



ThinScale Secure Remote Worker Profile Configuration Guide V 7.5



Table of Content

Table of Content	1
1. Secure Remote Worker Profile Overview	4
2. Profile	5
Profile Details	5
3. Secure Remote Worker	6
Secure Remote Worker Mode	6
General	7
4. Appearance	9
General Appearance	9
Language	10
Splash Screen	10
Appearance – Ribbon Bar	11
Ribbon and Status Bar Appearance	11
Appearance - KioskBar	12
General Settings	12
Notification Area	14
Window Control	15
Application Exclusion	15
Appearance – Display	17
5. Applications	19
Applications	19
Tile Appearance	21
Behaviour	21
Applications – VDI Connectors	22
Add StoreFront / RDS / Horizon / AVD (classic)/ AVD Connector	23
Secondary Broker	25
Connector List	26
Citrix Integration Options	27
Microsoft RDS Integration Options	29
VMware Horizon Integration Options	29
Applications – Connector Login	31
Applications – Login Options	33
Legal Notice / MOTD	36



Applications – Workspace Control	37
End of Session Options	38
Applications – LDAP Integration.....	39
Enable LDAP Password Change/Verification integration	39
Applications – Local Applications	41
Local Applications.....	42
Citrix, Microsoft RDS or VMware Horizon connections	43
6. Secure Browser	46
Secure Browser.....	46
General Appearance.....	47
General	48
VDI Controls.....	50
Secure Browser – Web Sites.....	51
Adding / Editing a Site	51
Secure Browser - URL Filtering	53
7. Access Policies.....	56
Network.....	56
Windows Update.....	57
8. Computer Settings.....	58
Local Device Restrictions	58
Ctrl+Alt+Del Screen	60
Computer Settings – Login Script	61
Computer Settings – Logoff Script.....	62
Computer Settings - Session Settings.....	63
Local Volume	63
Computer Settings - Session Security.....	64
Power Options.....	64
Computer Settings - Additional Registry Values	65
Additional Registry Values.....	65
Computer Settings - Proxy Server Settings	67
Computer Settings - Privacy Settings (Win10)	68
Computer Settings - Lock Screen.....	69
9. End Point Protection	70
Windows Security Centre Detection	70
End Point Protection - Windows Security Centre Detection.....	70



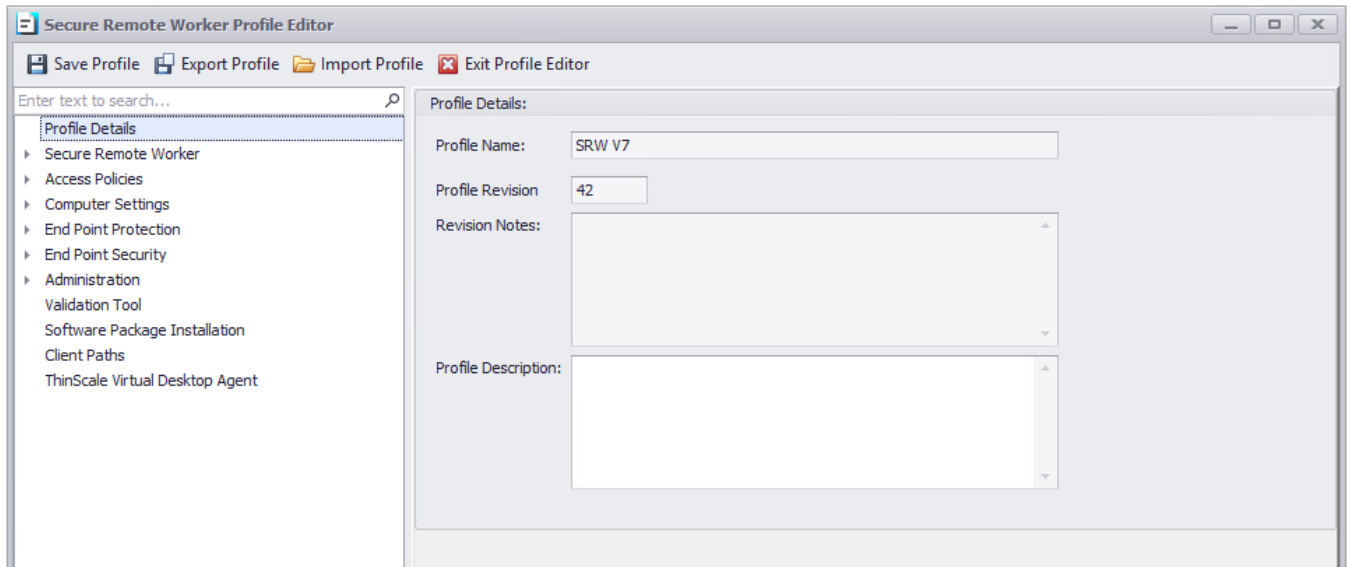
End Point Protection - Windows Patch Management.....	72
End Point Protection - Windows Firewall Control.....	78
Windows Firewall Control	78
10. End Point Security.....	82
End Point Security - Wi-Fi Adapters	83
End Point Security - Virtual Machine Detection.....	84
End Point Security - USB Device Blocking.....	84
End Point Security – Write Filter	84
End Point Security – Dual Persona	85
Enable Dual Persona.....	85
End Point Security – Temporary Storage	87
Enable Temporary Storage	87
End Point Security - Application Execution Prevention.....	89
Enable Application Execution Prevention	89
End Point Security - Application Execution Prevention (Offline)	95
End Point Security - Application Module Protection.....	97
End Point Security – Driver Execution Protection	98
End Point Security - Service Execution Prevention	99
Service Execution Prevention.....	99
Service Execution Prevention - User Notifications.....	101
11. Administration.....	103
Administrator Access.....	103
Administration – Screen Capture	104
SMTP Settings.....	104
Server Details	104
SMTP User Credentials	105
Default Values	105
12. Validation Tool.....	106
13. Software Package Installation	107
14. Client Paths	109
15. ThinScale Virtual Desktop Agent	110

1. Secure Remote Worker Profile Overview

The Secure Remote Worker profile provides all the configurations required for the Secure Remote Worker client.

This profile is JSON based and very easy to modify with the new Secure Remote Worker Profile Editor via the ThinScale Management Console.

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

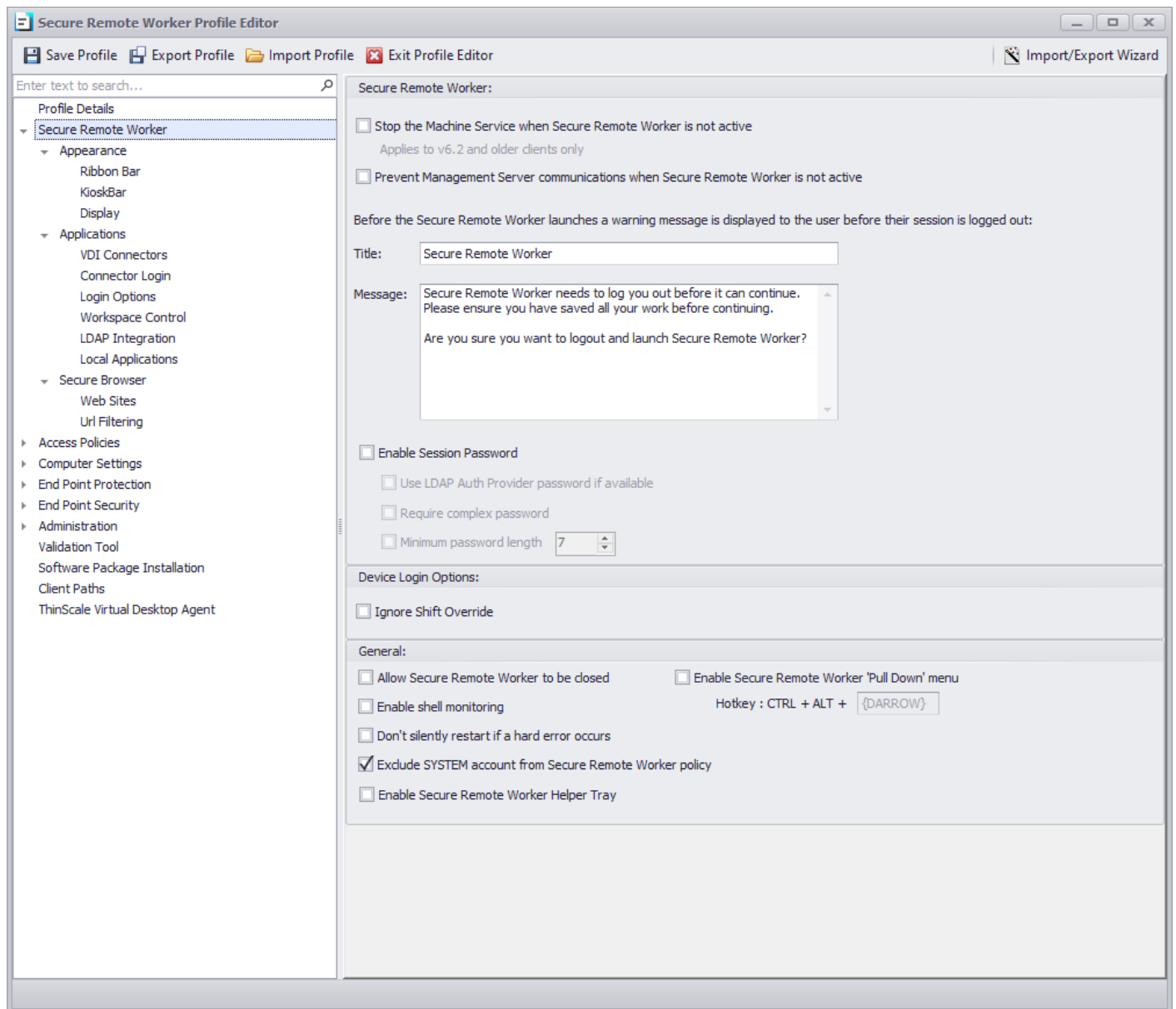
Shows the comments you added when editing a profile.

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. Secure Remote Worker



Secure Remote Worker Mode

Stop the Secure Remote Worker Machine Service when Secure Remote Worker is not active

If enabled, the Secure Remote Worker Machine Service will be stopped if not in Secure Remote Worker mode.

Prevent Management Server communication when Secure Remote Worker is not active

If enabled, communications between clients and the Management Server will be stopped when not in Secure Remote Worker mode.

Enable Session Password

If enabled, SRW users will be able to set up a local password that can be used to lock and unlock the user session

Use LDAP Auth Provider password if available

If enabled, the password used will be the one from the auth provider.

Require complex password

Complex passwords must include at least one of each of lower-case letters, upper-case letters, numbers, and symbols.

Minimum password length

If enabled, the password length must match the specified number.

General

Allow Secure Remote Worker to be closed

If enabled, users will be able to close the Secure Remote Worker UI.

Enable shell monitoring

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

Don't silently restart if a hard error occurs

This option has been retired and is no longer available.

Enable Secure Remote Worker 'Pull Down' menu

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



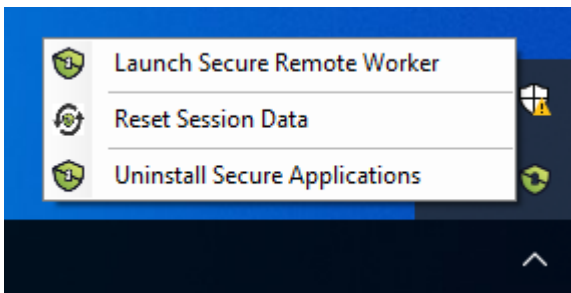
Secure Remote Worker's 'Pull Down' menu can be accessed even when connected to a full-screen remote session allow you access to options available on Secure Remote Worker's ribbon bar.

Exclude SYSTEM account from Secure Remote Worker policy

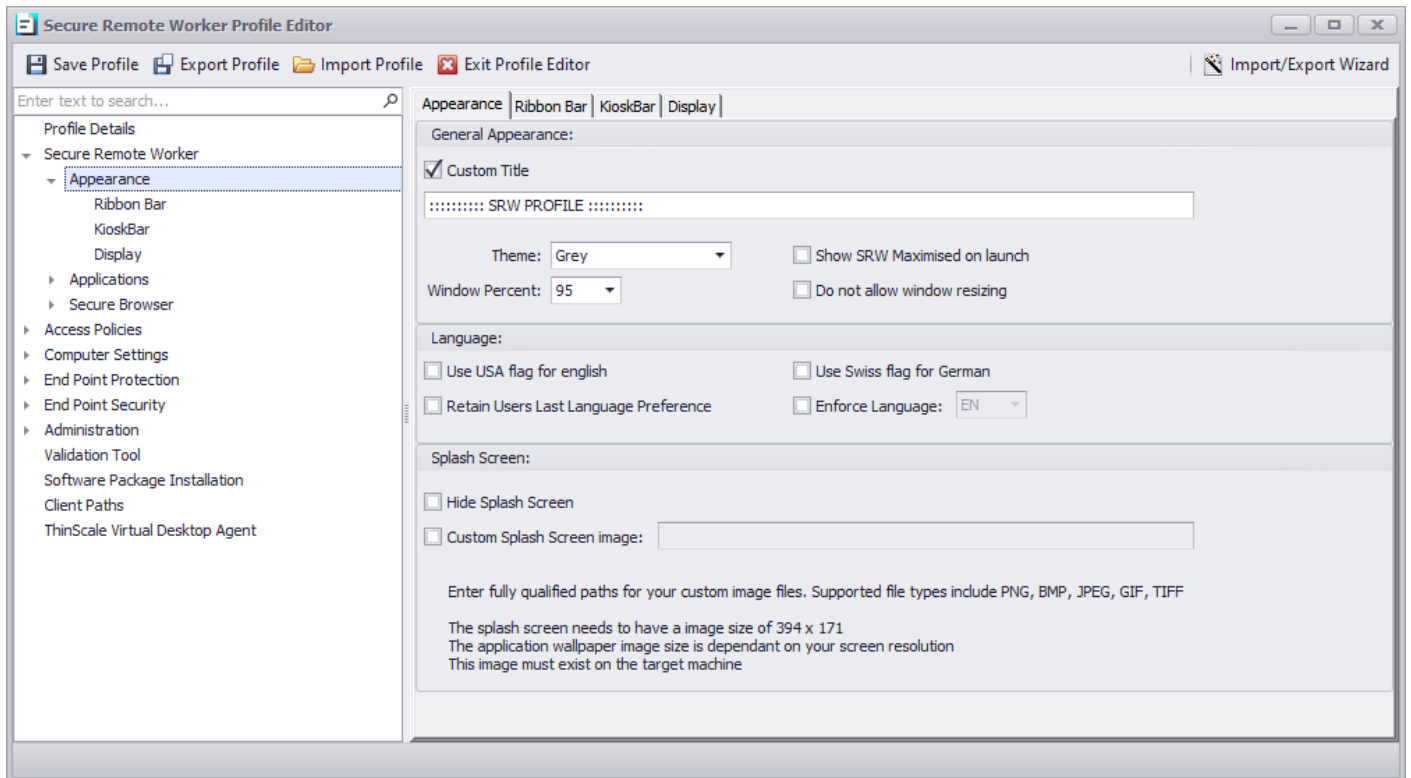
If enabled, an action performed under the SYSTEM account will be allowed to run. Useful when a write filter is installed on the machine.

Enable Secure Remote Worker Helper Tray

If enabled, the SRW tray icon will be displayed inside the user session



4. Appearance



General Appearance

Custom Title

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

Theme

Sets the theme Secure Remote Worker UI will use.

Show Secure Remote Worker Maximised on launch

If enabled, the Secure Remote Worker UI will launch maximised and will override the *Window Percent* setting.

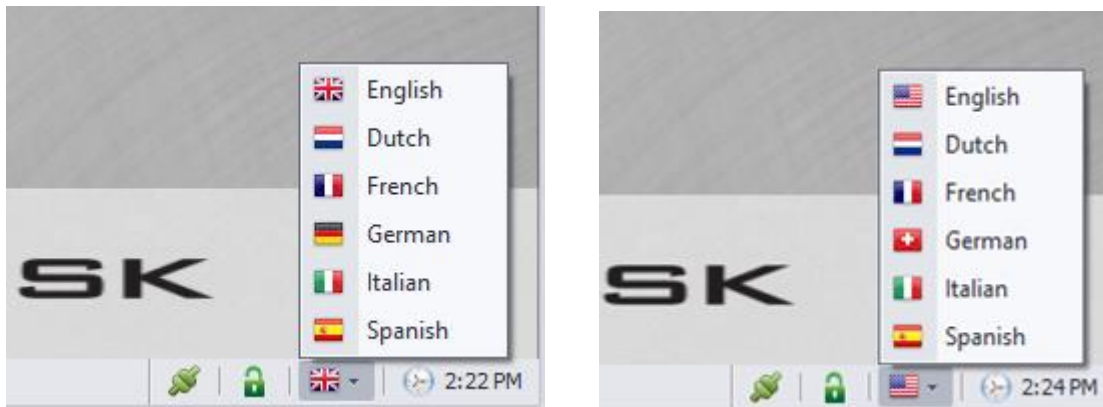
Window Percent

Set's the size of the Secure Remote Worker UI

Do not allow window resizing

When enabled the Secure Remote Worker 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

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

Enforce Language

Forces Secure Remote Worker to use the selected language.

Splash Screen

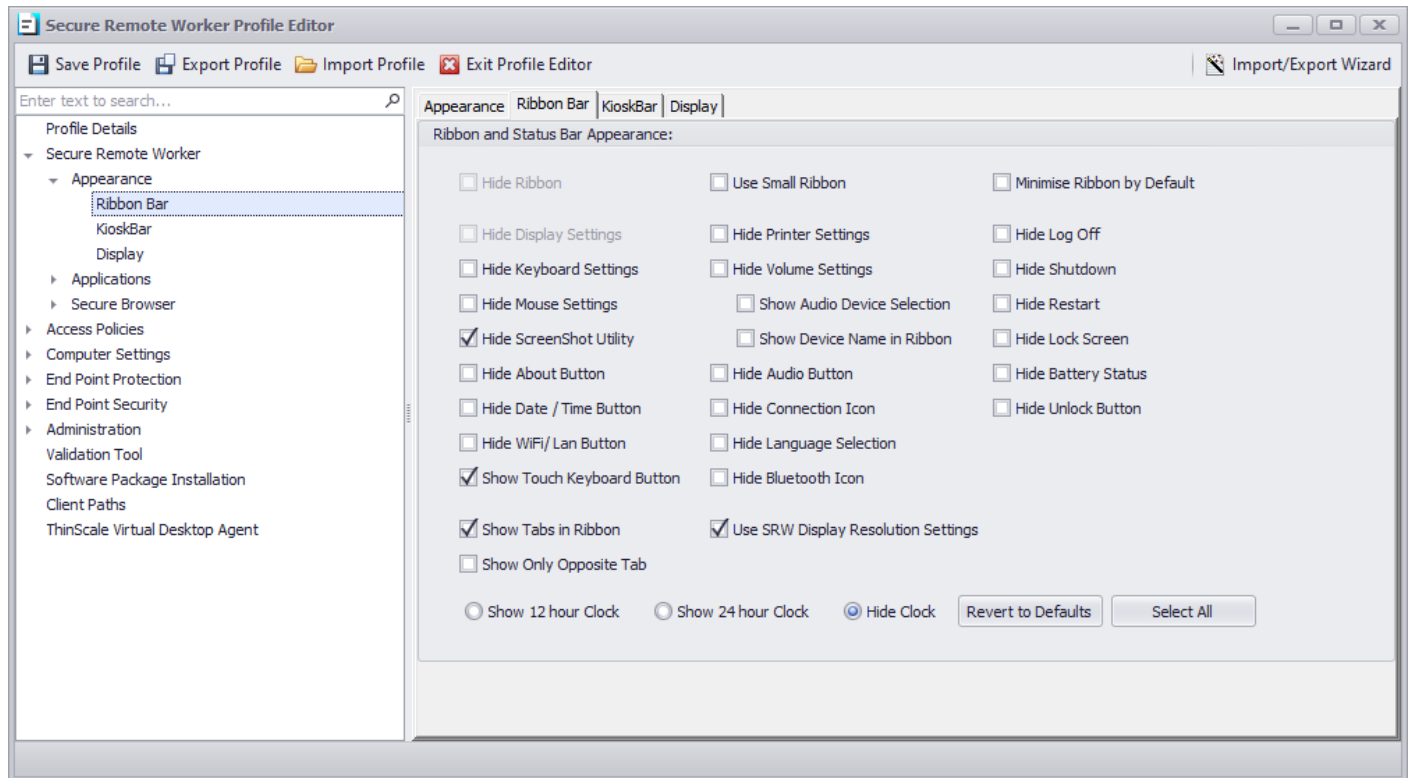
Hide Splash Screen

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 Secure Remote Worker Taskbar for the Secure Remote Worker client.

Use Secure Remote Worker Display Resolution Settings

If enabled, Secure Remote Worker 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 Secure Remote Worker is the main shell, or a timeout error will be shown.

Revert to Default

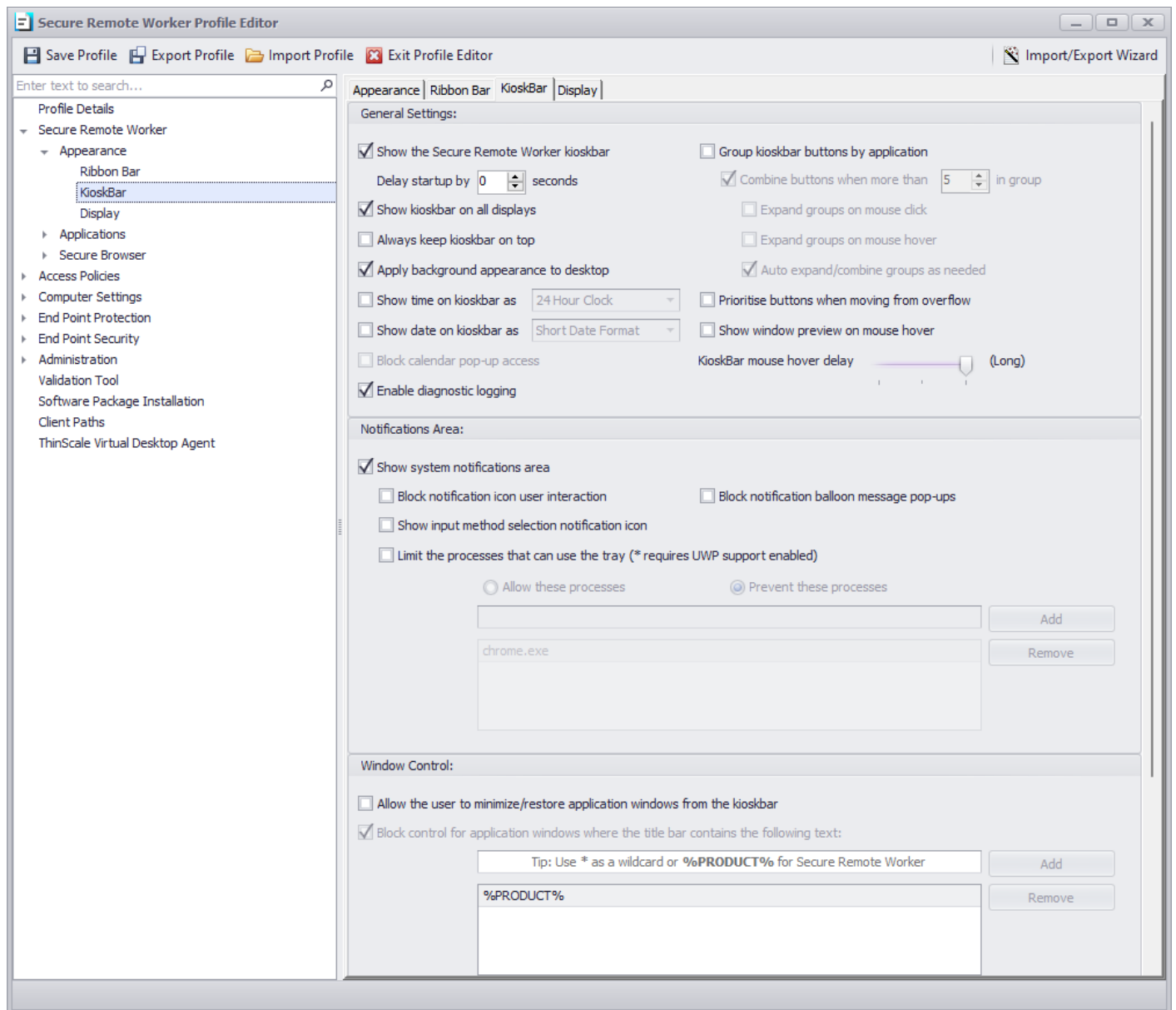
If clicked will reset all the settings to the default one.

Select All

If clicked will select all the options at once.

Appearance - KioskBar

General Settings



Show Secure Remote Worker kioskbar

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

Delay startup by

If enabled, Secure Remote Worker 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 Secure Remote Worker.

Show the KioskBar on all displays

If enabled, the Secure Remote Worker 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

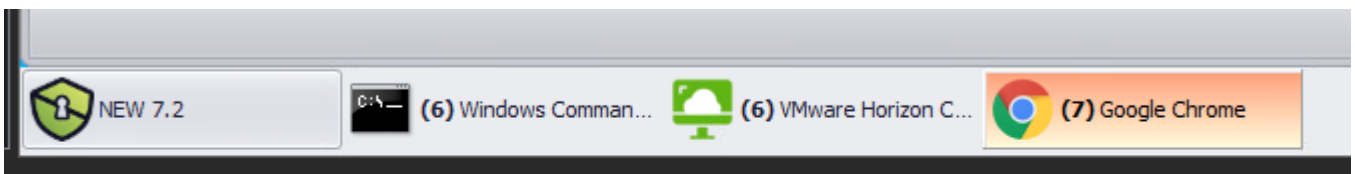
If enabled, a short or long date format will be displayed on the kioskbar.

Block calendar pop-up access

If enabled, the calendar pop-up will be denied.

Group kioskbar button by application

If enabled, the new SRW 7.2 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

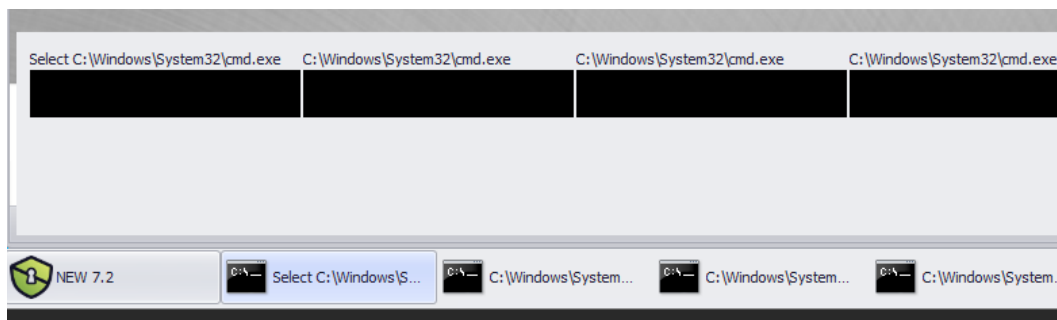
If enabled, groups will be expanded based on the space left on the taskbar

Prioritise buttons when moving from the overflow

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

Show window preview on mouse hover

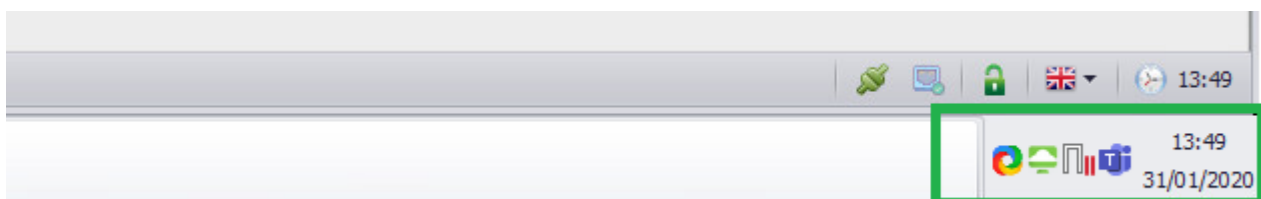
If enabled, applications preview will be displayed on mouse hover



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.



The screenshot shows a user interface for managing application exclusions. It features a text input field at the top with a placeholder tip: "Tip: Use * as a wildcard or %PRODUCT% for ThinkKiosk". Below the input field is a large, empty rectangular box for listing applications. To the right of the input field and the list box are two buttons: "Add" and "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

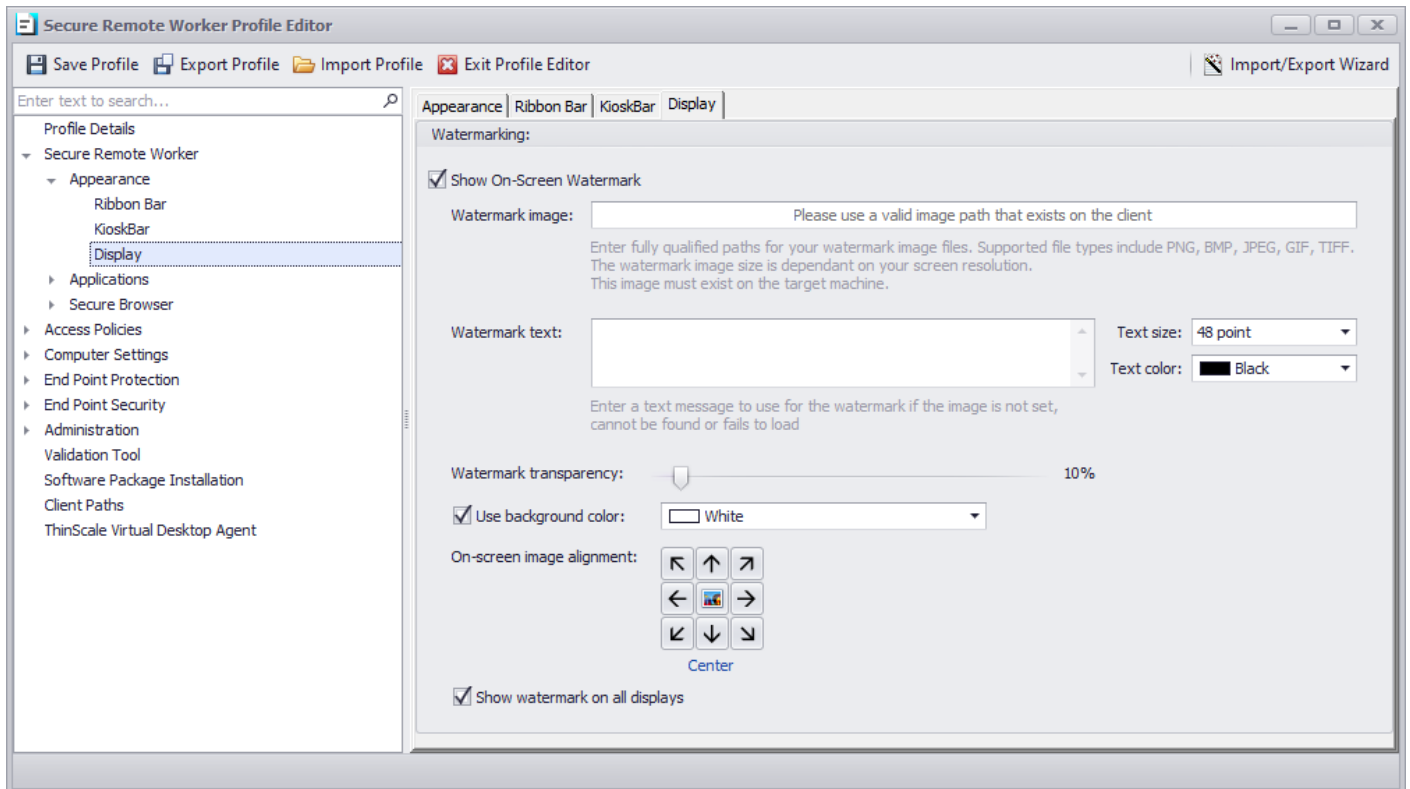
*notepad

%PRODUCT%

Add

Remove

Appearance – Display

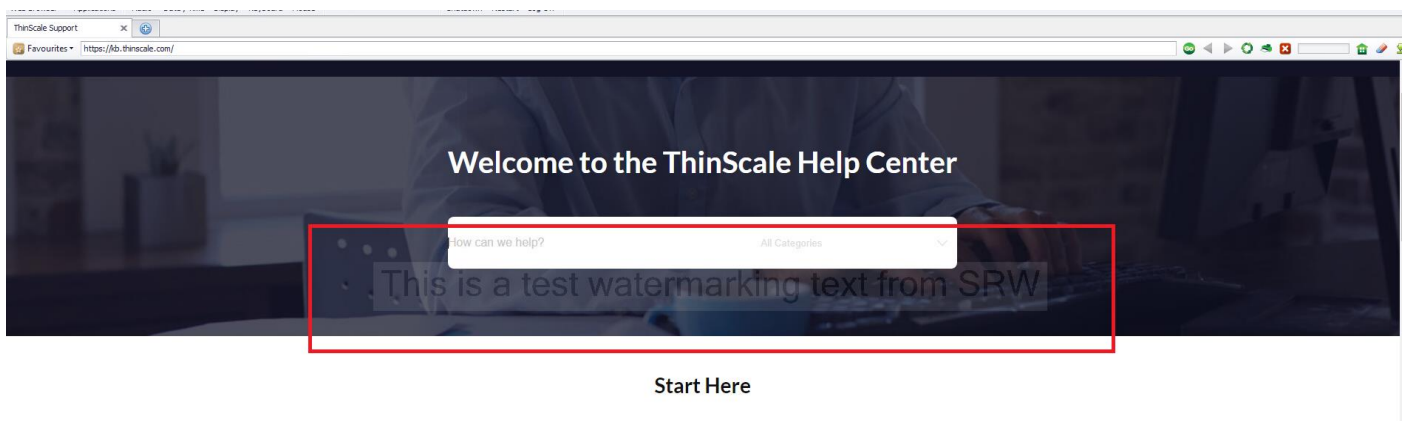


Watermark Image

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 SRW desktop.

Watermark transparency

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

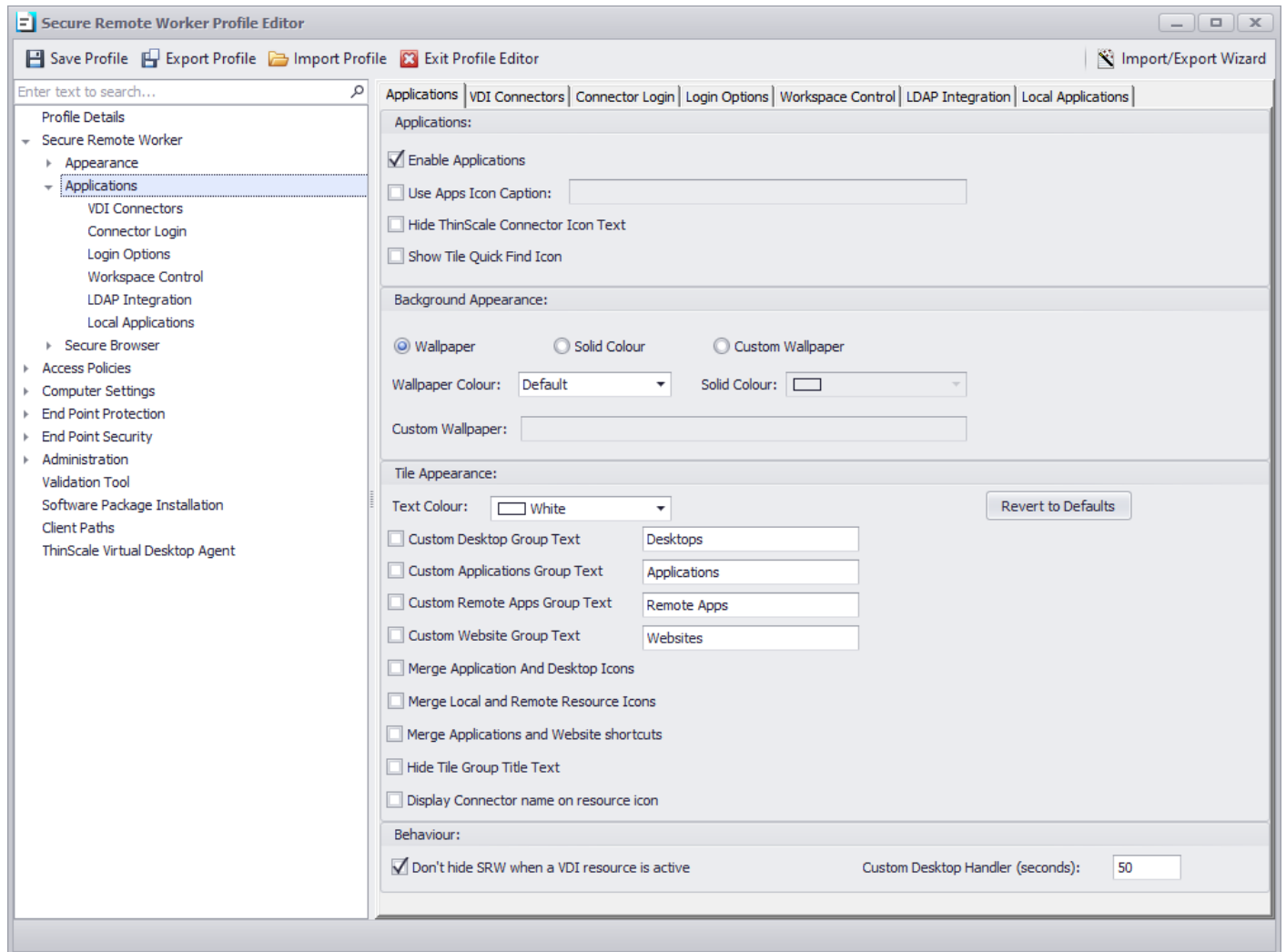
On-screen image alignment

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

Show watermark on all display

It enabled, the watermarking image/text overlay will be displayed to all monitors, otherwise only on the

5. Applications



Applications

Enable Application

If enabled, the application tab inside Secure Remote Worker Desktop will be shown.

Use Apps icon caption

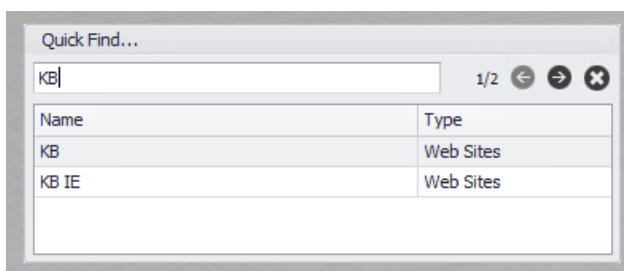
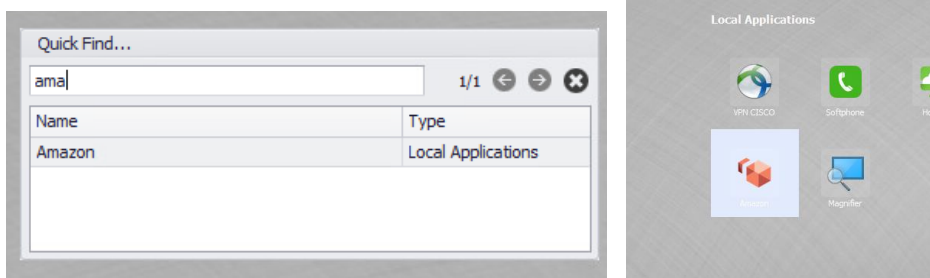
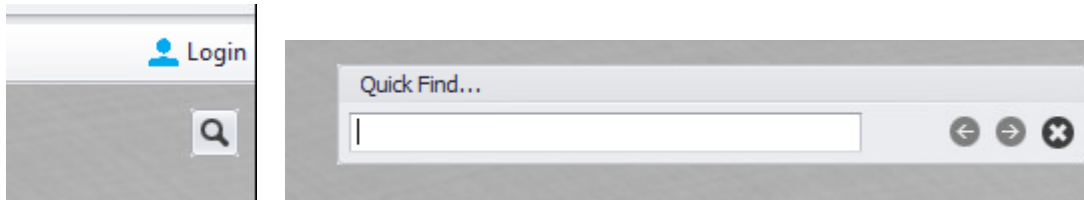
Provides a caption to use for the applications tab icon.

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 SRW 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 Secure Remote Worker.

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 the 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 Secure Remote Worker when a VDI resource is active

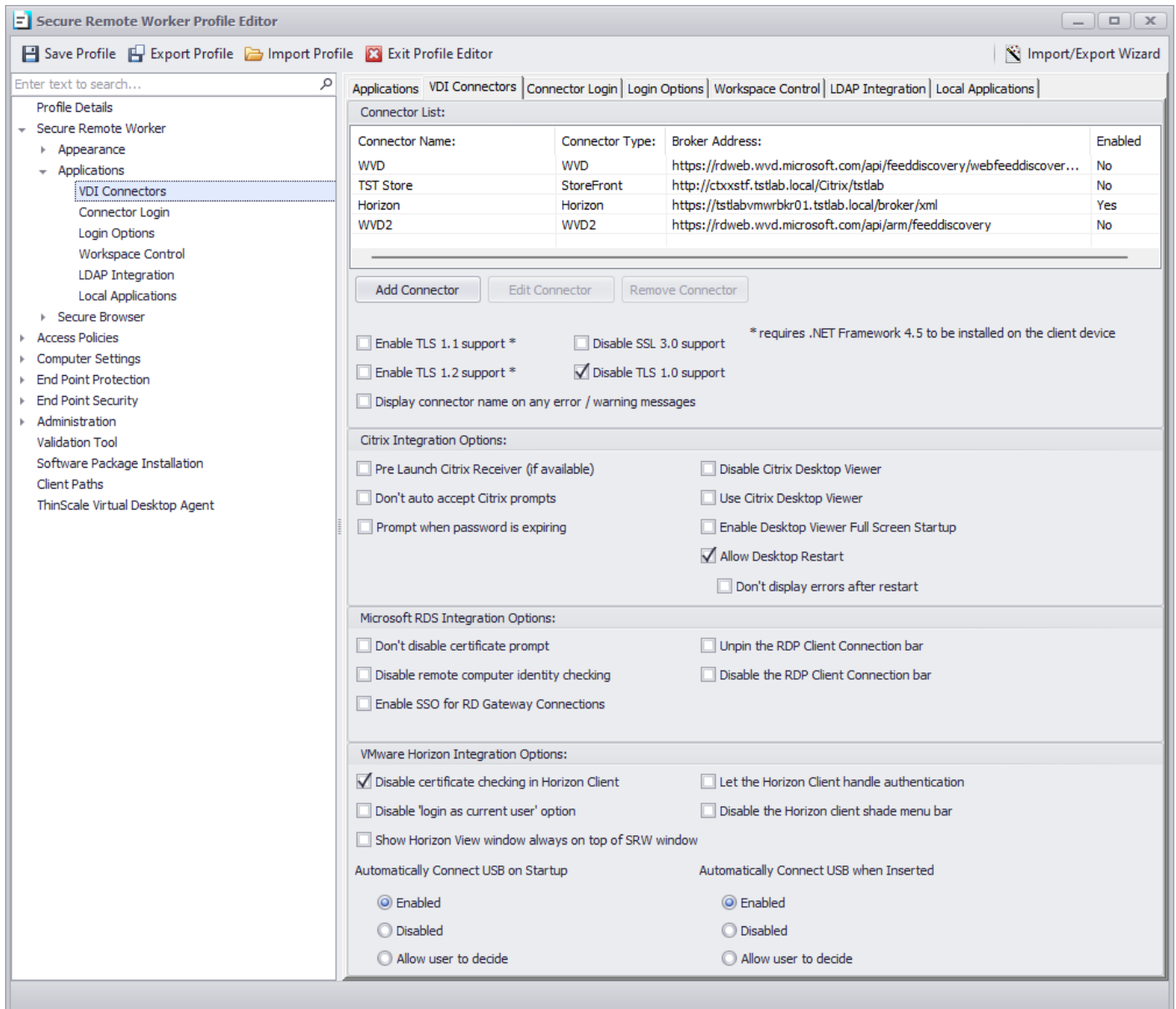
If enabled Secure Remote Worker will remain open in the background while in the foreground your VDI session is open.

Note: recommended if users want to switch between VDI session and Secure Remote Worker desktop.

Custom Desktop Handler

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

Applications – VDI Connectors



The screenshot shows the 'Secure Remote Worker Profile Editor' window with the 'VDI Connectors' tab selected. The left sidebar lists various configuration categories, with 'VDI Connectors' highlighted. The main panel displays a table of configured connectors and several integration options.

Connector List:

Connector Name:	Connector Type:	Broker Address:	Enabled
WVD	WVD	https://rdweb.wvd.microsoft.com/api/feeddiscovery/webfeeddiscover...	No
TST Store	StoreFront	http://cbxstf.tstlab.local/Citrix/tstlab	No
Horizon	Horizon	https://tstlabvmwrbr01.tstlab.local/broker/xml	Yes
WVD2	WVD2	https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery	No

Buttons: Add Connector, Edit Connector, Remove Connector

Integration Options:

- ☐ 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
- ☐ Don't auto accept Citrix prompts ☐ Use Citrix Desktop Viewer
- ☐ Prompt when password is expiring ☐ Enable Desktop Viewer Full Screen Startup
- ☒ 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 SRW window

Automatically Connect USB on Startup:

- ☒ Enabled
- ☐ Disabled
- ☐ Allow user to decide

Automatically Connect USB when Inserted:

- ☒ Enabled
- ☐ Disabled
- ☐ Allow user to decide

Add StoreFront / RDS / Horizon / AVD (classic)/ AVD Connector

Add StoreFront Connector

☐ 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)

Add Cancel

Add Windows Virtual Desktop Connector

☒ Connector Enabled

Primary Broker

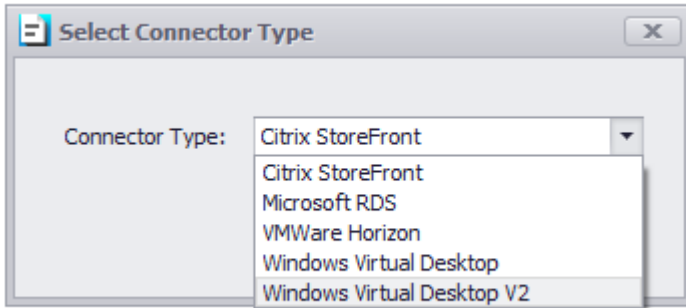
Connector Name:

☐ Display Desktop Resources ☐ Display Remote Applications

☐ Filter Resources

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

Add Cancel



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, 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.

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 second 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.

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 URLs are not contactable

A semicolon-delimited list of URLs' Secure Remote Worker will try to contact. If any of the URLs in the list are not contactable then Secure Remote Worker 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 7.2 support

Enables support for the TLS 7.2 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, Secure Remote Worker 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.

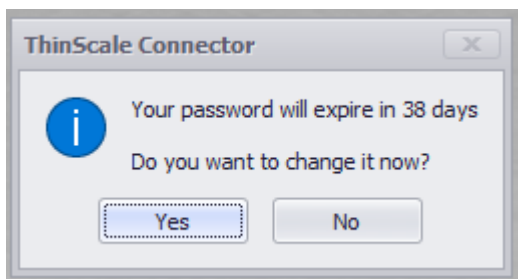
Note: Domain pass-through must be enabled in the "Manage Authentication Methods" in your StoreFront.

Don't auto accept Citrix prompts

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

Prompt when the 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 Startup

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 SRW 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 the '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

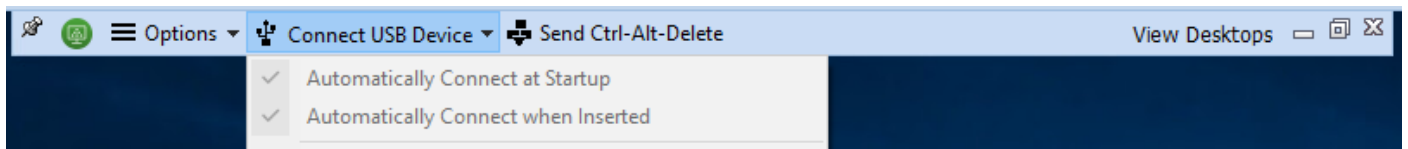
If enabled, Secure Remote Worker will disable Horizon's client 'share menu bar'.

Show Horizon View window always on top of Secure Remote Worker window

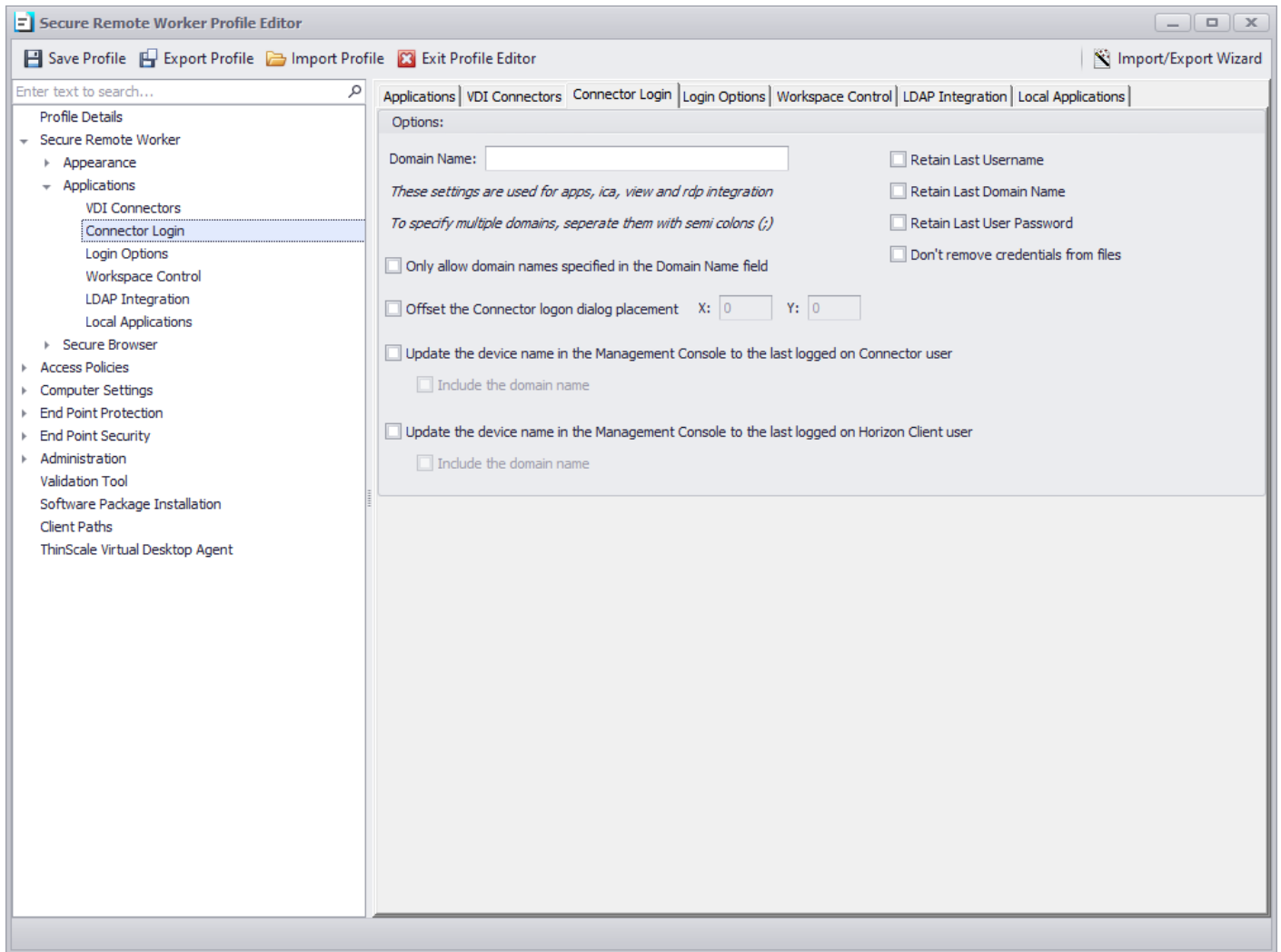
If enabled, the Horizon View will always be opened on top of the Secure Remote Worker window.

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

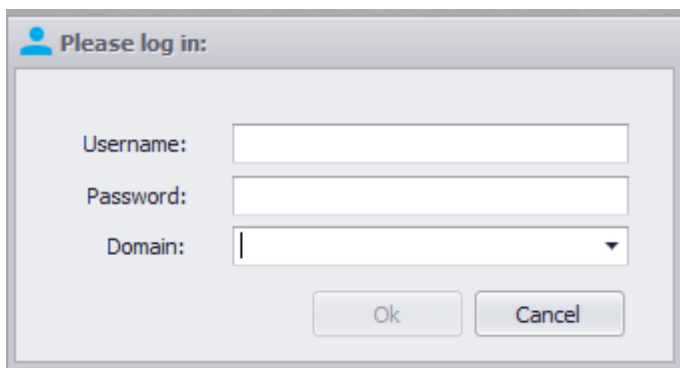


Applications – Connector Login



Domain Name

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



Retain 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 Secure Remote Worker profile.

Offset the connector login dialogue 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

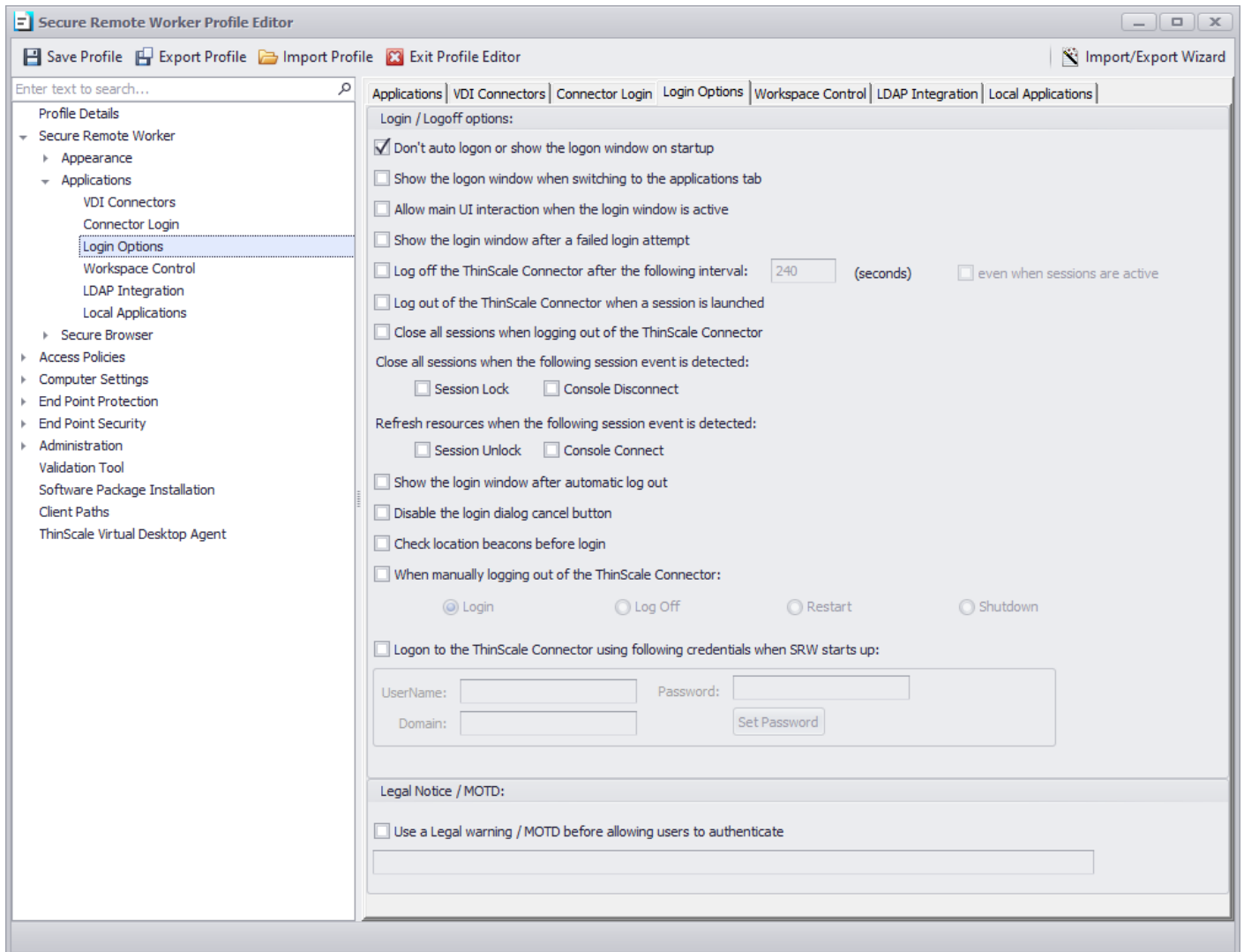
When enabled, the device name inside the Management Console will be renamed as the last connected user using the Thin Scale connector. **

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. **

****Secure Remote Worker 6.0 required**

Applications – Login Options



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

If enabled, Secure Remote Worker will not automatically show the ThinScale Connector Login dialog when Secure Remote Worker starts.

Show the logon window when switching to the applications tab

If enabled, Secure Remote Worker 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 Secure Remote Worker 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, Secure Remote Worker 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, Secure Remote Worker 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 Secure Remote Worker will close all the open sessions.

Refresh resources when the following event is detected

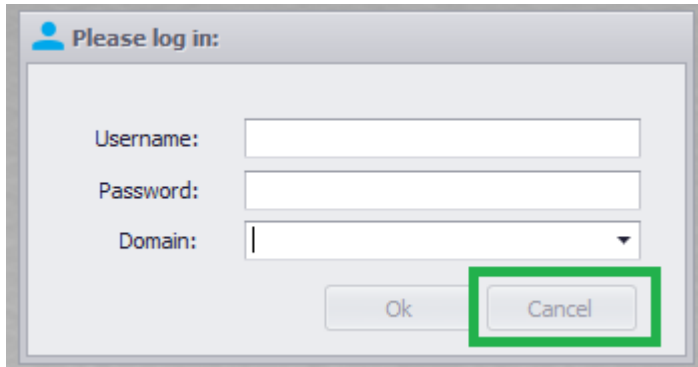
When the Windows machine is Unlocked, or the console is re Connected Secure Remote Worker will refresh all the open sessions.

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.



Check location beacons before login

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

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 Secure Remote Worker starts up

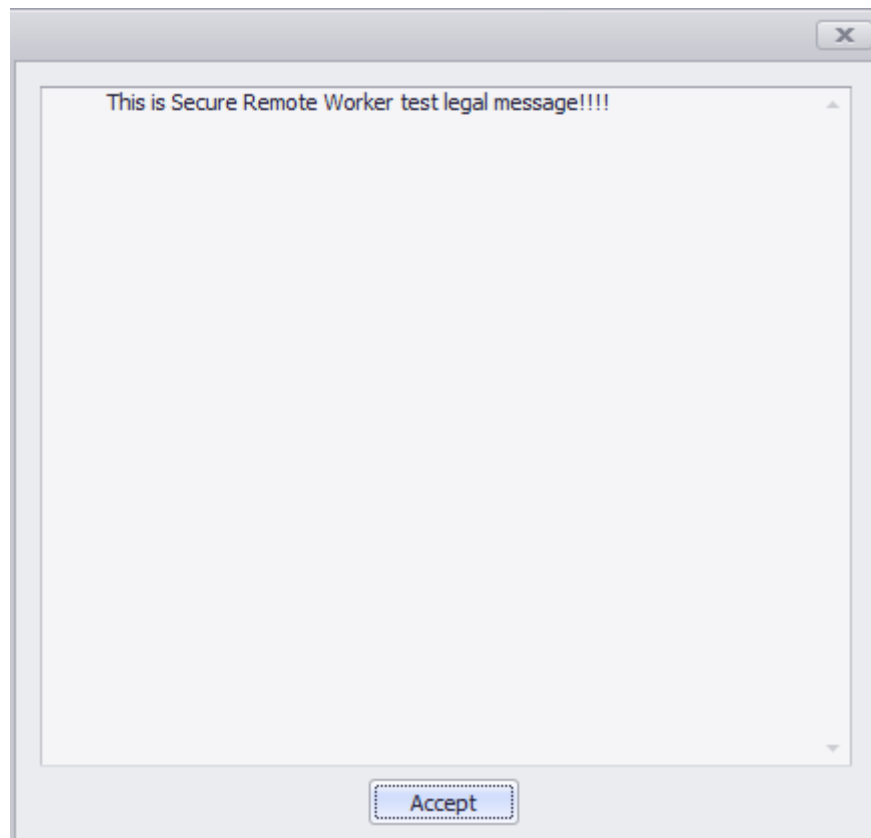
When enabled, Secure Remote Worker will use the supplied credentials to automatically log on to the Connector at startup.

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

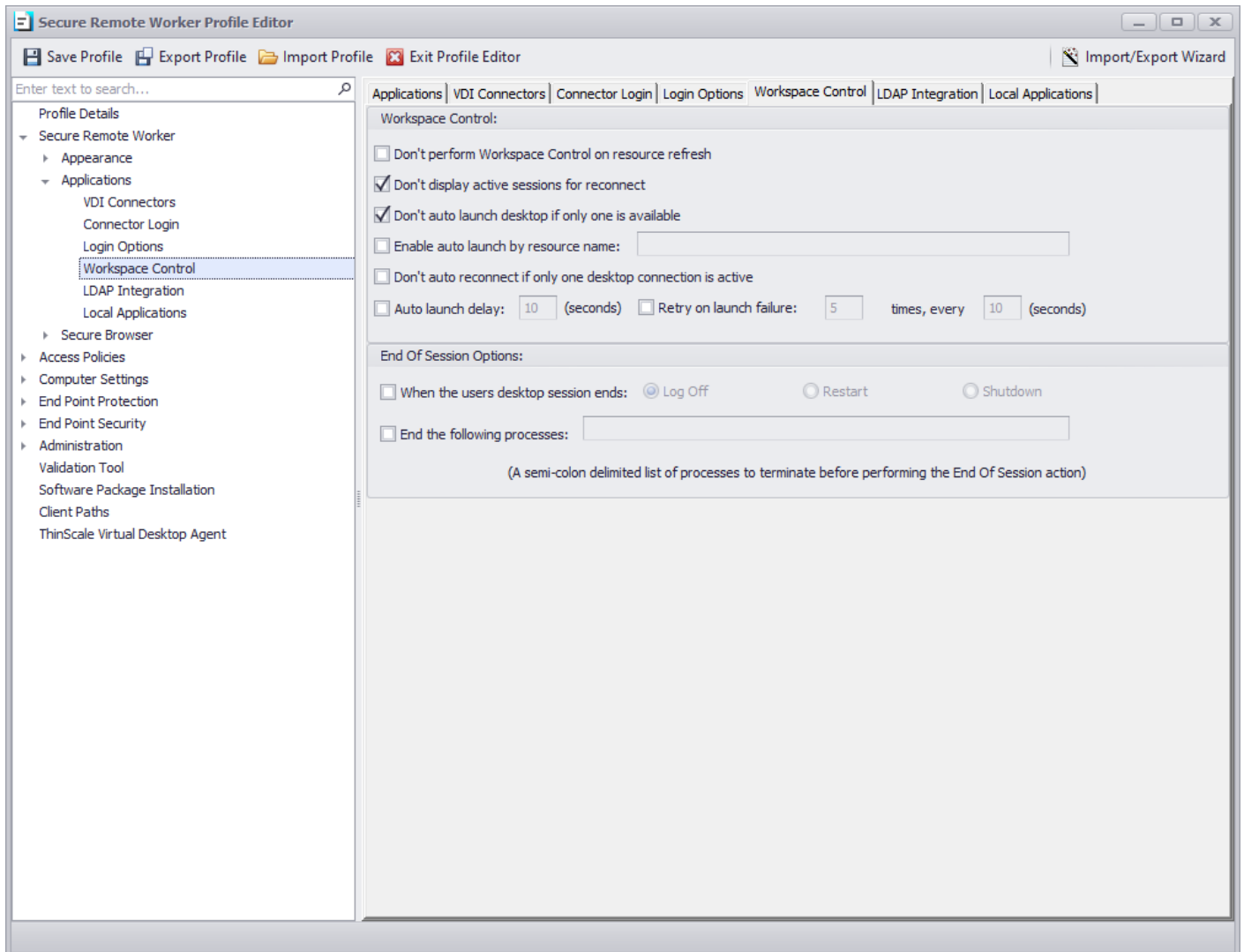
Legal Notice / MOTD

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 reconnecting

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, Secure Remote Worker 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, Secure Remote Worker 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 Secure Remote Worker 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 Secure Remote Worker 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

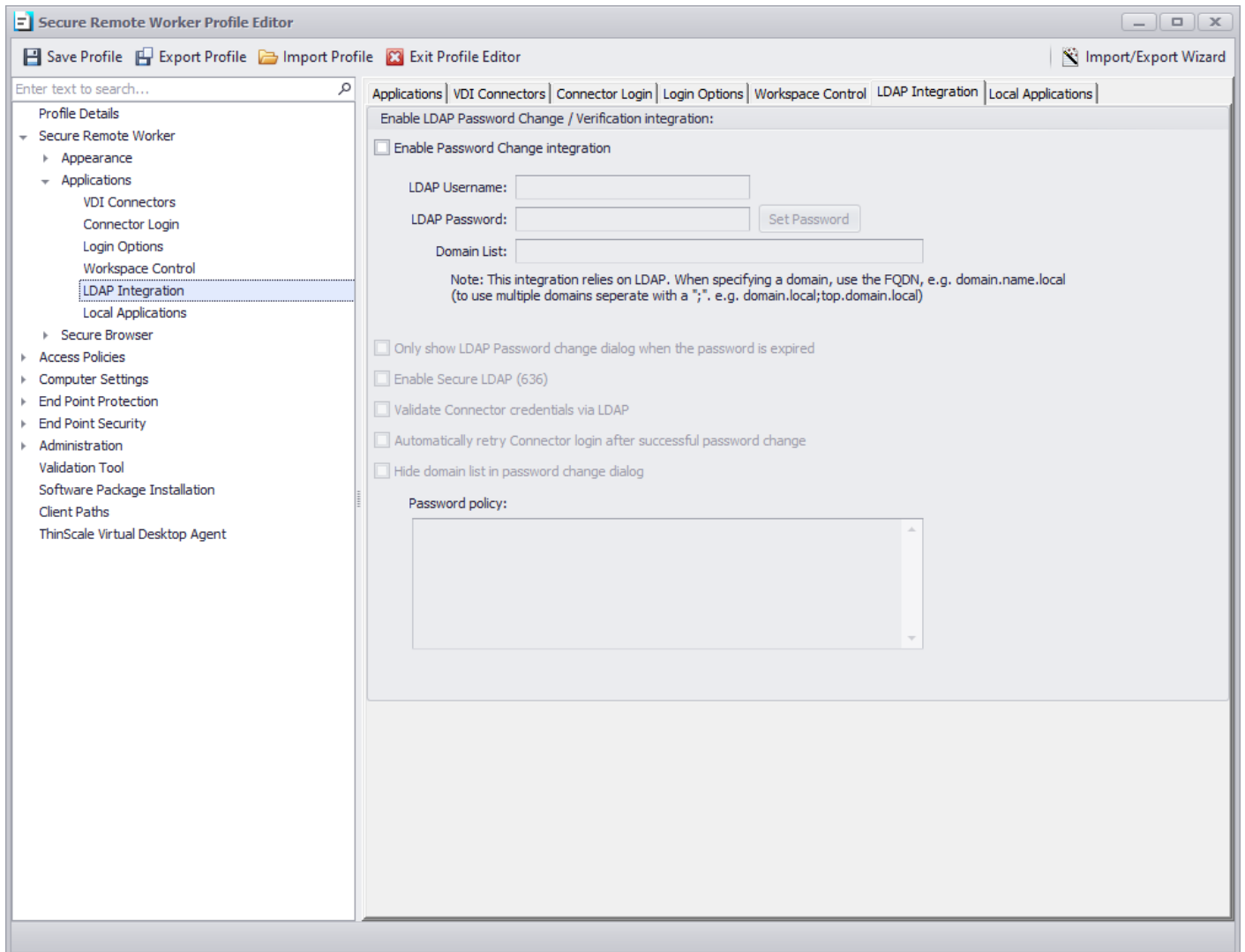
When the user's desktop session ends

When Secure Remote Worker 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 Secure Remote Worker will terminate before performing the configured end of session action.

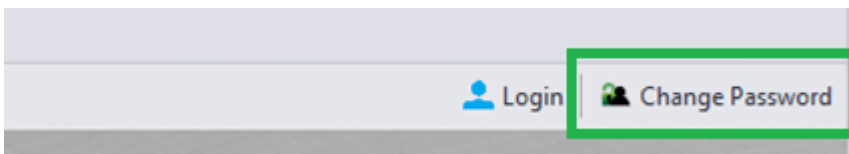
Applications – LDAP Integration



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.

Only show LDAP Password change dialog when the password is expired

If enabled, the "Change Password" button won't be shown to the user.

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. Secure Remote Worker will automatically retry the Connector login using changed credentials.

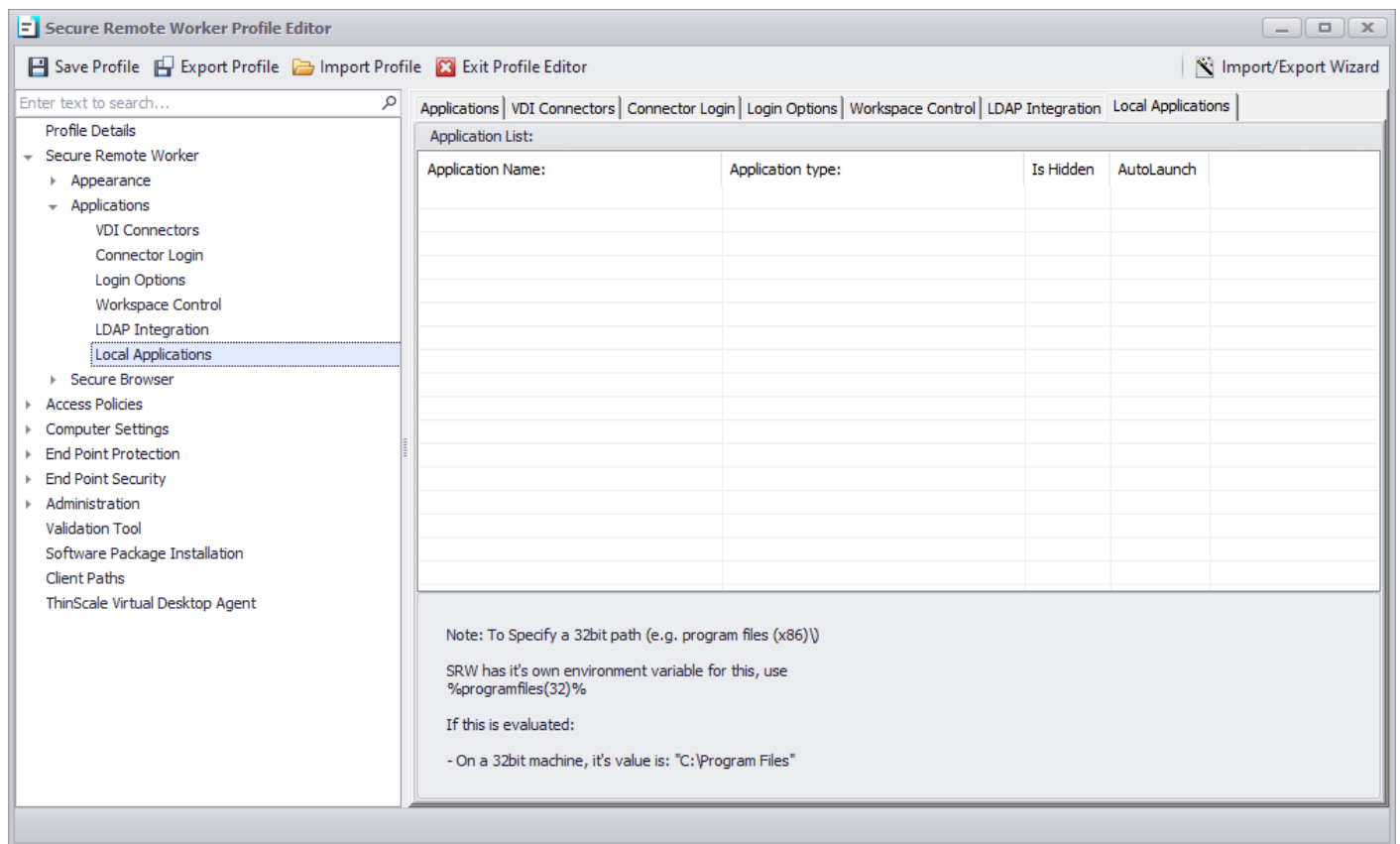
Hide domain list in password change dialog

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.

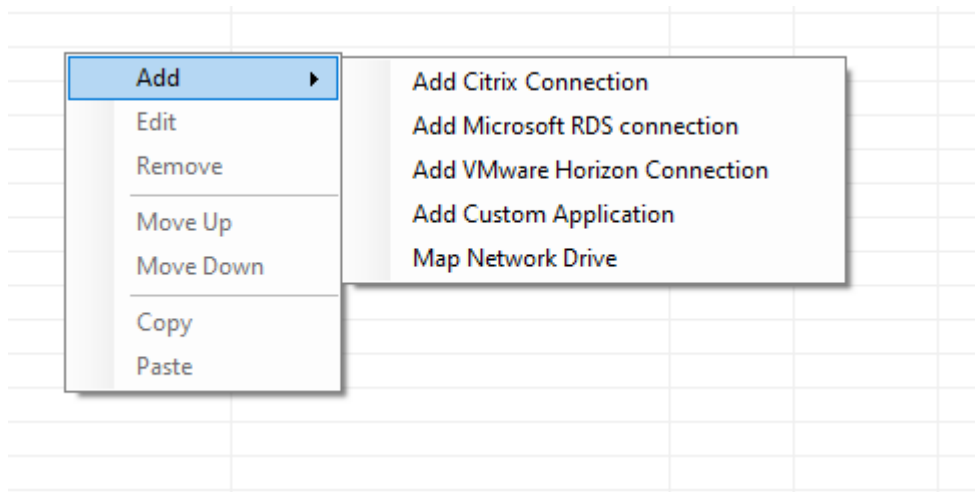
Applications – Local Applications



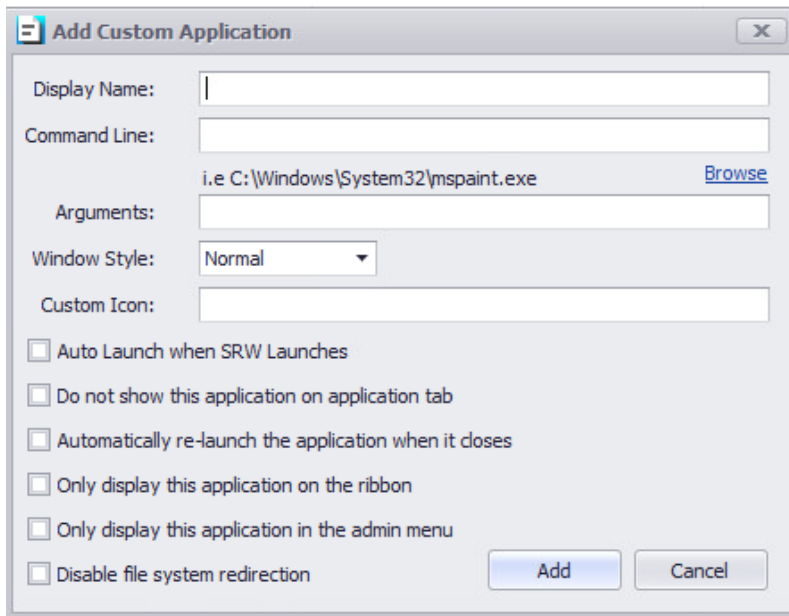
Application List

The list of local applications is available in the 'Applications Tab' of Secure Remote Worker.

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



Add Custom Application

Display Name:

Command Line: [Browse](#)

Arguments:

Window Style:

Custom Icon:

☐ Auto Launch when SRW 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

Display Name

The name of the applications will appear on the Secure Remote Worker 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 Secure Remote Worker Launches

The application will be launched when Secure Remote Worker 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 Secure Remote Worker application tab.

This can be useful when you want to configure an application to run when Secure Remote Worker 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 on the ribbon

The application will not be visible in the Secure Remote Worker applications tab but only on the 'Ribbon Bar'.

Only display this application in the admin menu

The application will not be visible in the Secure Remote Worker applications tab but only on the 'Admin' menu when Secure Remote Worker is unlocked.

Citrix, Microsoft RDS or VMware Horizon connections

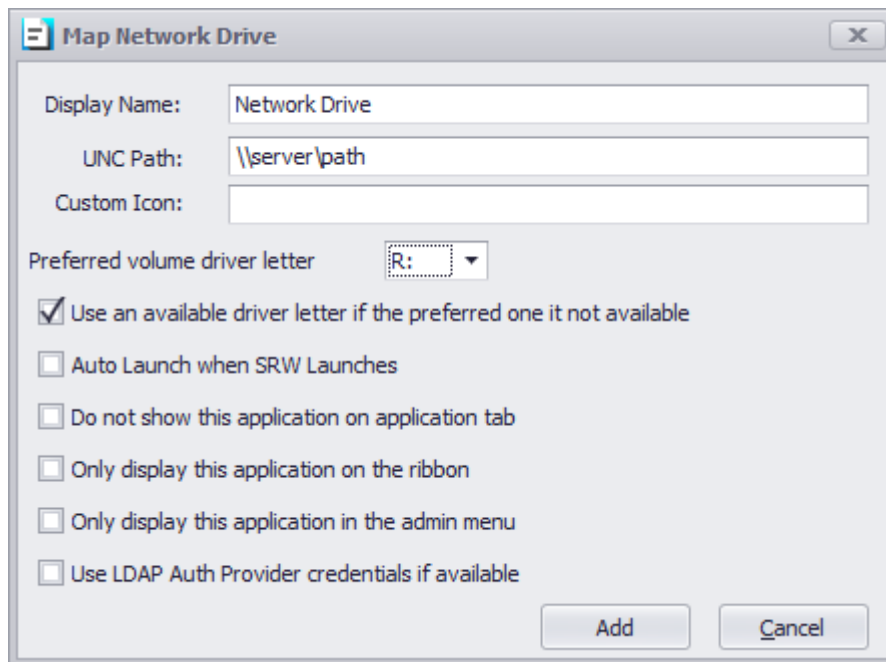
Display Name

The name of the applications will appear on the Secure Remote Worker application tab.

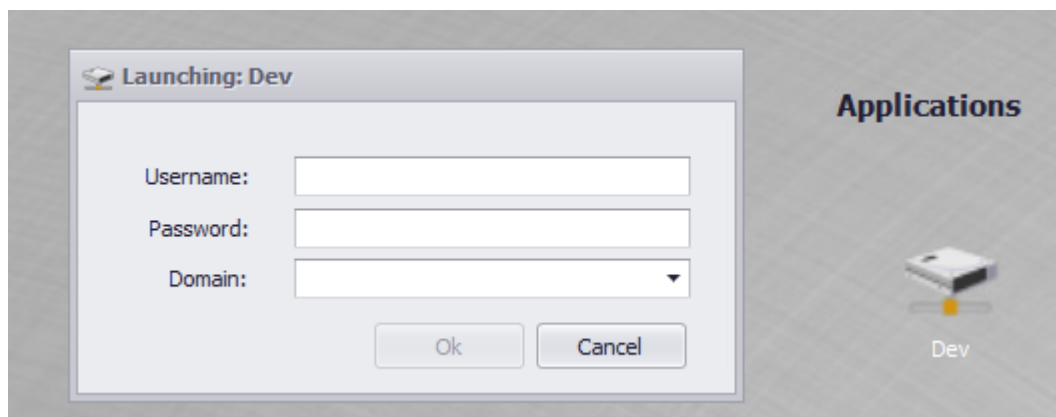
File contents

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 also available from Computer Settings Tab



Display Name

The name of the network drive will appear on the Secure Remote Worker application tab.

UNC Path

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

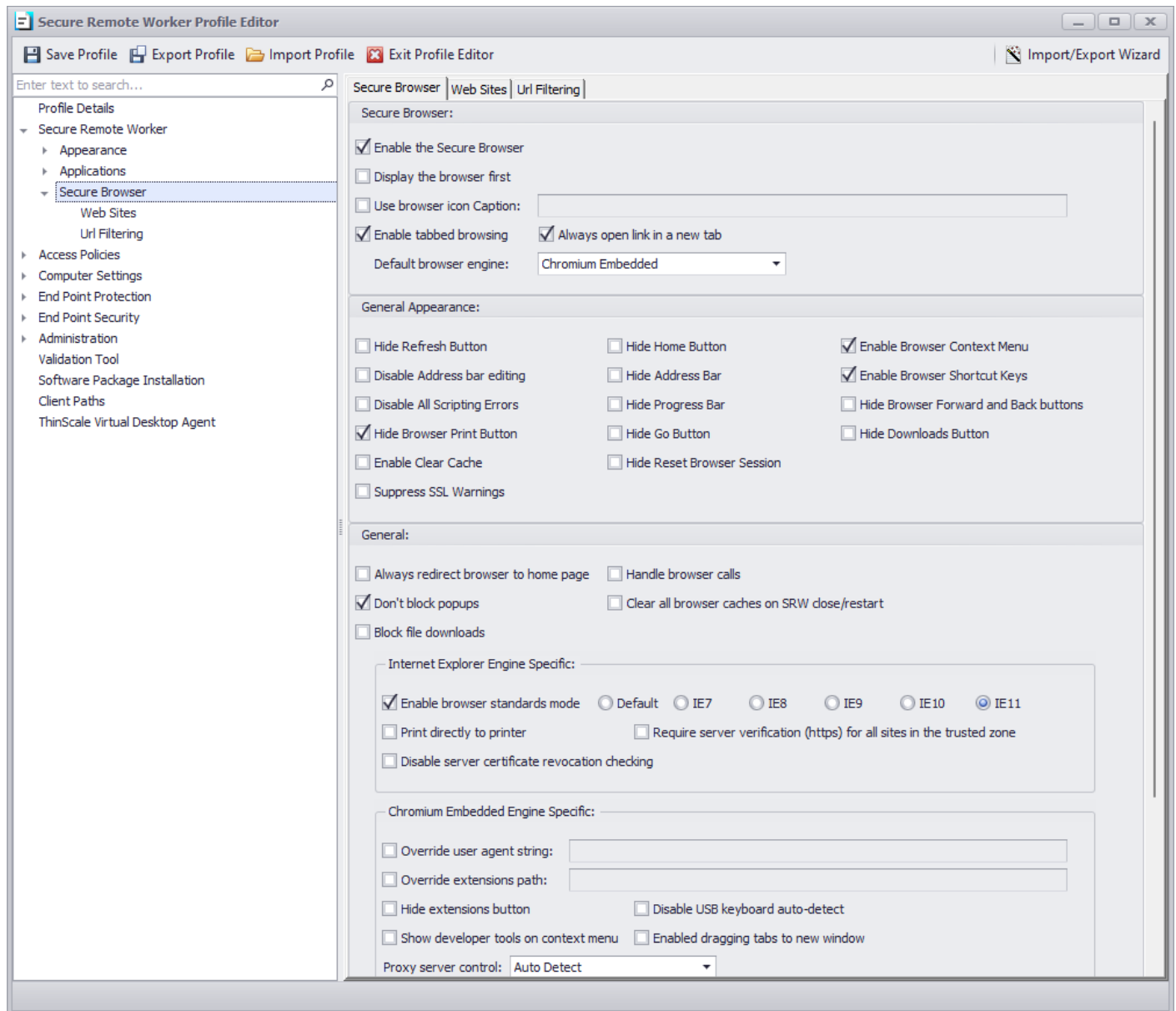
Auto Launch when SRW Launches

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

Use LDAP Auth Provider credentials if available

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

6. Secure Browser



Secure Browser

Enable the Secure Browser

If enabled will show the browser tab inside ThinKiosk Desktop.

Display the Browser first

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

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

The diverse options in this section configure what browser functionality is available to the ThinKiosk client.

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 the 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 a 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)

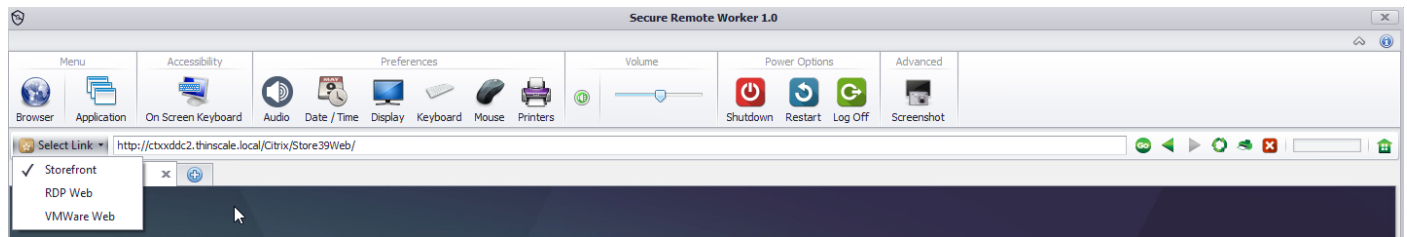
Fixes certain IE rendering problems when using Citrix VDI in a Box.

Manual Logoff redirect

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

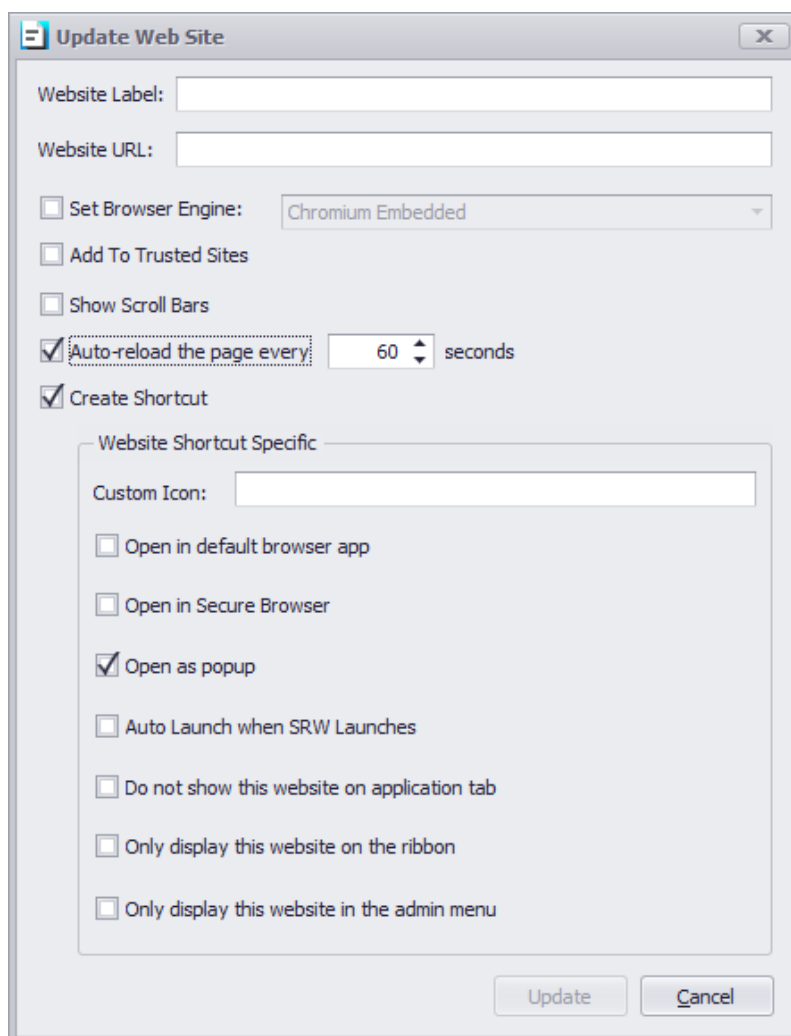
Secure Browser – Web Sites

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 Secure Remote Worker 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 the page

If enabled, the page will reload every X seconds

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 SRW browser

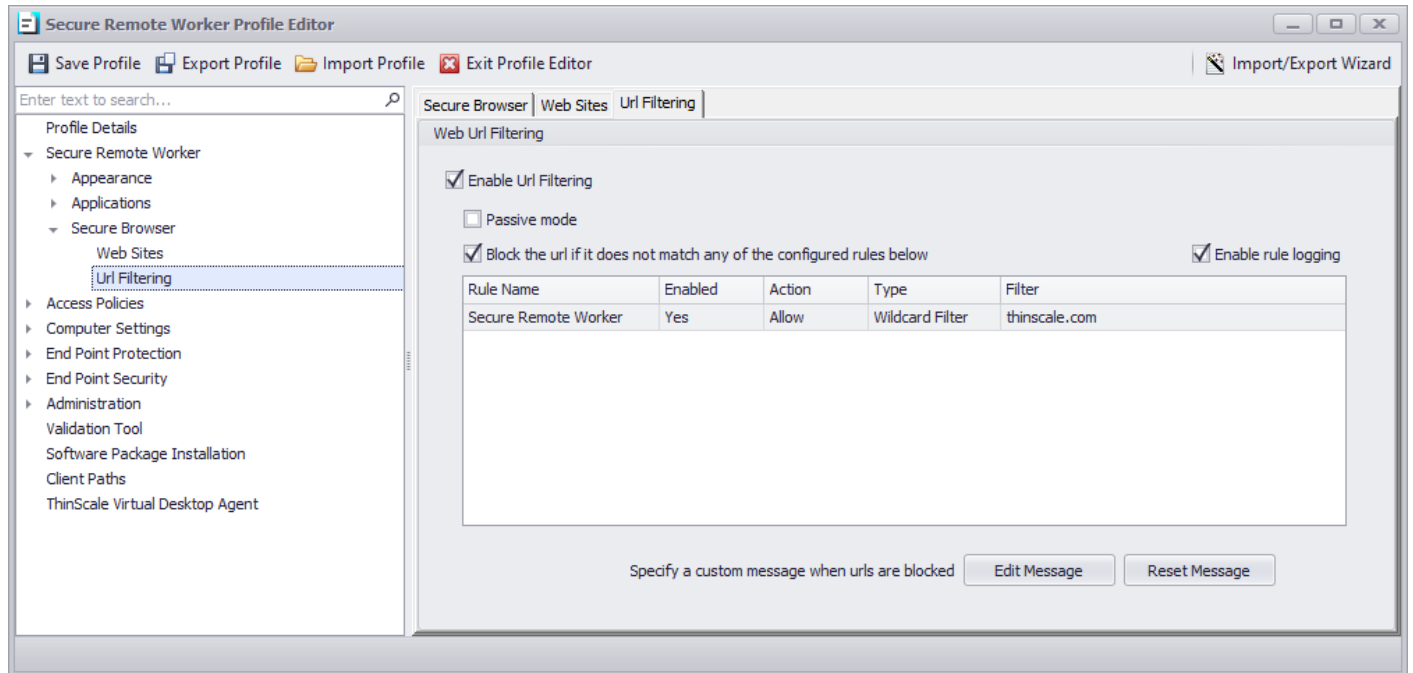
Open as popup

If enabled, the link will open using a popup browser

Auto Launch when SRW Launches

If enabled, the link will open when SRW launches

Secure Browser - URL Filtering



Enable URL Filtering

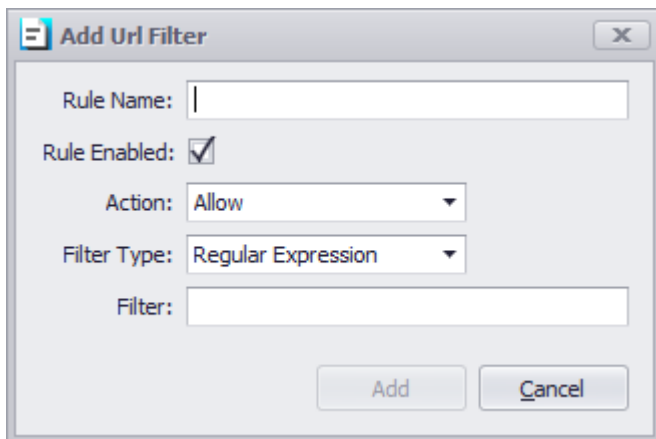
If enabled, the Administrator can create a list of Browser UR they want to block or allow navigations.

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.



Add Url Filter

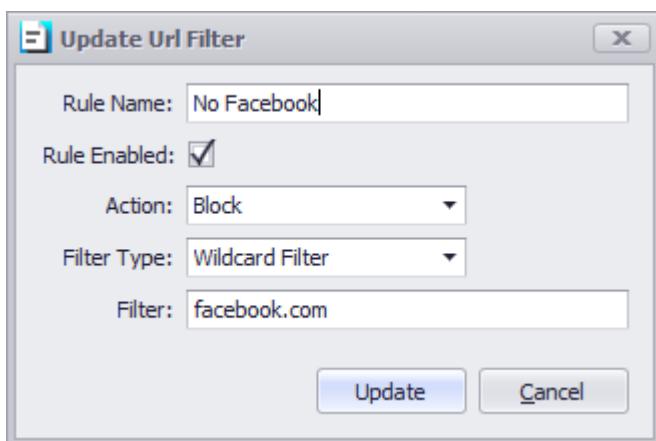
Rule Name:

Rule Enabled: ☒

Action:

Filter Type:

Filter:



Update Url Filter

Rule Name:

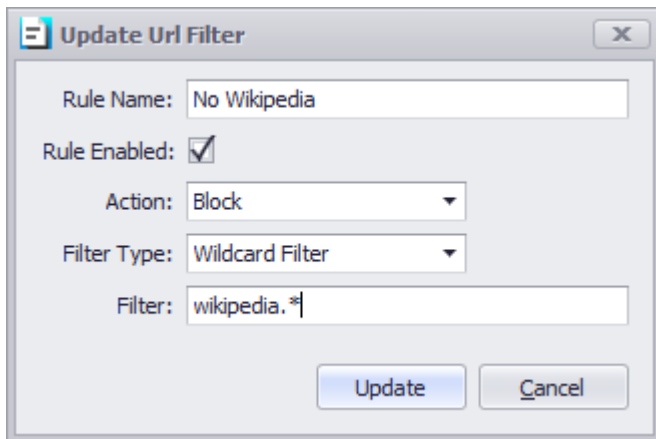
Rule Enabled: ☒

Action:

Filter Type:

Filter:

This rule will block facebook.com



Update Url Filter

Rule Name:

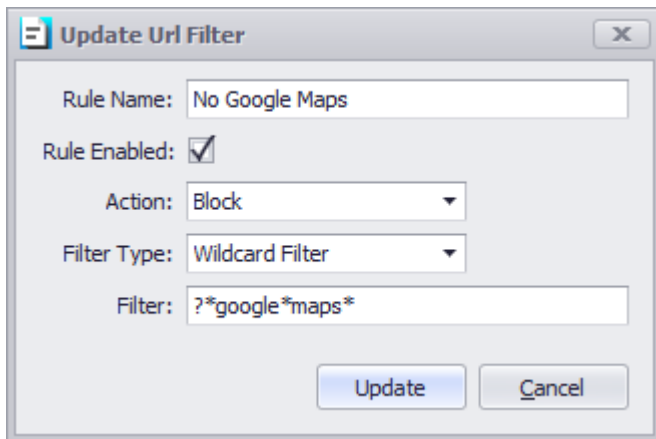
Rule Enabled: ☒

Action:

Filter Type:

Filter:

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



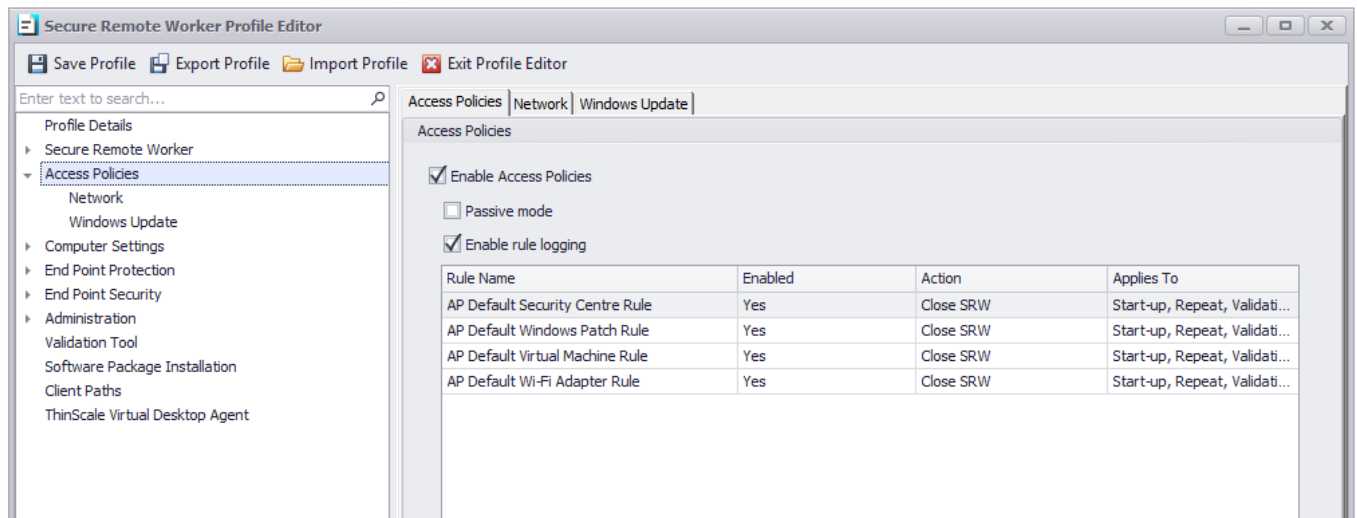
The 'Update Url Filter' dialog box contains the following fields and controls:

- Rule Name: No Google Maps
- Rule Enabled: ☒
- Action: Block
- Filter Type: Wildcard Filter
- Filter: ?*google*maps*
- Buttons: Update, Cancel

This rule will stop any searches containing google maps.

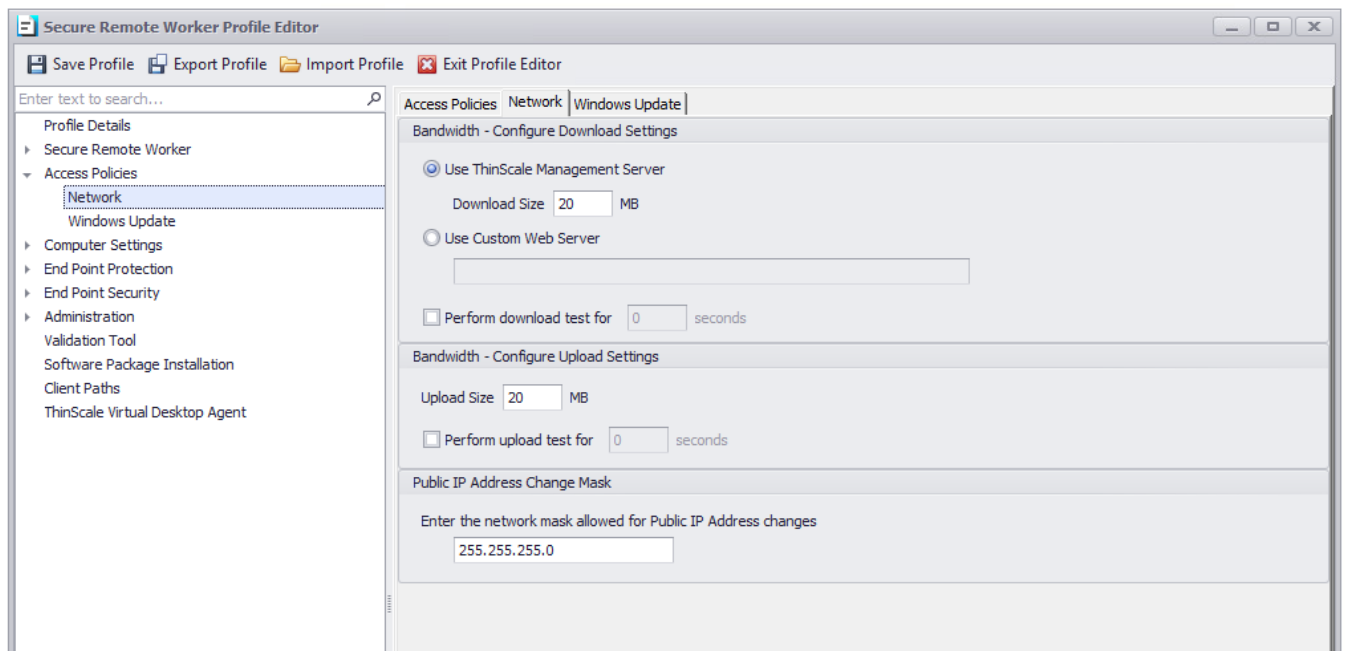
Rule Name	Enabled	Action	Type	Filter
No Facebook	Yes	Block	Wildcard Filter	facebook.com
No Funtime	Yes	Block	Wildcard Filter	reddit.*
No Google Maps	Yes	Block	Wildcard Filter	?*google*maps*

7. Access Policies



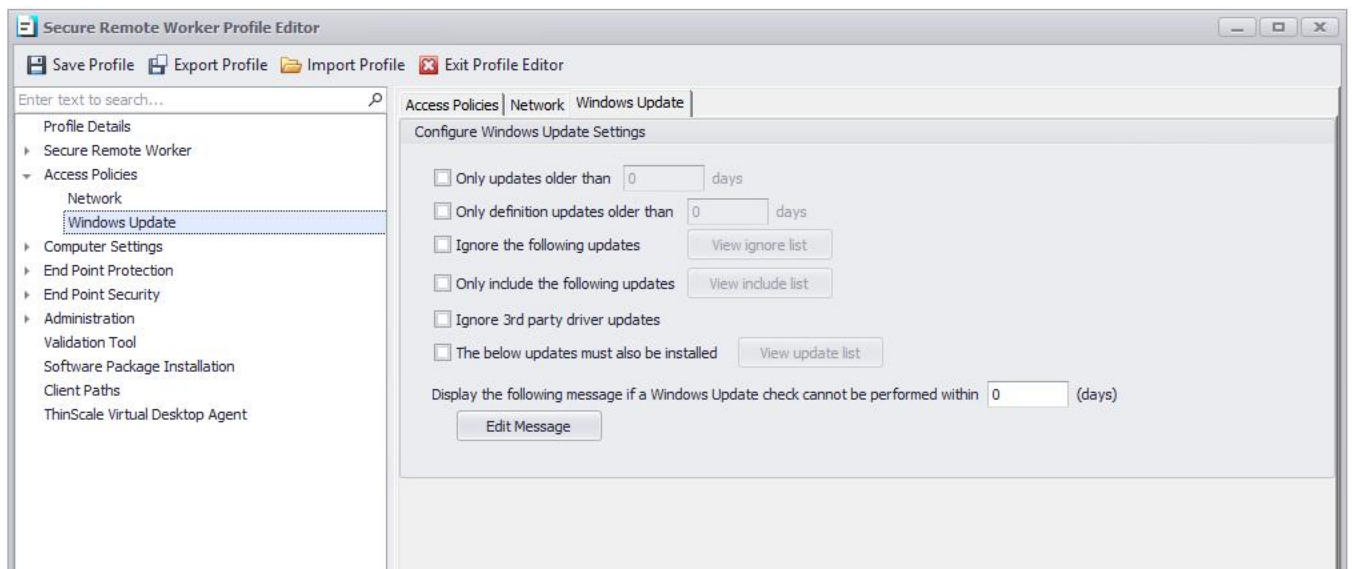
Please refer to the Knowledge Base [article](#) for more info.

Network

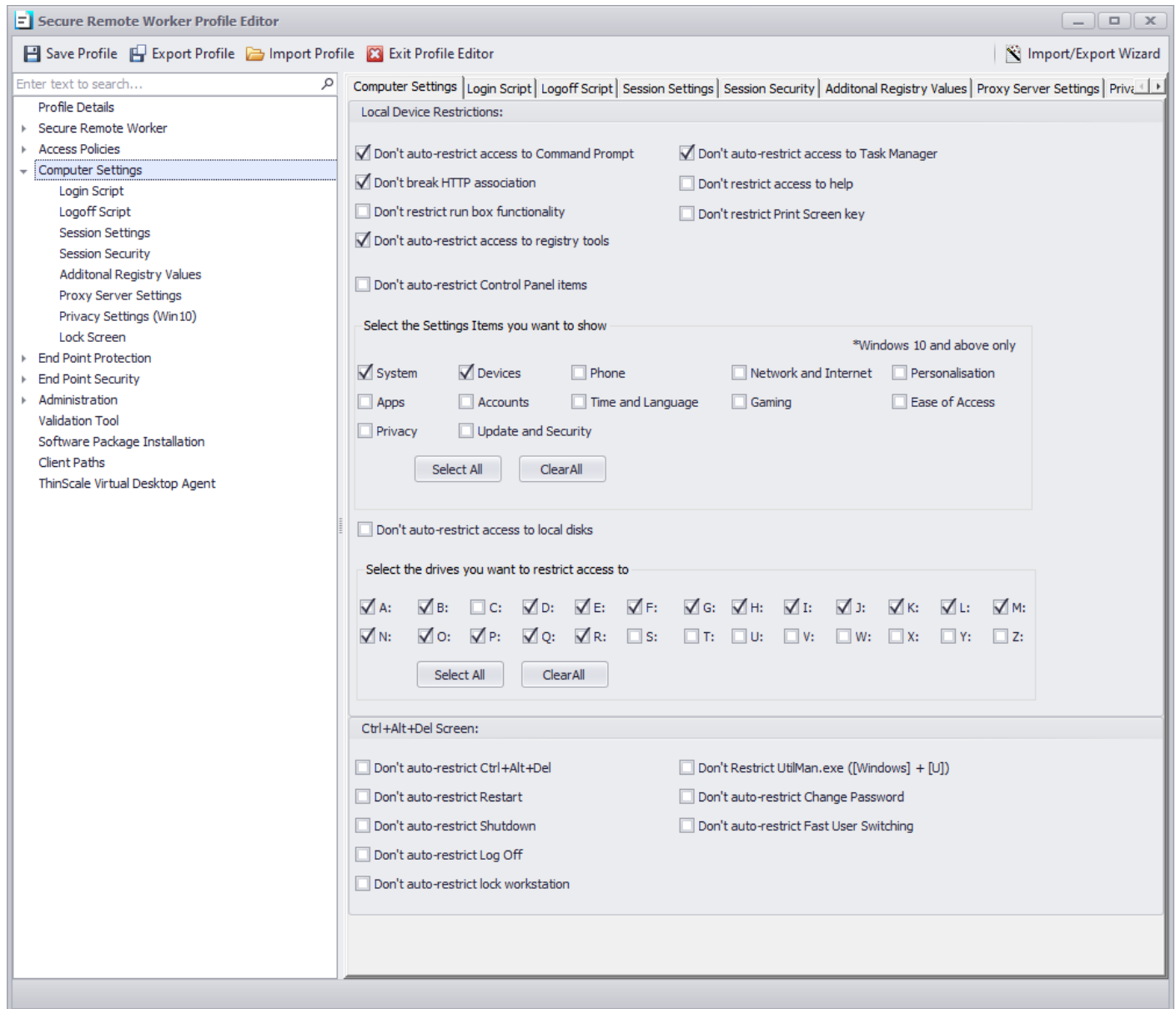


Use this section to test your download and upload speed.

Windows Update



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, use of Internet Explorer outside Secure Remote Worker is allowed.

Don't auto-restrict access to 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 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 7.2 SRW 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 disks

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 Secure Remote Worker 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

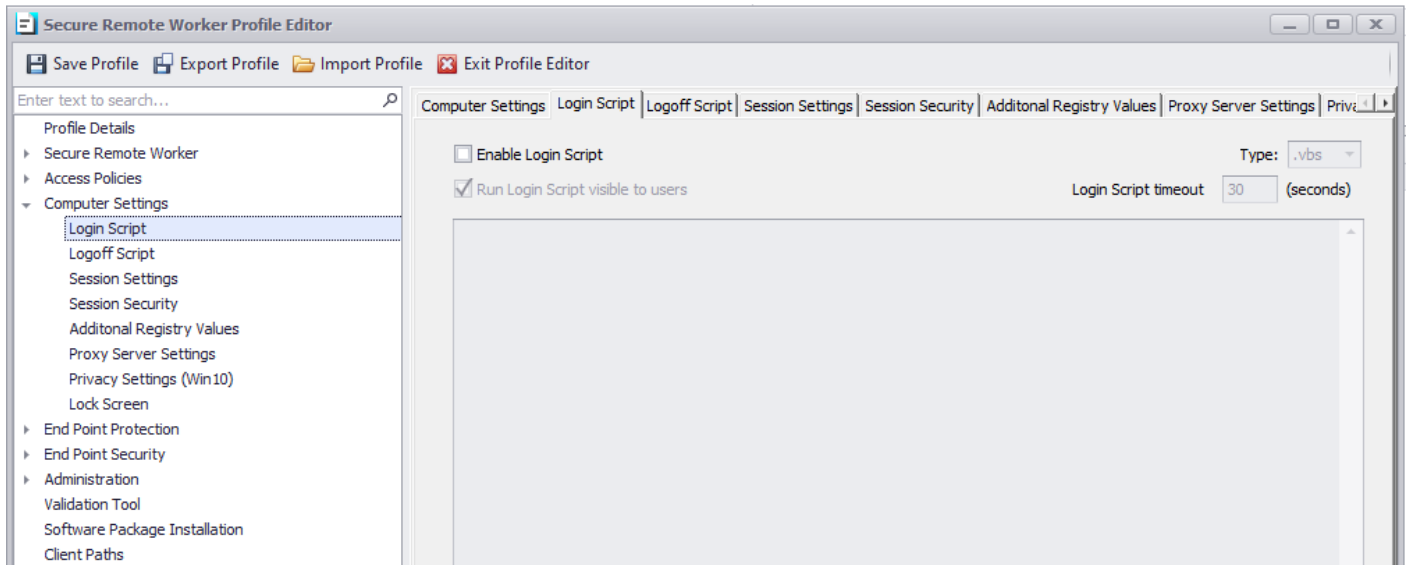
If enabled the Fast User Switching will be available from the lock screen.

Don't auto-restrict lock workstation

If enabled the users will be able to lock the local Secure Remote Worker workstation.

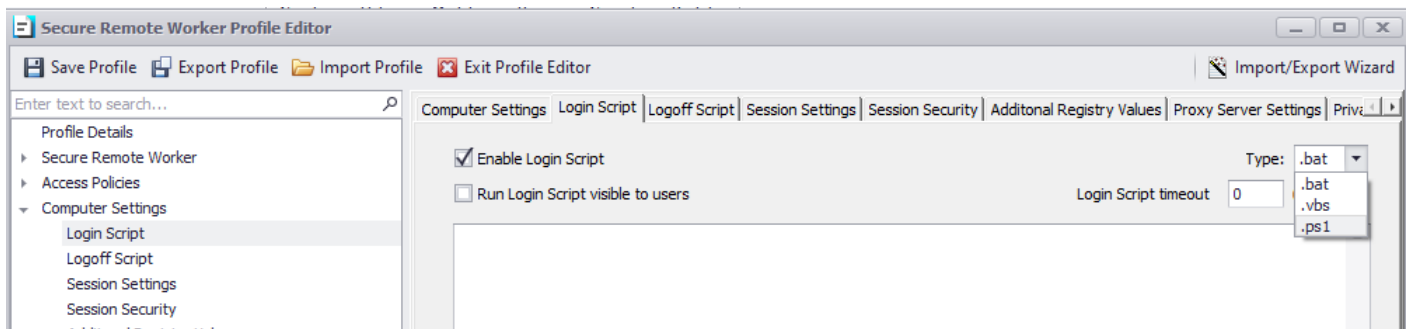
Note: those commands are restricted for the local machine only, for VDI pass through please refer to the Magic Filter Section in Session Settings.

Computer Settings – Login Script



Enable Login Script

Enables the supplied.VBS or. BAT or PS1 login script. The script will be applied when Secure Remote Worker UI is first started



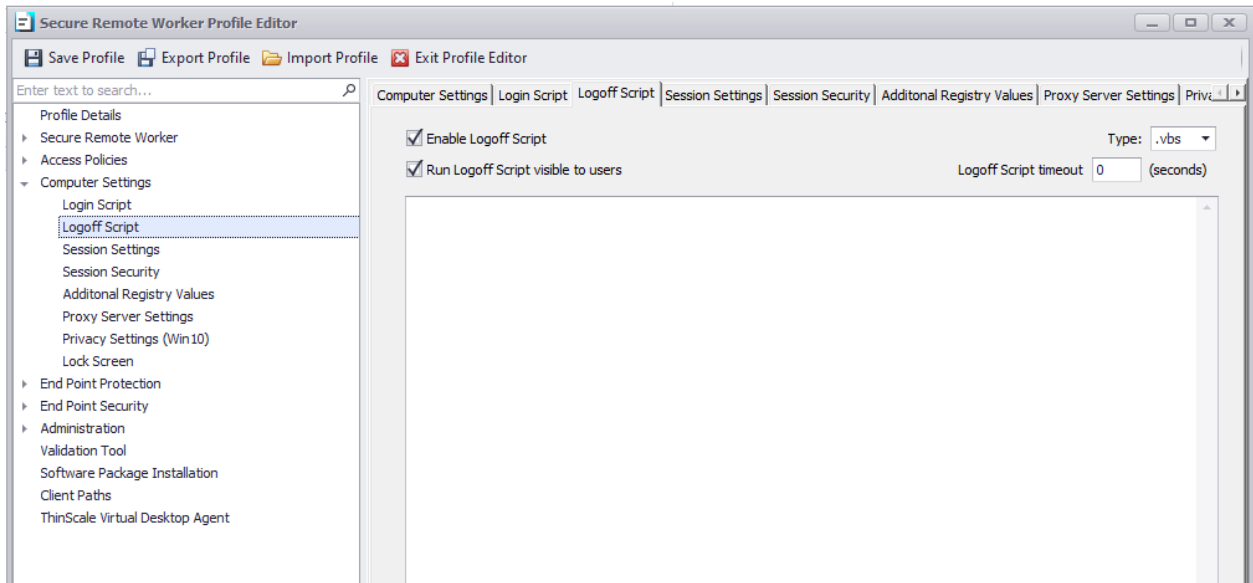
Run Login Script Visible to users

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

Login Script Timeout

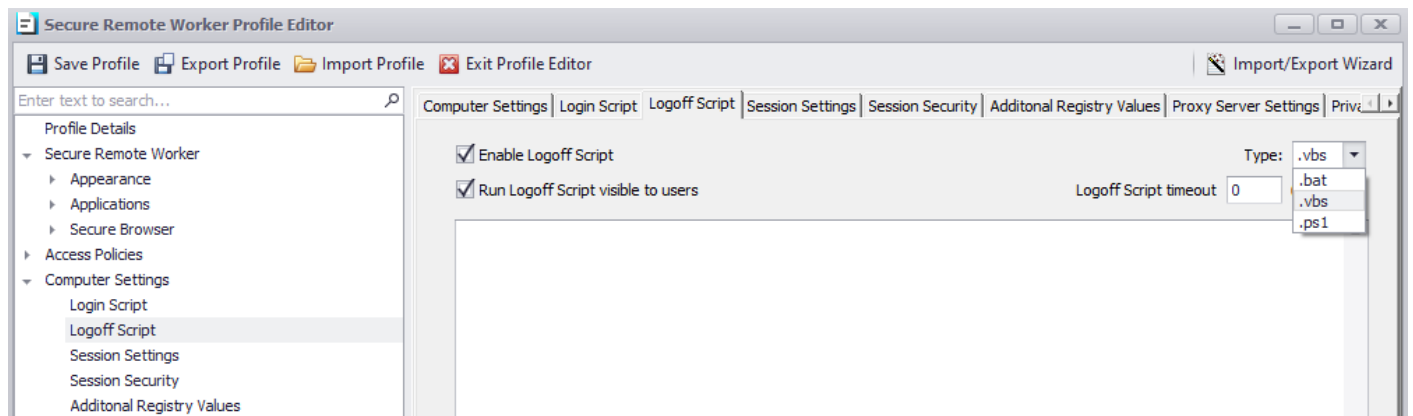
Determines how long the scripts will run before stopping their execution.

Computer Settings – Logoff Script



Enable Logoff Script

Enables the supplied.VBS or. BAT or PS1 logoff script. The script will be applied when Secure Remote Worker UI is closed



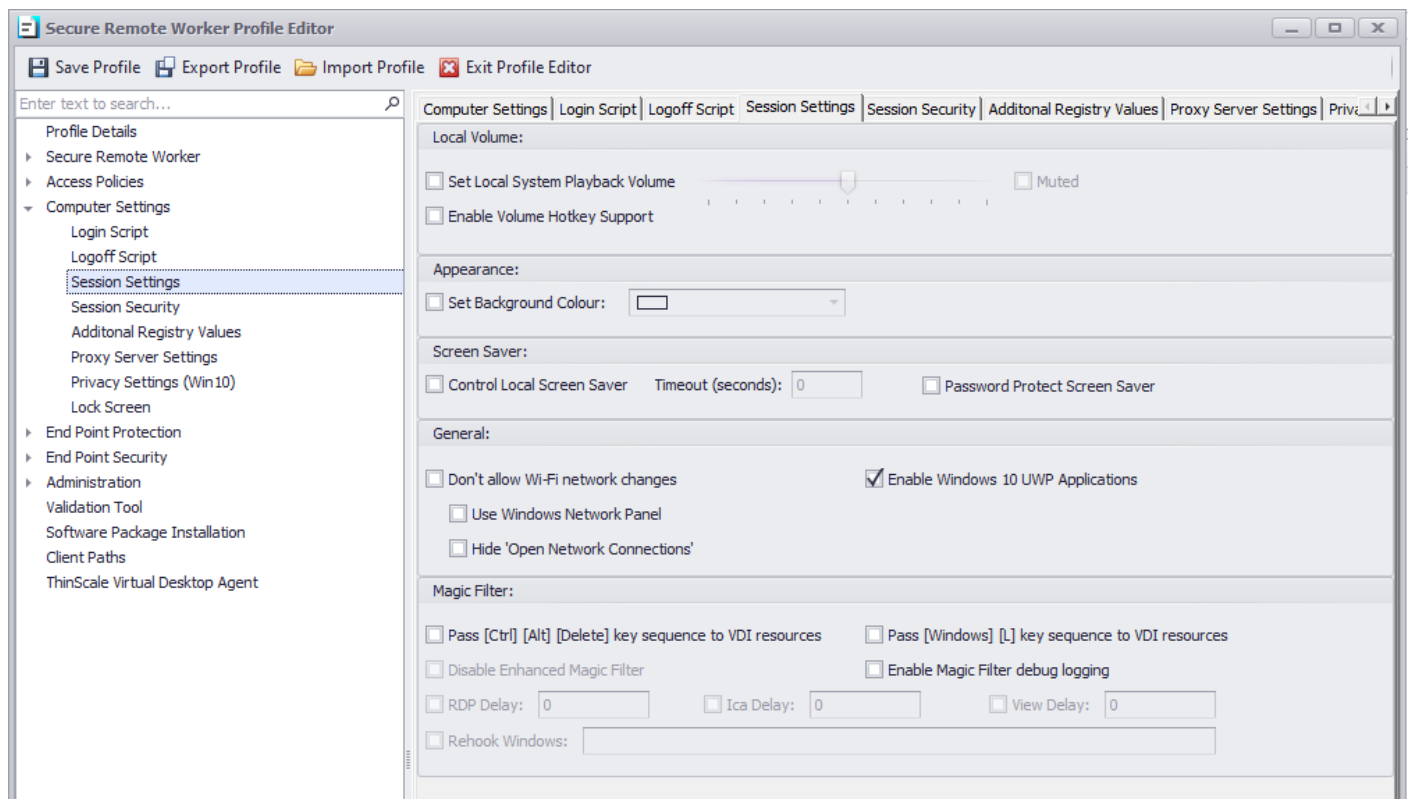
Run Logoff Script Visible to users

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

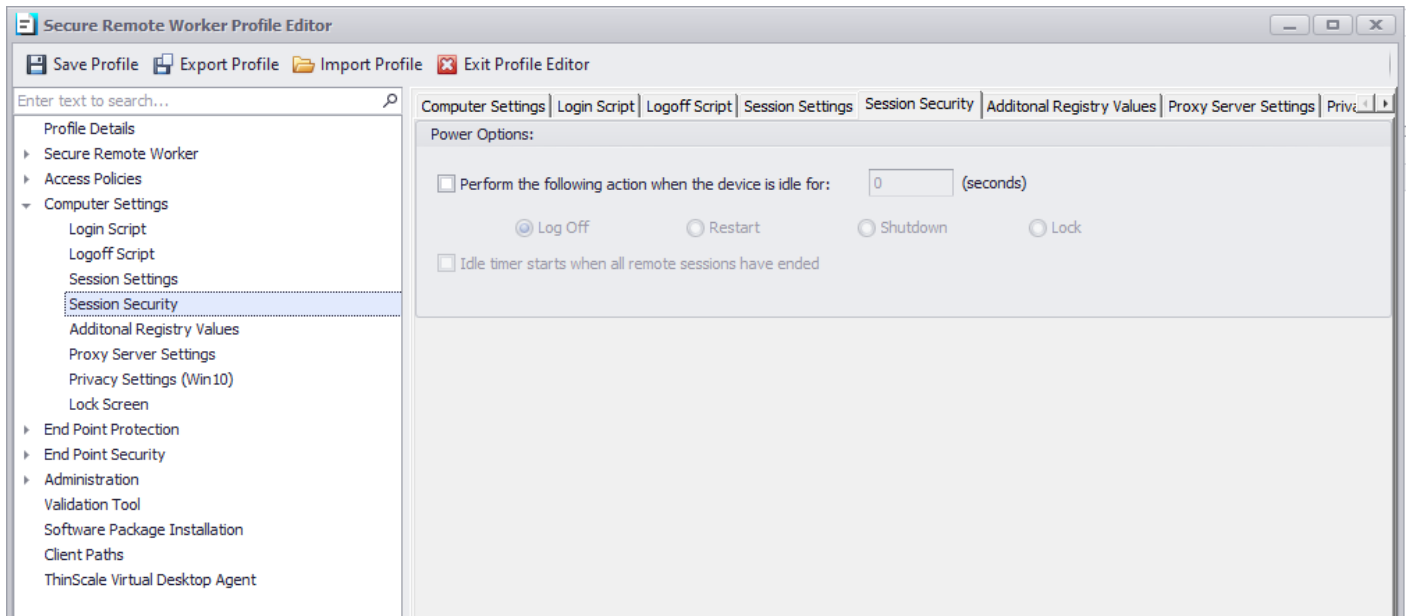
Set Local Volume

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

Enable Volume Hotkey Support

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

Computer Settings - Session Security



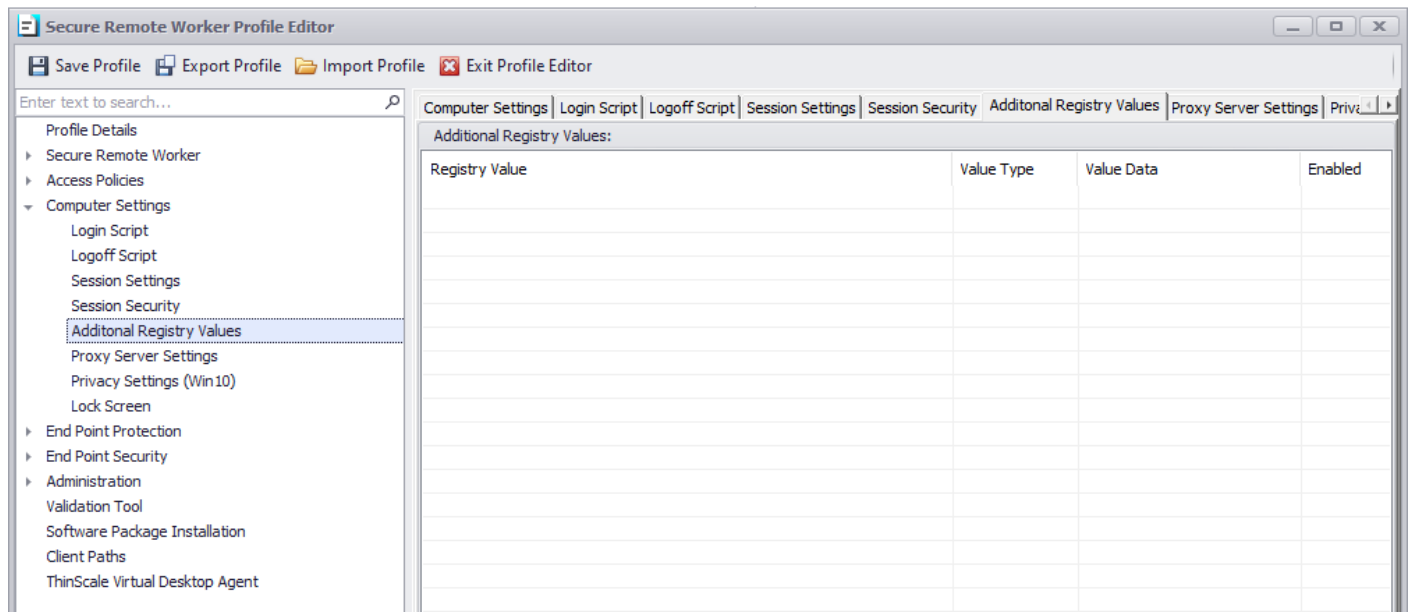
Power Options

Perform the following action when the device is idle for

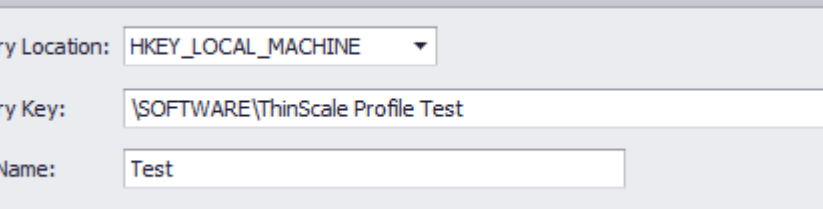
If enabled, Secure Remote Worker will perform the selected action when the local device has been idle for the configured number of seconds.

The idle timer starts when all remote sessions have ended

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



Simply pick the location hive between HKLM or HKCU, add the Registry Key location, a value name, a type and data.



Add Registry Value

Registry Location: HKEY_LOCAL_MACHINE ▼

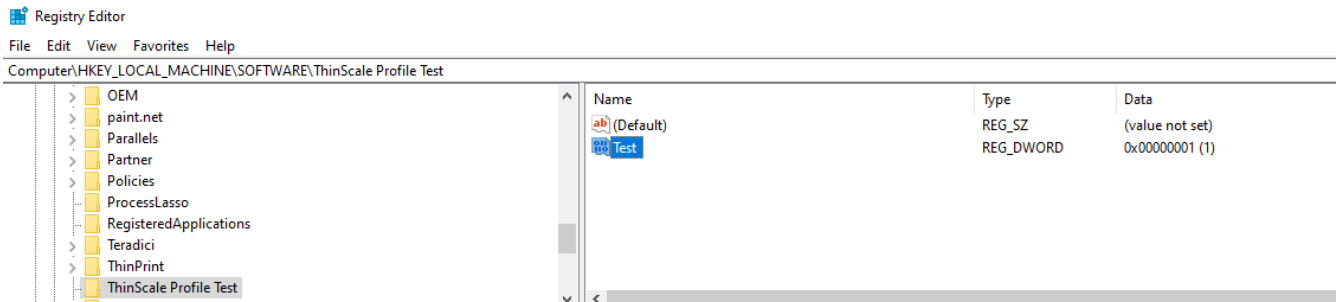
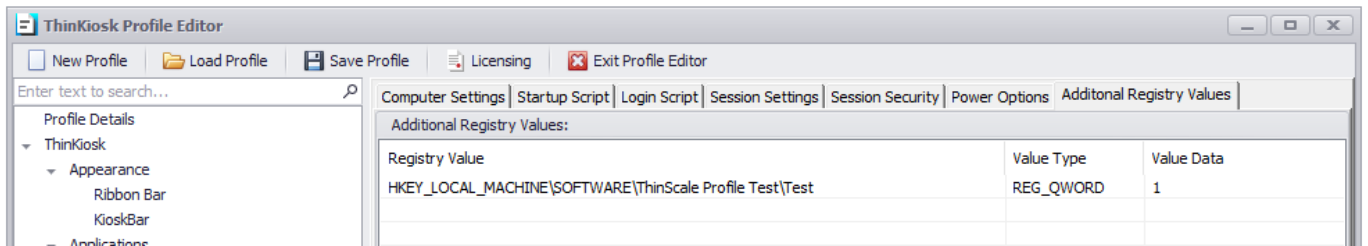
Registry Key: \\SOFTWARE\\ThinScale Profile Test

Value Name: Test

Value Type: REG_QWORD ▼

Value Data: 1

Add Cancel



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

Also unlocking SRW will remove the applied keys

Computer Settings - Proxy Server Settings

Secure Remote Worker Profile Editor

Save Profile Export Profile Import Profile Exit Profile Editor

Enter text to search...

- Profile Details
- Secure Remote Worker
- Access Policies
- Computer Settings
 - Login Script
 - Logoff Script
 - Session Settings
 - Session Security
 - Additional Registry Values
 - Proxy Server Settings**
 - Privacy Settings (Win10)
 - Lock Screen
- End Point Protection
- End Point Security
- Administration
 - Validation Tool
 - Software Package Installation
 - Client Paths
 - ThinScale Virtual Desktop Agent

Computer Settings | Login Script | Logoff Script | Session Settings | Session Security | Additional Registry Values | Proxy Server Settings | Privacy Settings

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 separate entries.

☐ Bypass proxy server for local addresses

Advanced Settings

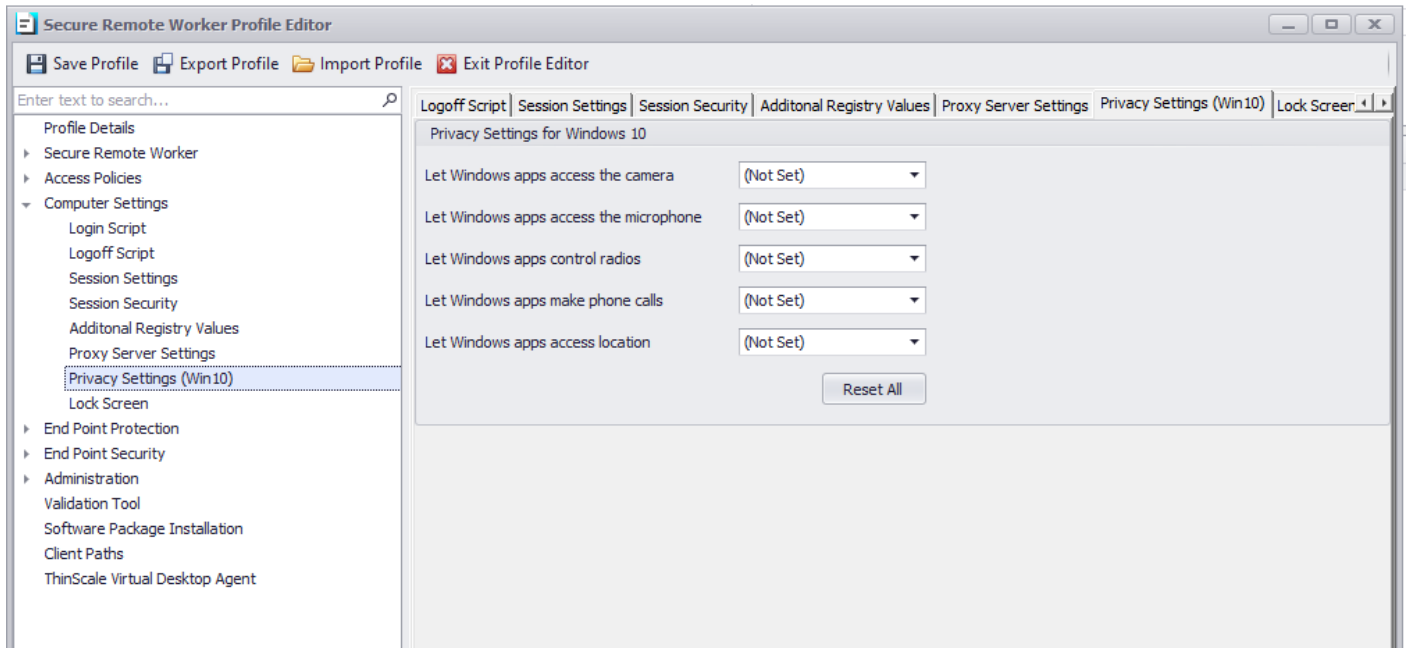
Type	Proxy Address	Port
HTTP	<input type="text"/>	<input type="text" value="0"/>
Secure	<input type="text"/>	<input type="text" value="0"/>
FTP	<input type="text"/>	<input type="text" value="0"/>
Socks	<input type="text"/>	<input type="text" value="0"/>

☐ Use the same proxy server for all protocols

Advanced Internet Settings:

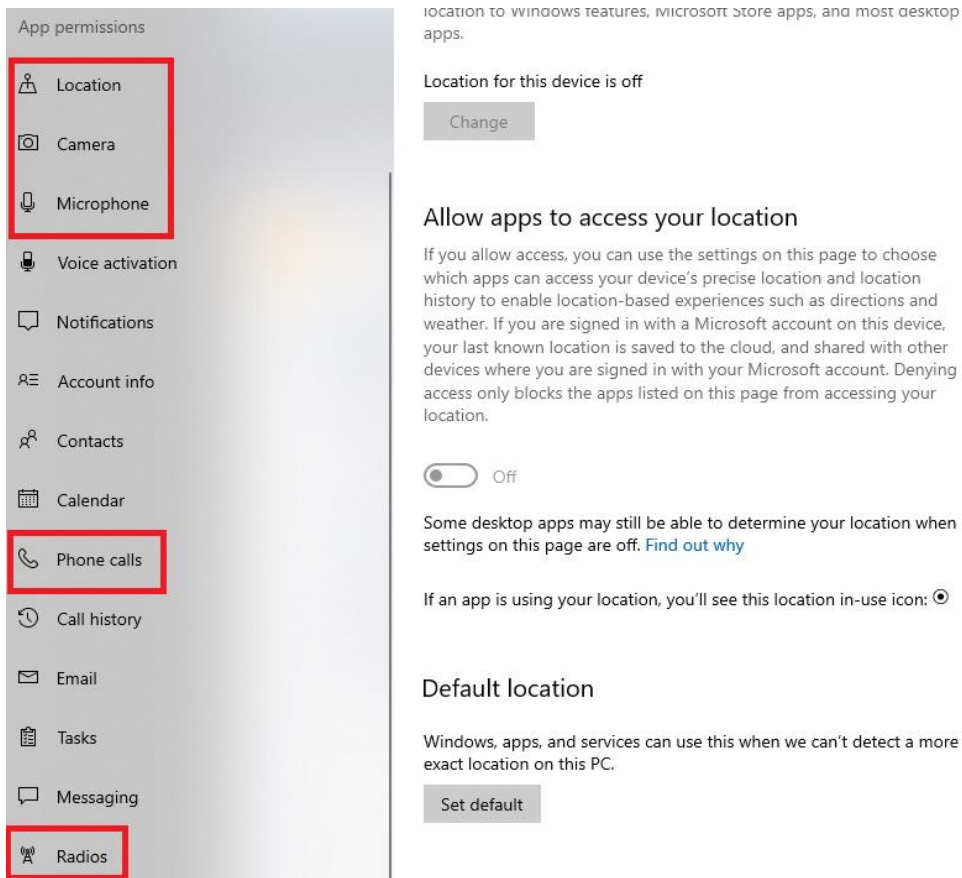
<input type="checkbox"/> PrivDiscUIShown	<input type="checkbox"/> Use HTTP 1.1
<input type="checkbox"/> Use HTTP 1.1 through proxy connections	<input type="checkbox"/> Warn On Intranet
<input type="checkbox"/> Send URL path as UTF-8	<input type="checkbox"/> Do not save encrypted pages on disc
<input type="checkbox"/> Warn if changing between secure and not secure mode	<input type="checkbox"/> Check for server certificate revocation
<input type="checkbox"/> Enable Integrated Windows Authentication	<input type="checkbox"/> Enable Autodial
<input type="checkbox"/> No Net Autodial	<input type="checkbox"/> Global User Offline
<input type="checkbox"/> Always show encoded addresses	<input type="checkbox"/> Show Notification bar for encoded addresses

Computer Settings - Privacy Settings (Win10)

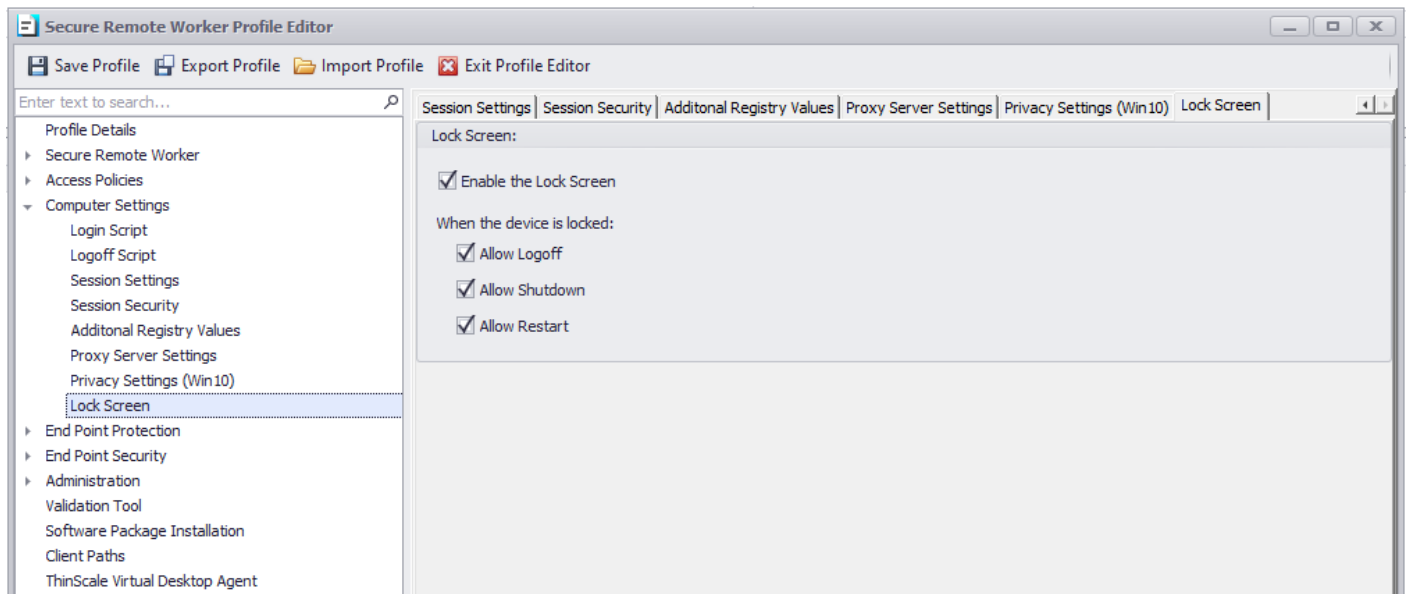


Privacy Settings in Windows 10 can be accessed by going into Settings / Privacy / App Permissions.

These options represent the same options that windows displayed just grouped.

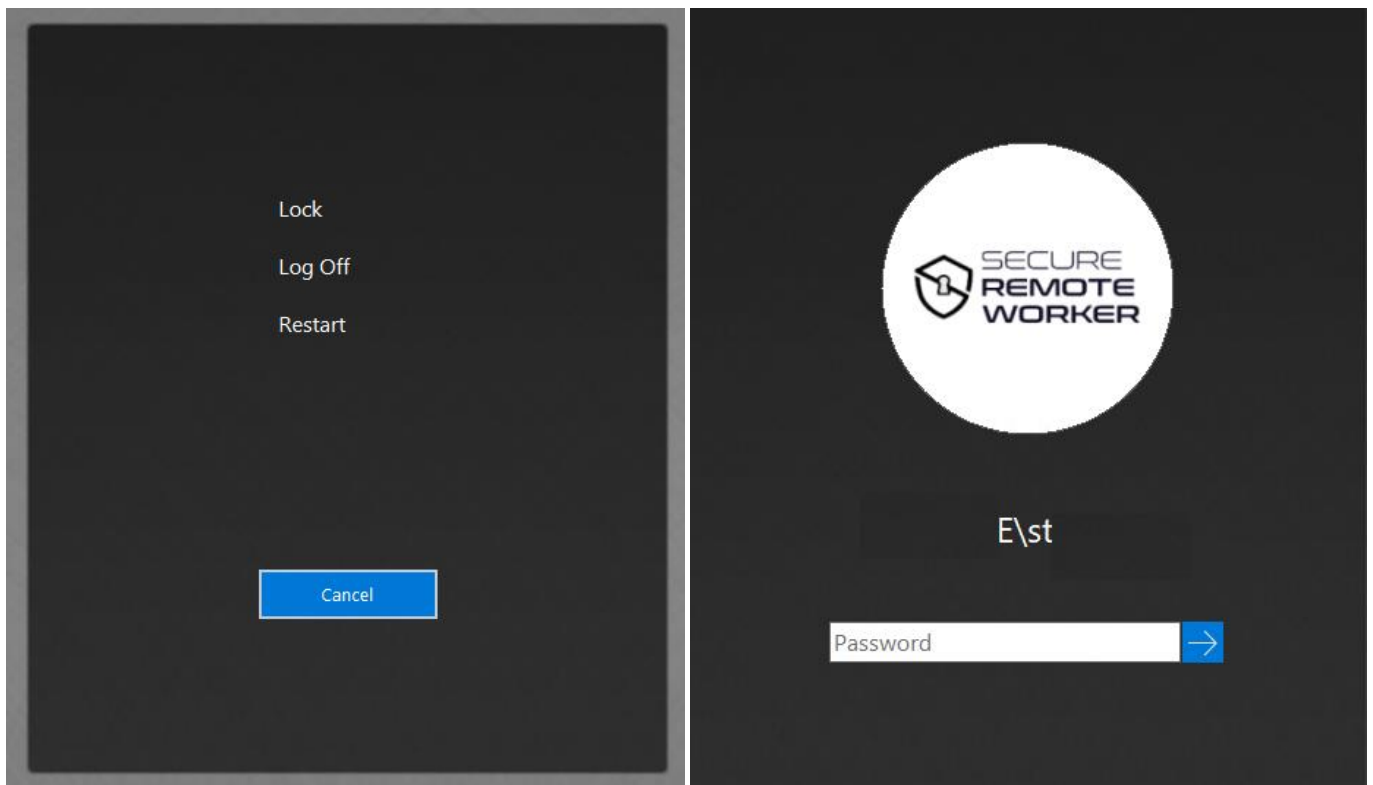


Computer Settings - Lock Screen



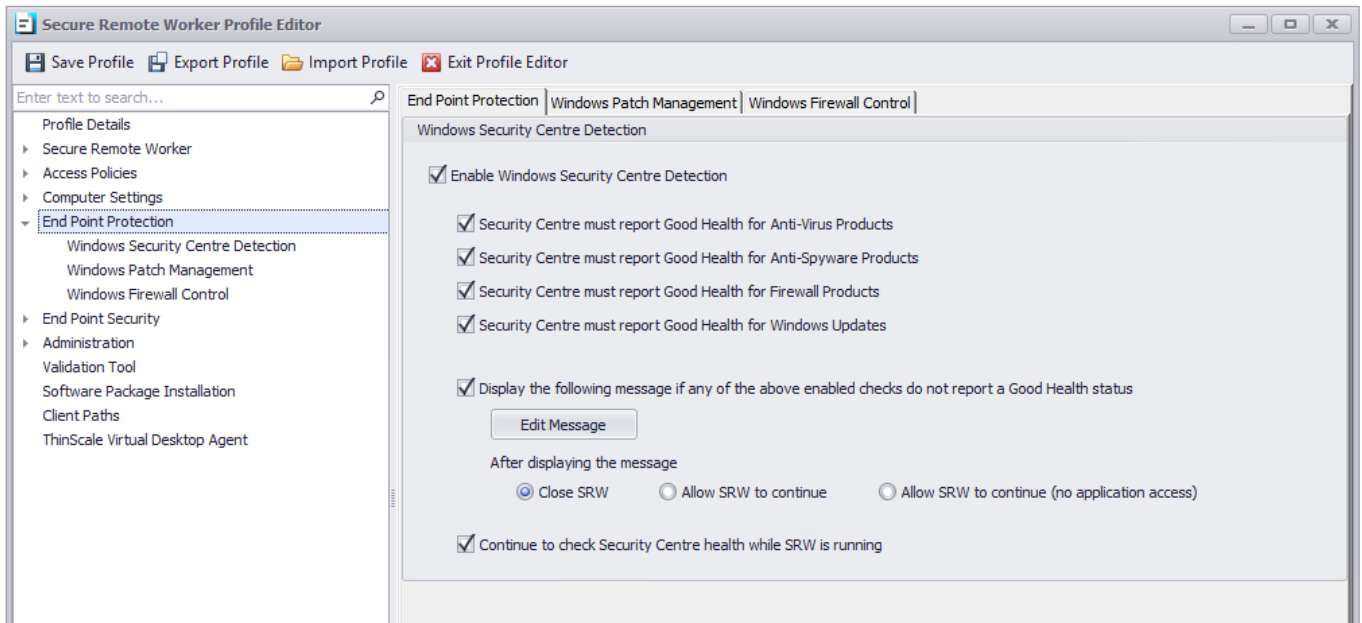
If enabled, the CAD screen will be replaced by the ThinScale Lock Screen where users will be able to lock and unlock their screen using the Auth Provider assigned to the device folder.

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



9. End Point Protection

Windows Security Centre Detection



End Point Protection - Windows Security Centre Detection

Enable Security Centre Detection

If enabled, Secure Remote Worker 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.



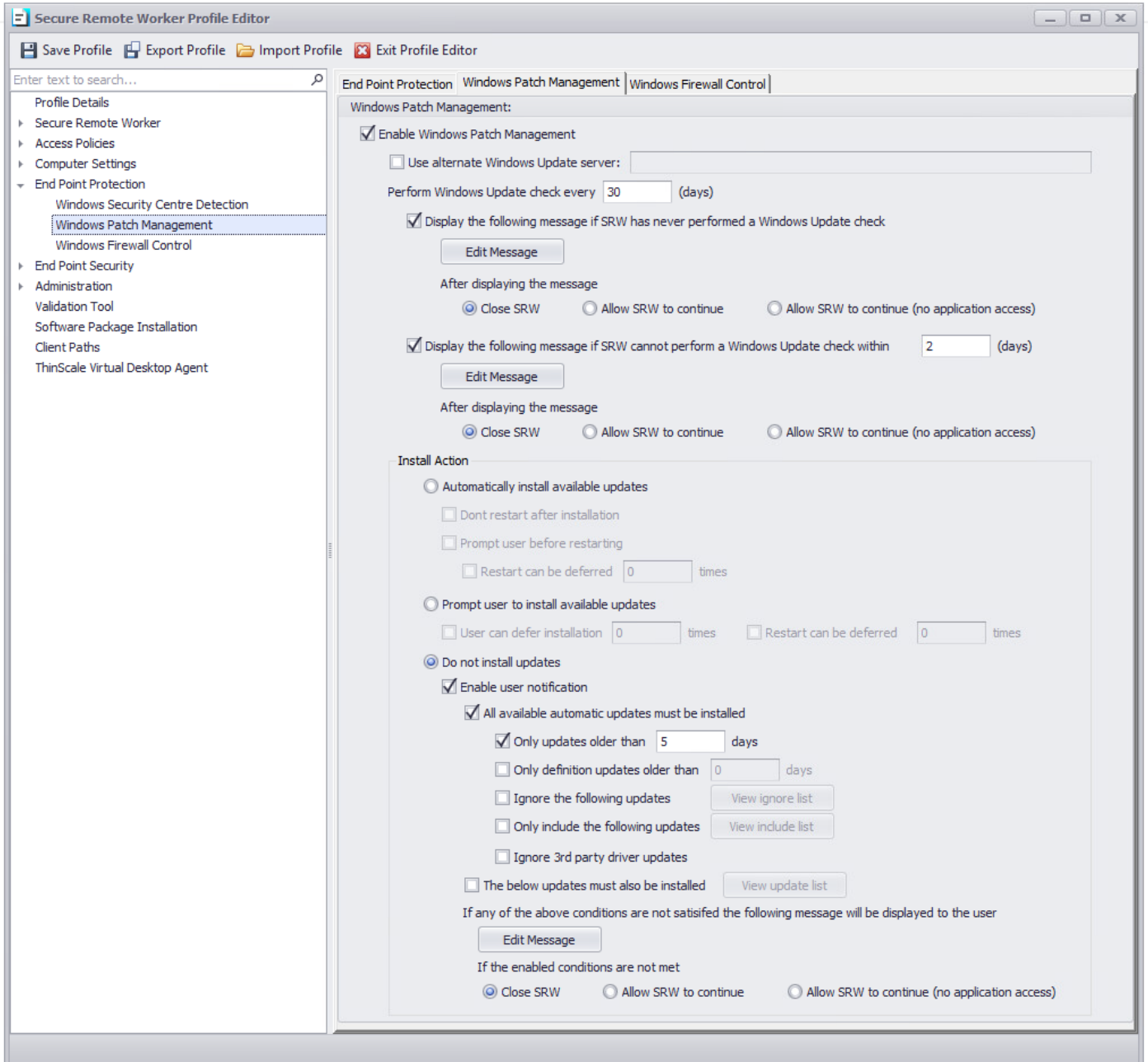
After displaying this message

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

Continue to check Security Centre health while Secure Remote Worker is running.

Secure Remote Worker 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



The screenshot shows the 'Secure Remote Worker Profile Editor' window. The left sidebar contains a tree view with the following items: Profile Details, Secure Remote Worker, Access Policies, Computer Settings, End Point Protection (selected), Windows Security Centre Detection, Windows Patch Management (highlighted), Windows Firewall Control, End Point Security, Administration, Validation Tool, Software Package Installation, Client Paths, and ThinScale Virtual Desktop Agent.

The main pane is titled 'End Point Protection | Windows Patch Management | Windows Firewall Control'. The 'Windows Patch Management' tab is active, showing the following settings:

- ☒ Enable Windows Patch Management
 - ☐ Use alternate Windows Update server:
 - Perform Windows Update check every (days)
 - ☒ Display the following message if SRW has never performed a Windows Update check
 -
 - After displaying the message:
 - ☒ Close SRW
 - ☐ Allow SRW to continue
 - ☐ Allow SRW to continue (no application access)
 - ☒ Display the following message if SRW cannot perform a Windows Update check within (days)
 -
 - After displaying the message:
 - ☒ Close SRW
 - ☐ Allow SRW to continue
 - ☐ Allow SRW to continue (no application access)
- Install Action
 - ☐ Automatically install available updates
 - ☐ Dont restart after installation
 - ☐ Prompt user before restarting
 - ☐ Restart can be deferred times
 - ☐ Prompt user to install available updates
 - ☐ User can defer installation times
 - ☐ Restart can be deferred times
 - ☒ Do not install updates
 - ☒ Enable user notification
 - ☒ All available automatic updates must be installed
 - ☒ Only updates older than days
 - ☐ Only definition updates older than days
 - ☐ Ignore the following updates
 - ☐ Only include the following updates
 - ☐ Ignore 3rd party driver updates
 - ☐ The below updates must also be installed
 - If any of the above conditions are not satisfied the following message will be displayed to the user
 -
 - If the enabled conditions are not met:
 - ☒ Close SRW
 - ☐ Allow SRW to continue
 - ☐ Allow SRW to continue (no application access)

Enable Windows Patch Management

If enabled Secure Remote Worker will check for Windows Updates.

Use alternate Windows Update server

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

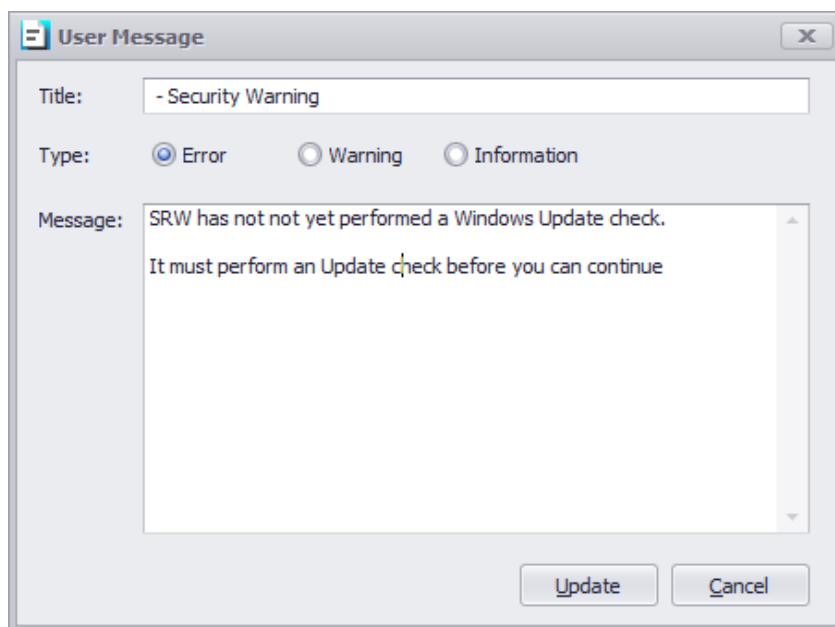
Perform Windows Update check every

If enabled, Secure Remote Worker will check for updates every specified number of days.

Display the following message if Secure Remote Worker 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. Secure Remote Worker can either be closed, allow to continue or allow to continue without access to any applications or browser.

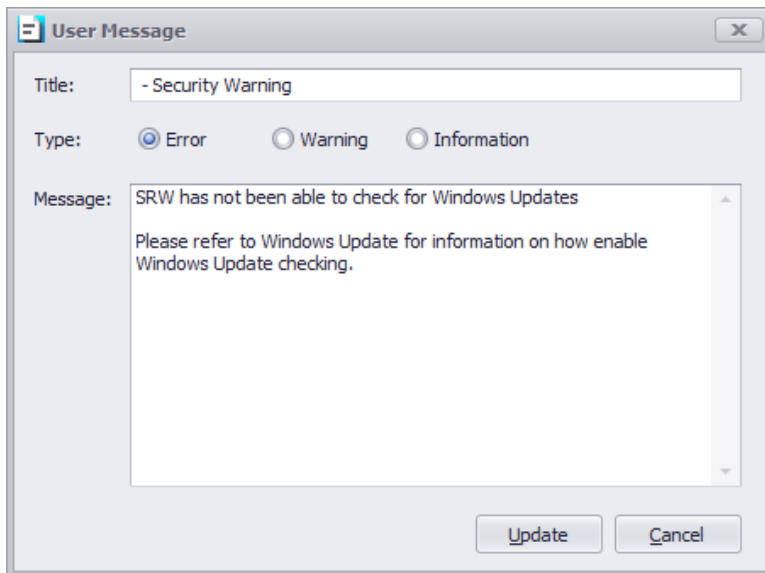
Note: Error, Warning, Information refers to the icon style of the message box.



Display the following message if Secure Remote Worker cannot perform a Windows Update check within

If enabled, a machine where Windows updates couldn't be performed for a certain number of days will receive this message. This message can be modified as you like and different actions can be selected based on the results. Secure Remote Worker 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 Secure Remote Worker detects available updates for installation

Automatically install available updates

If enabled, Secure Remote Worker will silently install available updates.

Don't restart after installation

If enabled, Secure Remote Worker 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 Secure Remote Worker 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.

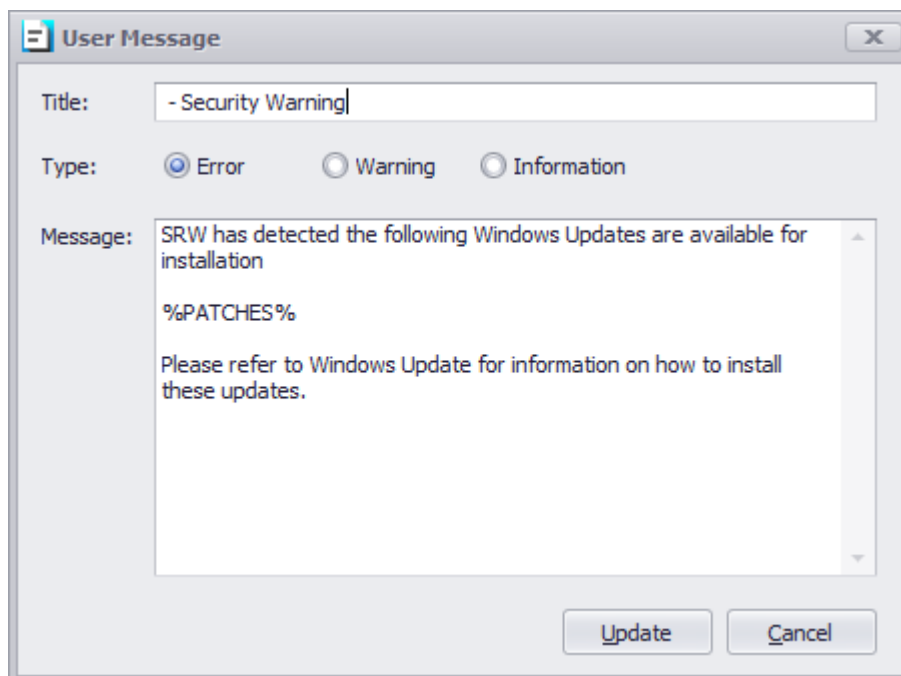
Do not install updates

If enabled, Secure Remote Worker 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. Secure Remote Worker 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 Secure Remote Worker” is selected, users must install all available updates, or they won’t be able to use Secure Remote Worker.

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

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

Only updates older than

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

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

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

Only definition updates older than

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

If enabled, and “Allow Secure Remote Worker to Continue” is selected, the user will be able to launch Secure Remote Worker

If enabled, and “Allow Secure Remote Worker to continue (no application)” is selected, the user will be able to use Secure Remote Worker 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.

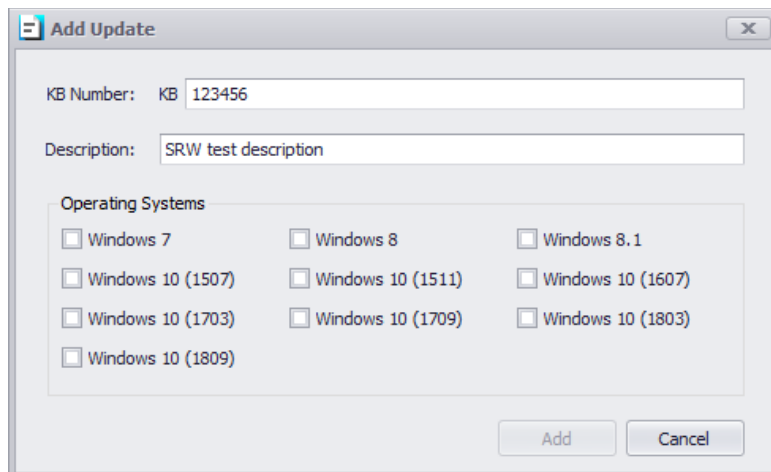
The below updates must also be installed

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

If enabled, and “Close Secure Remote Worker” is selected, users must install all configured updates, or they will not be able to use Secure Remote Worker.

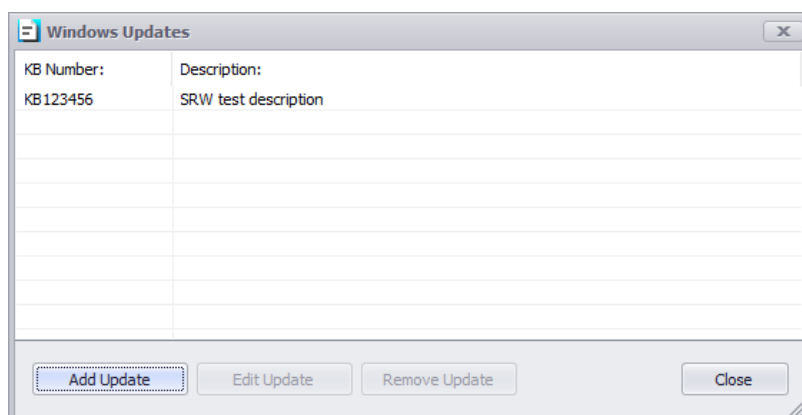
If enabled, and “Allow Secure Remote Worker to Continue” is selected, the user will be able to launch Secure Remote Worker.

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



The 'Add Update' dialog box contains the following fields and options:

- KB Number:** A text field with 'KB' as a prefix and '123456' as the value.
- Description:** A text field with the value 'SRW test description'.
- Operating Systems:** A group box containing several checkboxes:
 - ☐ Windows 7
 - ☐ Windows 8
 - ☐ Windows 8.1
 - ☐ Windows 10 (1507)
 - ☐ Windows 10 (1511)
 - ☐ Windows 10 (1607)
 - ☐ Windows 10 (1703)
 - ☐ Windows 10 (1709)
 - ☐ Windows 10 (1803)
 - ☐ Windows 10 (1809)
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.



The 'Windows Updates' window displays a table of updates:

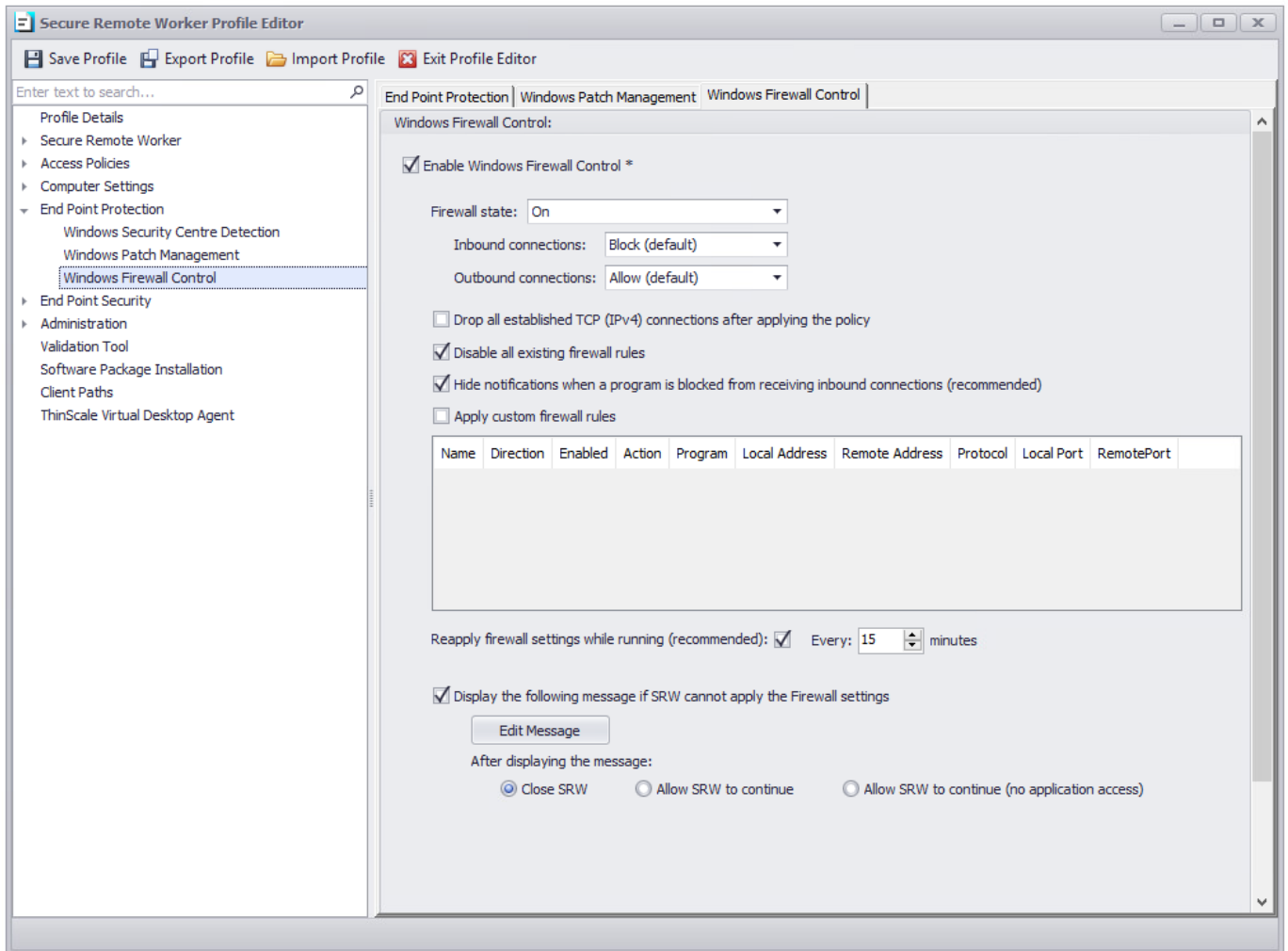
KB Number:	Description:
KB123456	SRW test description

At the bottom, there are buttons for 'Add Update', 'Edit Update', 'Remove Update', and 'Close'.

Note: you can now use a regular expression to filter specific updates.

i.e.: hp* will ignore/install everything containing the hp word

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

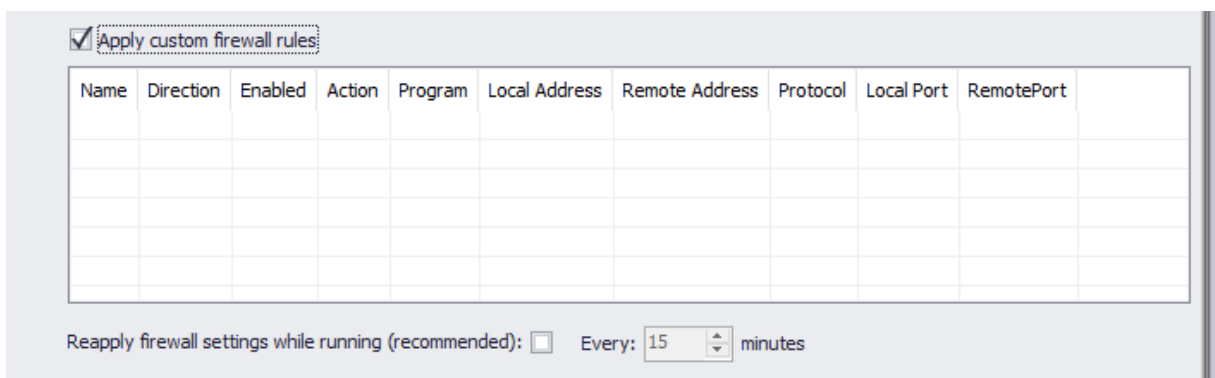
If enabled, Secure Remote Worker will disable all current Windows firewall rules. Secure Remote Worker will do a backup of all the existing rulesets and then disable them. When Secure Remote Worker policies are removed all original Firewall rules are recreated.

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

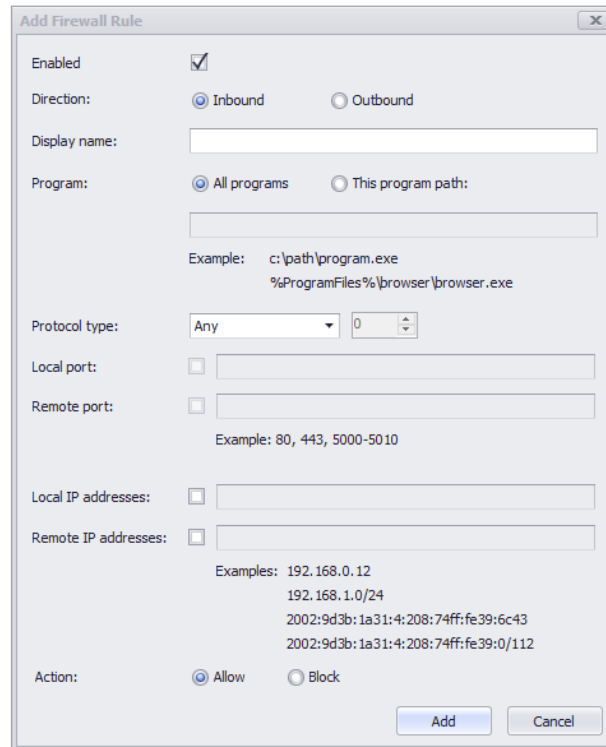
Create custom rules for inbound and outbound traffic.



☒ Apply custom firewall rules

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

Reapply firewall settings while running (recommended): ☐ Every: 15 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: Any 0

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

Add Cancel


Reapply firewall setting while running

If enabled, the Secure Remote Worker firewall rules setting will be reapplied based on the amount specified.

Display the following message if Secure Remote Worker 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. Secure Remote Worker 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.

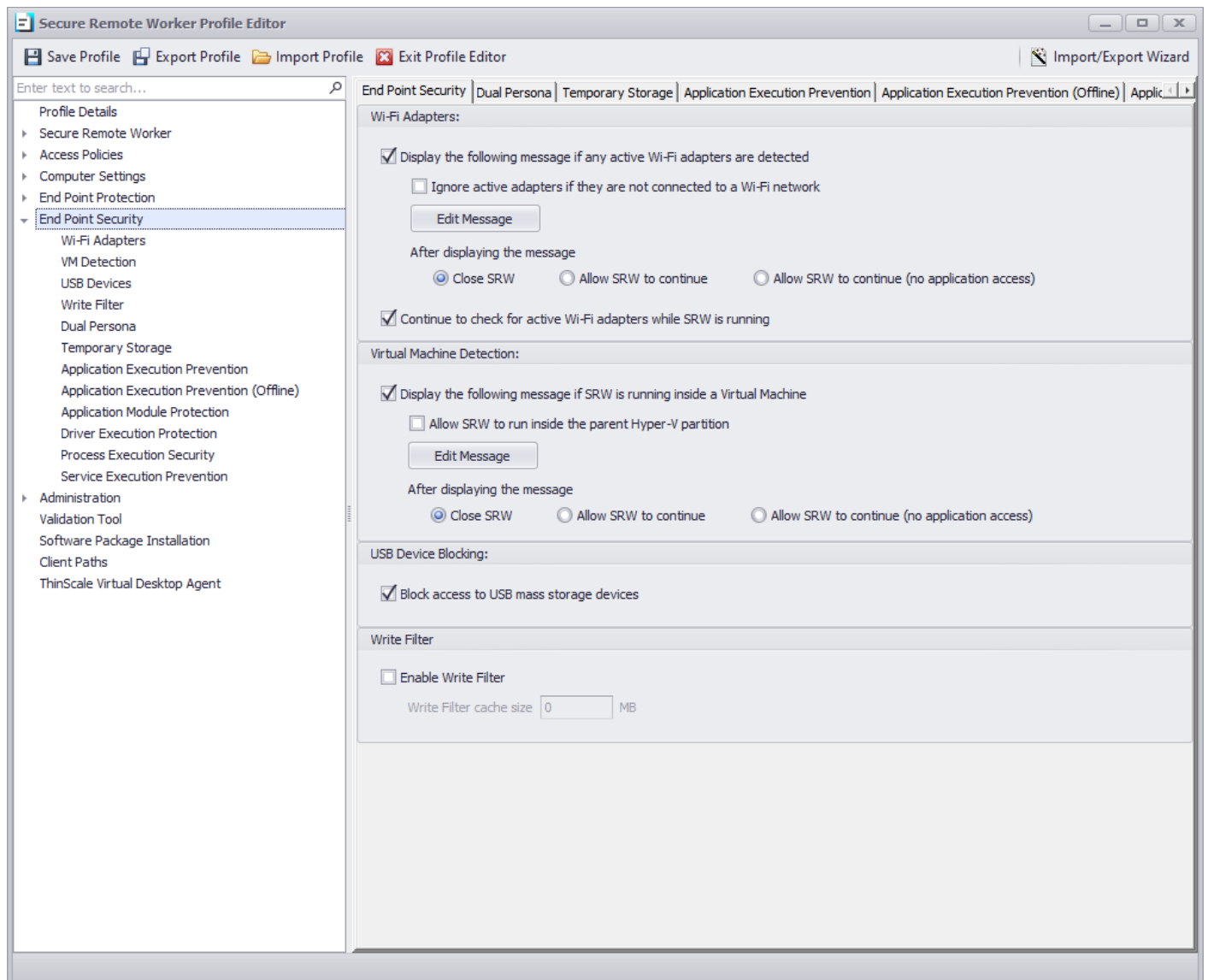
 User Message ✕

Title:

Type: ☒ Error ☐ Warning ☐ Information

Message:

10. End Point Security

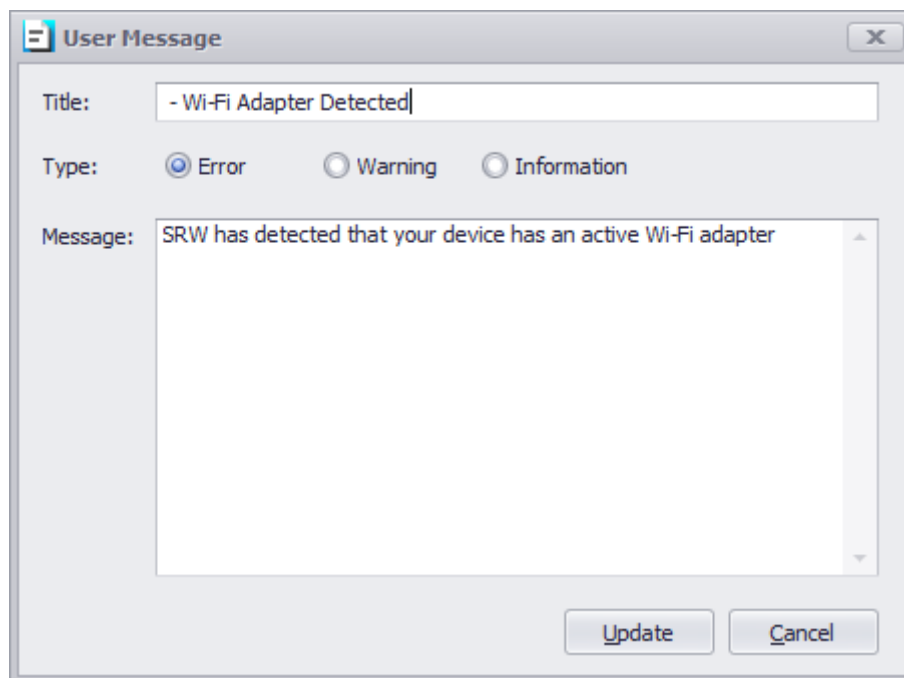


End Point Security - Wi-Fi Adapters

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

If enabled, a message will be displayed to the user if the Secure Remote Worker 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.

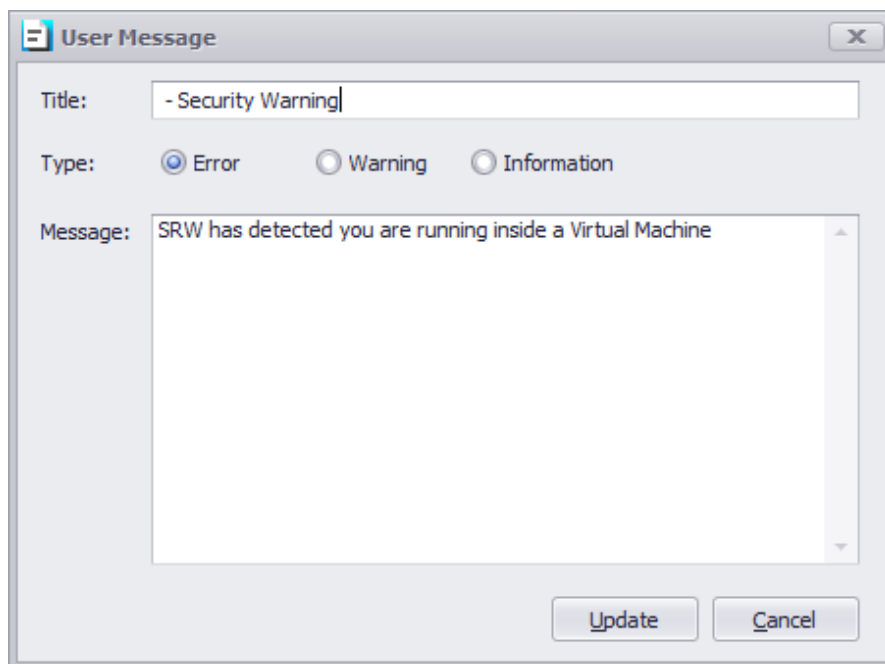
Secure Remote Worker can be either close, allow to continue or allow to continue without access to any application or browser.



End Point Security - Virtual Machine Detection

Display the following message if Secure Remote Worker is running inside a Virtual Machine

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



Allow Secure Remote Worker to run inside the parent Hyper-V partition

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

End Point Security - USB Device Blocking

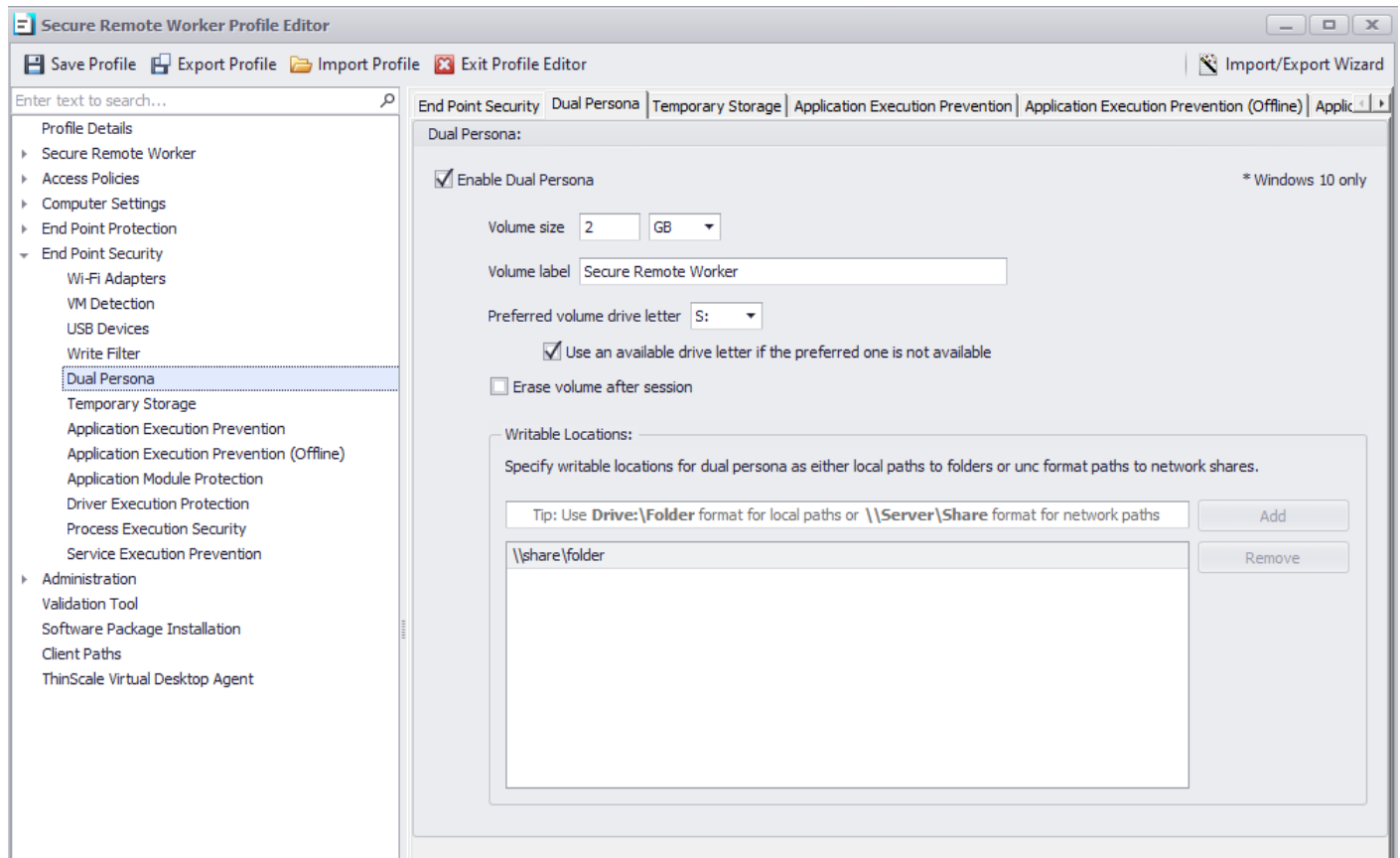
Block access to USB mass storage devices

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

End Point Security – Write Filter

If enabled, a VHDx will be created and the entire C: Drive will be filter protected

End Point Security – Dual Persona



Enable Dual Persona

Dual Persona is a new technology in SRW 7 that lets you move the SRW local windows user profile away from the local hard drive of the personal device (C:\Users) to an encrypted virtual volume.

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

When enabled, users will only be able to save data to this encrypted volume, all other locations, including all local hard drive volumes, are marked read-only when accessed from within the SRW session.

Only applications running inside the SRW session have access to the virtual volume.

Enable Dual Persona

Select to enable Dual Persona

Volume Size

Select the maximum size of the virtual volume. The Dual Personal 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 Dual Persona volume

Preferred Volume Drive Letter

Select the drive letter that will be assigned to the Dual Persona 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, SRW will use the first available drive letter on the device.

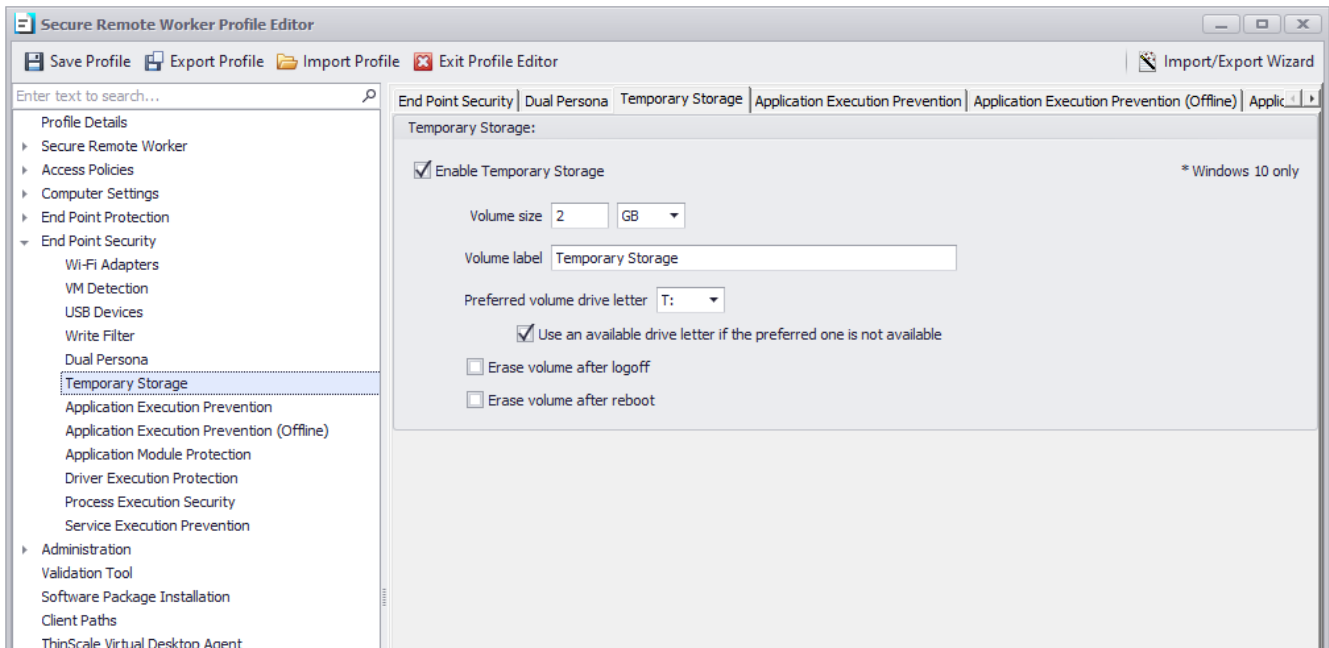
Erase Volume after the session

When enabled, all data that was saved to the virtual volume during the SRW session will be deleted.

Writable Location

If enabled, you can specify share drive or local folders where users can save data into it, while still protecting the entire C: drive.

End Point Security – Temporary Storage



Enable Temporary Storage

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

The encrypted virtual volume is managed by SRW and is only made available when SRW 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, SRW will use the first available drive letter on the device.

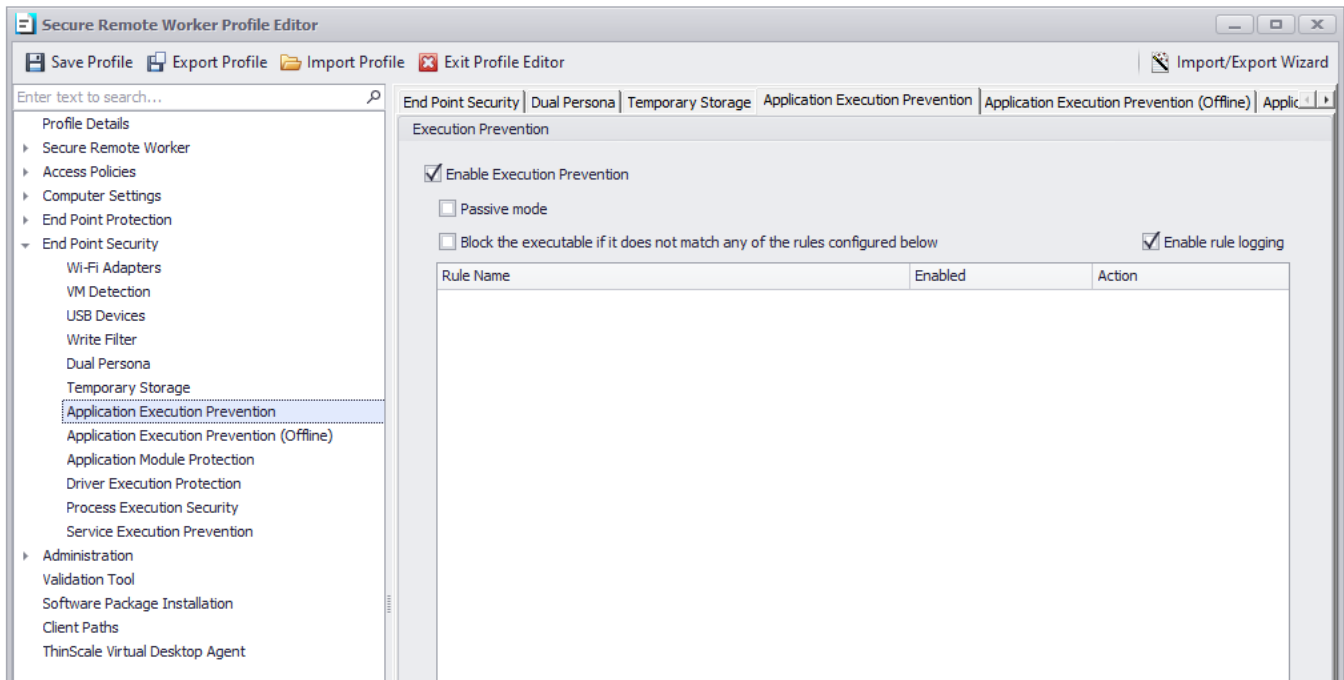
Erase Volume after logoff

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

Erase Volume after reboot

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

End Point Security - 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.

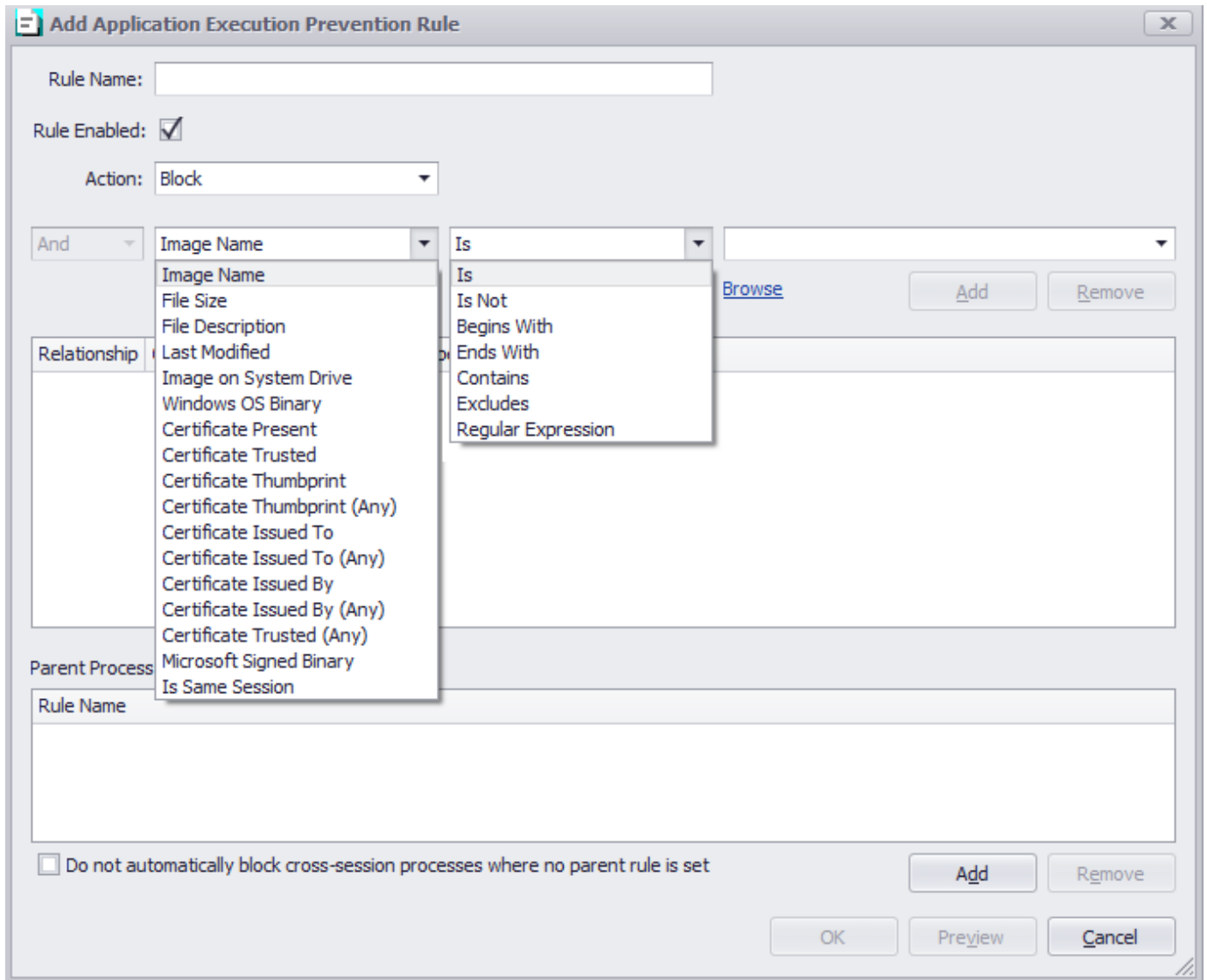
Enable rule logging

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/ Edit Rule Dialog Box



Add Application Execution Prevention Rule

Rule Name:

Rule Enabled: ☒

Action: Block

Relationship: And

Parent Process: Image Name

Rule Name: Is

Image Name
File Size
File Description
Last Modified
Image on System Drive
Windows OS Binary
Certificate Present
Certificate Trusted
Certificate Thumbprint
Certificate Thumbprint (Any)
Certificate Issued To
Certificate Issued To (Any)
Certificate Issued By
Certificate Issued By (Any)
Certificate Trusted (Any)
Microsoft Signed Binary
Is Same Session

[Browse](#) Add Remove

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

Add Remove OK Preview Cancel

Rule Name

Describe the name of the rule to be applied.

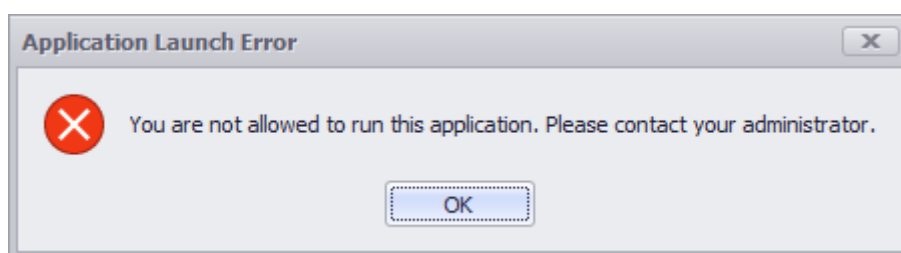
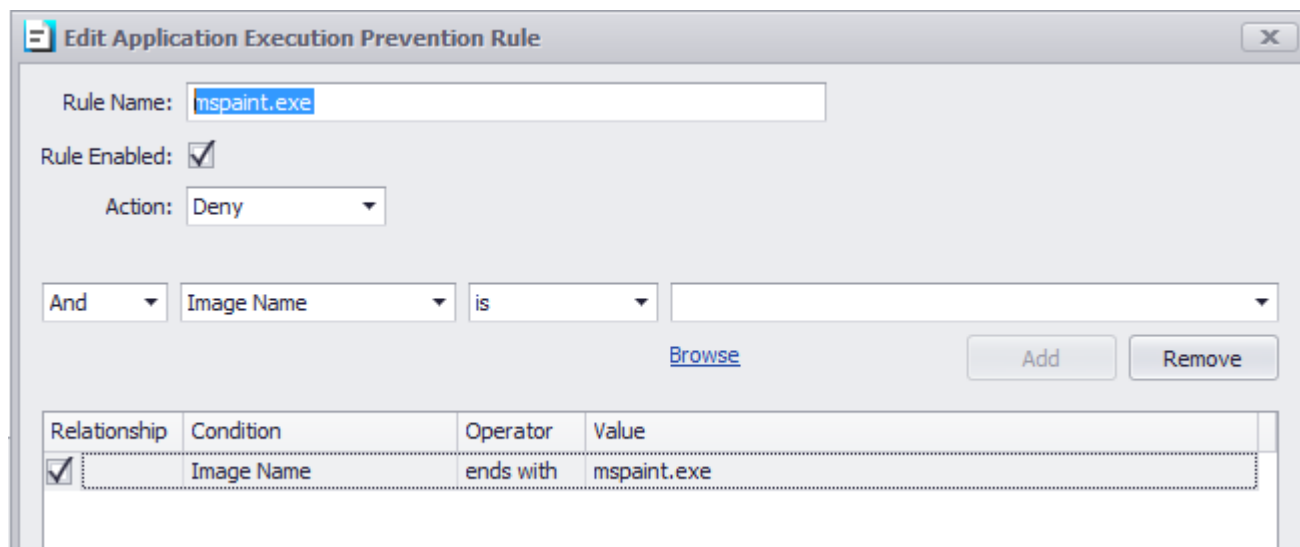
Action

Select “Allow” or “Deny” allowing or denying 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.

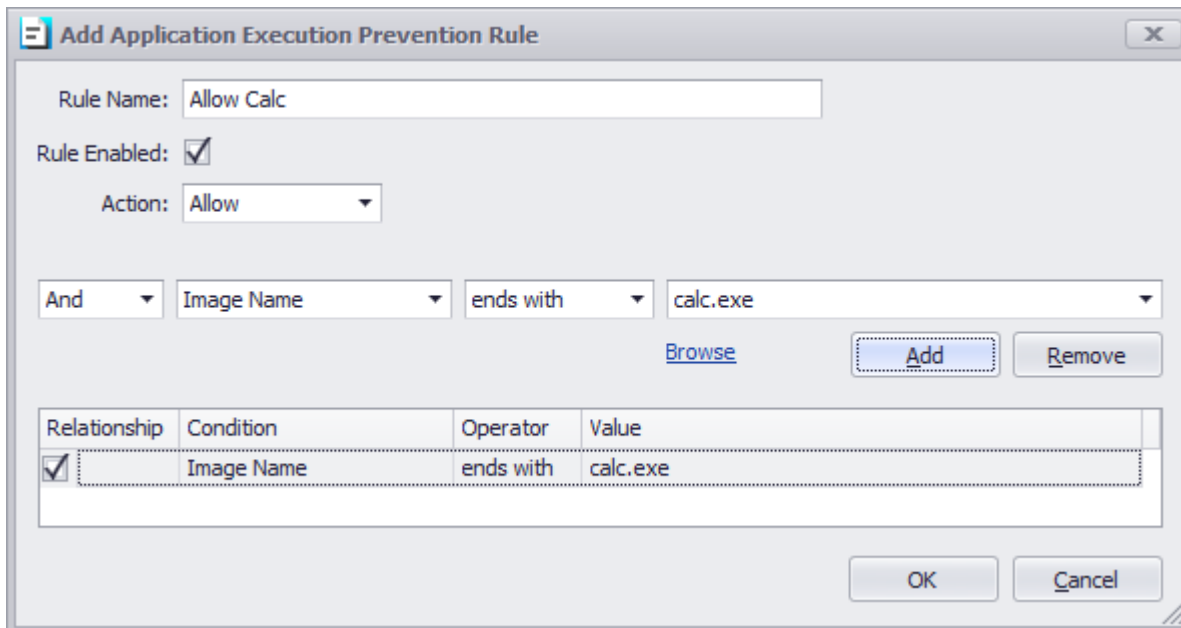
An example of the rule can be seen in the screenshot below. The rule will deny, the locally installed notepad application, from executing. When the user accessing that application will click on the icon, they will be prompted with a dialog message.



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: ☒

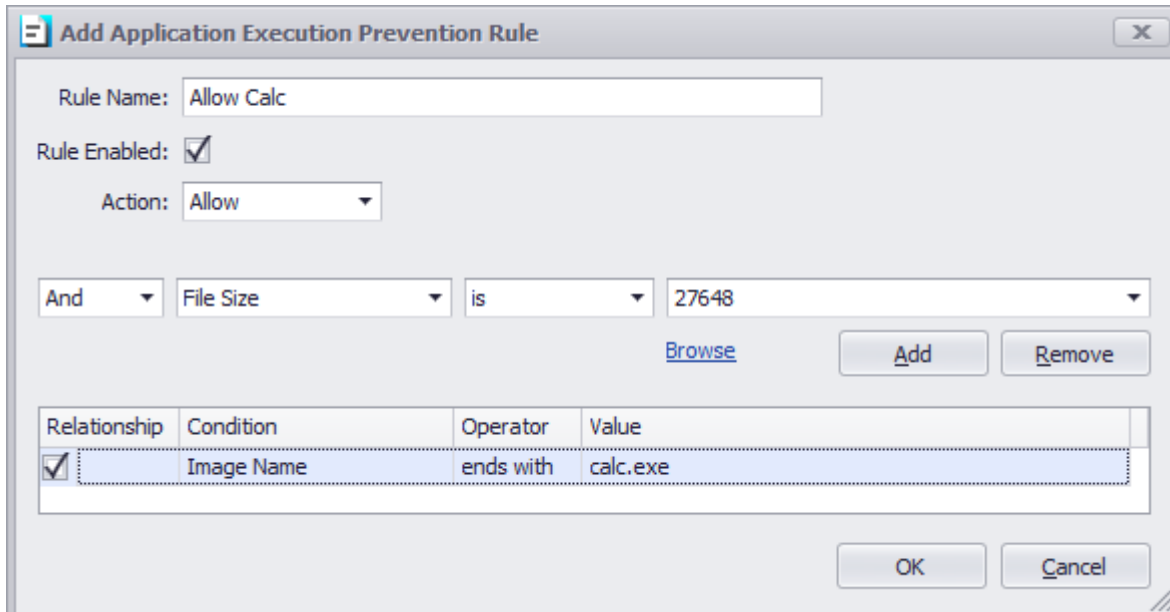
Action:

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:

[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:

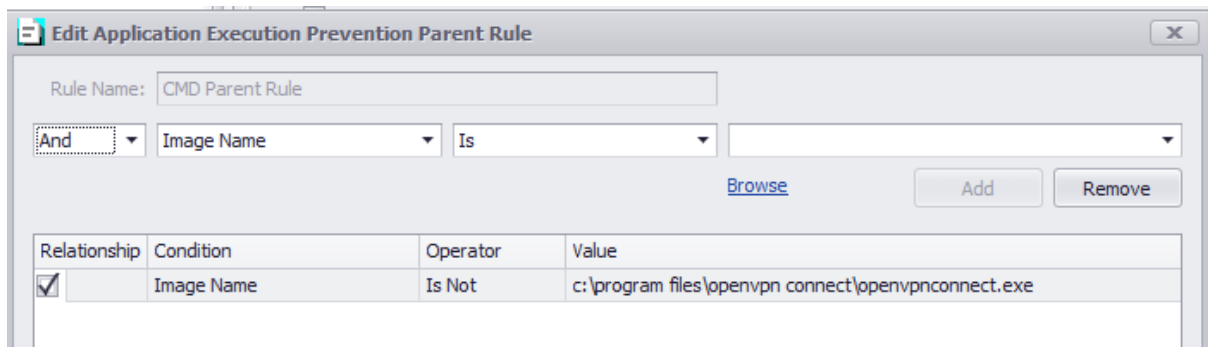
Application Execution Prevention is a system-level function that can prevent a system from operating correctly until the active Secure Remote Worker profile is corrected and reloaded. By default, Secure Remote Worker applications will be allowed once verified by a signed security certificate. Blocking 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 Secure Remote Worker 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 (i.e.: VPN) follow this example:


1- Select the Parent Process



The dialog box is titled "Edit Application Execution Prevention Parent Rule". It contains a "Rule Name" field with the value "CMD Parent Rule". Below this, there is a dropdown menu set to "And", followed by "Image Name" and "Is". To the right of "Is" is a text field and a "Browse" button. Further right are "Add" and "Remove" buttons. At the bottom, there 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

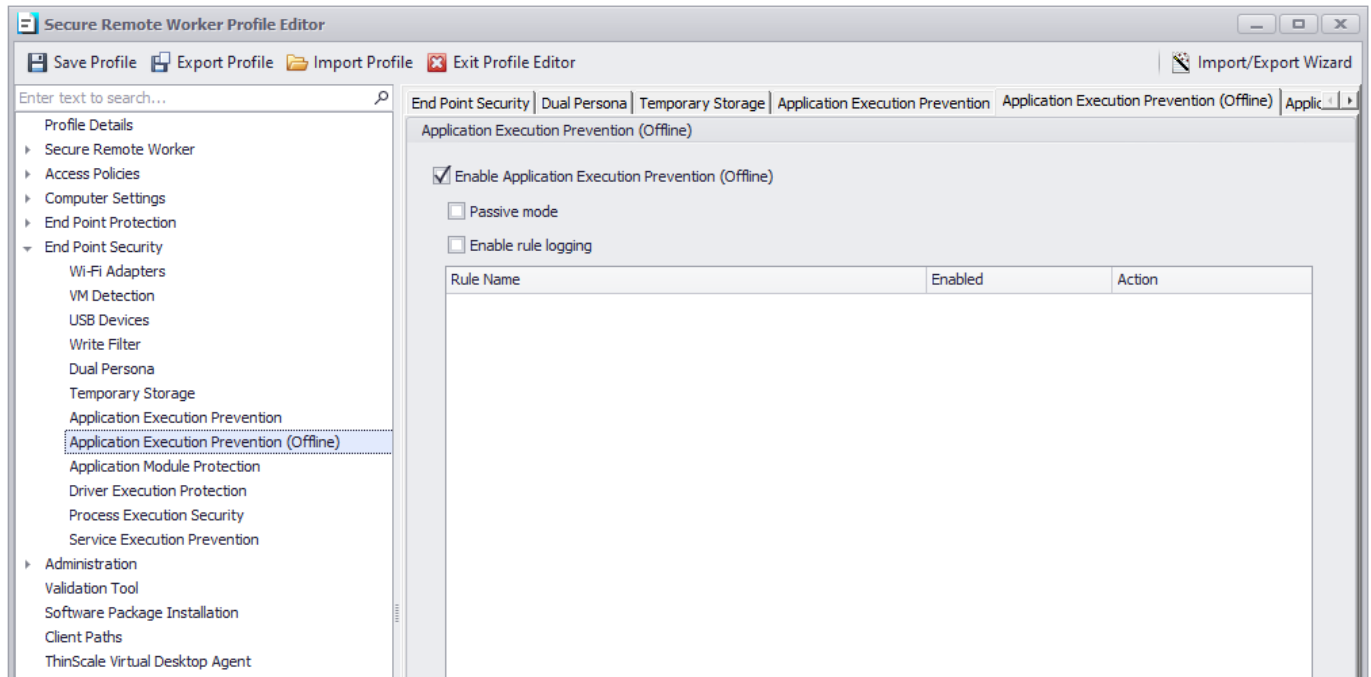


The dialog box is titled "Add Application Execution Prevention Rule". It contains a "Rule Name" field with the value "CMD". Below this, there is a "Rule Enabled" checkbox which is checked. Under "Action", there is a dropdown menu set to "Block". Below this, there is a dropdown menu set to "And", followed by "Image Name" and "Ends With". To the right of "Ends With" is a text field and a "Browse" button. Further right are "Add" and "Remove" buttons. At the bottom, there 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.

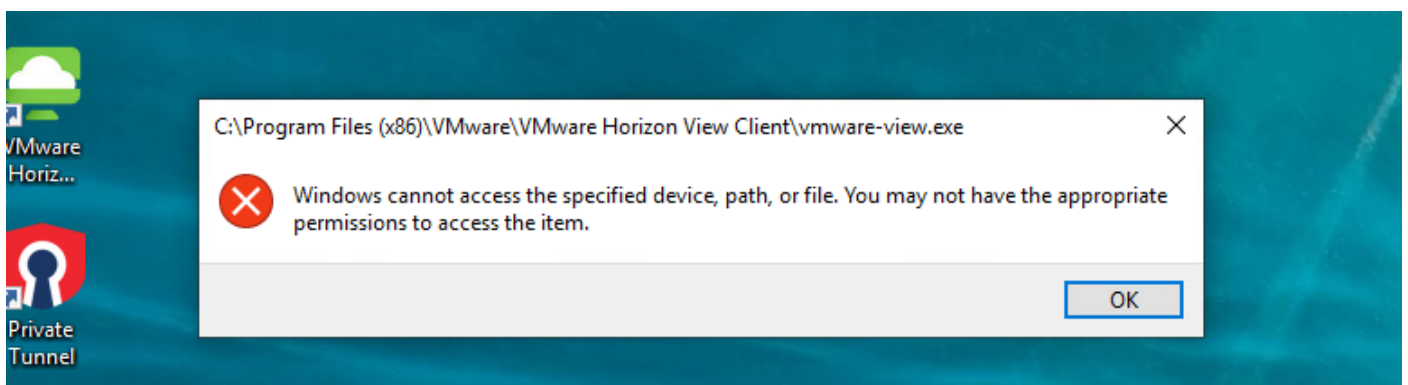
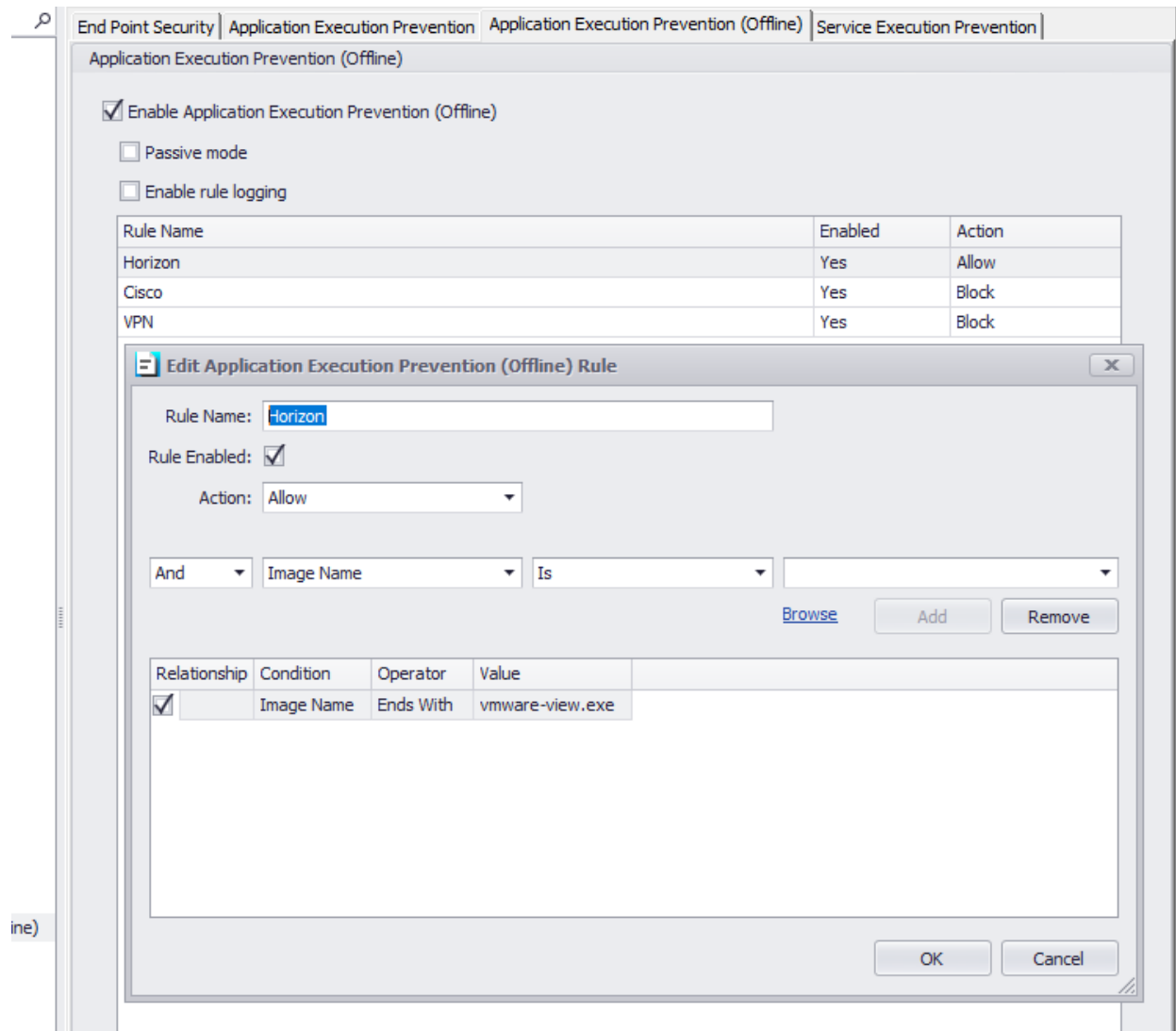
End Point Security - Application Execution Prevention (Offline)



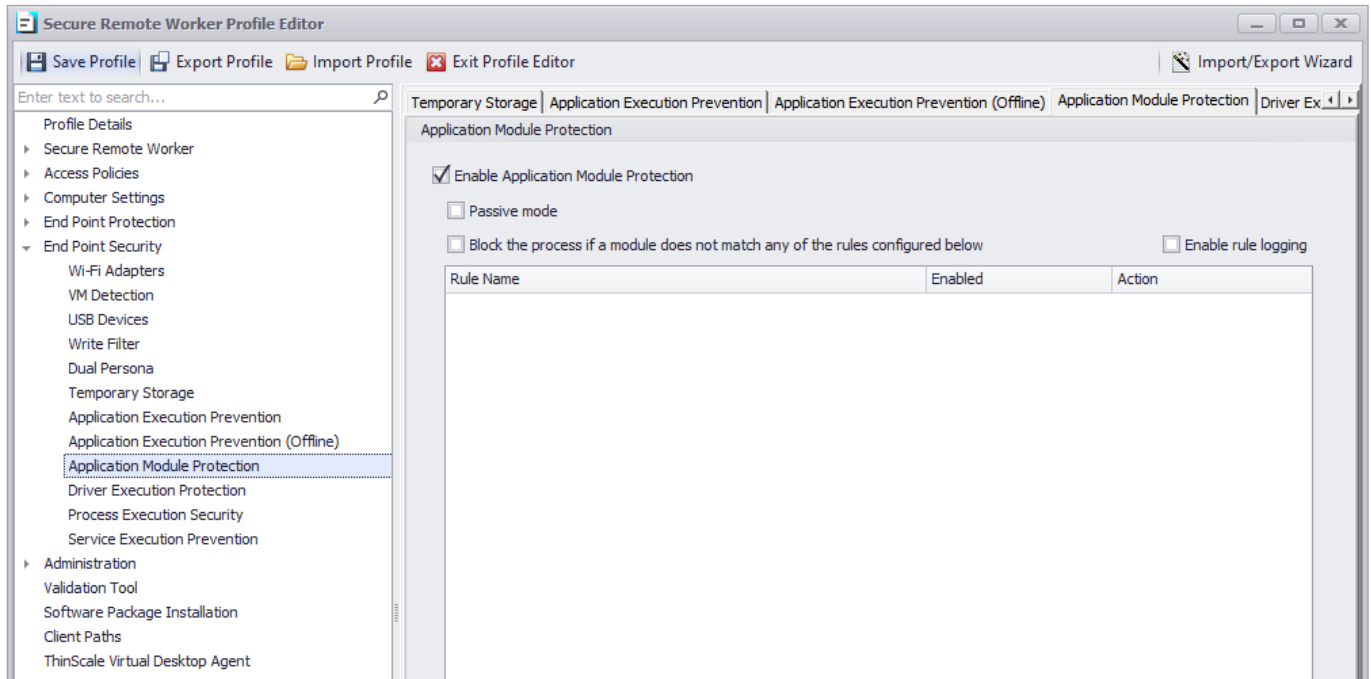
The AEP (Offline) mode is the same as the normal AEP with the only difference that is targeting applications outside the SRW session.

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

Let's see an example rule blocking the Horizon view client when the SRW session is not enabled



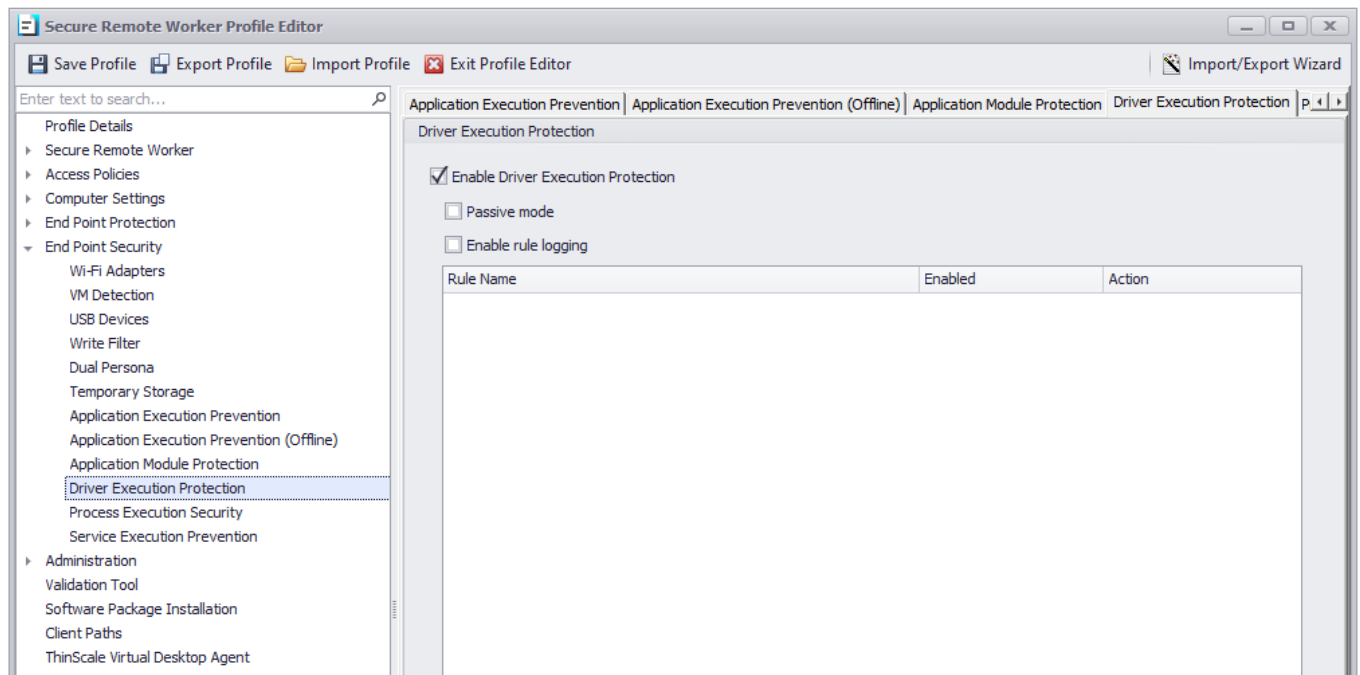
End Point Security - Application Module Protection



Application Module Protection provides control over what application modules (DLL's) are allowed to be loaded by applications running when Secure Remote Worker is active. DLL's can be whitelisted or backlisted giving complete control over what executable code is running within the secure environment.

Should an already allowed executable try to load a module that is not permitted, SRW will terminate the process and optionally log the user out of the Secure Remote Worker session.

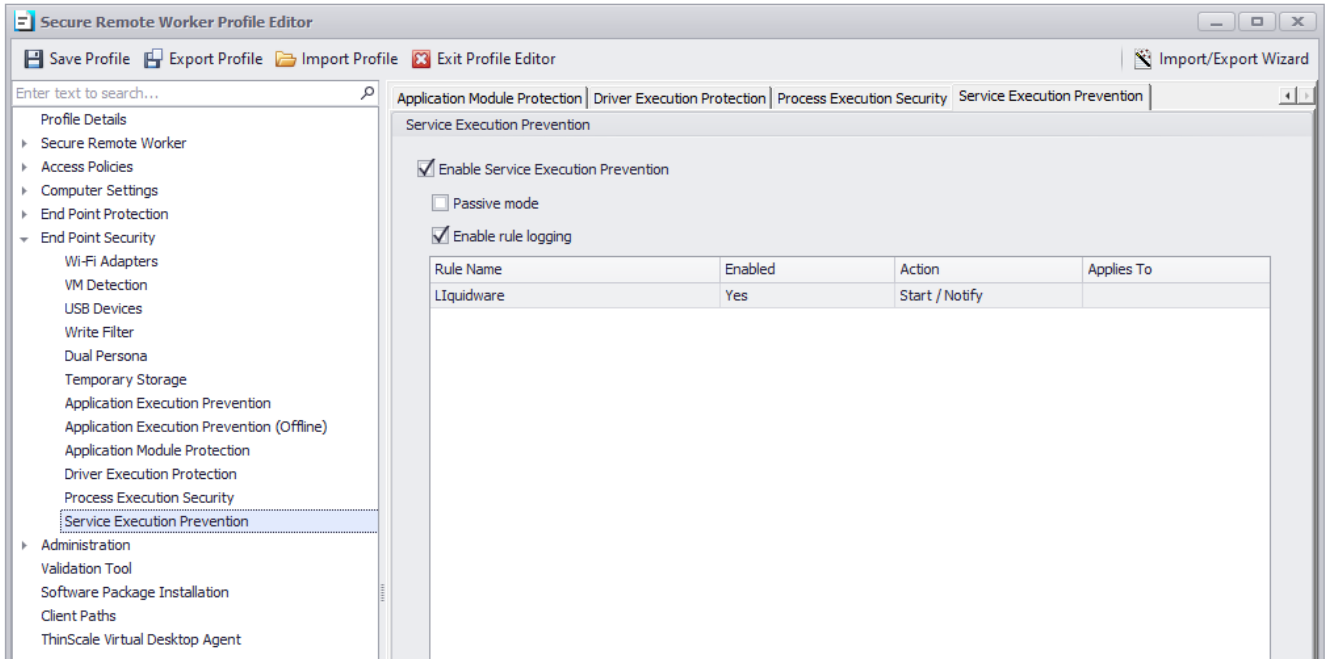
End Point Security – Driver Execution Protection



Driver Execution Protection provides functionality to blacklist Windows drivers.

If a Windows driver, that matches a configured rule, is installed and running on the system, SRW will not run.

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 overall 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 Secure Remote Worker policies are in place.

Service Execution Prevention

Enable Service Execution Prevention

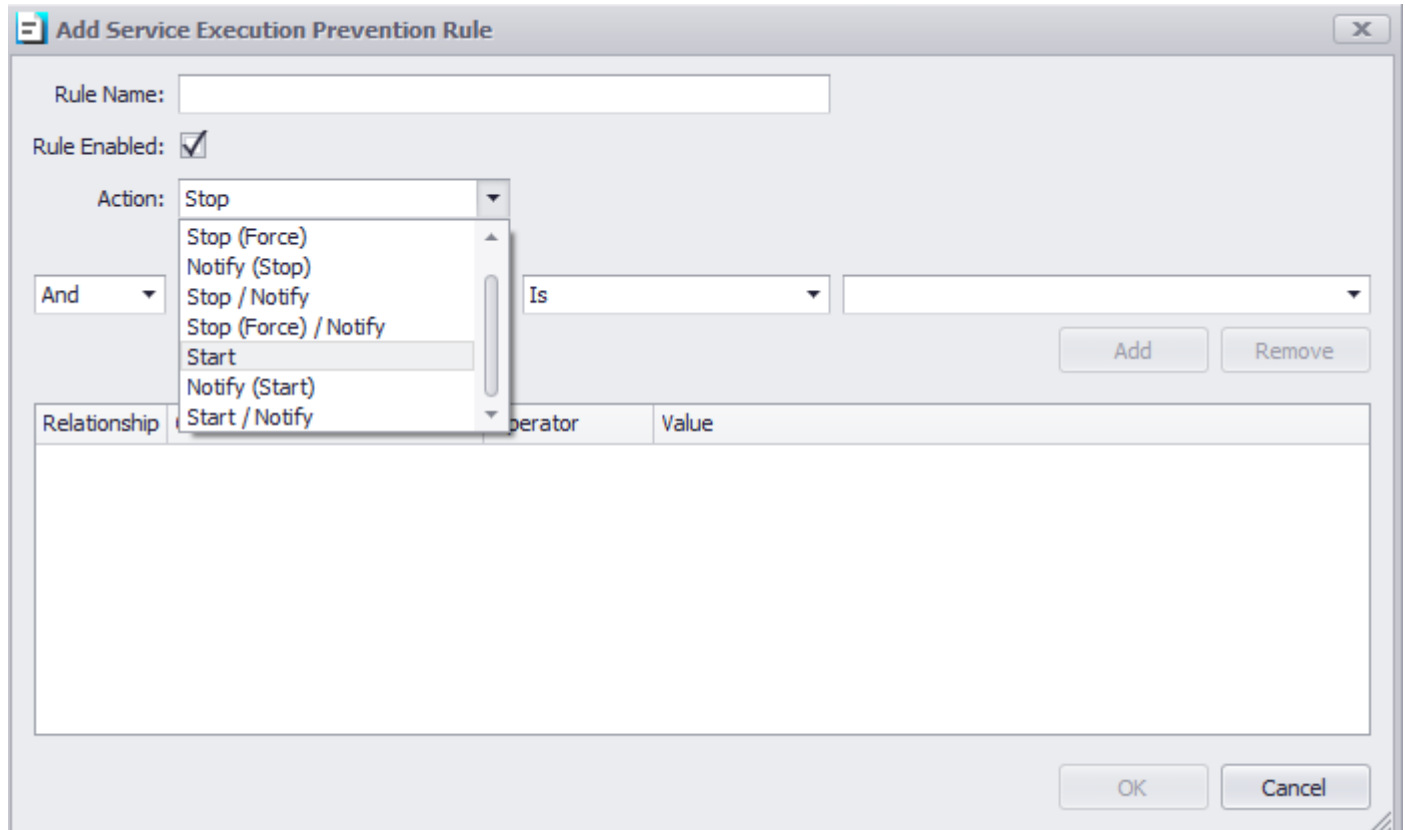
If enabled, SEP real-time monitoring will scan any services that match rules and apply any required actions.

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.



Action setting

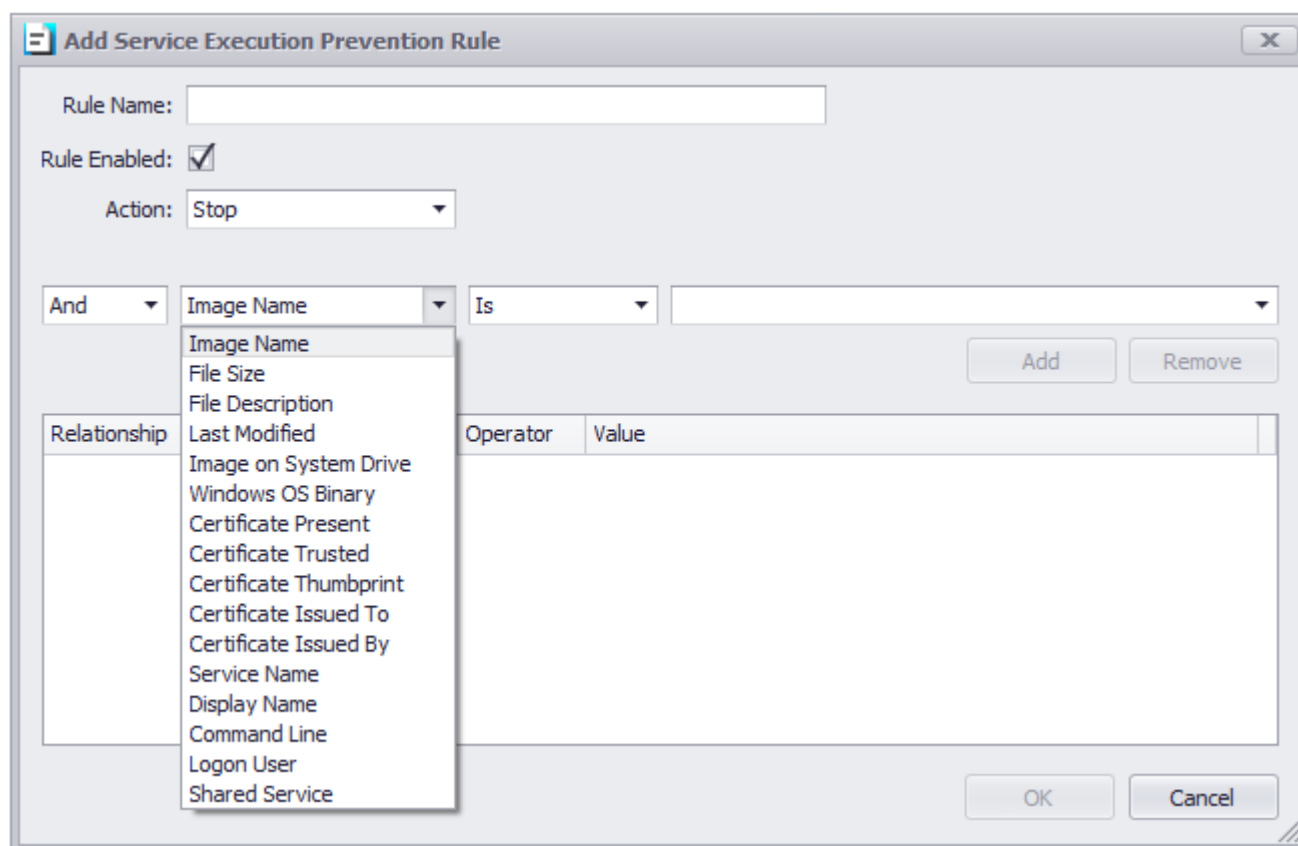
The action setting control how SEP responds to a service should it match a rule. Some action settings may cover multiple actions in which case actions are applied in the following order:

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.

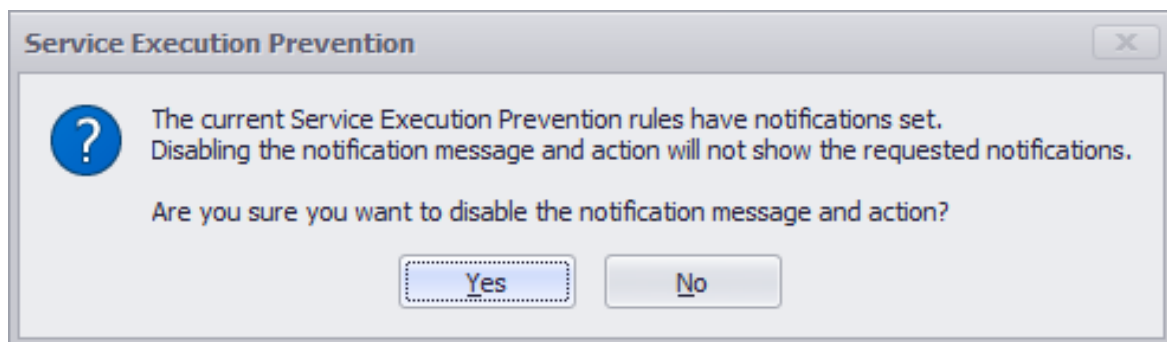
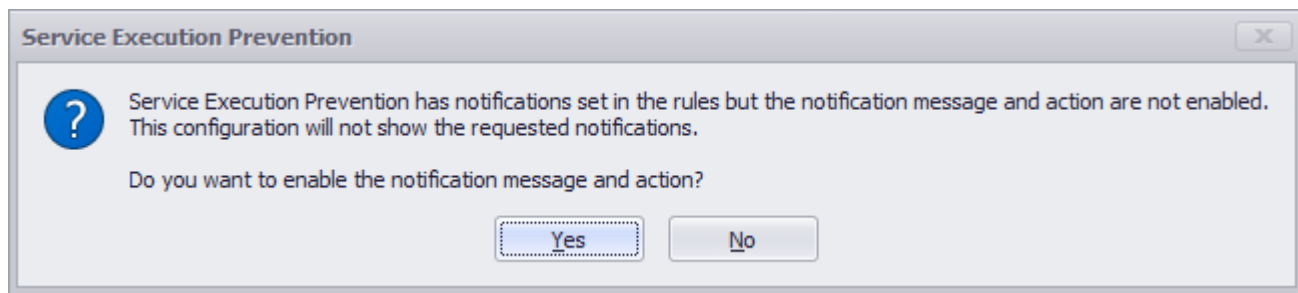


The dialog box titled "Add Service Execution Prevention Rule" contains the following fields and controls:

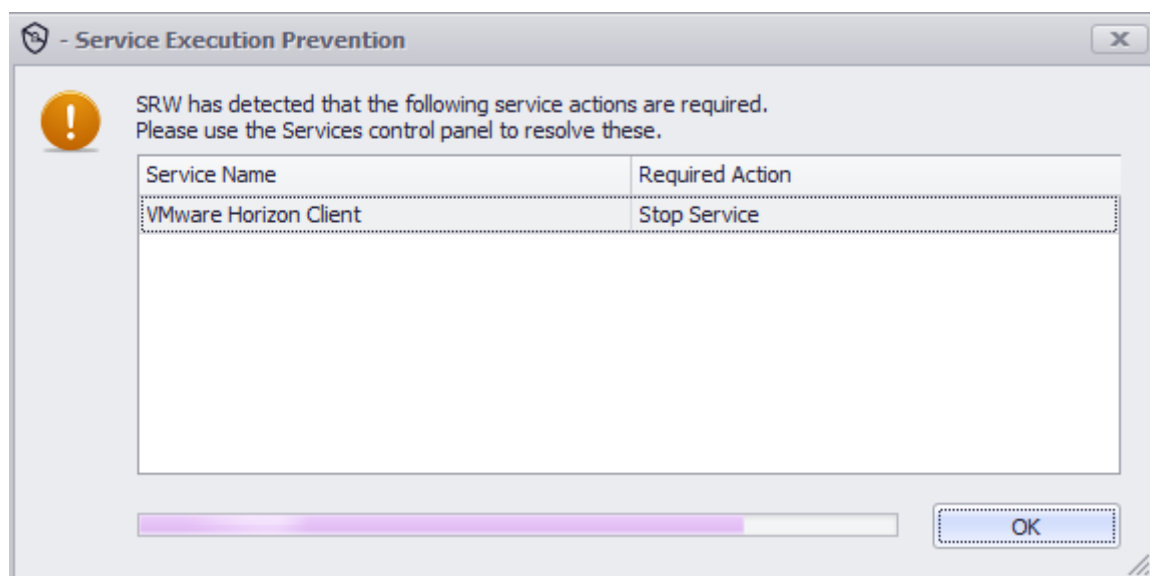
- Rule Name:** A text input field.
- Rule Enabled:** A checkbox, currently checked.
- Action:** A dropdown menu with "Stop" selected.
- Condition Builder:**
 - Relationship:** A dropdown menu with "And" selected.
 - Image Name:** A dropdown menu with a list of available conditions: Image Name, File Size, File Description, Last Modified, Image on System Drive, Windows OS Binary, Certificate Present, Certificate Trusted, Certificate Thumbprint, Certificate Issued To, Certificate Issued By, Service Name, Display Name, Command Line, Logon User, and Shared Service.
 - Is:** A dropdown menu.
 - Value:** A text input field.
 - Buttons:** "Add" and "Remove" buttons are located to the right of the "Is" dropdown.
- Operator/Value Table:** A table with two columns, "Operator" and "Value", for additional conditions.
- Buttons:** "OK" and "Cancel" buttons are at the bottom right.

Service Execution Prevention - User Notifications

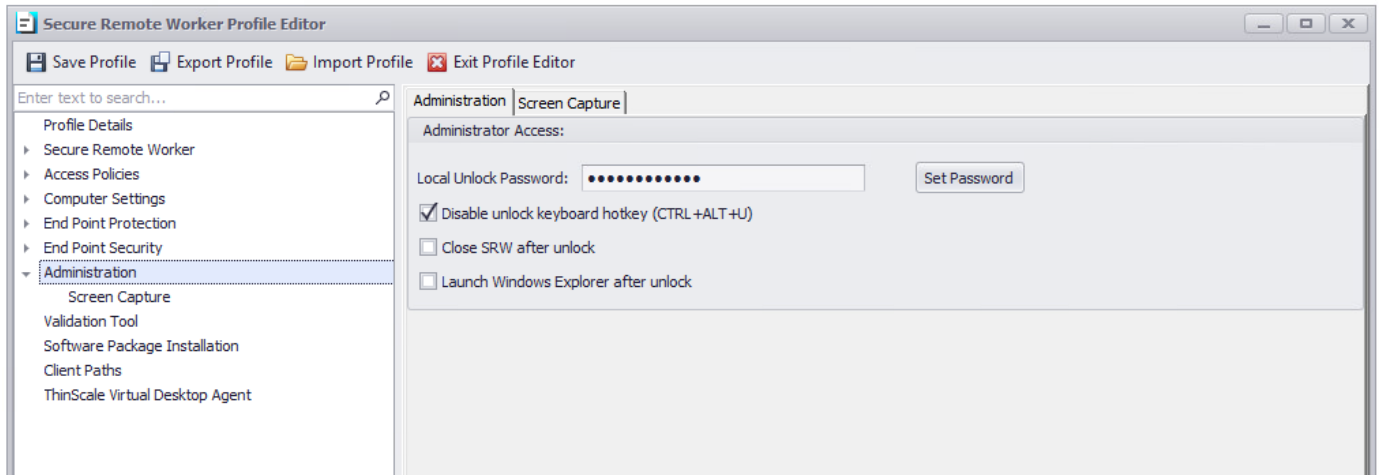
If rules are defined that use the “Notify” action the SEP profile setting for message display should be checked. If this setting is not checked the user will not be presented with any notifications even if rules request it. If the editor detects rules that require notifications one of the following warnings 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 Secure Remote Worker to close – if required this action is performed once the notifications dialog closes.



11. Administration



Administrator Access

Local Unlock Password

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

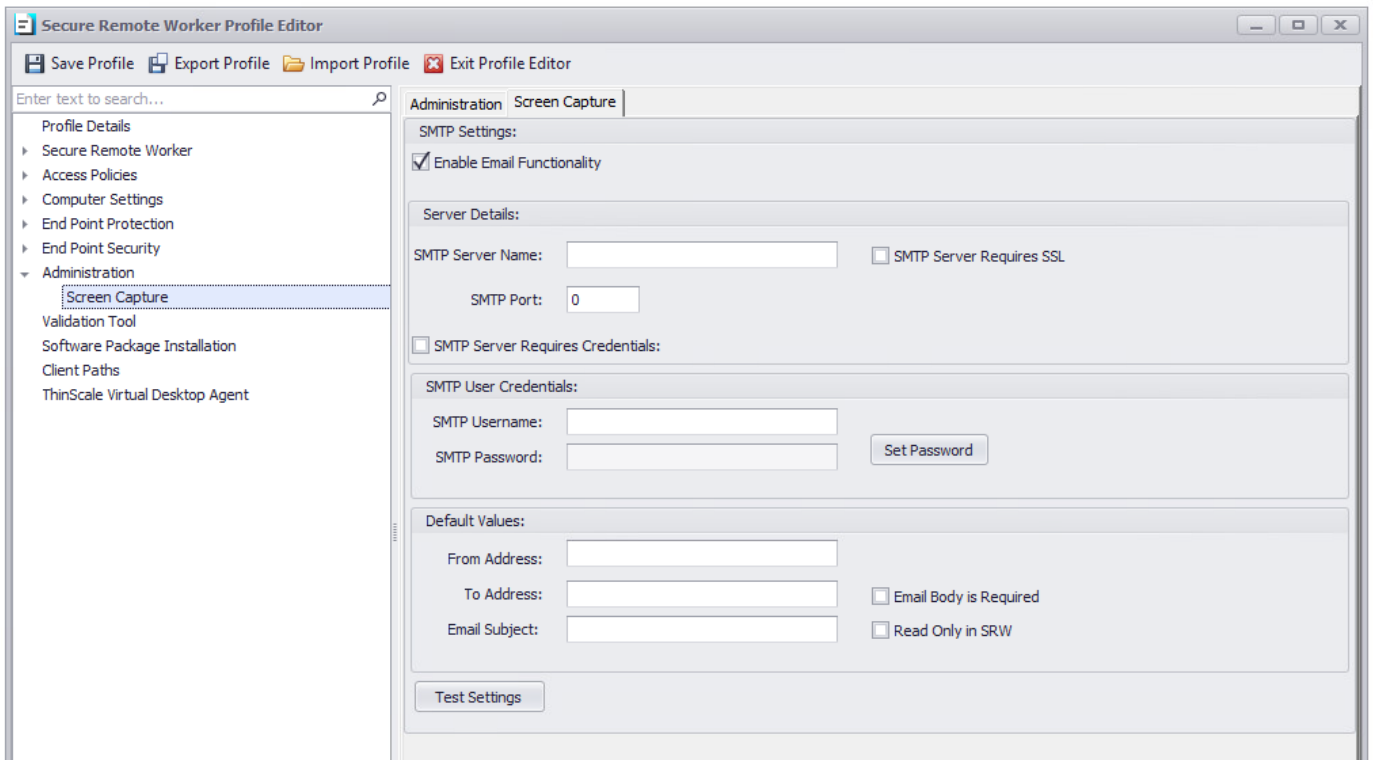
Disable unlock keyboard hotkey (CTRL+ALT+U)

If enabled, users cannot unlock Secure Remote Worker using the CTRL+ALT+U key sequence.

Launch Windows Explorer after an unlock

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

Administration – Screen Capture



Secure Remote Worker Profile Editor

Save Profile Export Profile Import Profile Exit Profile Editor

Enter text to search...

Profile Details

- Secure Remote Worker
- Access Policies
- Computer Settings
- End Point Protection
- End Point Security
- Administration
 - Screen Capture
- Validation Tool
- Software Package Installation
- Client Paths
- ThinScale Virtual Desktop Agent

Administration Screen Capture

SMTP Settings:

☒ Enable Email Functionality

Server Details:

SMTP Server Name: ☐ SMTP Server Requires SSL

SMTP Port:

☐ SMTP Server Requires Credentials:

SMTP User Credentials:

SMTP Username:

SMTP Password: Set Password

Default Values:

From Address:

To Address: ☐ Email Body is Required

Email Subject: ☐ Read Only in SRW

Test Settings

SMTP Settings

Enable Email Functionality

Email functionality is required for the screen-shot option with Secure Remote Worker.

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.

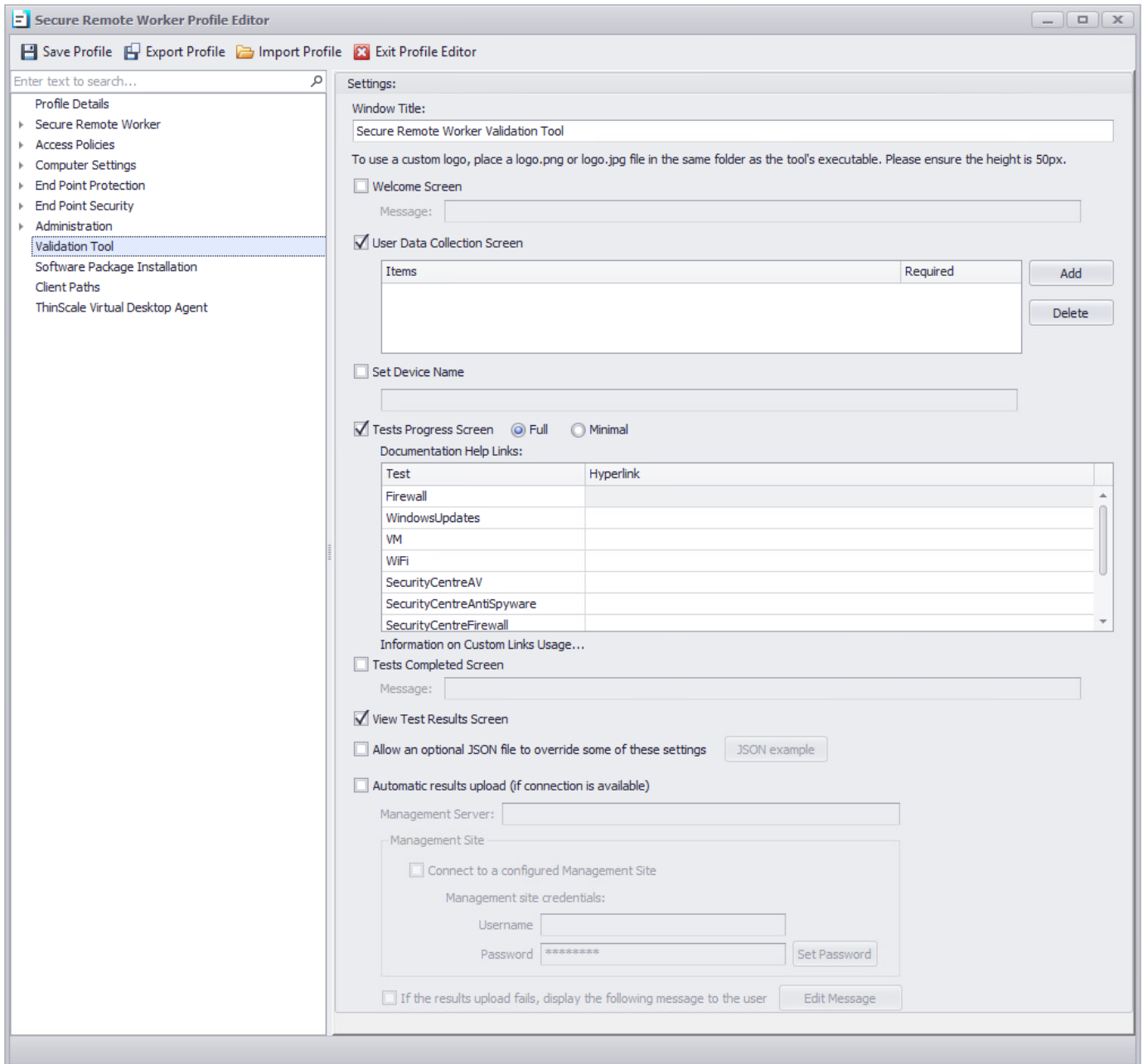
Email Body is required

If enabled, the email's body cannot be empty.

Read Only in Secure Remote Worker

If enabled the Secure Remote Worker user cannot change the default values of "from address", "to address" or "email subject".

12. Validation Tool



The screenshot shows the "Secure Remote Worker Profile Editor" window. The left sidebar lists various profile settings, with "Validation Tool" selected under the "Administration" category. The main area displays the "Settings:" for the "Secure Remote Worker Validation Tool".

Settings:

Window Title: Secure Remote Worker Validation Tool

To use a custom logo, place a logo.png or logo.jpg file in the same folder as the tool's executable. Please ensure the height is 50px.

☐ Welcome Screen

Message:

☒ User Data Collection Screen

Items	Required
<input type="text"/>	<input type="text"/>

☐ Set Device Name

☒ Tests Progress Screen ☒ Full ☐ Minimal

Documentation Help Links:

Test	Hyperlink
Firewall	
WindowsUpdates	
VM	
WiFi	
SecurityCentreAV	
SecurityCentreAntiSpyware	
SecurityCentreFirewall	

Information on Custom Links Usage...

☐ Tests Completed Screen

Message:

☒ View Test Results Screen

☐ Allow an optional JSON file to override some of these settings

☐ Automatic results upload (if connection is available)

Management Server:

Management Site

☐ Connect to a configured Management Site

Management site credentials:

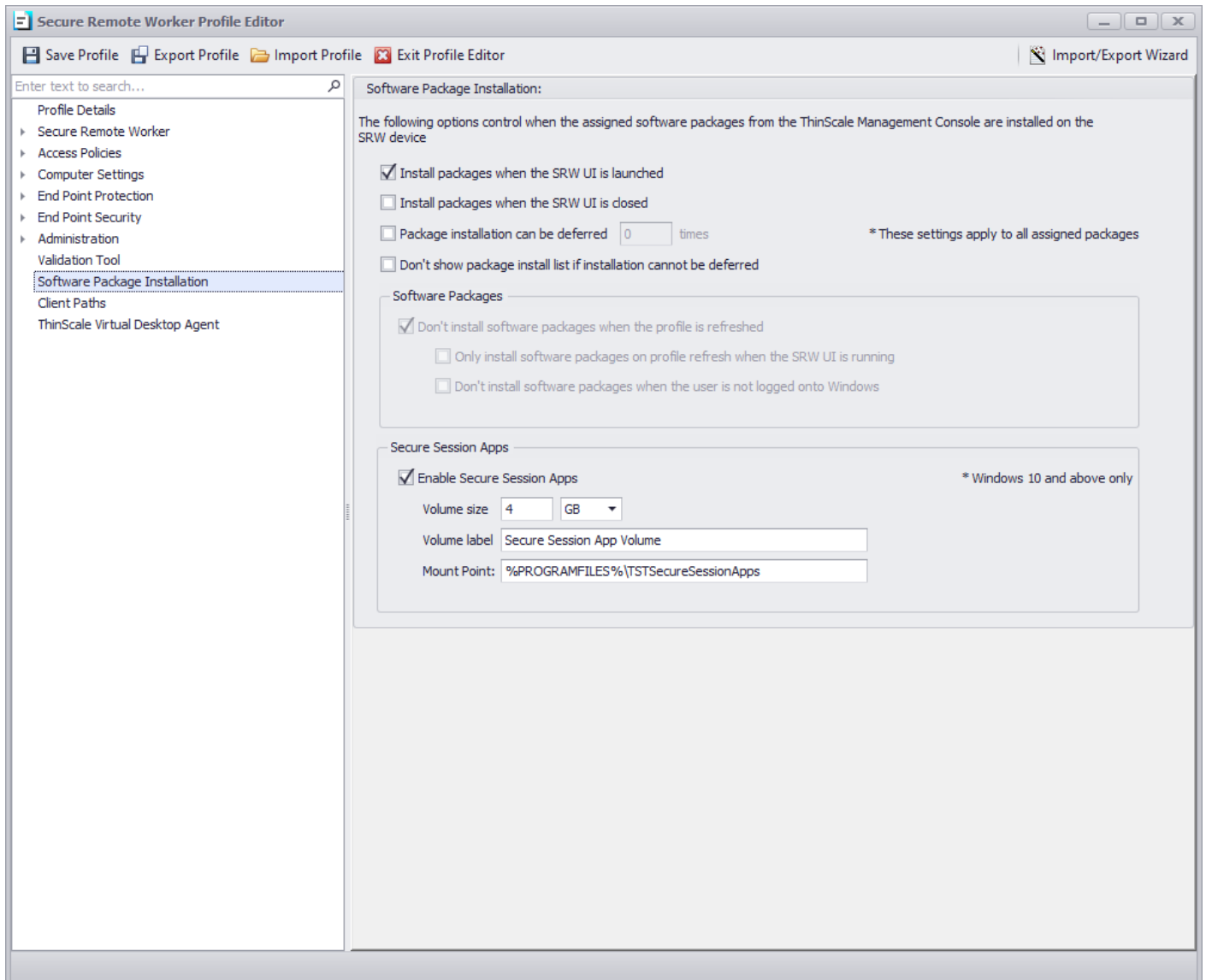
Username

Password

☐ If the results upload fails, display the following message to the user

Please refer to the "Secure Remote Worker Validation Tool" doc for more information.

13. Software Package Installation



The following options will control when software packages will be deployed on the Secure Remote Worker devices

Install software packages when the Secure Remote Worker UI is launched

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

Install software packages when the Secure Remote Worker UI is closed

If enabled, software packages assigned to the folder will be deployed when the Secure Remote Worker 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 Secure Remote Worker 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.

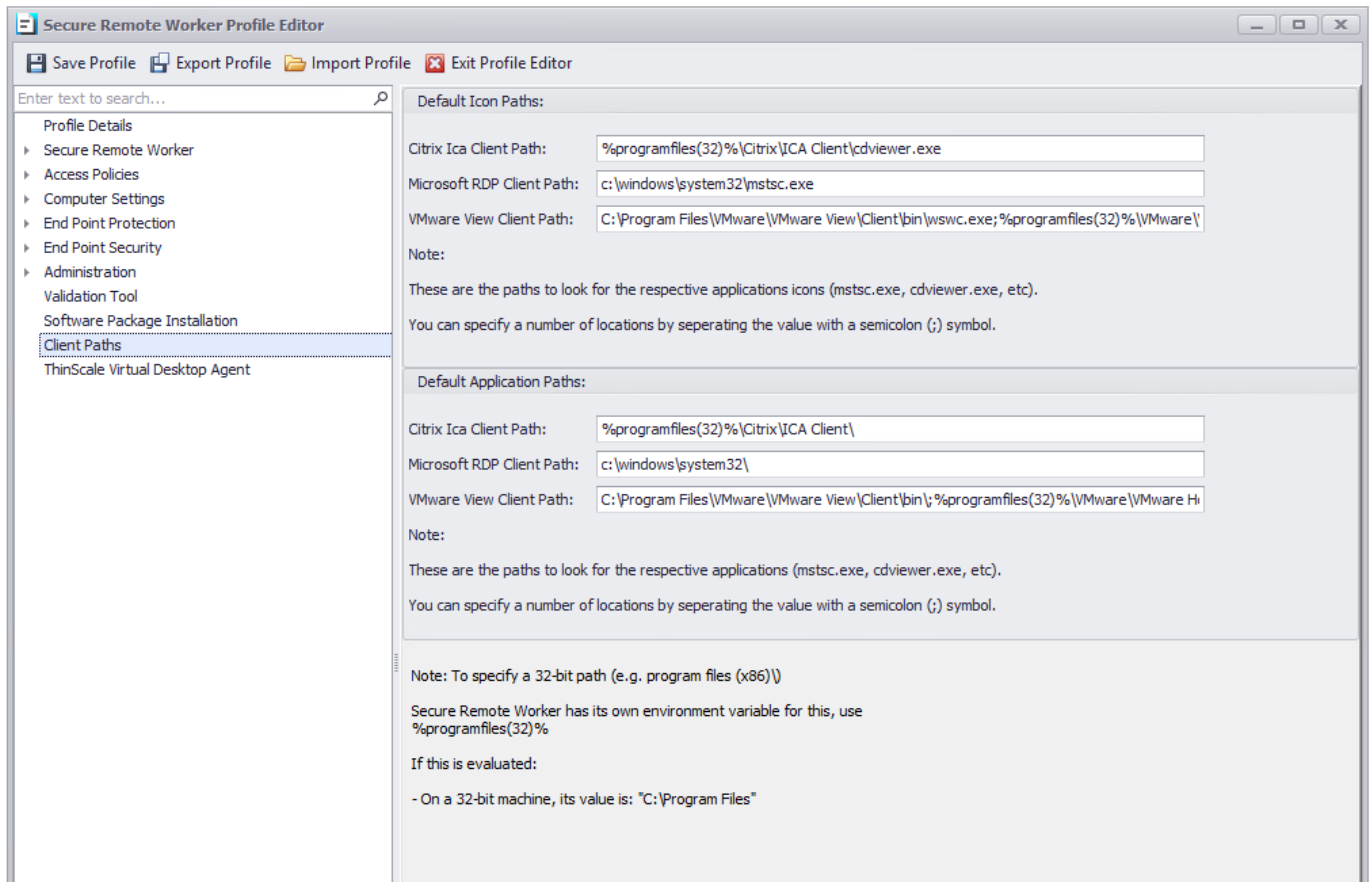
Package installation can be deferred

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

Secure Session Packages

When enabled, this setting will define the size and the mounting point where the new ThinScale Secure Session Apps will be installed.

14. Client Paths



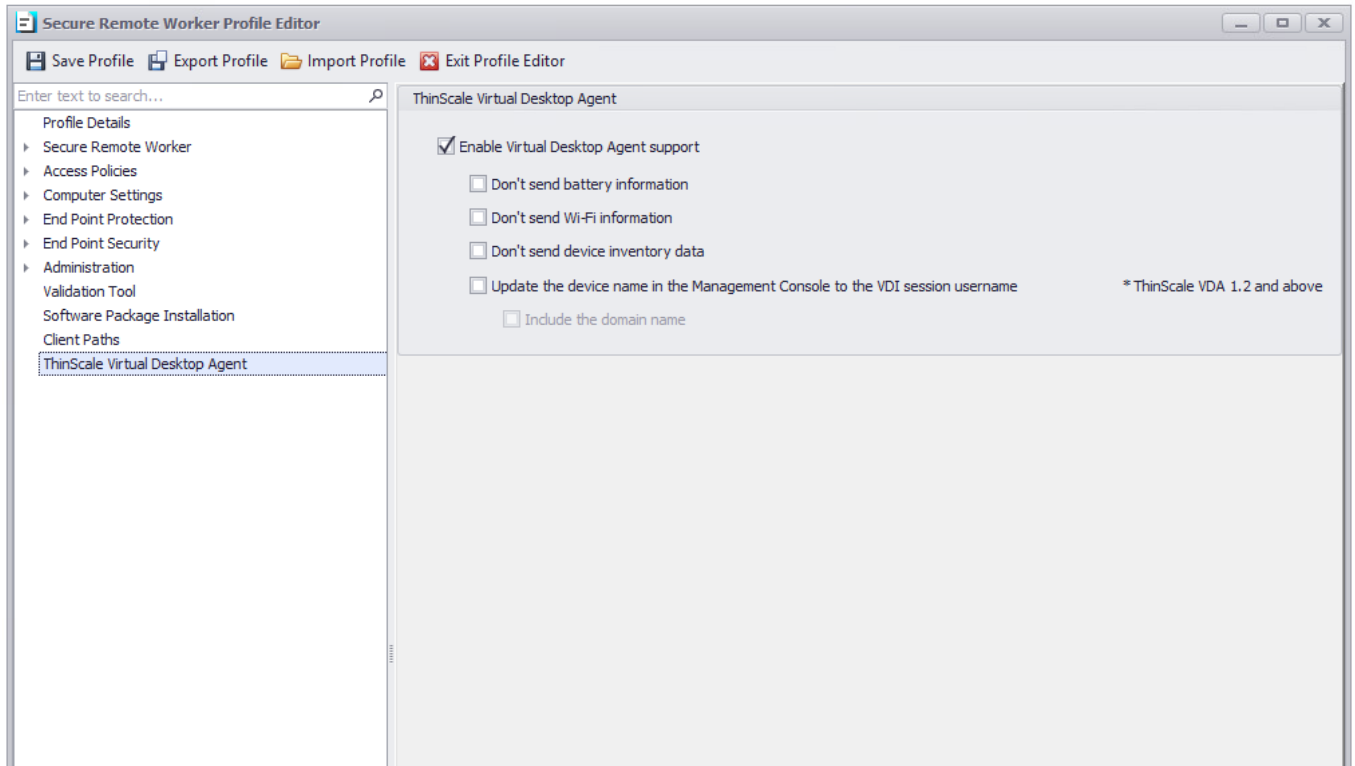
Default Icon Paths

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

Default Application Paths

Locations where Secure Remote Worker will look for the installation of the Citrix, Microsoft, and VMware clients.

15. ThinScale Virtual Desktop Agent



Enable Virtual Desktop Agent support

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