THINSCALE

DESKTOP AGENT

Profile Configuration Guide

WWW.THINSCALE.COM

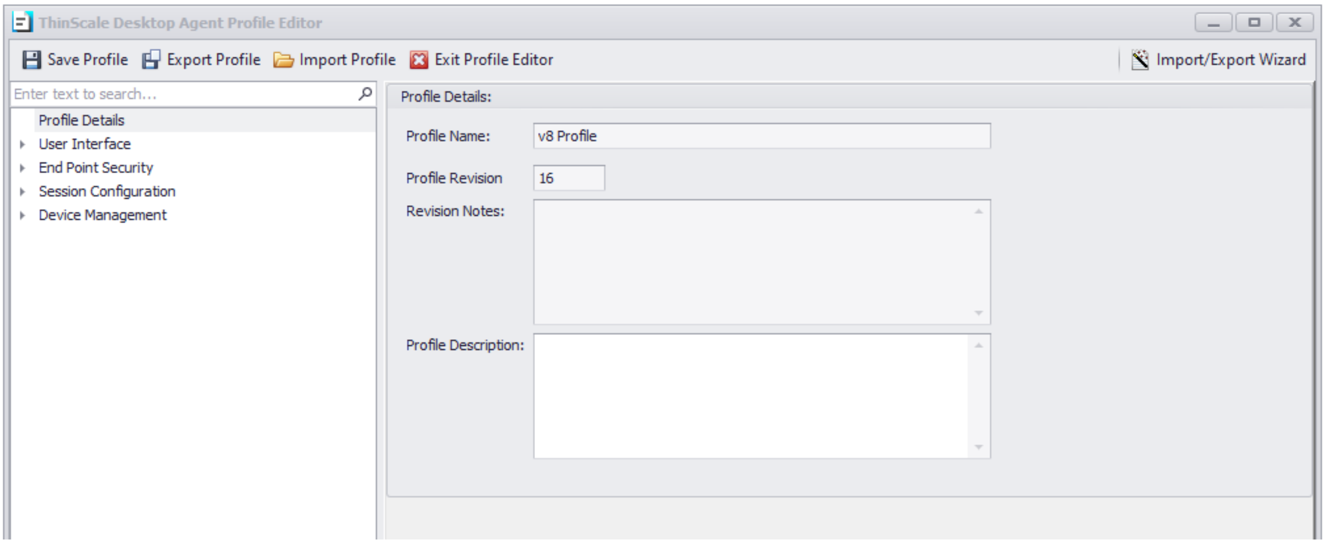
Table of Contents

1. ThinScale Desktop Agent (TDA) Profile Overview

The TDA profile provides all the configurations required for the Desktop Agent client.

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

2. Profile



Profile Details:

Profile Name: v8 Profile

Profile Revision 16

Revision Notes:

Profile Description:

Profile Details

Profile Name

Shows the profile’s name.

Profile Revision

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

Revision Notes

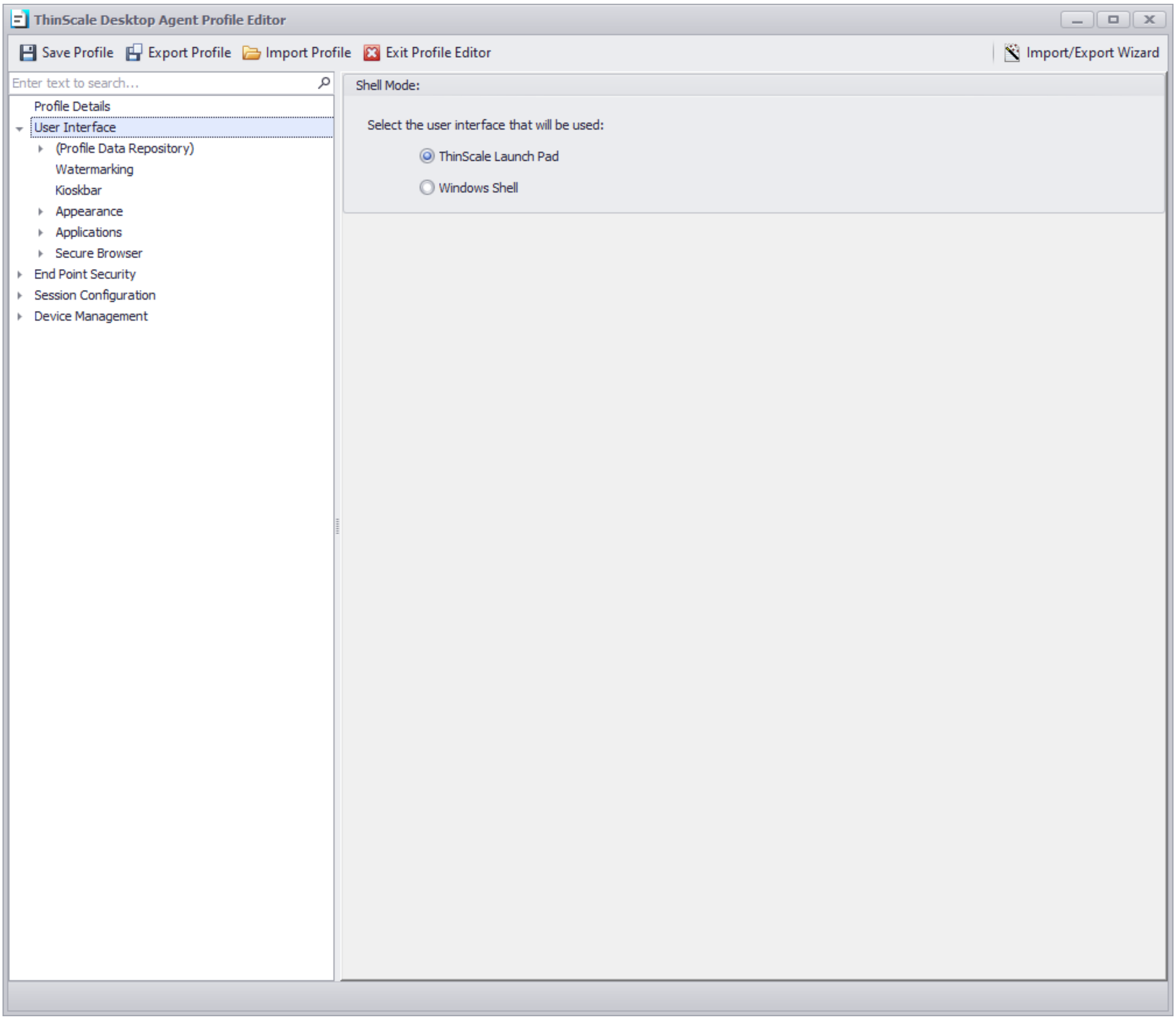
Shows the comments you added when editing a profile.

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. User Interface



Shell Mode:

Select the user interface that will be used:

● ThinScale Launch Pad

○ Windows Shell

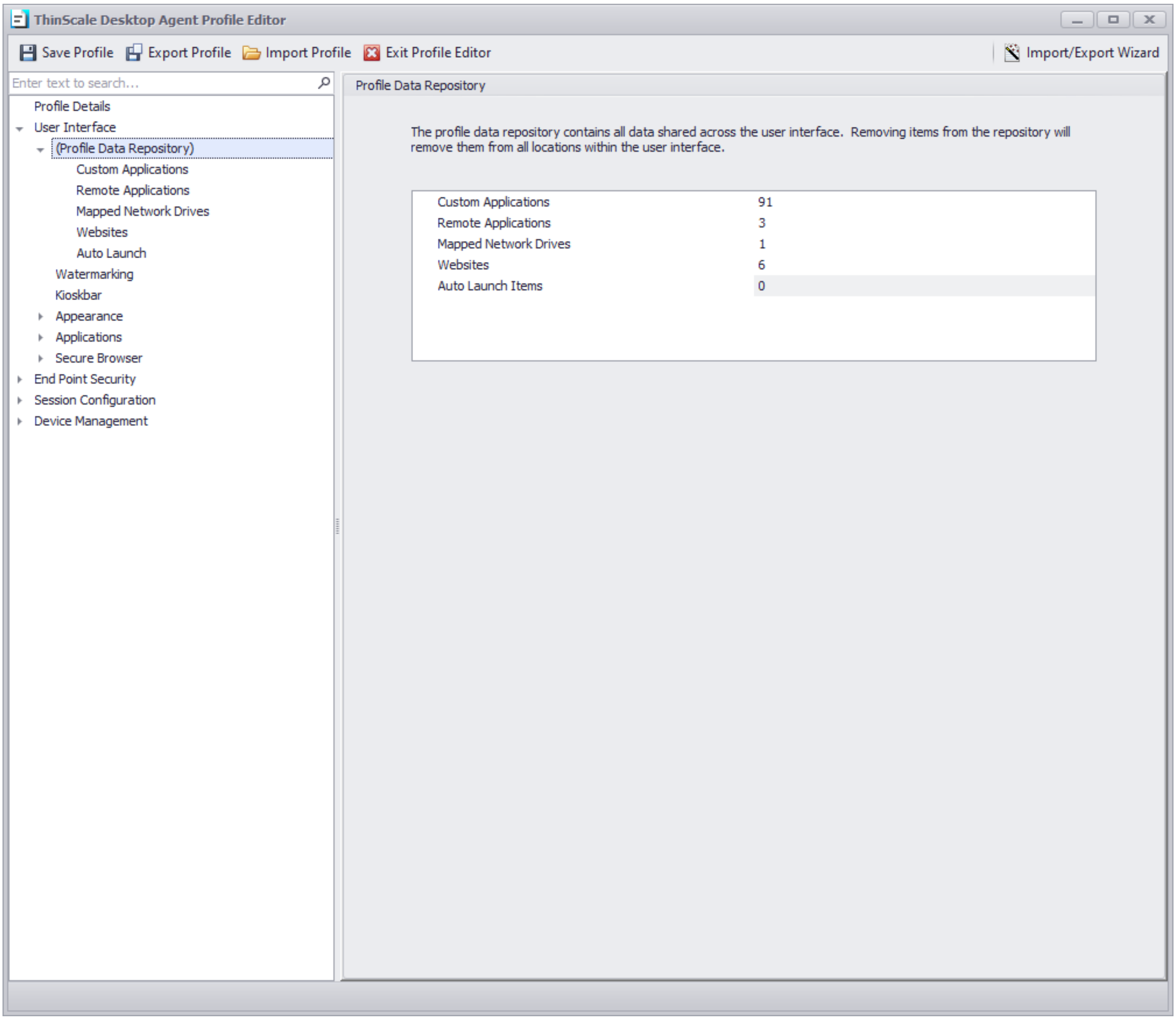
ThinScale Launch Pad

If enabled, TDA will launch its UI and the operating system desktop will be hidden from the user.

Windows Shell

If enabled, TDA will NOT launch its UI, and the user will be able to see their desktop, but in a restricted mode.

User Interface – Profile Data Repository

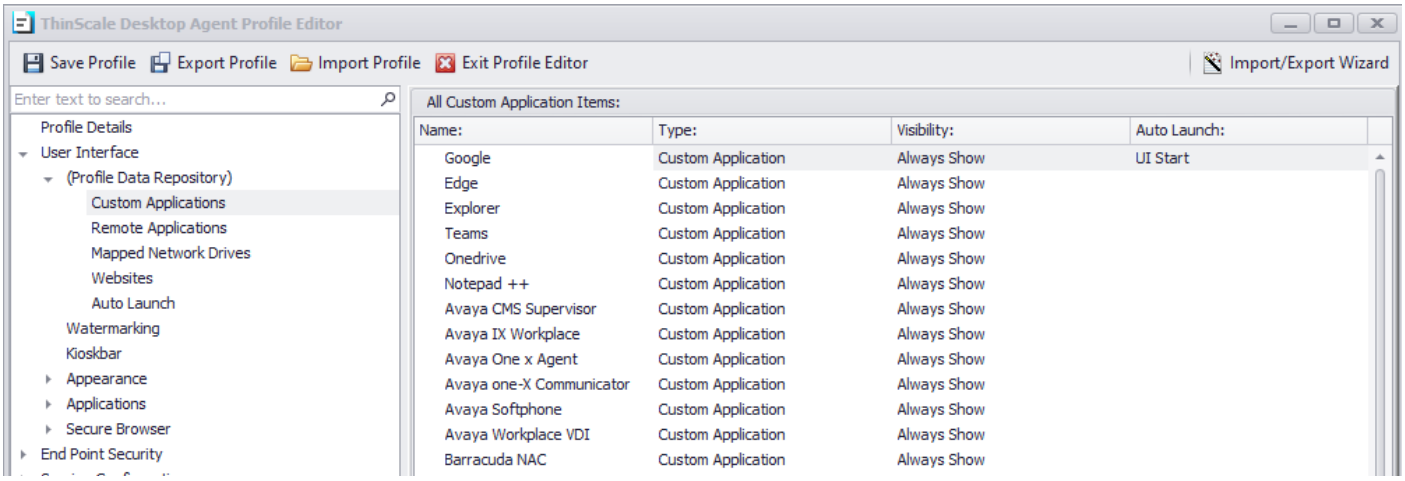


The profile data repository contains all data shared across the user interface. Removing items from the repository will remove them from all locations within the user interface.

Custom Applications	91
Remote Applications	3
Mapped Network Drives	1
Websites	6
Auto Launch Items	0

The profile data repository contains all the custom applications, remote applications, network drive and websites. When an application is set to auto lunch you will also see them here. Removing an application from the repository will also remove it from the Application Desktop Tab.

User Interface – Custom Applications



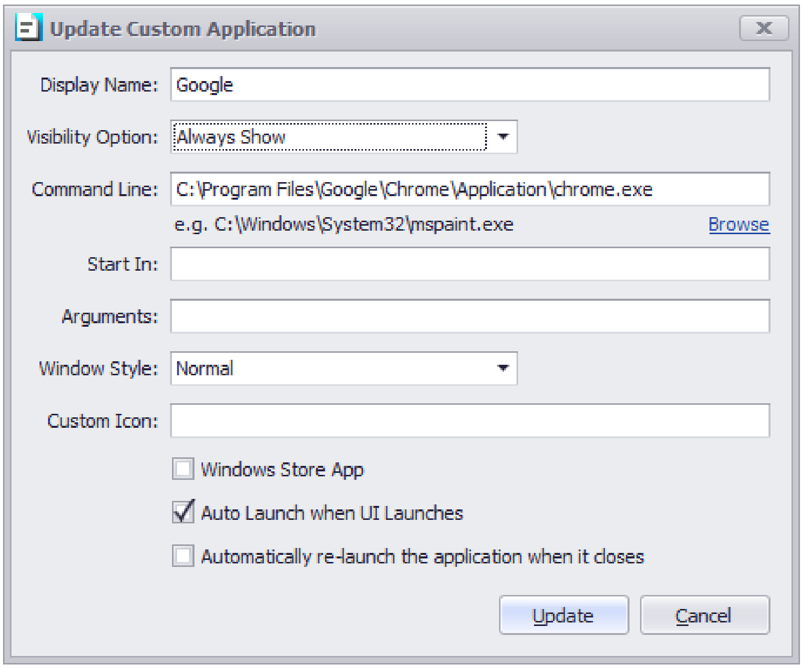
ThinScale Desktop Agent Profile Editor

All Custom Application Items:

Name:	Type:	Visibility:	Auto Launch:
Google	Custom Application	Always Show	UI Start
Edge	Custom Application	Always Show	
Explorer	Custom Application	Always Show	
Teams	Custom Application	Always Show	
Onedrive	Custom Application	Always Show	
Notepad ++	Custom Application	Always Show	
Avaya CMS Supervisor	Custom Application	Always Show	
Avaya IX Workplace	Custom Application	Always Show	
Avaya One x Agent	Custom Application	Always Show	
Avaya one-X Communicator	Custom Application	Always Show	
Avaya Softphone	Custom Application	Always Show	
Avaya Workplace VDI	Custom Application	Always Show	
Barracuda NAC	Custom Application	Always Show	

The Custom Applications Tab is used to setup applications shortcut, that the TDA will display inside its Desktop.

Example Google Chrome



Update Custom Application

Display Name:	Google
Visibility Option:	Always Show
Command Line:	C:\Program Files\Google\Chrome\Application\chrome.exe
	e.g. C:\Windows\System32\mspaint.exe
Start In:	
Arguments:	
Window Style:	Normal
Custom Icon:	

□ Windows Store App

☑ Auto Launch when UI Launches

□ Automatically re-launch the application when it closes

Display Name

The name of the applications will appear on the TDA application tab.

Visibility Option

Location where the application will be displayed.

Command Line

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

Start in

Start in 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.

Windows Store

Only applicable when using a Windows Store App.

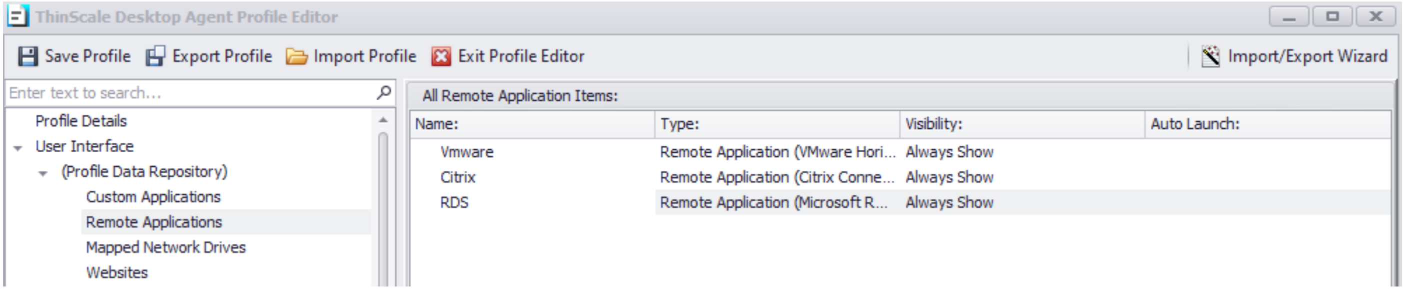
Auto Launch when UI Launches

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

Automatically relaunch the application when it closes

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

User Interface – Remote Applications


ThinScale Desktop Agent Profile Editor

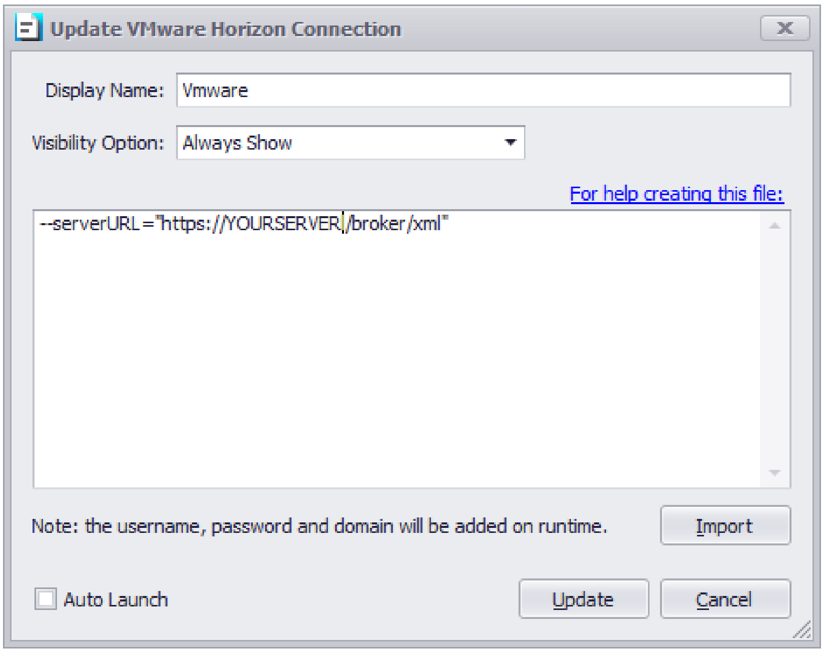
All Remote Application Items:

Name:	Type:	Visibility:	Auto Launch:
Vmware	Remote Application (VMware Hori...	Always Show	
Citrix	Remote Application (Citrix Conne...	Always Show	
RDS	Remote Application (Microsoft R...	Always Show	

Remote Applications are similar to custom applications, but are more related to VDI connection like Citrix/Vmware and Remote Desktop

Remote Applications are being configured in similar manner to custom applications, but they serve for adding VDI connections, such as Citrix, VMware, and Remote Desktop.

Example VMware


Update VMware Horizon Connection

Display Name: Vmware

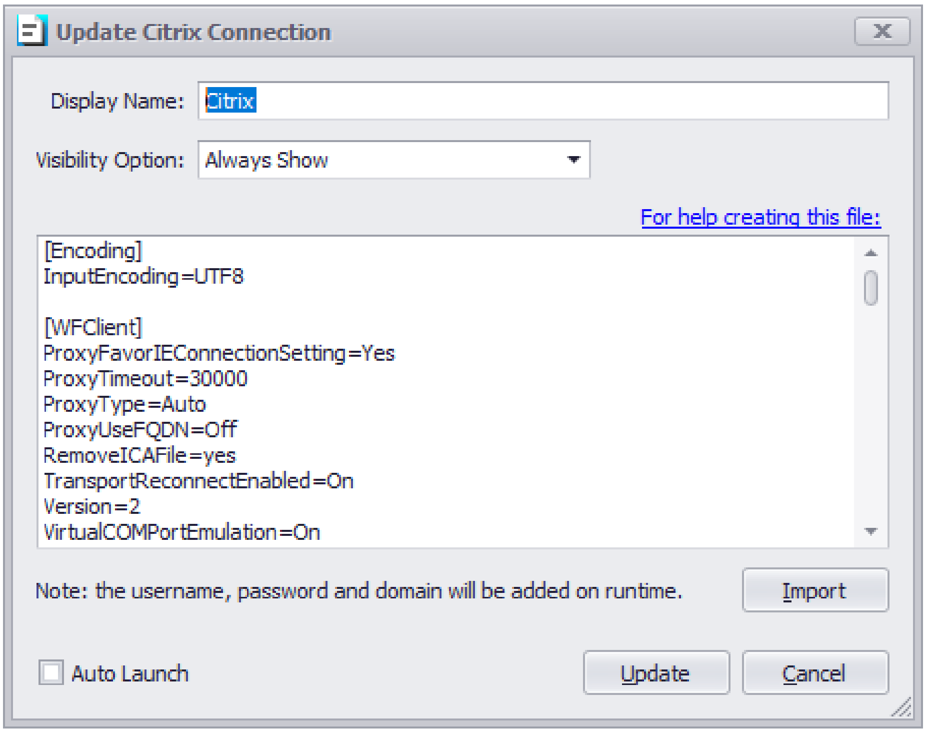
Visibility Option: Always Show

For help creating this file:

```
--serverURL="https://YOURSERVER/broker/xml"
```

Note: the username, password and domain will be added on runtime.

Example Citrix



Display Name: Citrix

Visibility Option: Always Show

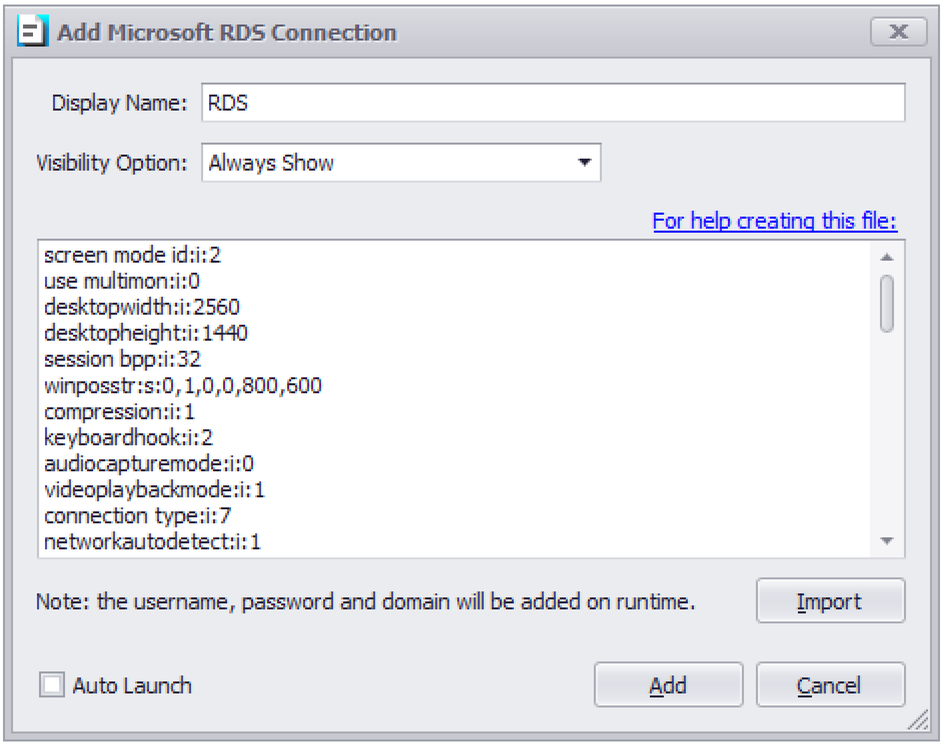
```
[Encoding]
InputEncoding=UTF8

[WFClient]
ProxyFavorIEConnectionSetting=Yes
ProxyTimeout=30000
ProxyType=Auto
ProxyUseFQDN=Off
RemoveICAFile=yes
TransportReconnectEnabled=On
Version=2
VirtualCOMPortEmulation=On
```

Note: the username, password and domain will be added on runtime.

□ Auto Launch

Example RDS



Display Name: RDS

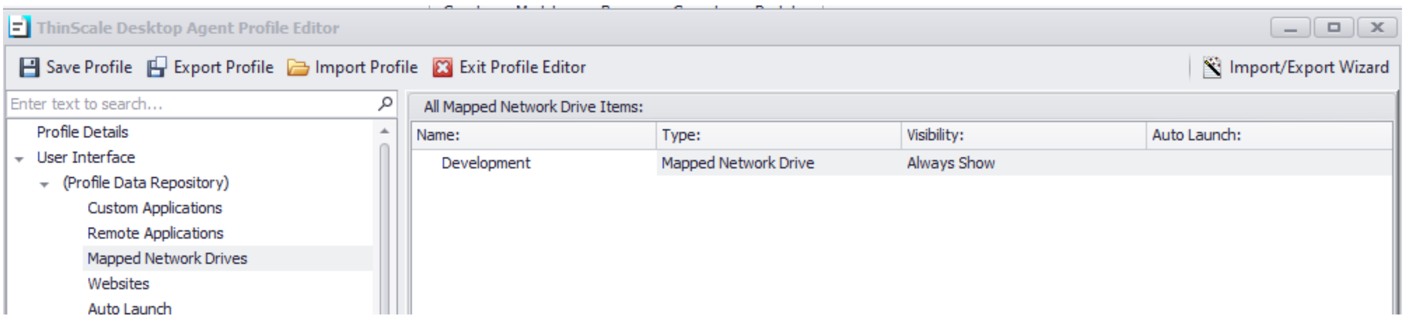
Visibility Option: Always Show

```
screen mode id:i:2
use multimon:i:0
desktopwidth:i:2560
desktopheight:i:1440
session bpp:i:32
winposstr:s:0,1,0,0,800,600
compression:i:1
keyboardhook:i:2
audiocapturemode:i:0
videoplaybackmode:i:1
connection type:i:7
networkautodetect:i:1
```

Note: the username, password and domain will be added on runtime.

□ Auto Launch

User Interface – Mapped Networks Drives



ThinScale Desktop Agent Profile Editor

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

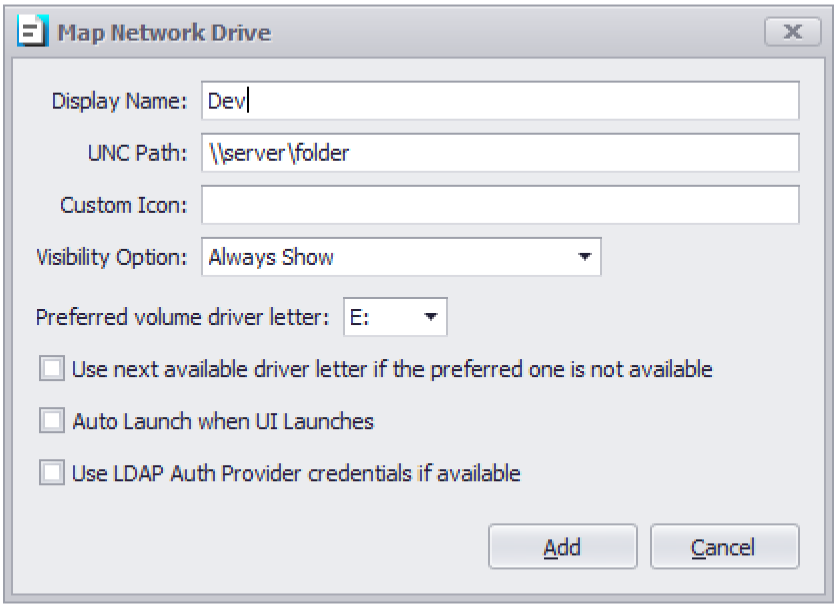
Enter text to search...

- Profile Details
- User Interface
  - (Profile Data Repository)
    - Custom Applications
    - Remote Applications
    - Mapped Network Drives
    - Websites
    - Auto Launch

All Mapped Network Drive Items:

Name:	Type:	Visibility:	Auto Launch:
Development	Mapped Network Drive	Always Show	

Example Drive



Map Network Drive

Display Name: Dev

UNC Path: \\server\folder

Custom Icon:

Visibility Option: Always Show

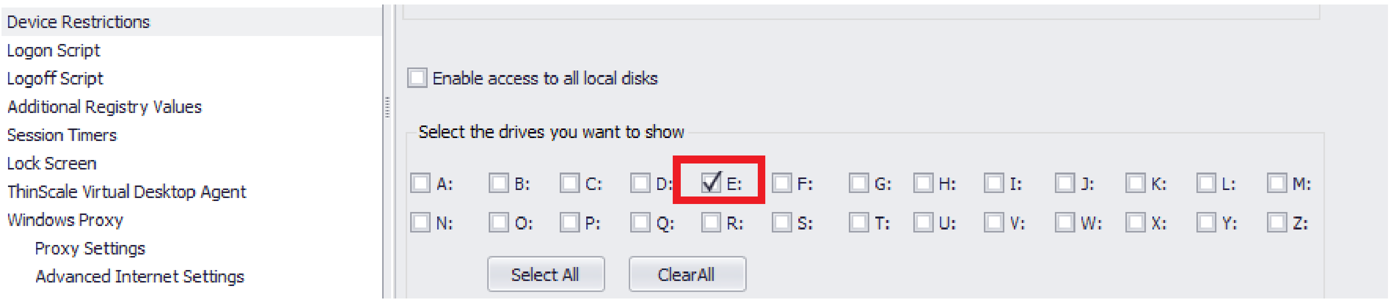
Preferred volume driver letter: E:

□ Use next available driver letter if the preferred one is not available

□ Auto Launch when UI Launches

□ Use LDAP Auth Provider credentials if available

Note: make sure to also allow the letter in the Session Configuration > Device Restrictions



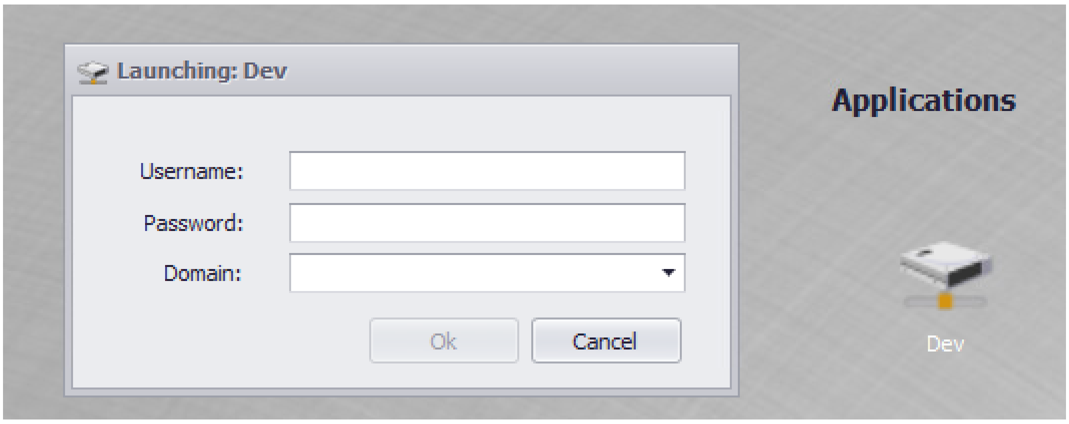
- Device Restrictions
- Logon Script
- Logoff Script
- Additional Registry Values
- Session Timers
- Lock Screen
- ThinScale Virtual Desktop Agent
- Windows Proxy
  - Proxy Settings
  - Advanced Internet Settings

□ Enable access to all local disks

Select the drives you want to show

□ A: □ B: □ C: □ D: ☑ E: □ F: □ G: □ H: □ I: □ J: □ K: □ L: □ M:

□ N: □ O: □ P: □ Q: □ R: □ S: □ T: □ U: □ V: □ W: □ X: □ Y: □ Z:



Display Name

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

UNC Path

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

Custom Icon

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

Visibility Option

Location where the application will be displayed.

Use next available drive letter

If enabled, the drive letter will be decided based on the availability on the user’s PC.

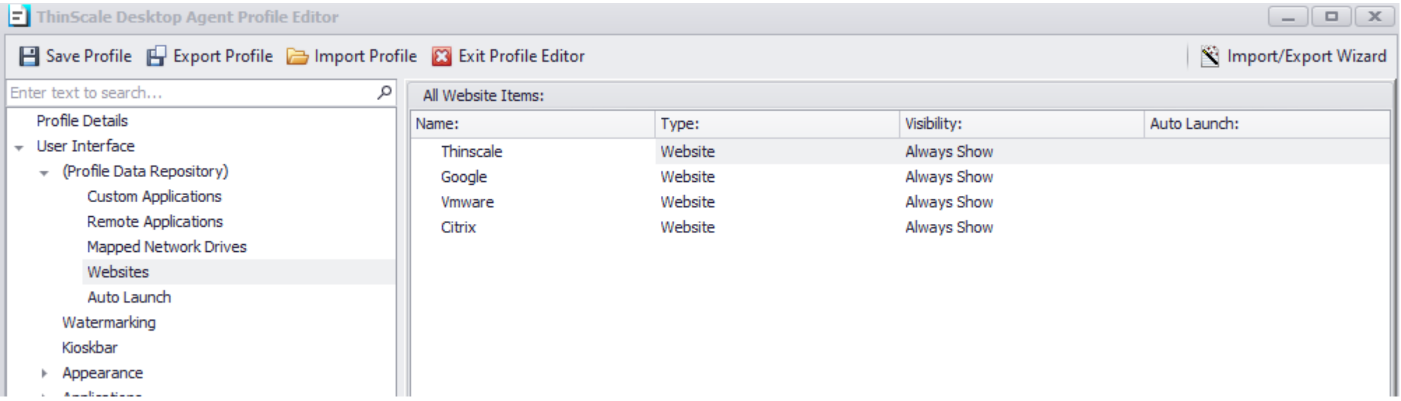
Auto Launch when UI Launches

If enabled, the drive will automatically launch at TDA UI launch.

Use LDAP Auth Provider credentials if available

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

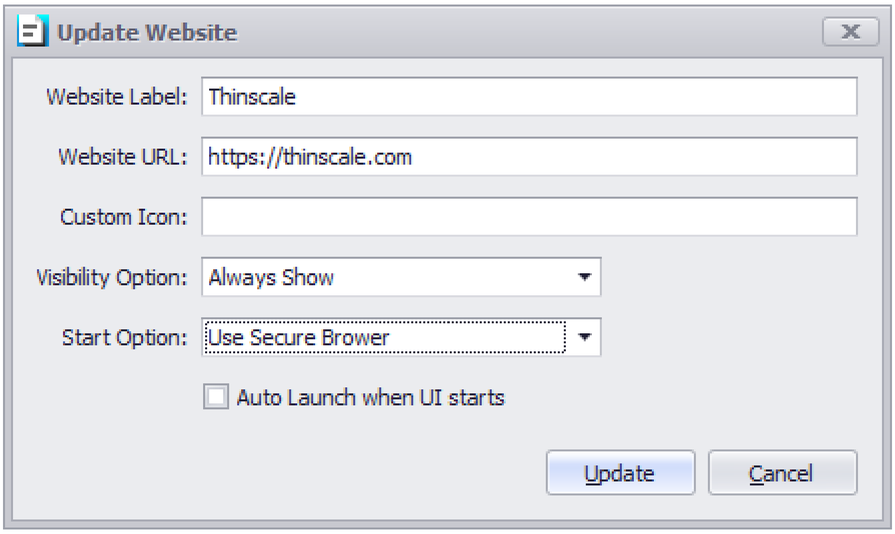
User Interface – Websites



All Website Items:

Name:	Type:	Visibility:	Auto Launch:
Thinscale	Website	Always Show	
Google	Website	Always Show	
Vmware	Website	Always Show	
Citrix	Website	Always Show	

Example

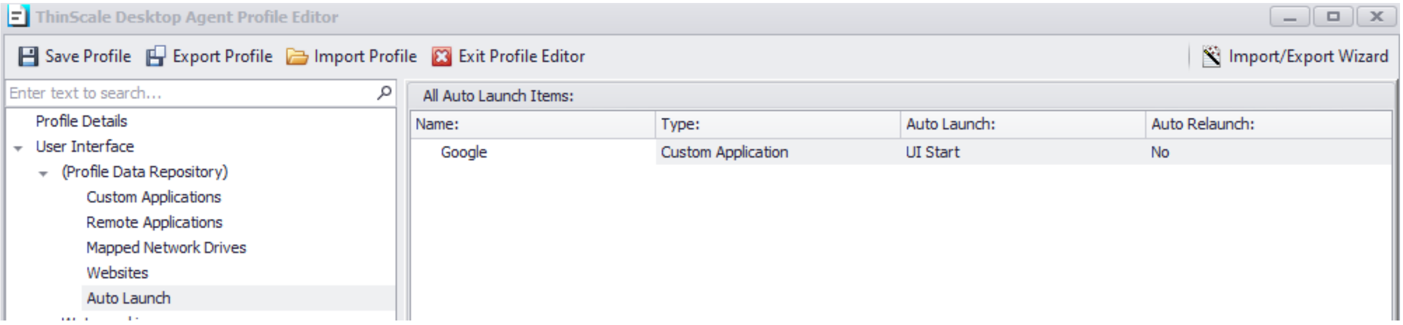


Update Website

Website Label:	Thinscale
Website URL:	https://thinscale.com
Custom Icon:	
Visibility Option:	Always Show
Start Option:	Use Secure Brower

☐ Auto Launch when UI starts

User Interface – Auto Launch



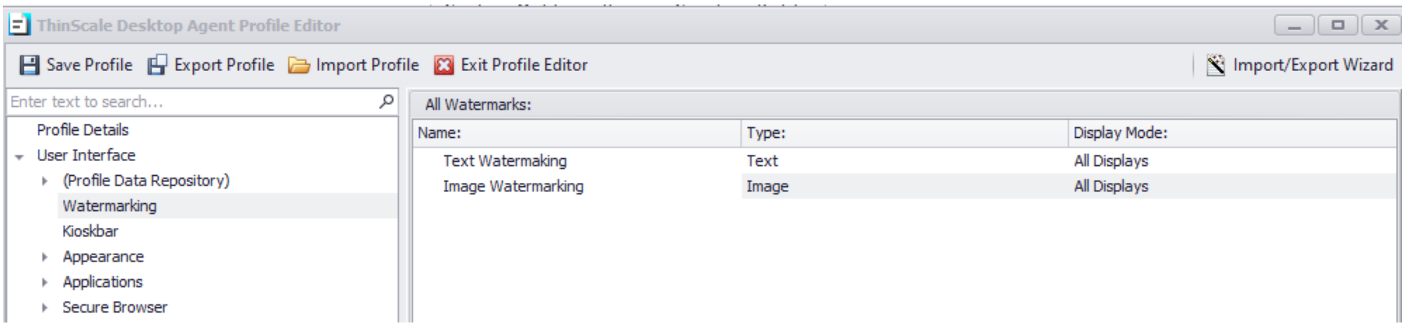
All Auto Launch Items:

Name:	Type:	Auto Launch:	Auto Relaunch:
Google	Custom Application	UI Start	No

When a Website, Custom or Remote Application is set to auto launch when the UI starts, it will be displayed inside the Auto Launch Tab.

This is very useful to track which applications are set to start automatically.

User Interface – Watermarking

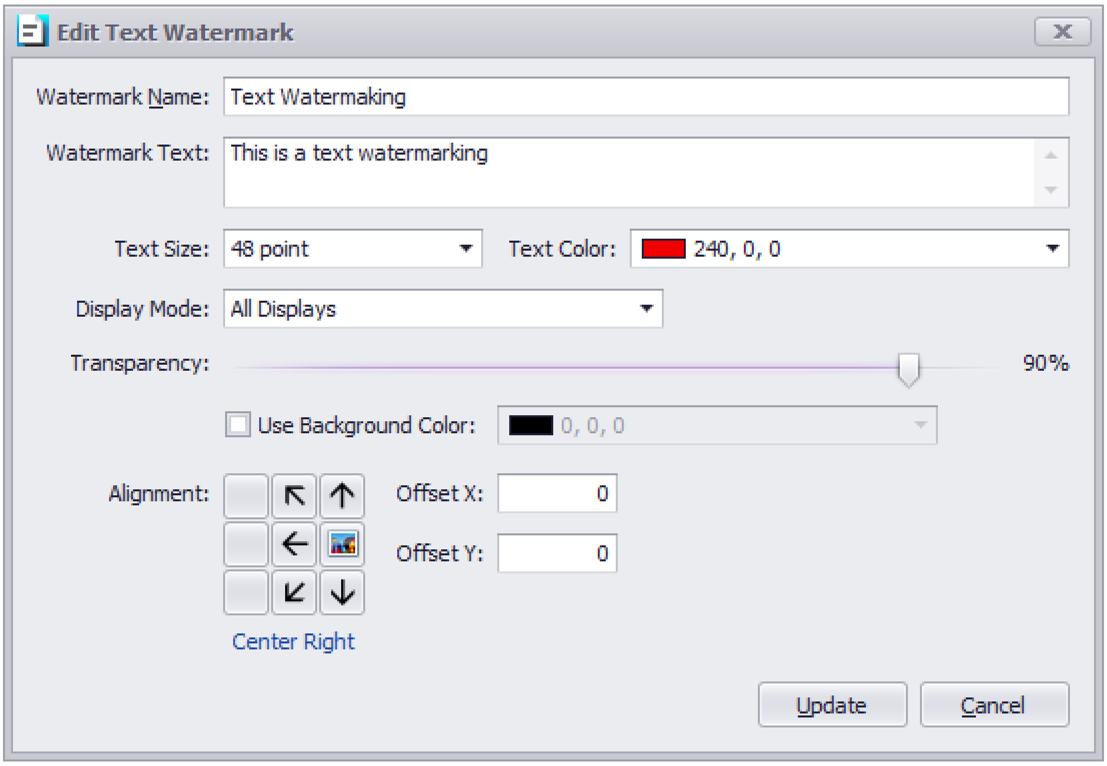


All Watermarks:

Name:	Type:	Display Mode:
Text Watermaking	Text	All Displays
Image Watermarking	Image	All Displays

The TDA offers the choice of multiple types of watermarking across the user screen.

You will be able to set up a text watermarking, which will use a static text overlay on the screen, or alternatively, an image watermarking, which will overlay an image of your choice on the screen.



Watermark Name: Text Watermaking

Watermark Text: This is a text watermarking

Text Size: 48 point

Text Color: 🟥 240, 0, 0

Display Mode: All Displays

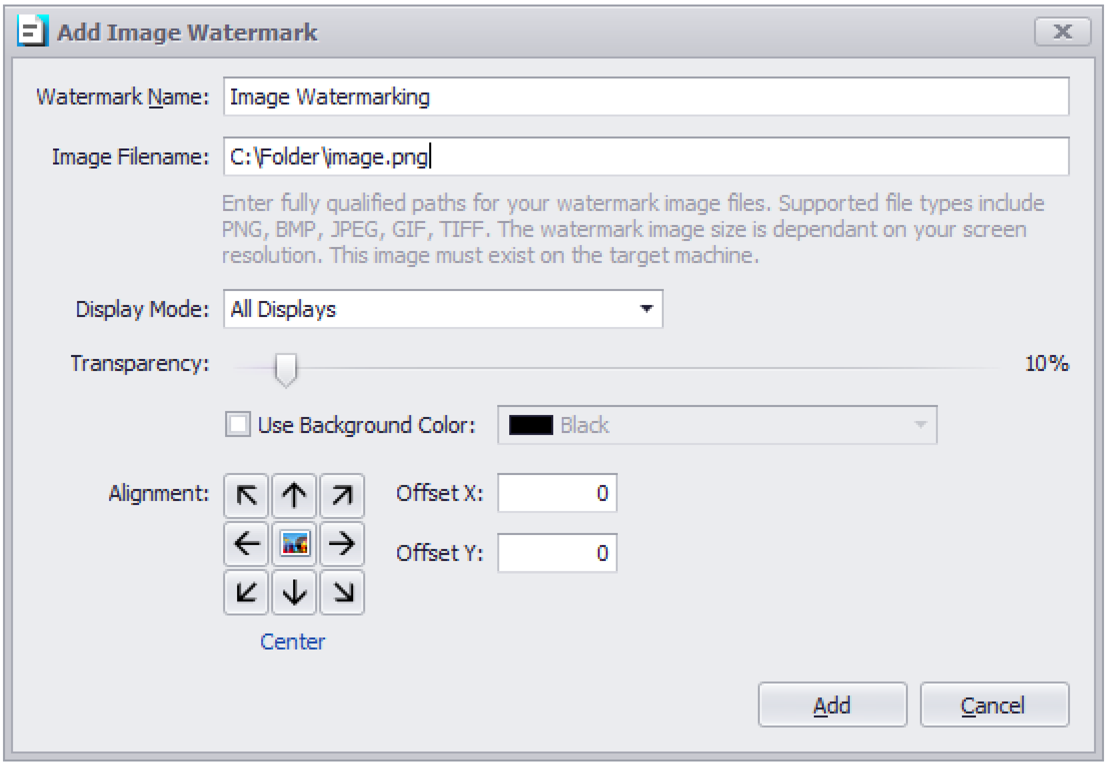
Transparency: 90%

☐ Use Background Color: ■ 0, 0, 0

Alignment: Center Right

Offset X: 0

Offset Y: 0



Add Image Watermark

Watermark Name: Image Watermarking

Image Filename: C:\Folder\image.png

Enter fully qualified paths for your watermark image files. Supported file types include PNG, BMP, JPEG, GIF, TIFF. The watermark image size is dependant on your screen resolution. This image must exist on the target machine.

Display Mode: All Displays

Transparency: 10%

□ Use Background Color: Black

Alignment: Center

Offset X: 0

Offset Y: 0

Watermark text

If enabled, administrator can show a personalized text on the screen as an overlay text.

Image Filename

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

Display Mode

If enabled, the watermarking image/text overlay will be displayed to all monitors, the primary or the secondary one.

Transparency

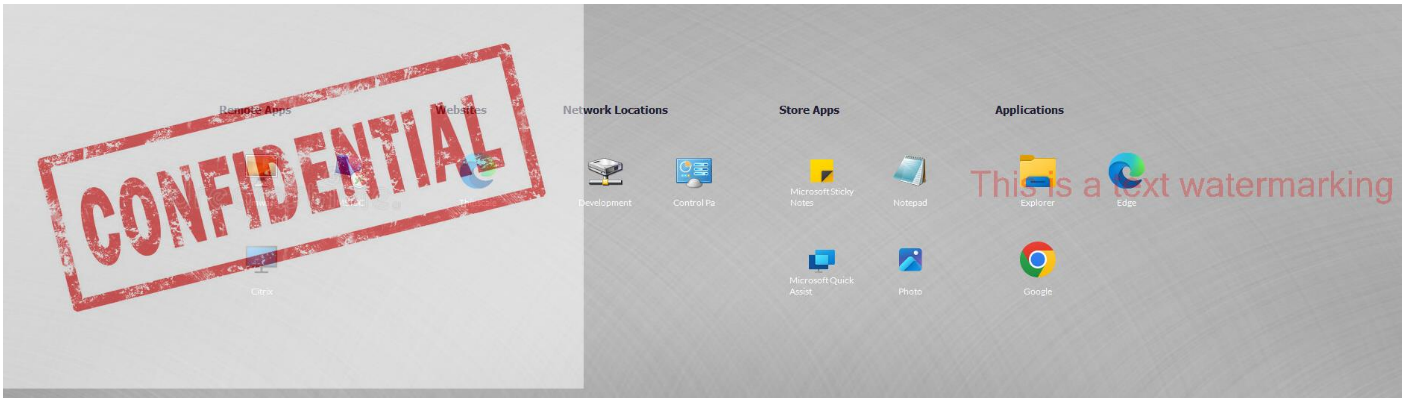
It is the transparency's value of the text/image displayed within the TDA desktop.

Use Background Color

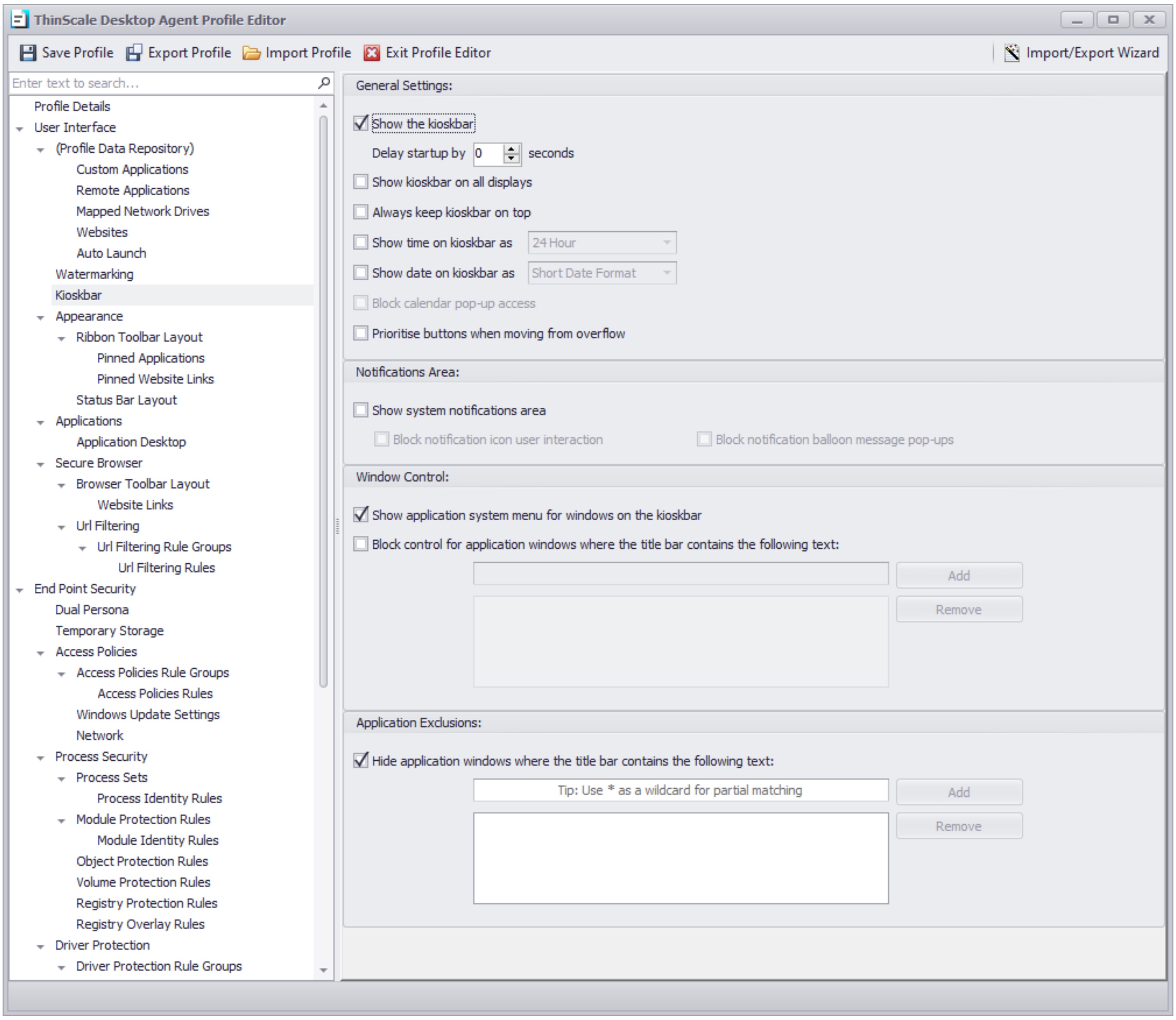
If enabled, you will be able to choose a color of your choice as a background colour.

Alignment

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



User Interface – Kioskbar



General Settings:

☑ Show the kioskbar

Delay startup by 0 seconds

☐ Show kioskbar on all displays

☐ Always keep kioskbar on top

☐ Show time on kioskbar as 24 Hour

☐ Show date on kioskbar as Short Date Format

☐ Block calendar pop-up access

☐ Prioritise buttons when moving from overflow

Notifications Area:

☐ Show system notifications area

☐ Block notification icon user interaction ☐ Block notification balloon message pop-ups

Window Control:

☑ Show application system menu for windows on the kioskbar

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

Application Exclusions:

☑ Hide application windows where the title bar contains the following text:

Tip: Use * as a wildcard for partial matching

Show the kioskbar

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

Delay startup by

If enabled, TDA 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 TDA.

Show the KioskBar on all displays

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

Always keep KioskBar on top

If enabled, the TDA KioskBar will be always visible in the foreground of any window (VDI included).

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

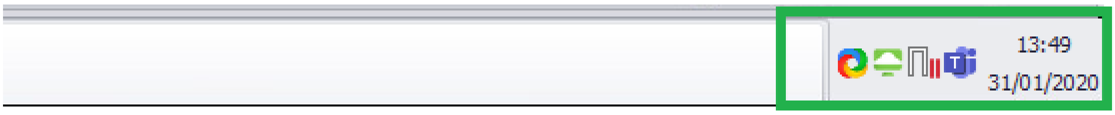
If enabled, the calendar pop-up will be denied.

Prioritise buttons when moving from the overflow

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

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

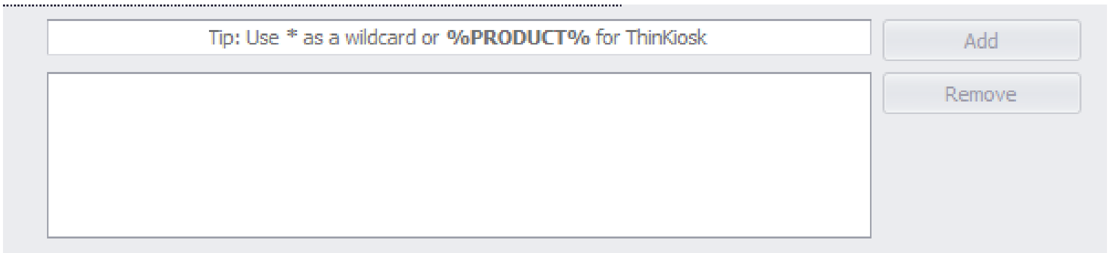
If enabled, balloon tooltip messages on the notification area will be hidden.

Show application system menu for windows on the kioskbar

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

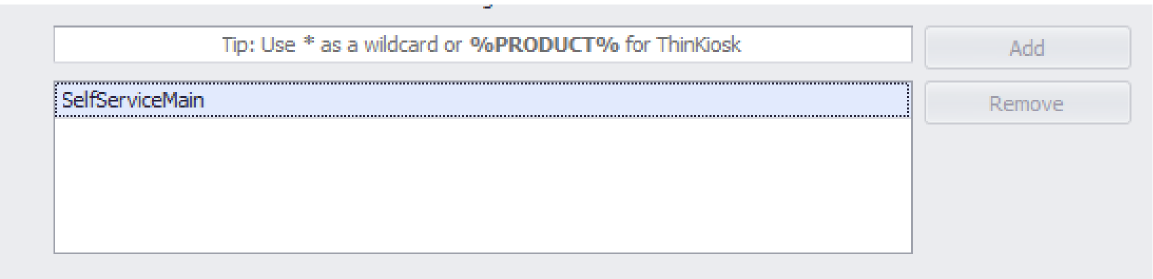
Block control for application windows where the title bar contains the following text

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


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

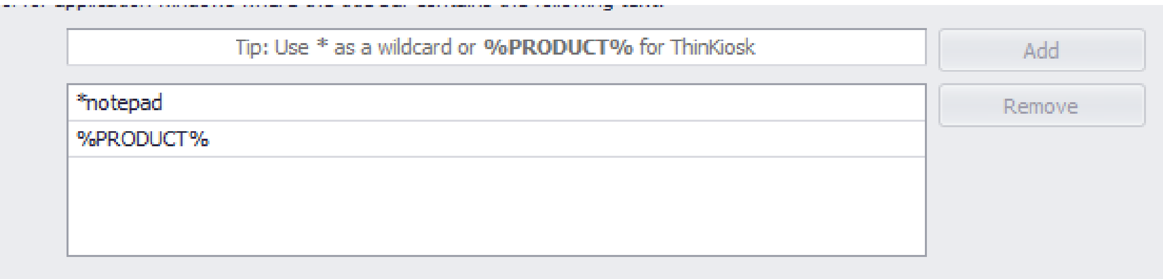
Hide application windows where the title bar contains the following text

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


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

SelfServiceMain

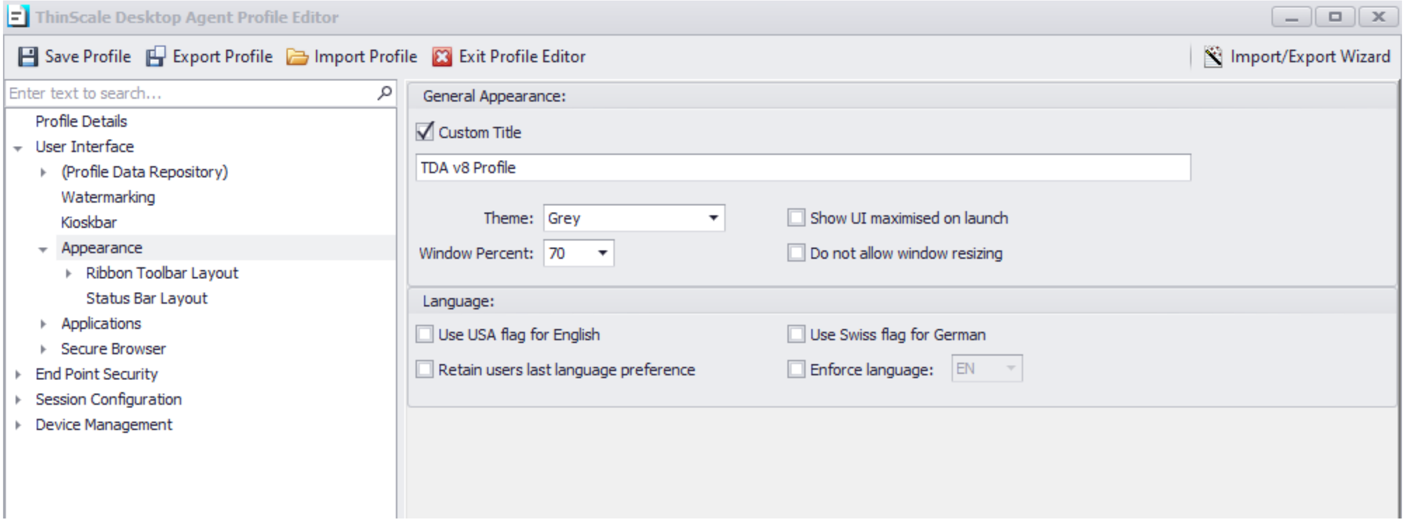
i.e.


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

*notepad

%PRODUCT%

User Interface – Appearance



General Appearance:

☑ Custom Title

TDA v8 Profile

Theme: Grey

Window Percent: 70

□ Show UI maximised on launch

□ Do not allow window resizing

Language:

□ Use USA flag for English

□ Retain users last language preference

□ Use Swiss flag for German

□ Enforce language: EN

Custom Title

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

Theme

Sets the theme TDA UI will use.

Window Percent

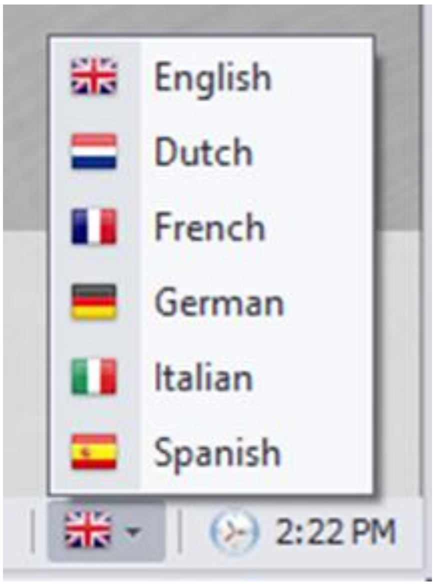
Set's the size of the TDA UI

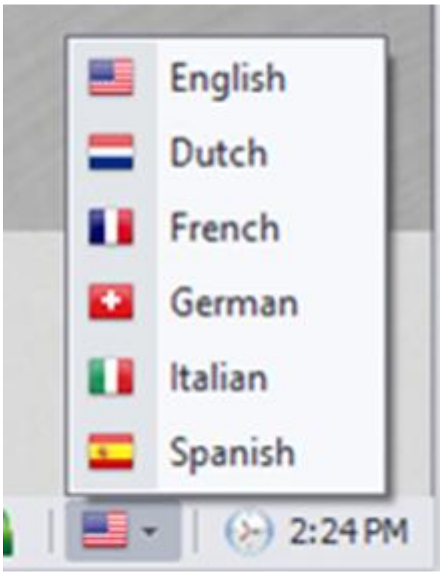
Show UI Maximised on launch

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

Do not allow window resizing

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





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.

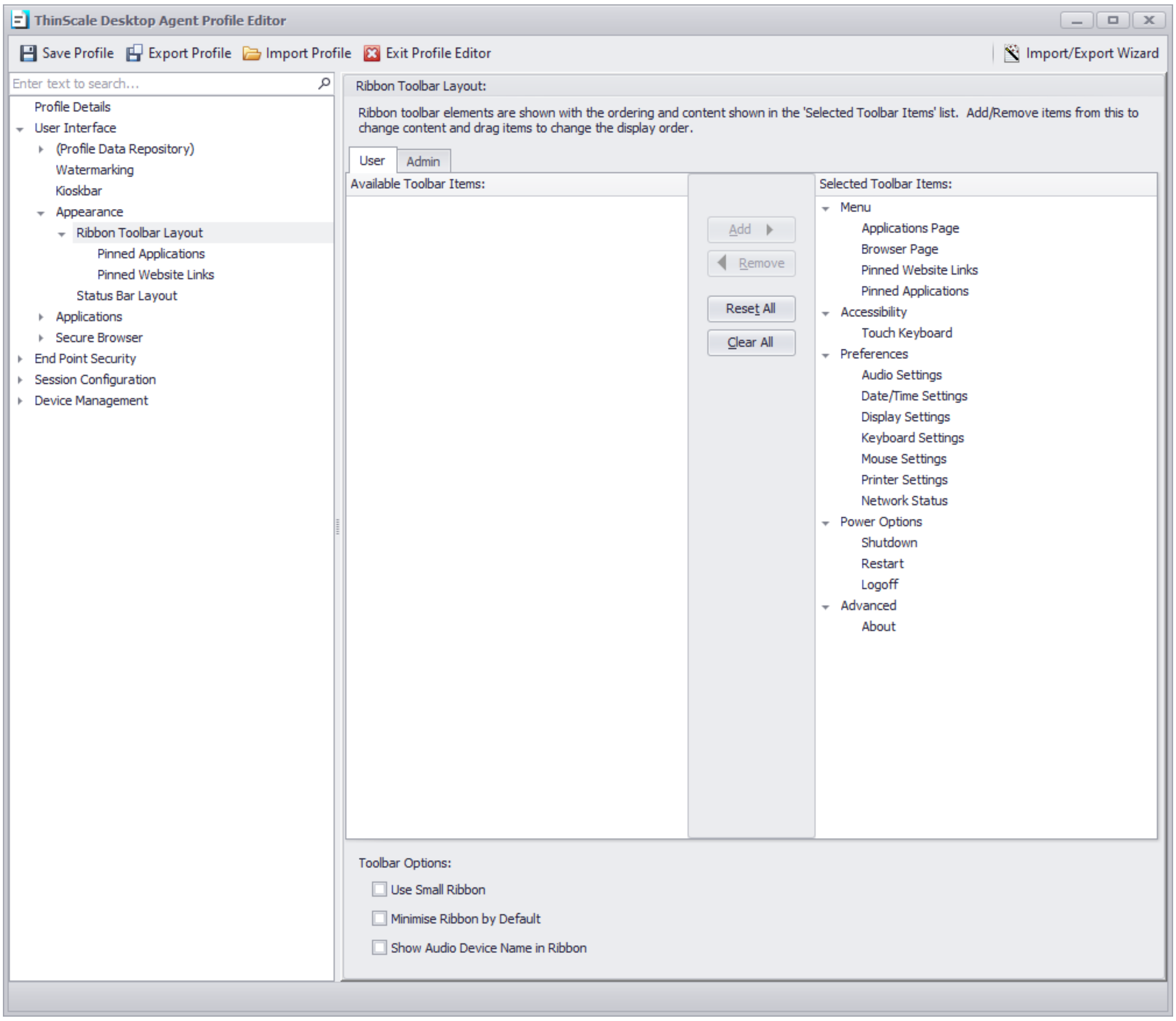
Retain Users Last Language Preference

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

Enforce Language

Forces TDA to use the selected language.

User Interface – Ribbon Toolbar Layout



Ribbon Toolbar Layout:

Ribbon toolbar elements are shown with the ordering and content shown in the 'Selected Toolbar Items' list. Add/Remove items from this to change content and drag items to change the display order.

Toolbar Options:

□ Use Small Ribbon

□ Minimise Ribbon by Default

□ Show Audio Device Name in Ribbon

The Ribbon Toolbar Layout provides administrators with the flexibility to display only the options accessible to the user and arrange them in a preferred order.

Use Small Ribbon

If enabled, ribbon bar icons will be shown in smaller size

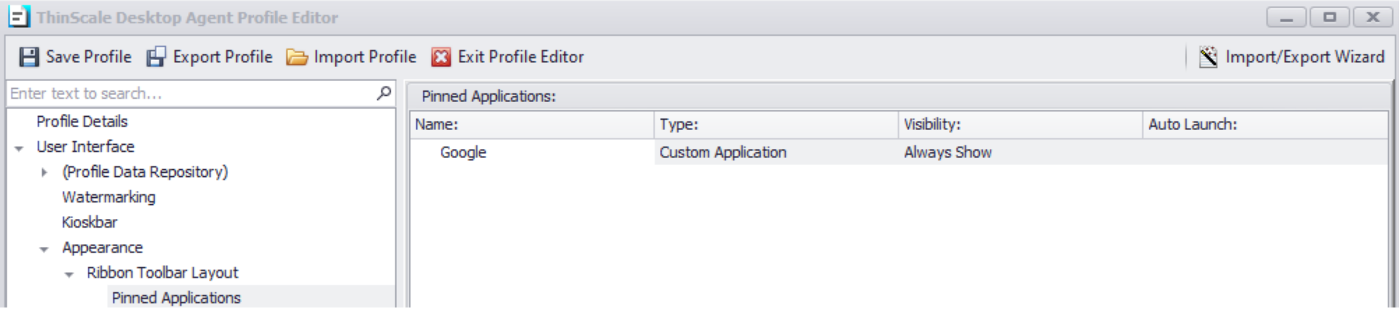
Minimise Ribbon by default

If enabled, the ribbon bar will be minimised by default

Show Audio Device Name in Ribbon

If enabled, the audio device name will be displayed on the ribbon bar.

User Interface – Pinned Applications

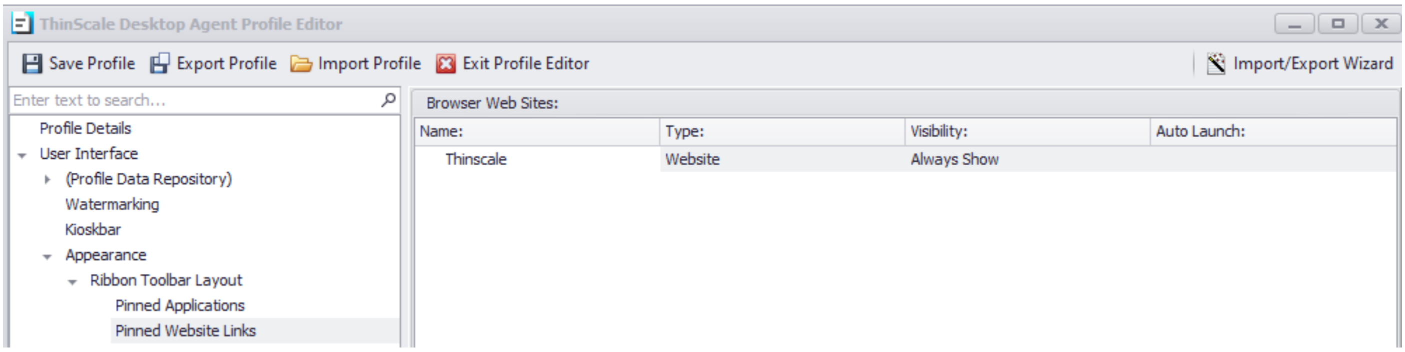


Name:	Type:	Visibility:	Auto Launch:
Google	Custom Application	Always Show	

Pinned Applications are application that can be accessed within the main ribbon bar.

Useful to keep the TDA Desktop clean and only show perhaps applications that are not used consistently.

User Interface – Pinned Websites Links

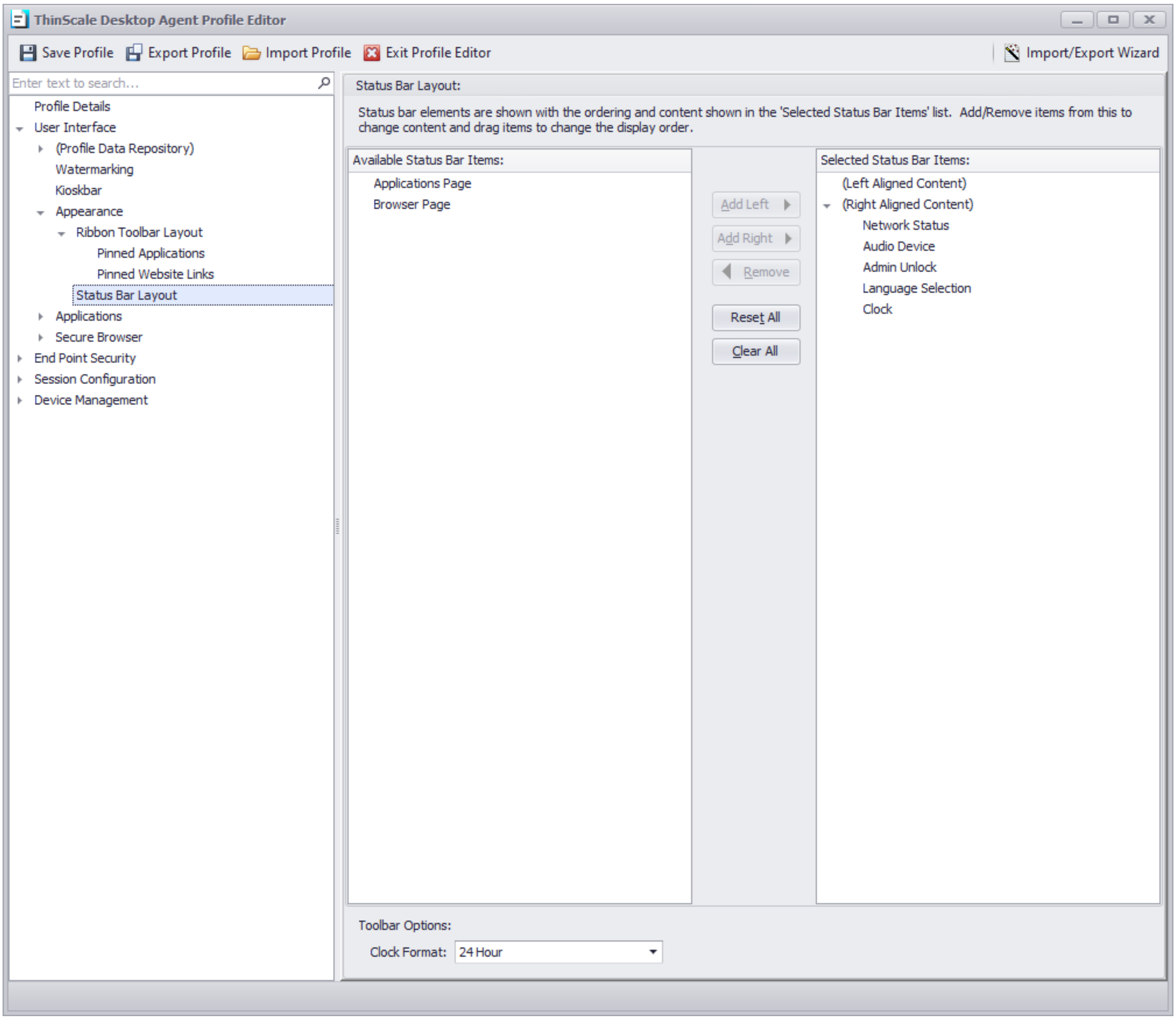


Name:	Type:	Visibility:	Auto Launch:
Thinscale	Website	Always Show	

Pinned Website Links are websites that can be accessed within the main ribbon bar.

Useful to keep the TDA Desktop clean and only show perhaps websites that are not used browsed.

User Interface – Status Bar Layout



ThinScale Desktop Agent Profile Editor

Status Bar Layout:

Status bar elements are shown with the ordering and content shown in the 'Selected Status Bar Items' list. Add/Remove items from this to change content and drag items to change the display order.

Available Status Bar Items:
- Applications Page
- Browser Page

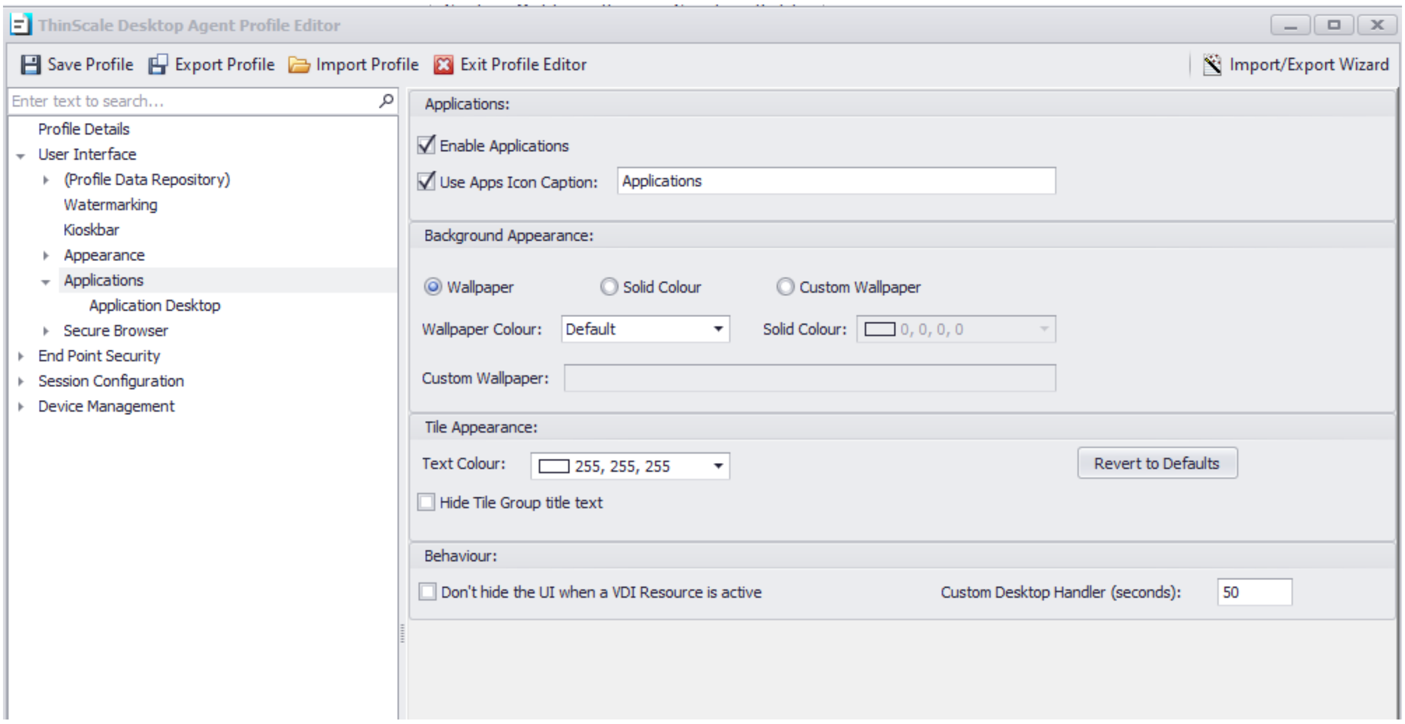
Selected Status Bar Items:
- (Left Aligned Content)
- (Right Aligned Content)
  - Network Status
  - Audio Device
  - Admin Unlock
  - Language Selection
  - Clock

Toolbar Options:

Clock Format: 24 Hour

The Status Toolbar Layout provides administrators with the flexibility to display applets like language, battery status and network to the user, and arrange them in a preferred order.

User Interface – Applications



Applications:

☑ Enable Applications

☑ Use Apps Icon Caption: Applications

Background Appearance:

● Wallpaper ○ Solid Colour ○ Custom Wallpaper

Wallpaper Colour: Default Solid Colour: 0, 0, 0, 0

Custom Wallpaper:

Tile Appearance:

Text Colour: 255, 255, 255

□ Hide Tile Group title text

Behaviour:

□ Don't hide the UI when a VDI Resource is active Custom Desktop Handler (seconds): 50

Enable Applications

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

Use Apps Icon Caption

Provides a caption to use for the applications tab icon.

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 TDA.

Text Colour

The colour of the application’s text name.

Hide Tile Group Title Text

Hides the group headings in the applications tab.

Revert to Default

When clicked the default settings will be applied back.

Don’t hide TDA when a VDI resource is active

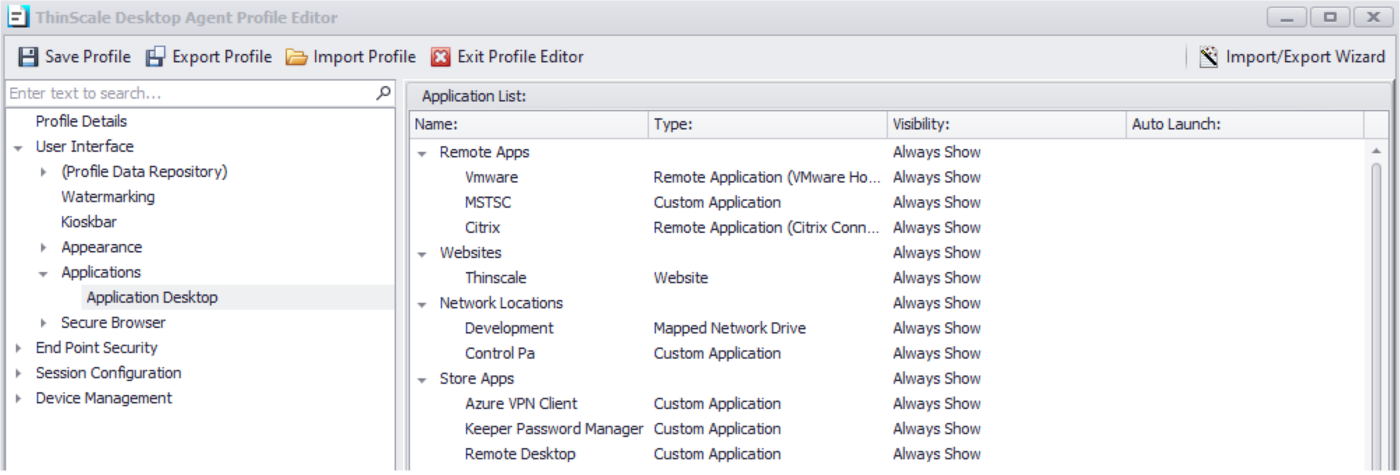
If enabled TDA will remain open in the background while in the foreground your VDI session is open.

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

Custom Desktop Handler

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

User Interface – Application Desktop



- Profile Details
- User Interface
  - (Profile Data Repository)
  - Watermarking
  - Kioskbar
  - Appearance
  - Applications
    - Application Desktop
  - Secure Browser
- End Point Security
- Session Configuration
- Device Management

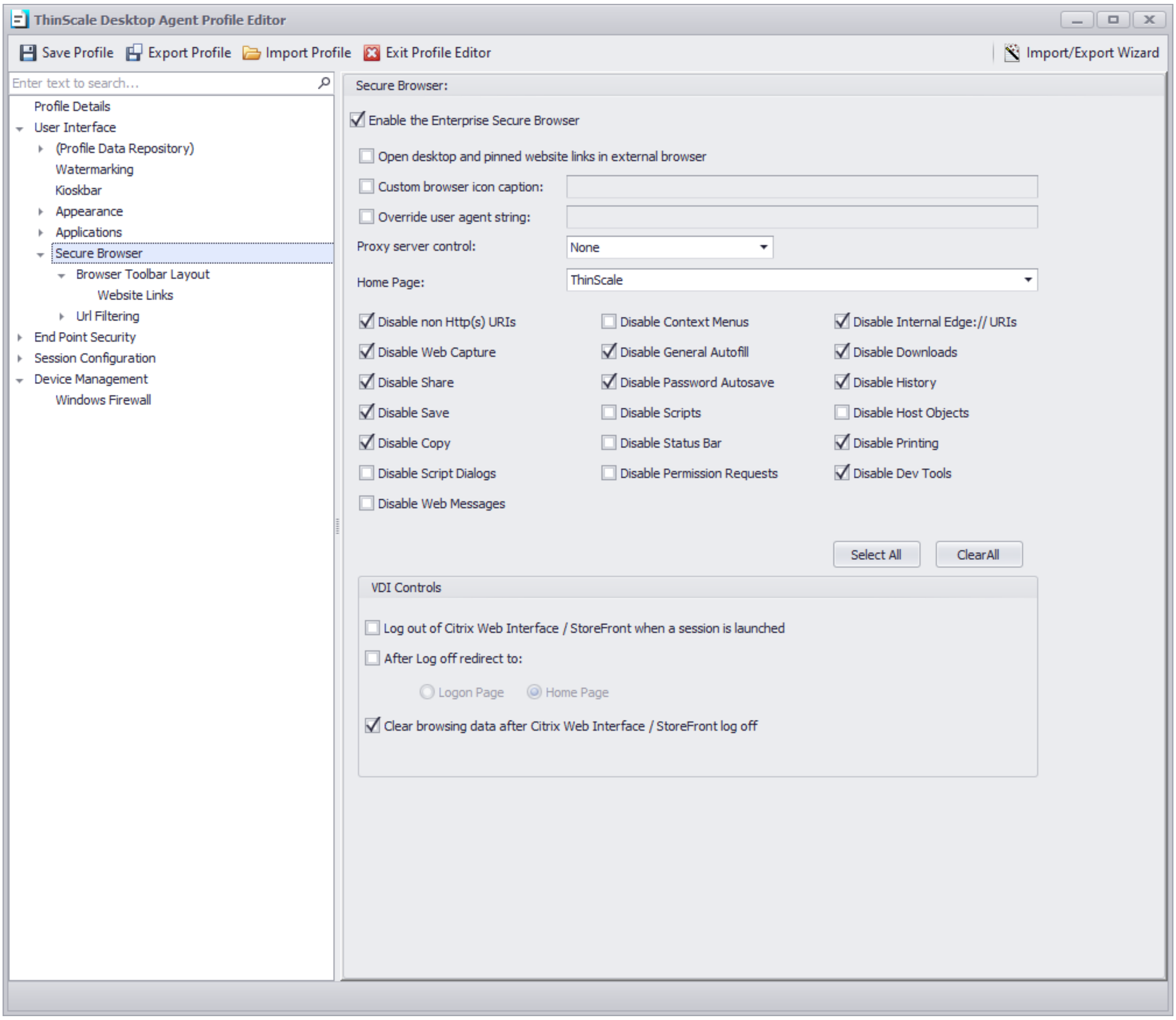
Application List:

Name:	Type:	Visibility:	Auto Launch:
Remote Apps		Always Show	
Vmware	Remote Application (VMware Ho...	Always Show	
MSTSC	Custom Application	Always Show	
Citrix	Remote Application (Citrix Conn...	Always Show	
Websites		Always Show	
Thinscale	Website	Always Show	
Network Locations		Always Show	
Development	Mapped Network Drive	Always Show	
Control Pa	Custom Application	Always Show	
Store Apps		Always Show	
Azure VPN Client	Custom Application	Always Show	
Keeper Password Manager	Custom Application	Always Show	
Remote Desktop	Custom Application	Always Show	

The Application Desktop Tab serves as the repository for managing applications, allowing you to organize and display them within the TDA Desktop.

This feature enables the customization of groups to include applications, websites, and shared drives according to your preferences.

User Interface – Secure Browser



Secure Browser:

☑ Enable the Enterprise Secure Browser

☐ Open desktop and pinned website links in external browser

☐ Custom browser icon caption:

☐ Override user agent string:

Proxy server control: None

Home Page: ThinScale

☑ Disable non Http(s) URIs	☐ Disable Context Menus	☑ Disable Internal Edge:// URIs
☑ Disable Web Capture	☑ Disable General Autofill	☑ Disable Downloads
☑ Disable Share	☑ Disable Password Autosave	☑ Disable History
☑ Disable Save	☐ Disable Scripts	☐ Disable Host Objects
☑ Disable Copy	☐ Disable Status Bar	☑ Disable Printing
☐ Disable Script Dialogs	☐ Disable Permission Requests	☑ Disable Dev Tools
☐ Disable Web Messages		

VDI Controls

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

☐ After Log off redirect to:

○ Logon Page ● Home Page

☑ Clear browsing data after Citrix Web Interface / StoreFront log off

Enable the Enterprise Secure Browser

If enabled, will show the browser tab inside ThinKiosk Desktop.

Use Browser Icon Caption

Provides a caption to use for the browser tab icon.

Override user agent string

If enabled, user will be able to override the browser user agent string.

i.e.

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36

Proxy server control

If enabled, the browser will detect or not the proxy option enabled on the user desktop.

Home Page

Selects the home page URL from the list.

Disable Browser Options

You can disable all the buttons, object and right click context menus by enabling the checkboxes.

For more information, please hover over the options.

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

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

After Log off redirect to:

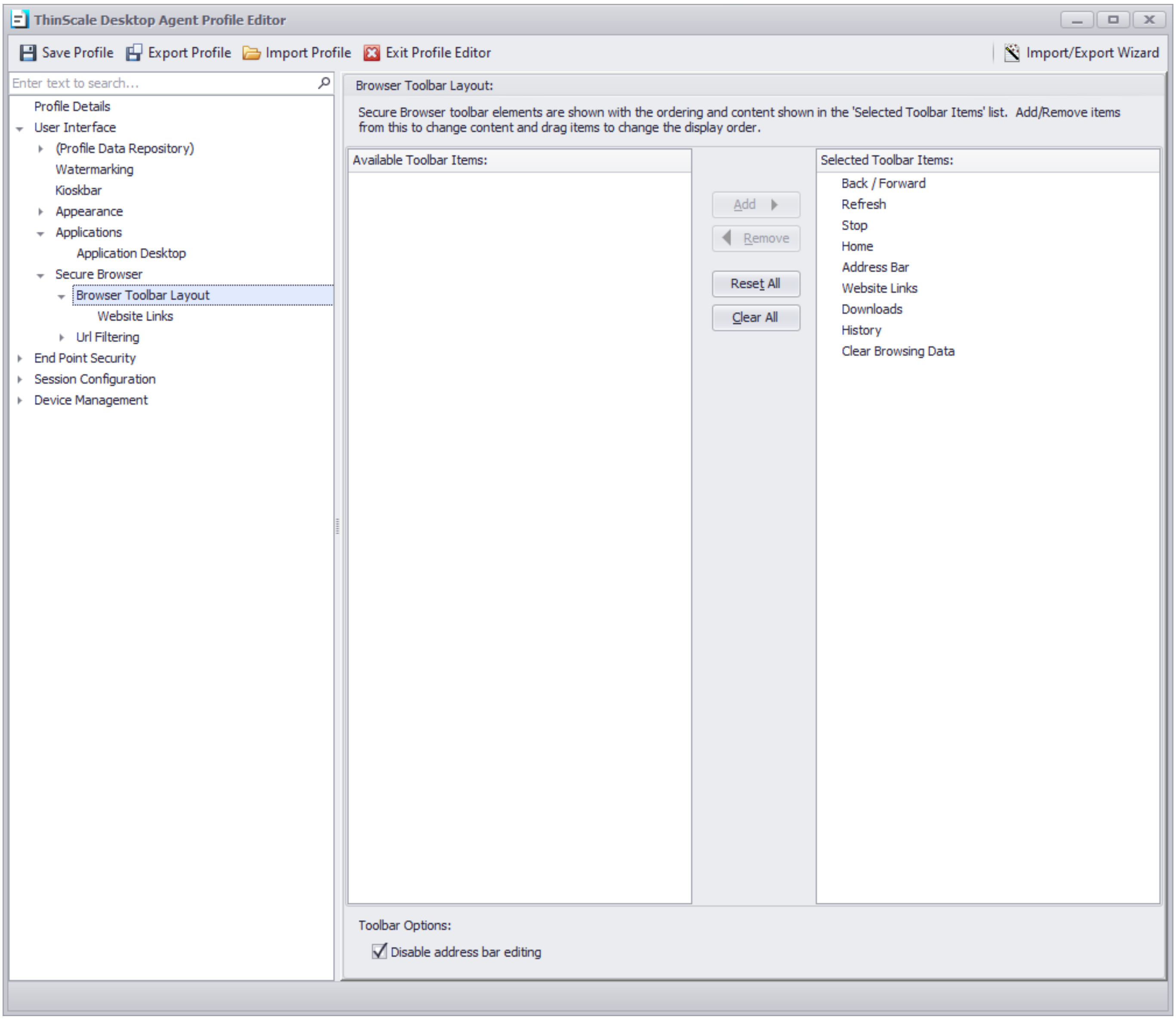
Logon Page will redirect to the Storefront logon Page.

Home Page will redirect to the Home Page Link.

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.

User Interface –Browser Toolbar Layout



ThinScale Desktop Agent Profile Editor

Browser Toolbar Layout:

Secure Browser toolbar elements are shown with the ordering and content shown in the 'Selected Toolbar Items' list. Add/Remove items from this to change content and drag items to change the display order.

Available Toolbar Items:

Selected Toolbar Items:

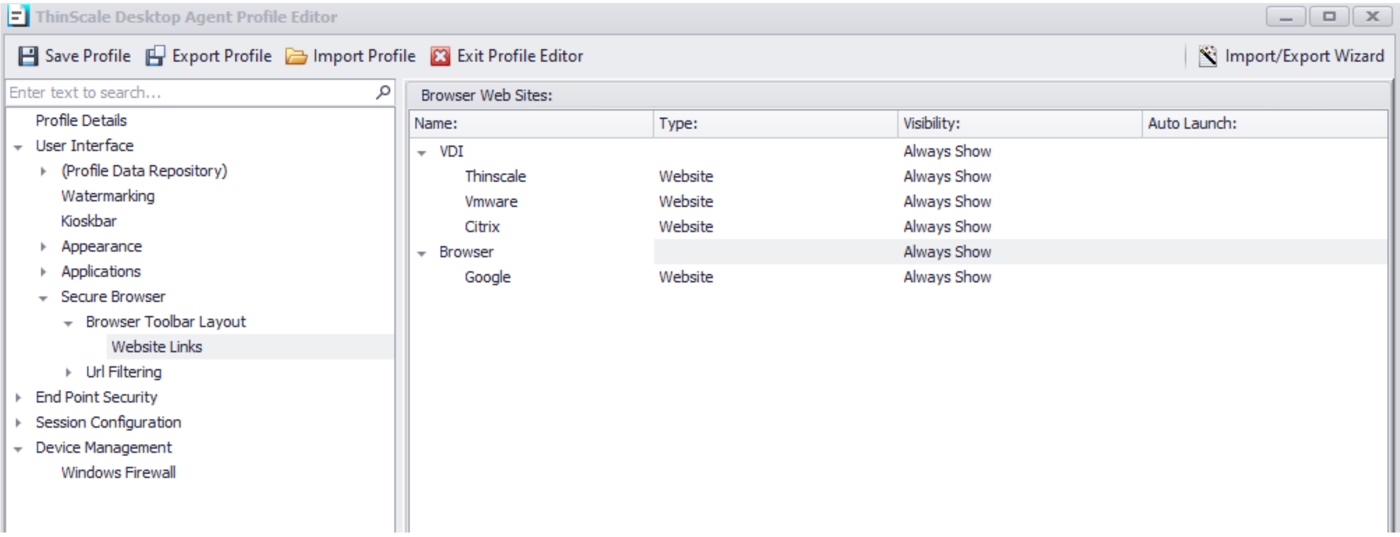
- Back / Forward
- Refresh
- Stop
- Home
- Address Bar
- Website Links
- Downloads
- History
- Clear Browsing Data

Toolbar Options:

☑ Disable address bar editing

Secure Browser toolbar elements are shown with the ordering and content shown in the 'Selected Toolbar Items' list. Add/Remove items from this to change content and drag items to change the display order.

User Interface – Web Sites



ThinScale Desktop Agent Profile Editor

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

Enter text to search...

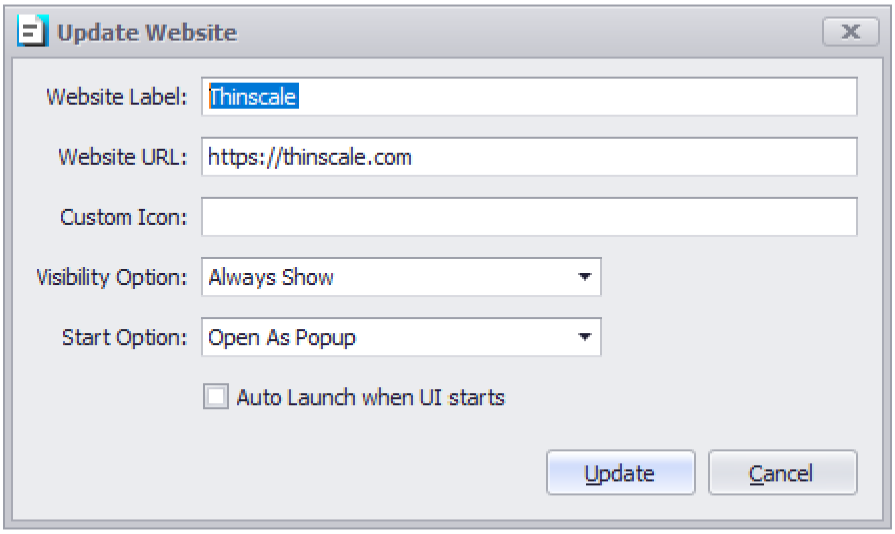
- Profile Details
- User Interface
  - (Profile Data Repository)
  - Watermarking
  - Kioskbar
  - Appearance
  - Applications
  - Secure Browser
    - Browser Toolbar Layout
      - Website Links
    - Url Filtering
- End Point Security
- Session Configuration
- Device Management
  - Windows Firewall

Browser Web Sites:

Name:	Type:	Visibility:	Auto Launch:
VDI		Always Show	
Thinscale	Website	Always Show	
Vmware	Website	Always Show	
Citrix	Website	Always Show	
Browser		Always Show	
Google	Website	Always Show	

A list of websites available in the Favourite option.

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



Update Website

Website Label:	Thinscale
Website URL:	https://thinscale.com
Custom Icon:	
Visibility Option:	Always Show
Start Option:	Open As Popup

□ Auto Launch when UI starts

Website Label

The text that appears in the ‘Select Link’ drop down on the TDA UI.

Website URL

URL the browser will navigate to when selected.

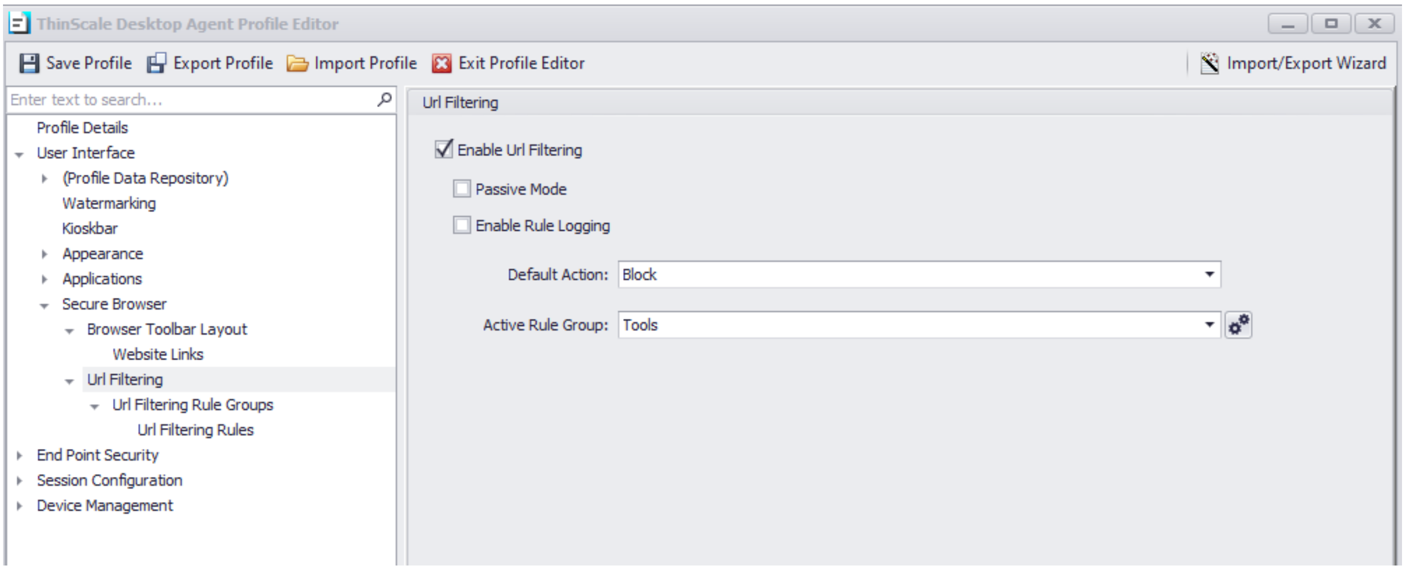
Custom Icon

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

Visibility Option

Location where the application will be displayed.

User Interface – Url Filtering



Url Filtering

☑ Enable Url Filtering

□ Passive Mode

□ Enable Rule Logging

Default Action: Block

Active Rule Group: Tools

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.

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.

Default Rule Action:

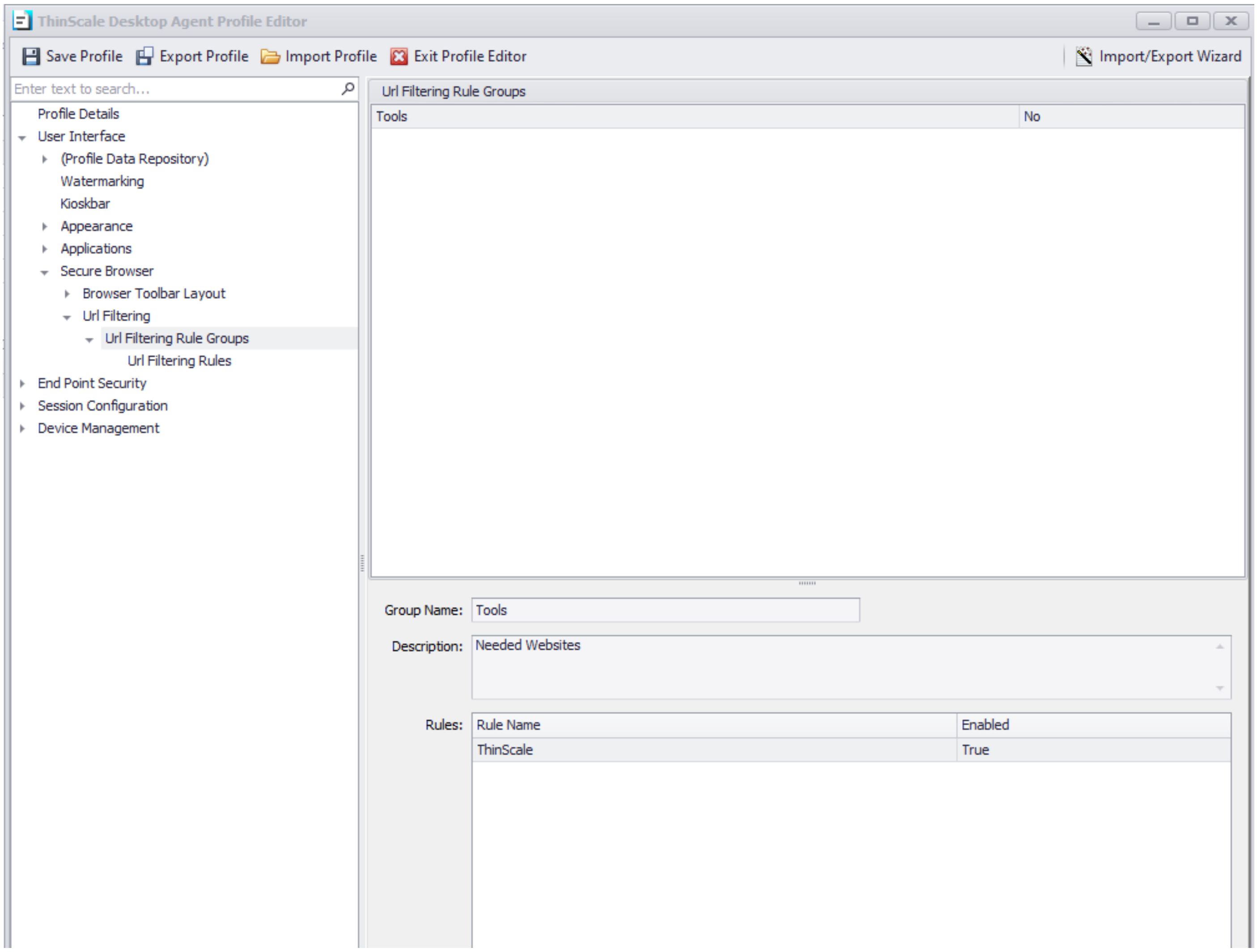
Block: will block all URLs from navigation and a whitelist approach will need to be utilized to allow only specific links.

Allow: will allow all URLs from navigation and a blacklist approach will need to be utilized to block only specific links.

Active Rule Group

Select the Rule Group you have created which will contain all the Url Filtering Rule.

User Interface – Url Filtering Rule Groups



Tools	No

Group Name: Tools

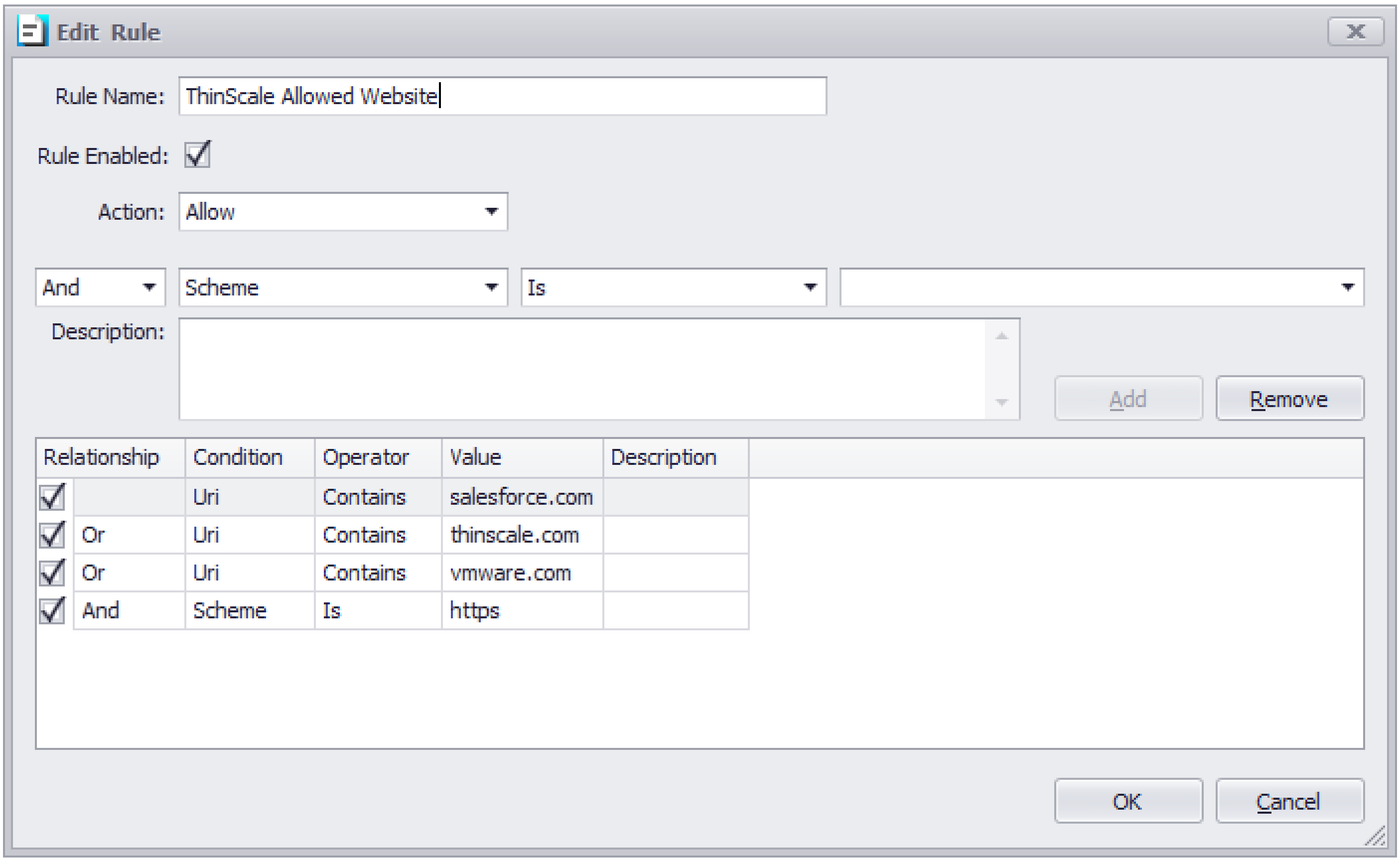
Description: Needed Websites

Rules:

Rule Name	Enabled
ThinScale	True

The Url Filtering Rule Groups enables administrators to group together URLs based on their perceived safety or trustworthiness, depending on the default action.

Example Allowed Rule



Rule Name: ThinScale Allowed Website

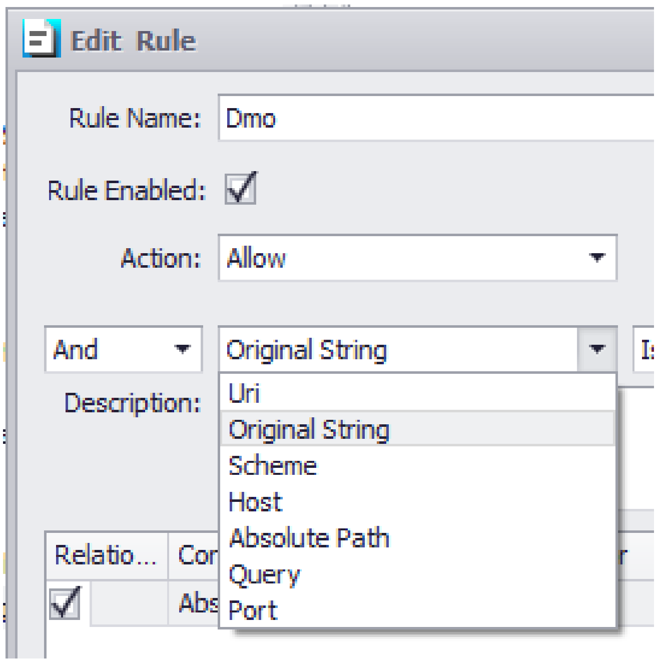
Rule Enabled: ☑

Action: Allow

And | Scheme | Is |

Description:

	Relationship	Condition	Operator	Value	Description
☑		Uri	Contains	salesforce.com	
☑	Or	Uri	Contains	thinscale.com	
☑	Or	Uri	Contains	vmware.com	
☑	And	Scheme	Is	https	



Edit Rule

Rule Name: Dmo

Rule Enabled: ☑

Action: Allow

And | Original String

Description:

Original string (e.g., the original string of the URL http://www.contoso.com:80//thick%20and%20thin.htm is http://www.contoso.com//thick and thin.htm

Scheme (e.g., https)

Host (e.g., the host part of the URL https://thinscale.com/contact is thinscale.com

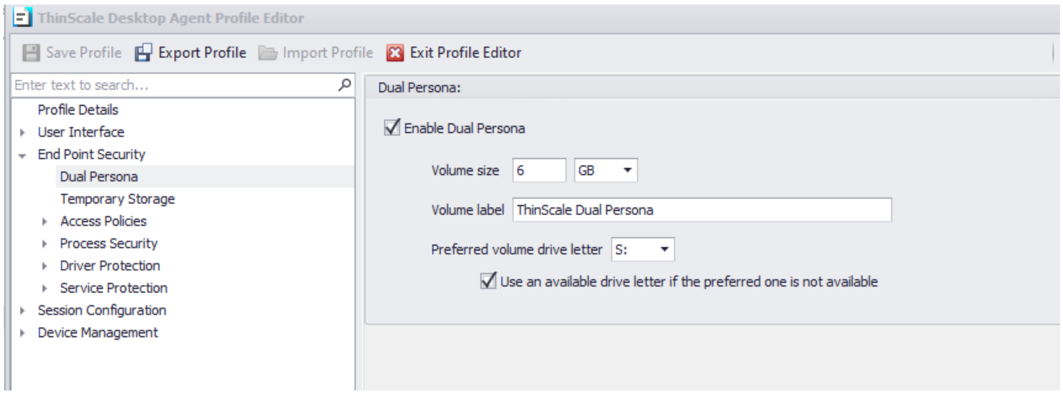
Absolute Path (e.g., the absolute path of the URL https://thinscale.com/contacts is /contacts

Query (e.g., the query of the URL http://www.contoso.com/catalog/shownew.htm?date=today is ?date=today

Port (e.g., the port of the URL https://thinscale.com/contact is 443

4. End Point Security

End Point Security – Dual persona



Dual Persona:

☑ Enable Dual Persona

Volume size 6 GB

Volume label ThinScale Dual Persona

Preferred volume drive letter S:

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

Enable Dual Persona

Dual Persona is a technology that lets you move the TDA 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 TDA and is only made available when TDA 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 TDA session. Only applications running inside the TDA session have access to the virtual volume.

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.

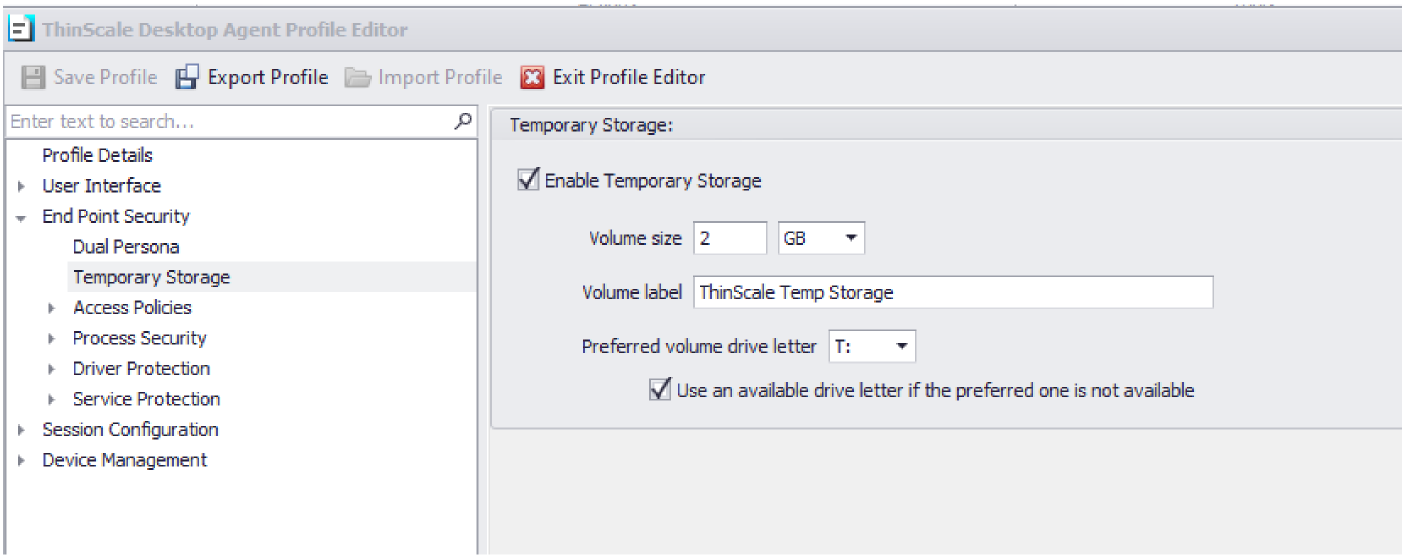
Preferred Volume Drive Letter

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, TDA will use the first available drive letter on the device.

End Point Security – Temporary Storage



Temporary Storage:

☑ Enable Temporary Storage

Volume size 2 GB

Volume label ThinScale Temp Storage

Preferred volume drive letter T:

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

Enable Temporary Storage

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

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

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

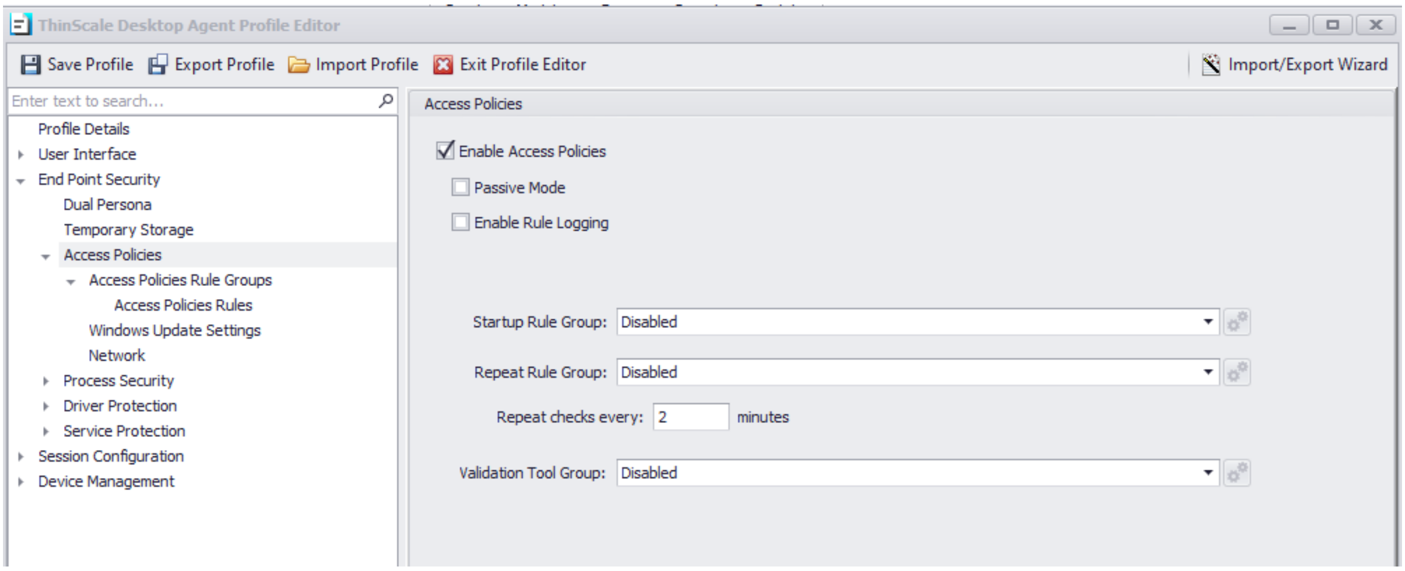
Preferred Volume Drive Letter

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, TDA will use the first available drive letter on the device.

End Point Security – Access Policies



ThinScale Desktop Agent Profile Editor

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

Enter text to search...

- Profile Details
- User Interface
- End Point Security
  - Dual Persona
  - Temporary Storage
  - Access Policies
    - Access Policies Rule Groups
      - Access Policies Rules
    - Windows Update Settings
    - Network
  - Process Security
  - Driver Protection
  - Service Protection
- Session Configuration
- Device Management

Access Policies

☑ Enable Access Policies

□ Passive Mode

□ Enable Rule Logging

Startup Rule Group: Disabled

Repeat Rule Group: Disabled

Repeat checks every: 2 minutes

Validation Tool Group: Disabled

Passive mode

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

Enable rule logging

If enabled, the administrator will be able to retrieve information about the rules that have been running, from the TDA logs file.

Startup Rule Group

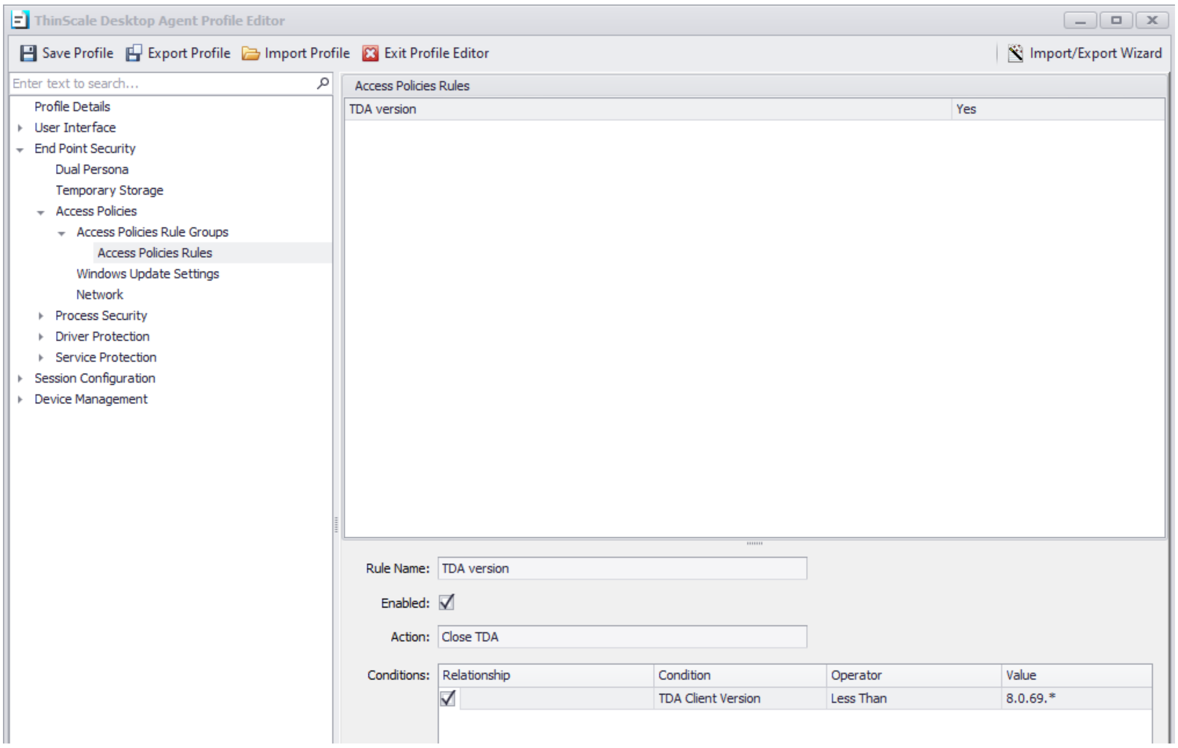
If enabled, rule created inside this group will run when the TDA session is starting

Repeat Rule Group

If enabled, rule created inside this group will run inside TDA session every x minutes

Please refer to the Knowledge Base article for more info.

End Point Security – Access Policies Rule Groups



TDA version	Yes

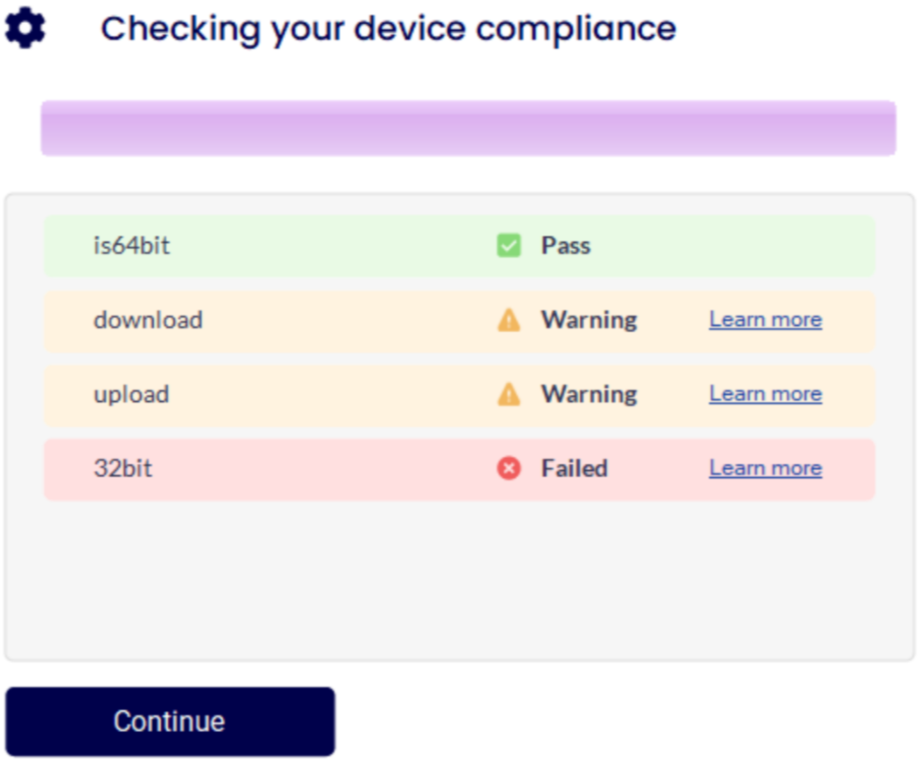
Rule Name: TDA version

Enabled: ☑

Action: Close TDA

Conditions:

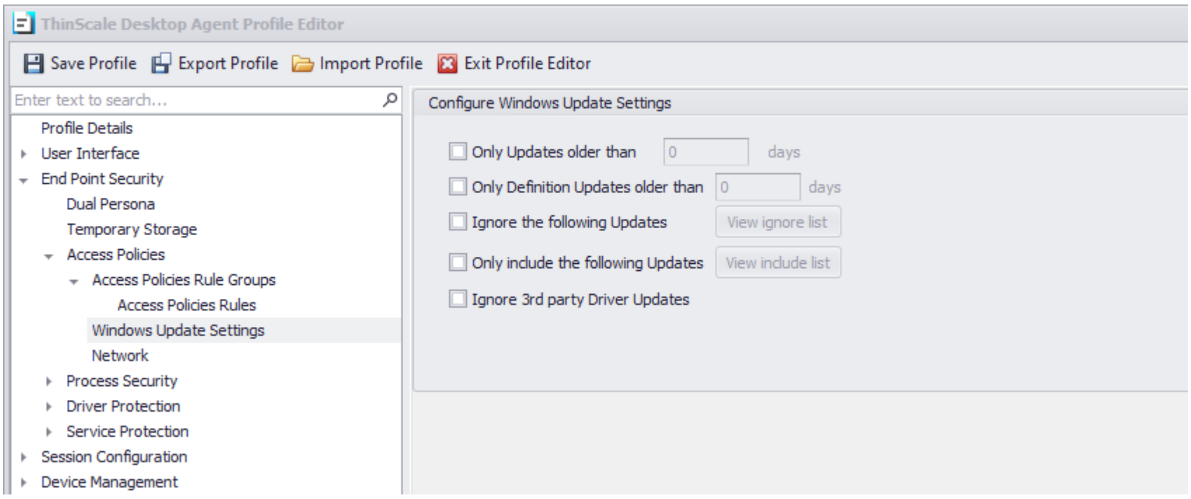
Relationship	Condition	Operator	Value
☑	TDA Client Version	Less Than	8.0.69.*



Checking your device compliance

is64bit	✓ Pass	
download	⚠ Warning	Learn more
upload	⚠ Warning	Learn more
32bit	⊗ Failed	Learn more

End Point Security – Windows Update Settings


ThinScale Desktop Agent Profile Editor

Save Profile | Export Profile | Import Profile | Exit Profile Editor

Enter text to search...

- Profile Details
- User Interface
- End Point Security
  - Dual Persona
  - Temporary Storage
  - Access Policies
    - Access Policies Rule Groups
      - Access Policies Rules
    - Windows Update Settings
    - Network
  - Process Security
  - Driver Protection
  - Service Protection
- Session Configuration
- Device Management

Configure Windows Update Settings

□ Only Updates older than 0 days

□ Only Definition Updates older than 0 days

□ Ignore the following Updates [View ignore list]

□ Only include the following Updates [View include list]

□ Ignore 3rd party Driver Updates

Only updates older than

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

Only definition updates older than

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

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

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.

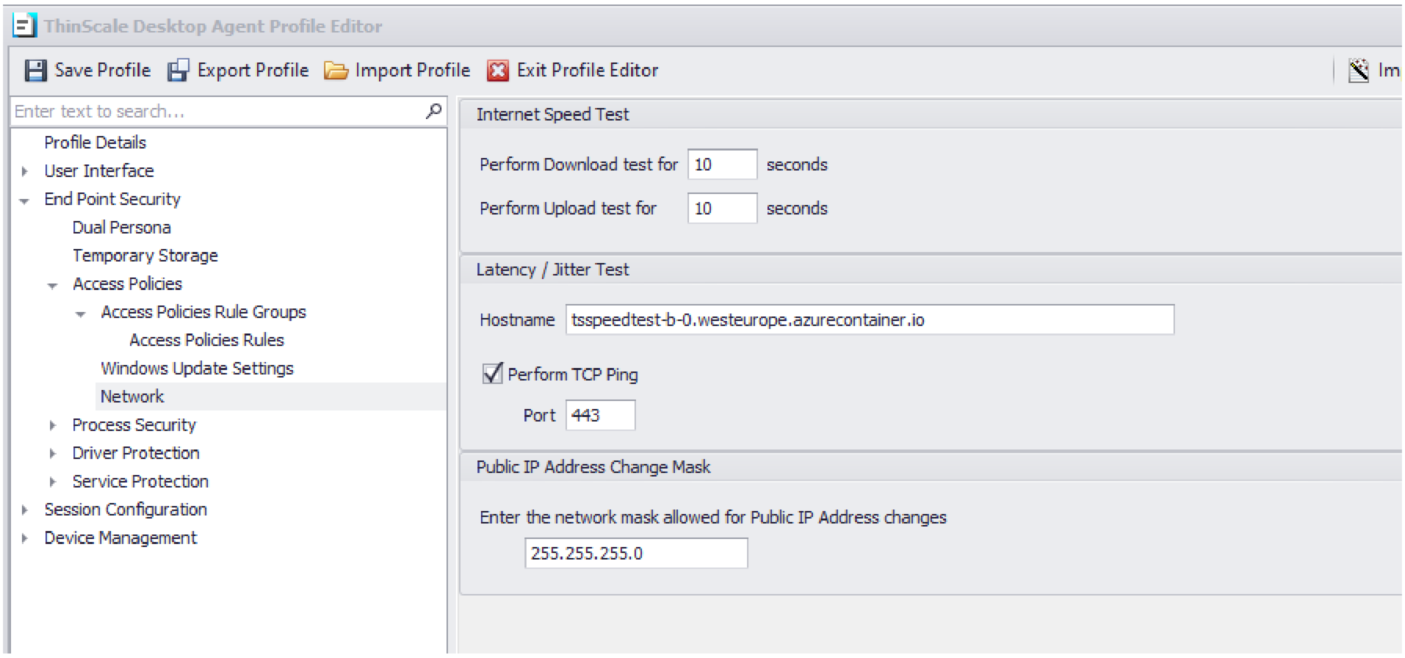
Only include the following updates

If enabled, only specific updates in the list will need be installing.

Ignore 3rd party driver updates

If enabled, all the 3rd party drivers’ updates will be ignored.

End Point Security – Network



Internet Speed Test

Perform Download test for 10 seconds

Perform Upload test for 10 seconds

Latency / Jitter Test

Hostname tsspeedtest-b-0.westeurope.azurecontainer.io

☑ Perform TCP Ping

Port 443

Public IP Address Change Mask

Enter the network mask allowed for Public IP Address changes

255.255.255.0

Perform Download test

If enabled, the download test against the Hostname section will be performed for x seconds

Perform Upload test

If enabled, the upload test against the Hostname section will be performed for x seconds

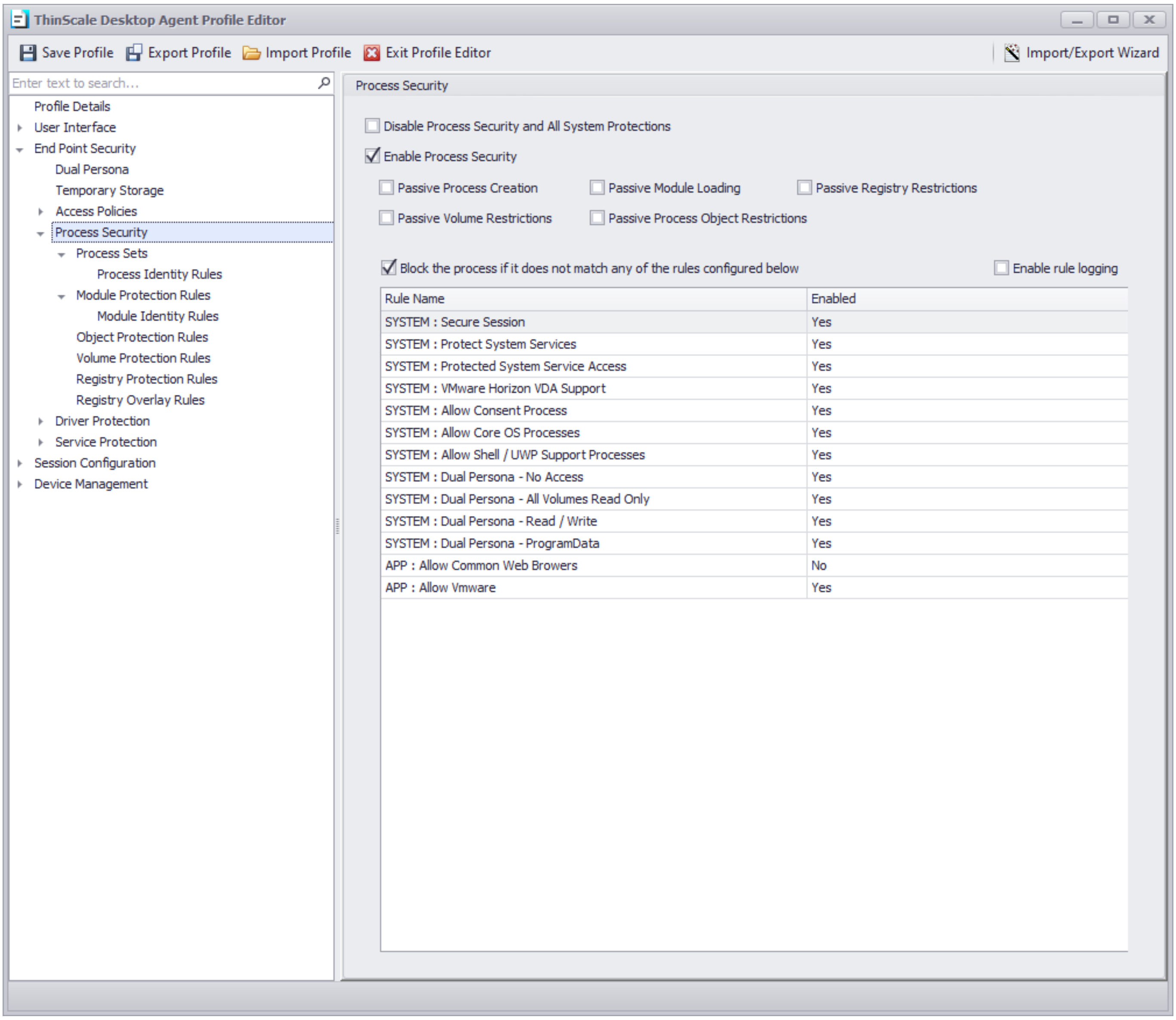
Hostname

The Url to run the test against to.

Perform TCP Ping

If enabled, the TDA will verify network connectivity against that specific hostname and port number.

End Point Security – Process Security



ThinScale Desktop Agent Profile Editor

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

Enter text to search...

- Profile Details
- User Interface
- End Point Security
  - Dual Persona
  - Temporary Storage
  - Access Policies
  - Process Security
    - Process Sets
      - Process Identity Rules
    - Module Protection Rules
      - Module Identity Rules
    - Object Protection Rules
    - Volume Protection Rules
    - Registry Protection Rules
    - Registry Overlay Rules
  - Driver Protection
  - Service Protection
- Session Configuration
- Device Management

Process Security

☐ Disable Process Security and All System Protections

☑ Enable Process Security

☐ Passive Process Creation ☐ Passive Module Loading ☐ Passive Registry Restrictions

☐ Passive Volume Restrictions ☐ Passive Process Object Restrictions

☑ Block the process if it does not match any of the rules configured below ☐ Enable rule logging

Rule Name	Enabled
SYSTEM : Secure Session	Yes
SYSTEM : Protect System Services	Yes
SYSTEM : Protected System Service Access	Yes
SYSTEM : VMware Horizon VDA Support	Yes
SYSTEM : Allow Consent Process	Yes
SYSTEM : Allow Core OS Processes	Yes
SYSTEM : Allow Shell / UWP Support Processes	Yes
SYSTEM : Dual Persona - No Access	Yes
SYSTEM : Dual Persona - All Volumes Read Only	Yes
SYSTEM : Dual Persona - Read / Write	Yes
SYSTEM : Dual Persona - ProgramData	Yes
APP : Allow Common Web Browers	No
APP : Allow Vmware	Yes

Please Note: Rules may be different from these screen

Caution: Do not alter, amend, or remove SYSTEM rules. Modifying these rules may lead to instability in the TDA session.

Disable Process Security and All System Protections

If enabled, all the default rule applied by the Process Security engine will be disabled.

A restart is needed when applied.

Disabling this option is only recommended for troubleshooting.

Enable Process Security

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

Passive modes

If enabled, any of the Process Security function (Volume, Module, Registry, etc) will be ignored.

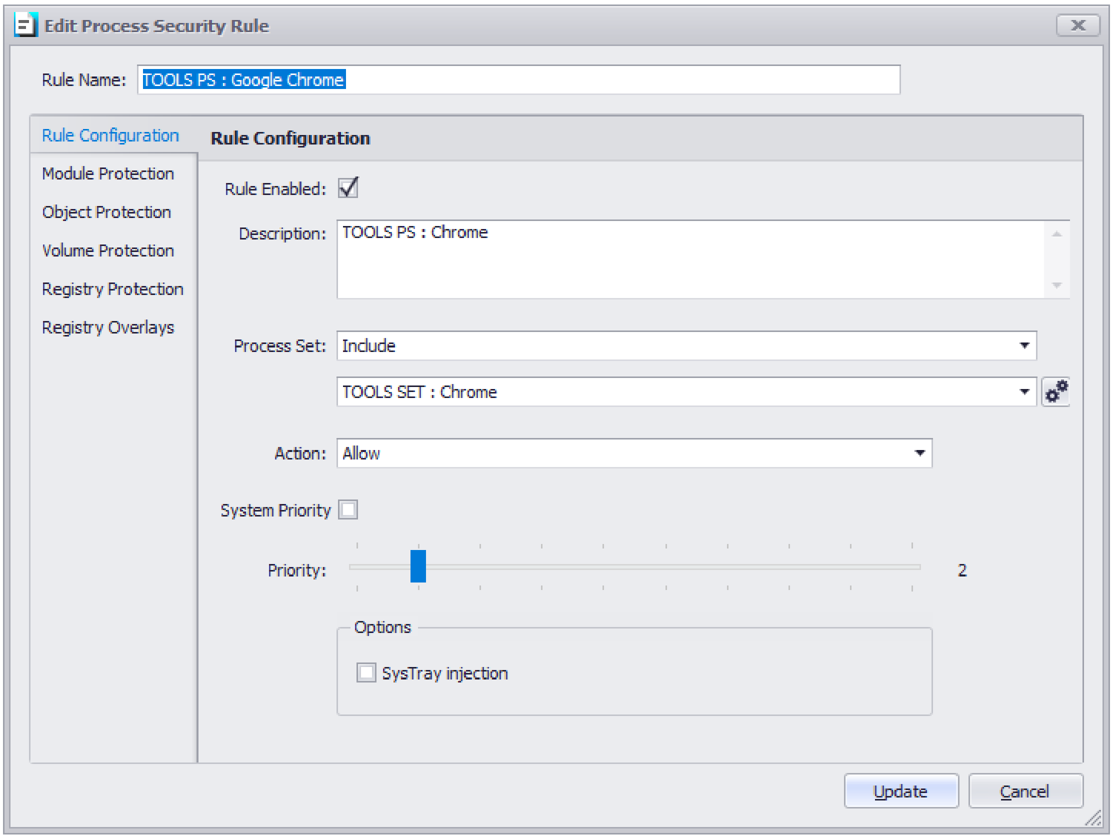
Enable rule logging

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

i.e., Google Chrome Allowed Rule



Rule Name: TOOLS PS : Google Chrome

Rule Configuration

Rule Enabled: ☑

Description: TOOLS PS : Chrome

Process Set: Include

TOOLS SET : Chrome

Action: Allow

System Priority □

Priority: 2

□ SysTray injection

Process Sets

A Process Sets is a repository where all your process identity (executable name, thumbprints, hashes and more) are stored.

Action

Specify the desired action (Allow/Block/No Action) to be applied to the processes listed.

System Priority

When activated, System Priority takes precedence over a standard priority, even when the latter is configured to a value of 10.

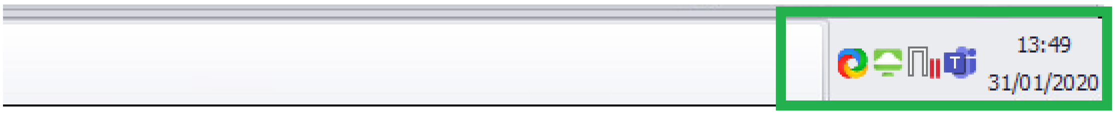
A System Priority will mandate the application of a rule ahead of any other rule within the process Set.

Priority

If activated, administrators have the option to assign elevated priority to processes, allowing the engine to prioritize this specific set of rules over others.

Systray Injection

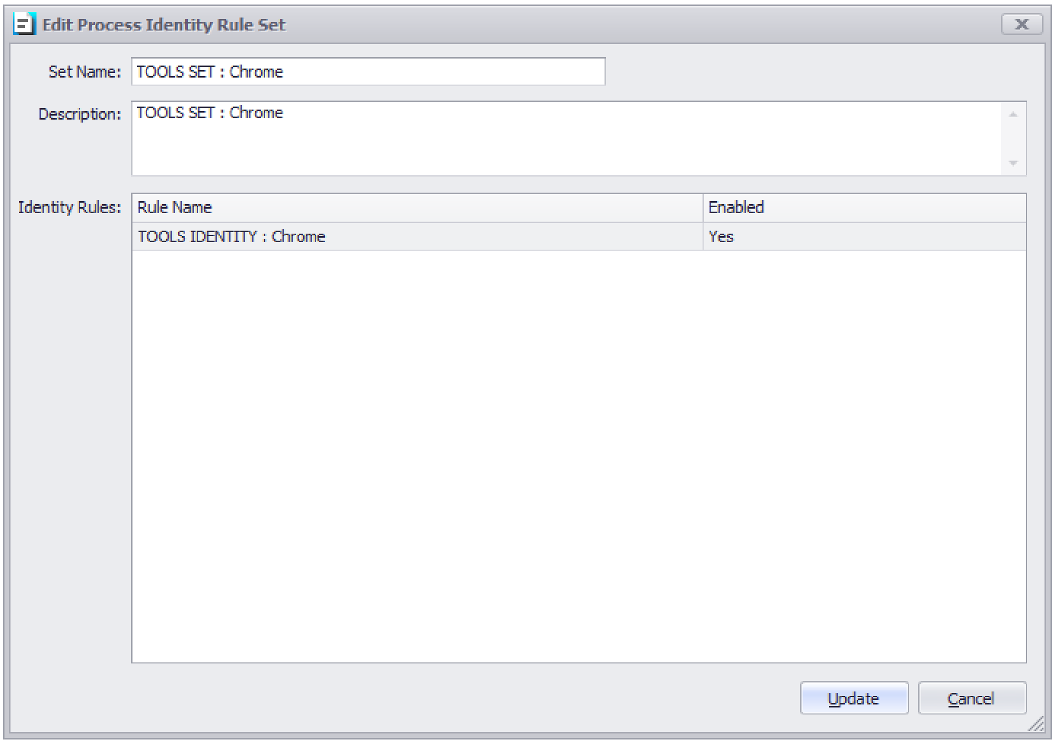
If enabled, process with the injection enabled can display their icons inside the left button system notification area.


13:49
31/01/2020

Process Identity

A process Identity entails the configuration by an administrator of criteria determining whether an executable is permitted or denied from execution.

i.e., Google Chrome



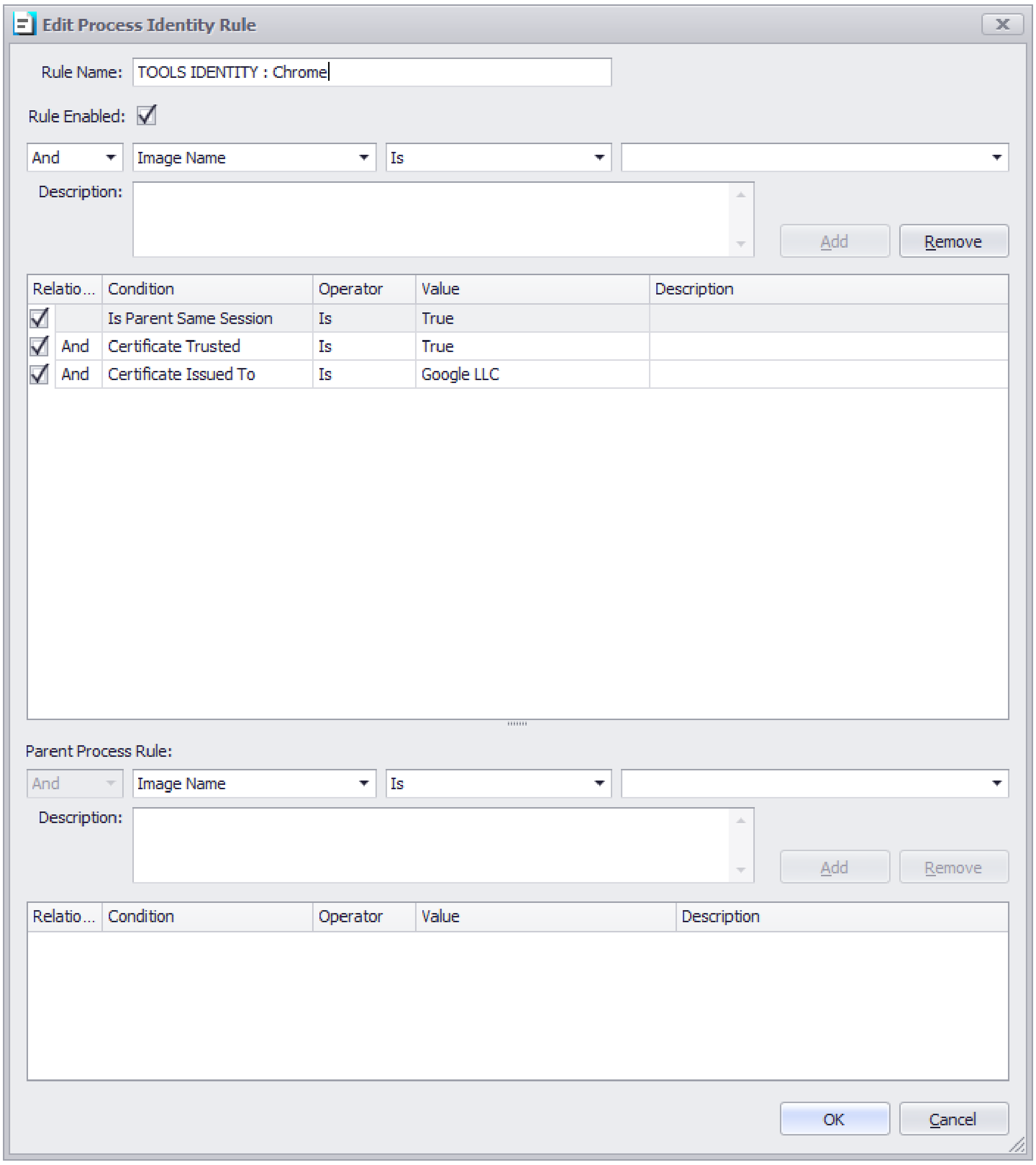
Set Name: TOOLS SET : Chrome

Description: TOOLS SET : Chrome

Identity Rules:

Rule Name	Enabled
TOOLS IDENTITY : Chrome	Yes

Please Note: Naming may be different in your console



Rule Name: TOOLS IDENTITY : Chrome

Rule Enabled: ☑

And | Image Name | Is

Description:

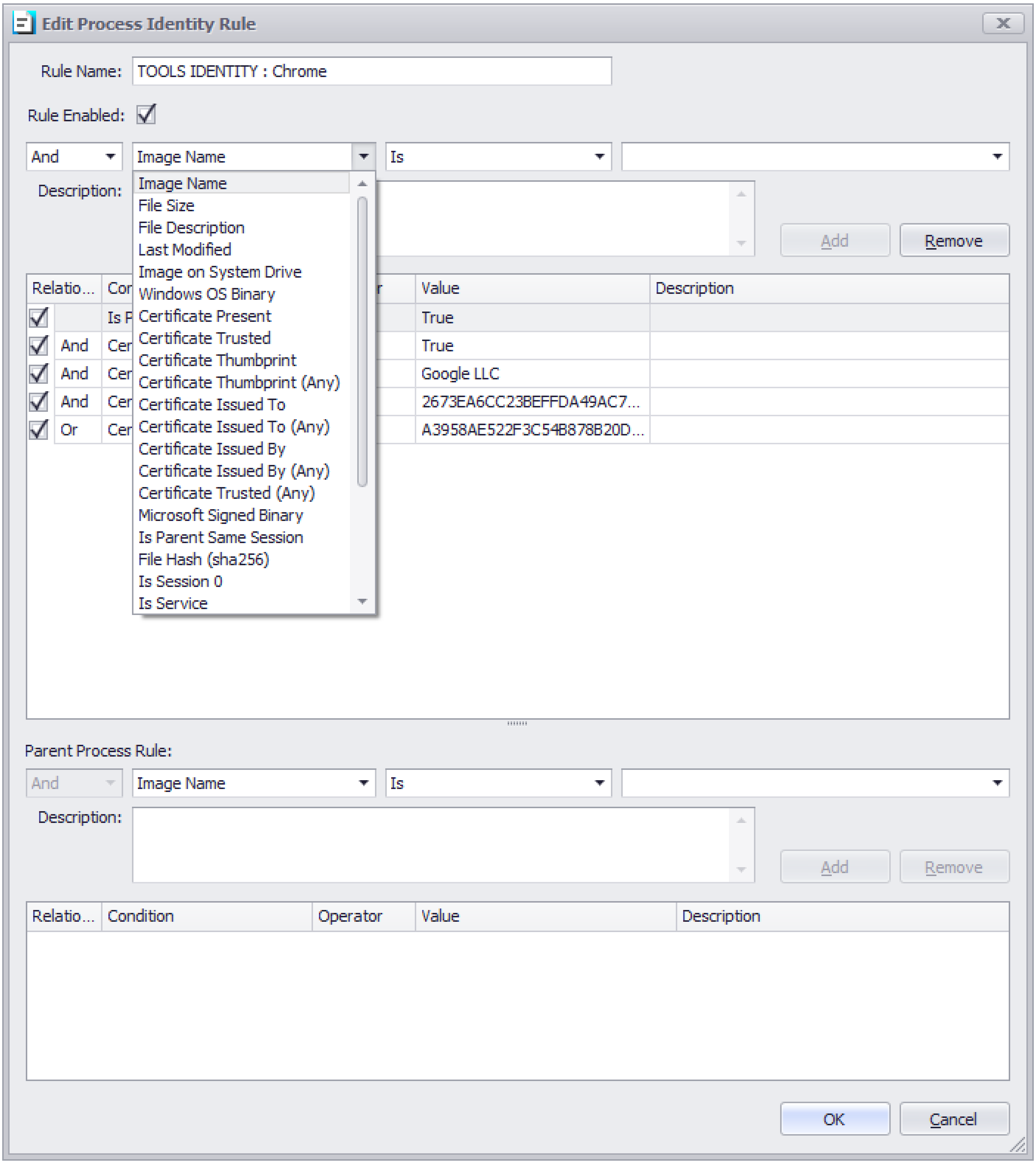
Relatio...	Condition	Operator	Value	Description
☑	Is Parent Same Session	Is	True	
☑ And	Certificate Trusted	Is	True	
☑ And	Certificate Issued To	Is	Google LLC	

Parent Process Rule:

And | Image Name | Is

Description:

Relatio...	Condition	Operator	Value	Description



Edit Process Identity Rule

Rule Name: TOOLS IDENTITY : Chrome

Rule Enabled: ☑

And | Image Name | Is |

Description:

	Relatio...	Cor	r	Value	Description
☑		Is P		True	
☑	And	Cer		True	
☑	And	Cer		Google LLC	
☑	And	Cer		2673EA6CC23BEFFDA49AC7...	
☑	Or	Cer		A3958AE522F3C54B878B20D...	

Parent Process Rule:

And | Image Name | Is |

Description:

Relatio...	Condition	Operator	Value	Description

Rule Name

Describe the name of the rule to be applied.

Action

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

Adding a rule

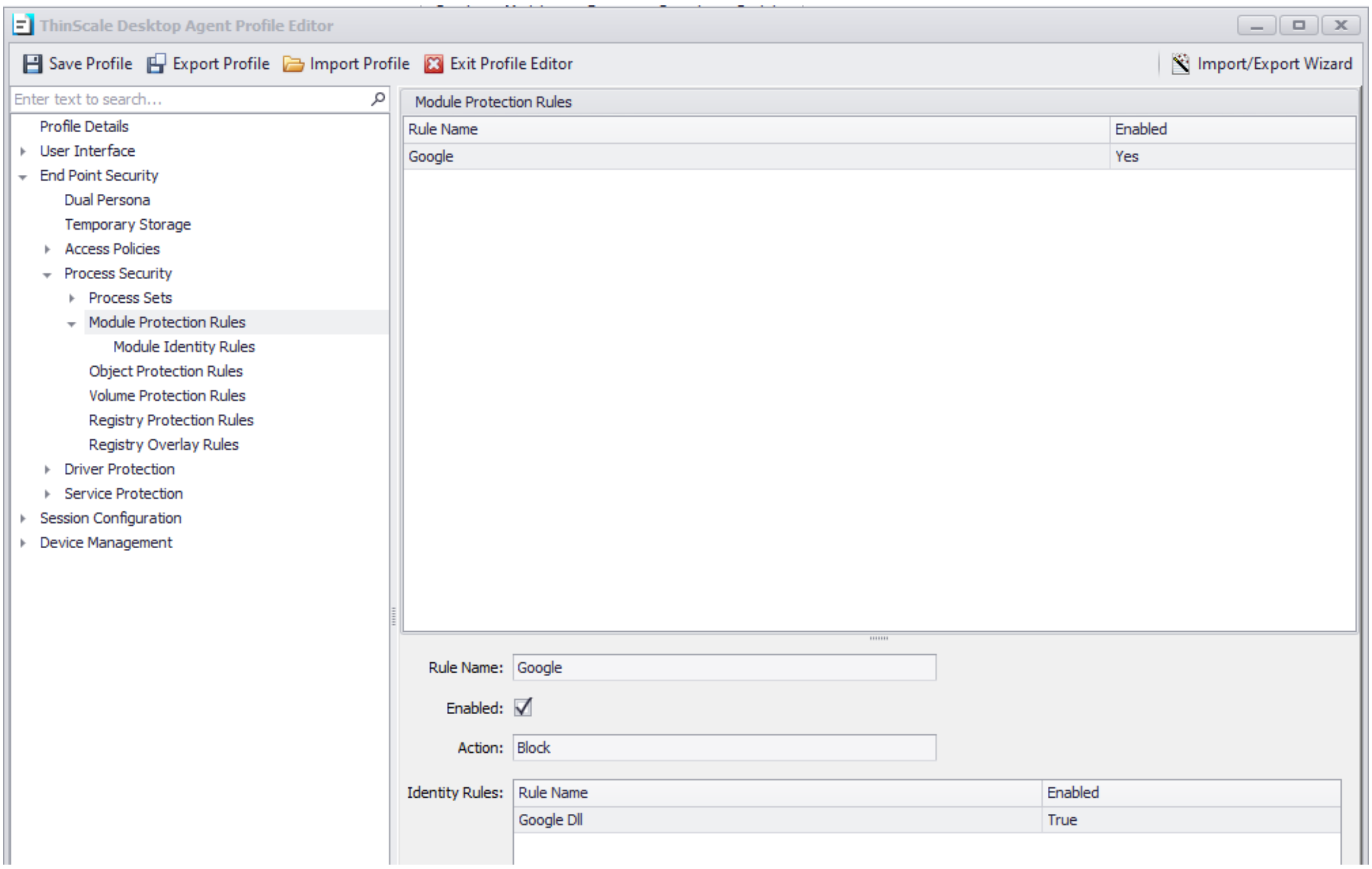
When creating a rule, there are relationships and conditions you can use to match or not a specific file name, size of the file, last modified date and time, Windows OS binary and all the other options in the profile editor.

An example of the rule can be seen in the screenshot below. The rule will allow execution, the locally installed Chrome application.

WARNING:

Process Security is a system-level function that can prevent a system from operating correctly until the active TDA profile is corrected and reloaded. By default, TDA applications will be allowed once verified by a signed security certificate. Blocking all applications without any rules defined will prevent the TDA session from launching correctly.

End Point Security – Module Protection Rule



Rule Name	Enabled
Google	Yes

Rule Name: Google

Enabled: ☑

Action: Block

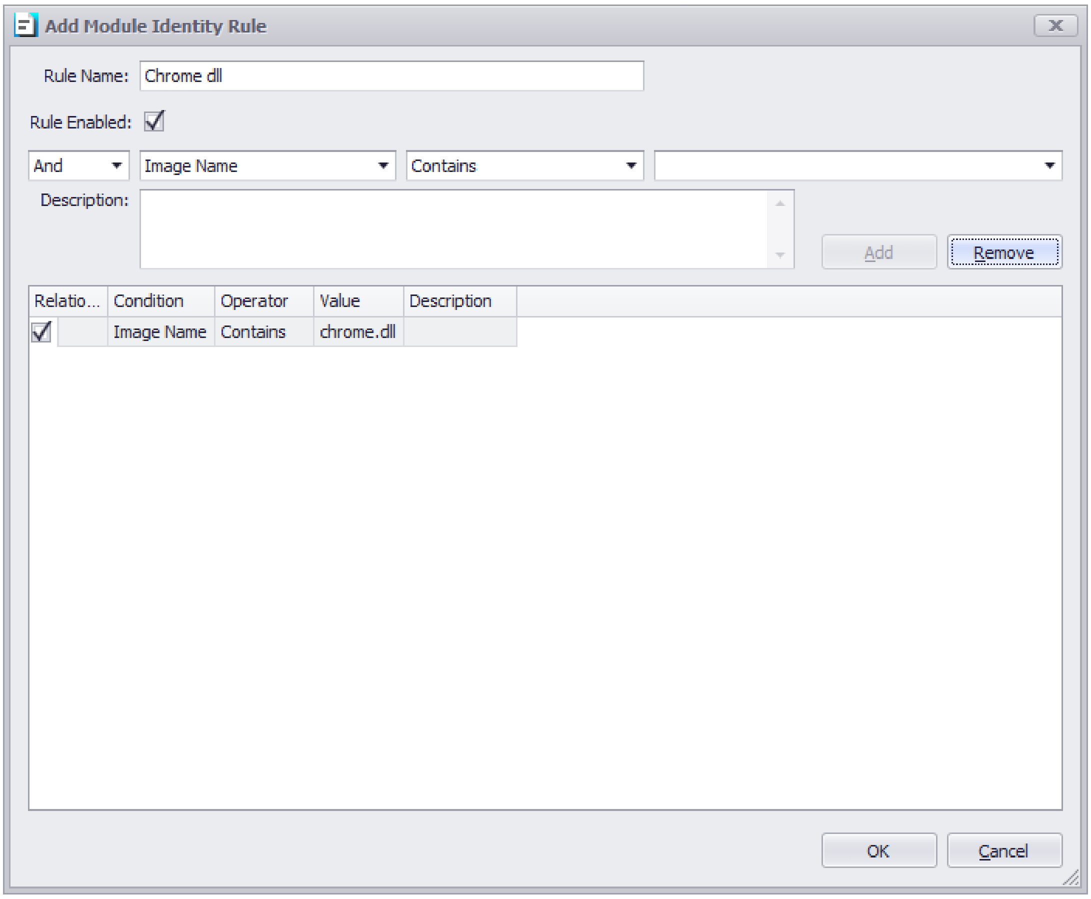
Identity Rules:

Rule Name	Enabled
Google Dll	True

Module Protection provides control over what application modules (DLL's) are allowed to be loaded by applications running when the TDA 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, TDA will terminate the process or optionally log the user out of the TDA session if selected in the profile.

i.e., Google



Add Module Identity Rule

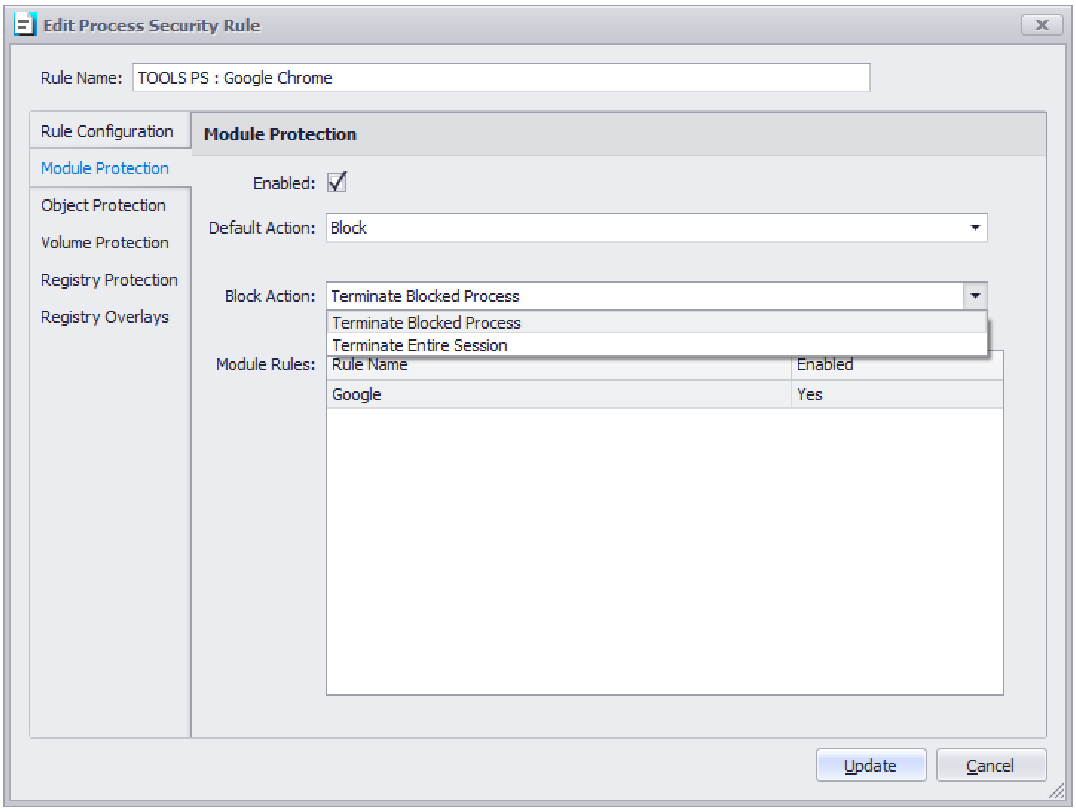
Rule Name: Chrome dll

Rule Enabled: ☑

And | Image Name | Contains |

Description:

Relatio...	Condition	Operator	Value	Description
☑	Image Name	Contains	chrome.dll	



Edit Process Security Rule

Rule Name: TOOLS PS : Google Chrome

Module Protection

Enabled: ☑

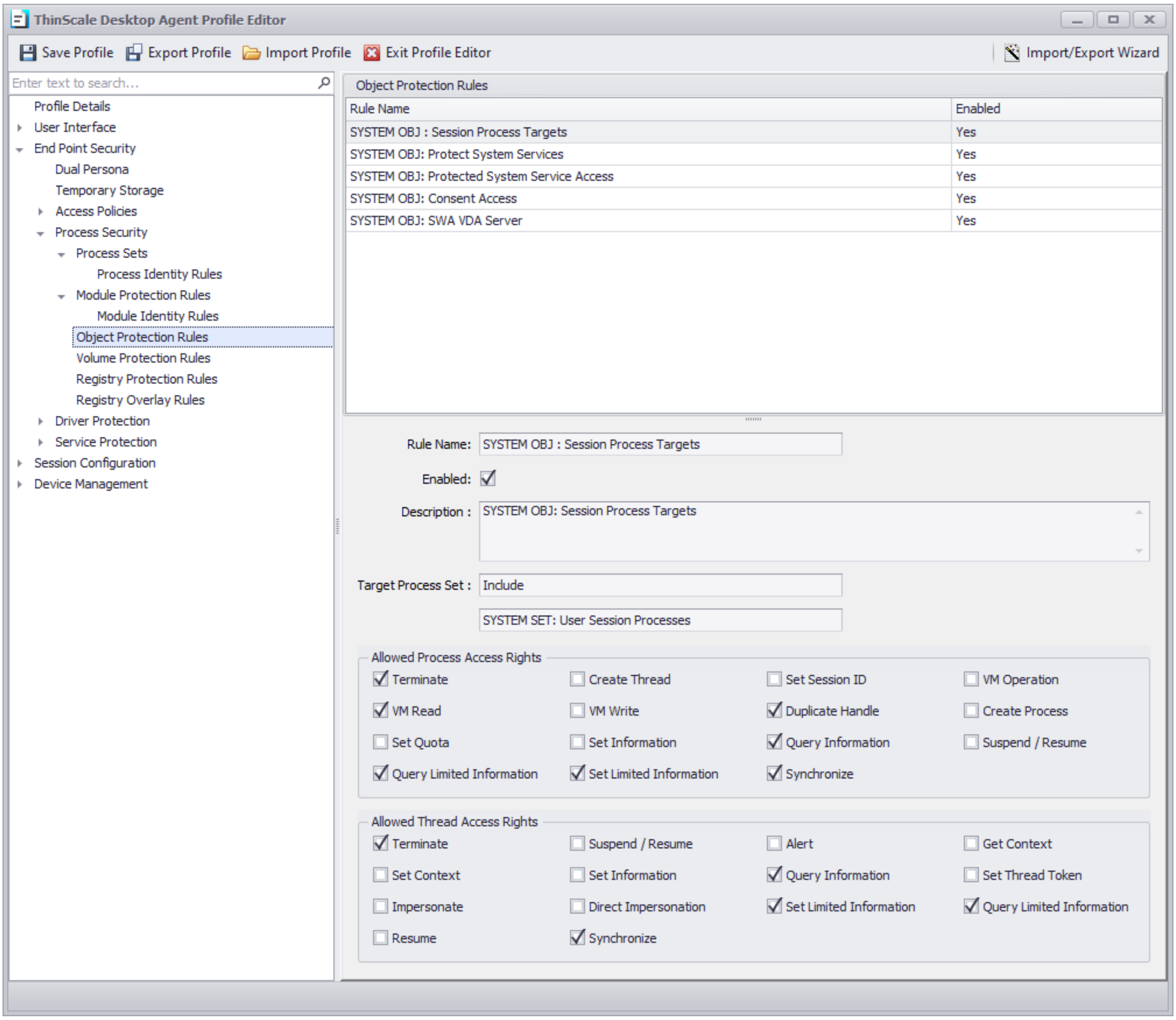
Default Action: Block

Block Action: Terminate Blocked Process

Module Rules:

Rule Name	Enabled
Google	Yes

End Point Security – Object Protection Rules



ThinScale Desktop Agent Profile Editor

- Profile Details
- User Interface
- End Point Security
  - Dual Persona
  - Temporary Storage
  - Access Policies
  - Process Security
    - Process Sets
      - Process Identity Rules
    - Module Protection Rules
      - Module Identity Rules
    - Object Protection Rules
    - Volume Protection Rules
    - Registry Protection Rules
    - Registry Overlay Rules
  - Driver Protection
  - Service Protection
- Session Configuration
- Device Management

Object Protection Rules

Rule Name	Enabled
SYSTEM OBJ : Session Process Targets	Yes
SYSTEM OBJ: Protect System Services	Yes
SYSTEM OBJ: Protected System Service Access	Yes
SYSTEM OBJ: Consent Access	Yes
SYSTEM OBJ: SWA VDA Server	Yes

Rule Name: SYSTEM OBJ : Session Process Targets

Enabled: ☑

Description : SYSTEM OBJ: Session Process Targets

Target Process Set : Include

SYSTEM SET: User Session Processes

Allowed Process Access Rights

☑ Terminate	□ Create Thread	□ Set Session ID	□ VM Operation
☑ VM Read	□ VM Write	☑ Duplicate Handle	□ Create Process
□ Set Quota	□ Set Information	☑ Query Information	□ Suspend / Resume
☑ Query Limited Information	☑ Set Limited Information	☑ Synchronize	

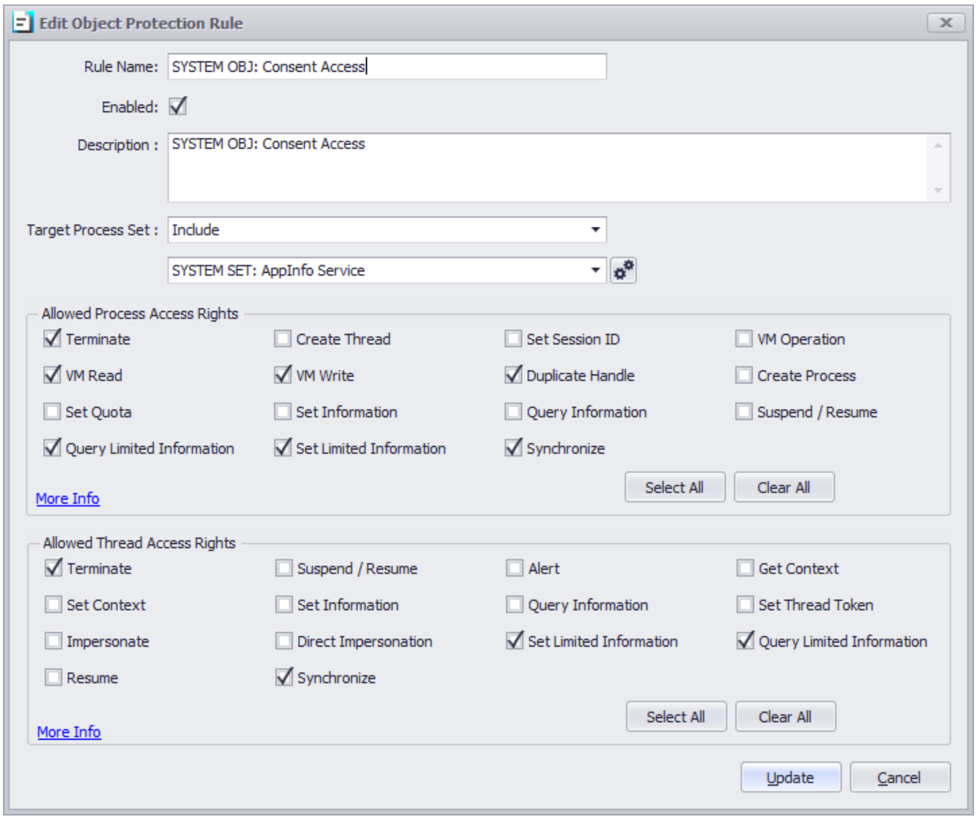
Allowed Thread Access Rights

☑ Terminate	□ Suspend / Resume	□ Alert	□ Get Context
□ Set Context	□ Set Information	☑ Query Information	□ Set Thread Token
□ Impersonate	□ Direct Impersonation	☑ Set Limited Information	☑ Query Limited Information
□ Resume	☑ Synchronize		

Object Protection Rules provides control over what level of access rights processes and threads are allowed to have.

More information can be found here or here.

In our example, the Consent Process will only have specific rights assigned to its executables.



Edit Object Protection Rule

Rule Name: SYSTEM OBJ: Consent Access

Enabled: ☑

Description : SYSTEM OBJ: Consent Access

Target Process Set : Include

SYSTEM SET: AppInfo Service

Allowed Process Access Rights

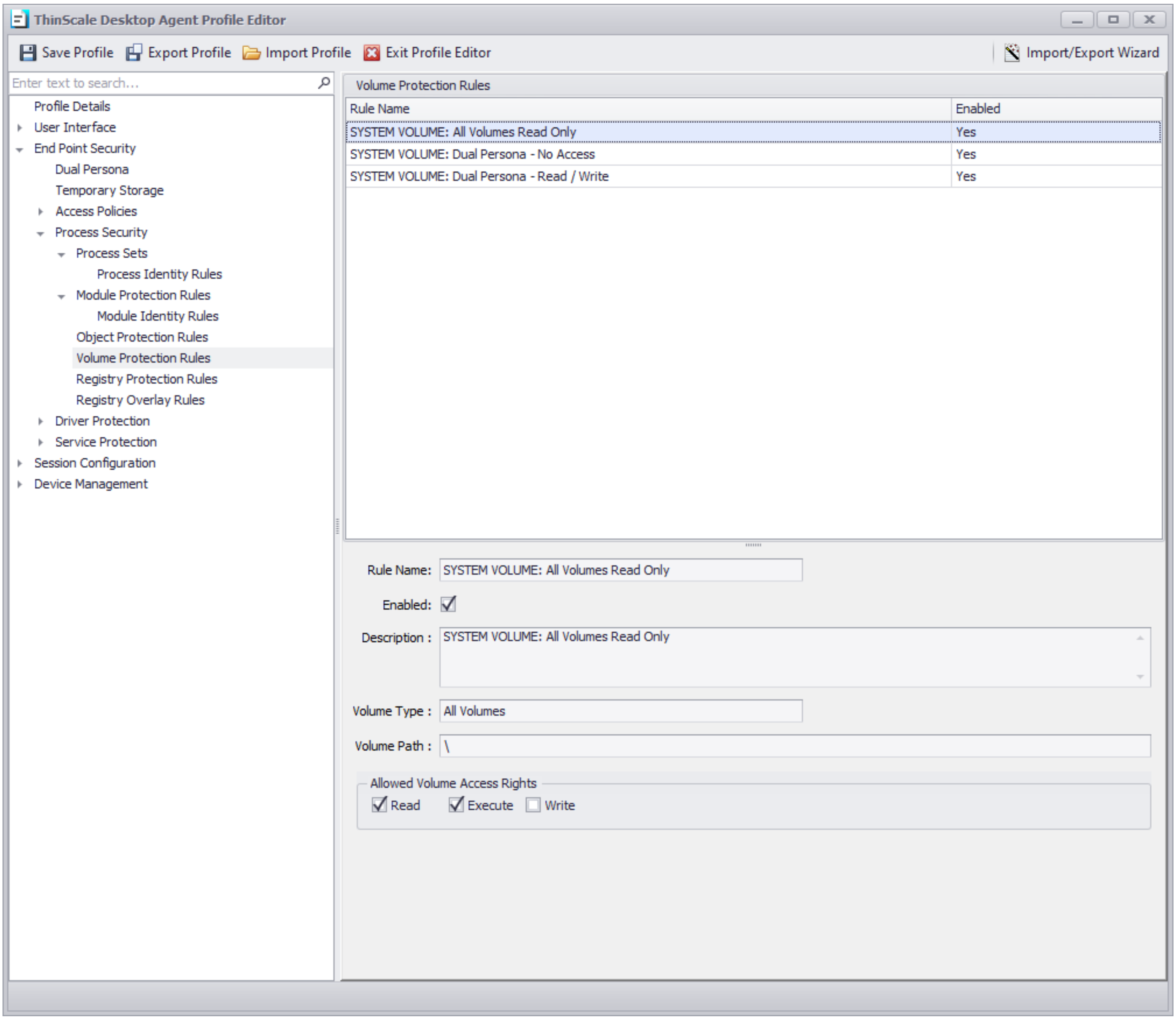
☑ Terminate	□ Create Thread	□ Set Session ID	□ VM Operation
☑ VM Read	☑ VM Write	☑ Duplicate Handle	□ Create Process
□ Set Quota	□ Set Information	□ Query Information	□ Suspend / Resume
☑ Query Limited Information	☑ Set Limited Information	☑ Synchronize	

Allowed Thread Access Rights

☑ Terminate	□ Suspend / Resume	□ Alert	□ Get Context
□ Set Context	□ Set Information	□ Query Information	□ Set Thread Token
□ Impersonate	□ Direct Impersonation	☑ Set Limited Information	☑ Query Limited Information
□ Resume	☑ Synchronize		

An Object Protection Rule will be usually coupled with a Process Sets and Identity rule and the “consent” is an example of. If we look at the Process Identity for the “Consent Processes”, only the processes that matches these following rules will be allowed to have the Object Protection Rule.

End Point Security – Volume Protection Rules



Rule Name	Enabled
SYSTEM VOLUME: All Volumes Read Only	Yes
SYSTEM VOLUME: Dual Persona - No Access	Yes
SYSTEM VOLUME: Dual Persona - Read / Write	Yes

Rule Name: SYSTEM VOLUME: All Volumes Read Only

Enabled: ☑

Description : SYSTEM VOLUME: All Volumes Read Only

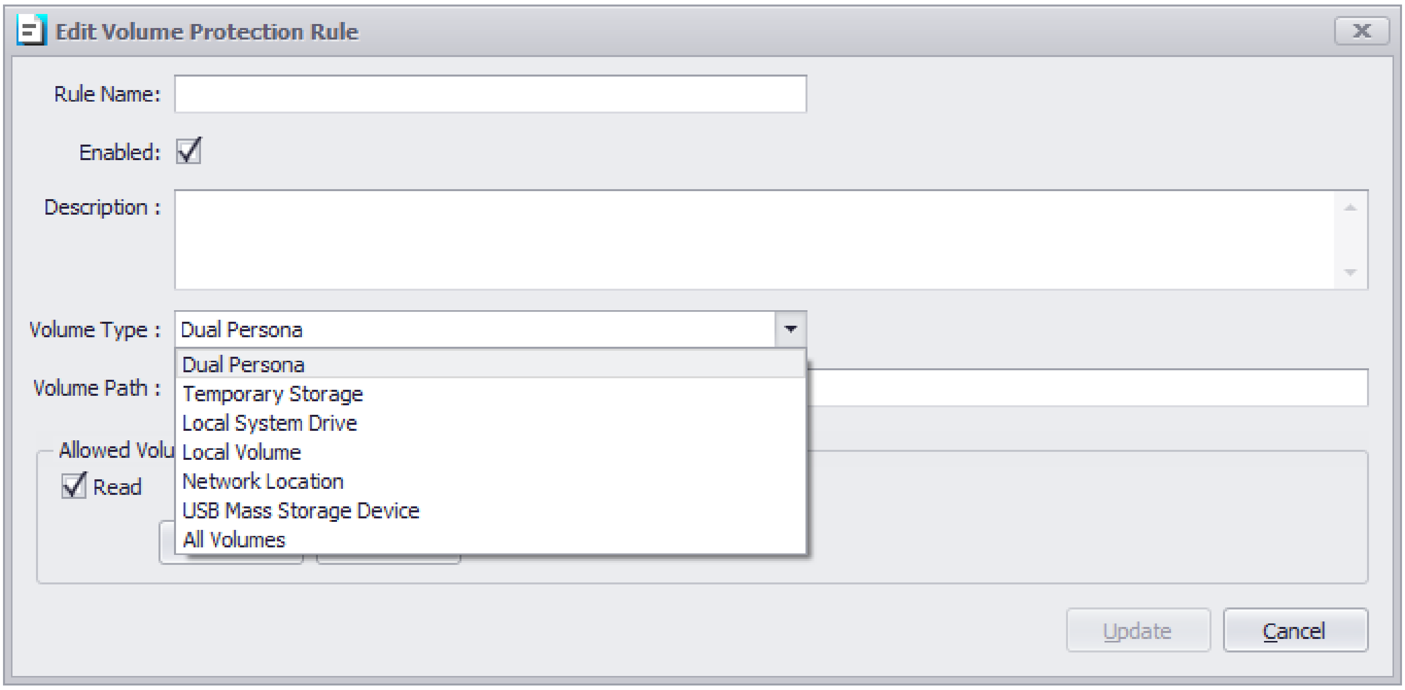
Volume Type : All Volumes

Volume Path : \

Allowed Volume Access Rights

☑ Read ☑ Execute □ Write

Volume Protection Rules provides control over what level of access a process has against a particular volume.



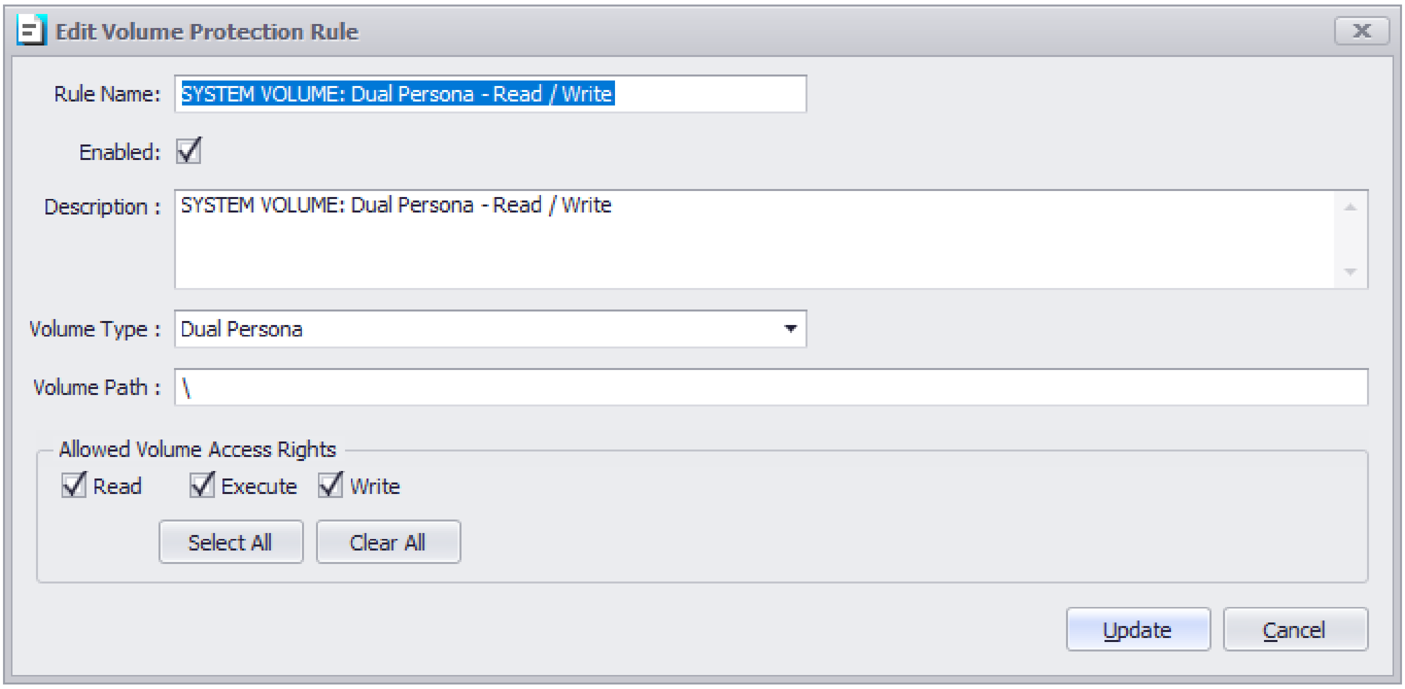
Edit Volume Protection Rule

Rule Name:

Enabled: ☑

Description :

Volume Type : Dual Persona



Edit Volume Protection Rule

Rule Name: SYSTEM VOLUME: Dual Persona - Read / Write

Enabled: ☑

Description : SYSTEM VOLUME: Dual Persona - Read / Write

Volume Type : Dual Persona

Volume Path : \

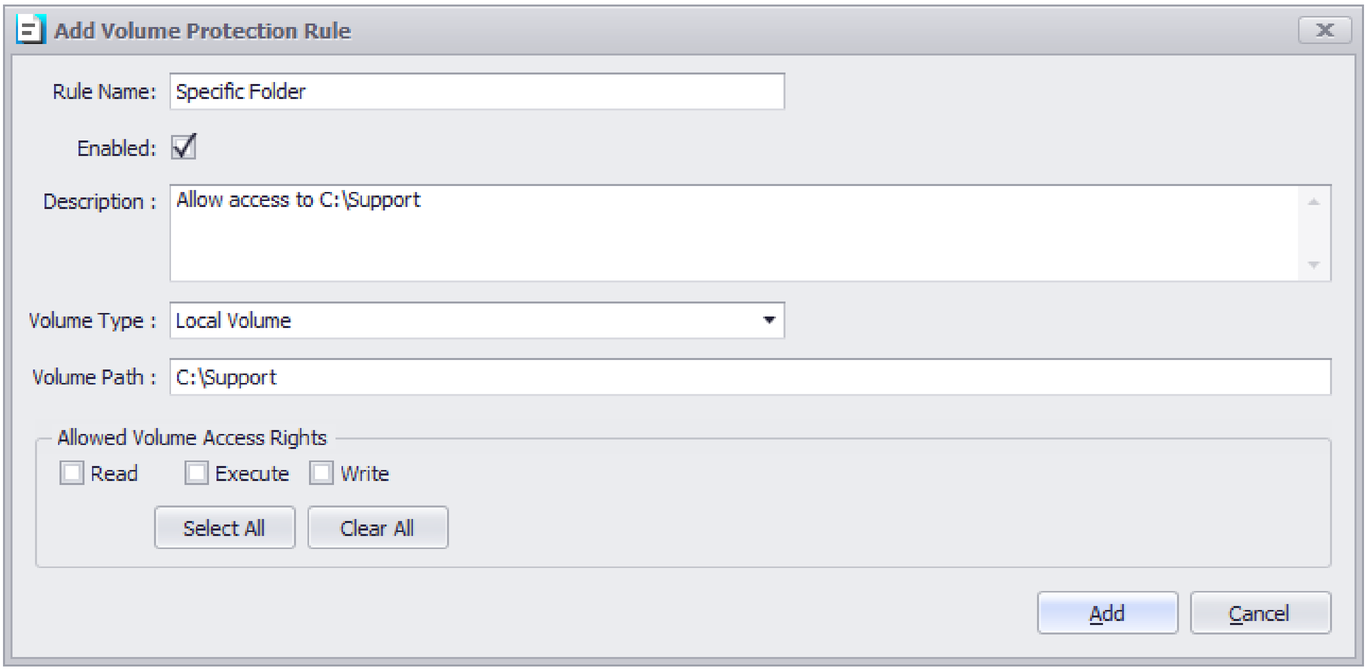
Allowed Volume Access Rights

☑ Read ☑ Execute ☑ Write

In this example the Dual Persona Volume has Full Access to Read, Write and Execute.

Note: the “\” in the rule will automatically translate the location of the Dual Persona volume. You do NOT need to specify any letters.

To give access to a specific folder please use the Local Volume rule lithe the following:



Add Volume Protection Rule

Rule Name: Specific Folder

Enabled: ☑

Description : Allow access to C:\Support

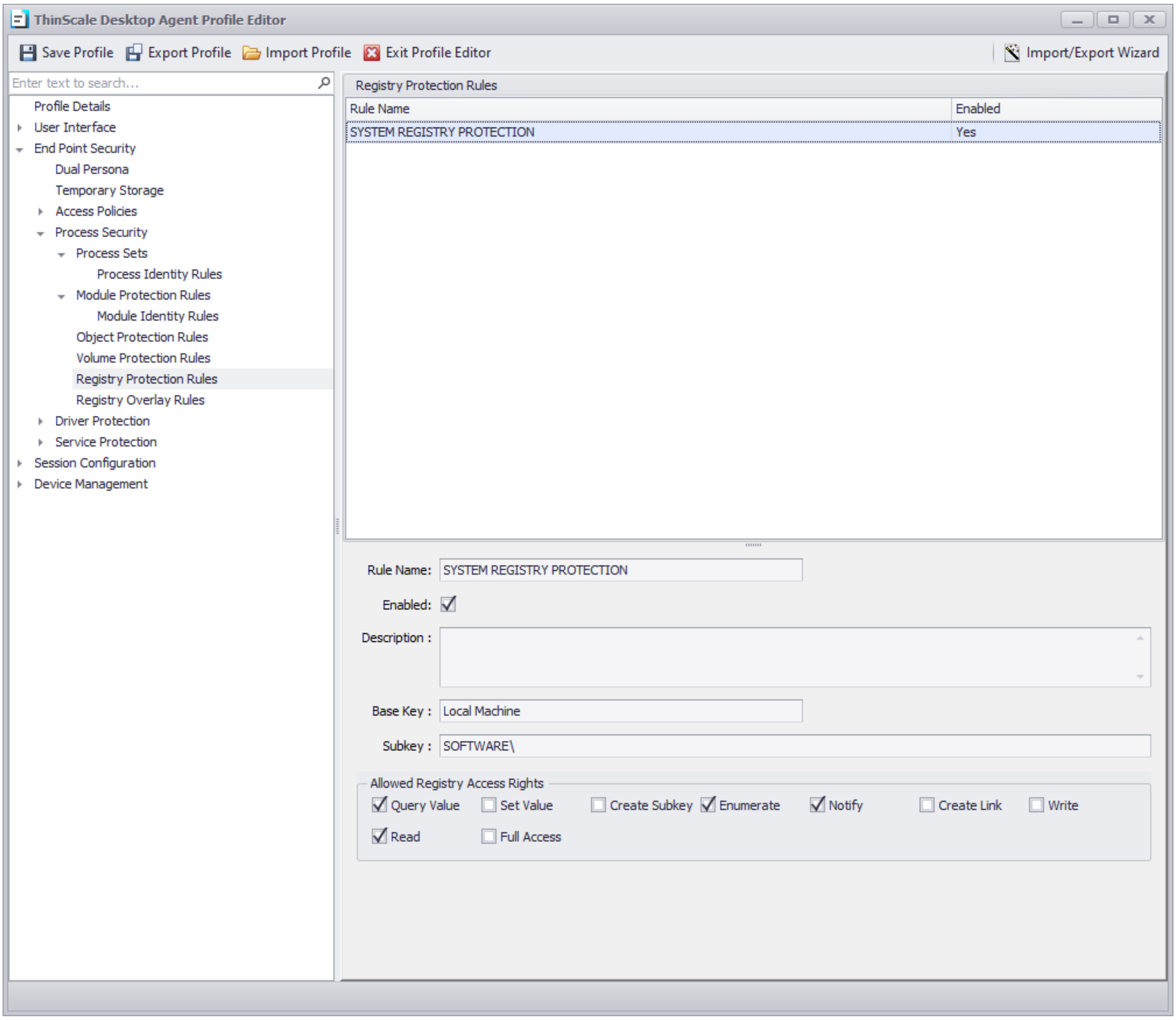
Volume Type : Local Volume

Volume Path : C:\Support

Allowed Volume Access Rights

□ Read □ Execute □ Write

End Point Security – Registry Protection Rules



Rule Name	Enabled
SYSTEM REGISTRY PROTECTION	Yes

Rule Name: SYSTEM REGISTRY PROTECTION

Enabled: ☑

Description :

Base Key : Local Machine

Subkey : SOFTWARE\

Allowed Registry Access Rights

☑ Query Value ☐ Set Value ☐ Create Subkey ☑ Enumerate ☑ Notify ☐ Create Link ☐ Write

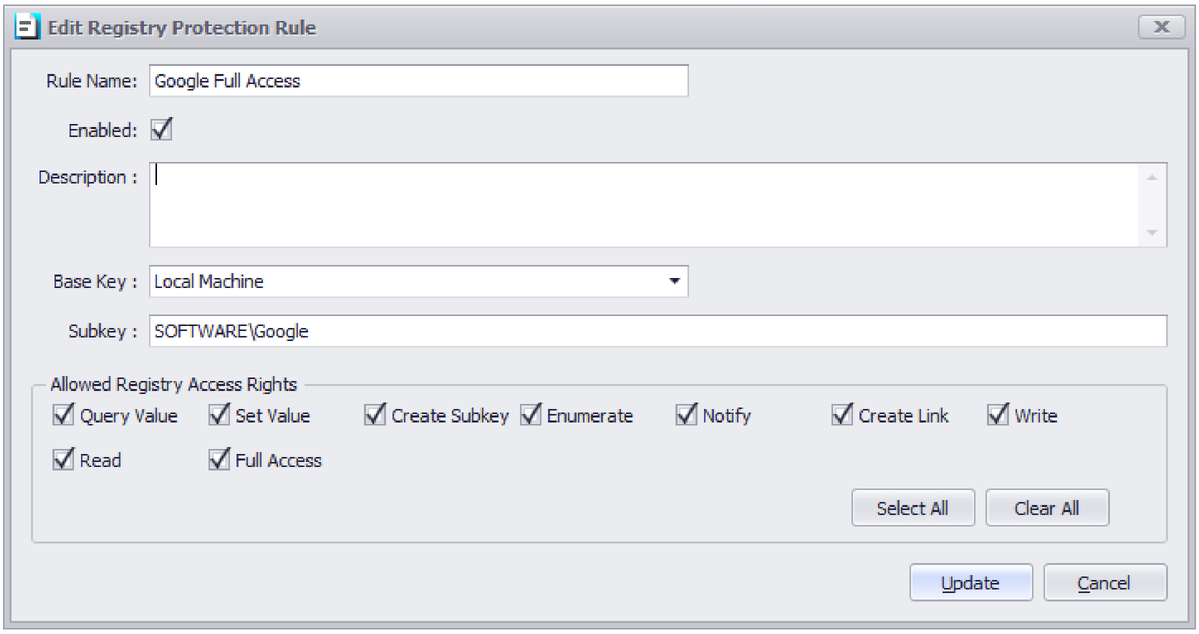
☑ Read ☐ Full Access

Please Note: naming may be different in your profile

Registry Protection is a security layer exclusively for Registry Key hives.

More information can be found here.

i.e., Google Chrome



Edit Registry Protection Rule

Rule Name: Google Full Access

Enabled: ☑

Description :

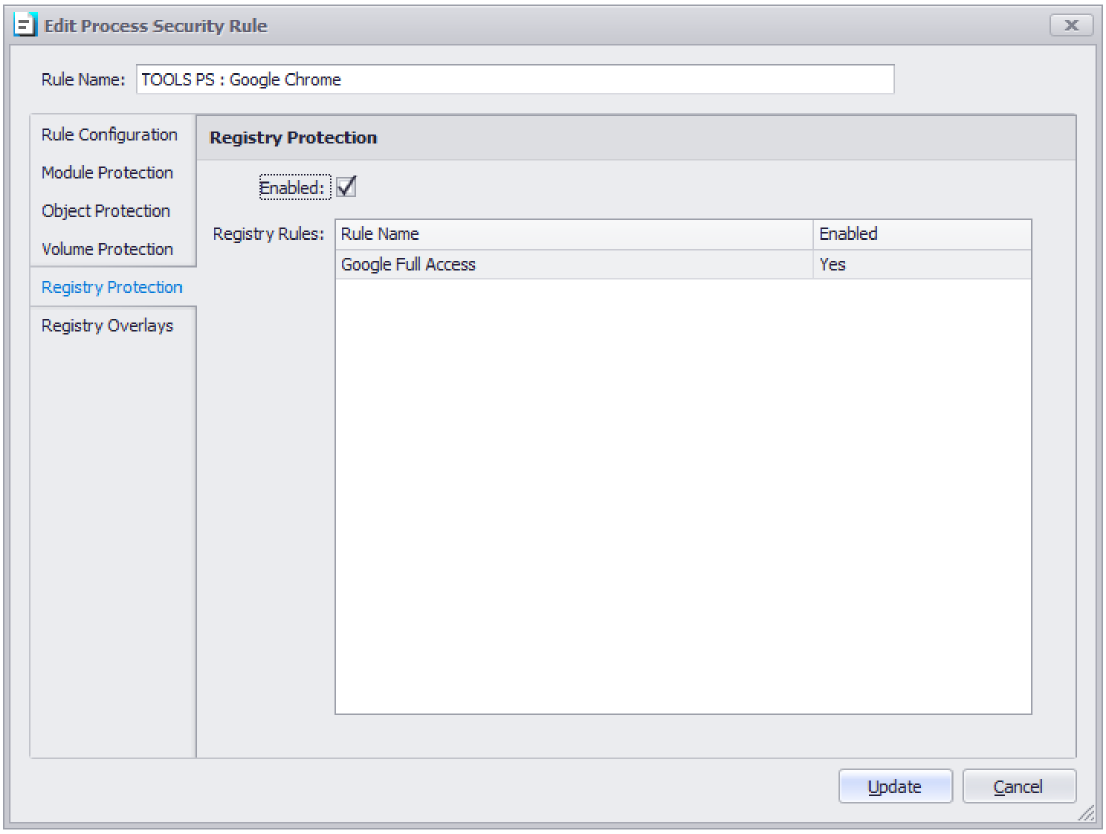
Base Key : Local Machine

Subkey : SOFTWARE\Google

Allowed Registry Access Rights

☑ Query Value ☑ Set Value ☑ Create Subkey ☑ Enumerate ☑ Notify ☑ Create Link ☑ Write

☑ Read ☑ Full Access



Edit Process Security Rule

Rule Name: TOOLS PS : Google Chrome

Registry Protection

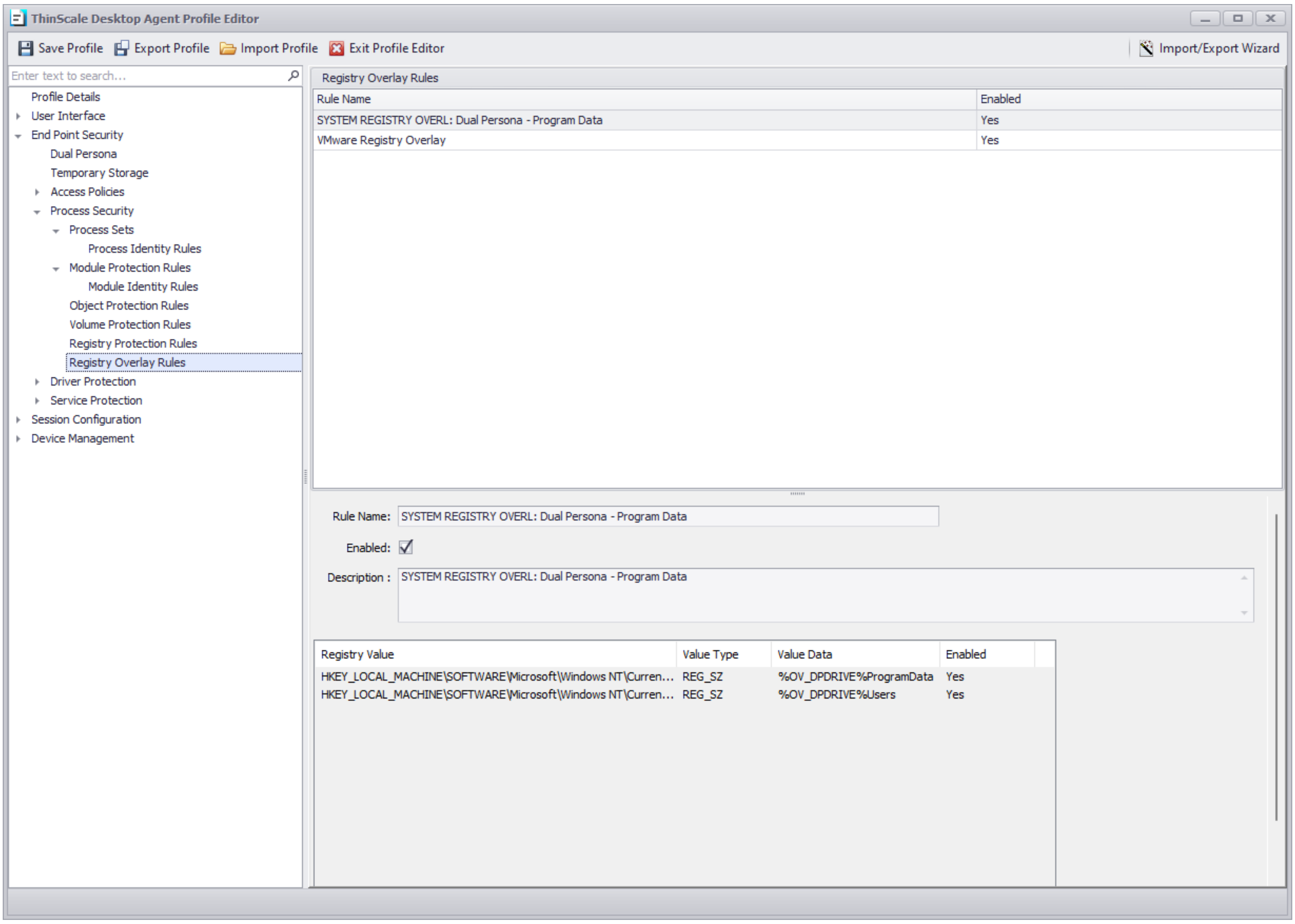
Enabled: ☑

Registry Rules:

Rule Name	Enabled
Google Full Access	Yes

When allowing a Registry Protection rule like the above, the system will work from the top down in a cascading order and will allow access to **SOFTWARE** first and then **Google** hive.

End Point Security – Registry Overlay Rule



Registry Overlay Rules

Rule Name	Enabled
SYSTEM REGISTRY OVERL: Dual Persona - Program Data	Yes
VMware Registry Overlay	Yes

Rule Name: SYSTEM REGISTRY OVERL: Dual Persona - Program Data

Enabled: ☑

Description : SYSTEM REGISTRY OVERL: Dual Persona - Program Data

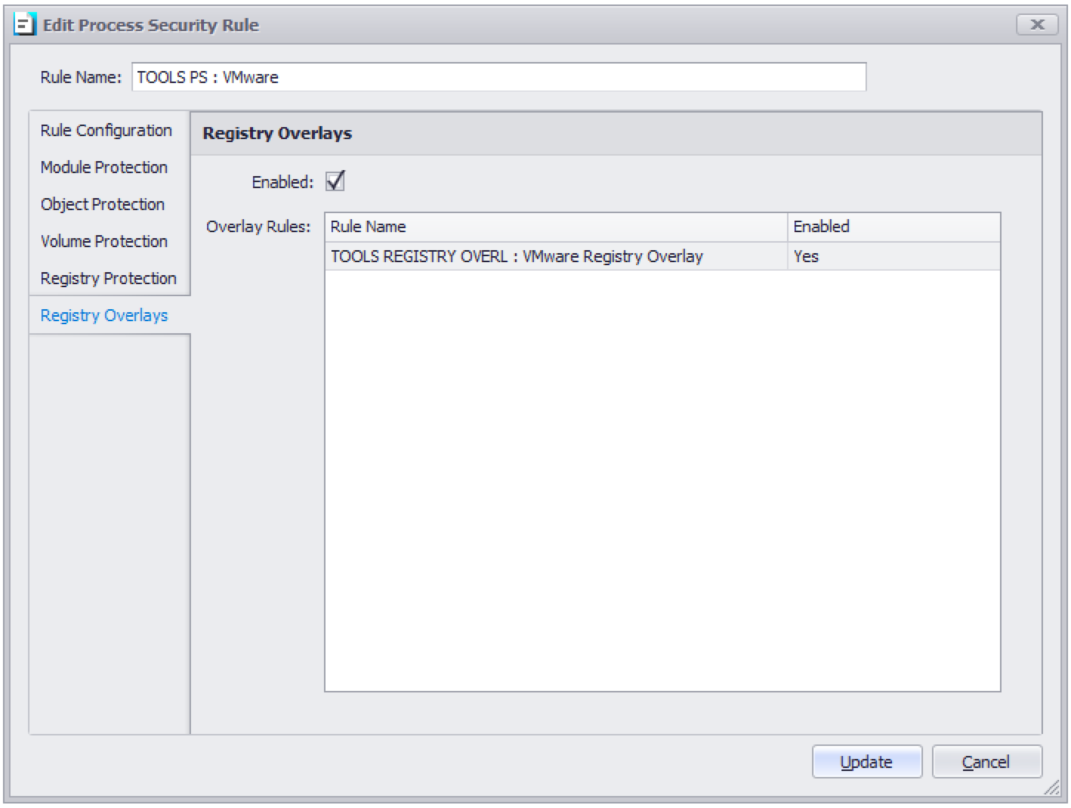
Registry Value	Value Type	Value Data	Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Curren…	REG_SZ	%OV_DPDRIVE%ProgramData	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Curren…	REG_SZ	%OV_DPDRIVE%Users	Yes

Please Note: naming may be different in your profile

Registry Overlay is used to apply specific registry key only to a specific Process Set.

Unlike Additional Registry keys which apply to every process in the system, Registry Overlays are only applicable and seen by the processes identified by the associated Process Security Rule.

i.e., Vmware



Edit Process Security Rule

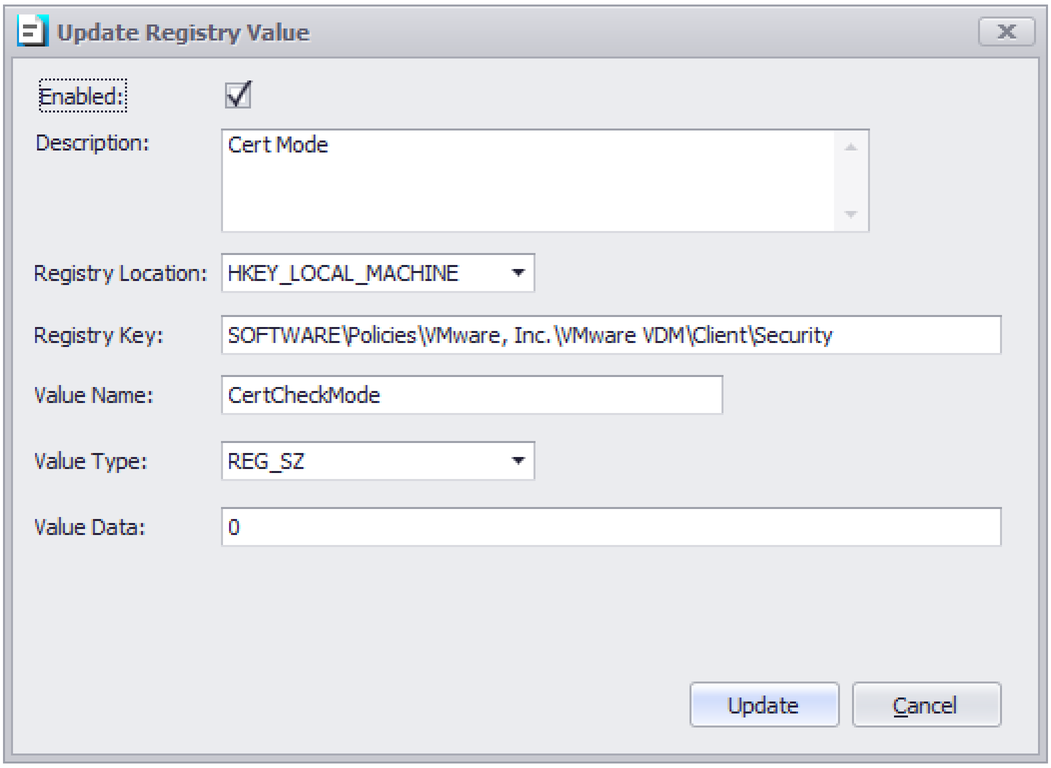
Rule Name: TOOLS PS : VMware

Registry Overlays

Enabled: ☑

Overlay Rules:

Rule Name	Enabled
TOOLS REGISTRY OVERL : VMware Registry Overlay	Yes



Update Registry Value

Enabled: ☑

Description: Cert Mode

Registry Location: HKEY_LOCAL_MACHINE

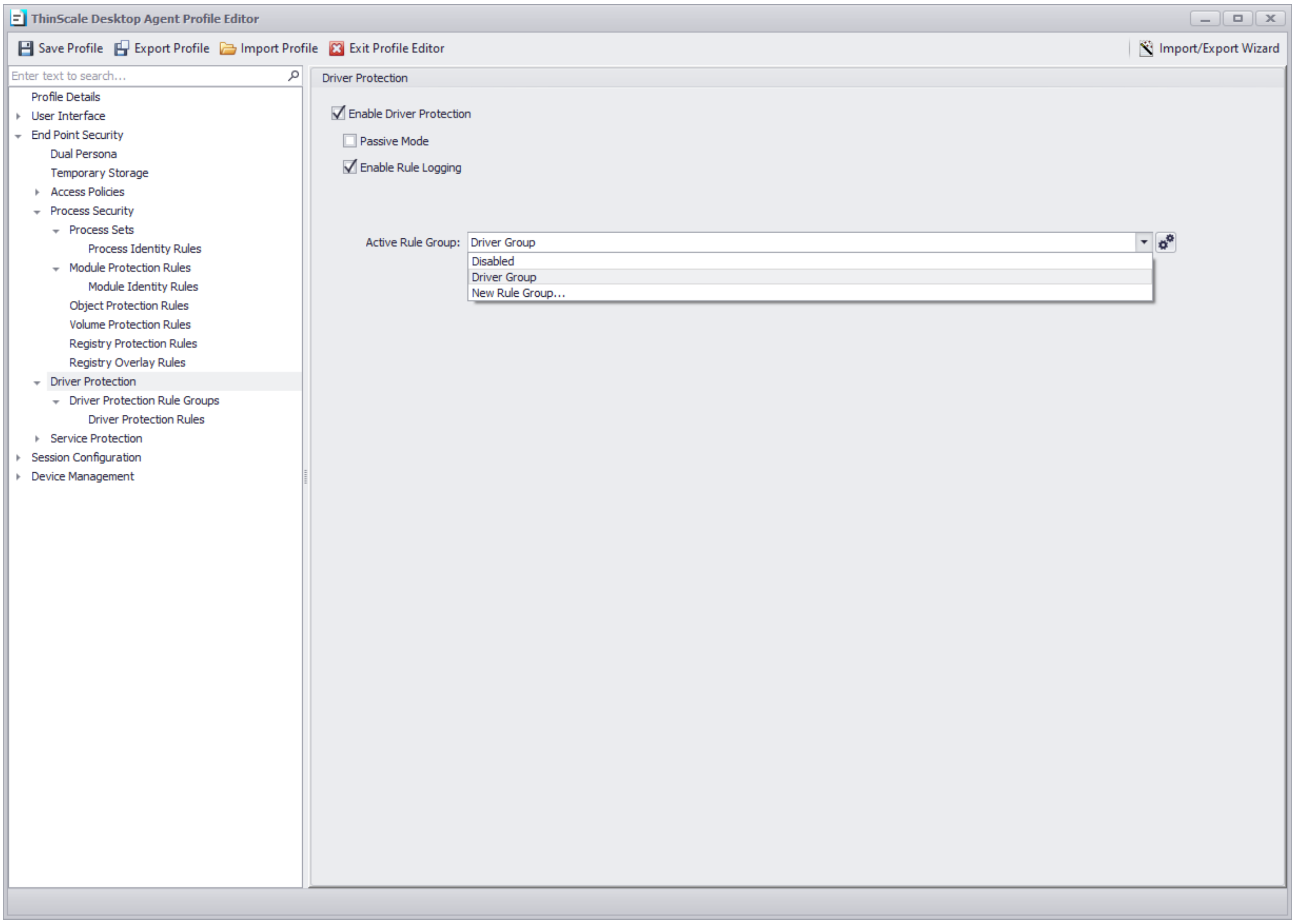
Registry Key: SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\Security

Value Name: CertCheckMode

Value Type: REG_SZ

Value Data: 0

End Point Security – Driver Protection



☑ Enable Driver Protection

□ Passive Mode

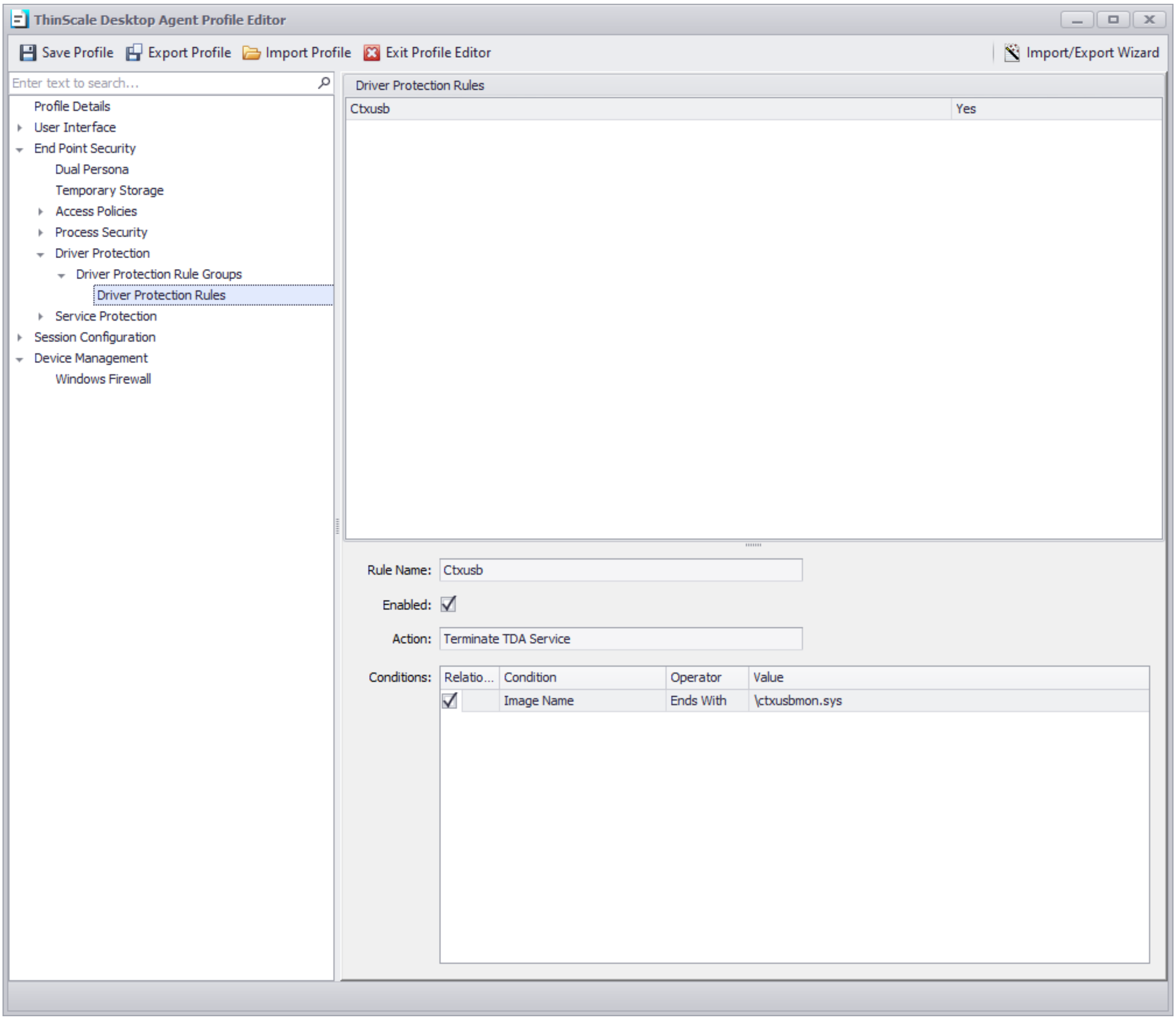
☑ Enable Rule Logging

Active Rule Group: Driver Group

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, TDA will not run.

i.e., Citrix



Driver Protection Rules

Ctxusb	Yes

Rule Name: Ctxusb

Enabled: ☑

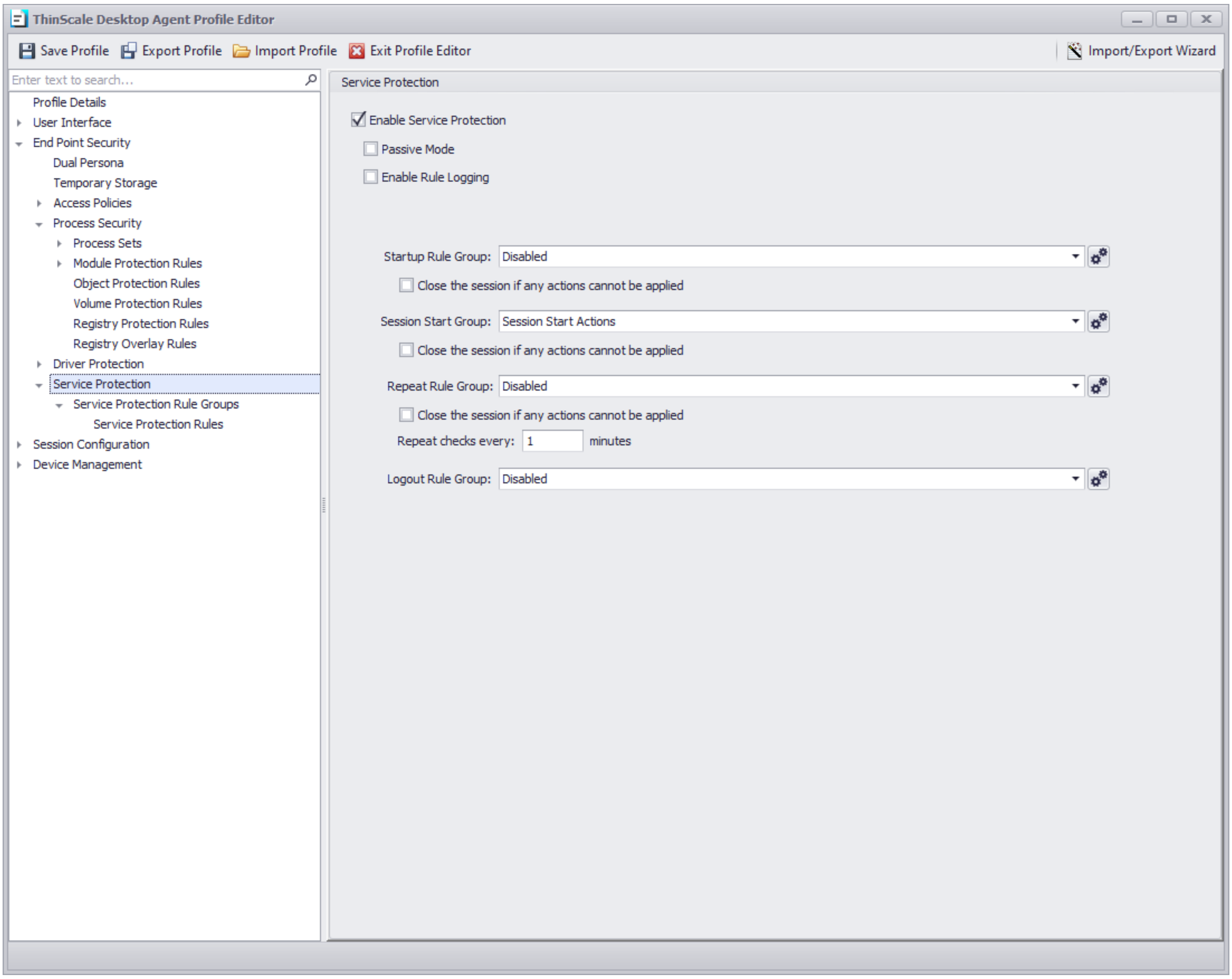
Action: Terminate TDA Service

Conditions:

Relatio...	Condition	Operator	Value
☑	Image Name	Ends With	\ctxusbmon.sys

In this illustration, should the Citrix driver be detected as mounted during the initiation of the TDA session, the activation of the session by TDA will be prevented.

End Point Security – Service Protection



Service Protection

☑ Enable Service Protection

□ Passive Mode

□ Enable Rule Logging

Startup Rule Group: Disabled

□ Close the session if any actions cannot be applied

Session Start Group: Session Start Actions

□ Close the session if any actions cannot be applied

Repeat Rule Group: Disabled

□ Close the session if any actions cannot be applied

Repeat checks every: 1 minutes

Logout Rule Group: Disabled

Service Protection builds on existing Process Security technology to provide Windows services execution control at the system level. An administrator can define rules for a profile to control what services can run or should be stopped. Control is asserted overall service applications including all Windows services.

Service Protection has 4 areas of operation:

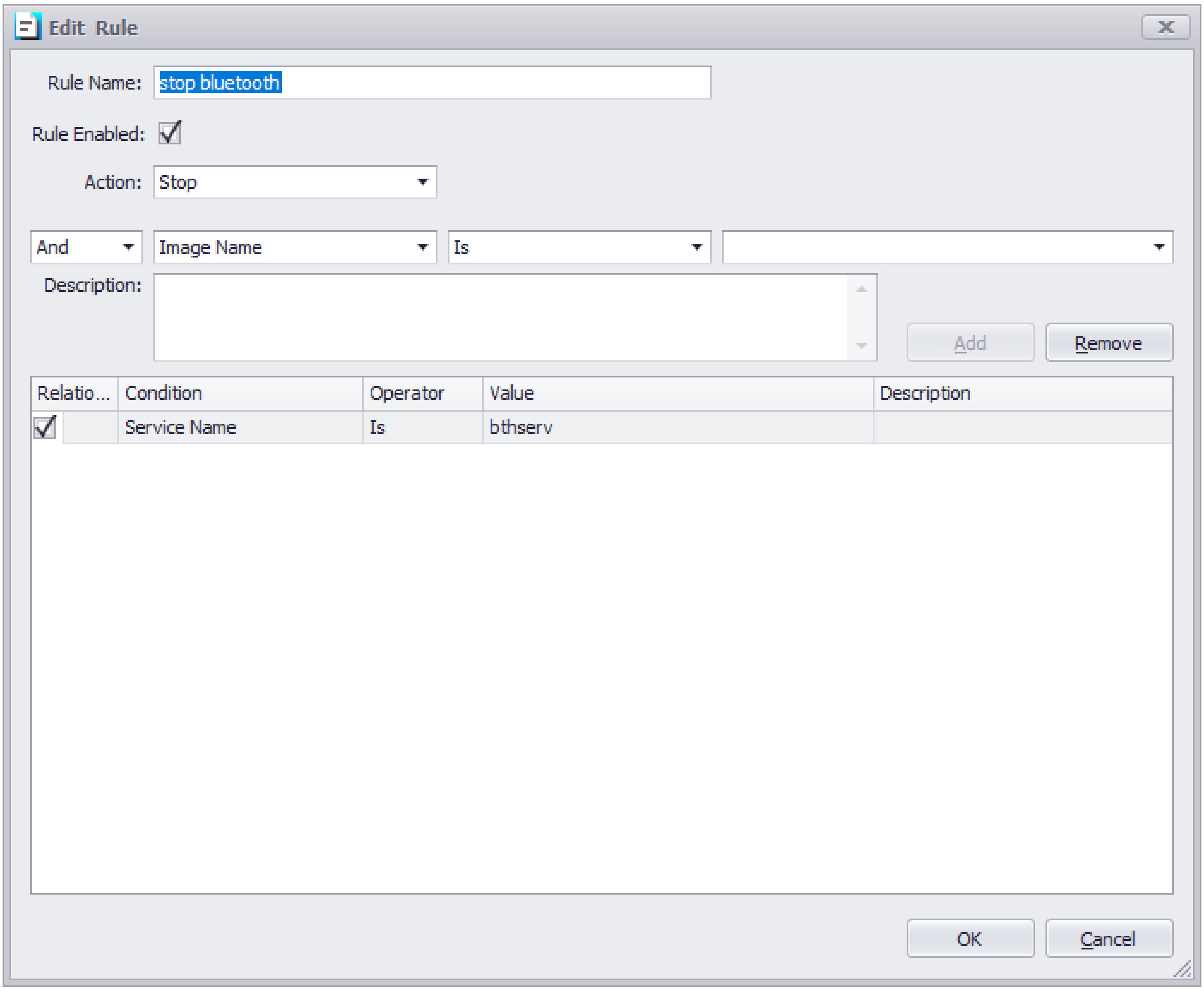
at start-up: services are scanned for compliance before the TDA fully starts and all the rules will be applied beforehand.

at **session start-up**: services are scanned for compliance while the TDA is initializing the secure session, and all the rules will be applied during initialisation.

repeat: services are scanned for compliance in real-time while TDA policies are in place and all the rules will be applied while the TDA session is running every x.

at logout: services are scanned for compliance while the TDA is logging off and all the rules will be applied at logout

i.e., Stopping Bluetooth service



Rule Name: stop bluetooth

Rule Enabled: ☑

Action: Stop

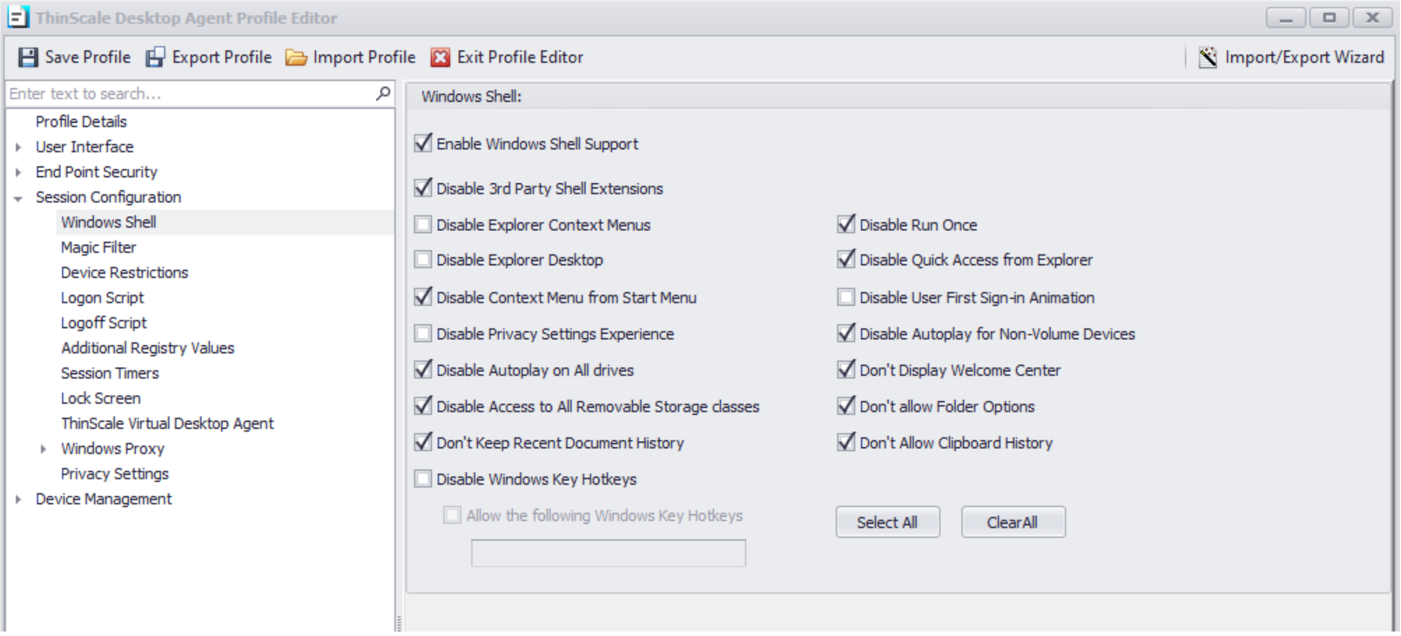
And | Image Name | Is |

Description:

Relatio...	Condition	Operator	Value	Description
☑	Service Name	Is	bthserv	

5. Session Configuration

Session Configuration – Windows Shell



Windows Shell:

☑ Enable Windows Shell Support

☑ Disable 3rd Party Shell Extensions

□ Disable Explorer Context Menus

□ Disable Explorer Desktop

☑ Disable Context Menu from Start Menu

□ Disable Privacy Settings Experience

☑ Disable Autoplay on All drives

☑ Disable Access to All Removable Storage classes

☑ Don't Keep Recent Document History

□ Disable Windows Key Hotkeys

□ Allow the following Windows Key Hotkeys

☑ Disable Run Once

☑ Disable Quick Access from Explorer

□ Disable User First Sign-in Animation

☑ Disable Autoplay for Non-Volume Devices

☑ Don't Display Welcome Center

☑ Don't allow Folder Options

☑ Don't Allow Clipboard History

Enable Windows Shell Support

If enabled, explorer.exe will be able to run in the back of the TDA session.

Disable 3rd Party Shell Extensions

If enabled, 3rd party shell extensions will be disabled.

Disable Explorer context menu

If enabled, the right click context menu will be disabled.

Disable Run Once

If enabled, the system ignores the run-once list.

Disable Explorer Desktop

If enabled, the main desktop will be disabled.

Disable Quick Access

If enabled, quick access will be disabled.

Disable Start context menu

If enabled, the start right click context menu will be disabled.

Disable first animation

If enabled, the first sign-in animation will be disabled.

Disable Privacy Setting

If enabled, the privacy settings will be disabled.

Disable auto-play MTP devices

If enabled, Autoplay feature from MTP devices like cameras or phones will be disabled.

Disable auto-play all drives

If enabled, Autoplay feature for all drives will be disabled.

Disable welcome screen

If enabled, the Windows welcome experience will be disabled.

Disable Access to All Removable Storage classes

If enabled, access to all the removable storage devices will be blocked.

Disable folder options

If enabled, explore “Folder Options” will be disabled.

Don't keep document history

If enabled, all documents history will be deleted.

Disable clipboard history

If enabled, clipboard history (Ctrl-S) will be disabled.

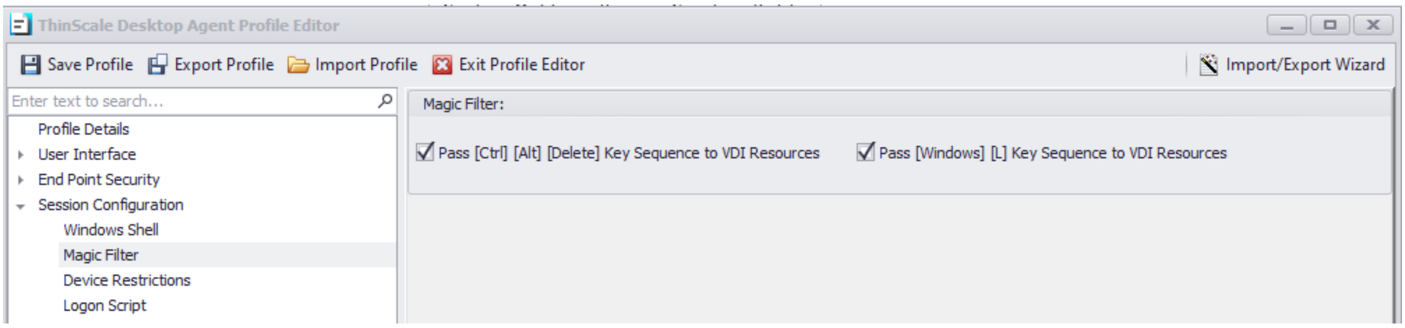
Disable Windows Hotkeys

If enabled, all the windows hotkeys will be disabled.

Allow the following windows Hotkeys

If enabled in conjunction with the "Disabled Windows Hotkeys" setting, you'll have the capability to designate the specific Win-Key combination you wish to permit.

Session Configuration – Magic Filter



Magic Filter:

☑ Pass [Ctrl] [Alt] [Delete] Key Sequence to VDI Resources

☑ Pass [Windows] [L] Key Sequence to VDI Resources

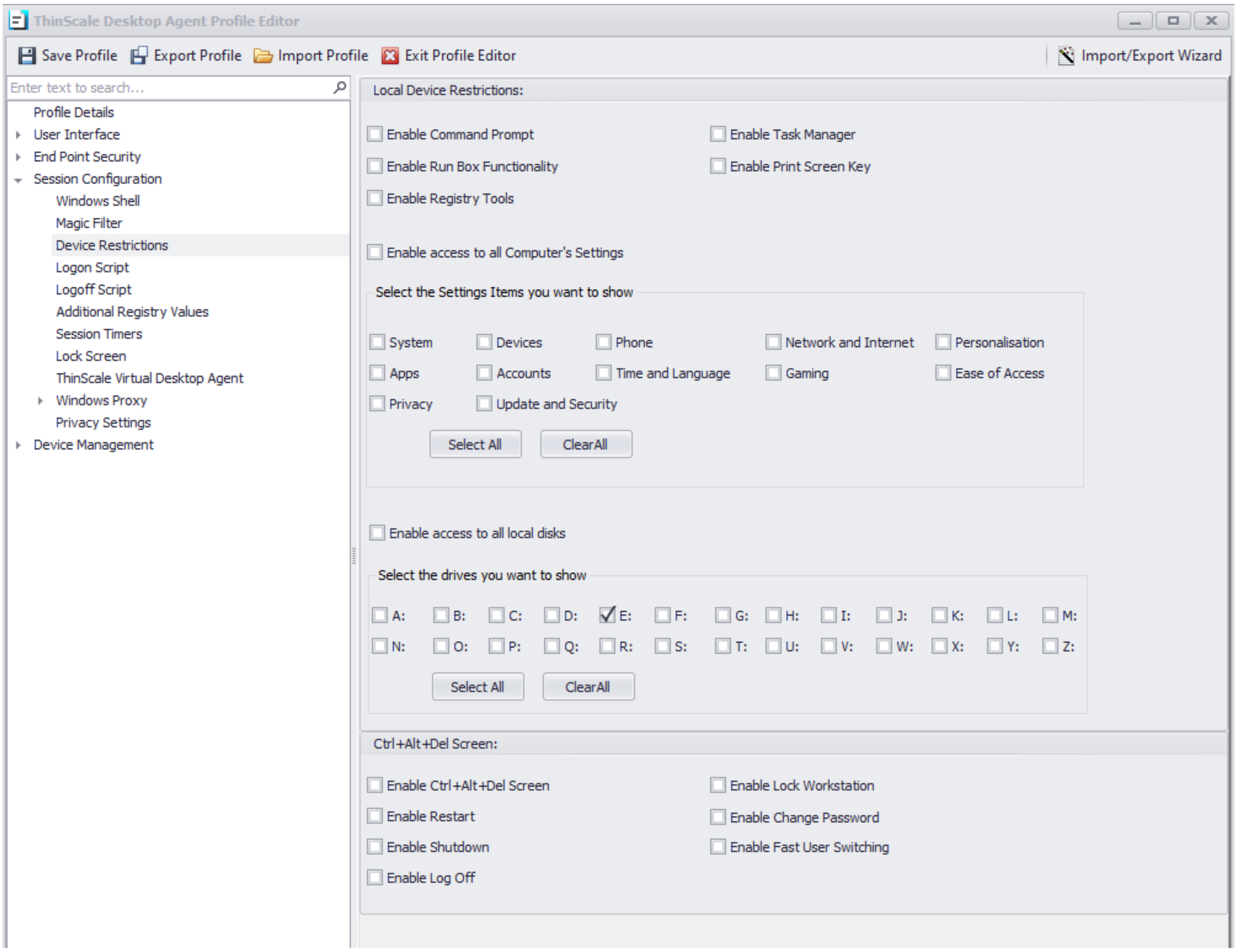
Pass [Ctrl] [Alt] [Delete] key sequence to VDI resources

If enabled, the CTRL-ALT-DEL keystrokes will be passed only to the VDI session.

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

If enabled, the WIN-L keystrokes will be passed only to the VDI session.

Session Configuration – Device Restrictions



Local Device Restrictions:

□ Enable Command Prompt
□ Enable Task Manager
□ Enable Run Box Functionality
□ Enable Print Screen Key
□ Enable Registry Tools

□ Enable access to all Computer's Settings

Select the Settings Items you want to show

□ System □ Devices □ Phone □ Network and Internet □ Personalisation
□ Apps □ Accounts □ Time and Language □ Gaming □ Ease of Access
□ Privacy □ Update and Security

Select All ClearAll

□ Enable access to all local disks

Select the drives you want to show

□ A: □ B: □ C: □ D: ☑ E: □ F: □ G: □ H: □ I: □ J: □ K: □ L: □ M:
□ N: □ O: □ P: □ Q: □ R: □ S: □ T: □ U: □ V: □ W: □ X: □ Y: □ Z:

Select All ClearAll

Ctrl+Alt+Del Screen:

□ Enable Ctrl+Alt+Del Screen
□ Enable Lock Workstation
□ Enable Restart
□ Enable Change Password
□ Enable Shutdown
□ Enable Fast User Switching
□ Enable Log Off

Enable Command Prompt

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

Enable Task Manager

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

Enable Run Box Functionality

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

Enable Print Screen key

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

Enable Registry Tools

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

Enable access to all Computer's Settings

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 TDA 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.

Select the drives you want to show

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

Enable Ctrl+Alt+Del Screen

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

Enable Lock Workstation

If enabled, the users will be able to lock the local TDA 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

Enable Restart

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

Enable Change Password

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

Enable Shutdown

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

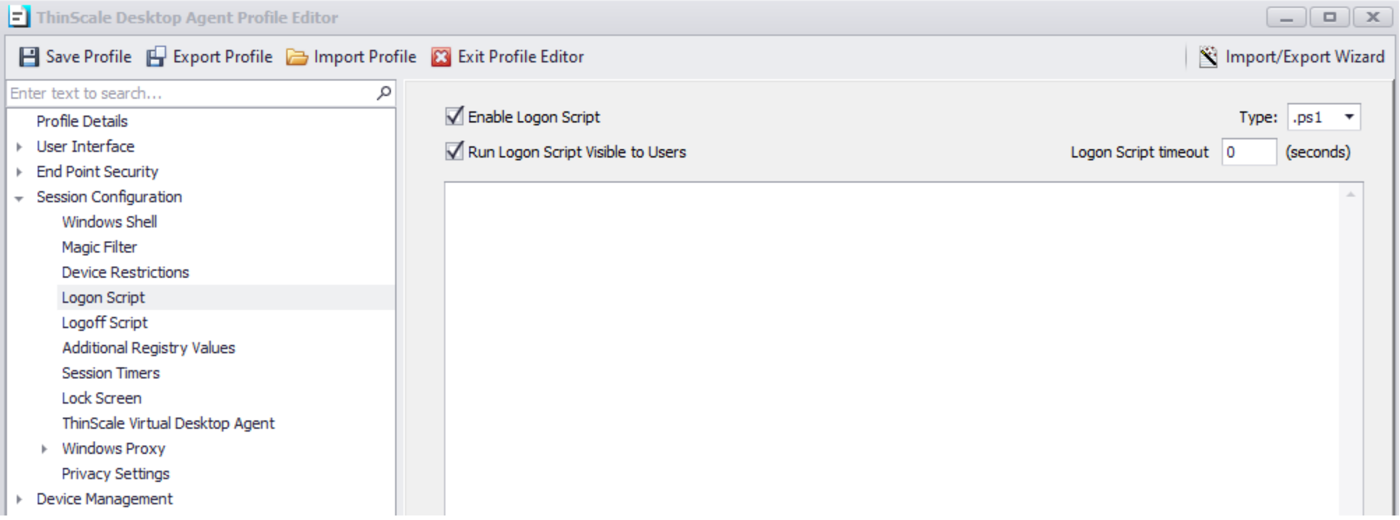
Enable Fast User Switching

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

Enable Log Off

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

Session Configuration – Logon Script



☑ Enable Logon Script

Type: .ps1

☑ Run Logon Script Visible to Users

Logon Script timeout 0 (seconds)

Enable Login Script

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

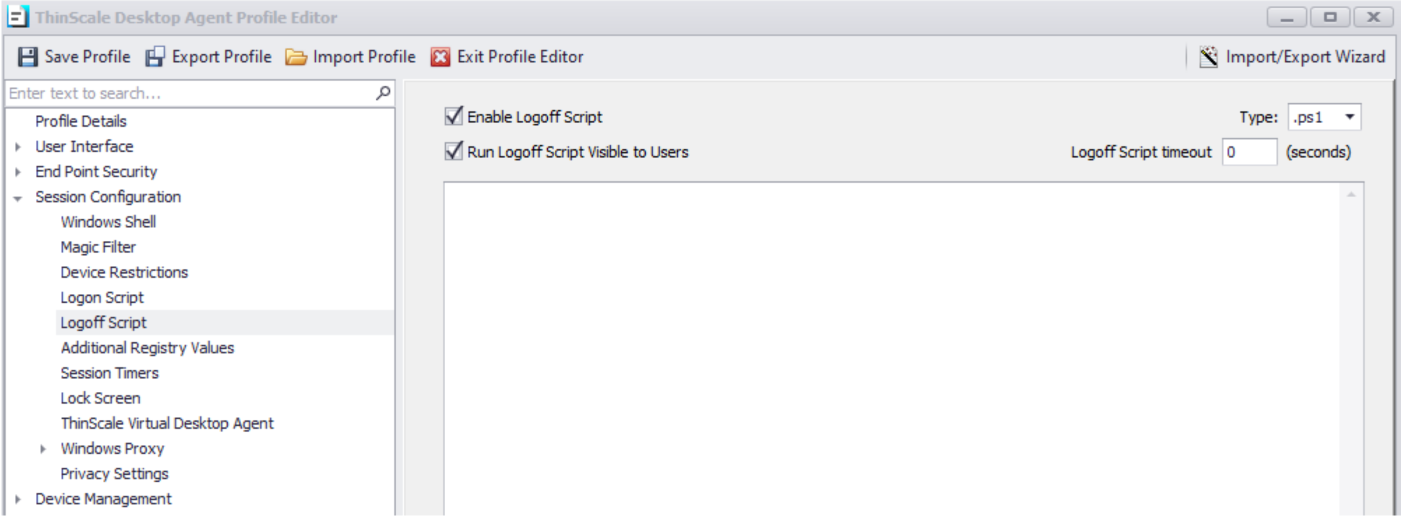
Run Login Script Visible to users

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

Session Configuration – Logoff Script



☑ Enable Logoff Script

Type: .ps1

☑ Run Logoff Script Visible to Users

Logoff Script timeout 0 (seconds)

Enable Logoff Script

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

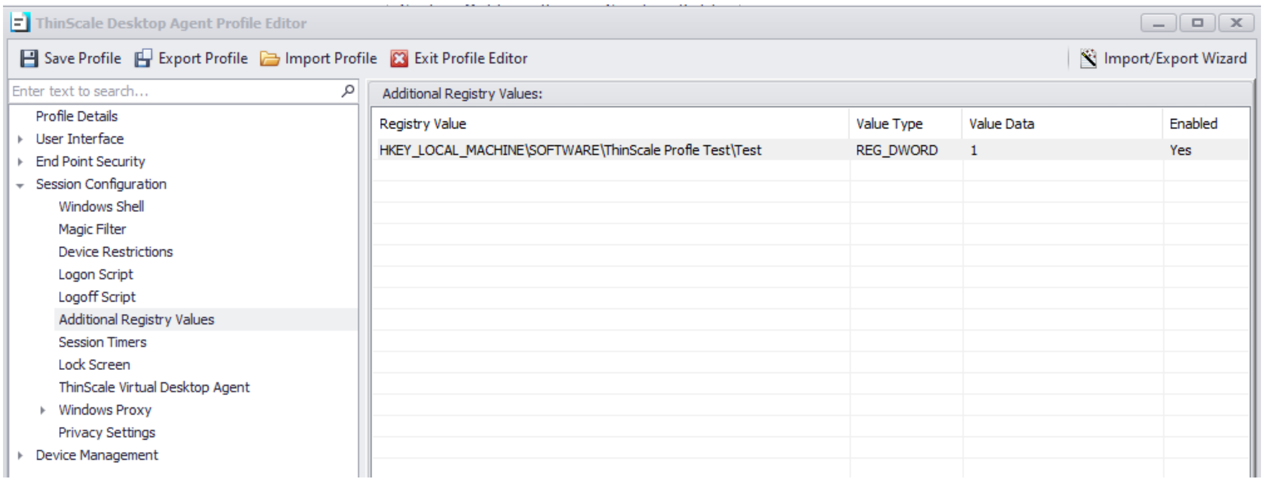
Run Logoff Script Visible to users

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.

Session Configuration – Additional Registry Value



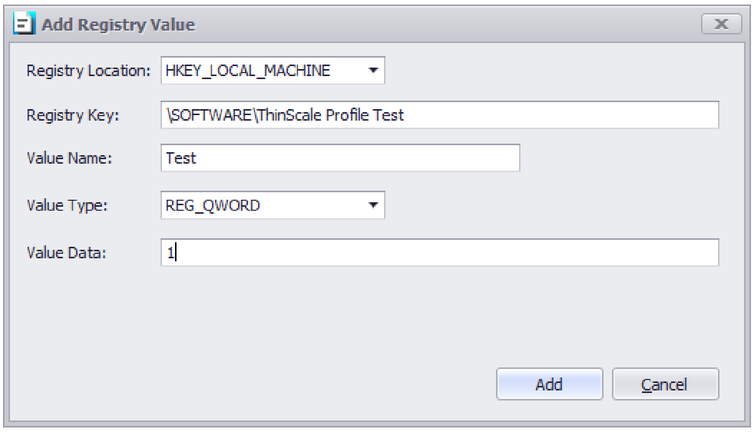
ThinScale Desktop Agent Profile Editor

Additional Registry Values:

Registry Value	Value Type	Value Data	Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\ThinScale Profle Test\Test	REG_DWORD	1	Yes

Using the TDA, it is possible to incorporate non-persistent custom registry keys that are enforced by the TDA engine.

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



Add Registry Value

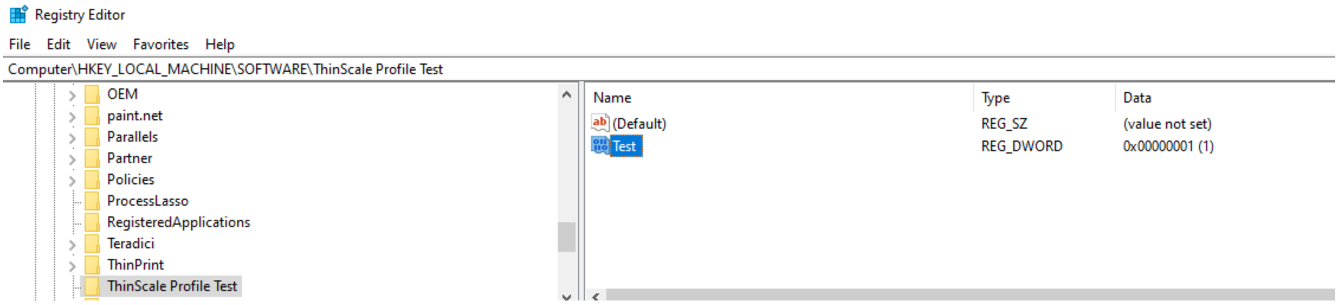
Registry Location: HKEY_LOCAL_MACHINE

Registry Key: \SOFTWARE\ThinScale Profile Test

Value Name: Test

Value Type: REG_QWORD

Value Data: 1



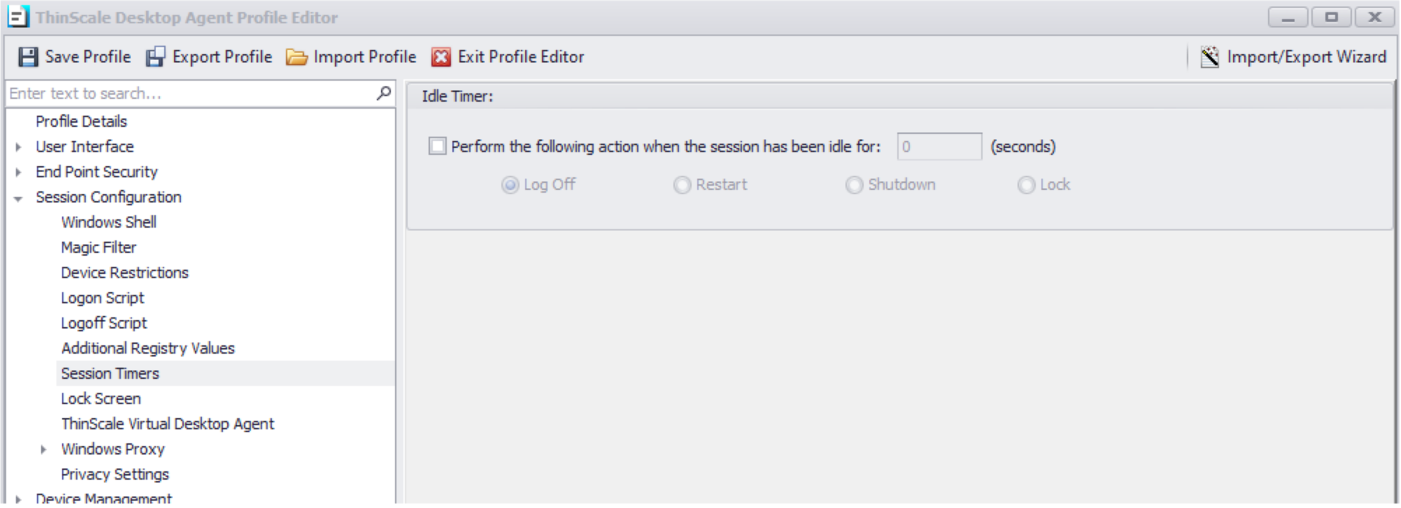
Registry Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\ThinScale Profile Test

Name	Type	Data
(Default)	REG_SZ	(value not set)
Test	REG_DWORD	0x00000001 (1)

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

Session Configuration – Session Timers



Idle Timer:

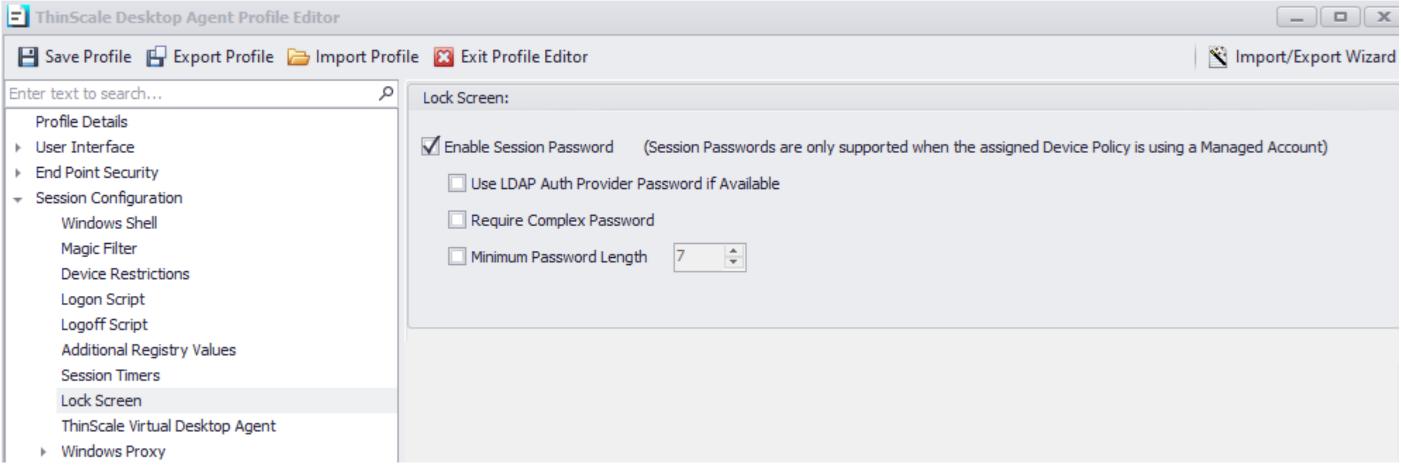
□ Perform the following action when the session has been idle for: 0 (seconds)

● Log Off ○ Restart ○ Shutdown ○ Lock

Perform the following action when the device is idle for

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

Session Configuration – Lock Screen



Lock Screen:

☑ Enable Session Password (Session Passwords are only supported when the assigned Device Policy is using a Managed Account)

□ Use LDAP Auth Provider Password if Available

□ Require Complex Password

□ Minimum Password Length 7

When activated, TDA users have the capability to establish a local password, which can be employed to secure and release the user session.

Enable Session Password

If enabled, TDA 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.

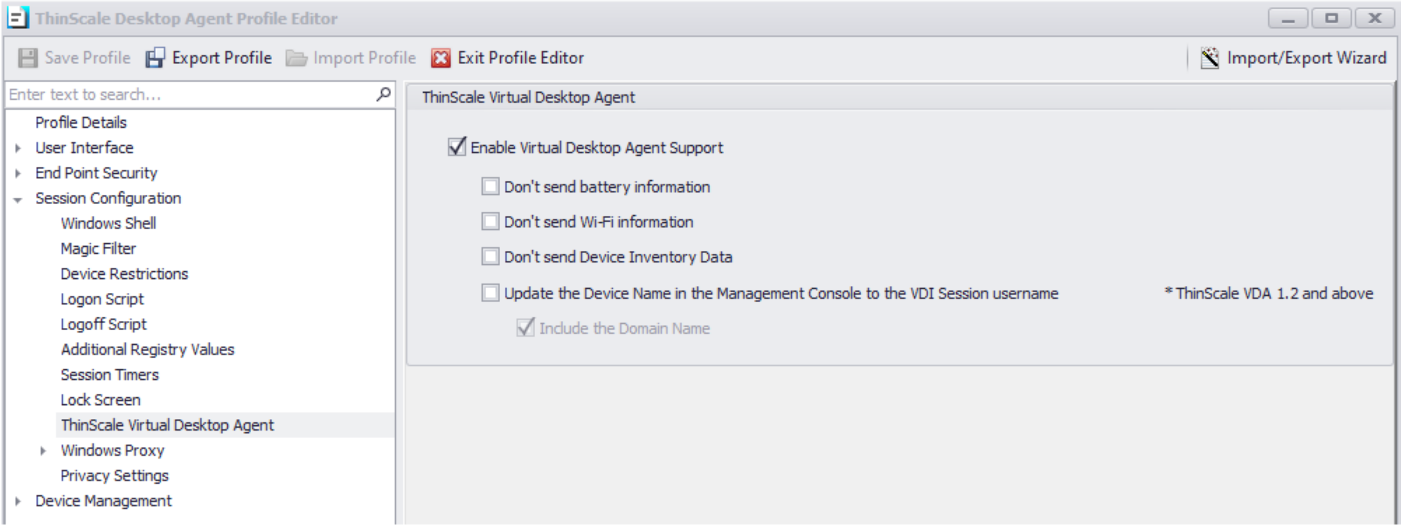
Require complex password

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.

Session Configuration – ThinScale Virtual Desktop Agent



ThinScale Virtual Desktop Agent

☑ Enable Virtual Desktop Agent Support

□ Don't send battery information

□ Don't send Wi-Fi information

□ Don't send Device Inventory Data

□ Update the Device Name in the Management Console to the VDI Session username * ThinScale VDA 1.2 and above

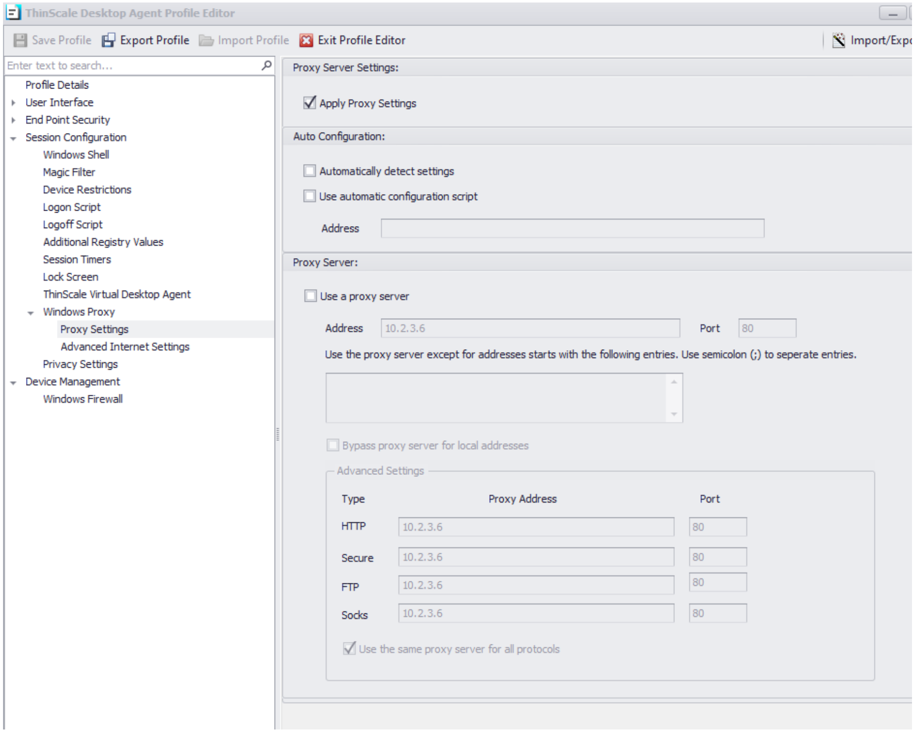
☑ Include the Domain Name

Enable Virtual Desktop Agent support

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

With the aid of the TDA only users utilizing the TDA will be allowed to connect and lunch a VDI session being a Citrix, Vmware, WVD and Amazon Workspace

Session Configuration – Windows Proxy Settings



Proxy Server Settings:

☑ Apply Proxy Settings

Auto Configuration:

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy Server:

☐ Use a proxy server

Address 10.2.3.6 Port 80

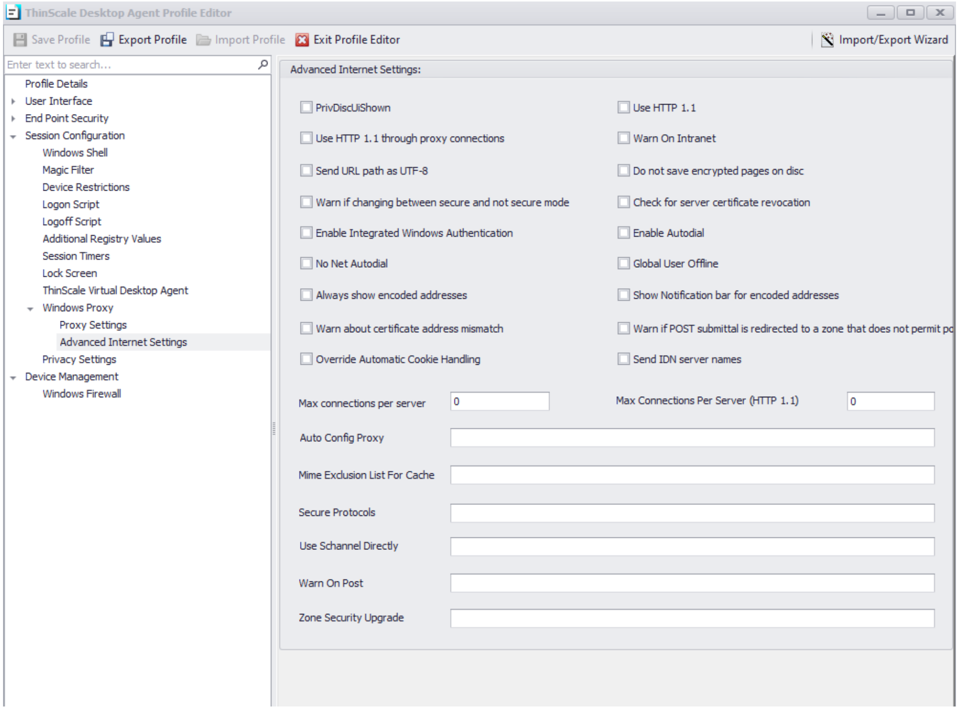
Use the proxy server except for addresses starts with the following entries. Use semicolon (;) to seperate entries.

☐ Bypass proxy server for local addresses

Advanced Settings

Type	Proxy Address	Port
HTTP	10.2.3.6	80
Secure	10.2.3.6	80
FTP	10.2.3.6	80
Socks	10.2.3.6	80

☑ Use the same proxy server for all protocols



Advanced Internet Settings:

☐ PrivDiscUiShown

☐ Use HTTP 1.1 through proxy connections

☐ Send URL path as UTF-8

☐ Warn if changing between secure and not secure mode

☐ Enable Integrated Windows Authentication

☐ No Net Autodial

☐ Always show encoded addresses

☐ Warn about certificate address mismatch

☐ Override Automatic Cookie Handling

☐ Use HTTP 1.1

☐ Warn On Intranet

☐ Do not save encrypted pages on disc

☐ Check for server certificate revocation

☐ Enable Autodial

☐ Global User Offline

☐ Show Notification bar for encoded addresses

☐ Warn if POST submittal is redirected to a zone that does not permit po

☐ Send IDN server names

Max connections per server 0

Max Connections Per Server (HTTP 1.1) 0

Auto Config Proxy

Mime Exclusion List For Cache

Secure Protocols

Use Schannel Directly

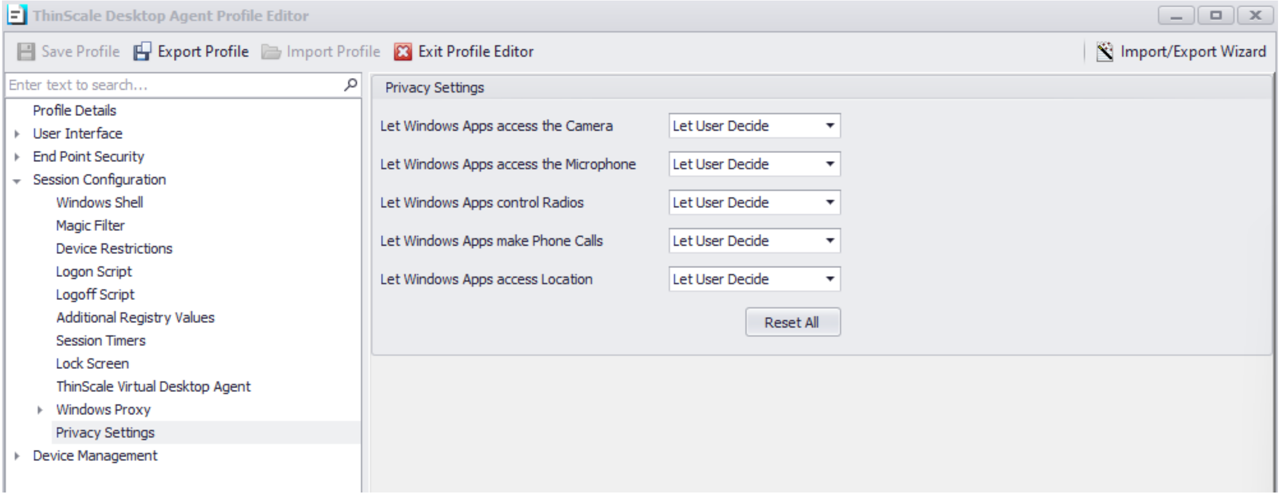
Warn On Post

Zone Security Upgrade

This Tab follows the standard Windows Proxy settings.

At the back of every option there is a virtual reg key that we applied only during the TDA session. When the TDA is logged off or unlocked those keys will be removed.

Session Configuration – Privacy Settings



Privacy Settings

Let Windows Apps access the Camera: Let User Decide

Let Windows Apps access the Microphone: Let User Decide

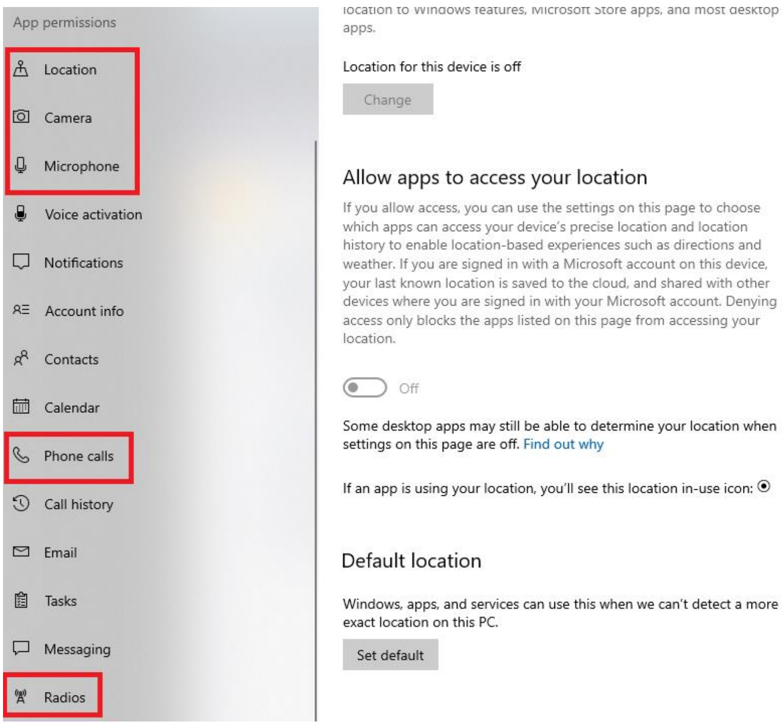
Let Windows Apps control Radios: Let User Decide

Let Windows Apps make Phone Calls: Let User Decide

Let Windows Apps access Location: Let User Decide

Accessing Privacy Settings in Windows 10/11 involves navigating to Settings > Privacy > App Permissions.

These selections mirror the options previously presented by Windows, now organized into cohesive groups.



location to Windows features, Microsoft Store apps, and most desktop apps.

Location for this device is off

Allow apps to access your location

If you allow access, you can use the settings on this page to choose which apps can access your device's precise location and location history to enable location-based experiences such as directions and weather. If you are signed in with a Microsoft account on this device, your last known location is saved to the cloud, and shared with other devices where you are signed in with your Microsoft account. Denying access only blocks the apps listed on this page from accessing your location.

Off

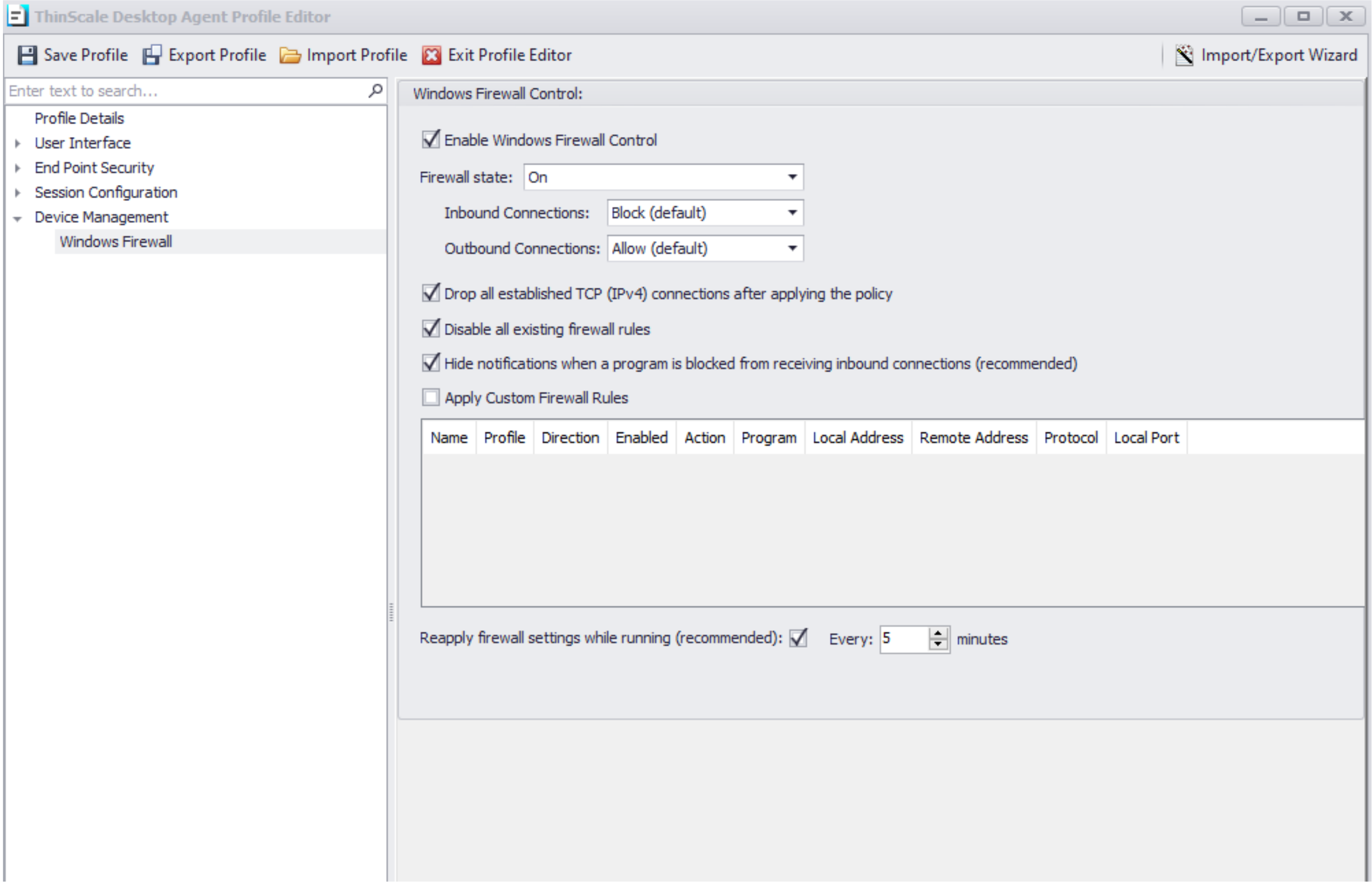
Some desktop apps may still be able to determine your location when settings on this page are off. Find out why

If an app is using your location, you'll see this location in-use icon: ⦿

Default location

Windows, apps, and services can use this when we can't detect a more exact location on this PC.

6. Device Management



Windows Firewall Control:

☑ Enable Windows Firewall Control

Firewall state: On

Inbound Connections: Block (default)

Outbound Connections: Allow (default)

☑ Drop all established TCP (IPv4) connections after applying the policy

☑ Disable all existing firewall rules

☑ Hide notifications when a program is blocked from receiving inbound connections (recommended)

□ Apply Custom Firewall Rules

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

Reapply firewall settings while running (recommended): ☑ Every: 5 minutes

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

Drop all established TCP connections

If enabled, TDA will truncate all existing TCP connection when the session is launched.

Disable all existing rules

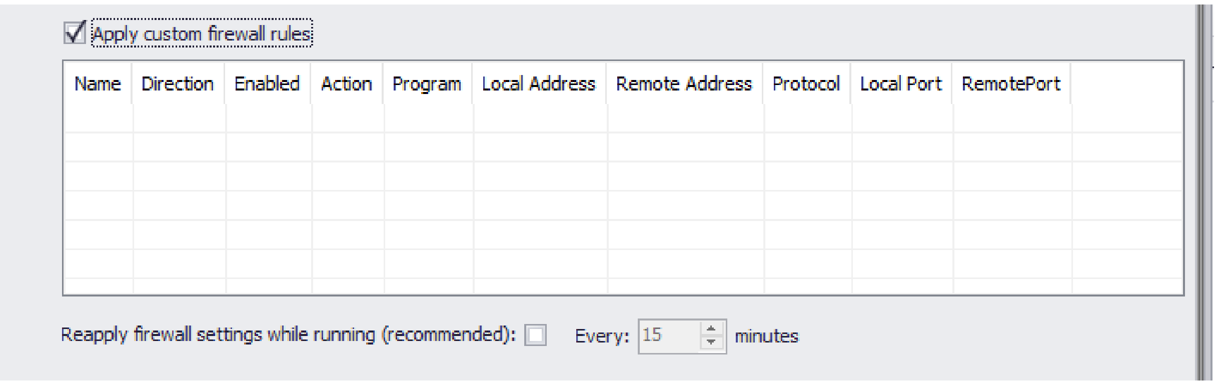
If enabled, TDA will disable all current Windows firewall rules. TDA will do a backup of all the existing rulesets and then disable them. When TDA policies are removed all original Firewall rules are recreated.

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

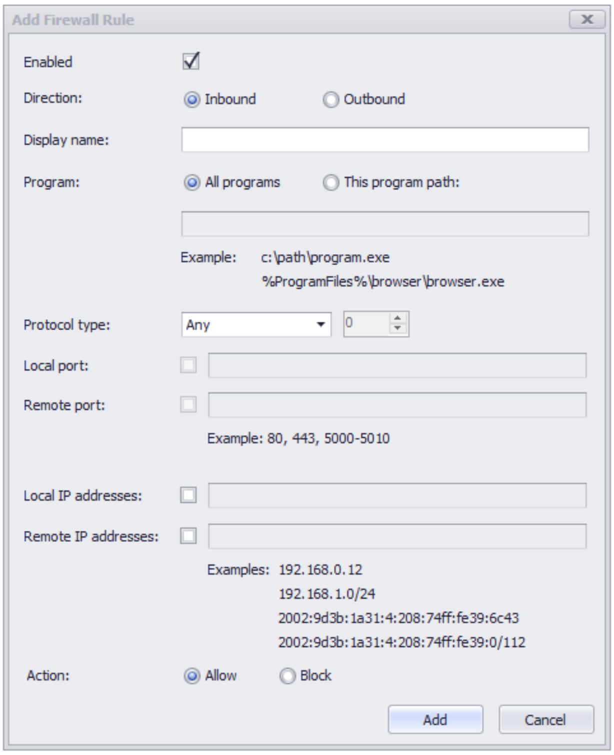
Create custom rules for inbound and outbound traffic.



☑ 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