications Tab' of ThinKiosk.

Local applications or Citrix Connection, Microsoft RDS or VMware Horizon connections can be added, edited or removed from the right-click context menu in the Application List in the Profile Editor.



Local Applications



The screenshot shows a dialog box titled "Add Custom Application". It contains the following fields and options:

- Display Name: [Empty text box]
- Command Line: [Empty text box]
- Arguments: i.e C:\Windows\System32\mspaint.exe [Browse button]
- Window Style: Normal [Dropdown menu]
- Custom Icon: [Empty text box]
- Auto Launch when ThinKiosk Launches:
- Do not show this application on application tab:
- Automatically re-launch the application when it closes:
- Only display this application on the ribbon:
- Only display this application in the admin menu:
- Disable file system redirection:
- Buttons: Add, Cancel

Display Name

The name of the applications that will appear on the ThinKiosk application tab.

Command Line

Path to the executable. (i.e. C:\Windows\System32\mspaint.exe)

Arguments

Any command-line arguments that need to be supplied.

Windows Style

Determines how the application is initially launched.

Custom Icon

The path of the icon file you wish to use instead of the default one.

Auto Launch when ThinKiosk Launches

The application will be launched when ThinKiosk initially launches. This option can serve as a replacement for the Windows Explorer 'Run' key.



Do not show this application on the application tab

Hides the application from the user in the ThinKiosk application tab.

This can be useful when you want to configure an application to run when ThinKiosk launches but not be visible to the user.

Automatically relaunch the application when it closes

If enabled, the application will auto relaunch after it has been closed manually.

Only display this application in the ribbon

The application will not be visible in the ThinKiosk applications tab but only on the “Ribbon Bar” inside the Favourites Apps Folder

Only display this application in the admin menu

The application will not be visible in the ThinKiosk applications tab but only on the ‘Admin’ menu when ThinKiosk is unlocked.

Citrix, Microsoft RDS or VMware Horizon connections

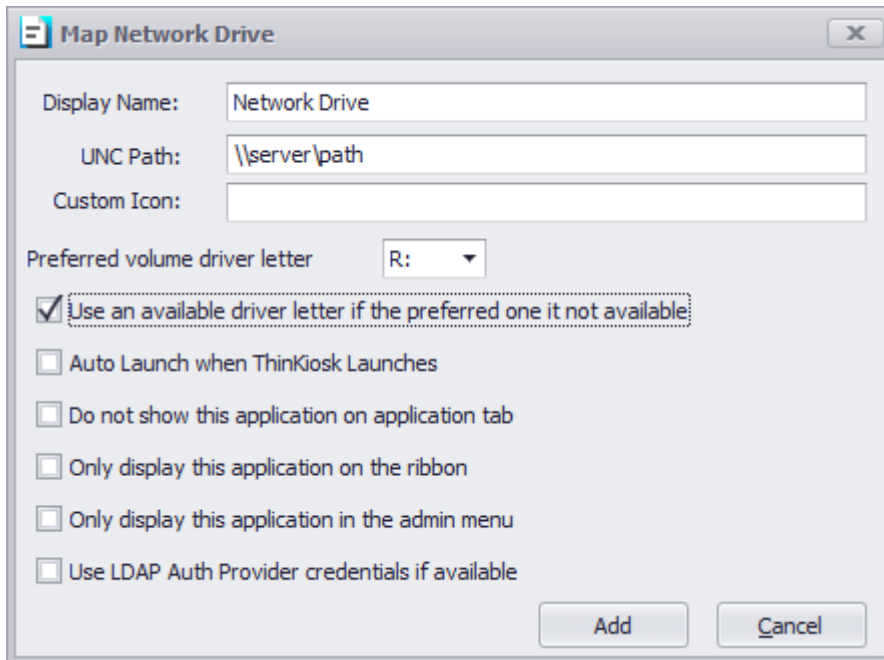
Display Name

The name of the applications that will appear on the ThinKiosk application tab.

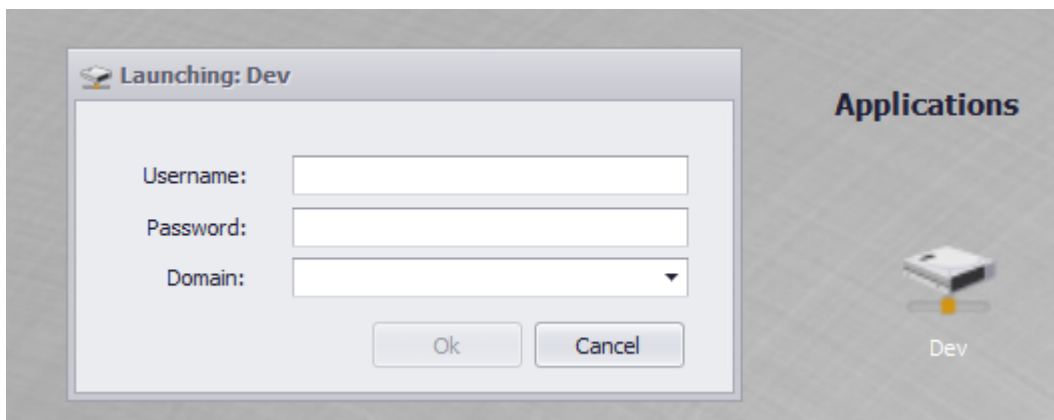
File contents

Please refer to the relevant Appendix section for details of the ICA, RDP and Horizon connection files.

Map Network Drive



Note: make sure the letter is available from Computer Settings Tab



Display Name

The name of the network drive will appear on the ThinKiosk application tab.

UNC Path

The network share path you want to provide to your users.



Auto Launch when ThinKiosk Launches

If enabled the drive will automatically launch at TK UI launch.

Use LDAP Auth Provider credentials if available

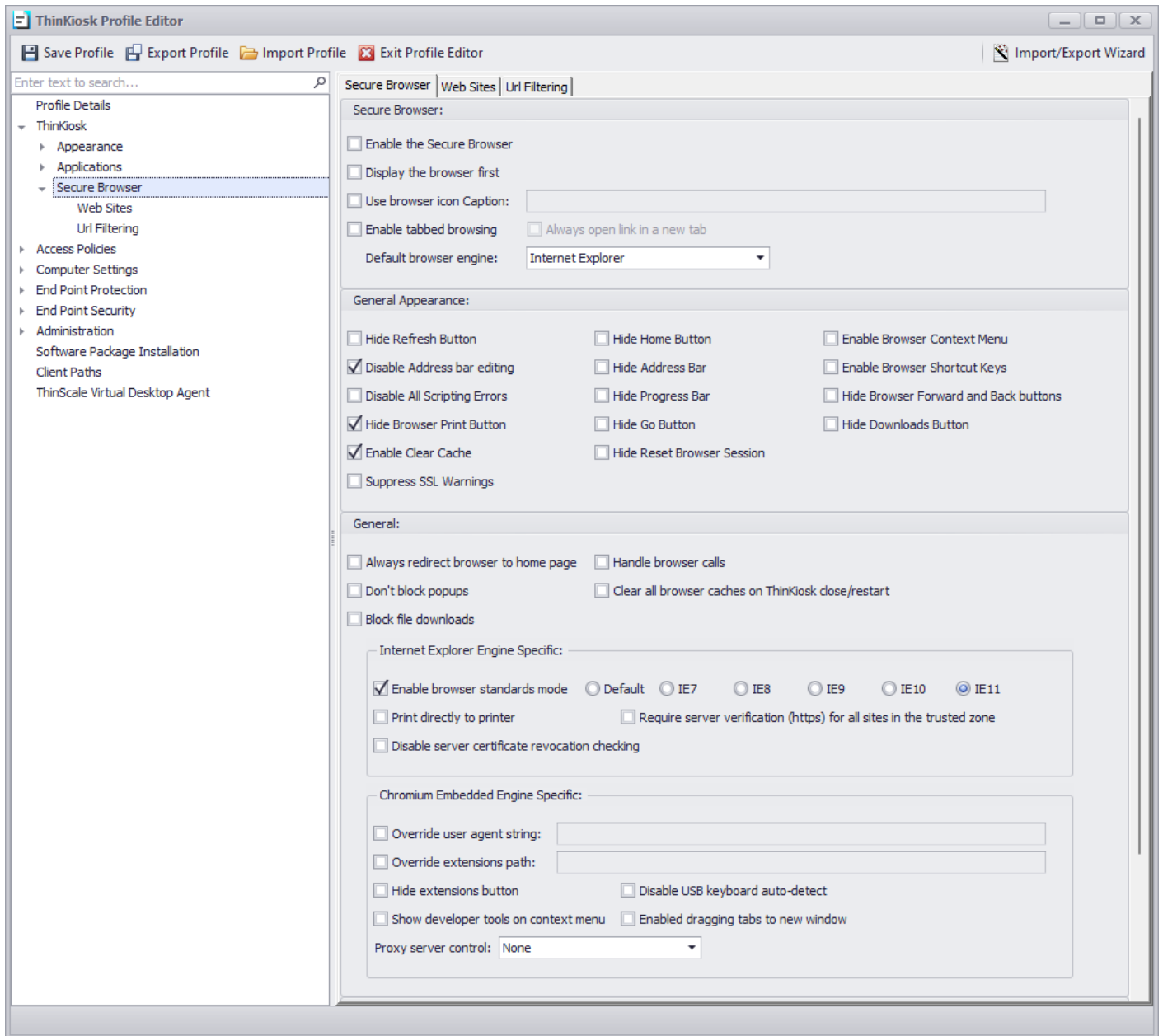
If enabled the drive will authenticate against the LDAP Auth Provider credentials

Reconnect at sign in

If enabled, TK will create a persistence connection to the driver.



6. Secure Browser



Secure Browser:

Enable the Secure Browser

If enabled will show the browser tab inside ThinkKiosk Desktop.

Display the Browser first

If enabled will show the browser tab as the main page within ThinkKiosk.



Use Browser icon caption

Provides a caption to use for the browser tab icon.

Enable tabbed browsing

If enabled, the user will have the option to open multiple browser tabs within ThinKiosk.

Always Open Lin in a new Tab

If enabled, every link will be open on a new tab.

Default Browser Engine:

You can now choose between Internet Explorer or Chrome browser.

General Appearance:

Disable Address bar editing

Prevents users from editing the current address bar URL and therefore cannot browse to websites not configured in the ThinKiosk profile.

Disable All Scripting Errors

Suppresses any scripting errors generated by any visited website.

Enable Clear Cache

If enabled, the button to clear the browser cache within the secure browser tab will be available.

Hide Download buttons

Hides the browsers download button.

Suppress SSL Warnings

Suppresses any website SSL warning that may appear due to website certificate problems.



General

Always redirect the browser to home page

If enabled, the browser's home button will navigate to the URL of the first site configured in the sites list.

If not enabled, the browser will navigate to the URL of the currently selected site in the list.

Don't block popups

If enabled, the browser will allow popup windows to be created by visited websites.

Block File downloads

If enabled, downloads will be blocked.

Handle Browser calls

Configures ThinKiosk as the default HTTP handler, allowing it to handle any website links that are clicked by external applications.

Clear all browser caches on ThinKiosk close/restart

If enabled, caches will be automatically cleared before the UI is closed or restarted.

Internet Explorer Engine Specific

Enable browser standards mode

Forces the ThinKiosk browser to use a particular IE version for rendering standards. The version of Internet Explorer installed on the ThinKiosk device cannot be lower than the standards version required.

Setting a standards version will also alter the browser user-agent to reflect the version of IE selected.

Print directly to printer

If enabled, print jobs are sent directly to the default printer. If not enabled, the user is presented with the standard Windows printer selection dialog.



Require server verification (HTTPS) for all sites in the trusted zone

Enable this option to force all sites configured in the trusted zone to be secure and use HTTPS.

Disable server certificate revocation checking (IE Only)

Disables server certificate revocation checking when enabled.

Chromium Embedded Engine Specific

Override user agent string

If enabled, a custom user agent string can be sent in the `User-Agent` HTTP header every time it requests any site.

Override extensions path

If enabled, a custom path can be set up for specific extensions.

Hide extensions button

If enabled, the extension button in the browser tab will be hidden

Show developer tool on the context menu

If enabled, a right-click mouse click will enable the debugger tool inside the selected website

Disable USB keyboard auto-detect

If enabled, chromium auto keyboard detection will be disabled. Useful for hybrid laptops

Enable dragging tabs to a new window

if enabled, browser windows can be dragged out from the ThinKiosk desktop.



VDI Controls:

Log off VDI resources after the following interval

If enabled, ThinKiosk will automatically log out of the ThinScale Connector after the configured number of seconds.

Even when sessions are active

If enabled, the Connector login will occur even if there are active remote sessions.

Log out of Citrix Web Interface / StoreFront when a session is launched

If enabled, ThinKiosk will automatically log out of the ThinScale Connector and the Citrix StoreFront / Web Interface website after launching a resource.

Clear web session after Citrix Web Interface/ Storefront logoff

If enabled, ThinKiosk will automatically clear the browser session after a Storefront is manually or automatically logged off.

Don't redirect from the Logged off-page back to the login page

By default, the ThinKiosk browser will automatically redirect users from the Web Interface / StoreFront 'logged off' page to the login page. Enabling this option will prevent this automatic redirection.

VDI in a Box mode (IE Rendering)

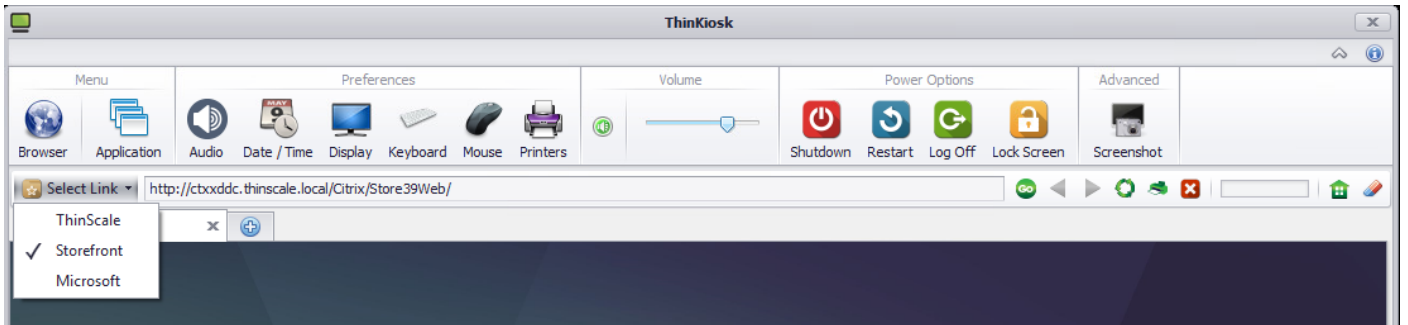
Fixes certain IE rendering problems when using Citrix VDI in a Box.

Manual Logoff redirect

When logging out of Citrix Web Interface / Storefront the browser will click the website's logout link. If this option is enabled, the browser will redirect to the current site's configured home page URL.

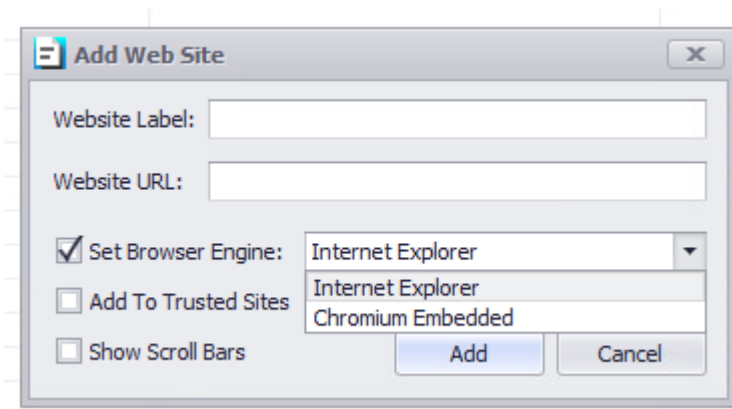
Secure Browser - Web Sites

A list of websites is available in the Select Link option.



Sites can be added, edited or removed from the right-click context menu in the Browser Sites list in the Profile Editor.

Adding / Editing a Site



Website Label

The text that appears in the 'Select Link' drop down on the ThinkKiosk UI.

Website URL

URL the browser will navigate to when selected



Set Browser Engine

URL will be opened using the desired browser engine.

Add to Trusted Windows

Adds the URL to the Internet Explorer Trusted sites list.

Show Scroll bars

Adds scrolls bars to the browser interface allowing you to scroll around the site if required.

Adding / Editing a Site

Update Web Site

Website Label:

Website URL:

Set Browser Engine: Chromium Embedded

Add To Trusted Sites

Show Scroll Bars

Auto-reload the page every seconds

Create Shortcut

Website Shortcut Specific

Custom Icon:

Open in default browser app

Open in Secure Browser

Open as popup

Auto Launch when SRW Launches

Do not show this website on application tab

Only display this website on the ribbon

Only display this website in the admin menu



Website Label

The text that appears in the 'Select Link' drop down on the TK UI.

Website URL

URL the browser will navigate to when selected.

Set Browser Engine

URL will be opened using the desired browser engine.

Add to Trusted Windows

Adds the URL to the Internet Explorer Trusted sites list.

Show Scroll bars

Adds scrolls bars to the browser interface allowing you to scroll around the site if required.

Auto reload page

If enabled, the page will reload every x

Create Shortcut

If enabled, a shortcut will be created inside the application list.

Open in default browser app

If enabled, the link will open using the default browser

Open in Secure Browser app

If enabled, the link will open using the TK browser

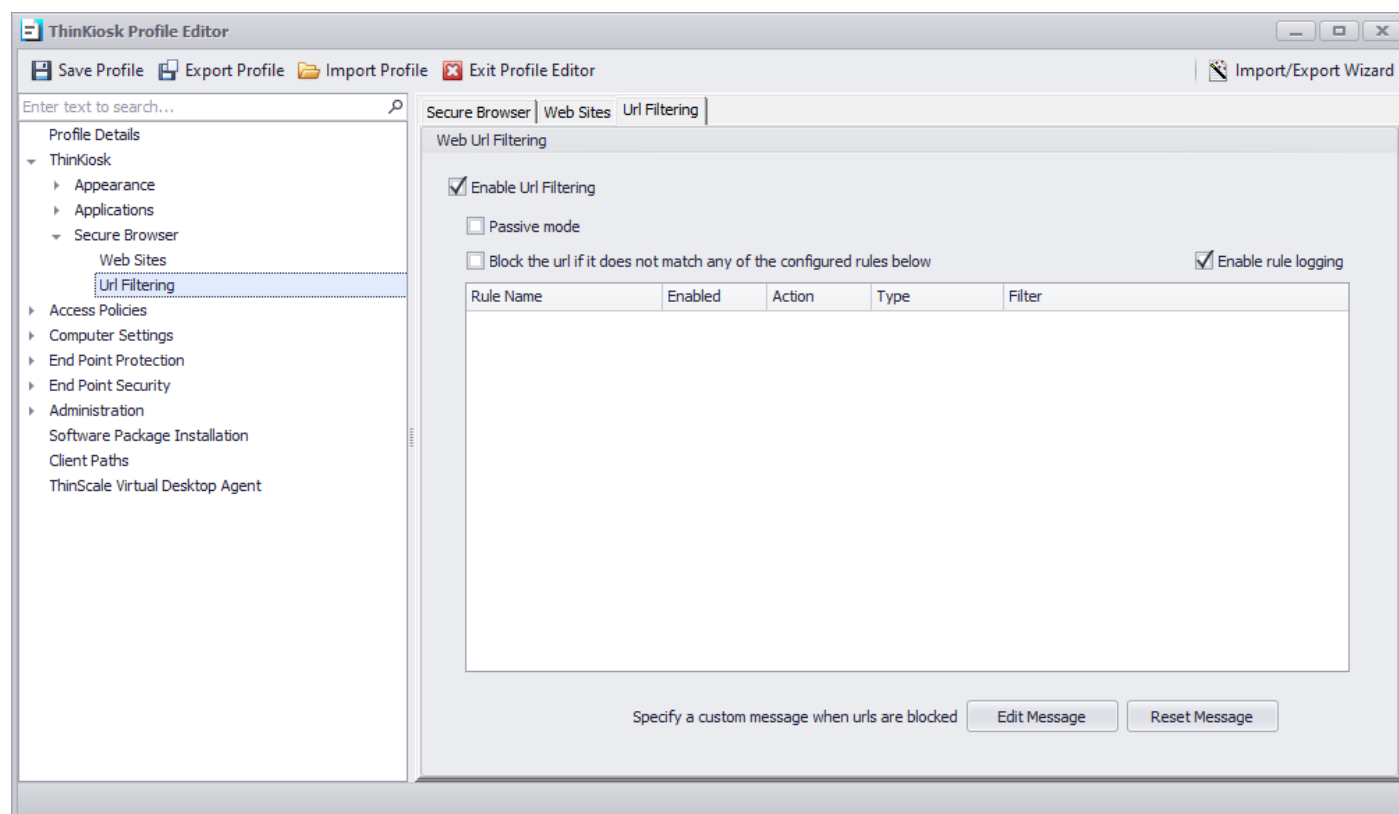
Open as popup

If enabled, the link will open using a popup browser

Auto Launch when ThinKiosk Launches

If enabled, the link will open when TK launches

Secure Browser - URL Filtering



Enable URL Filtering

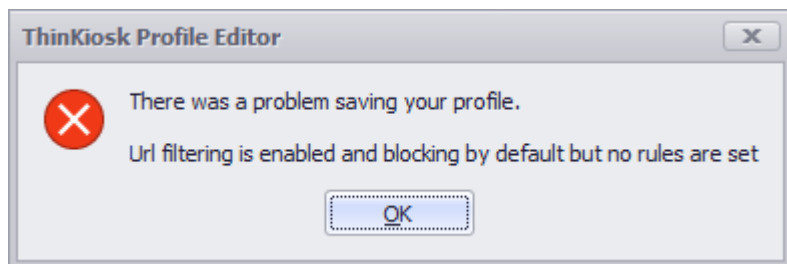
If enabled, the Administrator can create a list of Browser URLs they want to block or allow navigations.

Passive mode

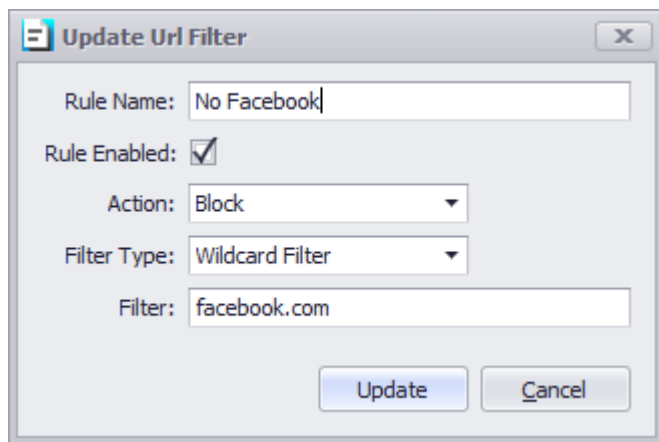
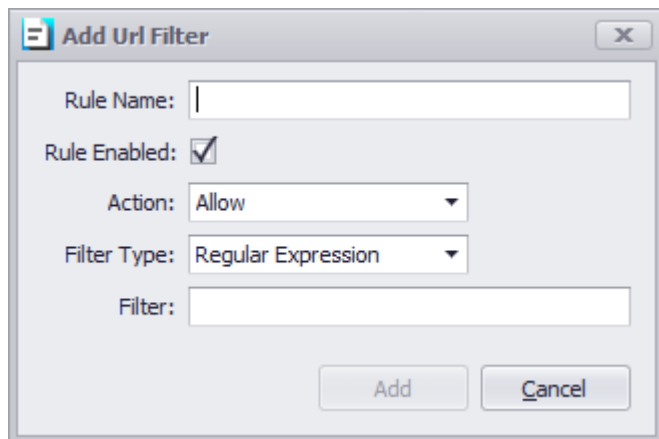
If enabled, any URLs added to the list will always be allowed navigation.

Block the executable if it does not match any of the configured rules below

If enabled, and no other rules are created in the list, the profile will show an error message.



To add a new rule simply right click the white space and click Add:



This rule will block facebook.com



Update Url Filter
✕

Rule Name:

Rule Enabled:

Action:

Filter Type:

Filter:

This rule will block any Wikipedia sites no matter what top domain level you use.

Update Url Filter
✕

Rule Name:

Rule Enabled:

Action:

Filter Type:

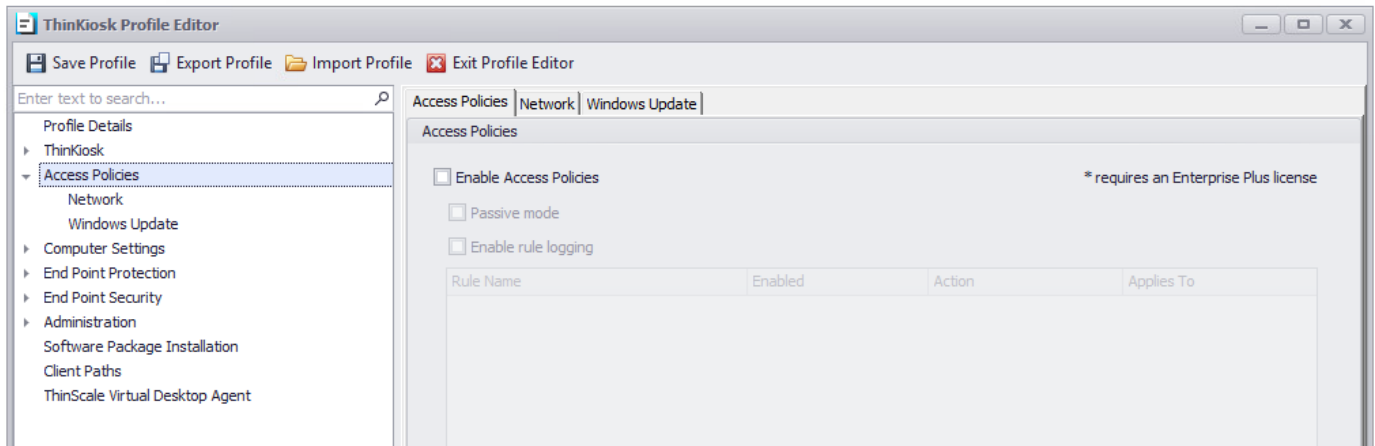
Filter:

This rule will stop any searches containing google maps.

Rule Name	Enabled	Action	Type	Filter
No Facebook	Yes	Block	Wildcard Filter	facebook.com
No Funtime	Yes	Block	Wildcard Filter	reddit.*
No Google Maps	Yes	Block	Wildcard Filter	?*google*maps*

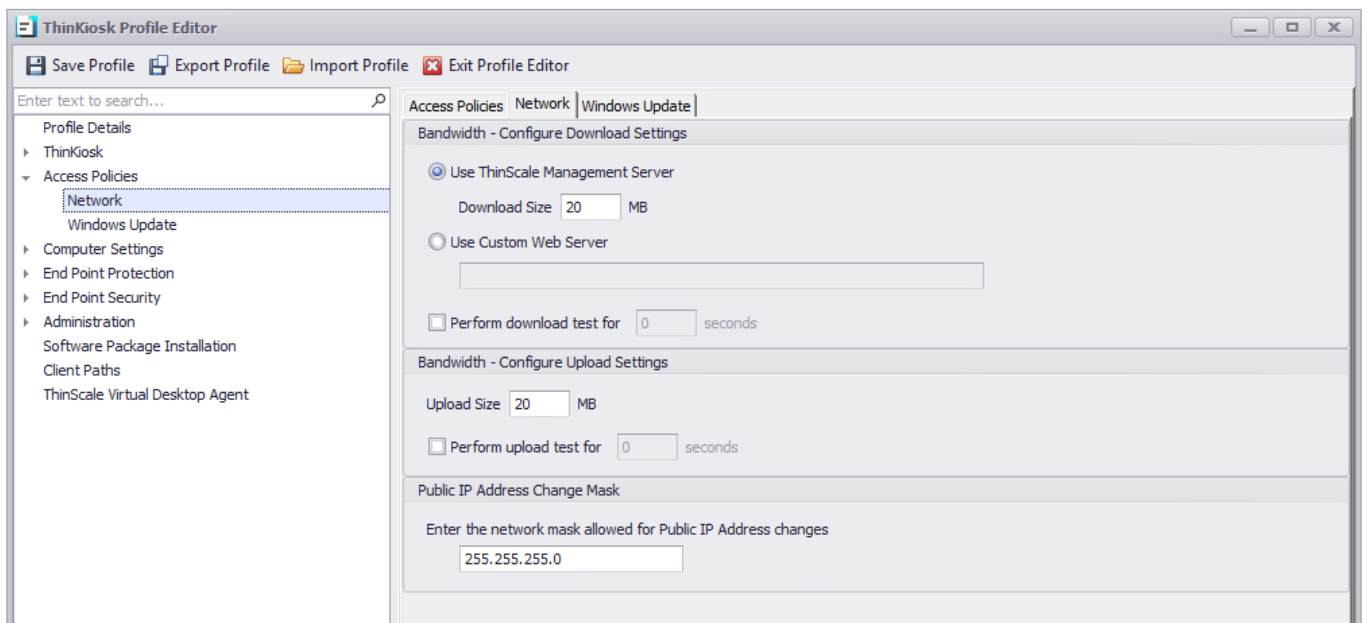


7. Access Policies



Please refer to the Knowledge Base article for more info.

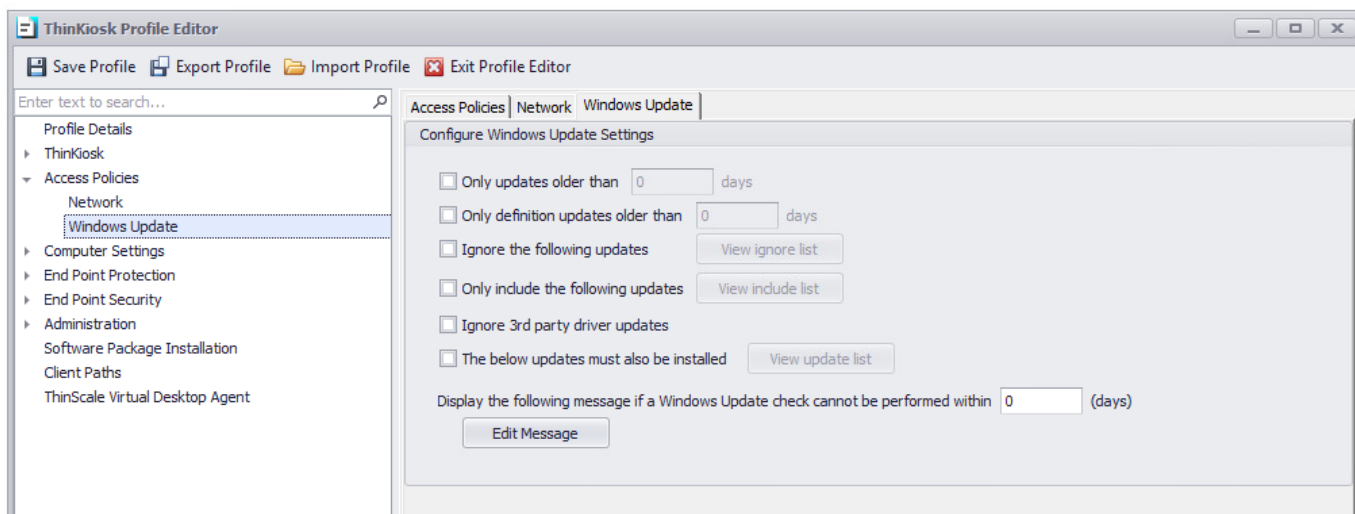
Network



Use this section to test your download and upload speed.



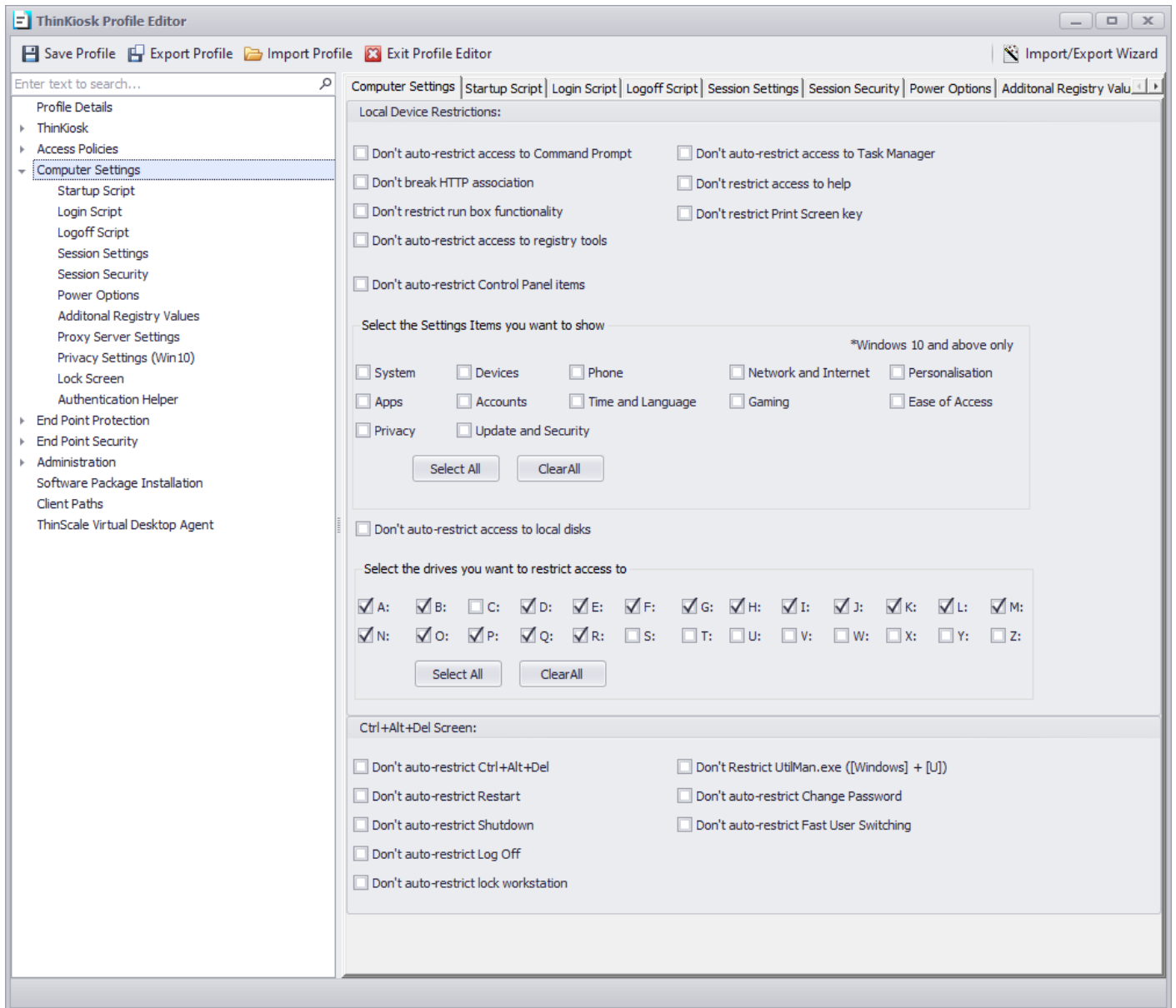
Windows Update



See [End Point Protection - Windows Patch Management](#) for more Info



8. Computer Settings



Local Device Restrictions

Don't auto-restrict access to Command Prompt

If enabled, users will have access to the Command Prompt.

Don't break HTTP association

When enabled, the use of Internet Explorer outside ThinKiosk is allowed.



Don't auto-restrict access to the task manager

If enabled, users will have access to the Windows Task Manager.

Don't Restrict Run box functionality

If enabled, users will have access to the Run option from the Windows Start Menu.

Don't Restrict access to Help

If enabled, users will have access to the help options in Explorer and the lock screen.

Don't Restrict access to the registry tool

If enabled, users will have access to the registry tools.

Don't Restrict Print Screen Key

If enabled, users will be able to use the Print Screen combination key.

Don't auto-restrict Control Panel Items

If enabled, users will have access to all Control Panel applets.

Select the Settings Items you want to show

If CAD is not blocked, the new 7.5 TK has the option to show the user a "restricted" view of the Settings Tab. Simply click the option you want to allow, and we will do the rest

Don't auto-restrict access to local drives

If enabled, access to local drives through Explorer views is allowed.

Select the drives you want to restrict access to

By selecting the letter, you will disallow access to that specific driver.

Ctrl+Alt+Del Screen:

**Don't auto-restrict Ctrl+Alt+Del**

If enabled, access to the local ThinKiosk devices lock screen will be available using the Ctrl+Alt+Del key sequence.

Don't auto-restrict Restart

If enabled the 'Restart' option will be available on the lock screen.

Don't Restrict UtilMan.exe ([Windows] + [U])

If enabled [Windows] + [U] functionality will be available on the lock screen.

Don't auto-restrict Shutdown

If enabled the 'Shutdown' option will be available on the lock screen.

Don't auto-restrict Change Password

If enabled the 'Change Password' option will be available on the lock screen.

Don't auto-restrict Log Off

If enabled the 'Log Off' option will be available on the lock screen.

Don't auto-restrict Fast User Switching

If enabled the Fast User Switching will be available from the lock screen.

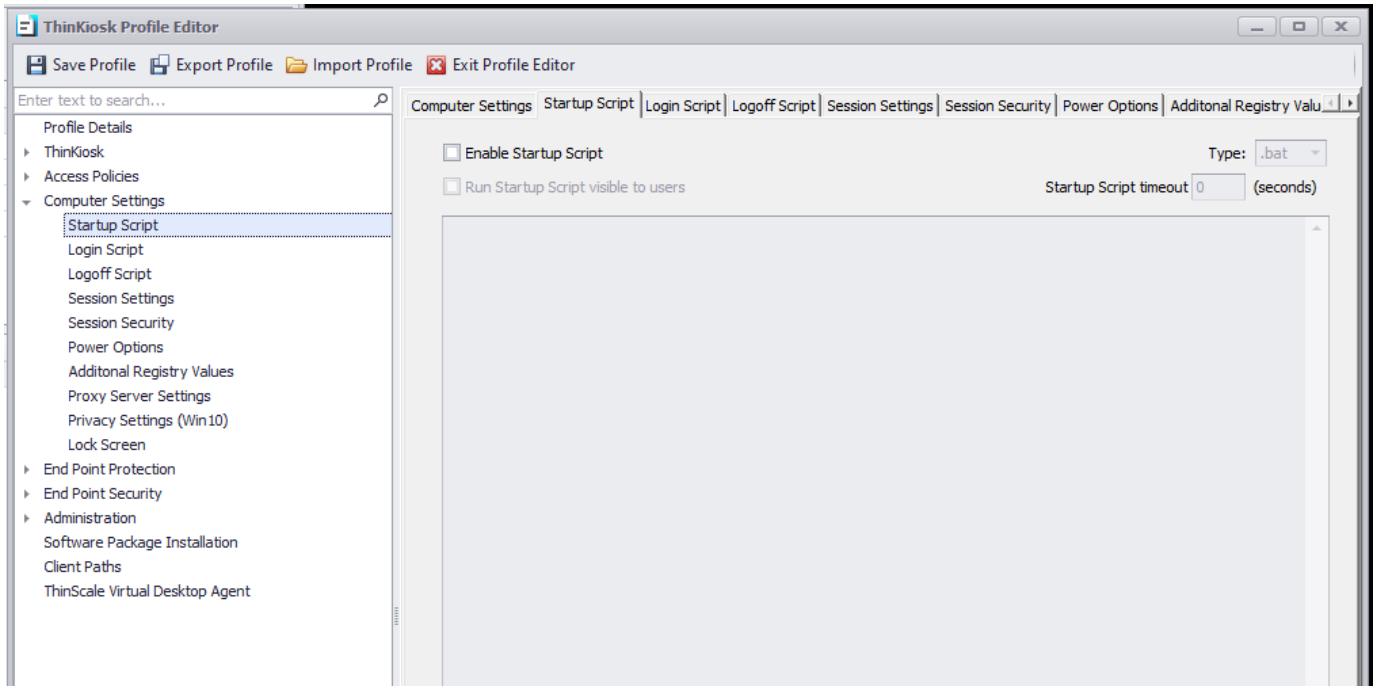
Don't auto-restrict lock workstation

If enabled the users will be able to lock the local ThinKiosk workstation.

Note: those commands are restricted for the local machine only, for VDI pass through please refer to the Magic Filter Section in Session Settings.



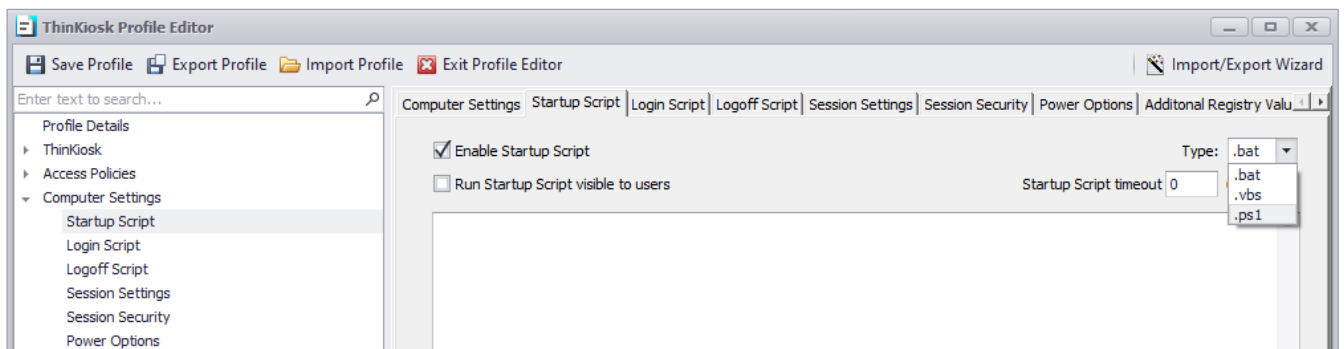
Computer Settings – Startup Script



Startup Script

Enable Startup Script

Enables the supplied.VBS or .BAT or PS1 startup script. The script is configured as a local group policy start-up script and will apply during the Windows boot process.



Run Startup Script Visible to users

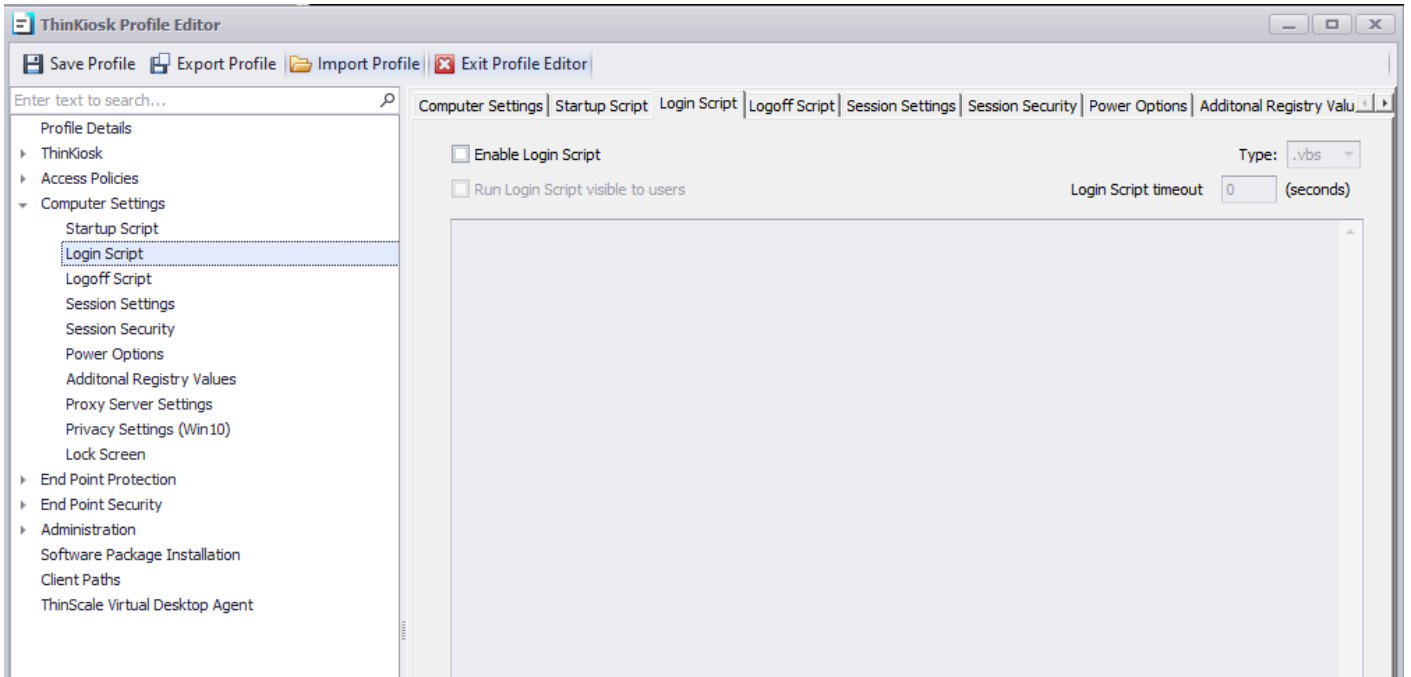
If enabled, any output from the script will be visible on the console of the device.

Startup Script Timeout

Determines how long the scripts will run before stopping their execution.



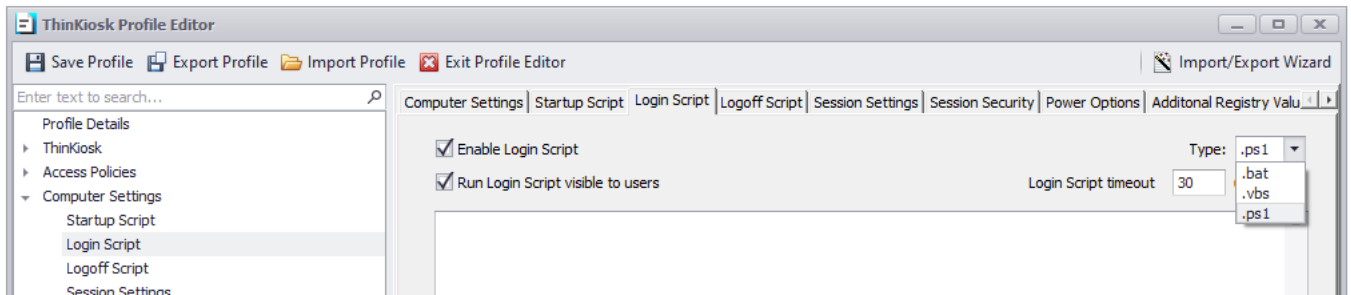
Computer Settings – Login Script



Login Script

Enable Login Script

Enables the supplied.VBS or .BAT or PS1 login up script. The script will be applied when ThinKiosk UI is first started



Run Login Script Visible to users

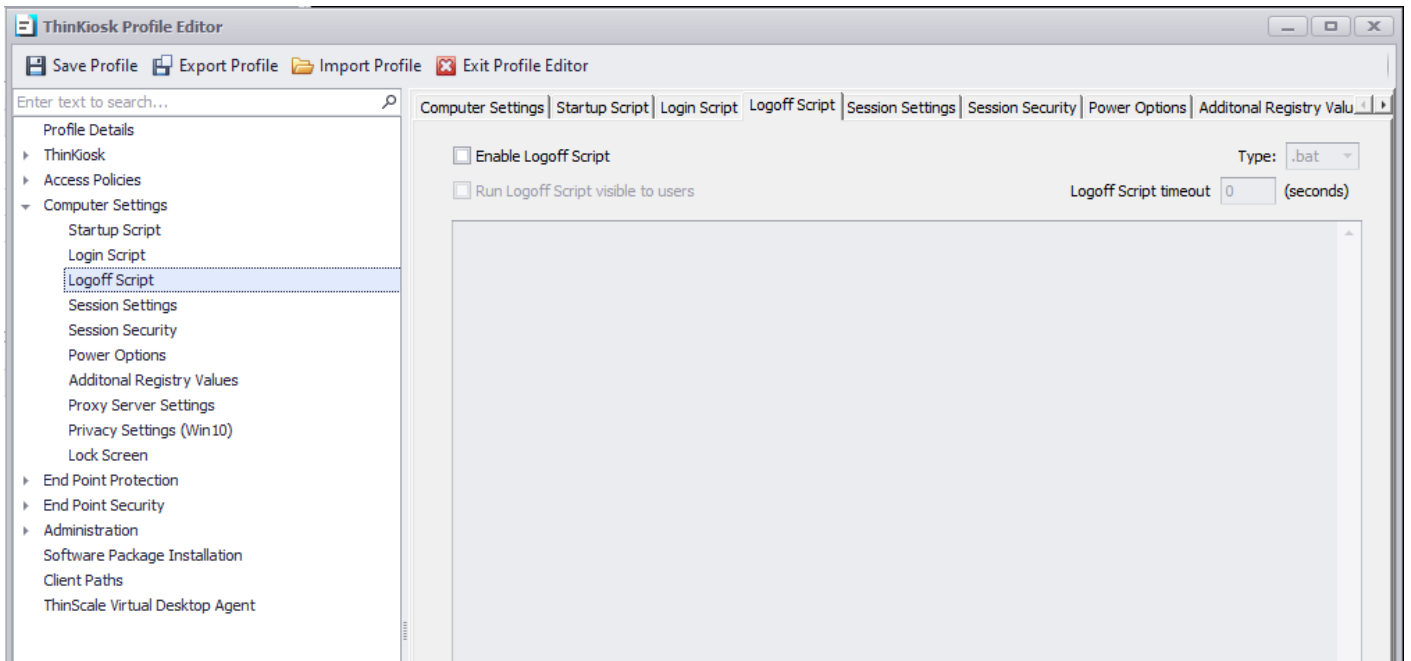
If enabled, any output from the script will be visible on the console of the device.

Login Script Timeout

Determines how long the scripts will run before stopping their execution.



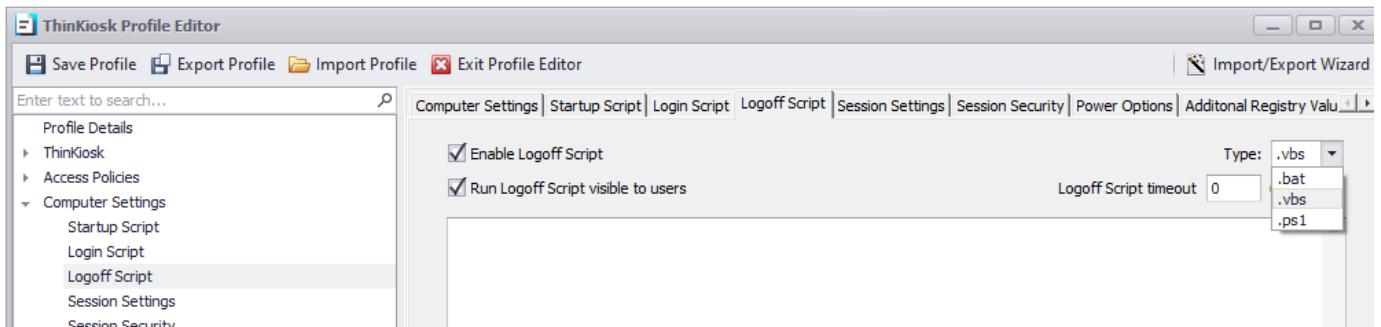
Computer Settings – Logoff Script



Logoff Script

Enable Logoff Script

Enables the supplied.VBS or .BAT logoff script. The script will be applied when ThinKiosk UI is closed



Run Logoff Script Visible to users

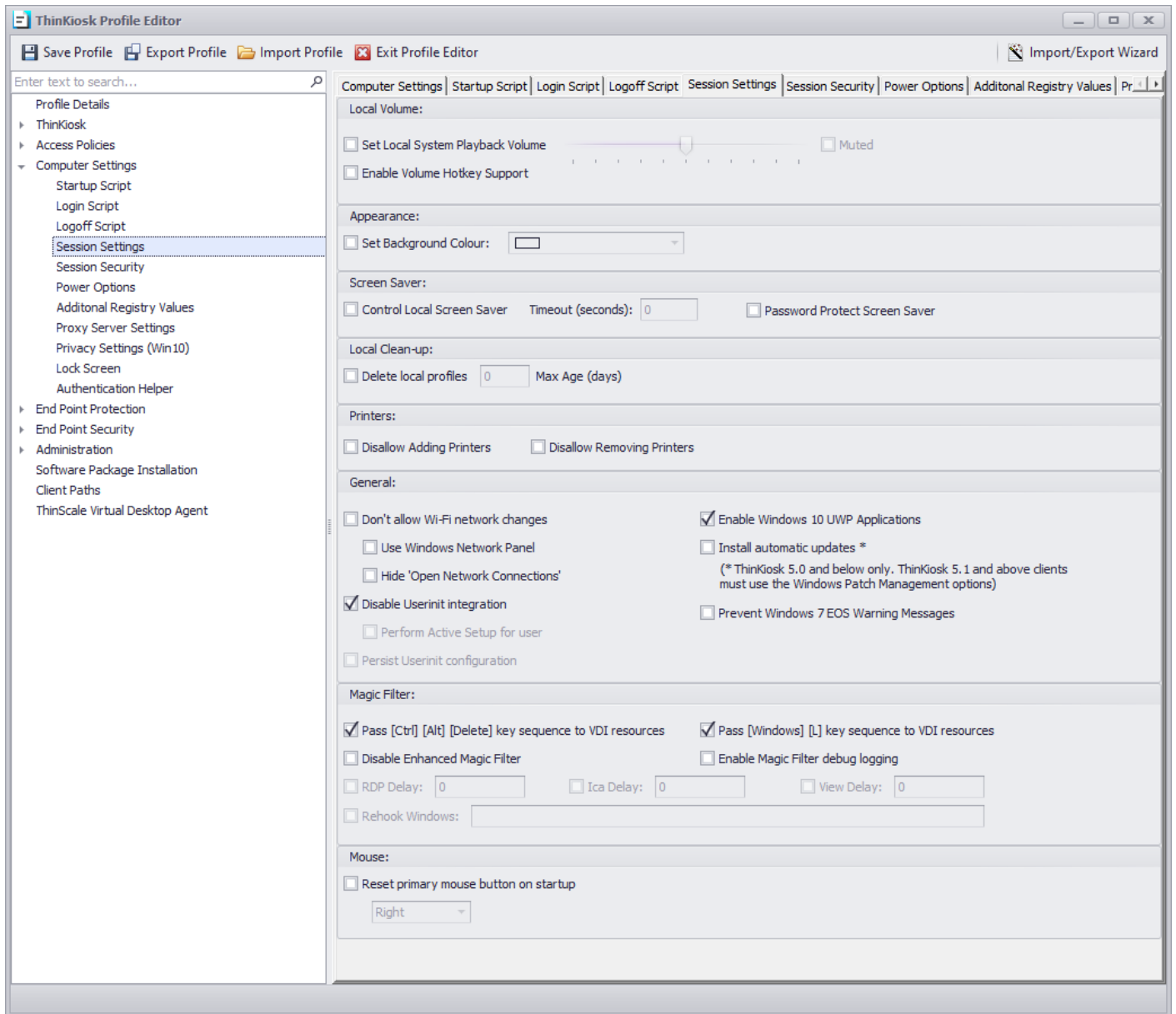
If enabled, any output from the script will be visible on the console of the device.

Logoff Script Timeout

Determines how long the scripts will run before stopping their execution.



Computer Settings - Session Settings



Local Volume

Set Local Volume

If enabled, will set the local device volume to the value configured on the start-up of ThinKiosk.

Enable Volume Hotkey Support

When enabled, ThinKiosk will control the Volume hotkeys. Enable this option when vendor volume applications are not available or applicable in your configuration.



Appearance:

Set Background Colour

If enabled, the desktop background colour will be set to the configured colour.

Screen Saver:

Control Local Screen Saver

If enabled, the local screen saver will kick in after the selected duration.

Password Protect Screen Saver

If enabled the local screen saver will be password protected.

Local Clean-up

Delete local profile

When enabled, local profiles that have not been used in the configured number of days will be deleted.

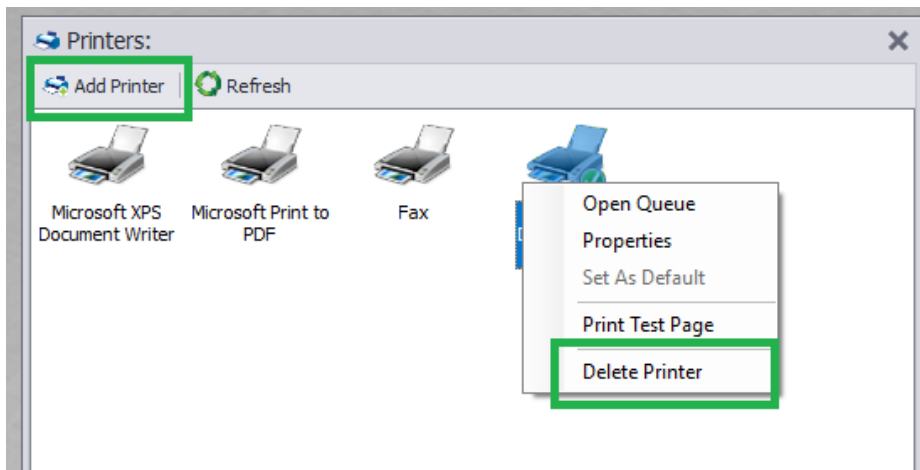
Printers

Disallow Adding Printers

If enabled, users can not add new printers when using the ThinKiosk Printers interface.

Disallow Removing Printers

If enabled, users can not remove existing printers when using the ThinKiosk Printers interface.



General

Don't allow Wi-Fi network changes

If enabled, users can only use ThinKiosk's Wi-Fi interface to view networks and signal strength. Users will not be able to connect to different networks.

Use Windows Network Panel

If enabled, the user will be able to launch the Windows Network panel directly without using the ThinKiosk's network dialog.

Hide "Open Network Connection"

If enabled, the option to open the network flyout will be disabled

Disable Userinit integration

ThinKiosk has its Userinit component that executes before the Windows userinit component during logon. ThinKiosk's userinit is required when using the 'Perform Active Setup for the user' option below.

Perform Active Setup for the user

If enabled, ThinKiosk will perform any required Active Setup configuration that would usually be performed by Windows Explorer.

ThinKiosk performs Active Setup asynchronously and is quicker than the Windows implementation. If this option is disabled, the Windows implementation is performed instead.



Enable Windows 10 UWP Applications (experimental)

If enabled, ThinkKiosk will allow the launching of Windows 10 UWP applications.

Install automatic updates

When enabled, ThinkKiosk, an on-device start-up will initiate a check and installation of automatic updates from Windows Update.

Note: In version 5.1 and above please refer to the Windows Update section.

Prevent Windows 7 EOS Warning Messages

When enabled, Windows 7 EOS Warning message will be disabled.

Magic Filter:

Pass [Ctrl] [Alt] [Delete] key sequence to VDI resources

If enabled, the keystroke will pass through the VDI environment.

Pass [Windows] [L] key sequence to VDI resources

If enabled, the keystroke will pass lock the VDI screen and not the local machine.

Disable Enhanced Magic Filter

If enabled, the Magic Filter key pass-through is disabled.



Magic Filter Delay Option:

RDP Delay

When using 'standard' Magic Filter, sending of pass-through keys to RDP windows is delayed by the configured amount of time.

ICA Delay

When using 'standard' Magic Filter, sending of pass-through keys to Citrix Receiver windows is delayed by the configured amount of time

View Delay

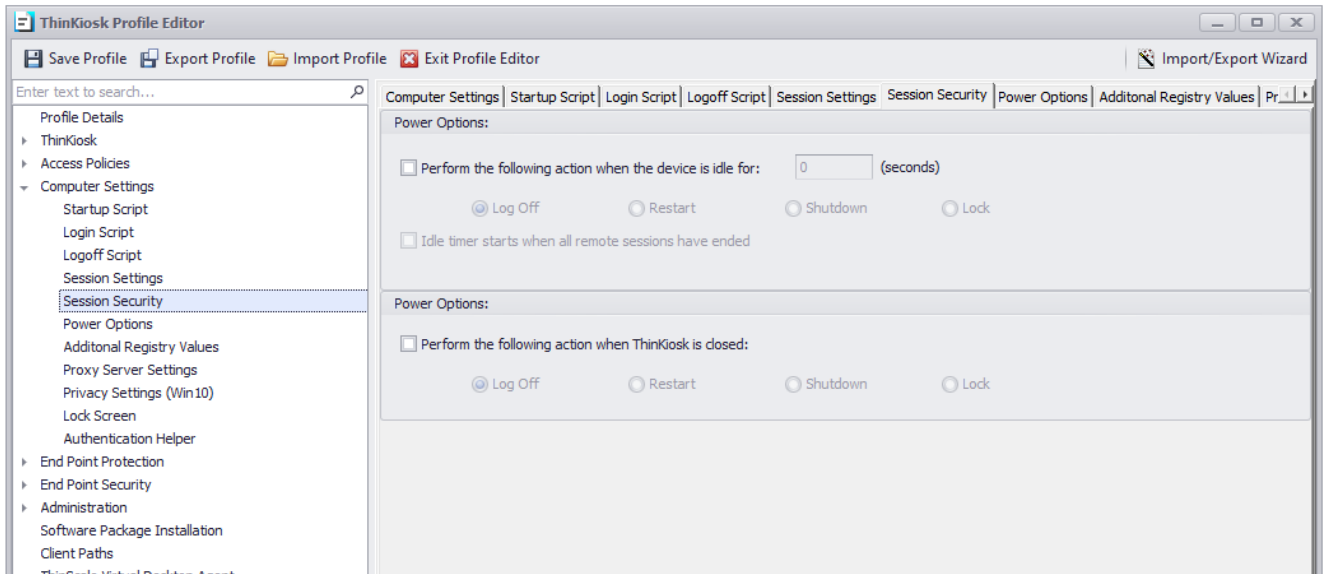
When using 'standard' Magic Filter, sending of pass-through keys to VMware Horizon windows is delayed by the configured amount of time.

Rehook Windows

Forces Magic Filter to monitor keystrokes sent to the additional windows with the configured class name.



Computer Settings - Session Security



Power Options:

Perform the following action when the device is idle for:

If enabled, ThinkKiosk will perform the selected action when the local device has been idle for the configured number of seconds.

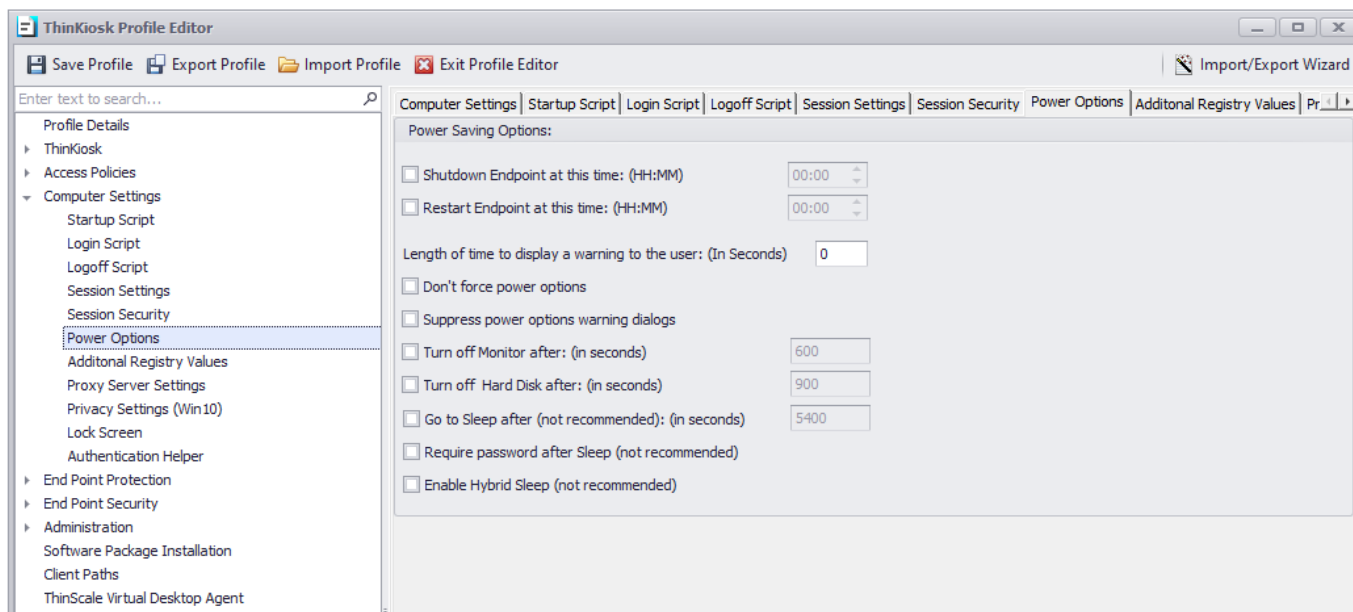
The idle timer starts when all remote sessions have ended

When enabled, ThinkKiosk will only start its idle timer when no remote sessions are running.

Perform the following action when ThinkKiosk is closed

When the ThinkKiosk UI is closed, the configured action will be performed on the client device.

Computer Settings – Power Option



Power Saving Options:

Shutdown Endpoint after this time

If enabled, ThinKiosk will shut down the device after the time of day specified.

Restart Endpoint at this time

If enabled, ThinKiosk will restart the device after the time of day specified.

Length of time to display a warning to the user

When a shutdown power event has occurred, a warning is displayed to the user before shutdown is initialised, this control how long that warning will be displayed.

Don't force power options

By default, ThinKiosk will apply the force flag when initialising power actions such as Logoff, Restart and Shutdown. Enabling this option will remove the force flag.



Suppress power options warning dialogs

When enabled the 'Are you sure?' warning dialogs will be suppressed when using the Logoff, Shutdown and Restart power option buttons.

Turn off Monitor after

If enabled, the Windows power plan is configured to turn off the monitor if the device is idle for more than the configured number of seconds.

Turn off Hard Disk after

If enabled, the Windows power plan is configured to turn off local hard disks if they are idle for more than the configured number of seconds.

Go to Sleep after

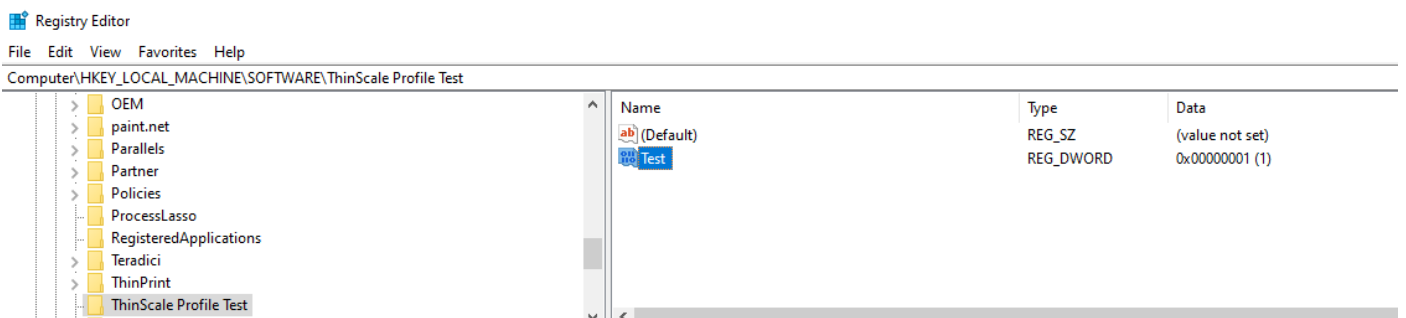
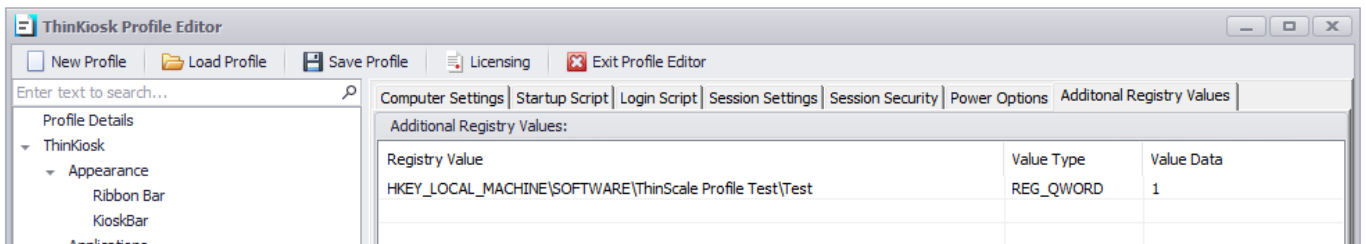
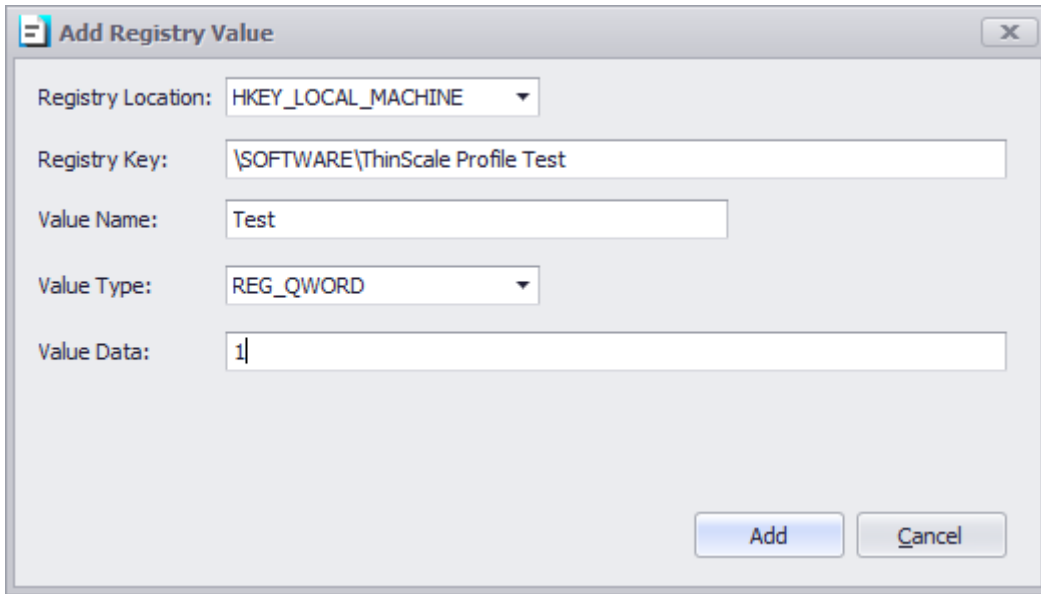
If enabled, the Windows power plan is configured to put the device into sleep mode if it is idle for more than the configured number of seconds.

Require password after Sleep

If enabled, Windows will prompt the password of the logged-on user when it wakes up.

Enable Hybrid Sleep

If enabled, the Windows power plan is configured to put the device into hybrid sleep mode if it is idle for more than the configured number of seconds.



Note: these reg keys are volatile, meaning when the TK logs off or unlocked, the keys are removed and are only applied when inside the TK session.

Also unlocking TK will remove the applied keys



Computer Settings - Proxy Server Settings

The screenshot shows the 'ThinKiosk Profile Editor' window with the 'Proxy Server Settings' tab selected. The interface includes a left-hand navigation pane, a top menu bar, and a main content area with several sections for configuring proxy settings.

ThinKiosk Profile Editor

Save Profile | Export Profile | Import Profile | Exit Profile Editor | Import/Export Wizard

Enter text to search...

- Profile Details
 - ThinkKiosk
 - Access Policies
 - Computer Settings
 - Startup Script
 - Login Script
 - Logoff Script
 - Session Settings
 - Session Security
 - Power Options
 - Additional Registry Values
 - Proxy Server Settings**
 - Privacy Settings (Win10)
 - Lock Screen
 - Authentication Helper
 - End Point Protection
 - End Point Security
 - Administration
 - Software Package Installation
 - Client Paths
 - ThinScale Virtual Desktop Agent

Proxy Server Settings:

Apply Proxy Settings

Auto Configuration:

Automatically detect settings

Use automatic configuration script

Address

Proxy Server:

Use a proxy server

Address Port

Use the proxy server except for addresses starts with the following entries. Use semicolon (;) to seperate entries.

Bypass proxy server for local addresses

Advanced Settings

Type	Proxy Address	Port
HTTP	<input type="text"/>	<input type="text" value="0"/>
Secure	<input type="text"/>	<input type="text" value="0"/>
FTP	<input type="text"/>	<input type="text" value="0"/>
Socks	<input type="text"/>	<input type="text" value="0"/>

Use the same proxy server for all protocols

Advanced Internet Settings:

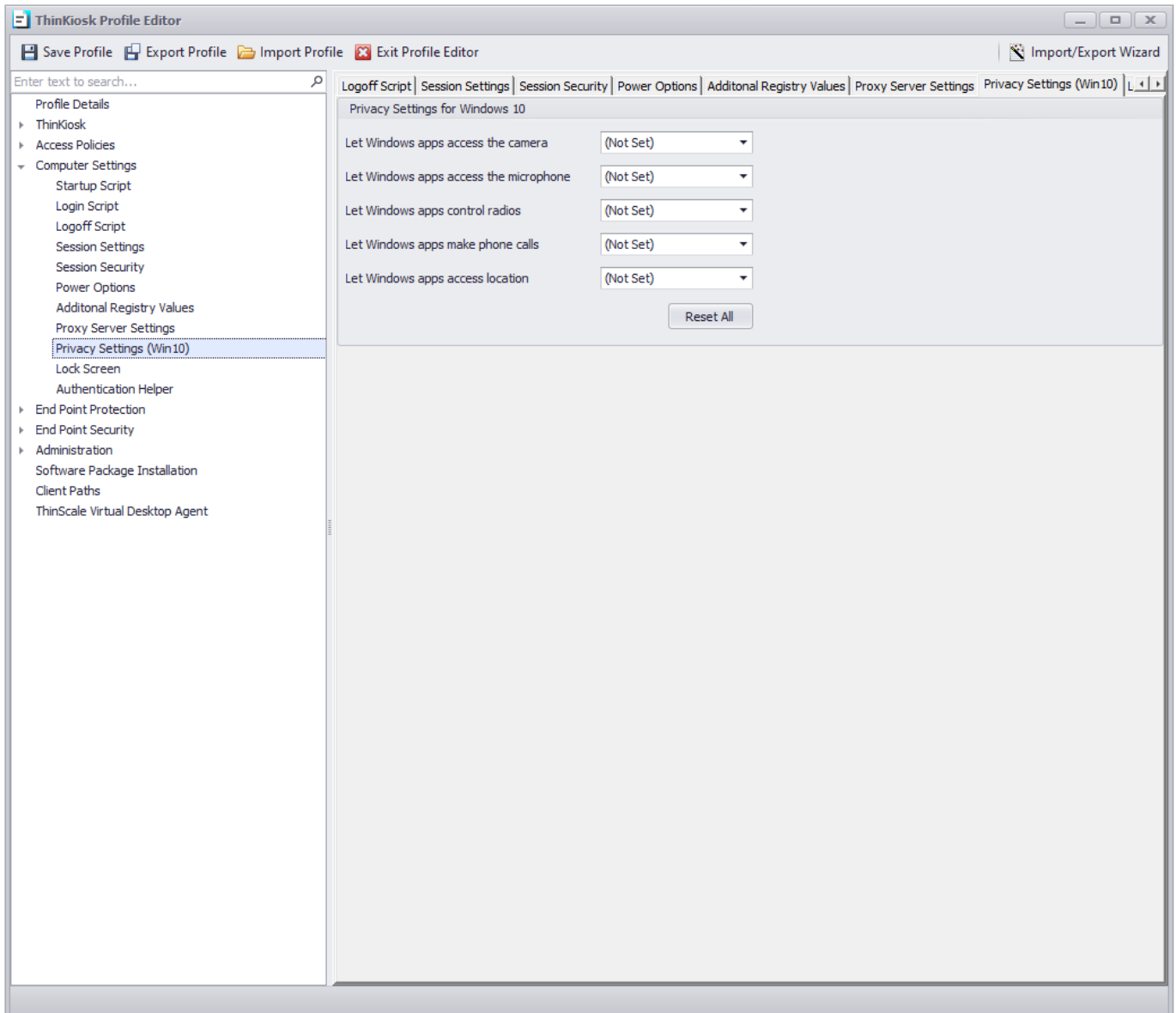
PrivDiscUIShown Use HTTP 1.1

Use HTTP 1.1 through proxy connections Warn On Intranet

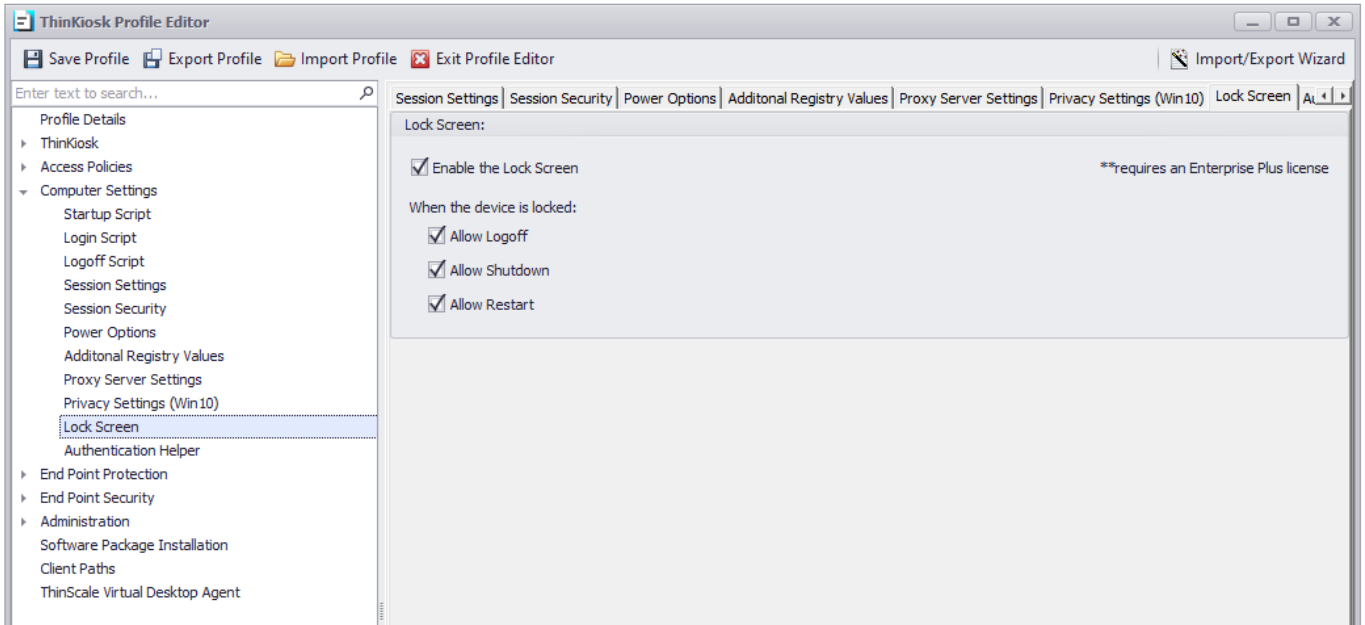
Send URL path as UTF-8 Do not save encrypted pages on disc



Computer Settings - Privacy Settings (Win10)

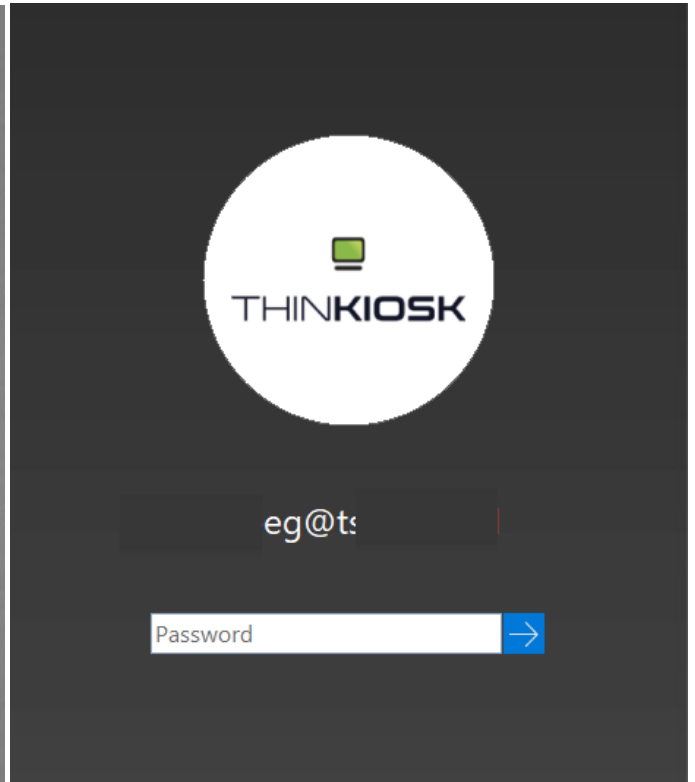
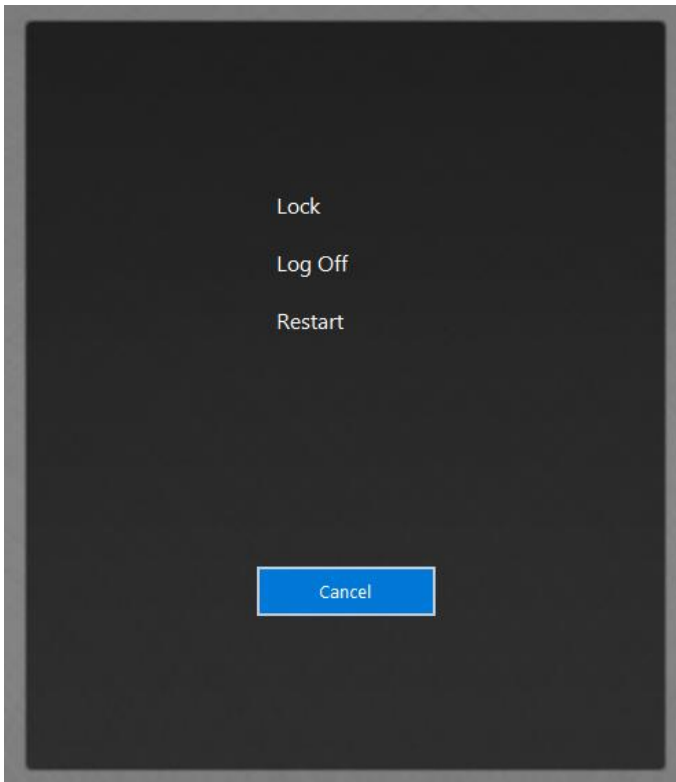


Computer Settings - Lock Screen



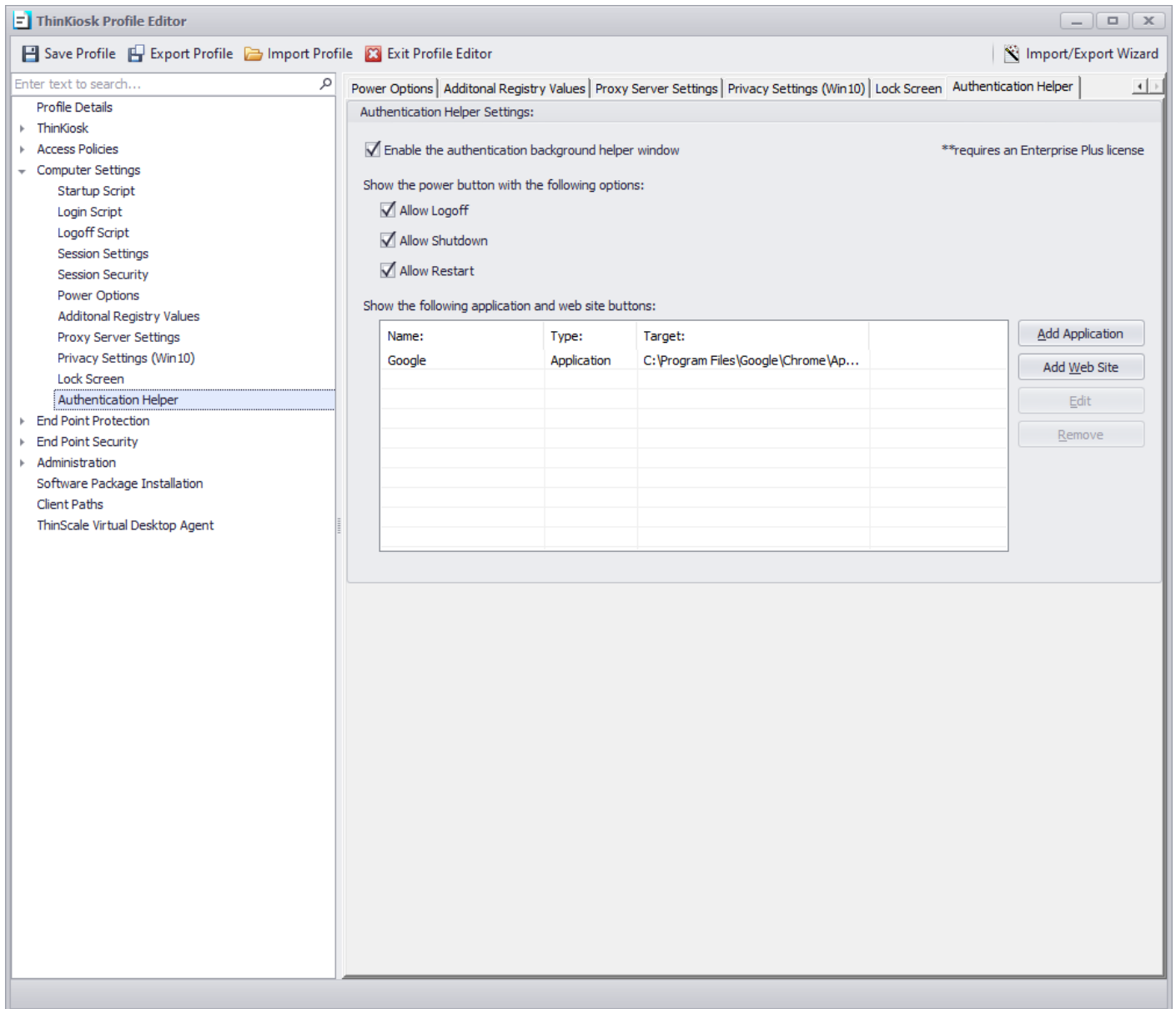
If enabled, the CAD screen will be replaced by the ThinScale Lock Screen where users will be able to lock and unlock their screen using the Auth Provider assigned to the device folder.

Additionally, you can also log off, shut down and restart.





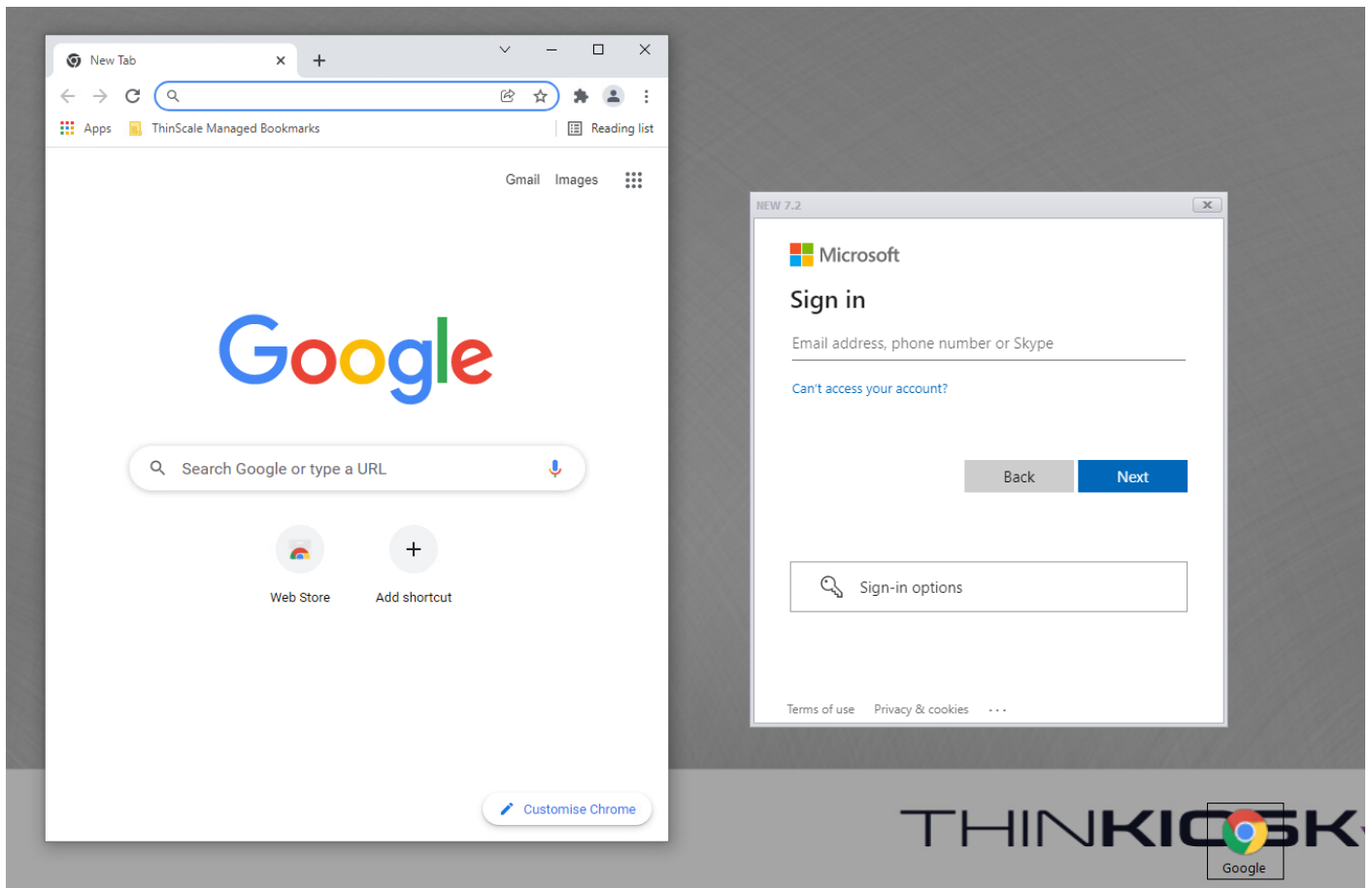
Computer Settings – Authentication Helper



The Authentication Helper Window is very useful in events where for any reason the main authentication provider is not working. Think about a scenario where a password need reset or expires.

With the Authentication Helper, you can launch a webpage, reset the password and then log in to TK just fine.

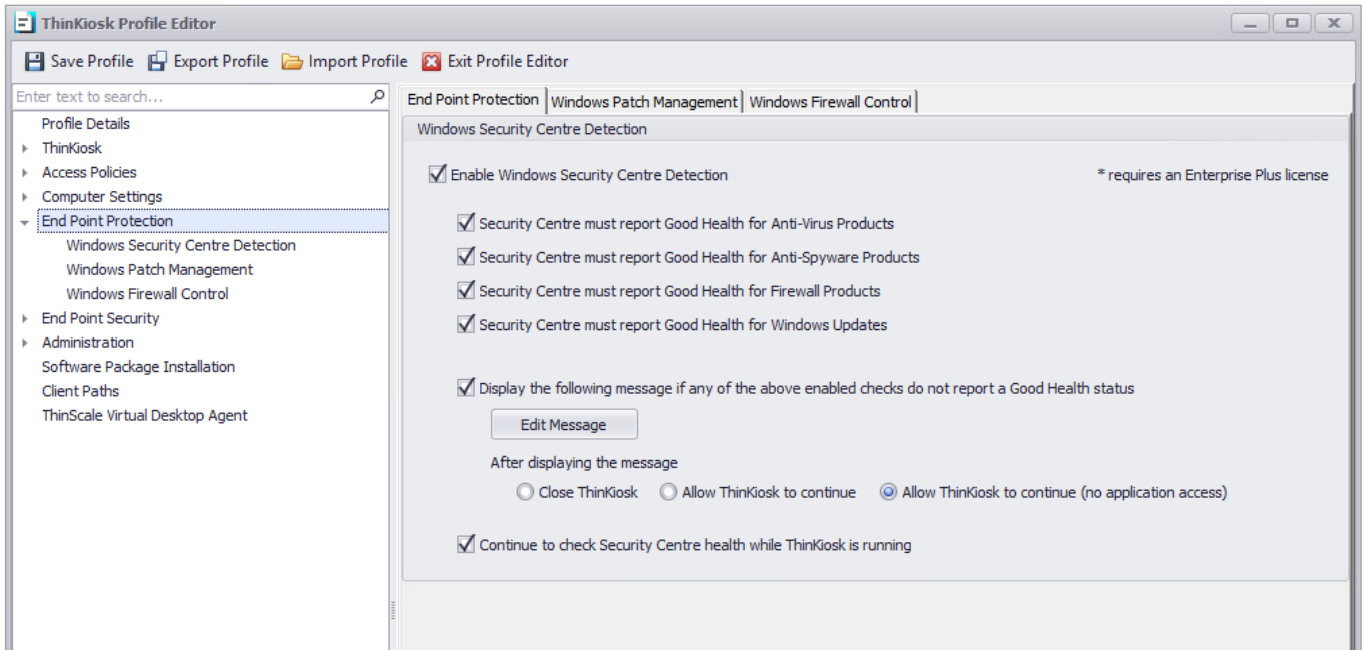
Alternatively, you can also launch an executable, log off, shut down or restart.





9. End Point Protection:

Windows Security Centre Detection

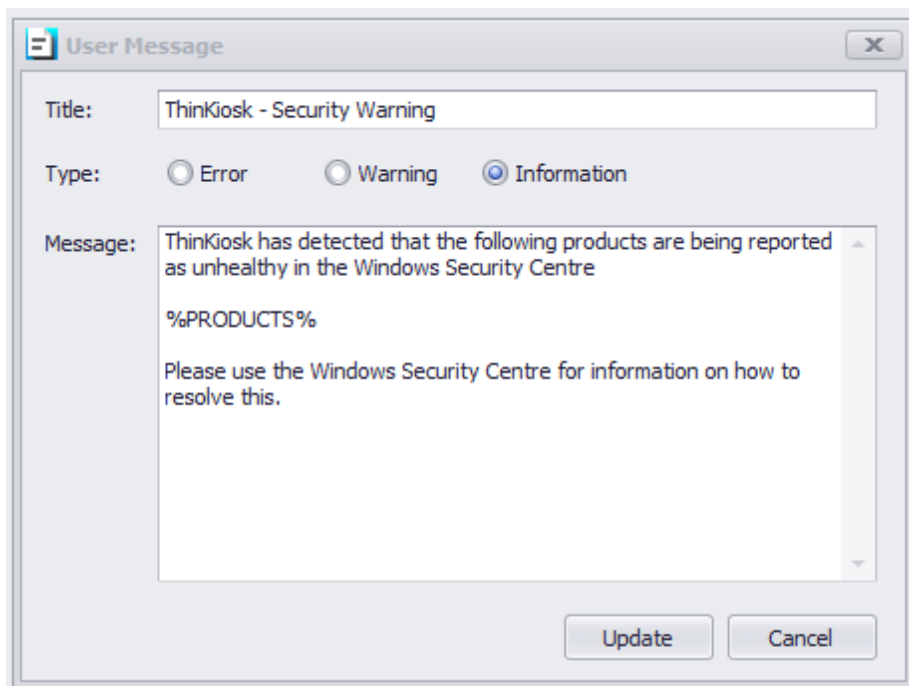


End Point Protection - Windows Security Centre Detection

Enable Security Centre detection

If enabled, ThinKiosk will scan the Windows Security Centre, for the health of Anti-virus, Anti-spyware, Firewall and Windows update. (only the selected components are scanned). If the Security Centre reports poor health results, a message will be shown to the user. This message can be modified as you like, and a different action can be selected based on the results.

Note: Error, Warning, Information refers to the icon style of the message box.



After displaying this message

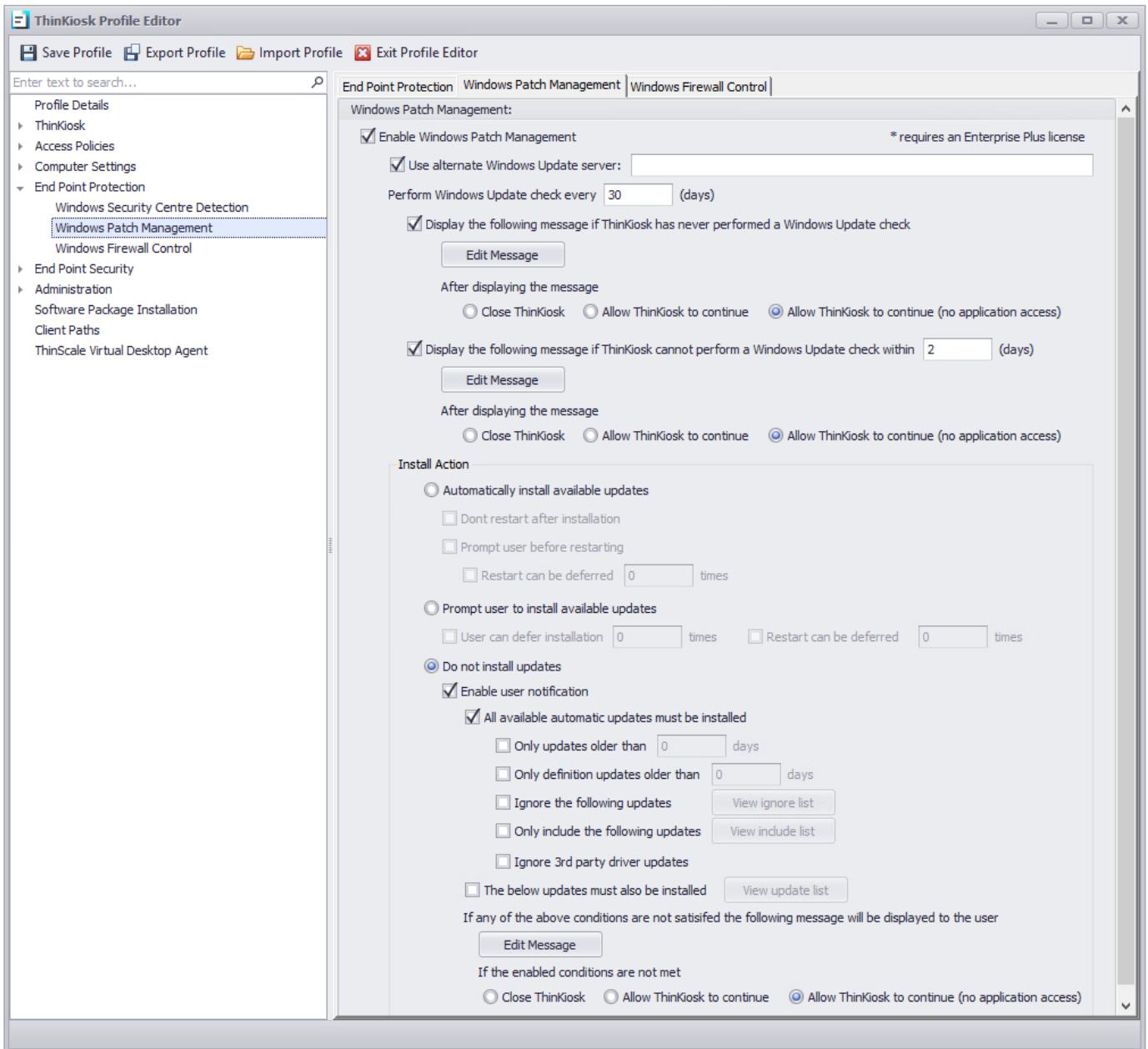
If the Security Centre has reported poor health for any of the configured components, Administrators can decide to close ThinKiosk, allow ThinKiosk to continue, or allow ThinKiosk to continue without access to any application.

Continue to check Security Centre health while ThinKiosk is running.

ThinKiosk will normally check the Security Centre health at every startup. Enabling this option will check the health at a regular interval.



End Point Protection - Windows Patch Management



Enable Windows Patch Management

If enabled ThinKiosk will check for Windows Updates.

Use alternate Windows Update server

If enabled, ThinKiosk will use a different server to retrieve updated information, such as a corporate WSUS server.

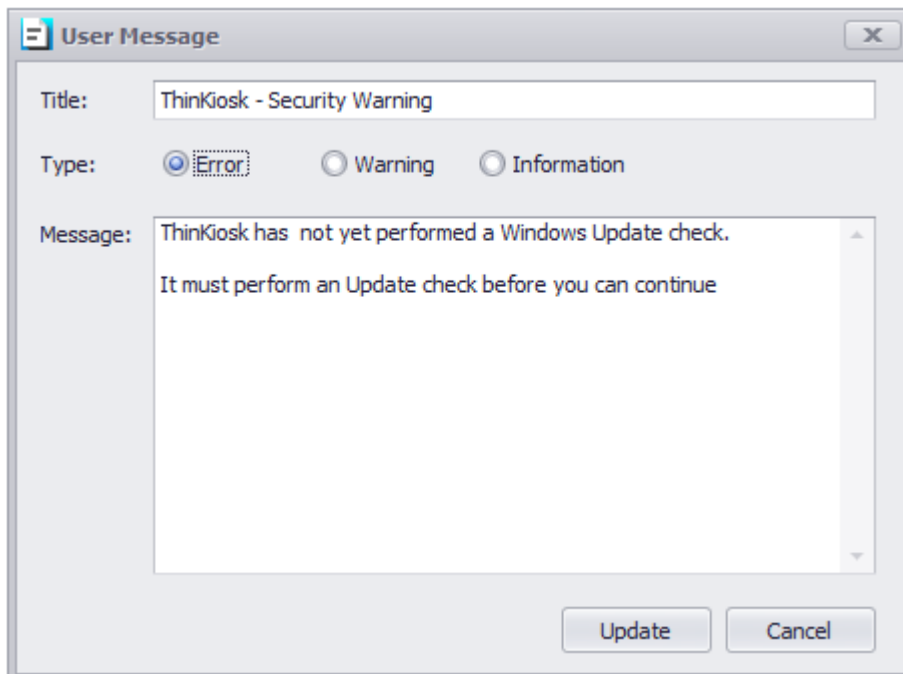
Perform Windows Update check every

If enabled, ThinkKiosk will check for updates every specified number of days.

Display the following message if ThinkKiosk has never performed a Windows Update check

If enabled, a machine where Windows updates have never been performed will receive this message. This message can be modified as you like and different actions can be selected based on the results. ThinkKiosk can either be closed, allow to continue or allow to continue without access to any applications or browser.

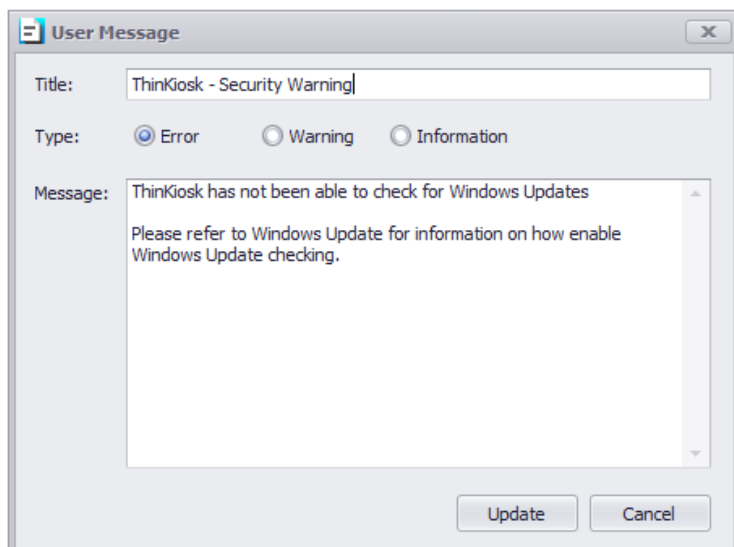
Note: Error, Warning, Information refers to the icon style of the message box.



Display the following message if ThinkKiosk cannot perform a Windows Update check within

If enabled, a machine where Windows updates couldn't be performed for a certain amount of days will receive this message. This message can be modified as you like and different actions can be selected based on the results. ThinkKiosk can either be closed, allow to continue or allow to continue without access to any applications or browser.

Note: Error, Warning, Information refers to the icon style of the message box.



Install Action

Determines the action that is performed when ThinkKiosk detects available updates for installation

Automatically install available updates

If enabled, ThinkKiosk will silently install available updates.

Don't restart after installation

If enabled, ThinkKiosk won't restart after the available updates have been installed.

Prompt user before restarting

If enabled, the user will see a countdown dialog box before ThinkKiosk will restart, giving the user time to save their work.

Restart can be deferred

If enabled, the user can defer a restart by the amount specified. When the last defer has been reached user cannot stop the auto-restart processes and a countdown dialog box will show the remaining time.

Prompt user to install available updates

If enabled, the user can decide to install or not any available updates.



Users can defer installation

If enabled, the user can defer the installation process.

Restart can be deferred

If enabled, the user can defer a restart. When the last defer have been reached user cannot stop the auto-restart processes and a countdown dialog box will show the remaining time.

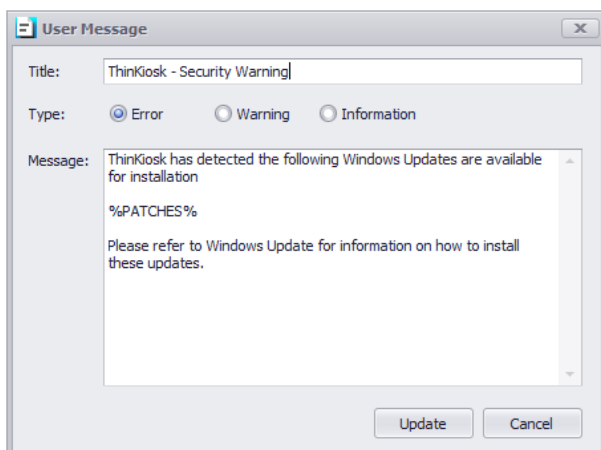
Do not install updates

If enabled, ThinKiosk won't install any available updates

Enable user notification

If enabled, a message will be displayed to the user. This message can be modified as you like, and a different action can be selected based on the results. ThinKiosk can either be closed, allow to continue or allow to continue without access to any applications or browser.

Note: Error, Warning, Information refers to the icon style of the message box.



All available automatic updates must be installed

If enabled, and “Close ThinKiosk” is selected, users must install all available updates, or they won't be able to use ThinKiosk.

If enabled, and “Allow ThinKiosk to Continue” is selected, the user will be able to launch ThinKiosk.



If enabled, and “Allow ThinKiosk to continue (no application)” is selected, the user will be able to use ThinKiosk but with no access to the applications or browser.

Only updates older than

If enabled, and “Close ThinKiosk” is selected, users must install only available updates older than the amount of day specified, or they won’t be able to use ThinKiosk.

If enabled, and “Allow ThinKiosk to Continue” is selected, the user will be able to launch ThinKiosk.

If enabled, and “Allow ThinKiosk to continue (no application)” is selected, the user will be able to use ThinKiosk but with no access to the applications or browser.

Only definition updates older than

If enabled, and “Close ThinKiosk” is selected, users must install only available definitions updates older than the amount of day specified, or they will not be able to use ThinKiosk.

If enabled, and “Allow ThinKiosk to Continue” is selected, the user will be able to launch ThinKiosk.

If enabled, and “Allow ThinKiosk to continue (no application)” is selected, the user will be able to use ThinKiosk but with no access to the applications or browser.

Ignore the following updates

If enabled, all the updates specified in the list will be ignored.

Note: if an update is added to the list after the update window check, a manual check will be necessary.



The below updates must also be installed

If enabled, the Administrator can create a list of the relevant updates the user must have installed on their machines.

If enabled, and “Close ThinKiosk” is selected, users must install all configured updates, or they won’t be able to use ThinKiosk.

If enabled, and “Allow ThinKiosk to Continue” is selected, the user will be able to launch ThinKiosk.

If enabled, and “Allow ThinKiosk to continue (no application)” is selected, the user will be able to use ThinKiosk but with no access to the applications or browser.

Add Update

KB Number: KB 123456

Description: ThinKiosk 5.1 test update

Operating Systems

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10 (1507)
- Windows 10 (1511)
- Windows 10 (1607)
- Windows 10 (1703)
- Windows 10 (1709)

Add Cancel

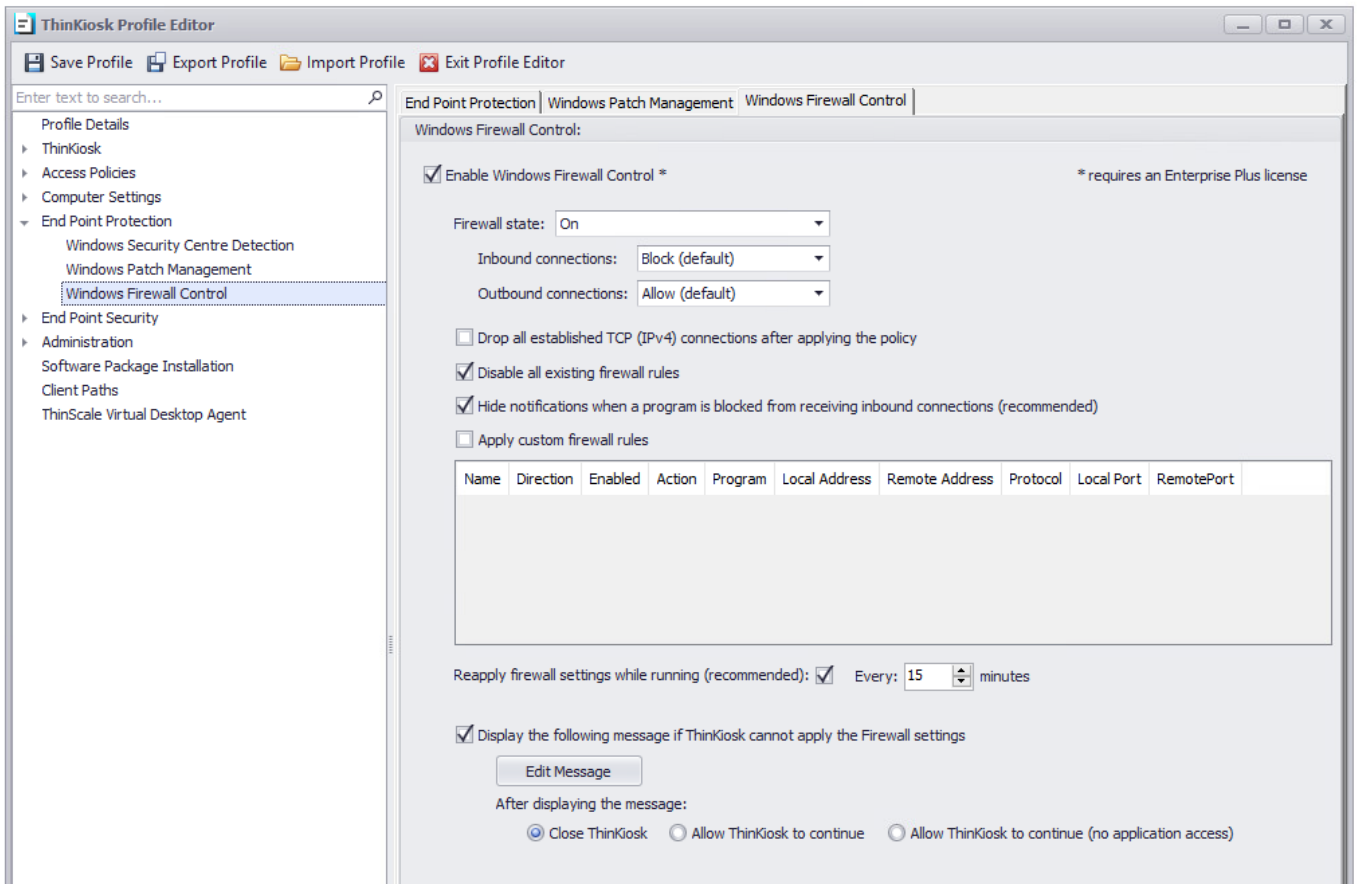
Windows Updates

KB Number:	Description:
KB 123456	ThinKiosk 5 test update

Add Update Edit Update Remove Update Close



End Point Protection - Windows Firewall Control



Windows Firewall Control

Enable Windows Firewall Control

If enabled, you will be able to control the Windows Firewall policy

Firewall state

Turns the Windows Firewall on or off.

Inbound connections

Configures the action that applies when no rules match the inbound network connection attempt

Outbound connections

Configures the action that applies when no rules match the outbound network connection attempt



Disable all existing rules

If enabled, ThinKiosk will disable all current Windows firewall rules. ThinKiosk will do a backup of all the existing rulesets and then disable them. When ThinKiosk policies are removed all original Firewall rules are recreated.

Hide notifications when a program is blocked from receiving inbound connections

If enabled, notifications coming from a program that has been blocked by the firewall will be suppressed.

Apply Custom firewall rules

Create custom rules for inbound and outbound traffic.

Apply custom firewall rules:

Name	Direction	Enabled	Action	Program	Local Address	Remote Address	Protocol	Local Port	RemotePort

Reapply firewall settings while running (recommended): Every: minutes

Add Firewall Rule

Enabled:

Direction: Inbound Outbound

Display name:

Program: All programs This program path:

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Protocol type:

Local port:

Remote port:

Example: 80, 443, 5000-5010

Local IP addresses:

Remote IP addresses:

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

Action: Allow Block

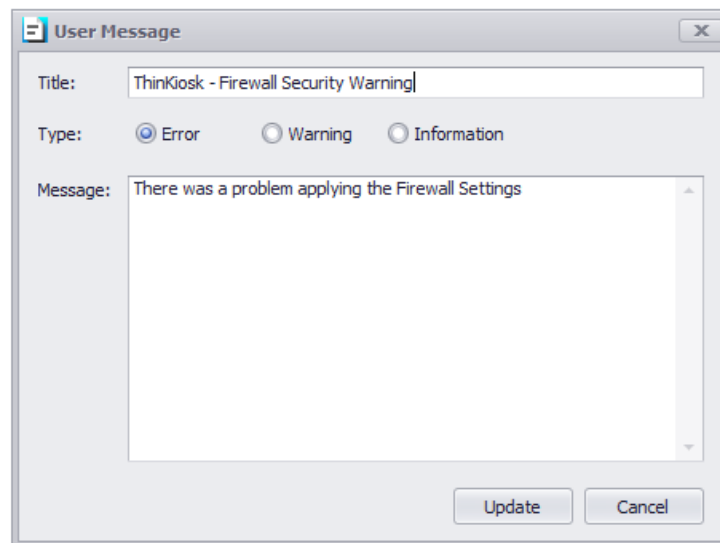
Reapply firewall setting while running

If enabled, the ThinKiosk firewall rules setting will be reapplied based on the amount specified.

Display the following message if ThinKiosk cannot apply the firewall settings

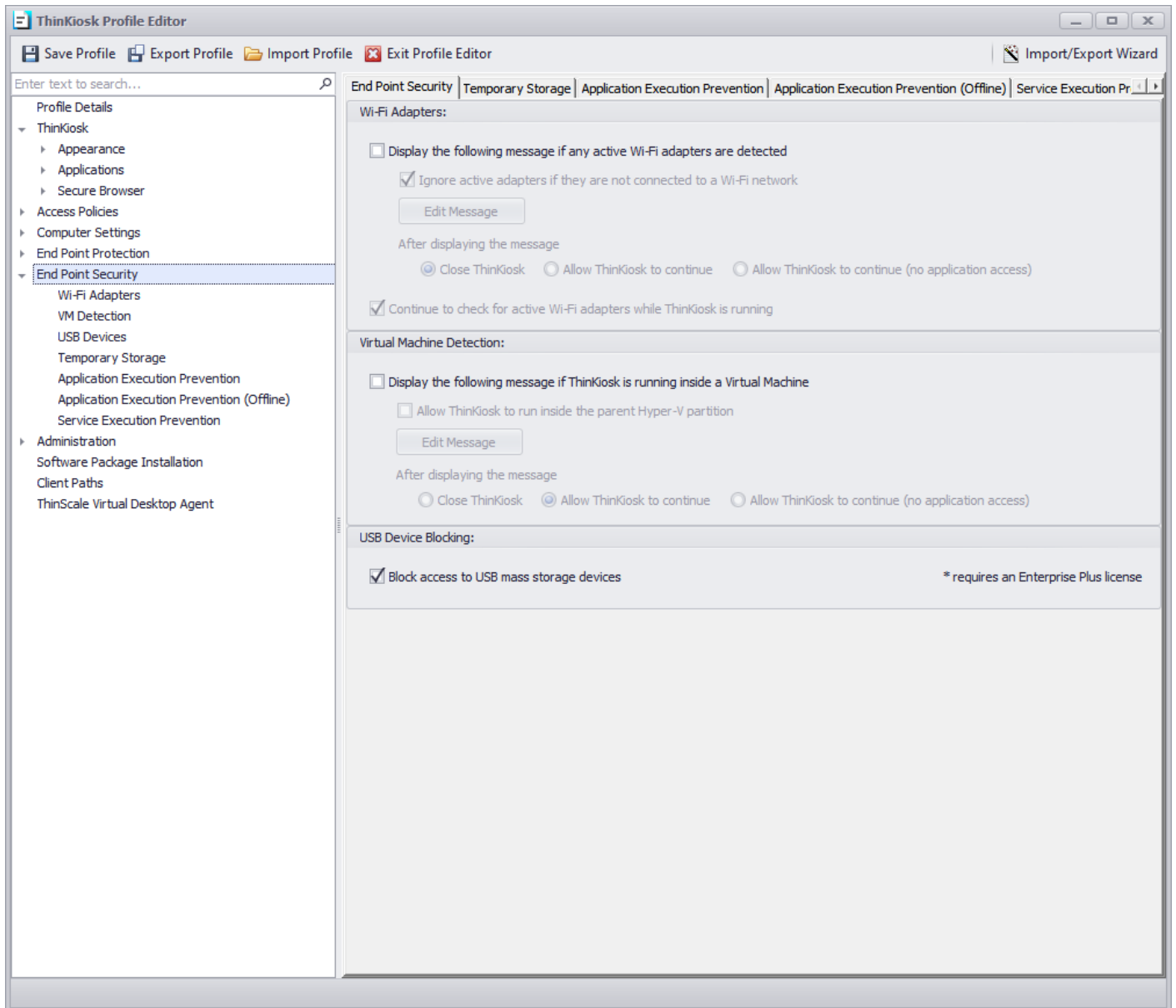
If enabled, a message will be displayed to the user. This message can be modified as you like, and different actions can be selected based on the results. ThinKiosk can be either close, allow to continue or allow to continue without access to any application or browser.

Note: Error, Warning, Information refers to the icon style of the message box.





10. End Point Security

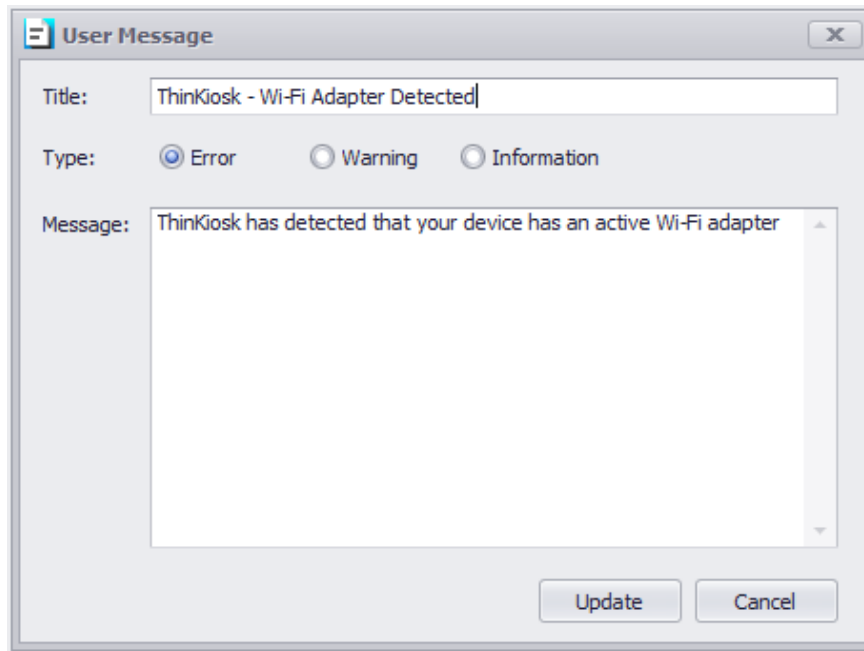


End Point Security - Wi-Fi Adapters

Display the following message if any active Wi-Fi adapters are detected

If enabled, a message will be displayed to the user if the ThinKiosk device has an active Wi-Fi adapter. This message can be modified as you like, and different actions can be selected based on the results.

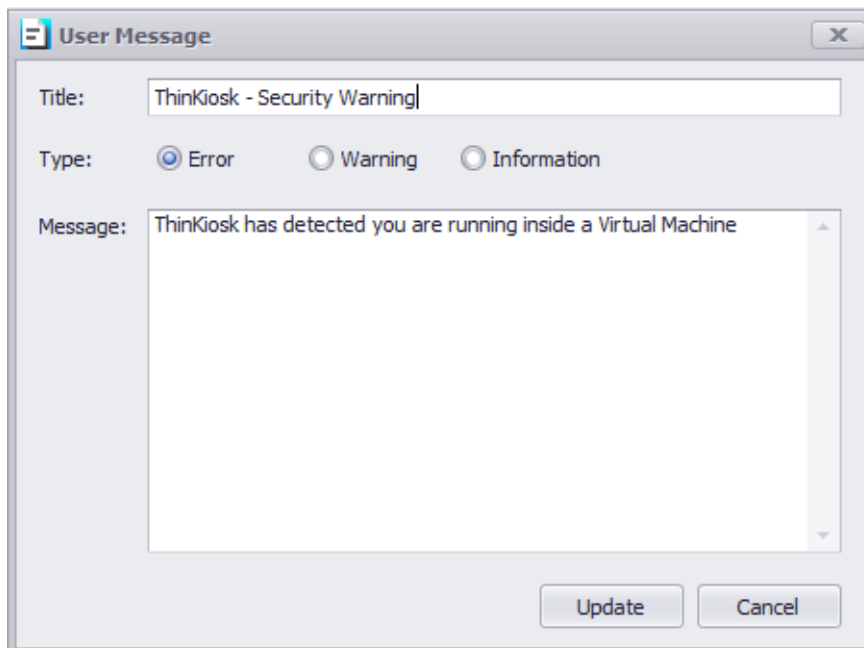
ThinkKiosk can be either close, allow to continue or allow to continue without access to any application or browser.



End Point Security - Virtual Machine Detection

Display the following message if ThinKiosk is running inside a Virtual Machine

If enabled, a message will be displayed to the user if ThinKiosk is running inside a Virtual Machine. This message can be modified as you like, and different actions can be selected based on the results. ThinKiosk can be either close, allow to continue or allow to continue without access to any application or browser.





Allow ThinKiosk to run inside the parent Hyper-V partition

If enabled, the above message will not be displayed if ThinKiosk is running inside the parent partition of a machine with the Hyper-V role installed.

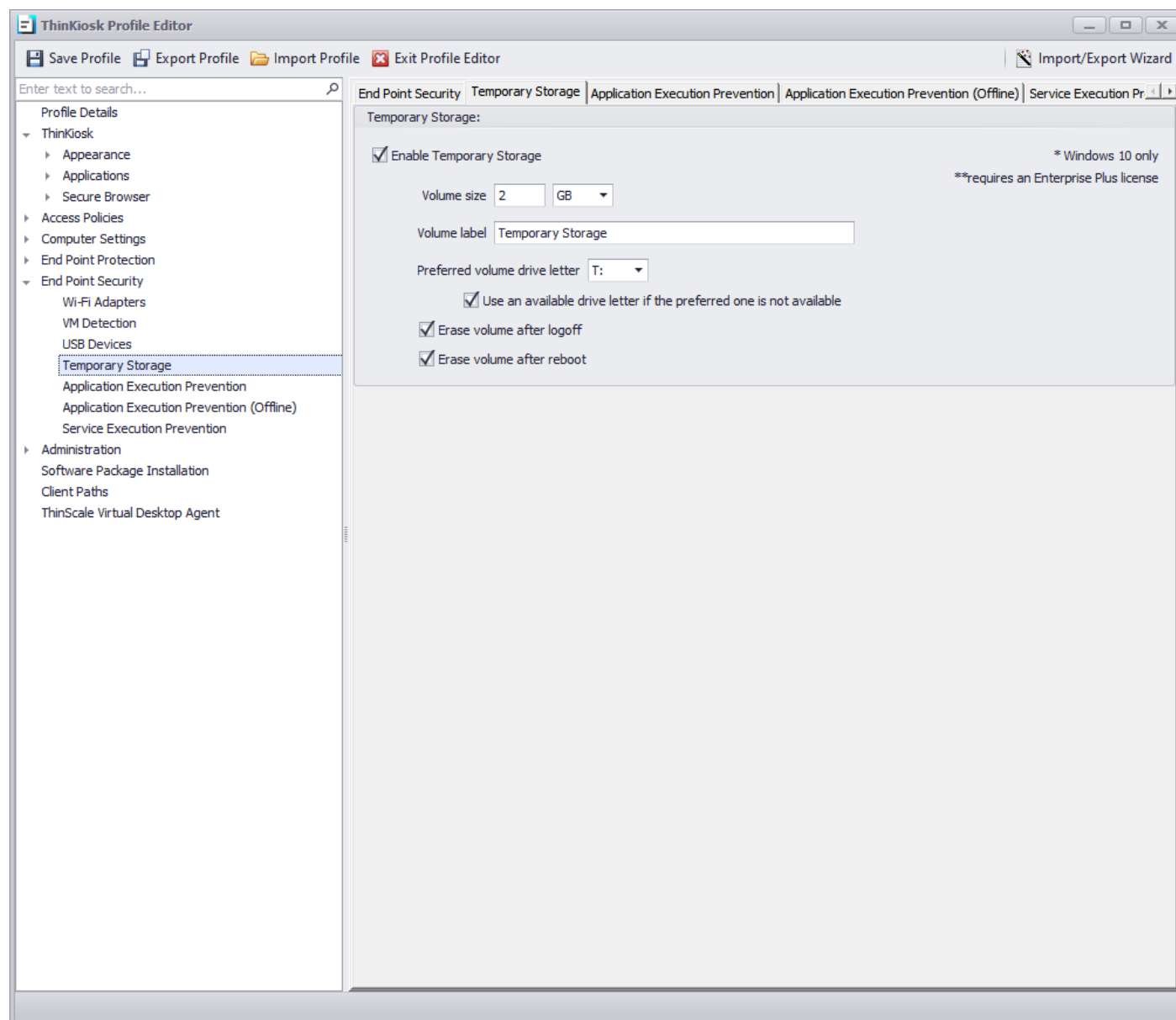
End Point Security - USB Device Blocking

Block access to USB mass storage devices

If enabled, any USB mass storage devices attached to the local machine will be blocked by default.



End Point Security – Temporary Storage



Enable Temporary Storage

Temporary Storage is a new technology in TK 7 that lets you create a temporary encrypted virtual volume on the personal device that users can use to save data from within the TK session.

The encrypted virtual volume is managed by TK and is only made available when TK is active.



Enable Temporary Storage

Select to enable Temporary Storage

Volume Size

Select the maximum size of the virtual volume. The Temporary Storage volume is dynamically sizing so will only consume actual hard disk space when data is saved to it.

Volume Label

Specify the formatted volume label of the Temporary Storage volume

Preferred Volume Drive Letter

Select the drive letter that will be assigned to the Temporary Storage Volume

Use an available drive letter if the preferred one is not available

If enabled and the preferred driver letter is in use on the local device, TK will use the first available drive letter on the device.

Erase Volume after logoff

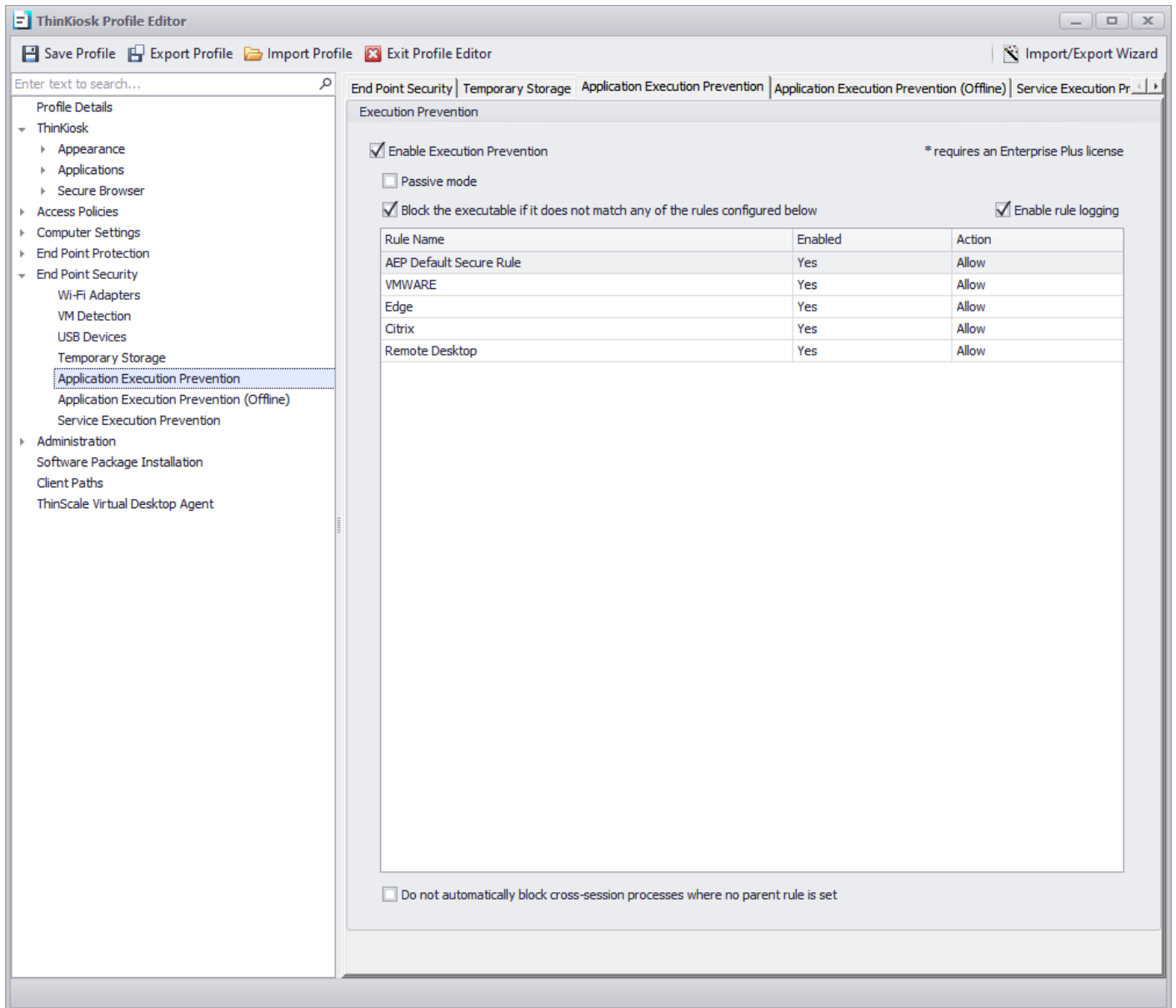
When enabled, all data that was saved to the virtual volume during the TK session will be deleted at the logoff

Erase Volume after reboot

When enabled, all data that was saved to the virtual volume during the TK session will be deleted when the device is rebooted



End Point Security - Application Execution Prevention



Application Execution Prevention

Enable Application Execution Prevention

If enabled, any processes added to the list will be allowed/ denied executing.

Passive mode

If enabled, any processes added to the list will always be allowed to execute.

Enable rule logging

If enabled, the administrator will be able to retrieve more information about the application being prevented from executing, from the logs file.

Block the executable if it does not match any of the configured rules below

If enabled, and no other rules are created in the list, the console will auto-create a rule for you to prevent incorrect system operation.

Add Application Execution Prevention Rule

Rule Name:

Rule Enabled:

Action: Block

And Is Same Session Is True

[Browse](#) Add Remove

Relationship	Condition	Operator	Value

Parent Process Rule:

Rule Name

Do not automatically block cross-session processes where no parent rule is set

Add Remove

OK Preview Cancel



Add/ Edit Rule Dialog Box

Rule Name

Describe the name of the rule to be applied.

Action

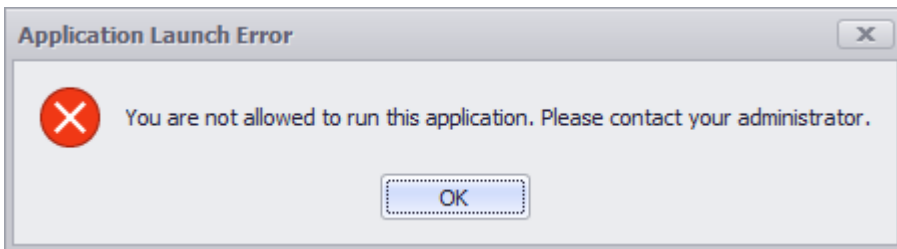
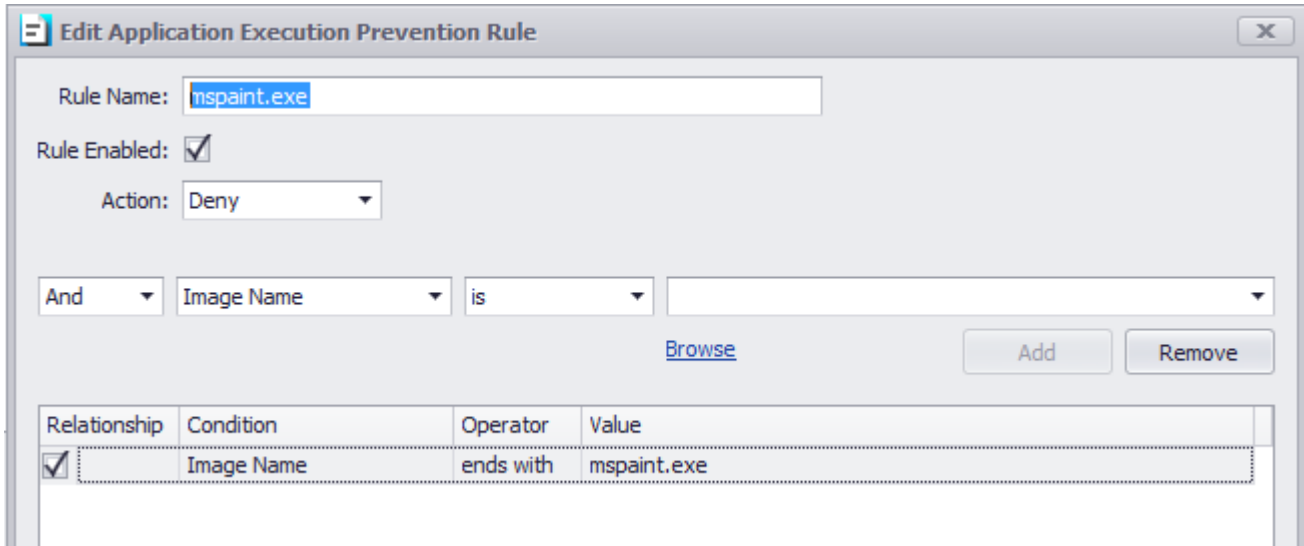
Select “Allow” or “Deny” to allow or deny Application execution.

Adding a rule

When creating a rule, there are relationships and conditions you can use to match or not a specific file name, size of the file, last modified date and time, Windows OS binary and all the other options in the profile editor.



An example of the rule can be seen in the screenshot below. The rule will deny, the locally installed notepad application, from executing. When the user accessing that application will click on the icon, they will be prompted with a dialog message.



Application Execution Prevention Processing Example

Application execution prevention rule processing is sequenced by the relationship between each condition in the rule and the preceding condition. For ‘and’ conditions the conditional test must all pass. For ‘or’ conditions they are examined as a “one of many” situation. The 1st condition in the rule will ignore the ‘relationship’ field as there are no preceding conditions. In the following example, we show a rule to allow only 2 very specific versions of “Calculator” given the filename and sizes.

First, we want to ensure the correct filename, so we add a condition to verify the filename. “Image Name” represents the full path and filename and the only condition where upper/lower case does not matter.



Rule Name:

Rule Enabled:

Action:

And ends with

[Browse](#)

Relationship	Condition	Operator	Value
<input checked="" type="checkbox"/>	Image Name	ends with	calc.exe

Secondly, we want to allow 2 possible file sizes as either of the 2. To do this we add another condition to test the file size as shown below. The value to check was obtained using the “Browse” action and selecting the required binary – the editor will automatically select the appropriate value and populate the field.

Rule Name:

Rule Enabled:

Action:

And is

[Browse](#)

Relationship	Condition	Operator	Value
<input checked="" type="checkbox"/>	Image Name	ends with	calc.exe

Finally, we need to add a second size to allow. The difference is we must select a relationship of ‘or’ to indicate “the 1st size or the 2nd size”. In the image below, we see all 3 conditions added. This can be read as “(image name) AND (1st size OR 2nd size)”.



Add Application Execution Prevention Rule ✕

Rule Name:

Rule Enabled:

Action:

Or is

[Browse](#)

Relationship	Condition	Operator	Value
<input checked="" type="checkbox"/>	Image Name	ends with	calc.exe
<input checked="" type="checkbox"/>	And File Size	is	27648
<input checked="" type="checkbox"/>	Or File Size	is	25432

WARNING:

Application Execution Prevention is a system-level function that can prevent a system from operating correctly until the active ThinKiosk profile is corrected and reloaded. By default, ThinKiosk applications will be allowed once verified by a signed security certificate. Blocking all applications without any rules defined will ask to insert a rule to allow windows applications. All applications launched via *any* method are filtered by AEP (if AEP is enabled and ThinKiosk is running).



Parent Rule

The new Parent Process Rule will allow creating specific rule sets where it will be possible to allow/ block processes created from a parent only.

Example: To block all cmd created by the system but only allow a cmd from a trusted source (ie: VPN) follow this example:

- 1- Select the Parent Process

The screenshot shows the 'Edit Application Execution Prevention Parent Rule' dialog box. The 'Rule Name' is 'CMD Parent Rule'. The condition is set to 'And', 'Image Name', and 'Is'. A 'Browse' button is visible. Below the condition fields is a table with the following data:

Relationship	Condition	Operator	Value
<input checked="" type="checkbox"/>	Image Name	Is Not	c:\program files\openvpn connect\openvpnconnect.exe

- 2- Add the cmd

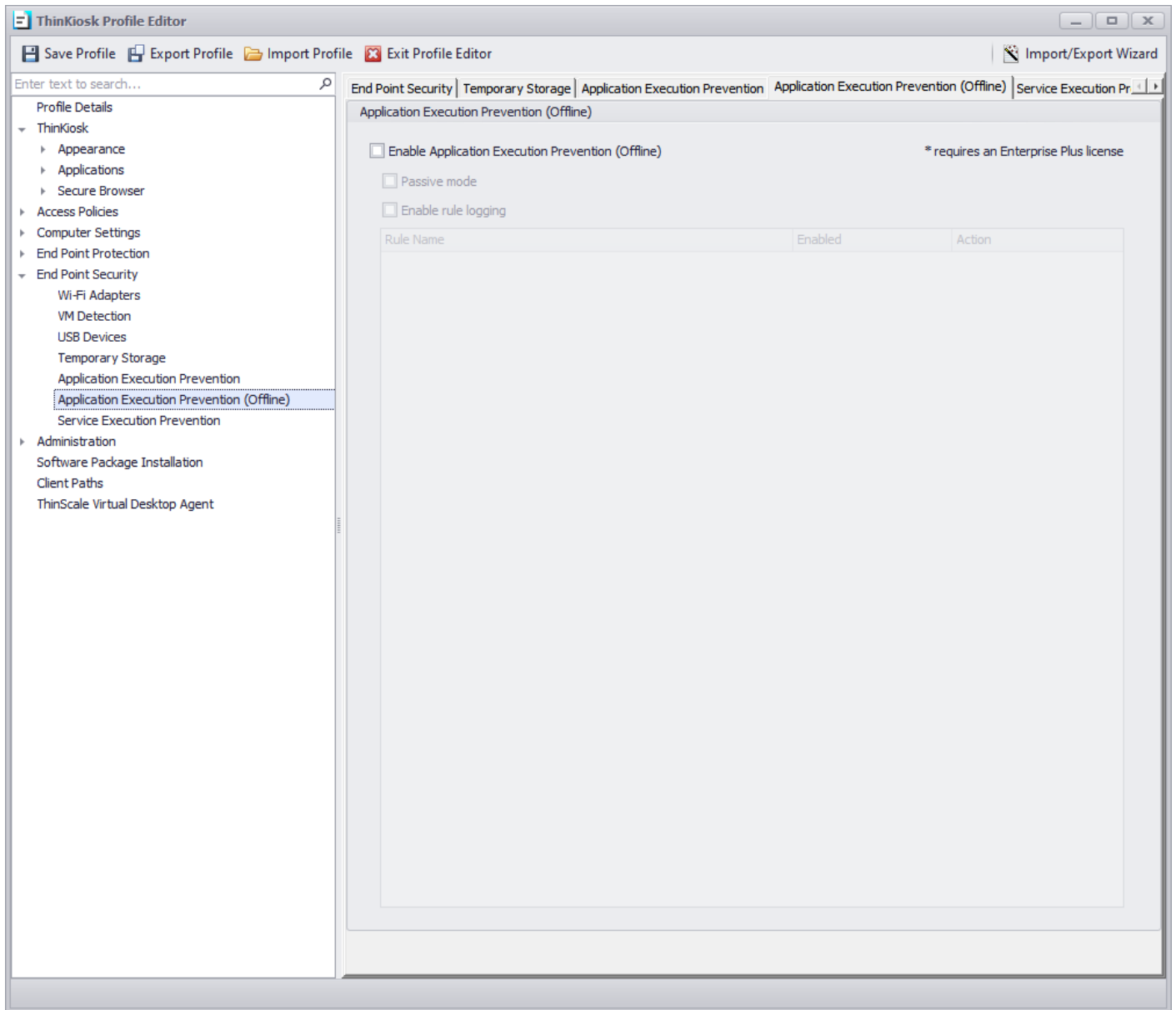
The screenshot shows the 'Add Application Execution Prevention Rule' dialog box. The 'Rule Name' is 'CMD'. 'Rule Enabled' is checked. The 'Action' is 'Block'. The condition is set to 'And', 'Image Name', and 'Ends With'. A 'Browse' button is visible. Below the condition fields is a table with the following data:

Relationship	Condition	Operator	Value
<input checked="" type="checkbox"/>	Image Name	Ends With	\cmd.exe

If the parent rule ISNOT open VPN in this case, block all cmd processes created on the system, otherwise allow it.



End Point Security - Application Execution Prevention (Offline)



The AEP (Offline) mode is the same as the normal AEP with the only difference that is targeting app applications outside the TK session.

There are cases where the administrator wants to stop application execution when the user is not logged in the TK session, the AEP offline is used to tackle exactly that use case.

Let's use an example rule blocking the Horizon view client when the TK session is not enabled.



End Point Security | Application Execution Prevention | Application Execution Prevention (Offline) | Service Execution Prevention

Application Execution Prevention (Offline)

Enable Application Execution Prevention (Offline)

Passive mode

Enable rule logging

Rule Name	Enabled	Action
Horizon	Yes	Allow
Cisco	Yes	Block
VPN	Yes	Block

Edit Application Execution Prevention (Offline) Rule

Rule Name:

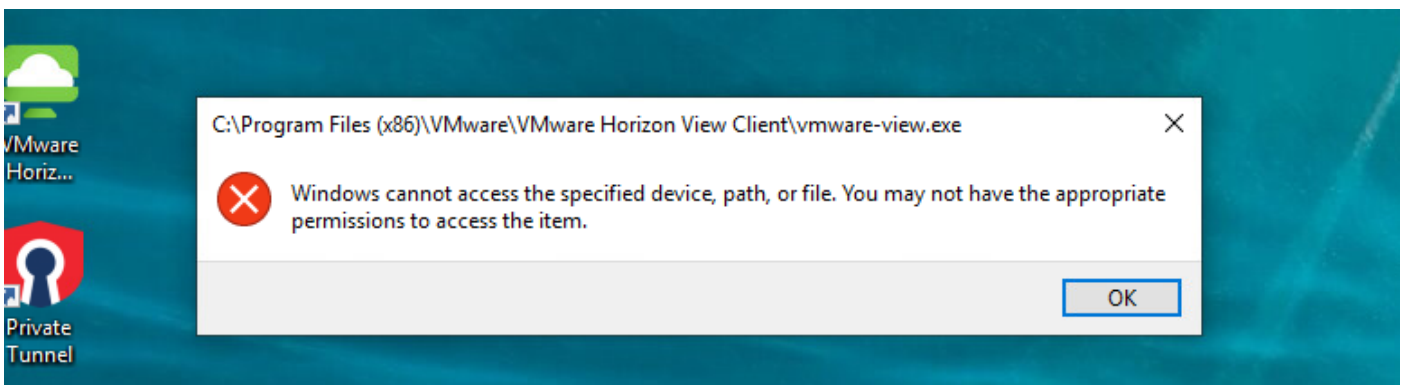
Rule Enabled:

Action:

And

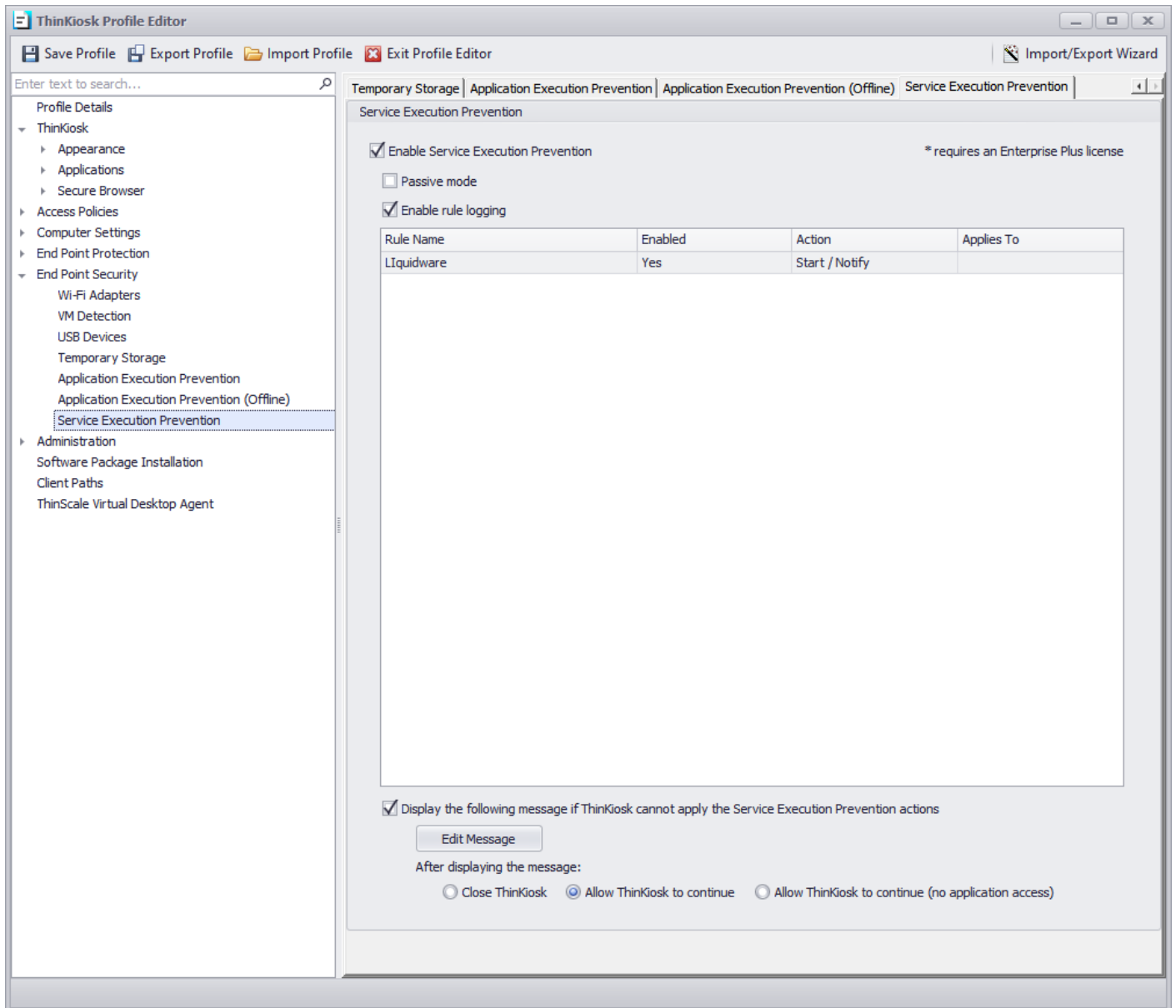
[Browse](#)

Relationship	Condition	Operator	Value
<input checked="" type="checkbox"/>	Image Name	Ends With	vmware-view.exe





End Point Security - Service Execution Prevention



Service Execution Prevention builds on existing Application Execution prevention technology to provide Windows services execution control at the system level. Using familiar concepts from AEP, an administrator can define rules for a profile to control what services can run or should be stopped. As with AEP, control is asserted over any service applications including all Windows services.

Service Execution Prevention has areas of operation - at start-up services are scanned for compliance, additionally, real-time monitoring of services takes place while ThinKiosk policies are in place.



Service Execution Prevention

Enable Service Execution Prevention

If enabled, SEP real-time monitoring will scan any services that match rules and apply any required actions.

Passive mode

If enabled, services will be scanned by Service Execution Prevention, but rule actions will not be applied.

Enable rule logging

If enabled, the administrator will be able to retrieve more information about service scanning and actions taken from the log files.

Add Service Execution Prevention Rule
X

Rule Name:

Rule Enabled:

Action: Stop

- Stop
- Stop (Force)
- Notify
- Stop / Notify
- Stop (Force) / Notify

And
Is

Add
Remove

Relationship	Condition	Operator	Value

OK
Cancel



Action setting

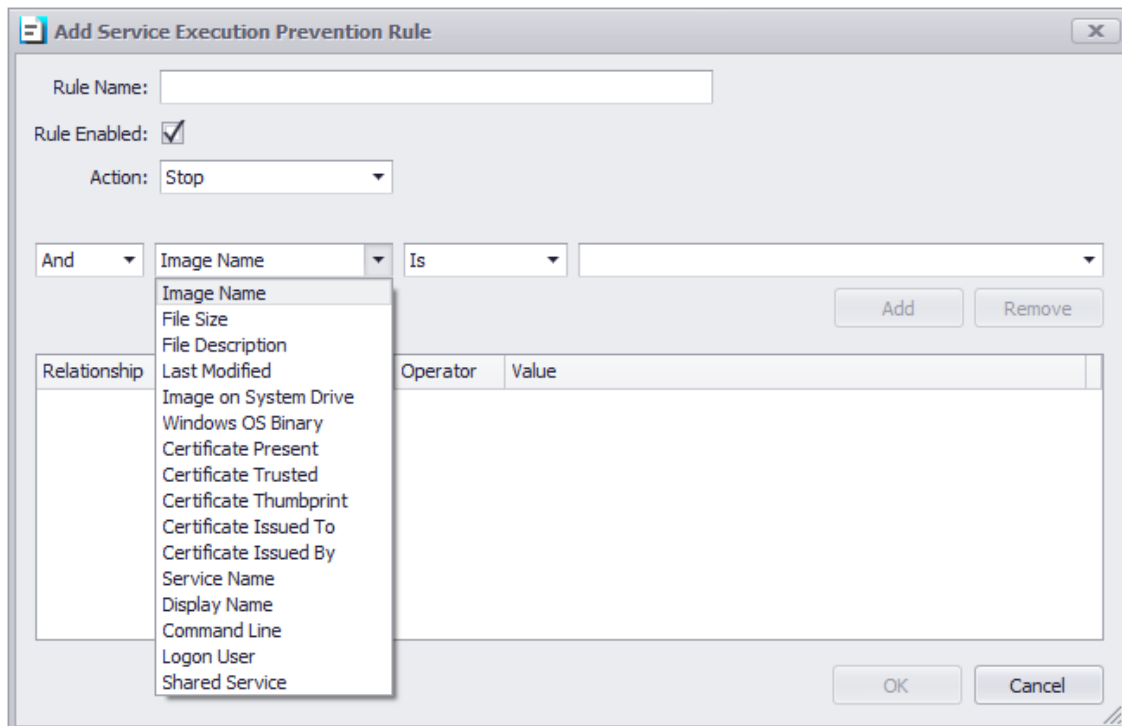
The action setting control how SEP responds to a service should it match a rule. Some action settings may cover multiple actions in which case actions are applied in the following order:

Action	Description
Start	Request the service to start cleanly.
Stop	Request the service to stop cleanly.
Stop (Force)	Request the service to stop cleanly - if it does not, force the service process to terminate. NOTE: shared Windows services will not be force stopped.
Notify	If all other actions have failed, notify the user to stop the service

Rule conditions

Condition values available to SEP rules are the same as are available to AEP rules with the addition of some service-specific items - Service Name, Display Name, Command-Line, Logon User and Shared Service.

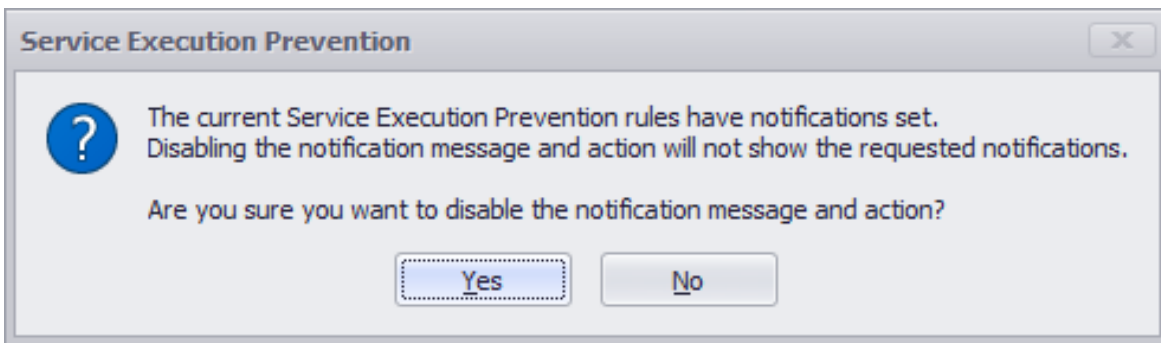
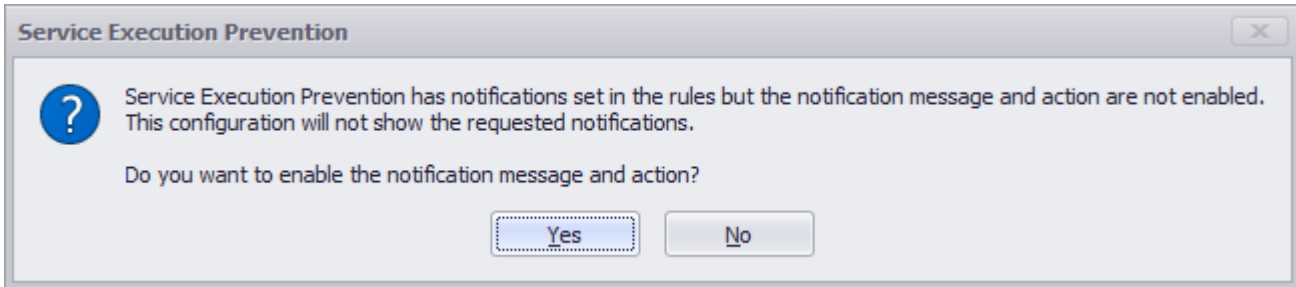
For standard service applications, the file detail conditions will reference the known service binary (also in the Command-Line condition). For shared Windows services (e.g. those that execute under the “svchost.exe” process), the file details will reference the binary containing the actual service and not the service host process – this could be either “.dll” or “.exe” file type.



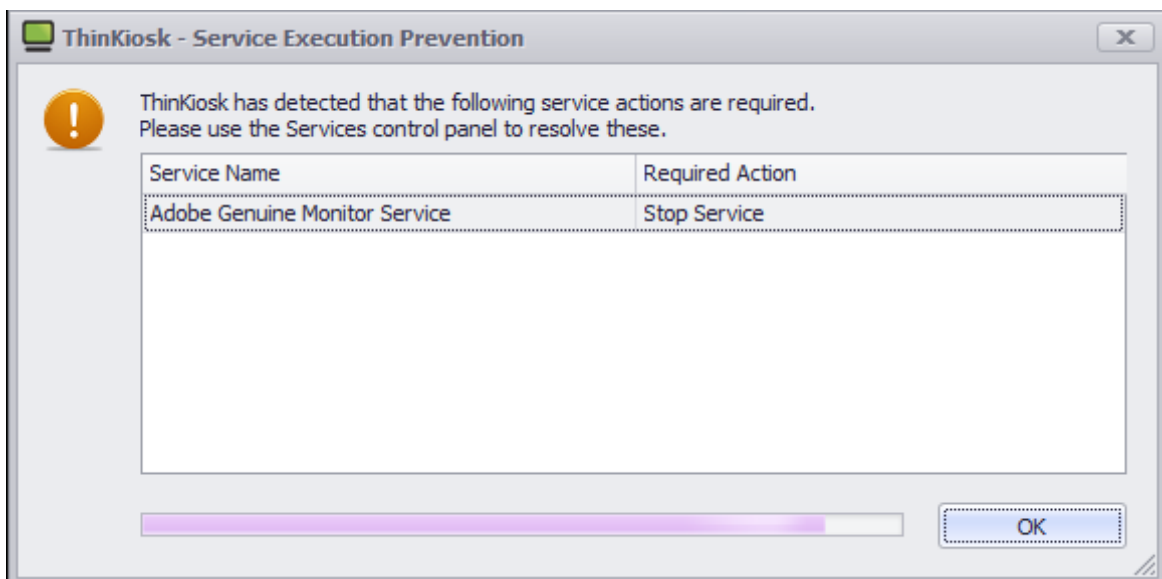


Service Execution Prevention - User Notifications

If rules are defined that use the “Notify” action the SEP profile setting for message display should be checked. If this setting is not checked the user will not be presented with any notifications even if rules request it. If the editor detects rules that require notifications one of the following warnings may be displayed.

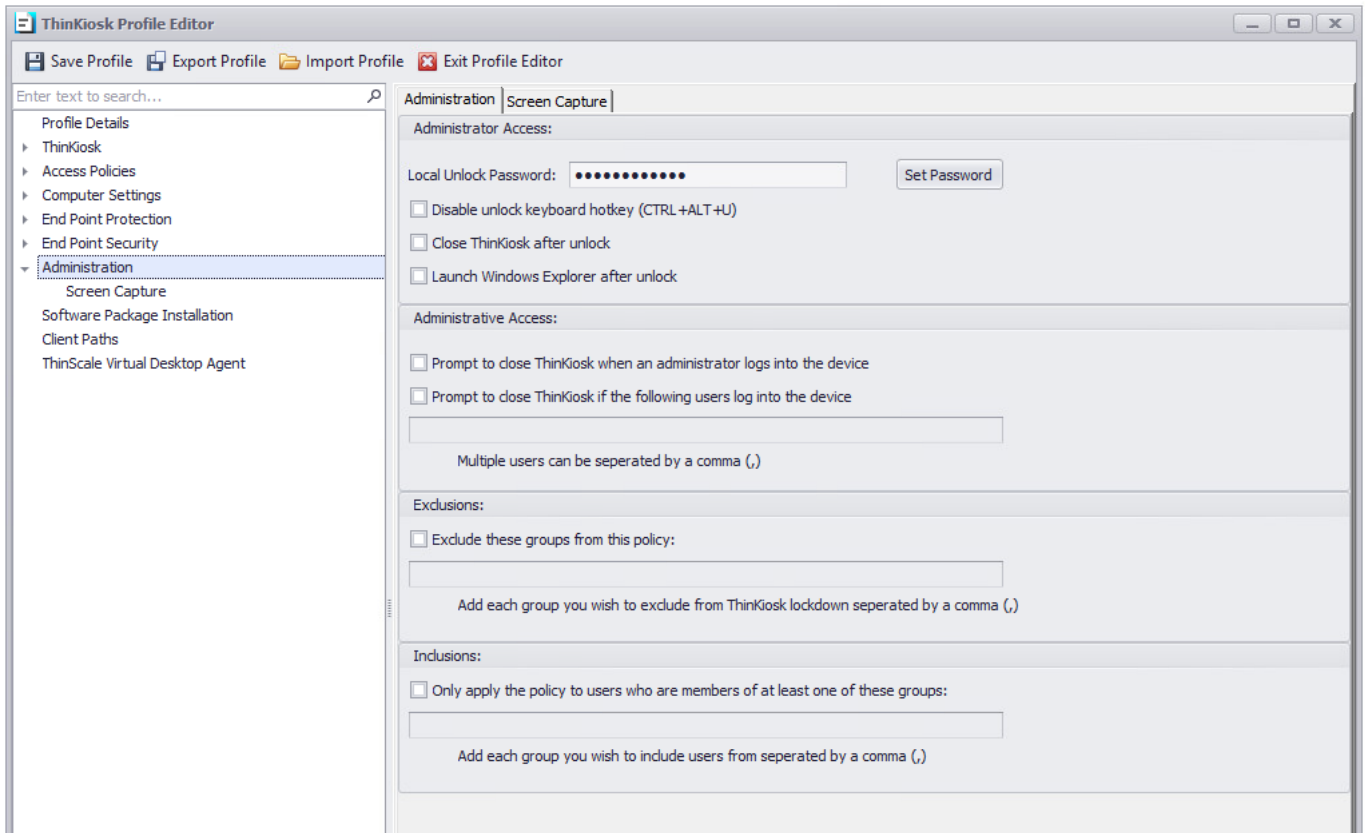


Should notifications be displayed to the user the following dialog is presented showing all requested service actions (one example action shown below). When the SEP profile setting is enabled an administrator may also require ThinKiosk to close – if required this action is performed once the notifications dialogue closes.





11. Administration



Administrator Access:

Local Unlock Password

The password is used when unlocking ThinKiosk via the padlock or CTRL+ALT+U key sequence (if not disabled).

Disable unlock keyboard hotkey (CTRL+ALT+U)

If enabled, users cannot unlock ThinKiosk using the CTRL+ALT+U key sequence.

Launch Windows Explorer after unlock

If enabled, once the machine is unlocked Windows Explorer will auto-launch.



Administrative Access:

Prompt to close ThinKiosk when an administrator logs into the device

If enabled, when an administrator logs on to the device ThinKiosk will prompt a message to “Close ThinKiosk”, “Unlock ThinKiosk”, or “Do Nothing”.

Prompt to close ThinKiosk if the following users log into the device

If enabled, when one of the listed users' logs on to the device ThinKiosk will prompt to “Close ThinKiosk”, “Unlock ThinKiosk”, or “Do Nothing”.

Exclusions:

Exclude these groups from this policy

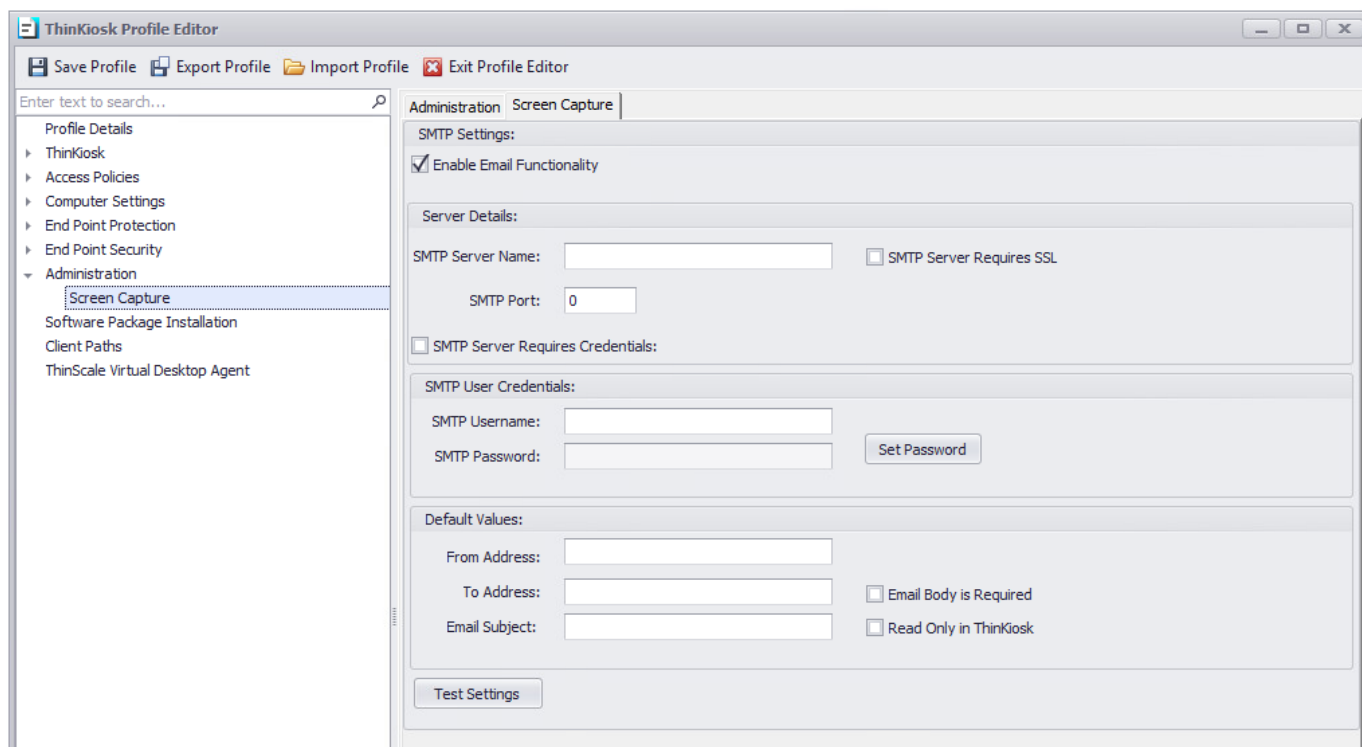
If enabled, users that are a member of any of the configured groups will not have ThinKiosk lockdown group policy applied to their session.

Inclusions:

Only apply the policy to users who are members of at least one of these groups

If enabled, users that are a member of any of the configured groups will have ThinKiosk lockdown group policy applied to their session.

Administration – Screen Capture



SMTP Settings:

Enable Email Functionality

Email functionality is required for the screen-shot option with ThinkKiosk.

Server Details:

SMTP Server Name

Hostname or IP address of the SMTP server to use.

SMTP Port

Port number the SMTP server is using.

SMTP User Credentials:

SMTP Username

The username is used to authenticate with the SMTP server.



SMTP Password

Password for the User account to authenticate with the SMTP server.

Default Values:

From Address

The default email address the email will be sent from.

To Address

The default email address the email will be sent to.

Email Subject

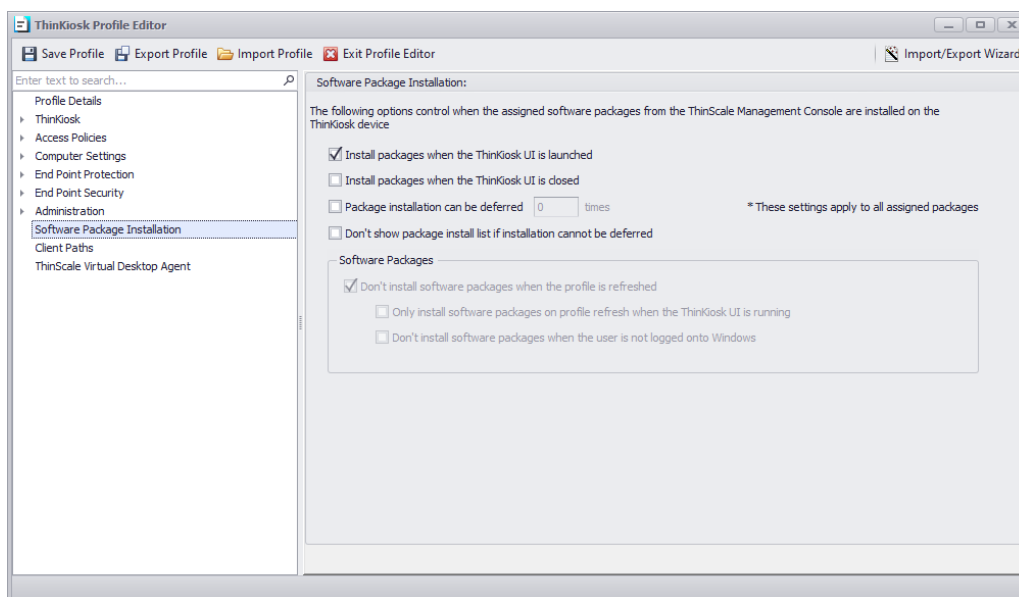
The default email subject.

Read Only in ThinKiosk

If enabled the ThinKiosk user cannot change the default values of “from address”, “to address” or “email subject”.



12. Software Package Installation



The following options will control when software packages will be deployed on the ThinKiosk devices:

Install software packages when the ThinKiosk UI is launched

If enabled, software packages assigned to the folder will be deployed when the ThinKiosk UI is launched.

Install software packages when the ThinKiosk UI is closed

If enabled, software packages assigned to the folder will be deployed when the ThinKiosk UI is closed.

Don't install software packages when the profile is refreshed

If enabled, software packages assigned to the folder won't be installed at a profile refresh.

Only install software packages on profile refreshed when the ThinKiosk UI is running

If enabled, software packages assigned to the folder will be installed at a profile refresh and when the UI is launched.

Don't install software packages when the user is not logged onto Windows

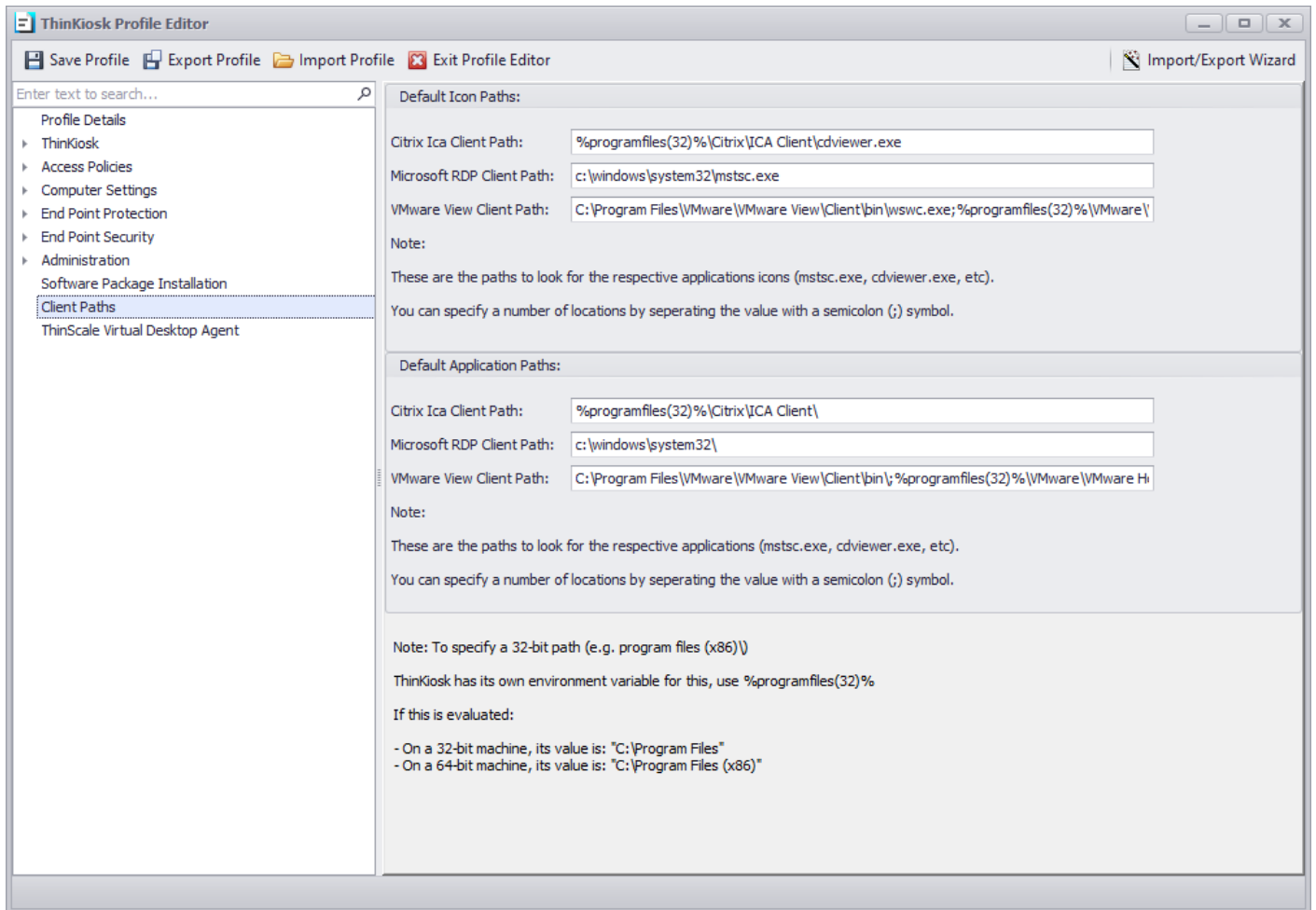
If enabled, software packages assigned to the folder won't be installed when the user is not logged in to the machine.

Package installation can be deferred

Select the number of times the user can defer the software installation.



13. Client Paths



Default Icon Paths:

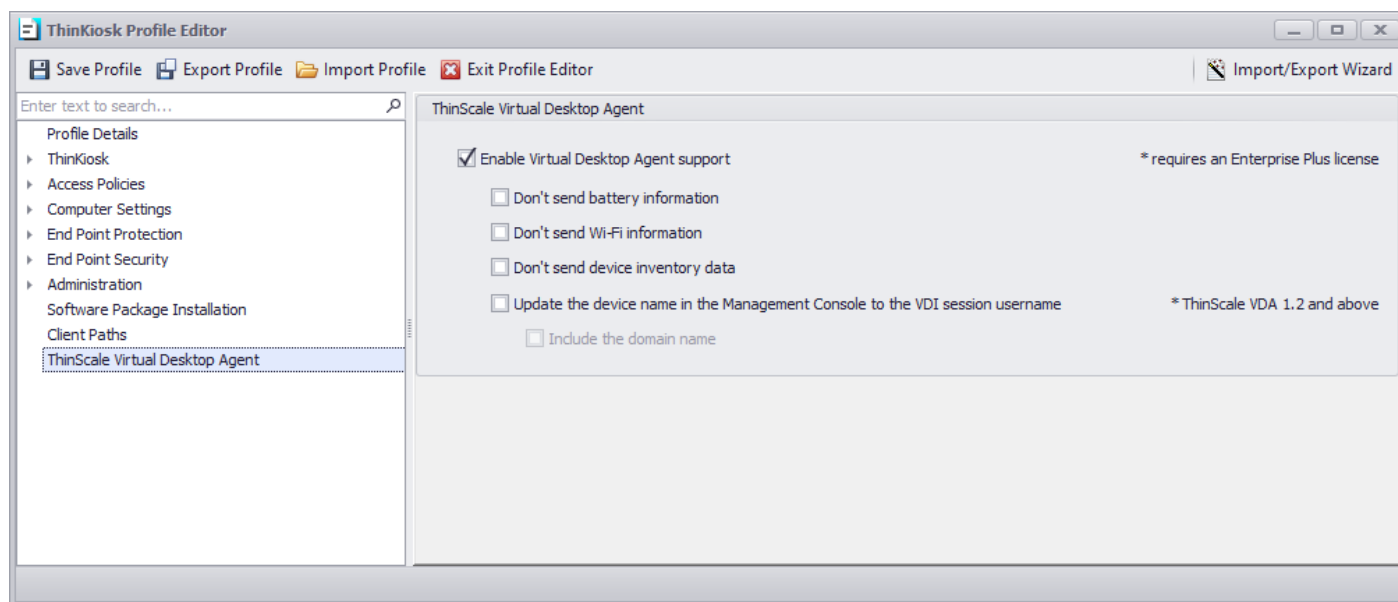
Paths to the client executables are used to extract the icons that will be displayed in the application tab.

Default Application Paths:

Locations where ThinKiosk will look for the installation of the Citrix, Microsoft and VMware clients.



14. ThinScale Virtual Desktop Agent



Enable Virtual Desktop Agent support:

When enabled, the ThinKiosk machine service will send to the VDA agent installed on the VDI server information like battery, Wi-fi and ThinKiosk device inventory data.