THINSCALE

ThinScale Management Console Administrator’s Guide

Table of Content

1. ThinScale Management Console

Introduction

The ThinScale Management Console makes it easy for you to:

- manage your **Devices**
- User Assignments
- create and assign **Profiles** to your **Devices**
- create Access Keys for your **Devices** to connect to
- assign one or more **Management Servers** to your Access Keys
- create, assign, and deploy **Software Packages**
- create and assign **Notifications**
- setting **Devices** and **Notifications** **Global Settings**
- look at the **Knowledge Base** articles
- Install and use **PowerShell Module**
- Manage **Devices** between **Management Servers**
- ThinScale Portal
- Authentication Providers
- Virtual Disks
- Licence Report
- Device Policies

The Management Console also supports multiple user accounts with role-based permissions. This enables you to delegate tasks to other people in your organisation without exposing the full administrator capabilities of the Console. Also, to help keep track of changes you can find an **Audit Log** of Console management events and actions recorded per user.

Supported Platforms and System Requirements

- Windows 10 (or greater)
  - At least 2 GB of RAM
  - At least 500 MB of free disk space
- .Net Framework 4.7.8 or greater
- .NET Core 6.0.6 Runtime specific
  - (If installed together with the Management Server)

https://dotnet.microsoft.com/en-us/download/dotnet/6.0

Installation

The default installation directories are listed below:

- **64-bit machine:** C:\Program Files (x86) \ThinScale Management Console
- **32-bit machine:** C:\Program Files\ThinScale Management Console

A silent installation is supported as below:
“msiexec /I ThinScaleManagementConsole-8.0.x.msi /QB /norestart”

Uninstalling

ThinScale Management Console is an MSI-based installation and will appear in Program and Features within the Windows Control Panel.

To uninstall:

1. Open Control Panel
2. Select Programs -> Program and Features
3. Right-click ThinScale Management Console and select ‘Uninstall’.
4. Follow the uninstall instructions.

Note: The Uninstall must be performed by a user with administrator privileges on the local device.

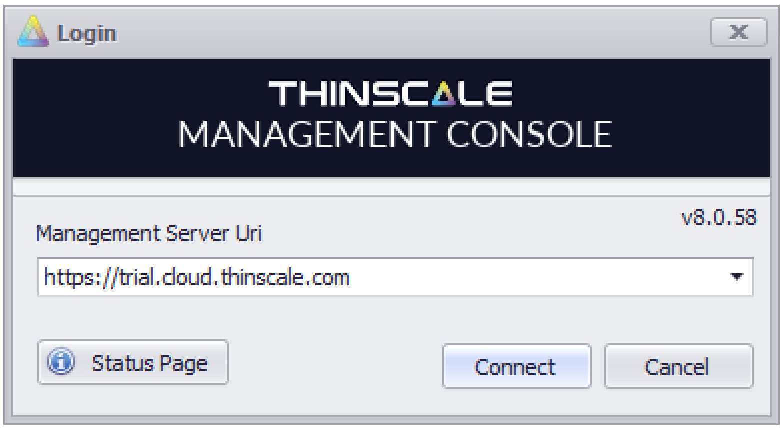
Things to know before you start

The ThinScale Management Server will disconnect idle Management Server connections after 30 minutes. You may change this value (see ThinScale Management Service Administrators guide).

All traffic, client or server-related, is relayed by the Management Server web service, at no point you are talking to a client PC. The exception to this rule is when remote controlling a ThinKiosk device, you are communicating directly with the device when the shadow window opens.

2. Login Dialog

Whenever you start the Management Console the first screen displayed is the Login dialog.



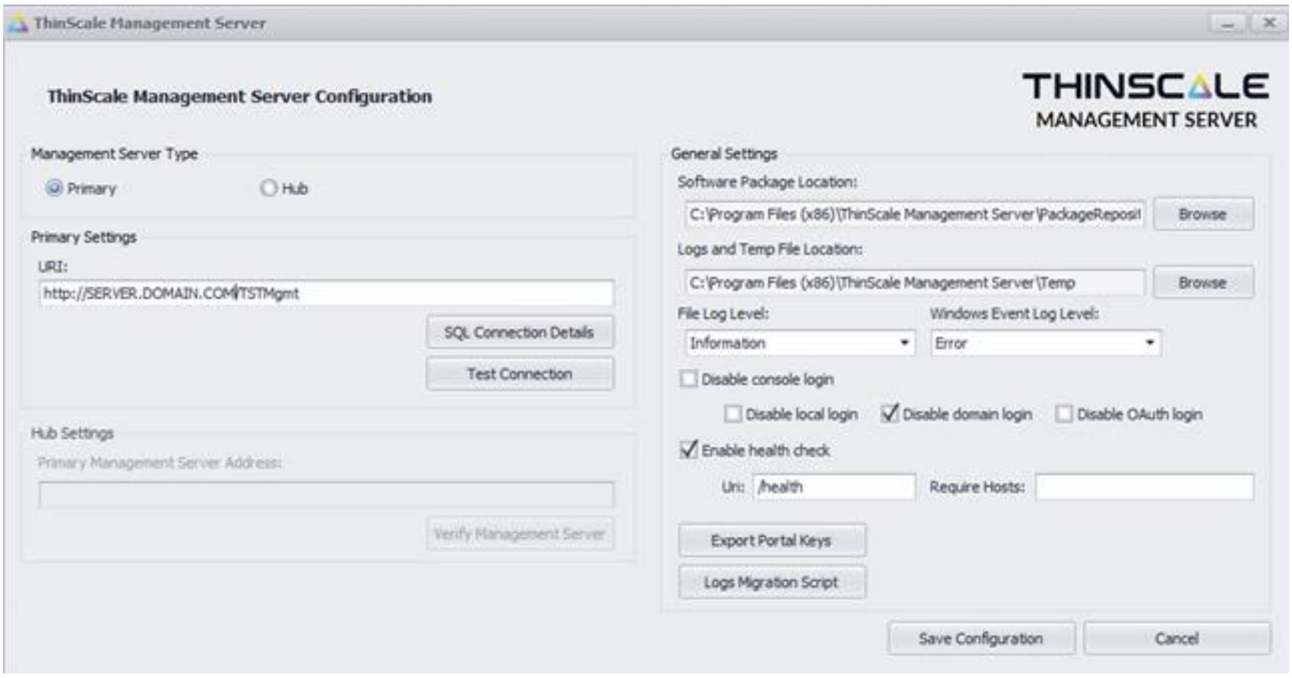
Please note version number may be different from the picture

Management Server Uri

This is the address of your Management Server.

You may choose any address if you have more than one Management Server configured. All Management Servers (*Primary* and *Hub*) are synchronised, and the data returned to the Console is identical.

Tip: You can find the address by opening the ***ThinScale Management Configuration*** application installed on your Windows server machine that is hosting the Management Server.



ThinScale Management Server

ThinScale Management Server Configuration

Management Server Type

● Primary ○ Hub

Primary Settings

URI: http://SERVER.DOMAIN.COM/TSTMgmt

Hub Settings

Primary Management Server Address:

General Settings

Software Package Location: C:\Program Files (x86)\ThinScale Management Server\PackageReposit

Logs and Temp File Location: C:\Program Files (x86)\ThinScale Management Server\Temp

File Log Level: Information

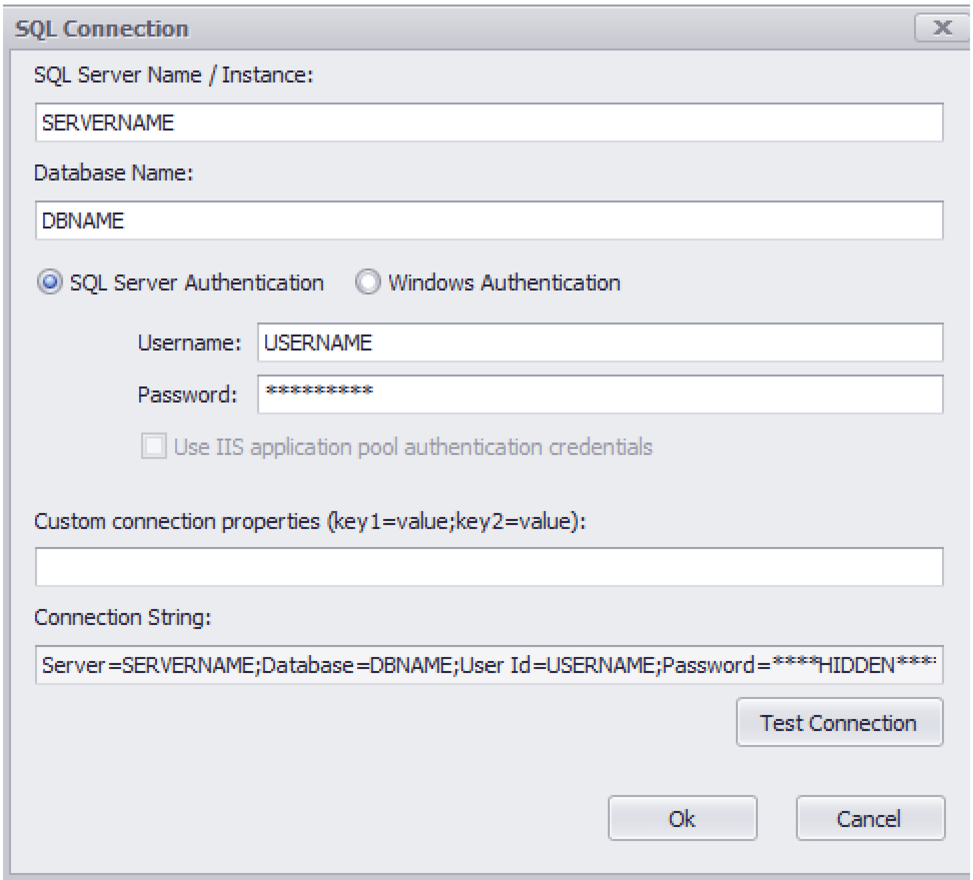
Windows Event Log Level: Error

□ Disable console login

□ Disable local login ☑ Disable domain login □ Disable OAuth login

☑ Enable health check

Uri: /health Require Hosts:



SQL Connection

SQL Server Name / Instance: SERVERNAME

Database Name: DBNAME

● SQL Server Authentication ○ Windows Authentication

Username: USERNAME

Password: **********

□ Use IIS application pool authentication credentials

Custom connection properties (key1=value;key2=value):

Connection String: Server=SERVERNAME;Database=DBNAME;User Id=USERNAME;Password=****HIDDEN***

During the initial setup of the first Management Server, an administrator account will have been created. The default username is **Administrator**, and the password can be set using the dialog box shown during installation.

Select ‘Native Login’ and use these credentials to log in.

Additional local user accounts can be created once logged into the console. Active Directory groups and users can also be added to your Roles, to allow domain authentication.
(See the Domain Account Roles section for more information on adding your domain users and groups)

Status Page

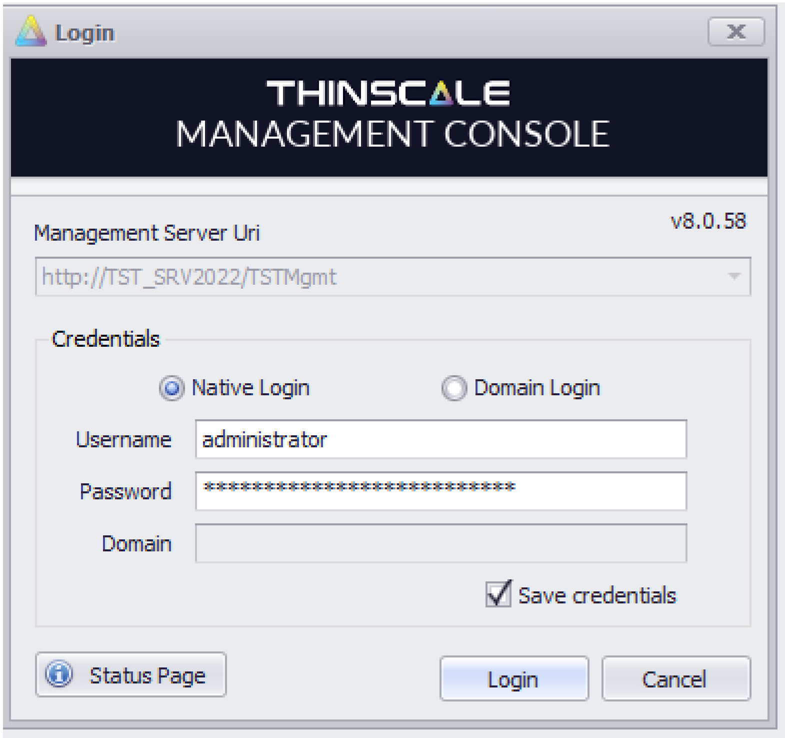
It will show the ThinScale Management Server Information over a web page if clicked.

Once you connect there are three ways you can connect:

Native / Domain Login / OAuth Login

The Management Server supports both Native (local accounts created within the Management Server) Domain Logins (Active Directory groups or users), and from the 8.0 via an Auth Provider.

Note: To use a domain account you need to login first with the native account and then add the user within the section in the Management console. See Domain Account Role Section



v8.0.58

Management Server Uri: http://TST_SRV2022/TSTMgmt

Credentials

● Native Login ○ Domain Login

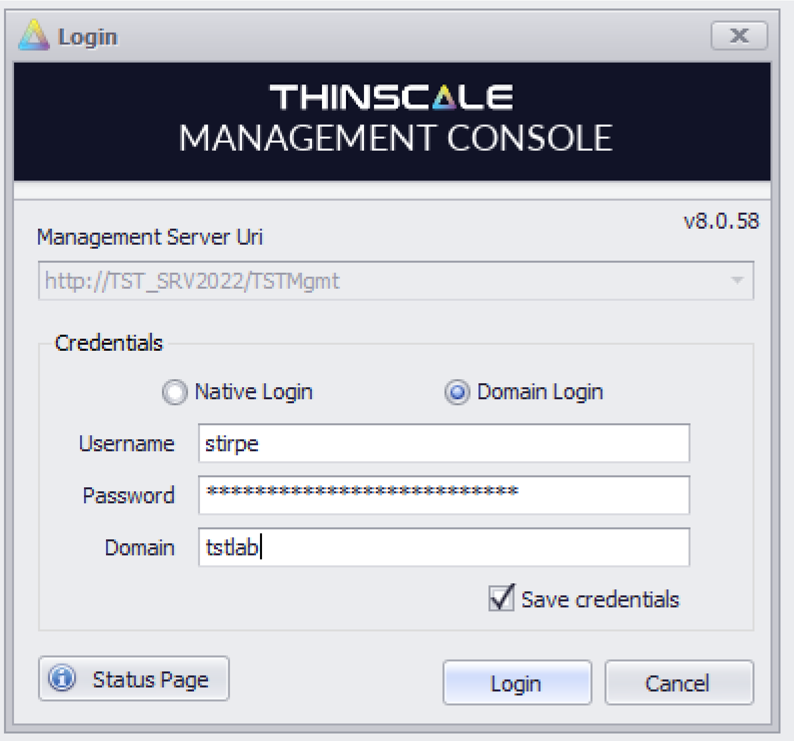
Username: administrator

Password: ****************************

Domain:

☑ Save credentials

Figure 1: Native Login



v8.0.58

Management Server Uri: http://TST_SRV2022/TSTMgmt

Credentials

○ Native Login ● Domain Login

Username: stirpe

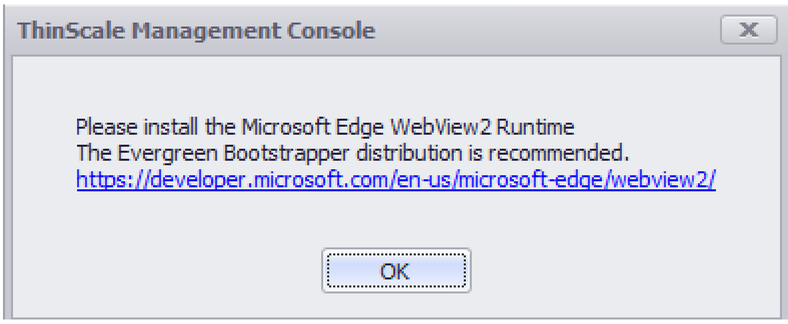
Password: ****************************

Domain: tstlab

☑ Save credentials

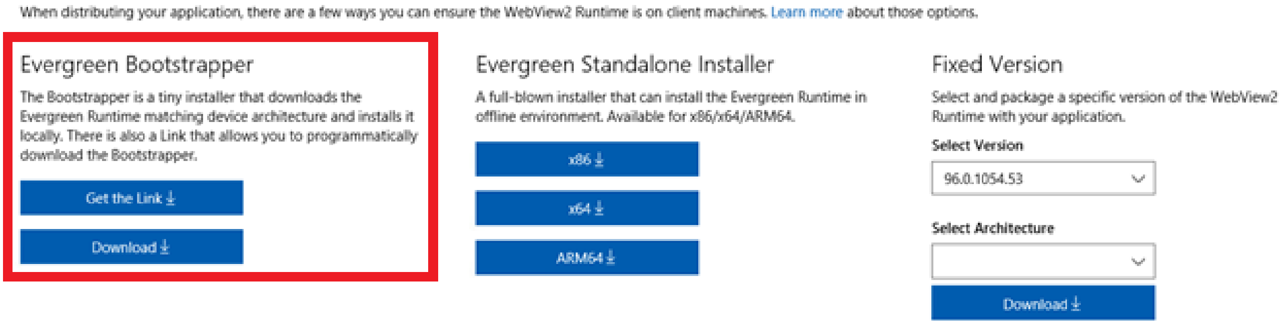
Figure 2: Domain Login

When an OAuth is utilized, a new component is needed if not already installed



Please install the Microsoft Edge WebView2 Runtime
The Evergreen Bootstrapper distribution is recommended.
https://developer.microsoft.com/en-us/microsoft-edge/webview2/

https://developer.microsoft.com/en-us/microsoft-edge/webview2/



When distributing your application, there are a few ways you can ensure the WebView2 Runtime is on client machines. Learn more about those options.

Evergreen Bootstrapper

The Bootstrapper is a tiny installer that downloads the Evergreen Runtime matching device architecture and installs it locally. There is also a Link that allows you to programmatically download the Bootstrapper.

Evergreen Standalone Installer

A full-blown installer that can install the Evergreen Runtime in offline environment. Available for x86/x64/ARM64.

Fixed Version

Select and package a specific version of the WebView2 Runtime with your application.

Select Version: 96.0.1054.53

Select Architecture:

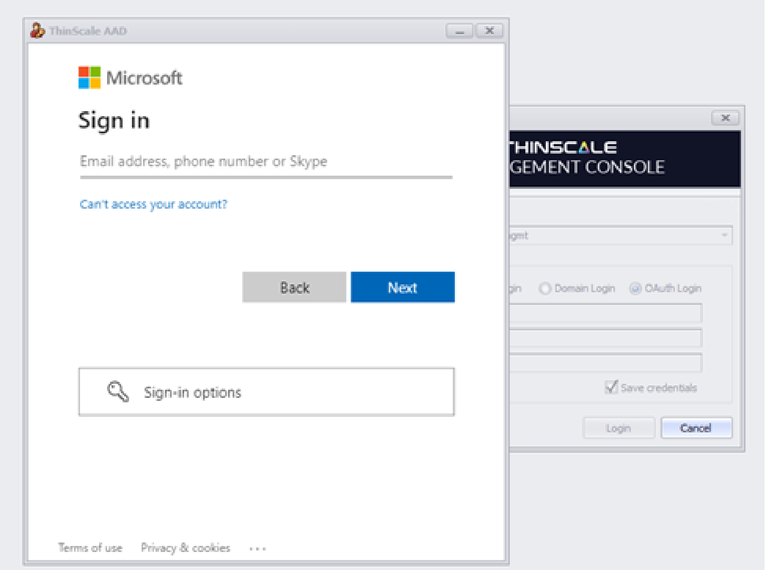
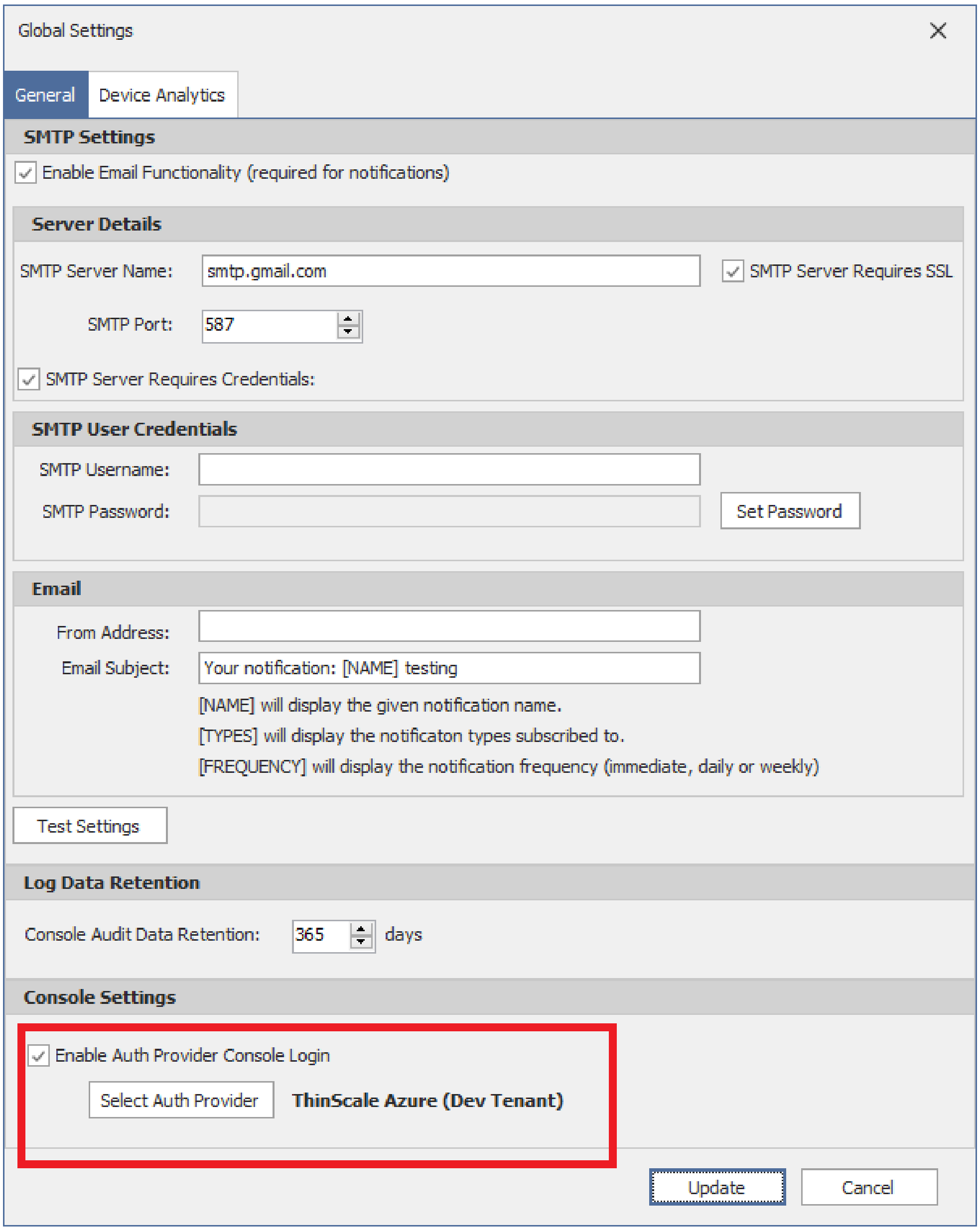


Figure 3: OAuth Login

To log in with the OAuth Login please add the Auth Provider inside Global Settings



Global Settings

SMTP Settings

☑ Enable Email Functionality (required for notifications)

Server Details

SMTP Server Name: smtp.gmail.com ☑ SMTP Server Requires SSL

SMTP Port: 587

☑ SMTP Server Requires Credentials:

SMTP User Credentials

SMTP Username:

SMTP Password:

Email

From Address:

Email Subject: Your notification: [NAME] testing

[NAME] will display the given notification name.

[TYPES] will display the notificaton types subscribed to.

[FREQUENCY] will display the notification frequency (immediate, daily or weekly)

Log Data Retention

Console Audit Data Retention: 365 days

Console Settings

☑ Enable Auth Provider Console Login

ThinScale Azure (Dev Tenant)

Save credentials

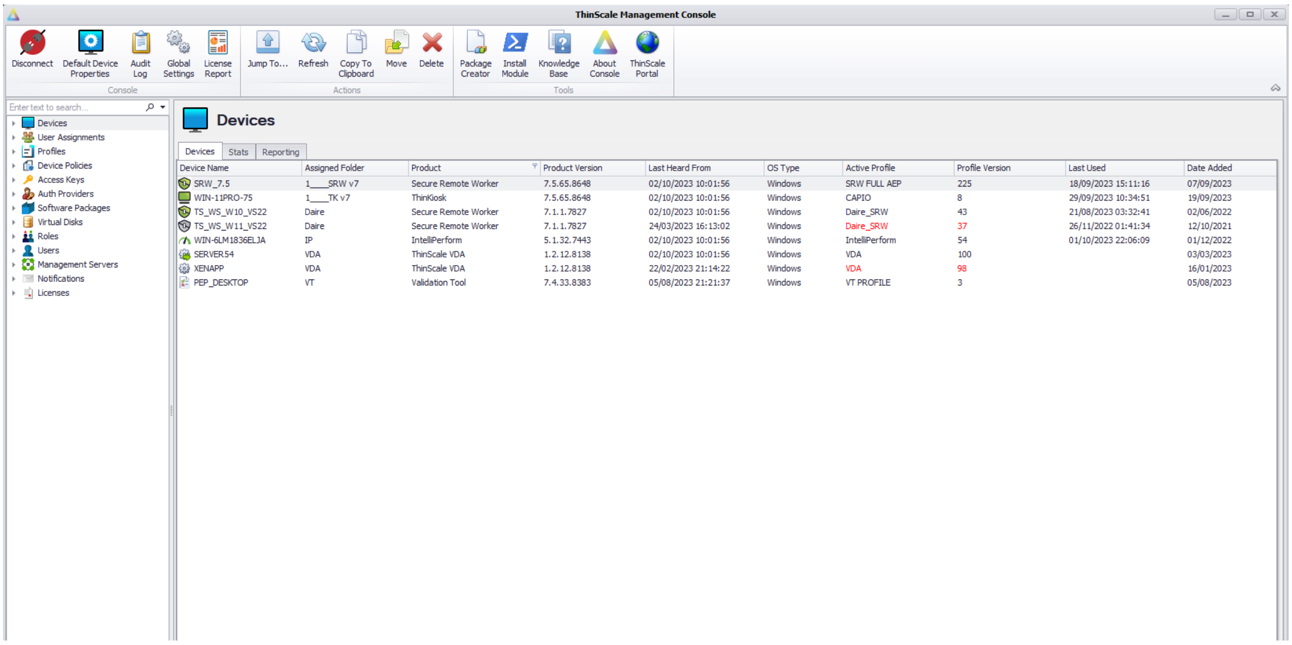
You can choose to save the password details of the last successful login attempt.

***Note:** This information is stored per a Windows user account and won't be viewable in case another user on the same machine logs on*

3. User Interface Overview

The Management Console dynamically updates based on what is selected in the tree menu on the left-hand side.

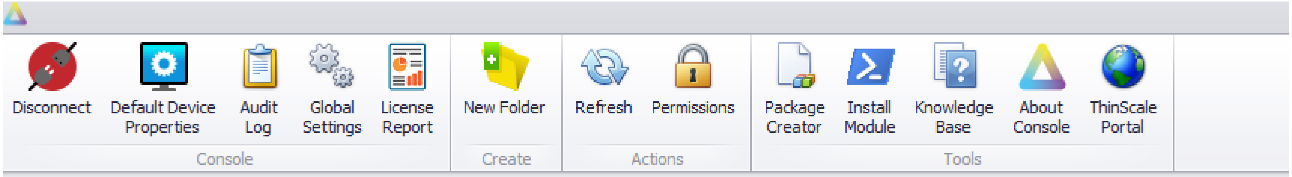
For example, selecting a Devices folder will update the top buttons with all the available actions that can be performed. You can also access these actions on the right-click context menu. To the right of the tree menu, the main area shows you a list of Devices in the selected folder.



Device Name	Assigned Folder	Product	Product Version	Last Heard From	OS Type	Active Profile	Profile Version	Last Used	Date Added
SRW_7.5	1____SRW v7	Secure Remote Worker	7.5.65.8648	02/10/2023 10:01:56	Windows	SRW FULL AEP	225	18/09/2023 15:11:16	07/09/2023
WIN-11PRO-75	1____TK v7	ThinKiosk	7.5.65.8648	02/10/2023 10:01:56	Windows	CAPIO	8	29/09/2023 10:34:51	19/09/2023
TS_WS_W10_VS22	Daire	Secure Remote Worker	7.1.1.7827	02/10/2023 10:01:56	Windows	Daire_SRW	43	21/08/2023 03:32:41	02/06/2022
TS_WS_W11_VS22	Daire	Secure Remote Worker	7.1.1.7827	24/03/2023 16:13:02	Windows	Daire_SRW	37	26/11/2022 01:41:34	12/10/2021
WIN-6LM1836ELJA	IP	IntelliPerform	5.1.32.7443	02/10/2023 10:01:56	Windows	IntelliPerform	54	01/10/2023 22:06:09	01/12/2022
SERVER54	VDA	ThinScale VDA	1.2.12.8138	02/10/2023 10:01:56	Windows	VDA	100		03/03/2023
XENAPP	VDA	ThinScale VDA	1.2.12.8138	22/02/2023 21:14:22	Windows	VDA	98		16/01/2023
PEP_DESKTOP	VT	Validation Tool	7.4.33.8383	05/08/2023 21:21:37	Windows	VT PROFILE	3		05/08/2023

Note: We are open to feedback on the design and placement of functionality in the Console. If you find something frustrating, please let us know and perhaps we can accommodate you in future releases.

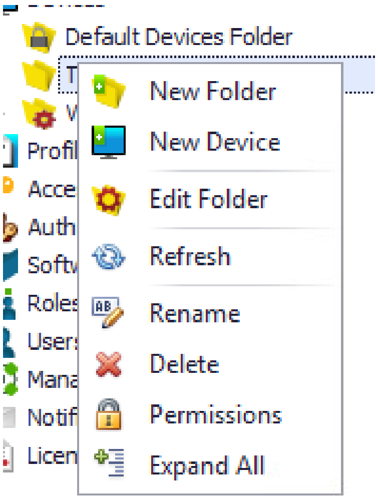
Menu Buttons



1. **Disconnect -** logs you off from the console
2. **Default Device Properties -** shows some settings about the devices
3. **Audit Log -** shows actions and events made with the console
4. **Global Settings -** SMTP settings are used to add email-based Notifications
5. **License Report –** will generate a report about license count that can be exported
6. **New Folder -** creates a new folder
7. **Refresh -** requests the latest data from the Management Server for the selected view
8. **Permission -** Opens the Permissions dialog for the object selected
9. **Package Creator -** a tool to help you create packaging for third-party software
10. **Migration Helper -** a tool to create registry keys or a start-up script to move one device from one server to another
11. **Install-Module -** Install the ThinScale Management PowerShell Module. (See ThinScale Management Platform PowerShell Guide document for more information)
12. **Knowledge Base -** ThinScale Knowledge Base Web Site
13. **About Console -** Version information about the Management Console
14. **ThinScale Portal-** my.thinscale.com Web site

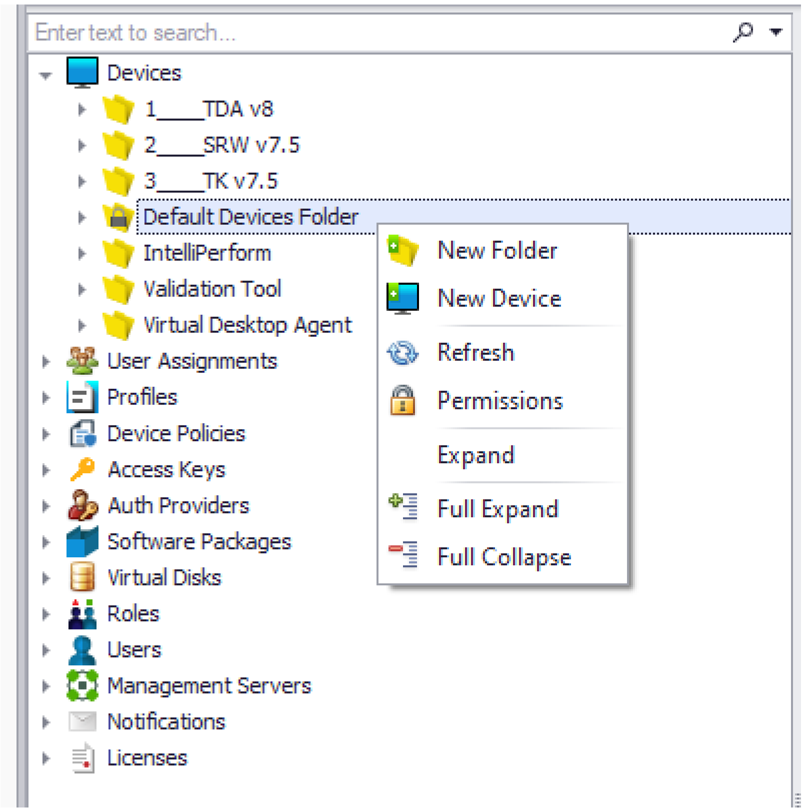
Folders

The folder context menu can be reached by right clicking a folder.



- **New Folder** – Creates a new folder under the specific item.
- **New Device** – Creates a new device under the specific folder.
- **Devices** – Opens the Device Context Menu
- **Edit Folder** - Opens the edit folder Context menu
- **Refresh** – Refreshes the console with the latest server information.
- **Rename** – Renames the folder.
- **Delete** – Deletes a folder (You can't delete a folder with contents or one to which you don't have permission).
- **Permissions** – Opens the Permission view attached to the folder.
- **Expand All** – Open all the nodes within the folder.

A special folder like a protected folder or a multi-select will have a limited menu:

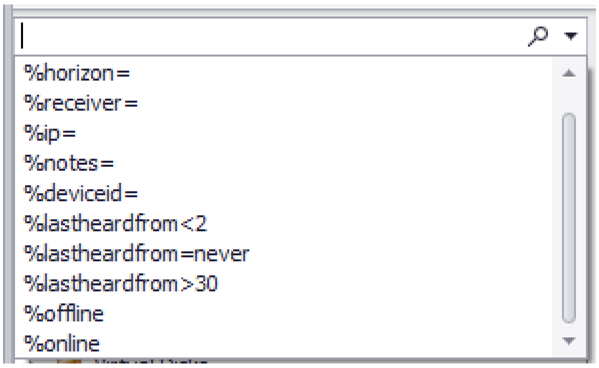


Search bar

The search bar allows a few special queries:

- UniqueId (%uniqueid)
- Horizon version (%horizon)
- Receiver version (%receiver)
- Ip Address (%ip)
- Notes (%notes)
- DeviceId (%deviceid)
- Last heard from devices (%lastheardfrom)
- Offline devices (%offline)
- Online devices (%online)

You can access examples by using the drop-down to the right of the search bar:



```
%horizon=
%receiver=
%ip=
%notes=
%deviceid=
%lastheardfrom<2
%lastheardfrom=never
%lastheardfrom>30
%offline
%online
```

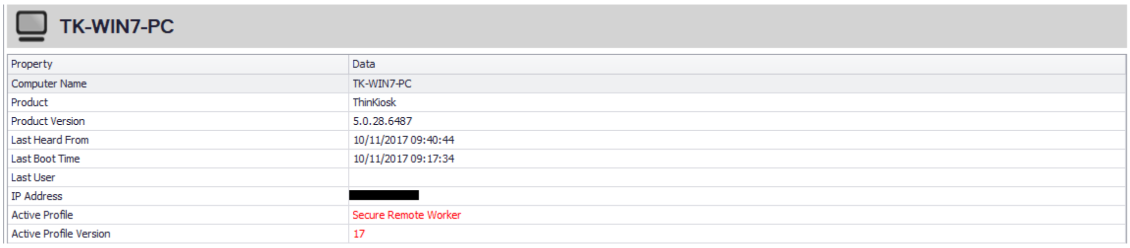
4. Devices

Devices can be organised by creating sub-folders and dragging and dropping them into the selected folder. Some customers organise them by user departments or geographical locations. Before deciding how to lay it out there are some things you may want to consider:

- By default, any new devices will register themselves in the **Default Devices Folder**. You can change this default by editing a **Site** and selecting a different default device folder. This way you can have new devices split into different folders depending on the **Site** they connecting to.

- Folders that do not have a **Profile** assigned will inherit the **Profile** from their parent folder(s).

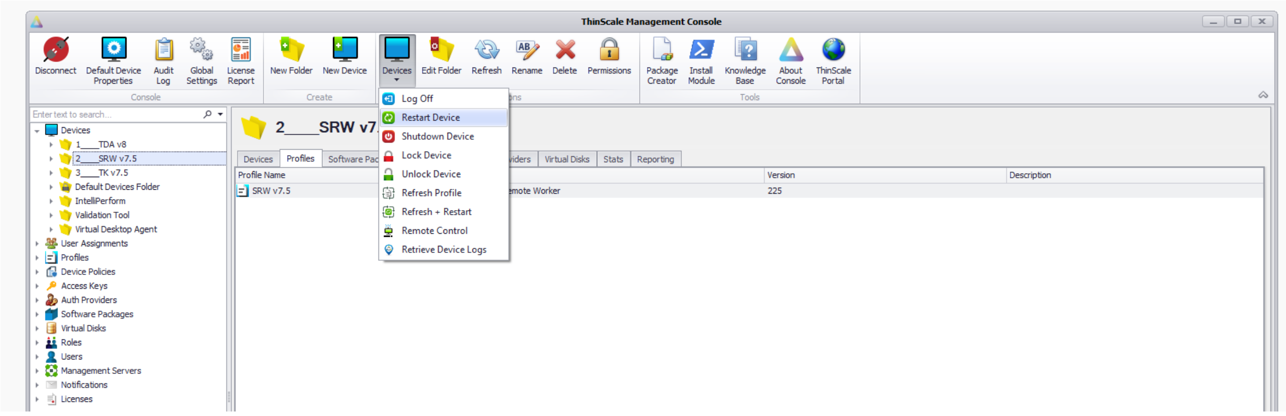
- Moving a Device from one folder to another will trigger a pending Profile update if required. This is indicated with red text for the **Active Profile** and **Profile Version** information in the Device view.



TK-WIN7-PC

Property	Data
Computer Name	TK-WIN7-PC
Product	ThinKiosk
Product Version	5.0.28.6487
Last Heard From	10/11/2017 09:40:44
Last Boot Time	10/11/2017 09:17:34
Last User	
IP Address	[redacted]
Active Profile	Secure Remote Worker
Active Profile Version	17

- The latest Profile is applied every time the Device logs on.
- Alternatively, it is possible to force a Profile update via the **Refresh Profile** option in the **Device** menu.



Profile Name		Version	Description
SRW v7.5	emote Worker	225	

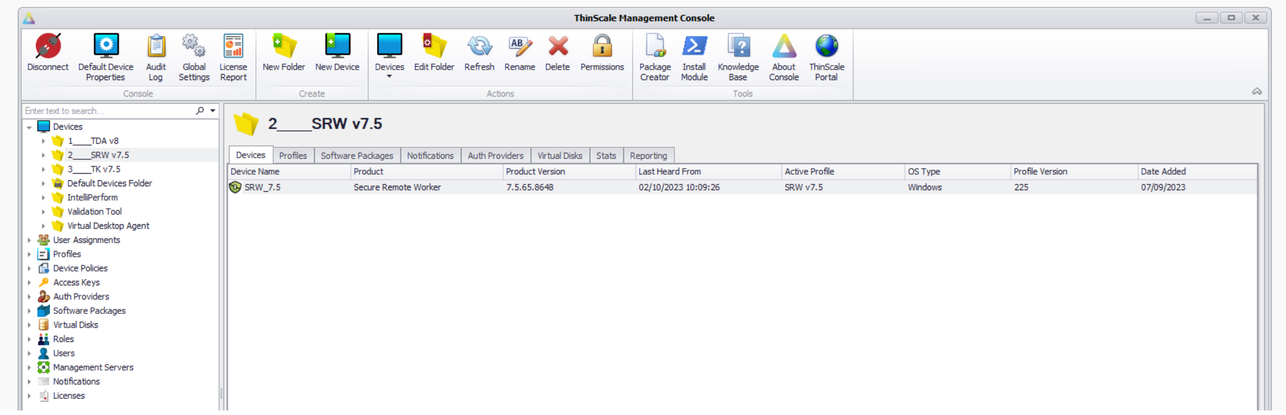
- Each device or device folder (along with every other Console object) can have different permissions applied. This makes it possible to control what Devices each Console user can see and what actions can be performed.

Device Folder

There are four tabs available when selecting a device folder from the tree list on the left.

Device Folder: Devices Tab

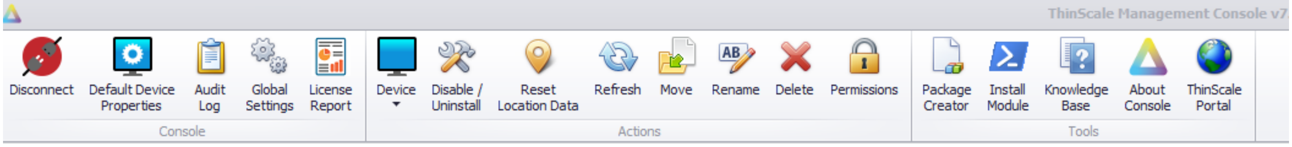
The first tab is a list of devices in the folder.



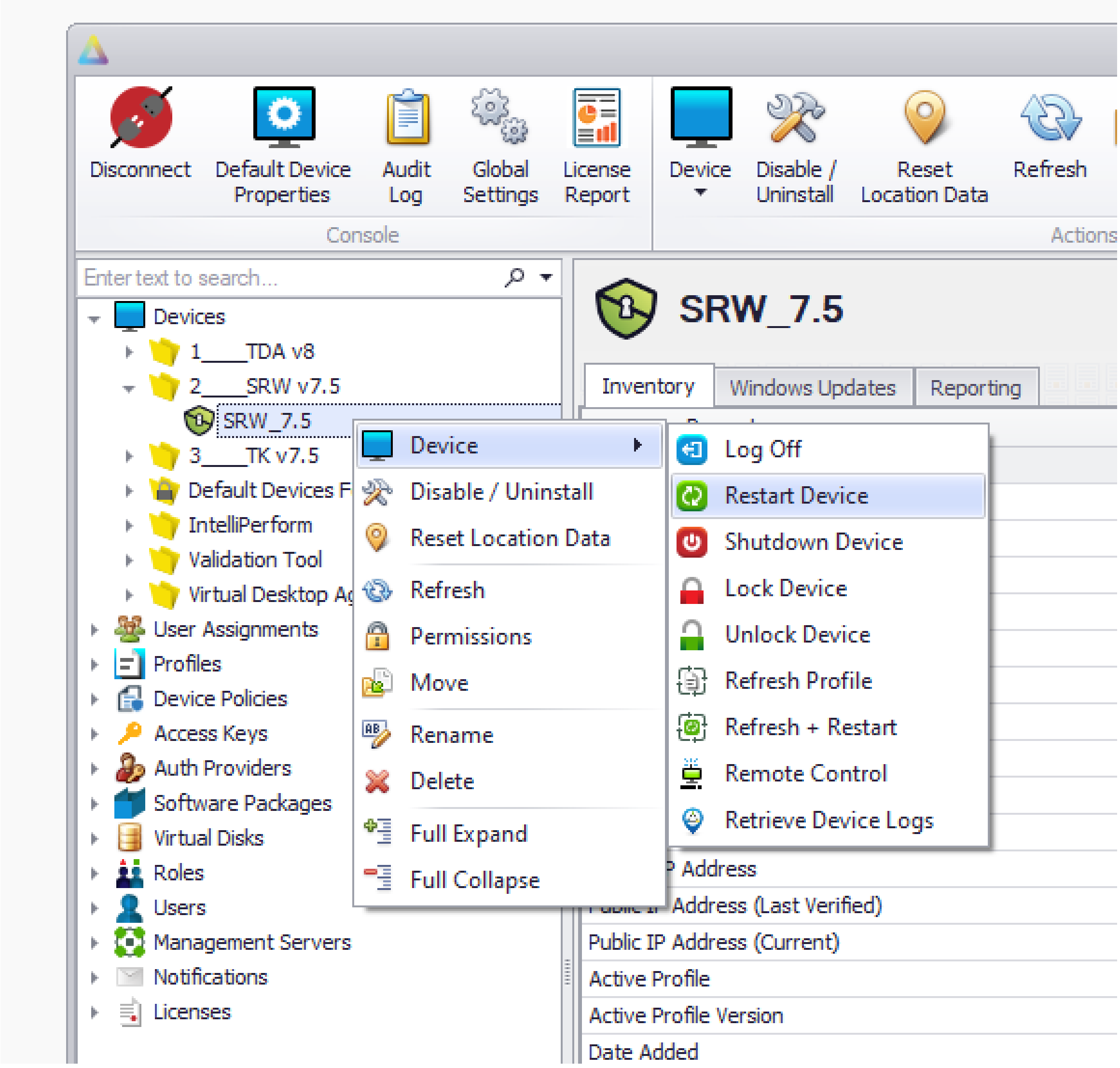
Device Name	Product	Product Version	Last Heard From	Active Profile	OS Type	Profile Version	Date Added
SRW_7.5	Secure Remote Worker	7.5.65.8648	02/10/2023 10:09:26	SRW v7.5	Windows	225	07/09/2023

Double-clicking a device will Jump To that device.

Selecting a device will update the ribbon bar with the actions that can be performed



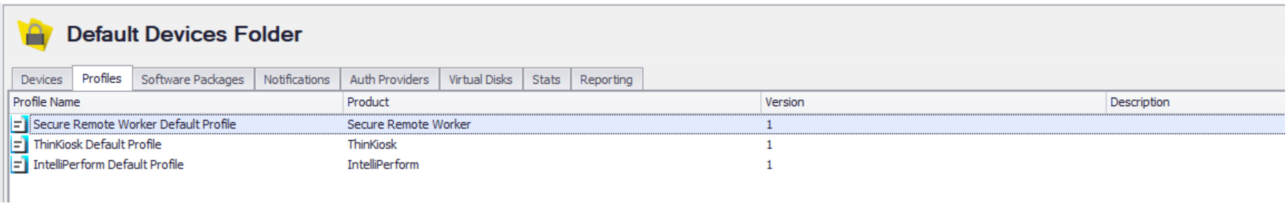
These options can also be accessed via the right-click context menu:



Note: The Device actions menu will only appear for an online device.

Device Folder: Assigned Profiles Tab

The **Assigned Profiles** tab shows what profile is assigned to the selected device folder:



Default Devices Folder

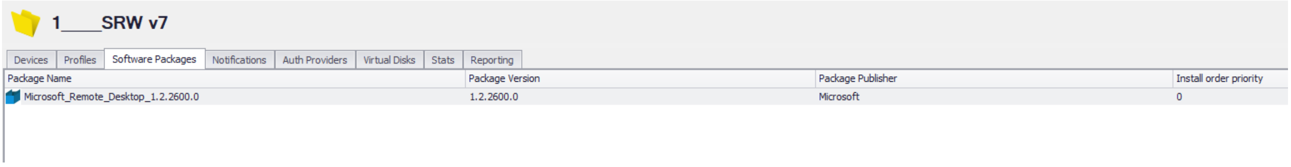
Profile Name	Product	Version	Description
Secure Remote Worker Default Profile	Secure Remote Worker	1	
ThinKiosk Default Profile	ThinKiosk	1	
IntelliPerform Default Profile	IntelliPerform	1	

All devices contained inside this folder will use this profile.

Any sub-folders will use this profile if one has not been directly assigned to that sub-folder. This works up the tree until a suitable profile is found. If one isn't found it will use the default profile shipped with the product.

Device Folder: Software Packages Tab

The **Software Packages** tab shows what packages are assigned to the selected device folder:

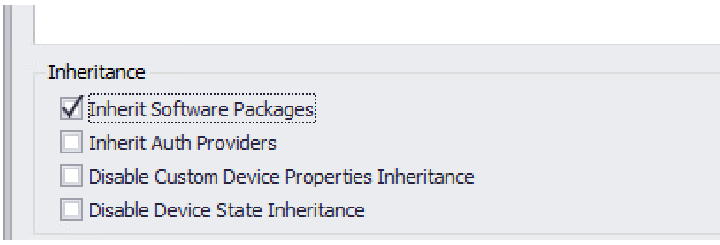


1____SRW v7

Package Name	Package Version	Package Publisher	Install order priority
Microsoft_Remote_Desktop_1.2.2600.0	1.2.2600.0	Microsoft	0

All devices contained inside this folder will install this software package.

Sub-folders will **not** inherit packages (unlike Assigned Profiles) unless specified in the folder properties.



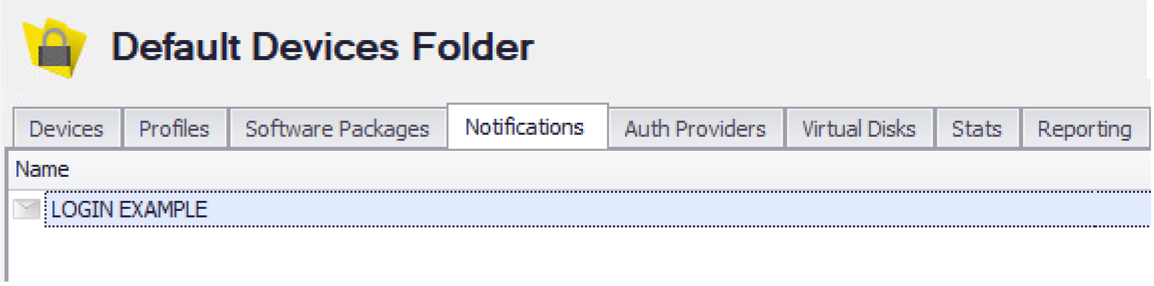
Inheritance

☑ Inherit Software Packages
□ Inherit Auth Providers
□ Disable Custom Device Properties Inheritance
□ Disable Device State Inheritance

Software packages must be assigned to each device folder that directly contains the device you wish to install the package.

Device Folder: Notification Tab

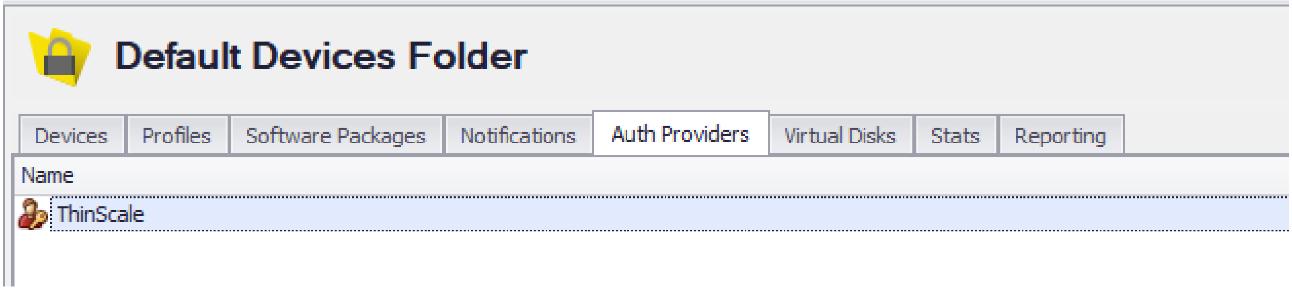
The **Notification** tab shows what notifications are assigned to the selected device folder:



Name
LOGIN EXAMPLE

Device Folder: Auth Providers Tab

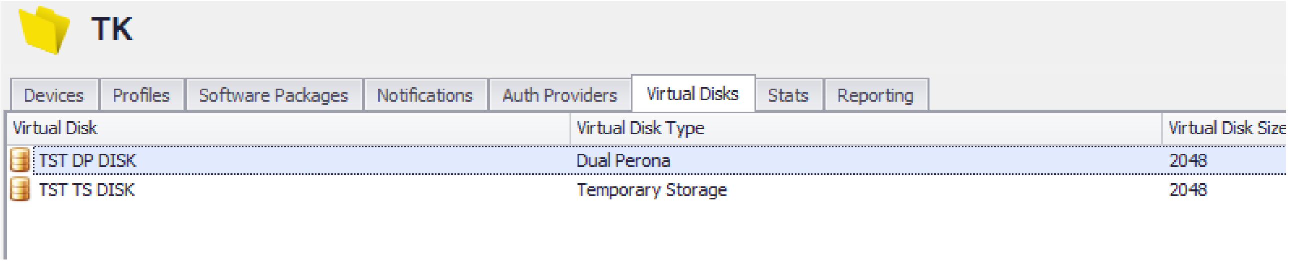
The **Auth Providers** tab shows what auth providers are assigned to the selected device folder:



Name
ThinScale

Device Folder: Virtual Disks Tab

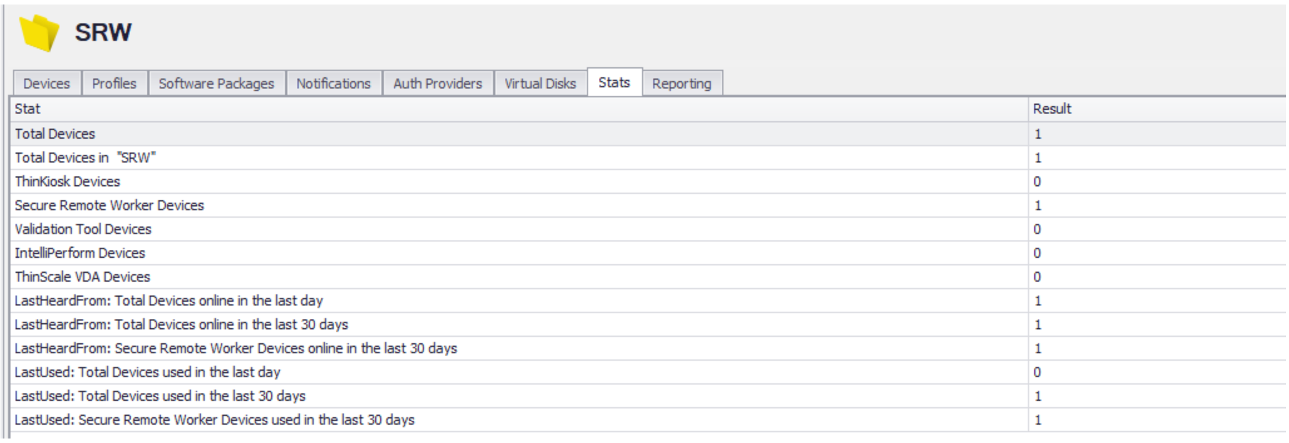
The **Virtual Disk** tab shows what virtual disks are assigned to the selected device folder:



Virtual Disk	Virtual Disk Type	Virtual Disk Size
TST DP DISK	Dual Perona	2048
TST TS DISK	Temporary Storage	2048

Device Folder: Stats Tab

The **Stats** tab shows the amount device contained in that folder:



SRW

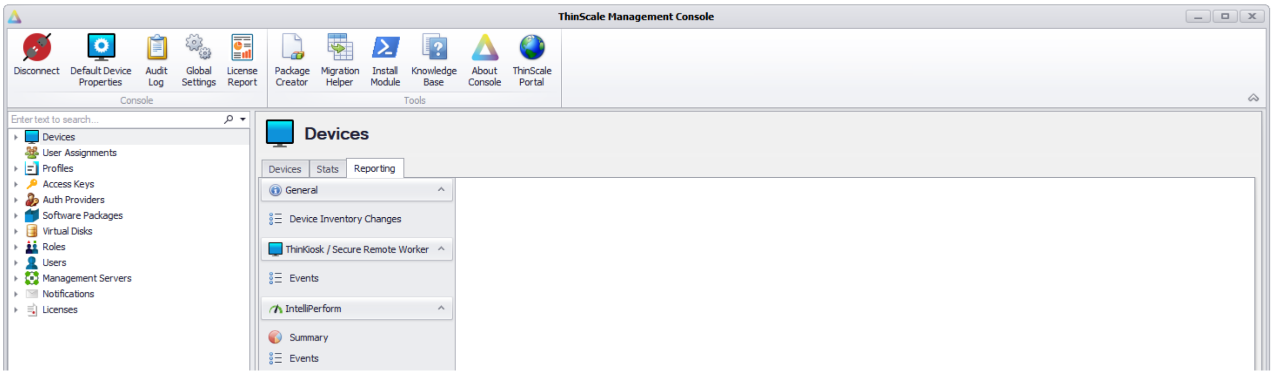
Devices | Profiles | Software Packages | Notifications | Auth Providers | Virtual Disks | Stats | Reporting

Stat	Result
Total Devices	1
Total Devices in "SRW"	1
ThinKiosk Devices	0
Secure Remote Worker Devices	1
Validation Tool Devices	0
IntelliPerform Devices	0
ThinScale VDA Devices	0
LastHeardFrom: Total Devices online in the last day	1
LastHeardFrom: Total Devices online in the last 30 days	1
LastHeardFrom: Secure Remote Worker Devices online in the last 30 days	1
LastUsed: Total Devices used in the last day	0
LastUsed: Total Devices used in the last 30 days	1
LastUsed: Secure Remote Worker Devices used in the last 30 days	1

Device Folder: Reporting Tab

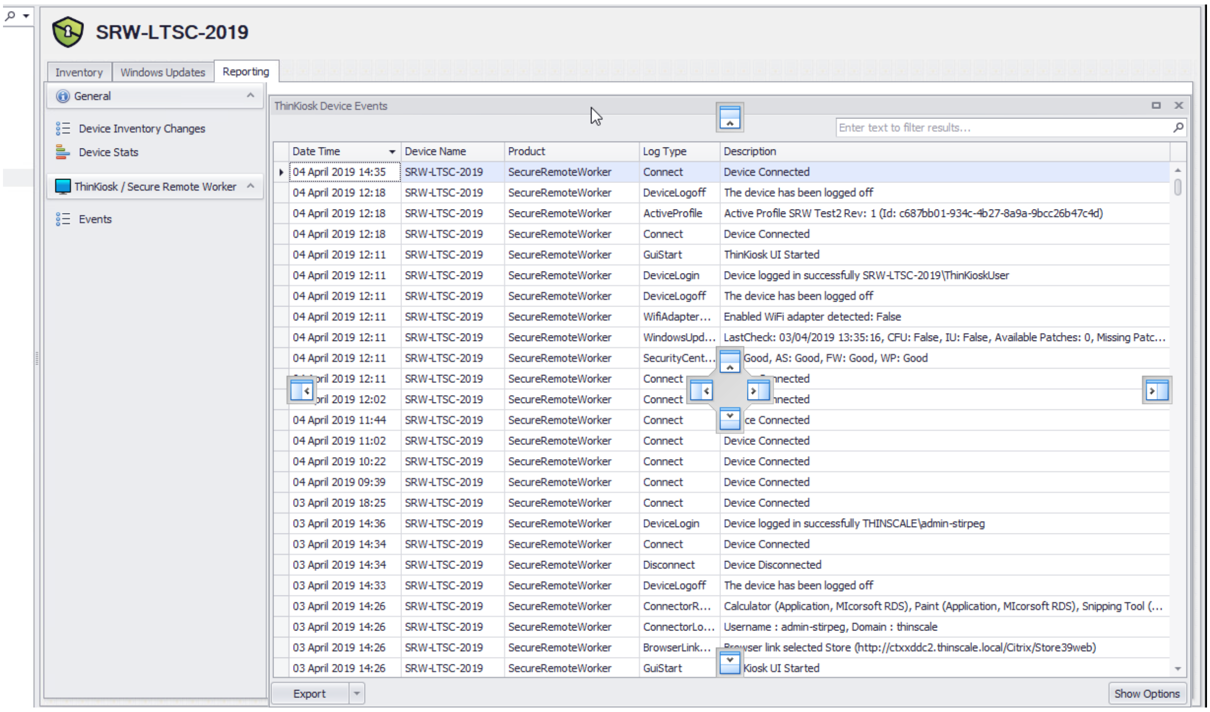
You can find the device reporting tab at:

- the root Devices level (shown below)
  - shows all reports available across all devices
- any device folder
  - shows the reports available for the devices contained in that folder and subfolder(s)
- individual devices
  - shows reports available only for that device



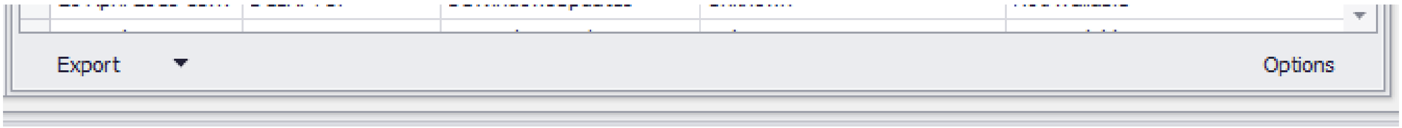
Features

- Multiple reports on screen side by side
- Reports can be undocked from the main window by dragging the report's header bar (shown below)

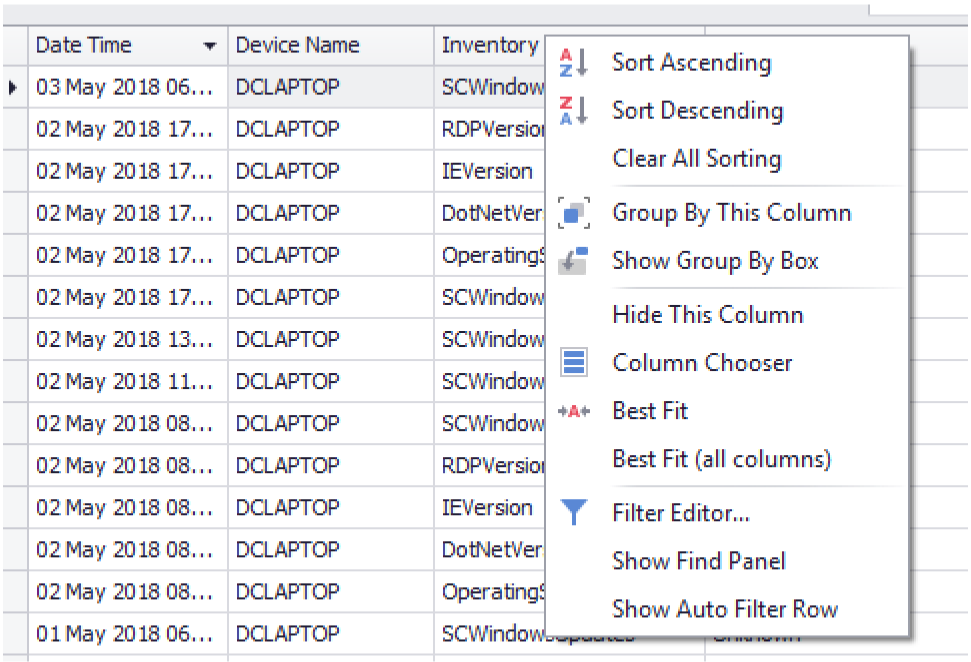


Date Time	Device Name	Product	Log Type	Description
04 April 2019 14:35	SRW-LTSC-2019	SecureRemoteWorker	Connect	Device Connected
04 April 2019 12:18	SRW-LTSC-2019	SecureRemoteWorker	DeviceLogoff	The device has been logged off
04 April 2019 12:18	SRW-LTSC-2019	SecureRemoteWorker	ActiveProfile	Active Profile SRW Test2 Rev: 1 (Id: c687bb01-934c-4b27-8a9a-9bcc26b47c4d)
04 April 2019 12:18	SRW-LTSC-2019	SecureRemoteWorker	Connect	Device Connected
04 April 2019 12:11	SRW-LTSC-2019	SecureRemoteWorker	GuiStart	ThinKiosk UI Started
04 April 2019 12:11	SRW-LTSC-2019	SecureRemoteWorker	DeviceLogin	Device logged in successfully SRW-LTSC-2019\ThinKioskUser
04 April 2019 12:11	SRW-LTSC-2019	SecureRemoteWorker	DeviceLogoff	The device has been logged off
04 April 2019 12:11	SRW-LTSC-2019	SecureRemoteWorker	WifiAdapter…	Enabled WiFi adapter detected: False
04 April 2019 12:11	SRW-LTSC-2019	SecureRemoteWorker	WindowsUpd…	LastCheck: 03/04/2019 13:35:16, CFU: False, IU: False, Available Patches: 0, Missing Patc…
04 April 2019 12:11	SRW-LTSC-2019	SecureRemoteWorker	SecurityCent…	Good, AS: Good, FW: Good, WP: Good
pril 2019 12:11	SRW-LTSC-2019	SecureRemoteWorker	Connect	nnected
pril 2019 12:02	SRW-LTSC-2019	SecureRemoteWorker	Connect	nnected
04 April 2019 11:44	SRW-LTSC-2019	SecureRemoteWorker	Connect	ce Connected
04 April 2019 11:02	SRW-LTSC-2019	SecureRemoteWorker	Connect	Device Connected
04 April 2019 10:22	SRW-LTSC-2019	SecureRemoteWorker	Connect	Device Connected
04 April 2019 09:39	SRW-LTSC-2019	SecureRemoteWorker	Connect	Device Connected
03 April 2019 18:25	SRW-LTSC-2019	SecureRemoteWorker	Connect	Device Connected
03 April 2019 14:36	SRW-LTSC-2019	SecureRemoteWorker	DeviceLogin	Device logged in successfully THINSCALE\admin-stirpeg
03 April 2019 14:34	SRW-LTSC-2019	SecureRemoteWorker	Connect	Device Connected
03 April 2019 14:34	SRW-LTSC-2019	SecureRemoteWorker	Disconnect	Device Disconnected
03 April 2019 14:33	SRW-LTSC-2019	SecureRemoteWorker	DeviceLogoff	The device has been logged off
03 April 2019 14:26	SRW-LTSC-2019	SecureRemoteWorker	ConnectorR…	Calculator (Application, MIcorsoft RDS), Paint (Application, MIcorsoft RDS), Snipping Tool (…
03 April 2019 14:26	SRW-LTSC-2019	SecureRemoteWorker	ConnectorLo…	Username : admin-stirpeg, Domain : thinscale
03 April 2019 14:26	SRW-LTSC-2019	SecureRemoteWorker	BrowserLink…	wser link selected Store (http://ctxxddc2.thinscale.local/Citrix/Store39web)
03 April 2019 14:26	SRW-LTSC-2019	SecureRemoteWorker	GuiStart	Kiosk UI Started

- **Export** and **Options** are available on every report.
    - Options will vary based on the chart. The defaults available on all charts are device filtering, start/end dates, and a results limit.



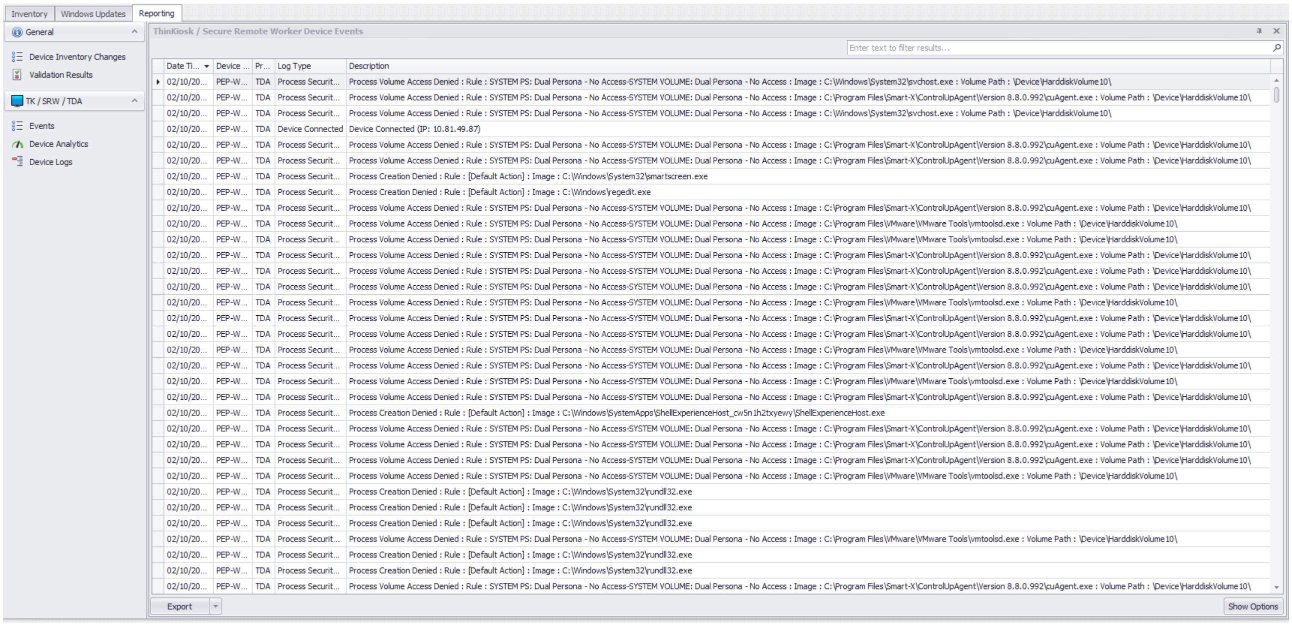
- In table reports, you can right-click the column header to bring up more options.



Date Time	Device Name	Inventory
03 May 2018 06...	DCLAPTOP	SCWindow
02 May 2018 17...	DCLAPTOP	RDPVersio
02 May 2018 17...	DCLAPTOP	IEVersion
02 May 2018 17...	DCLAPTOP	DotNetVer
02 May 2018 17...	DCLAPTOP	Operating$
02 May 2018 17...	DCLAPTOP	SCWindow
02 May 2018 13...	DCLAPTOP	SCWindow
02 May 2018 11...	DCLAPTOP	SCWindow
02 May 2018 08...	DCLAPTOP	SCWindow
02 May 2018 08...	DCLAPTOP	RDPVersio
02 May 2018 08...	DCLAPTOP	IEVersion
02 May 2018 08...	DCLAPTOP	DotNetVer
02 May 2018 08...	DCLAPTOP	Operating$
01 May 2018 06...	DCLAPTOP	SCWindowsUpdates

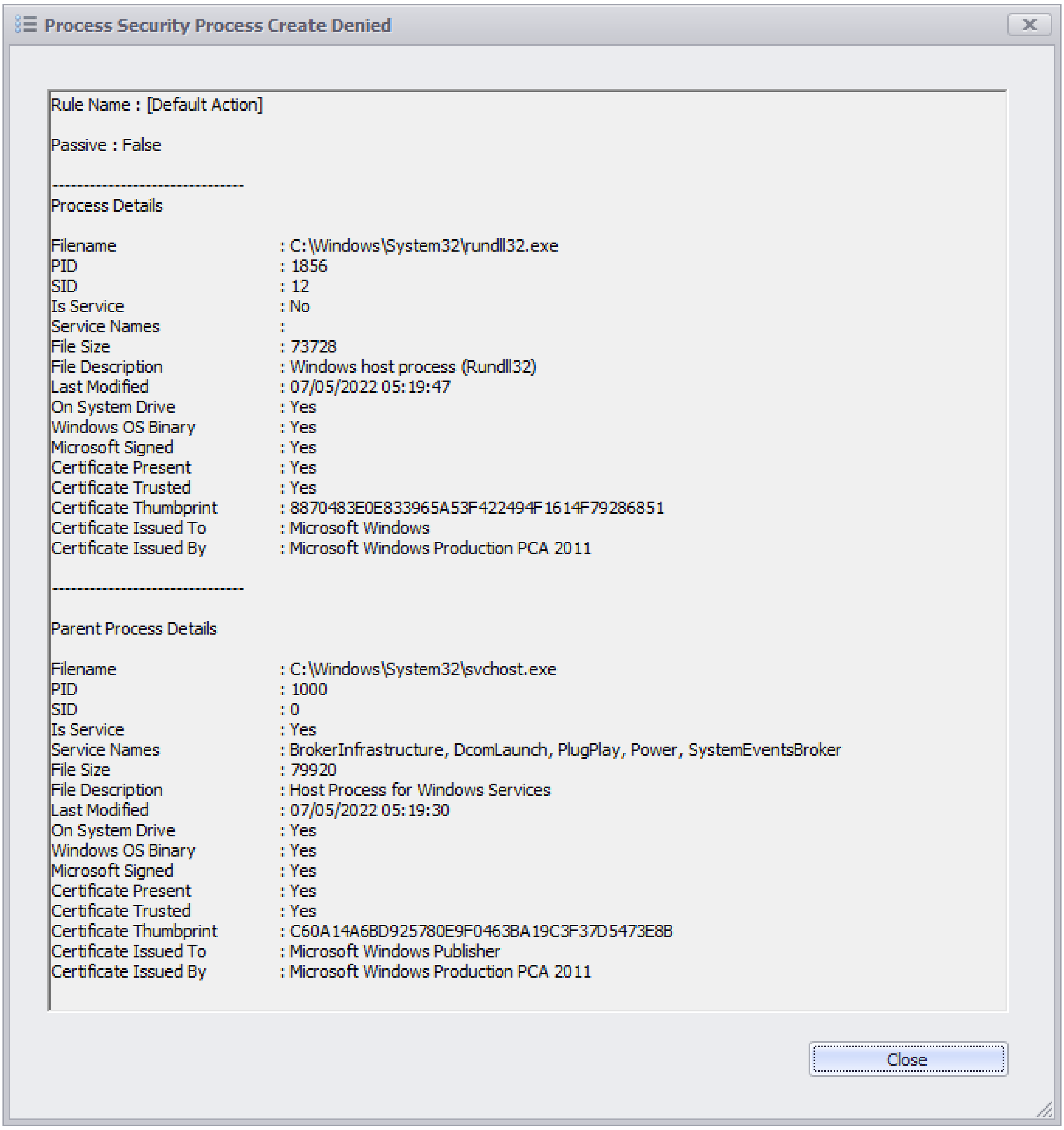
If a Device folder contains An IntelliPerform device, it will be also possible to see the data collected from IntelliPerform graphically with the use of line charts.
(Contact sales@thinscaletechnoogy.com) for more info about IntelliPerform software.

TDA Events



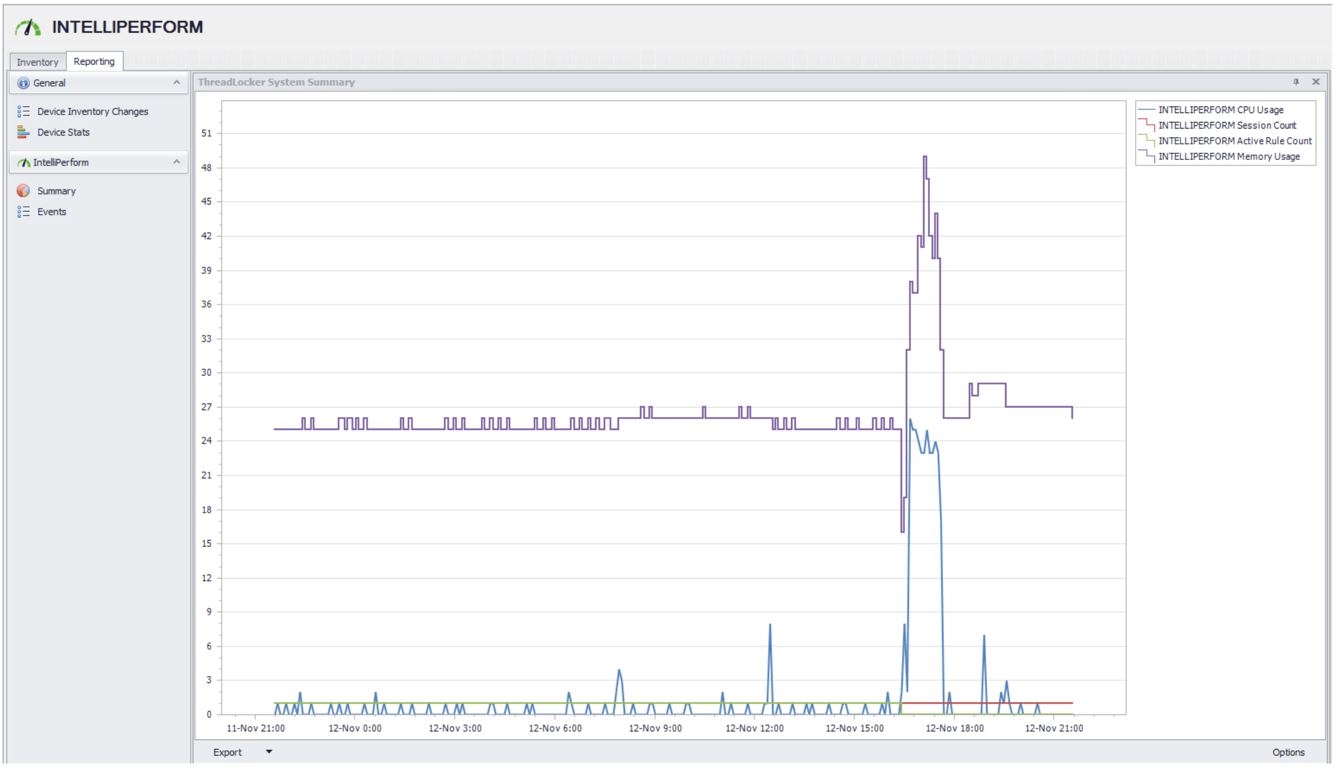
Date Ti...	Device ...	Pr...	Log Type	Description
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Windows\System32\svchost.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Windows\System32\svchost.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Device Connected	Device Connected (IP: 10.81.49.87)
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\System32\smartscreen.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\regedit.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\System32\rundll32.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\System32\rundll32.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\System32\rundll32.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\VMware\VMware Tools\vmtoolsd.exe : Volume Path : \Device\HarddiskVolume10\
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\System32\rundll32.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Creation Denied : Rule : [Default Action] : Image : C:\Windows\System32\rundll32.exe
02/10/20...	PEP-W...	TDA	Process Securit...	Process Volume Access Denied : Rule : SYSTEM PS: Dual Persona - No Access-SYSTEM VOLUME: Dual Persona - No Access : Image : C:\Program Files\Smart-X\ControlUpAgent\Version 8.8.0.992\cuAgent.exe : Volume Path : \Device\HarddiskVolume10\

TDA Events Details when double clicked



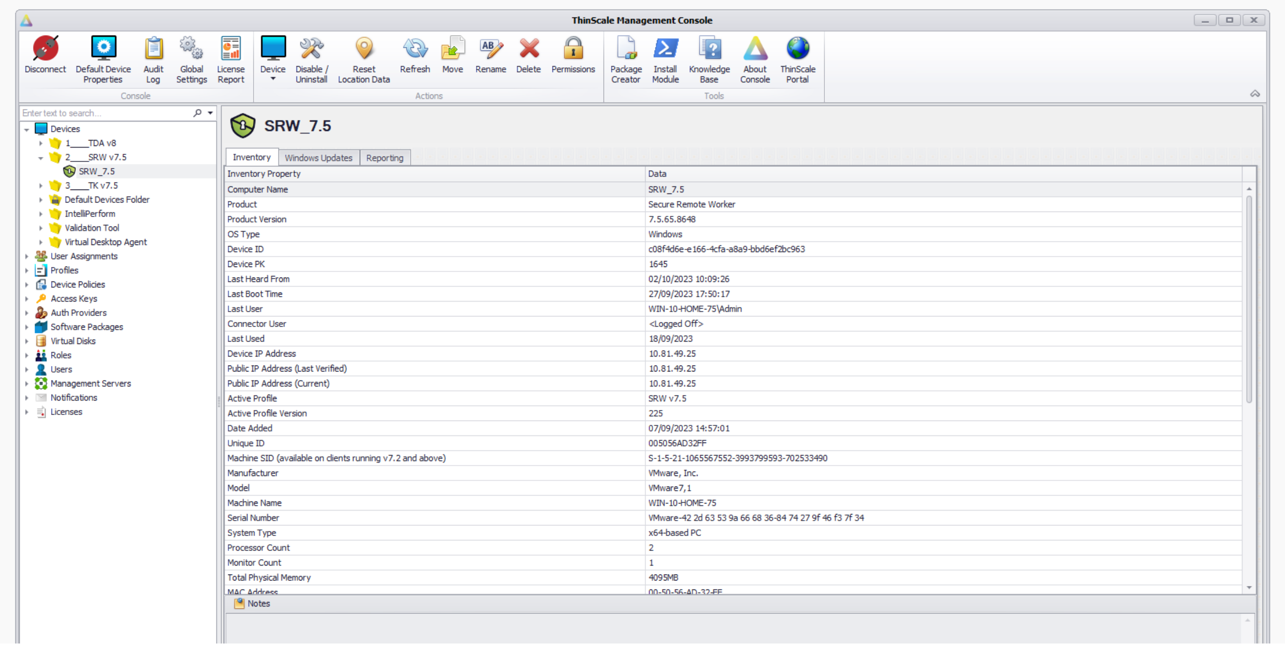
```
Rule Name : [Default Action]

Passive : False

--------------------------------
Process Details

Filename                    : C:\Windows\System32\rundll32.exe
PID                         : 1856
SID                         : 12
Is Service                  : No
Service Names               :
File Size                   : 73728
File Description            : Windows host process (Rundll32)
Last Modified               : 07/05/2022 05:19:47
On System Drive             : Yes
Windows OS Binary           : Yes
Microsoft Signed            : Yes
Certificate Present         : Yes
Certificate Trusted         : Yes
Certificate Thumbprint      : 8870483E0E833965A53F422494F1614F79286851
Certificate Issued To       : Microsoft Windows
Certificate Issued By       : Microsoft Windows Production PCA 2011

--------------------------------

Parent Process Details

Filename                    : C:\Windows\System32\svchost.exe
PID                         : 1000
SID                         : 0
Is Service                  : Yes
Service Names               : BrokerInfrastructure, DcomLaunch, PlugPlay, Power, SystemEventsBroker
File Size                   : 79920
File Description            : Host Process for Windows Services
Last Modified               : 07/05/2022 05:19:30
On System Drive             : Yes
Windows OS Binary           : Yes
Microsoft Signed            : Yes
Certificate Present         : Yes
Certificate Trusted         : Yes
Certificate Thumbprint      : C60A14A6BD925780E9F0463BA19C3F37D5473E8B
Certificate Issued To       : Microsoft Windows Publisher
Certificate Issued By       : Microsoft Windows Production PCA 2011
```

IntelliPerform



The data can be filtered by date and time, CPU usage, connected user or total locked processes, Alternatively, as previously stated, data can be exported in different formats.

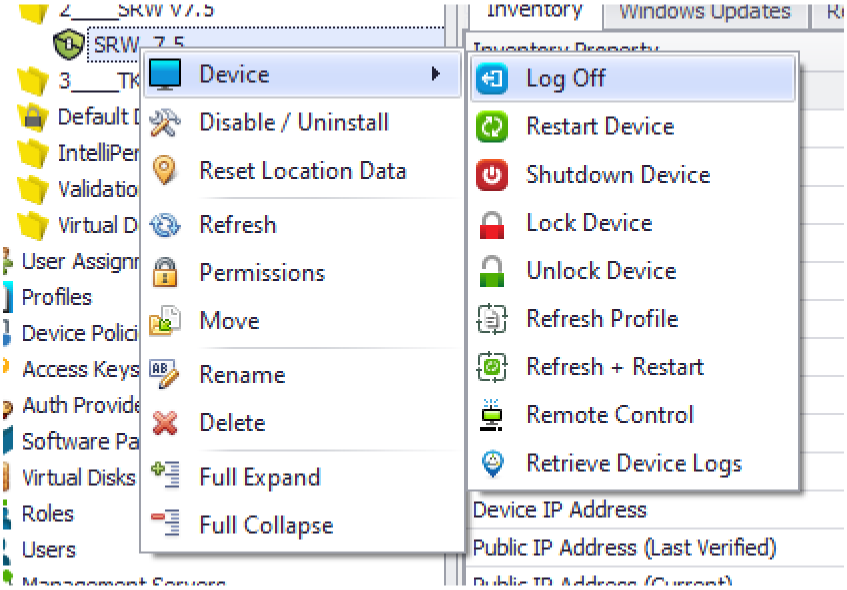
5. Device View



Inventory Property	Data
Computer Name	SRW_7.5
Product	Secure Remote Worker
Product Version	7.5.65.8648
OS Type	Windows
Device ID	c08f4d6e-e166-4cfa-a8a9-bbd6ef2bc963
Device PK	1645
Last Heard From	02/10/2023 10:09:26
Last Boot Time	27/09/2023 17:50:17
Last User	WIN-10-HOME-75\Admin
Connector User	<Logged Off>
Last Used	18/09/2023
Device IP Address	10.81.49.25
Public IP Address (Last Verified)	10.81.49.25
Public IP Address (Current)	10.81.49.25
Active Profile	SRW v7.5
Active Profile Version	225
Date Added	07/09/2023 14:57:01
Unique ID	005056AD32FF
Machine SID (available on clients running v7.2 and above)	S-1-5-21-1065567552-3993799593-702533490
Manufacturer	VMware, Inc.
Model	VMware7,1
Machine Name	WIN-10-HOME-75
Serial Number	VMware-42 2d 63 53 9a 66 68 36-84 74 27 9f 46 f3 7f 34
System Type	x64-based PC
Processor Count	2
Monitor Count	1
Total Physical Memory	4095MB
MAC Address	00-50-56-AD-32-FF

- You can reach the device view by clicking on any device.
- Here you will get a list of properties pertinent to the device.
- Properties can be copied by pressing CTRL + C with a value selected.
- You can write single Notes to better identify the device itself.

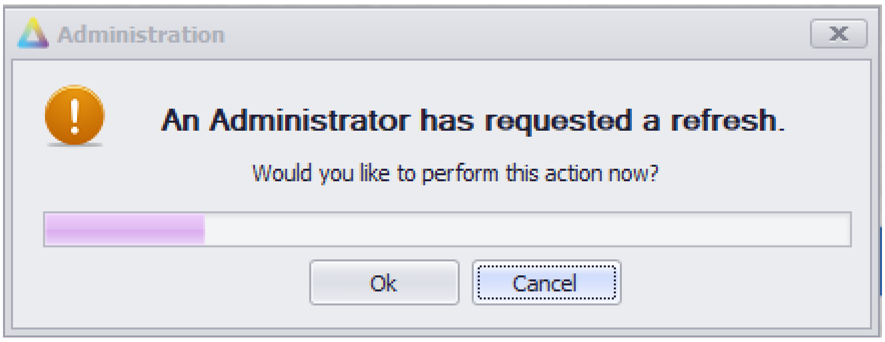
6. Device Actions



The device context menu contains a list of device actions that can be performed:

- **Log off** – Log off the current user *
- **Restart Device** – Sends a message to the device to restart the device *
- **Shutdown Device** - Sends a message to the device to shut down the device *
- **Lock Device** – sends a lock device command
- **Unlock Device** – sends an unlock device command
- **Refresh Profile** - Sends a message to the device to reload its profile *
- **Refresh + Restart** – sends a message to the device to reload its profile, then restart *
- **Remote Control** – Windows Vista and higher, will request a shadow session. The user must accept
- **Retrieve Device Logs** – Gets the device logs stored locally on the device. Useful for debugging.

Note: * delimits options where the user will be prompted for 15 seconds to proceed with the command, if 15 seconds pass, the command completes anyway.



An Administrator has requested a refresh.

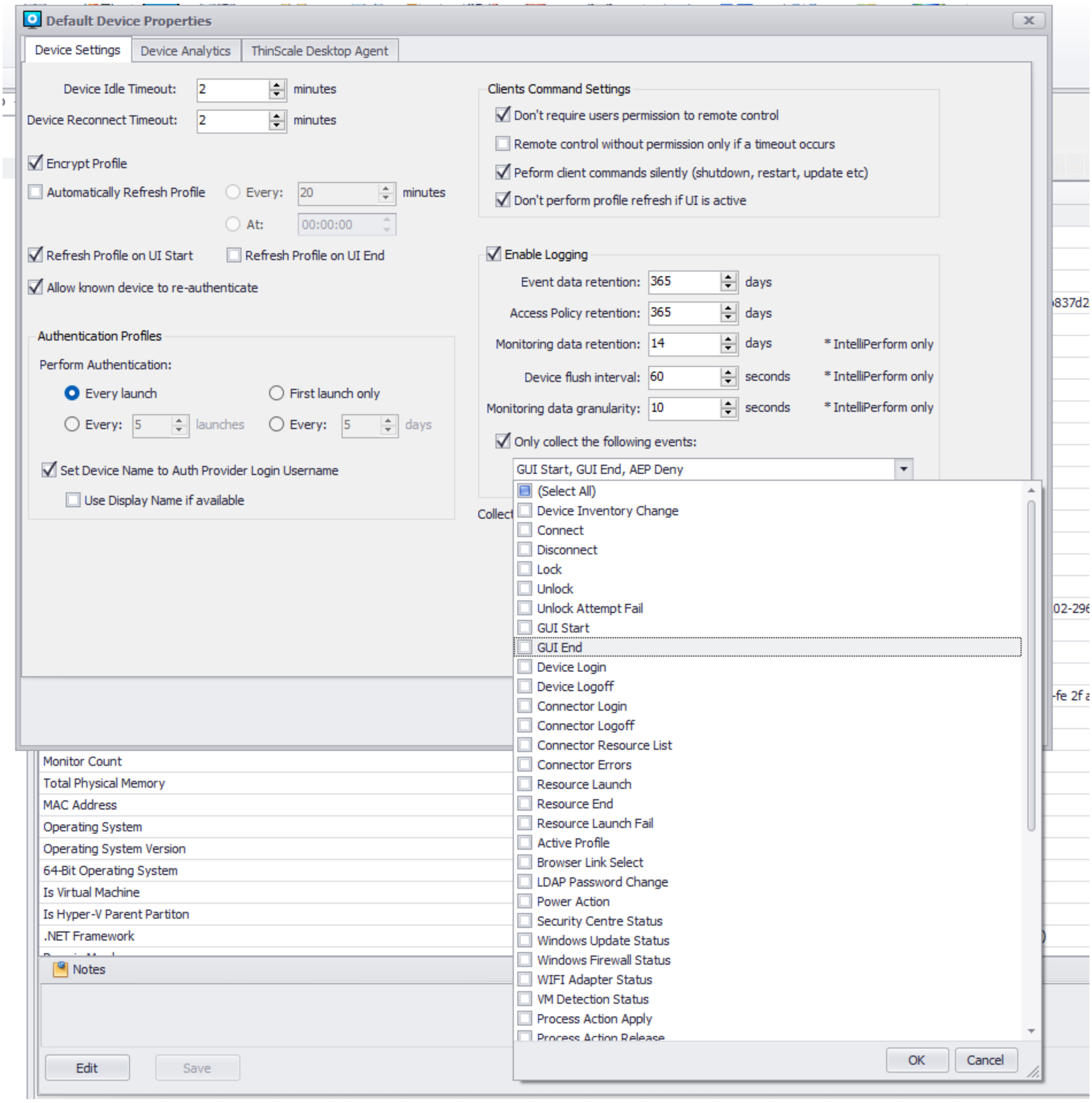
Would you like to perform this action now?

(A refresh command sent to the client will display this dialog to the user)

The device actions come in addition to a set of normal Console-related actions (Refresh, Rename, Delete and Permissions).

Note: If a device has been deleted, it will be re-added if the Device is still active with valid Access Keys/ Site credentials.

7. Default Device Properties



Device Idle Timeout: 2 minutes

Device Reconnect Timeout: 2 minutes

☑ Encrypt Profile

□ Automatically Refresh Profile ○ Every: 20 minutes

○ At: 00:00:00

☑ Refresh Profile on UI Start □ Refresh Profile on UI End

☑ Allow known device to re-authenticate

Authentication Profiles

Perform Authentication:

● Every launch ○ First launch only

○ Every: 5 launches ○ Every: 5 days

☑ Set Device Name to Auth Provider Login Username

□ Use Display Name if available

Clients Command Settings

☑ Don't require users permission to remote control

□ Remote control without permission only if a timeout occurs

☑ Peform client commands silently (shutdown, restart, update etc)

☑ Don't perform profile refresh if UI is active

☑ Enable Logging

Event data retention: 365 days

Access Policy retention: 365 days

Monitoring data retention: 14 days * IntelliPerform only

Device flush interval: 60 seconds * IntelliPerform only

Monitoring data granularity: 10 seconds * IntelliPerform only

☑ Only collect the following events:

GUI Start, GUI End, AEP Deny

- ▣ (Select All)
- □ Device Inventory Change
- □ Connect
- □ Disconnect
- □ Lock
- □ Unlock
- □ Unlock Attempt Fail
- □ GUI Start
- □ GUI End
- □ Device Login
- □ Device Logoff
- □ Connector Login
- □ Connector Logoff
- □ Connector Resource List
- □ Connector Errors
- □ Resource Launch
- □ Resource End
- □ Resource Launch Fail
- □ Active Profile
- □ Browser Link Select
- □ LDAP Password Change
- □ Power Action
- □ Security Centre Status
- □ Windows Update Status
- □ Windows Firewall Status
- □ WIFI Adapter Status
- □ VM Detection Status
- □ Process Action Apply
- □ Process Action Release

Monitor Count
Total Physical Memory
MAC Address
Operating System
Operating System Version
64-Bit Operating System
Is Virtual Machine
Is Hyper-V Parent Partiton
.NET Framework

The new Default Device Properties will let you choose what events you want to save in the DB with more control and granularity. **

*** Note: an SRW/TK machine service restart is required for this setting to be activated*

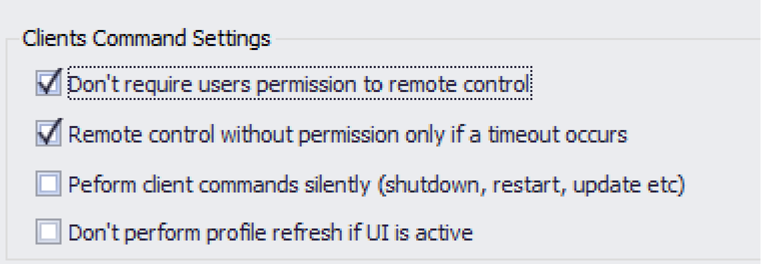
8. Device Remote Control

- The remote control is only supported on Windows 7 and higher versions of Windows up to and including Windows 10
- ThinKiosk on the client side will automatically create a firewall rule to allow RDP traffic in.
- Remote Control will not work through Network Address Translation; it works best on a LAN / WAN scenario.

Note: this feature only works on LAN and will not work when the ThinKiosk/SRW Client is connected to the ThinScale Server over a Public IP.

Requesting access

When an administrator requests control of the client, the user receives the following dialog to confirm or deny the connection, unless the option of controlling without user permission has been checked:



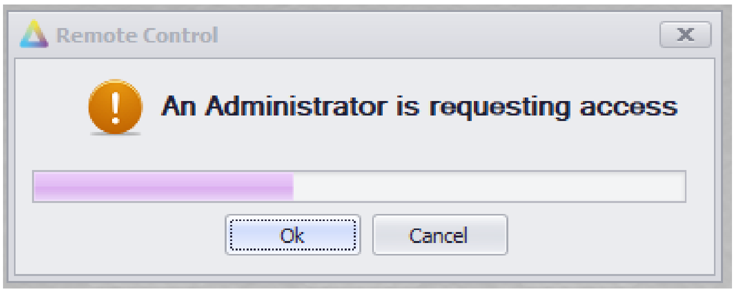
Clients Command Settings

☑ Don't require users permission to remote control

☑ Remote control without permission only if a timeout occurs

□ Peform client commands silently (shutdown, restart, update etc)

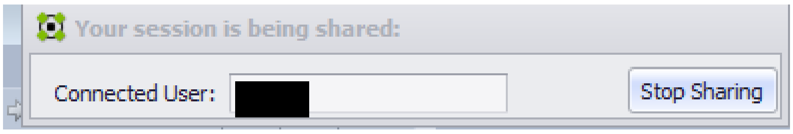
□ Don't perform profile refresh if UI is active



Remote Control

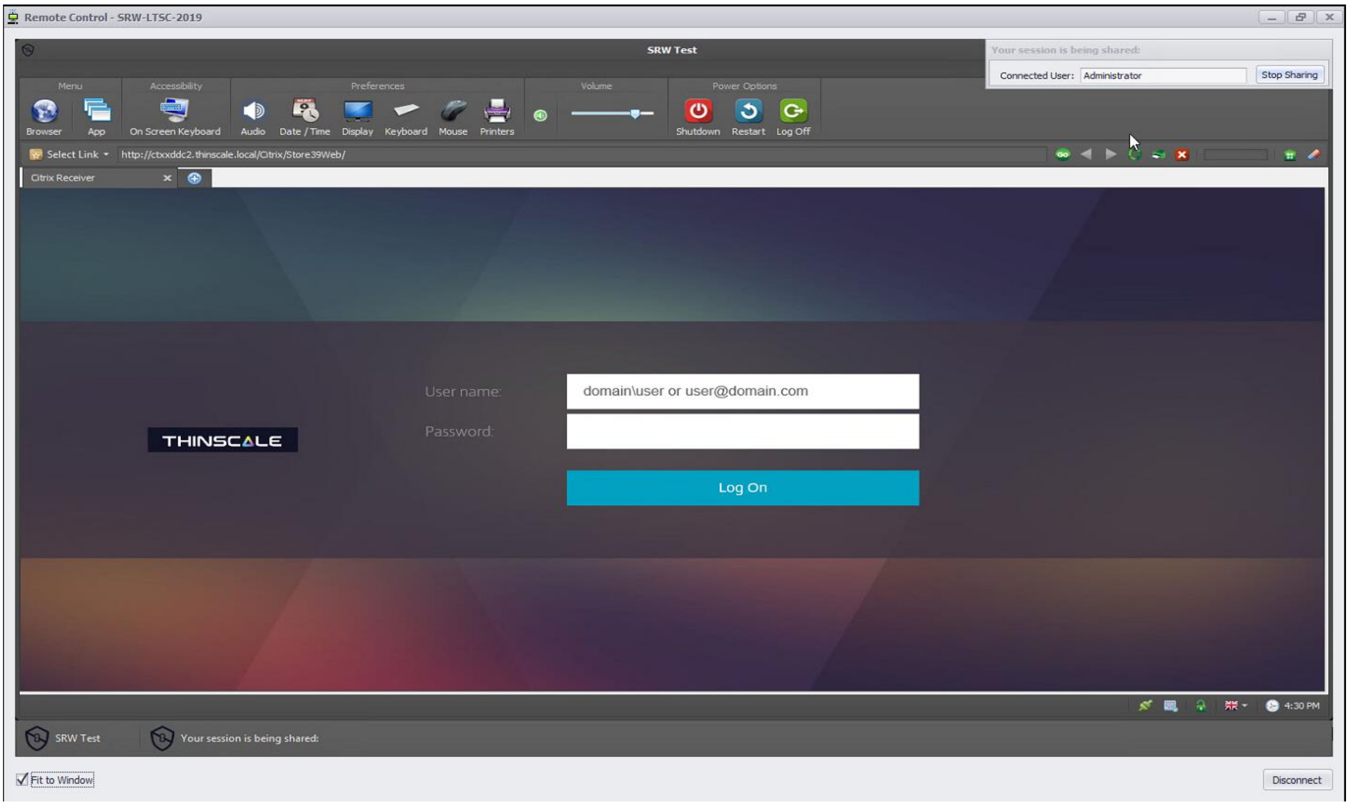
An Administrator is requesting access

If the user accepts, the RDP session is created and the PC from which the console is running creates a shadow connection to the ThinKiosk Device.
The user receives the following dialog allowing them to view who is connected and disconnect them if required:


Your session is being shared:

Connected User: [redacted]

The administrator receives the following shadow window:


Remote Control - SRW-LTSC-2019

SRW Test

Your session is being shared:

Connected User: Administrator

http://ctxxddc2.thinscale.local/Citrix/Store39Web/

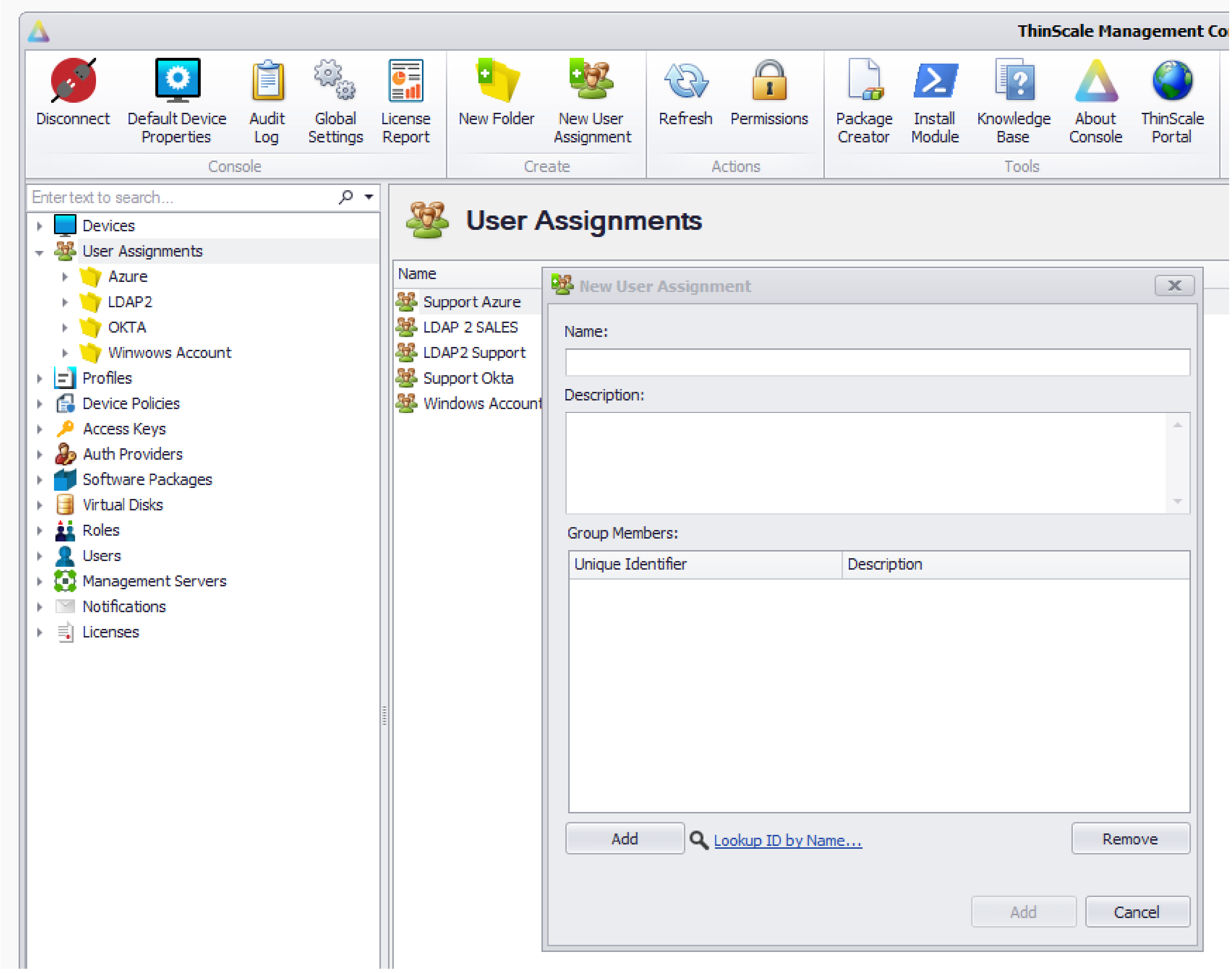
User name: domain\user or user@domain.com

Password:

Your session is being shared:

☑ Fit to Window

9. User Assignments



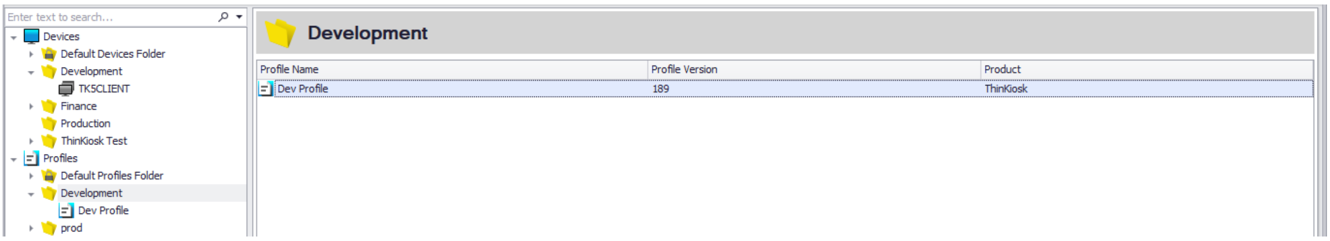
The new “User Assignments” let the administrators assign profiles and packages based on the group ID/s of the Authentication Providers.

A user that is a part of “Sales ID”, will receive a profile A and software package B, while a user that is part of “Development ID” will receive a profile C and a software package D, without the need for administrators to move devices and people around the console.

10. Profiles

Like Devices, Profiles can be organised into the required folder structure you wish for aesthetics, policy grouping, user departments or locations. Moving a Profile from one folder to another is purely an organisation task and will not affect running clients.

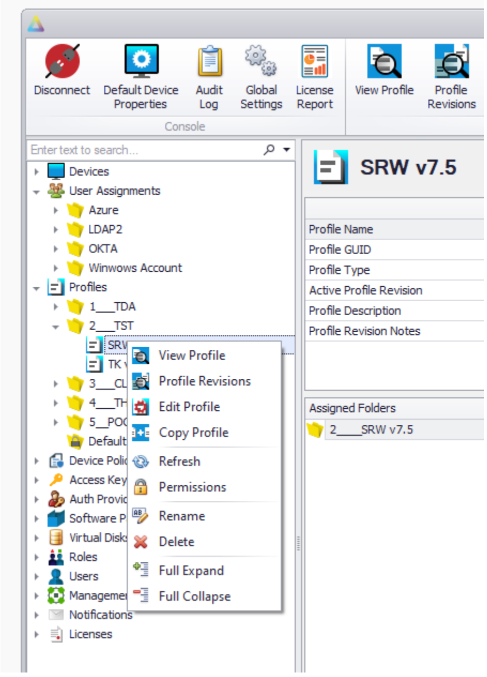
Profile Folder View



Profile Name	Profile Version	Product
Dev Profile	189	ThinKiosk

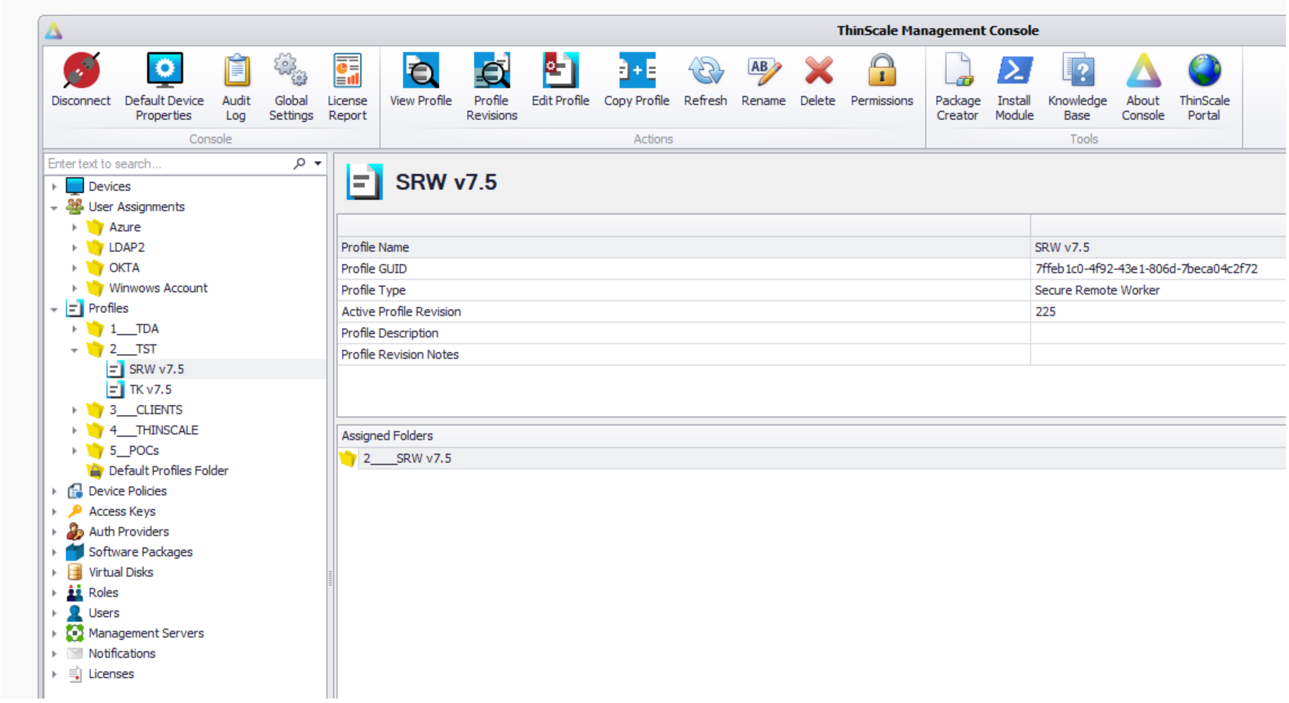
- By clicking a folder, you can view a list of profiles in this folder.
- Double-clicking a profile will use the "Jump to" function.
- Right clicking a profile will give you a context menu of options for that device.

Profile Context Menu



- **View Profile –** Opens a read-only view of the profile
- **Profile Revisions –** Opens a window that shows all the revisions made on that profile with comments and the date of the edit
- **Edit profile –** Modify the profile settings.
- **Copy Profile**- Copies the contents of the current profile into a new profile that you will be prompted to name.
- **Refresh –** Refreshes the current view to the latest server copy.
- **Rename –** Renames the profile selected
- **Delete –** Delete the profile from the console
- **Permissions –** Opens the Permission view attached to the folder.
- **Expand All –** Open all the nodes within the folder.

Profile View



SRW v7.5

Profile Name	SRW v7.5
Profile GUID	7ffeb1c0-4f92-43e1-806d-7beca04c2f72
Profile Type	Secure Remote Worker
Active Profile Revision	225
Profile Description	
Profile Revision Notes	

Assigned Folders
2____SRW v7.5

- You can reach the profile view by clicking on a Profile.
- Here you will get a list of properties pertinent to the device.
- You can also view the folders that have this profile assigned.

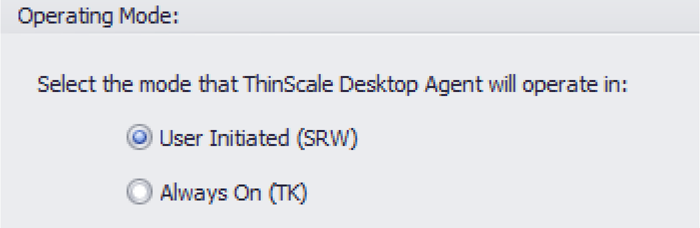
NEW

11. Device Policies

Device Policies encompass the comprehensive configuration settings required for our latest v8 ThinScale Desktop Agent (TDA).

Within these device policies, you will have the capability to define various configurations such as Modes, Device Login Preferences, Branding, and additional settings.

Operating Mode



Operating Mode:

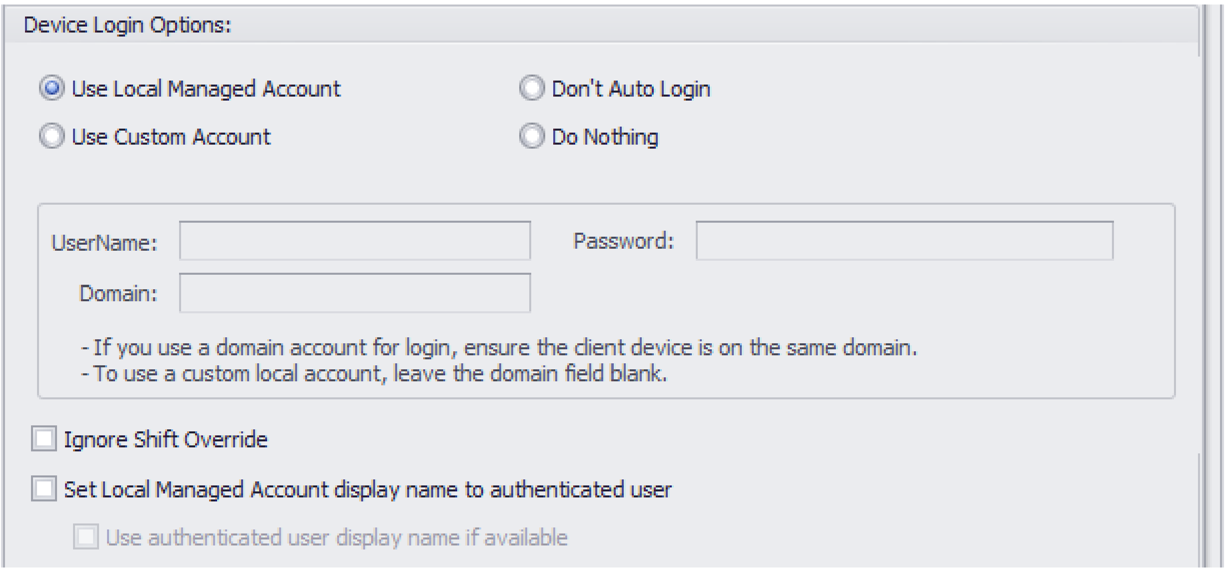
Select the mode that ThinScale Desktop Agent will operate in:

● User Initiated (SRW)

○ Always On (TK)

With the new TDA, it becomes feasible to seamlessly switch between SRW and TK modes without the necessity of reinstalling the client. You can effortlessly modify the mode and then restart the client.

Device Login Options



Device Login Options:

● Use Local Managed Account ○ Don't Auto Login

○ Use Custom Account ○ Do Nothing

UserName: Password:

Domain:

- If you use a domain account for login, ensure the client device is on the same domain.
- To use a custom local account, leave the domain field blank.

☐ Ignore Shift Override

☐ Set Local Managed Account display name to authenticated user

☐ Use authenticated user display name if available

Please note that Device Login Preferences are relevant only when operating in TK Mode.

Use Local Managed Account

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

Use Custom Account

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

Don’t Auto Login

Disables any configured auto-login settings.

Do Nothing

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

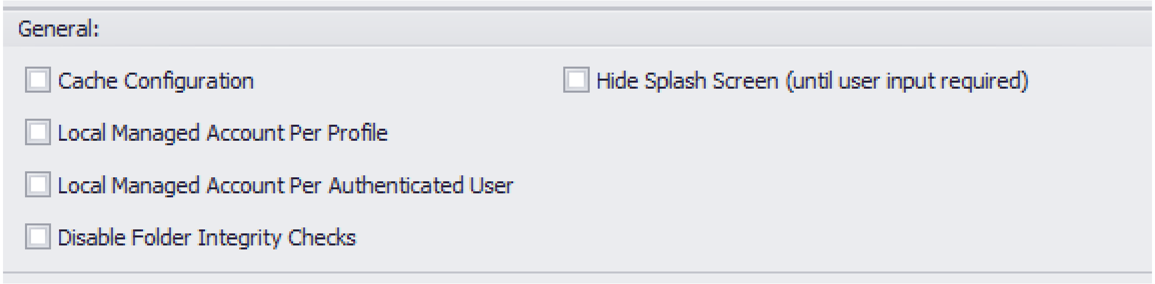
Ignore Shift Override

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

Set Local Managed Account display name to an authenticated user

If enabled, the display name while login to the machine will be set using the username typed in the Authentication Provider screen

General



General:

□ Cache Configuration

□ Local Managed Account Per Profile

□ Local Managed Account Per Authenticated User

□ Disable Folder Integrity Checks

□ Hide Splash Screen (until user input required)

Cache Configuration

If enabled, profiles assigned to the Device folder will be saved and encrypted locally. Please note there are two locations:

1. **Programdata\tda\devicedata\devicedata.cache**
2. **HKEY_LOCAL_MACHINE\SOFTWARE\ThinScale\TDA\DeviceGroupConfiguration**

Local Managed Account Per Profile

If enabled, TDA will create a separate Windows User Profile per profile assigned to the device folder

Local Managed Account Per Authentication User

If enabled, TDA will create a separate Windows User Profile for every user logged in using the Authentication Provider

Disable Folder Integrity Check

If enabled, the TDA will not check for the integrity of its Core Modules folders. Not recommended when in SRW Mode.

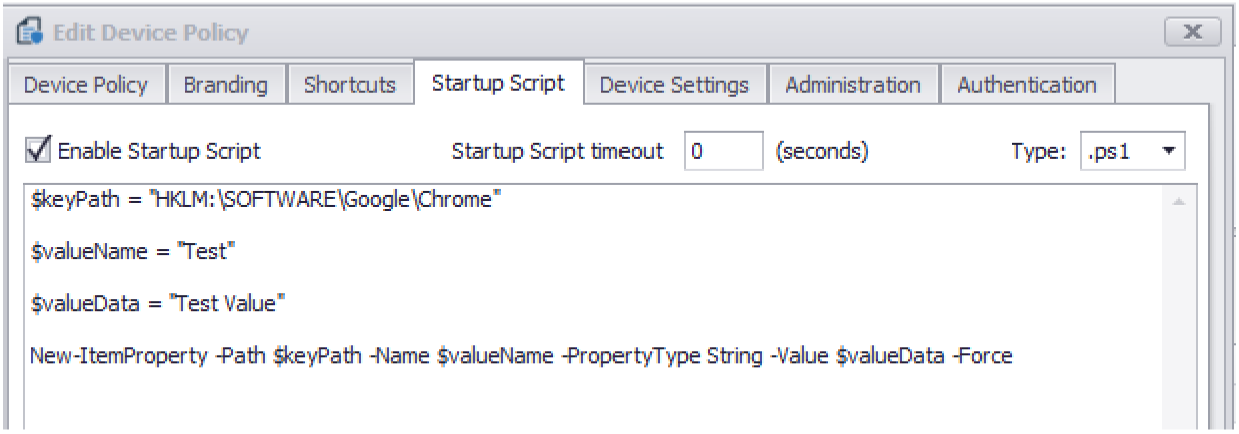
Hide Splash Screen

If enabled, the TDA will hide the loading of its initial UI screen, unless a user input is required.

Branding and Shortcut

With the introduction of v8, TDA now enables you to effortlessly configure custom splash screen images and personalized desktop icons directly through the Management Console. Simply upload your desired image within the device policy, use a .ico file for the desktop shortcut, and your customization is complete.

Startup Script



☑ Enable Startup Script   Startup Script timeout 0 (seconds)   Type: .ps1

```
$keyPath = "HKLM:\SOFTWARE\Google\Chrome"

$valueName = "Test"

$valueData = "Test Value"

New-ItemProperty -Path $keyPath -Name $valueName -PropertyType String -Value $valueData -Force
```

Enable Startup Script

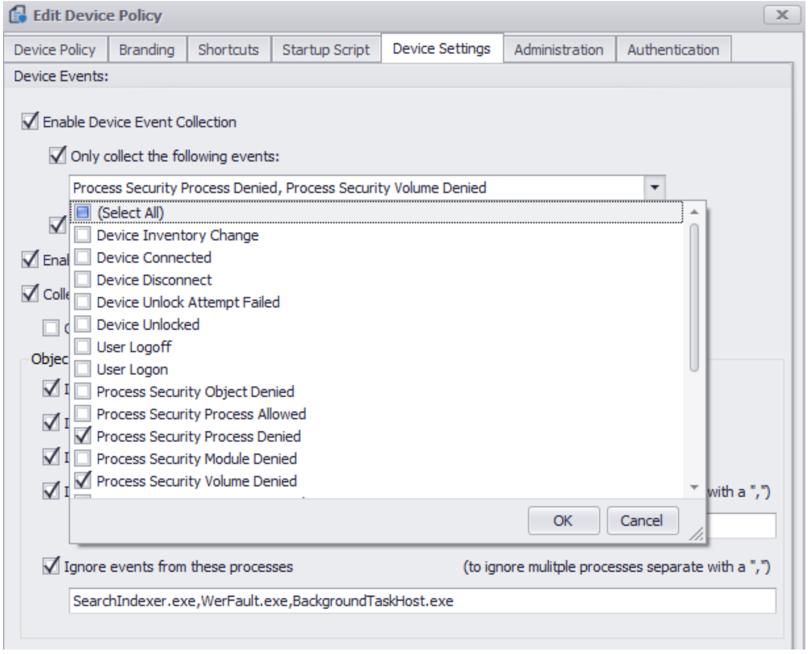
Enables the supplied.VBS or. BAT or PS1 startup script. The script is configured as a local group policy start-up script and will apply during the Windows boot process.

Startup Script Timeout

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

Device Settings

Inside the device settings tab, you'll have the capability to configure all the options pertaining to Device Logs. This includes the ability to selectively choose the events of greatest significance, gather results from Access Policies, exclude frequently recurring processes and services, and predominantly enable "Troubleshooting Mode."



Edit Device Policy

Device Policy | Branding | Shortcuts | Startup Script | Device Settings | Administration | Authentication

Device Events:

☑ Enable Device Event Collection

☑ Only collect the following events:

Process Security Process Denied, Process Security Volume Denied

- ■ (Select All)
- □ Device Inventory Change
- □ Device Connected
- □ Device Disconnect
- □ Device Unlock Attempt Failed
- □ Device Unlocked
- □ User Logoff
- □ User Logon
- □ Process Security Object Denied
- □ Process Security Process Allowed
- ☑ Process Security Process Denied
- □ Process Security Module Denied
- ☑ Process Security Volume Denied

OK | Cancel

☑

☑ Enal

☑ Colle

□ C

Objec

☑ I

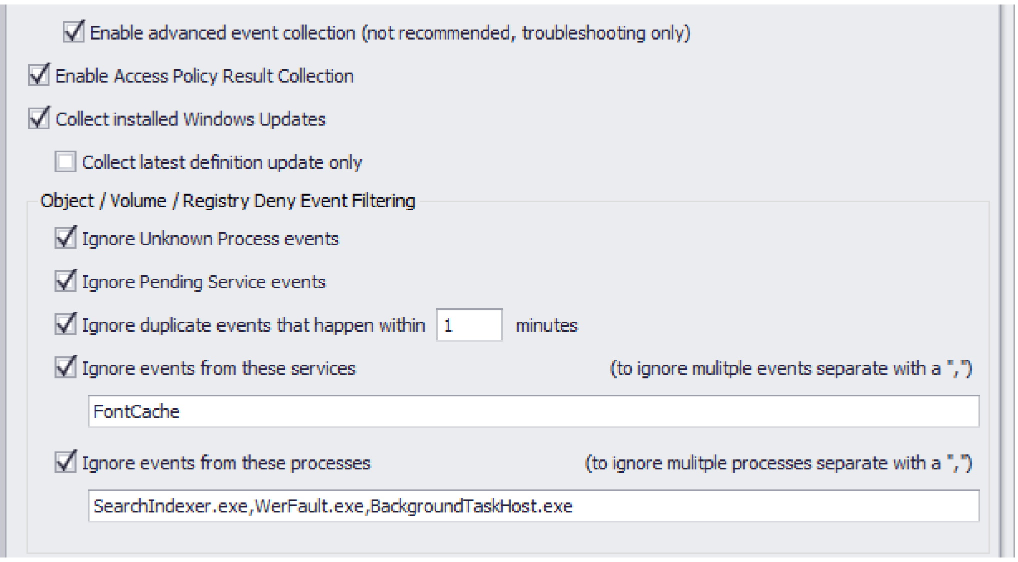
☑ I

☑ I

☑ I with a ",")

☑ Ignore events from these processes (to ignore mulitple processes separate with a ",")

SearchIndexer.exe,WerFault.exe,BackgroundTaskHost.exe



☑ Enable advanced event collection (not recommended, troubleshooting only)

☑ Enable Access Policy Result Collection

☑ Collect installed Windows Updates

□ Collect latest definition update only

Object / Volume / Registry Deny Event Filtering

☑ Ignore Unknown Process events

☑ Ignore Pending Service events

☑ Ignore duplicate events that happen within 1 minutes

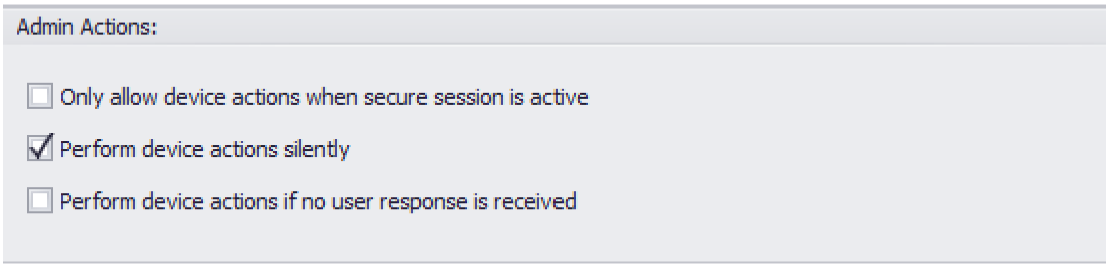
☑ Ignore events from these services (to ignore mulitple events separate with a ",")

FontCache

☑ Ignore events from these processes (to ignore mulitple processes separate with a ",")

SearchIndexer.exe,WerFault.exe,BackgroundTaskHost.exe

Admin Actions



Admin Actions:

□ Only allow device actions when secure session is active

☑ Perform device actions silently

□ Perform device actions if no user response is received

Only allow device action when in secure session

If enabled, actions like Restart, Profile Refresh will be only performed when the TDA session is active.

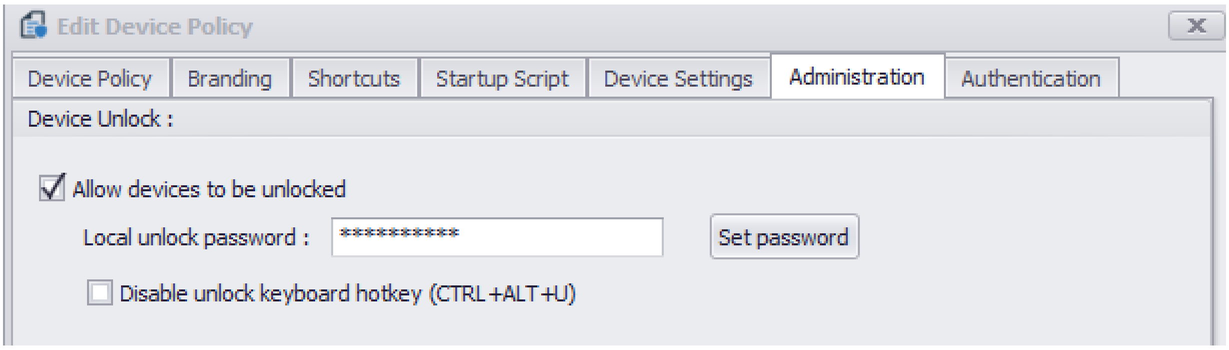
Perform device actions silently

If enabled, actions like Restart, Profile Refresh will be performed silently without user consent.

Perform device actions if no user response is received

If enabled, actions like Restart, Profile Refresh will be performed only when the user fails to accept or deny the request.

Administration



Device Unlock :

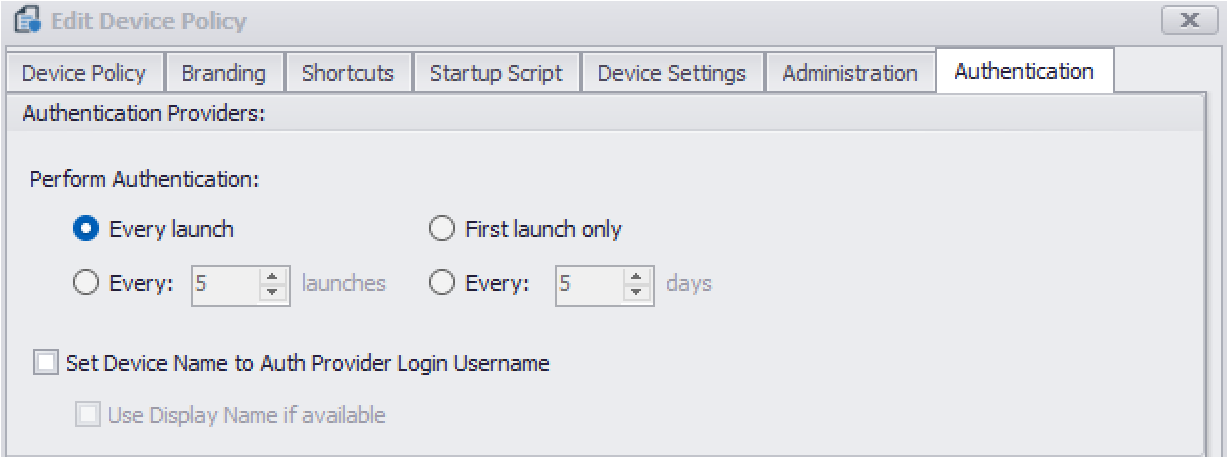
☑ Allow devices to be unlocked

Local unlock password : ***********

□ Disable unlock keyboard hotkey (CTRL+ALT+U)

Here is where you have the option to set the unlock password for the TDA client. Additionally, you can deactivate the unlock key hotkey (Ctrl-Alt-U) to exclusively require an unlock through the Management Console.

Authentication



Authentication Providers:

Perform Authentication:

● Every launch ○ First launch only

○ Every: 5 launches ○ Every: 5 days

□ Set Device Name to Auth Provider Login Username

□ Use Display Name if available

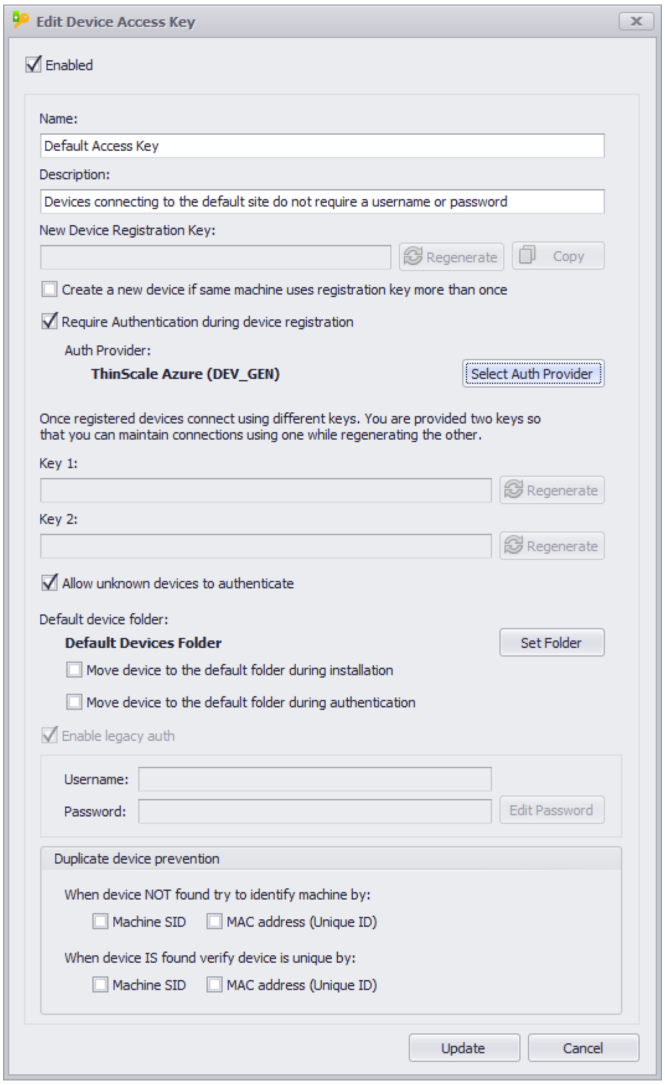
Here is where you have the option to control the behaviour of the Authentication Provider screen.

You can also set the option to rename the device connected to the server with the username typed in the Auth Provider screen.

12. Access Keys

Access Keys are the entry point for all devices into the Management Platform.

You can create any number of Access Keys that different devices can connect to. For example, you can create two Access Keys that have different credentials and default device folders. This will allow different devices connecting via the different Access Keys to require different credentials and can be registered into different device folders in the console assigning different profiles and packages if desired.



Edit Device Access Key

☑ Enabled

Name: Default Access Key

Description: Devices connecting to the default site do not require a username or password

New Device Registration Key:

□ Create a new device if same machine uses registration key more than once

☑ Require Authentication during device registration

Auth Provider: **ThinScale Azure (DEV_GEN)**

Once registered devices connect using different keys. You are provided two keys so that you can maintain connections using one while regenerating the other.

Key 1:

Key 2:

☑ Allow unknown devices to authenticate

Default device folder: **Default Devices Folder**

□ Move device to the default folder during installation

□ Move device to the default folder during authentication

☑ Enable legacy auth

Username:

Password:

Duplicate device prevention

When device NOT found try to identify machine by:

□ Machine SID □ MAC address (Unique ID)

When device IS found verify device is unique by:

□ Machine SID □ MAC address (Unique ID)

- Enter a Name and Description for your new Access Key
- Access Keys have 3 keys associated with them
  - Device Registration Key – Used by devices during initial installation
  - Key1 and Key2 – Used by devices to connect after installation
- Changing the Device Registration Key will not impact existing devices, but new installations will need to provide the updated key during installation
- Create a new device option – if a enabled every time a machine re-uses the registration key a duplicate entry is created in the Management Console
- NEW **Require Authentication** – if enabled during installation the machine will be forced to authenticate against an Authentication Provider (i.e., Azure, Okta or LDAP if the domain is available)
- Devices can use either Key1 or Key2 to authenticate to the Management Server. As long as one key is correct the device will authenticate.
- Using 2 keys allows the keys to be rotated without having to reinstall or reconfigure the devices using them
- Change the default device folder so new devices are placed into that folder. This way the new device will adopt the required Profile and Software Packages on login automatically.

Enable Legacy Auth

Enabling legacy authentication allows older devices (pre-V7) to connect to the Management Server.

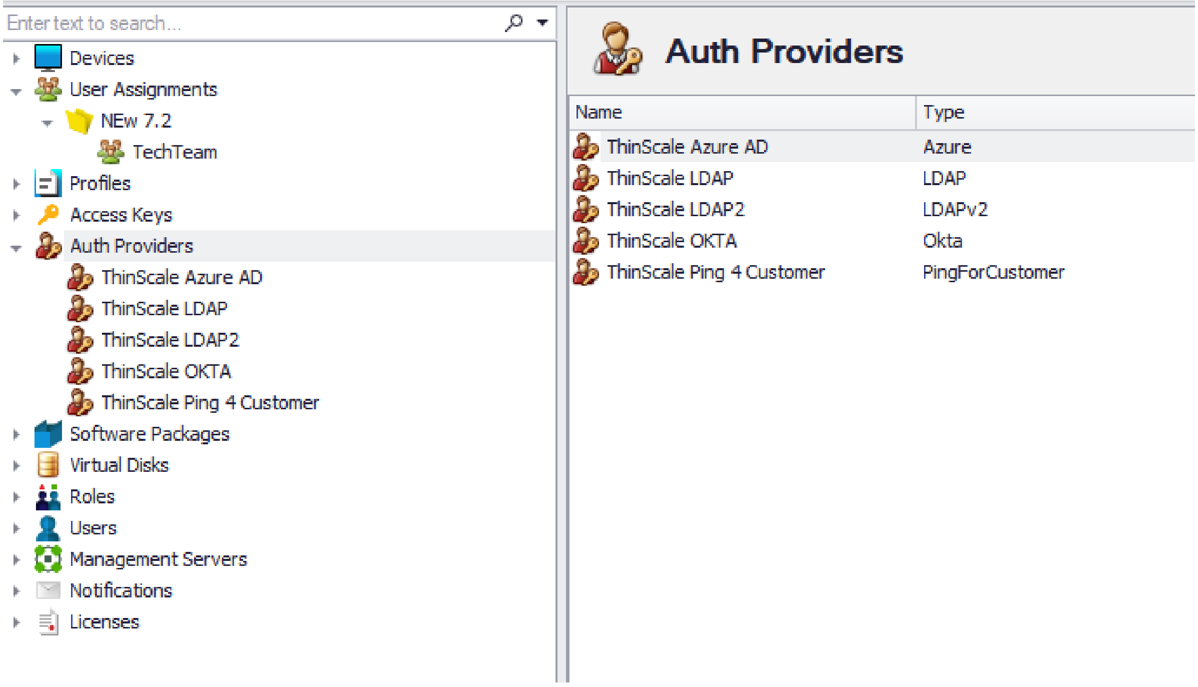
Legacy authentication uses the same username and password authentication that the older Sites feature used.

During the upgrade of your Management Server, all existing Sites will have an Access Key created with legacy authentication enabled and will use the same site username and password meaning there will be no interruption to your existing devices.

When deploying ThinKiosk or Secure Remote Worker V7 we recommend using Access Key authentication instead of the legacy authentication.

13. Authentication Providers

The new Authentication Providers will give the administrator the option to authenticate the console or the agents using SRW/TK machines against one of these Identities, before launching the application. That way the ThinScale Team has added another layer of security whereas a user must fully authenticate against an Azure AD, Ping Authentication or OKTA to fully launch SRW or TK.

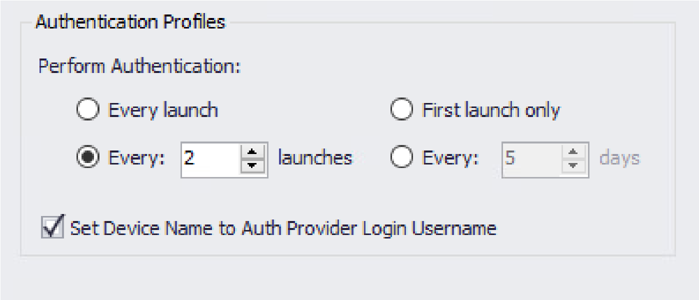


Auth Providers

Name	Type
ThinScale Azure AD	Azure
ThinScale LDAP	LDAP
ThinScale LDAP2	LDAPv2
ThinScale OKTA	Okta
ThinScale Ping 4 Customer	PingForCustomer

Additionally, the admin can use the below option to rename the device which authenticates with one of the below Providers, inside the management console.

Note: rename a device using Ping is currently not supported



Authentication Profiles

Perform Authentication:

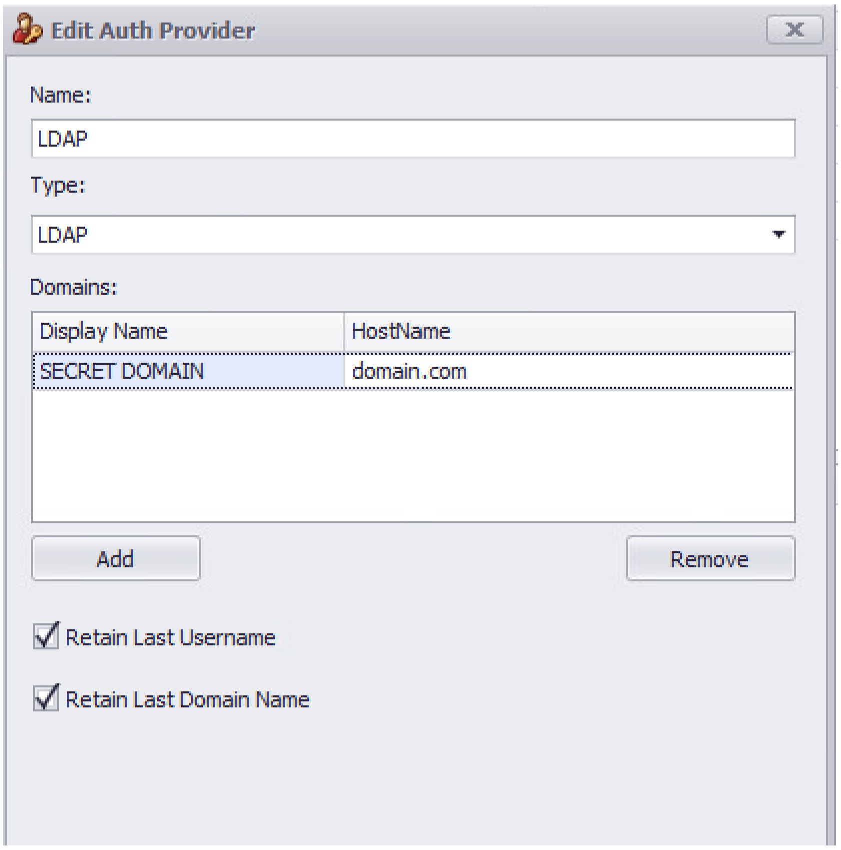
○ Every launch ○ First launch only

● Every: 2 launches ○ Every: 5 days

☑ Set Device Name to Auth Provider Login Username

Note: ThinScale is not in control of any of the settings in either Azure, Okta or Ping. So please talk with your Administrator for more info.

LDAP



Name:

LDAP

Type:

LDAP

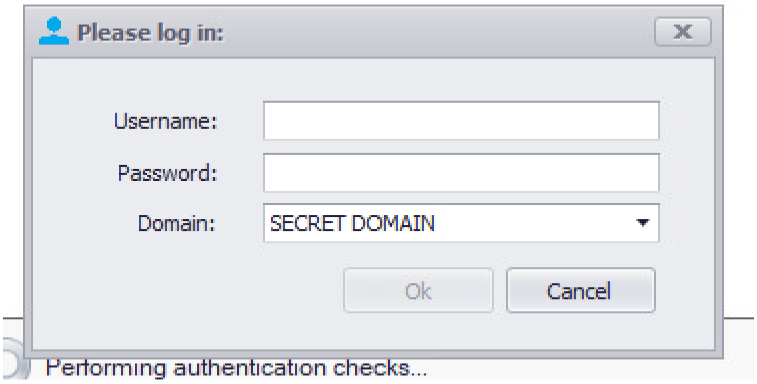
Domains:

Display Name	HostName
SECRET DOMAIN	domain.com

☑ Retain Last Username

☑ Retain Last Domain Name

Display Name: If enabled, the display name is the name that will be displayed on the endpoint. Useful if you want to hide domain name information from the user's view



Username:

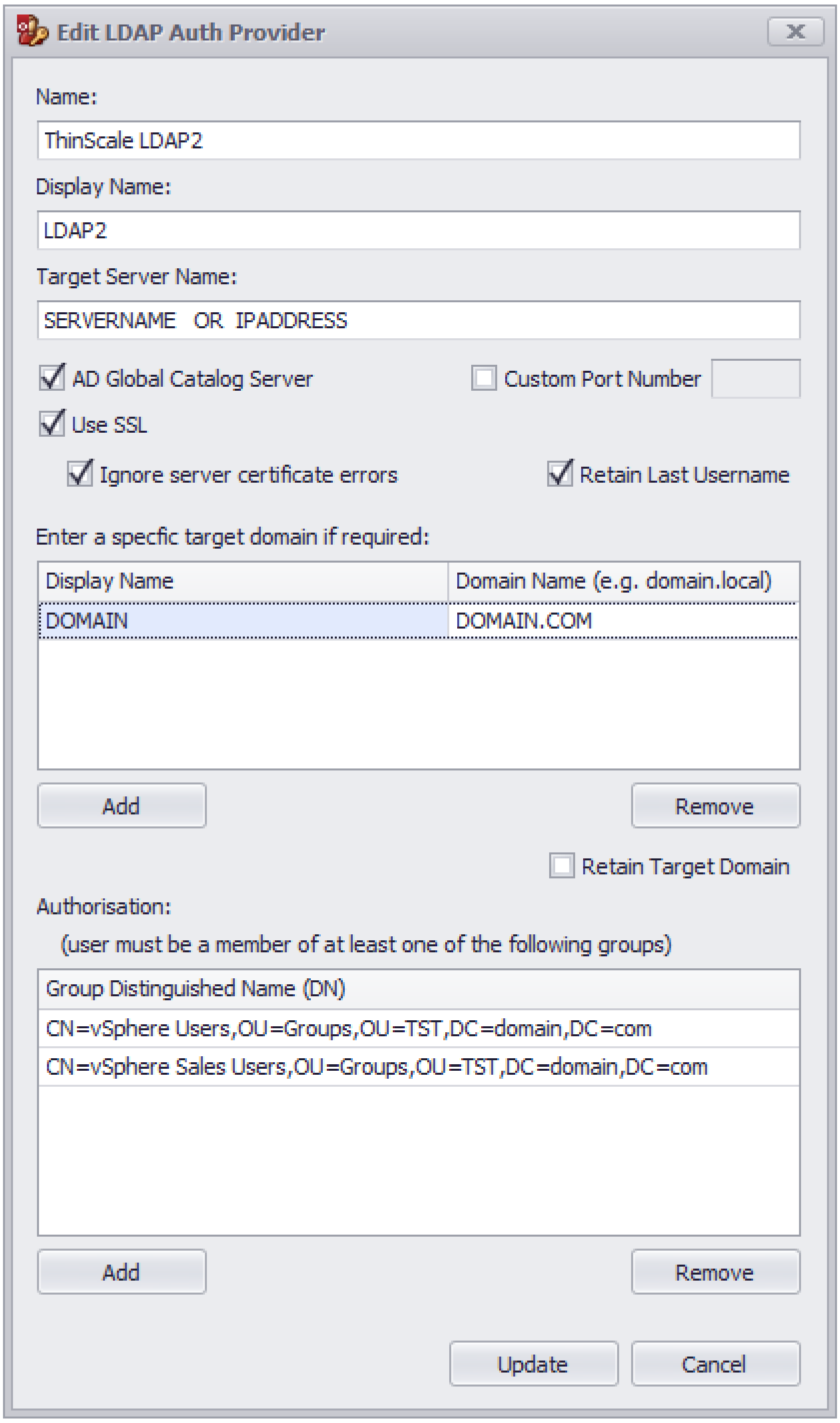
Password:

Domain: SECRET DOMAIN

Performing authentication checks...

The HostName is the actual domain hostname your user will authenticate against.

LDAP V2



Edit LDAP Auth Provider

Name: ThinScale LDAP2

Display Name: LDAP2

Target Server Name: SERVERNAME OR IPADDRESS

☑ AD Global Catalog Server

□ Custom Port Number

☑ Use SSL

☑ Ignore server certificate errors

☑ Retain Last Username

Enter a specfic target domain if required:

Display Name	Domain Name (e.g. domain.local)
DOMAIN	DOMAIN.COM

□ Retain Target Domain

Authorisation:

(user must be a member of at least one of the following groups)

Group Distinguished Name (DN)
CN=vSphere Users,OU=Groups,OU=TST,DC=domain,DC=com
CN=vSphere Sales Users,OU=Groups,OU=TST,DC=domain,DC=com

AD Global Catalog Server: The global catalog is a feature of AD domain controllers that allow for a domain controller to provide information on any object in the forest, regardless of whether the object is a member of the domain controller's domain.

Selecting this option forces the LDAP connection to use the default GC port (3268)

Custom Port Number: The port number that will be used when connecting to the target LDAP server.

Use SSL: if enabled, LDAP/S will be used

Retain Last Username: if enabled, the username typed in the dialog box will be retained

Target Domains: If your target LDAP server has a connection to multiple domains (child domains, forests etc.) they can be added as target domains to force authentication to a specific domain.

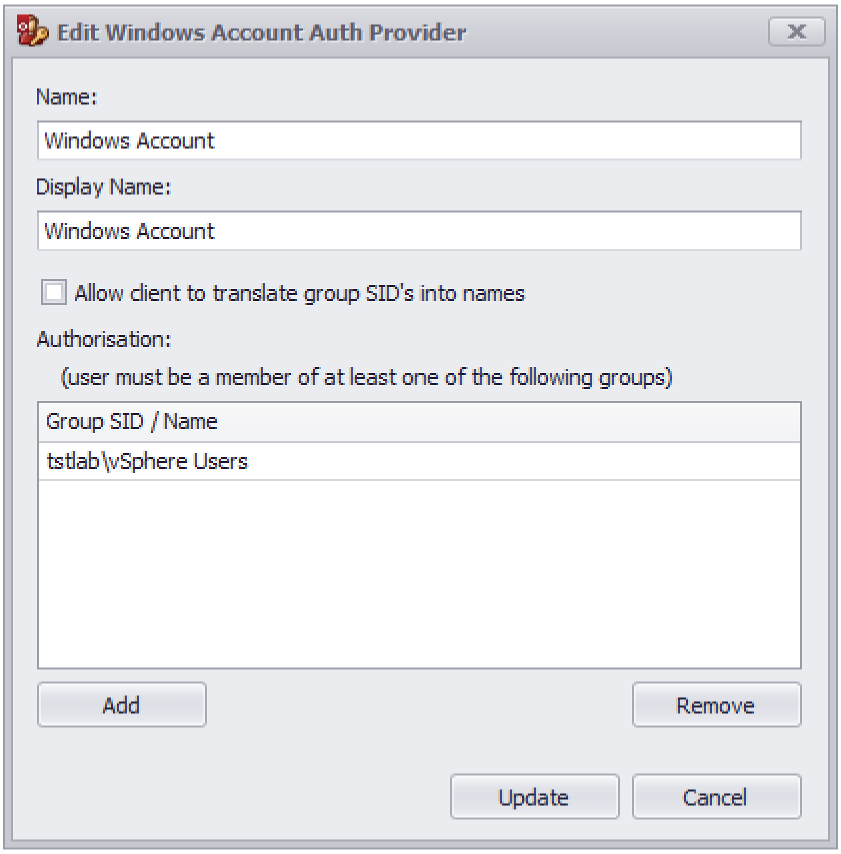
> **Display Name**: The name is displayed in the authentication dialog on the client device.
> **Domain Name**: the domain name that is appended to the username during authentication. (e.g., user@domain.com)

Retain Target Domain: if enabled, the last used domain will be retained

Authorisation: Optionally authorise the user by adding one or more LDAP groups.

If a group is included in the configuration, any authenticating user must be a member of at least one of the groups specified in the list to complete the authentication.

Windows Account



Name: Windows Account

Display Name: Windows Account

□ Allow client to translate group SID's into names

Authorisation:
(user must be a member of at least one of the following groups)

Group SID / Name
tstlab\vSphere Users

Azure, Ping, and Okta

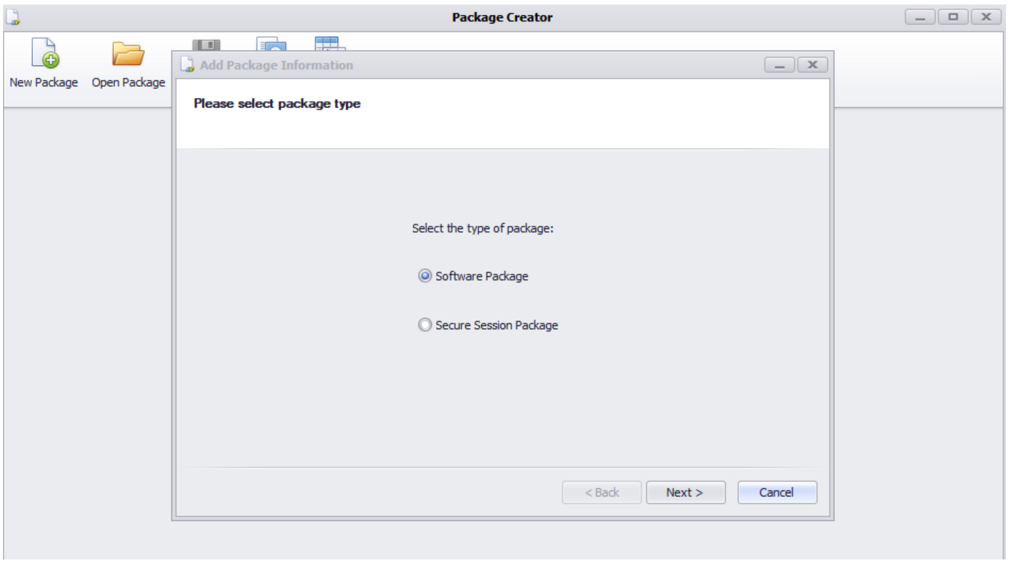
For the Azure, Ping and Okta Auth Provider please look at the KB articles with detailed step by step on how to configure them.

14. Software Packages

Software Packages can be deployed and installed on your devices. To create a software package, you can use the Package Creator tool.

Package Creator

The package creator tool will create a local zip file containing all the necessary installation files and metadata. This zip file can then be added to the Console at any time.

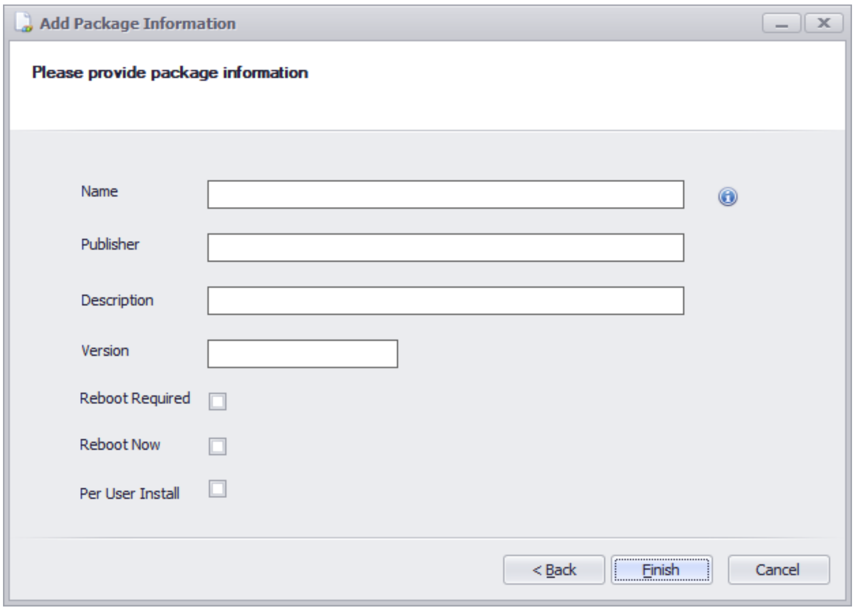


Please select package type

Select the type of package:

● Software Package

○ Secure Session Package



Please provide package information

Name

Publisher

Description

Version

Reboot Required ☐

Reboot Now ☐

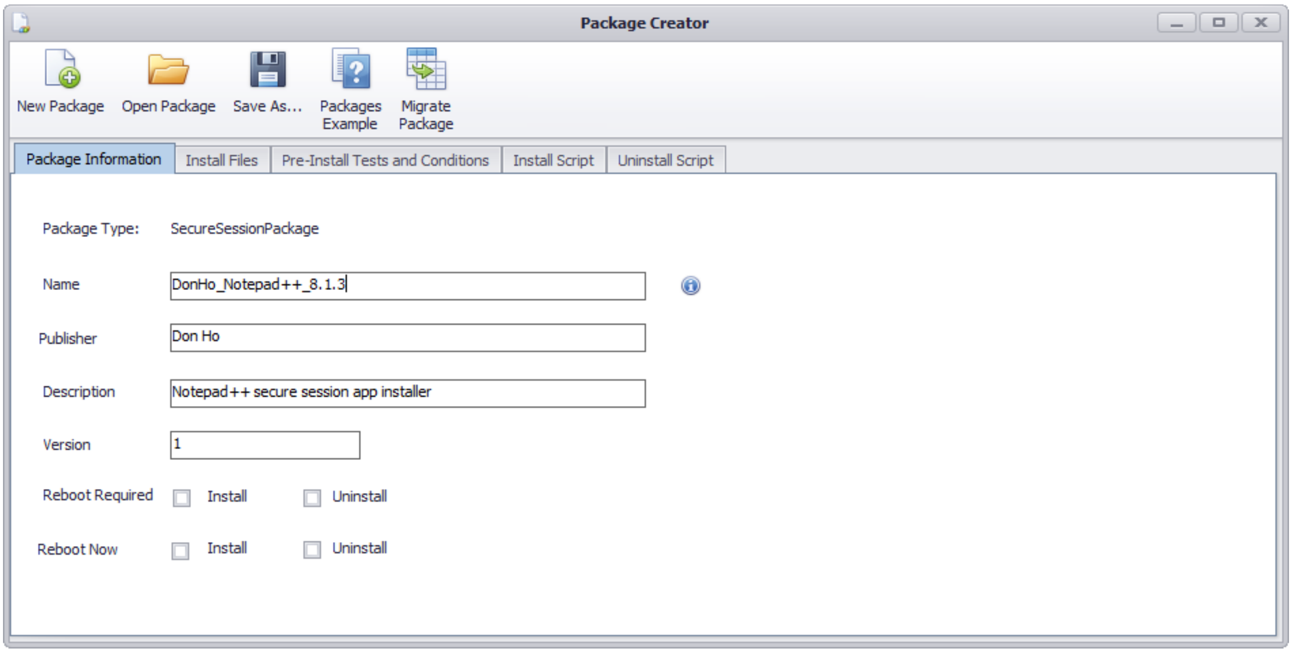
Per User Install ☐

Software Package

These are normal Software Packages that are deployed on the user's PC.

Secure Session Package (v8.0 Only)

These are the new Secure Session Packages that are deployed on the user's PC but inside a BitLocker Protected VHDx only inside the SRW session.



Package Type: SecureSessionPackage

Name: DonHo_Notepad++_8.1.3

Publisher: Don Ho

Description: Notepad++ secure session app installer

Version: 1

Reboot Required □ Install □ Uninstall

Reboot Now □ Install □ Uninstall

Name

Name of the package that will be displayed in the Management Console

Publisher

Name of the package publisher that will be displayed in the Management Console

Description

Description of the package that will be displayed in the Management Console

Version

A version of the package that will be displayed in the Management Console

Reboot Required

If enabled, the PC will reboot at the end of the installation

Reboot Now

If enabled, the PC will reboot as soon as the package is installed

Per User Install

If enabled, the package will be installed only on the SRW session

Install Files

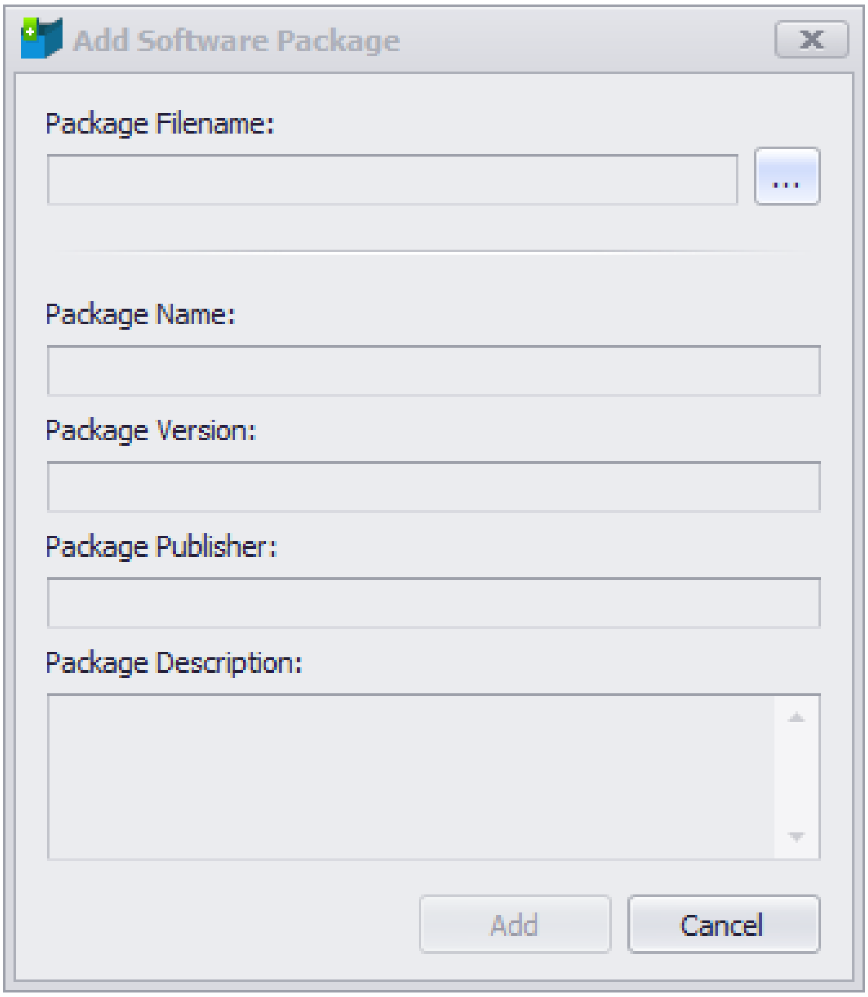
Install files are files that will be added to your package ZIP file and deployed when the package is installed.

The list must contain every file required by the package installation VB script.

- To add new files right click on the list view to bring up an Add/Edit/Remove context menu.
- The pre-install tests are **optional**. If you don't enter any the Install VBS script will run by default on the device. If you enter any pre-install tests, these will be evaluated on the device to see if the condition is met, if it is then the Install VBS script will run.
- You can create and manage packages separately from the Console. Whenever you are ready to add it, please follow the next steps.

Adding a new software package

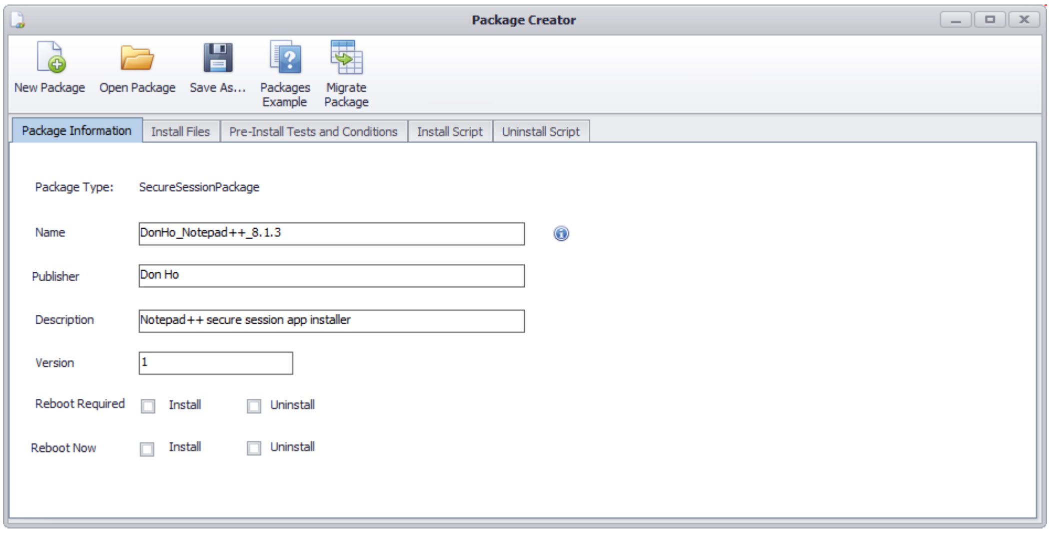
To add a new Software Package, browse to the location of the package from the **Add Software Package** dialog and click **Add**.



Once the package has been added to deploy to your Devices:

1. Select the device folder that contains the devices you wish to deploy the Software Package.
2. Click the **Software Packages** tab.
3. Click the **Assign Package** button from the ribbon bar or the right-click context menu.
4. Select the package and click OK. The package will be applied to the devices on their next login.

Example Notepad Secure Session Package



Package Type: SecureSessionPackage

Name: DonHo_Notepad++_8.1.3

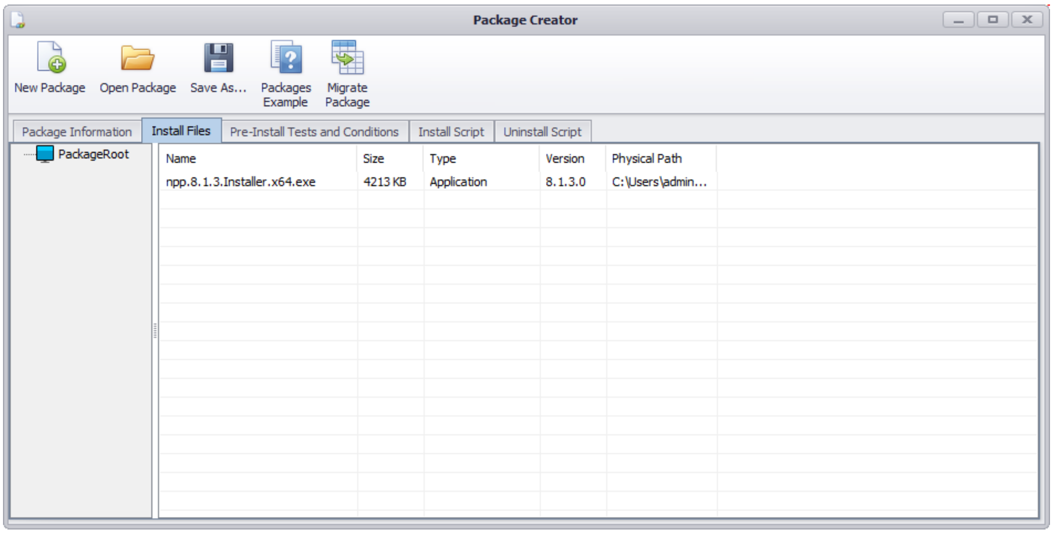
Publisher: Don Ho

Description: Notepad++ secure session app installer

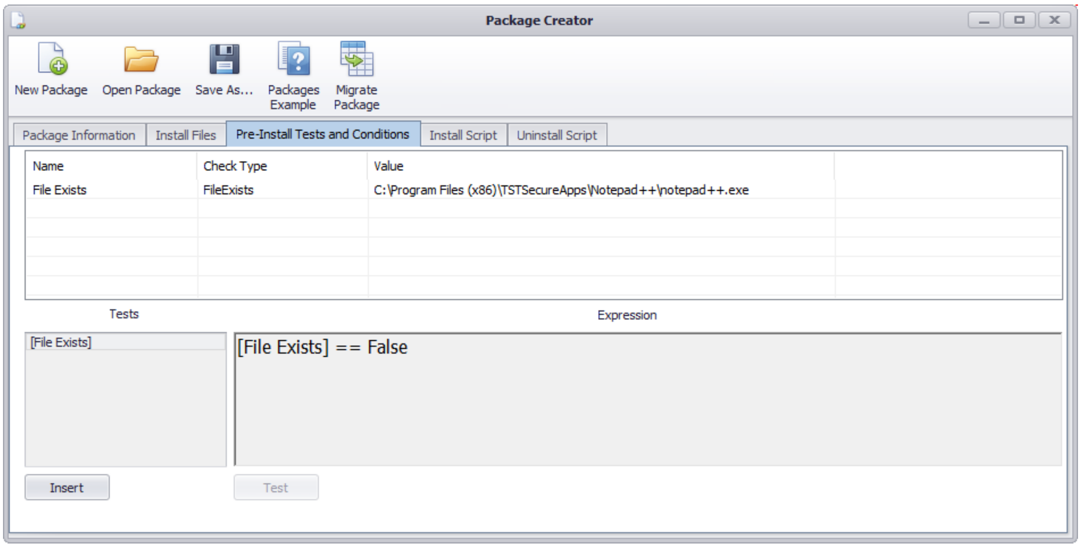
Version: 1

Reboot Required □ Install □ Uninstall

Reboot Now □ Install □ Uninstall



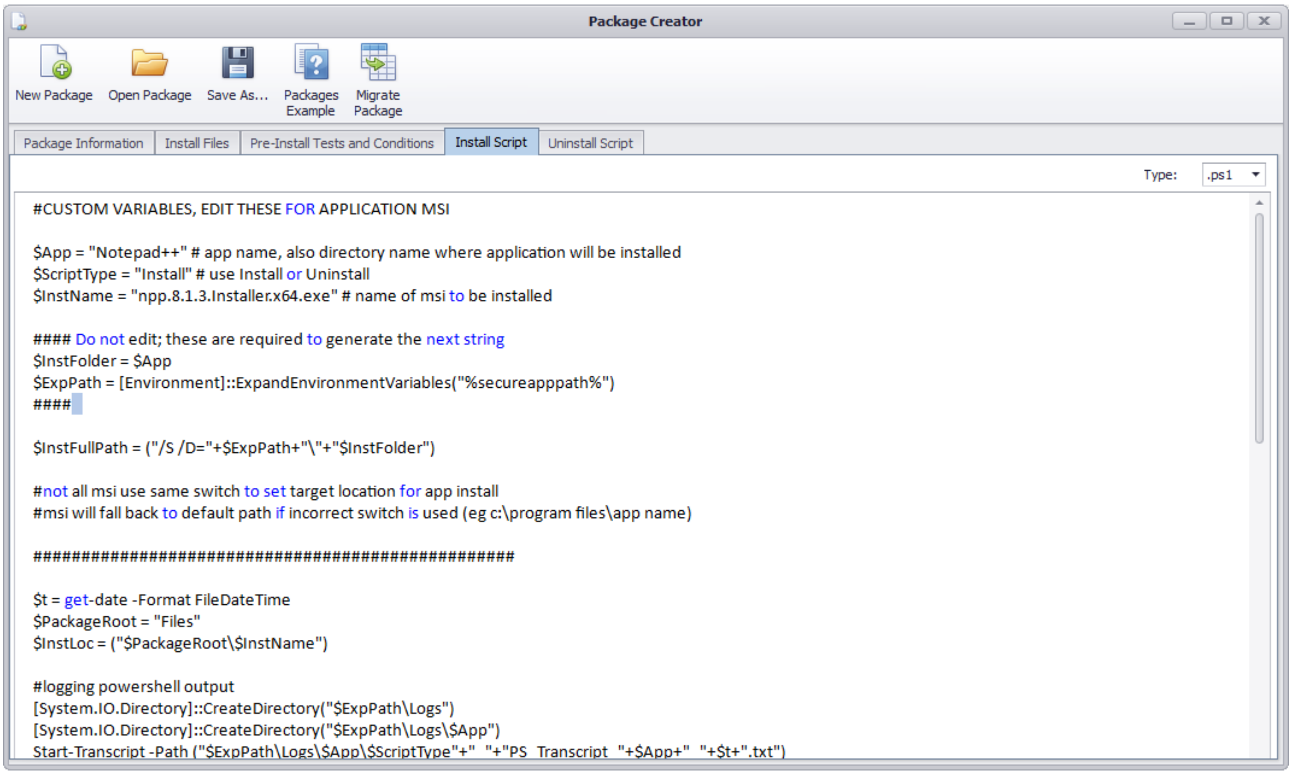
Name	Size	Type	Version	Physical Path
npp.8.1.3.Installer.x64.exe	4213 KB	Application	8.1.3.0	C:\Users\admin...



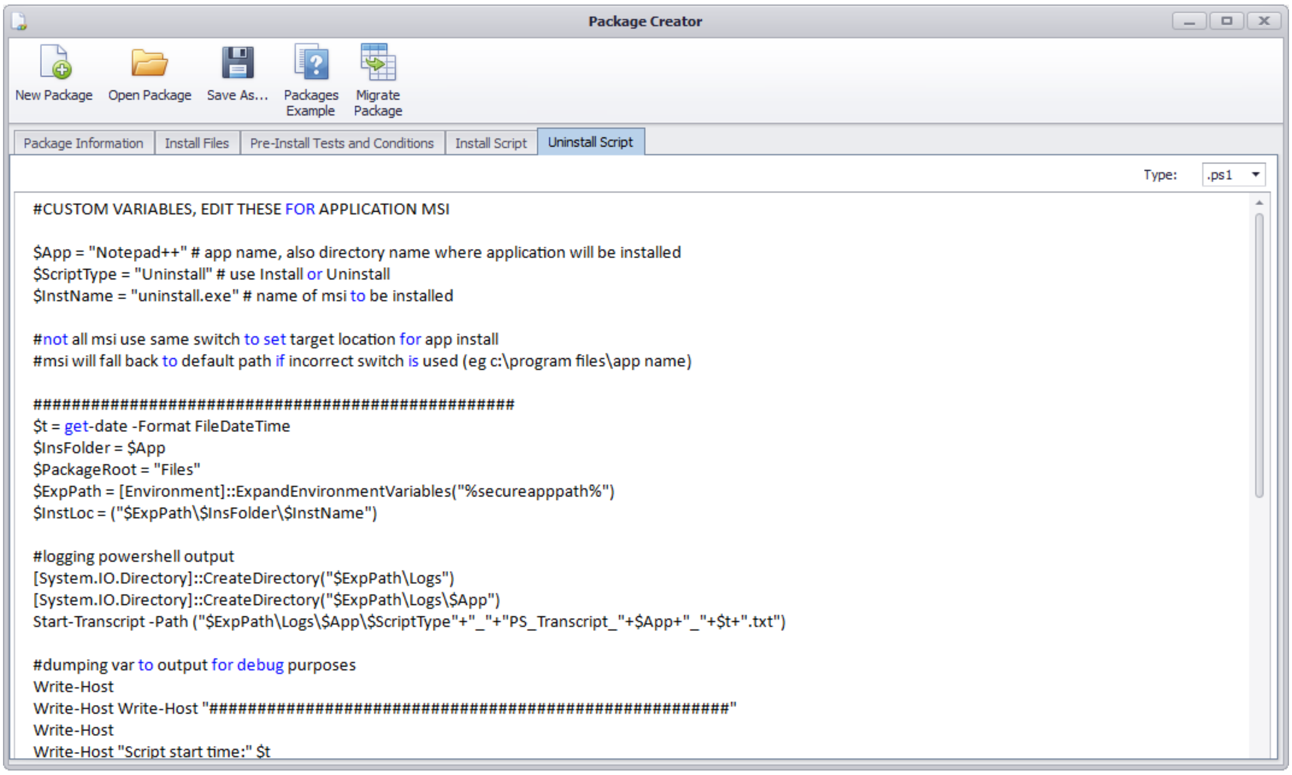
Name	Check Type	Value
File Exists	FileExists	C:\Program Files (x86)\TSTSecureApps\Notepad++\notepad++.exe

Tests: [File Exists]

Expression: [File Exists] == False



```
#CUSTOM VARIABLES, EDIT THESE FOR APPLICATION MSI

$App = "Notepad++" # app name, also directory name where application will be installed
$ScriptType = "Install" # use Install or Uninstall
$InstName = "npp.8.1.3.Installer.x64.exe" # name of msi to be installed

#### Do not edit; these are required to generate the next string
$InstFolder = $App
$ExpPath = [Environment]::ExpandEnvironmentVariables("%secureapppath%")
####

$InstFullPath = ("/S /D="+$ExpPath+"\"+"$InstFolder")

#not all msi use same switch to set target location for app install
#msi will fall back to default path if incorrect switch is used (eg c:\program files\app name)

##################################################

$t = get-date -Format FileDateTime
$PackageRoot = "Files"
$InstLoc = ("$PackageRoot\$InstName")

#logging powershell output
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs")
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs\$App")
Start-Transcript -Path ("$ExpPath\Logs\$App\$ScriptType"+"_"+"PS_Transcript_"+$App+"_"+$t+".txt")
```



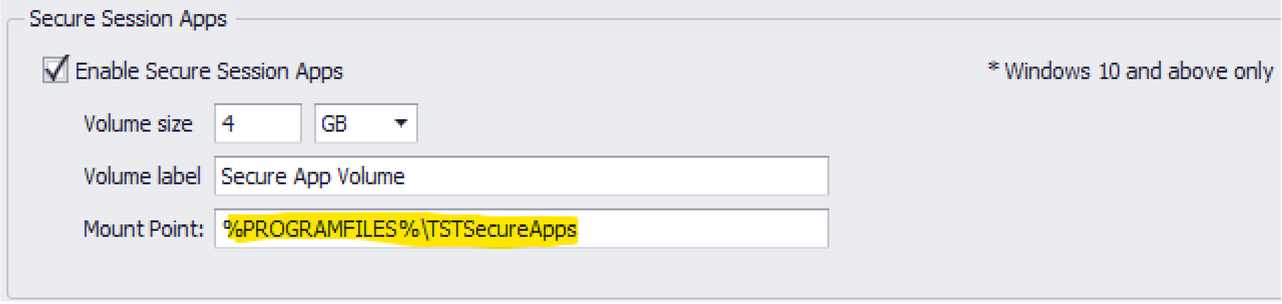
```
#CUSTOM VARIABLES, EDIT THESE FOR APPLICATION MSI

$App = "Notepad++" # app name, also directory name where application will be installed
$ScriptType = "Uninstall" # use Install or Uninstall
$InstName = "uninstall.exe" # name of msi to be installed

#not all msi use same switch to set target location for app install
#msi will fall back to default path if incorrect switch is used (eg c:\program files\app name)

##################################################
$t = get-date -Format FileDateTime
$InsFolder = $App
$PackageRoot = "Files"
$ExpPath = [Environment]::ExpandEnvironmentVariables("%secureapppath%")
$InstLoc = ("$ExpPath\$InsFolder\$InstName")

#logging powershell output
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs")
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs\$App")
Start-Transcript -Path ("$ExpPath\Logs\$App\$ScriptType"+"_"+"PS_Transcript_"+$App+"_"+$t+".txt")

#dumping var to output for debug purposes
Write-Host
Write-Host Write-Host "##########################################################"
Write-Host
Write-Host "Script start time:" $t
```

INSTALL SCRIPT PS1

```
#CUSTOM VARIABLES, EDIT THESE FOR APPLICATION MSI

$App = "Notepad++" # app name, also directory name where the application will be installed
$ScriptType = "Install" # use Install or Uninstall
$InstName = "npp.8.1.3.Installer.x64.exe" # name of msi to be installed

#### Do not edit; these are required to generate the next string
$InstFolder = $App
$ExpPath = [Environment]::ExpandEnvironmentVariables("%secureapppath%")
####

$InstFullPath = ("/S /D="+$ExpPath+"\"+"$InstFolder")

#not all msi use the same switch to set the target location for app install
#msi will fall back to the default path if an incorrect switch is used (e.g. c:\program files\app name)

##################################################

$t = get-date -Format FileDateTime
$PackageRoot = "Files"
$InstLoc = ("$PackageRoot\$InstName")

#logging PowerShell output
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs")
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs\$App")
Start-Transcript -Path ("$ExpPath\Logs\$App\$ScriptType"+"_"+"PS_Transcript_"+$App+"_"+$t+".txt")

#dumping var to output for debug purposes
Write-Host
Write-Host
Write-Host "######################################################"
Write-Host
Write-Host "Script start time:" $t
Write-Host "Script type:" $ScriptType
Write-Host "Application to be installed:" $App
Write-Host "Expanded Environment Variable:" $ExpPath
Write-Host "Root directory for the installer:" $PackageRoot
Write-Host "Installer file location:" $InstLoc
Write-Host "Target path for application:" $InsFolder
Write-Host "EXE switch for target path:" $InstFullPath
Write-Host
Write-Host
Write-Host "######################################################"
Write-Host
Write-Host
```

```
#creating install path and MSI_Store (to copy msi locally for debug purposes)
[System.IO.Directory]::CreateDirectory("$ExpPath\$InsFolder")
[System.IO.Directory]::CreateDirectory("$ExpPath\MSI_Store")

#copying MSI to a local path for debug purposes
robocopy /xc /xn /xo $PackageRoot "$ExpPath\MSI_Store" $InstName

Write-Host
Write-Host "######################################################################"
Write-Host
Write-Host "Performing" $ScriptType "of" $InstName "please wait"

#running EXE for the installer
Start-Process -NoNewWindow -Wait -FilePath $InstLoc -ArgumentList "$InstFullPath"

Write-Host
Write-Host "SHORTCUT FOR PROFILE LOCAL APPLICATION:"
Write-Host "$ExpPath\$InsFolder\notepad++.exe"
Write-Host
Write-Host "######################################################################"
Write-Host
Stop-Transcript
Write-Host
Write-Host "######################################################################"
Write-Host
```

The %secureapppath% system variable matches the mount point inside the Profile Editor



Secure Session Apps

☑ Enable Secure Session Apps

* Windows 10 and above only

Volume size: 4 GB

Volume label: Secure App Volume

Mount Point: %PROGRAMFILES%\TSTSecureApps

UNINSTALL SCRIPT PS1

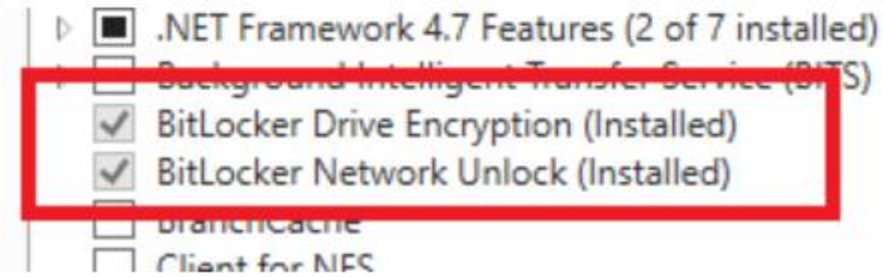
```
#CUSTOM VARIABLES, EDIT THESE FOR APPLICATION MSI

$App = "Notepad++" # app name, also directory name where the application will be installed
$ScriptType = "Uninstall" # use Install or Uninstall
$InstName = "uninstall.exe" # name of msi to be installed

#not all msi use the same switch to set the target location for app install
#msi will fall back to the default path if incorrect switch is used (eg c:\program files\app name)

##########################################################
$t = get-date -Format FileDateTime
$InsFolder = $App
$PackageRoot = "Files"
$ExpPath = [Environment]::ExpandEnvironmentVariables("%secureapppath%")
$InstLoc = ("$ExpPath\$InsFolder\$InstName")

#logging PowerShell output
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs")
[System.IO.Directory]::CreateDirectory("$ExpPath\Logs\$App")
Start-Transcript -Path ("$ExpPath\Logs\$App\$ScriptType"+"_"+"PS_Transcript_"+$App+"_"+$t+".txt")

#dumping var to output for debug purposes
Write-Host
Write-Host Write-Host "###############################################################"
Write-Host
Write-Host "Script start time:" $t
Write-Host "Script type:" $ScriptType
Write-Host "Application to be installed:" $App
Write-Host "Expanded Environment Variable:" $ExpPath
Write-Host "Root directory for installer:" $PackageRoot
Write-Host "Installer file location:" $InstLoc
Write-Host "Target path for application:" $InsFolder
Write-Host
Write-Host Write-Host "###############################################################"
Write-Host
Write-Host

#creating install path and MSI_Store (to copy msi locally for debug purposes)
[System.IO.Directory]::CreateDirectory("$ExpPath\$InsFolder")
[System.IO.Directory]::CreateDirectory("$ExpPath\MSI_Store")

#copying MSI to local path for debug purposes
robocopy /xc /xn /xo $PackageRoot "$ExpPath\MSI_Store" $InstName

Write-Host
Write-Host "###############################################################"
```

```
Write-Host
Write-Host "Performing" $ScriptType "of" $InstName "please wait"

#running uninstaller
Start-Process "$InstLoc" -Wait -ArgumentList "/S"

Write-Host
Write-Host "############################################################"
Write-Host
Stop-Transcript
Write-Host
Write-Host "############################################################"
Write-Host
```

Please check our library of already made package from the ThinScale Portal

15. Virtual Disks

Before you start creating the Disk make sure that your server has these 2 features enabled:



▷ ■ .NET Framework 4.7 Features (2 of 7 installed)

□ Background Intelligent Transfer Service (BITS)

☑ BitLocker Drive Encryption (Installed)

☑ BitLocker Network Unlock (Installed)

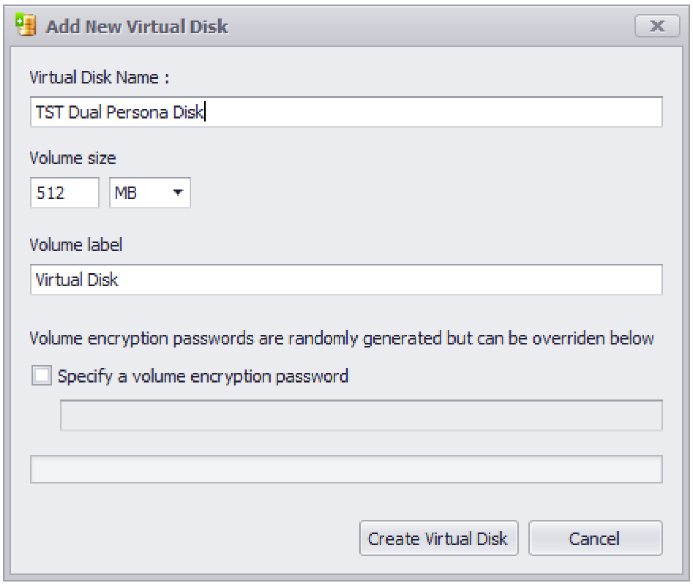
□ BranchCache

□ Client for NFS

Virtual Disks are required by Home Edition Operating Systems when the Dual Persona or Temporary Storage features are enabled in your ThinKiosk or Secure Remote Worker profiles.

The same virtual disk can be assigned to multiple device folders, but a separate disk is required for Dual Persona and Temporary Storage if both technologies are enabled.

Simply create a new virtual disk, select a name, size, volume label and optionally an encryption password



Add New Virtual Disk

Virtual Disk Name : TST Dual Persona Disk

Volume size: 512 MB

Volume label: Virtual Disk

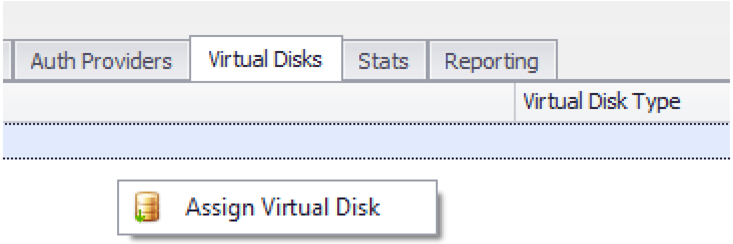
Volume encryption passwords are randomly generated but can be overriden below

□ Specify a volume encryption password

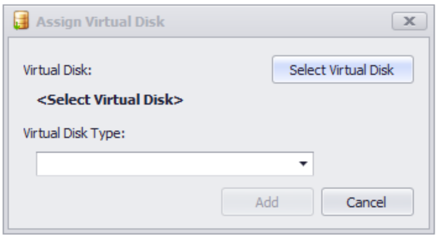
Note: Volume Label must be less or equal to 32 characters.

Assign to the folder where your devices are and select a type

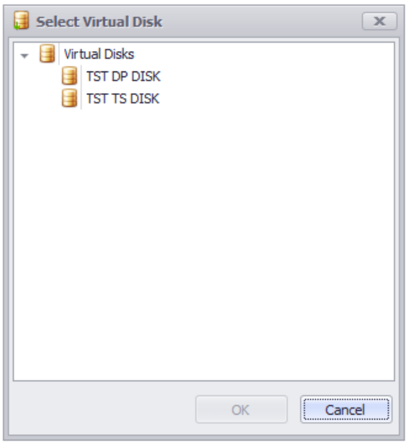
Right-click Assign Virtual Disk

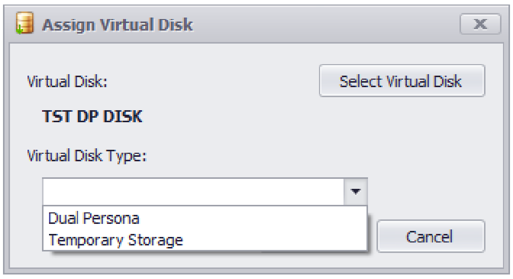


Select the Disk and select the Type

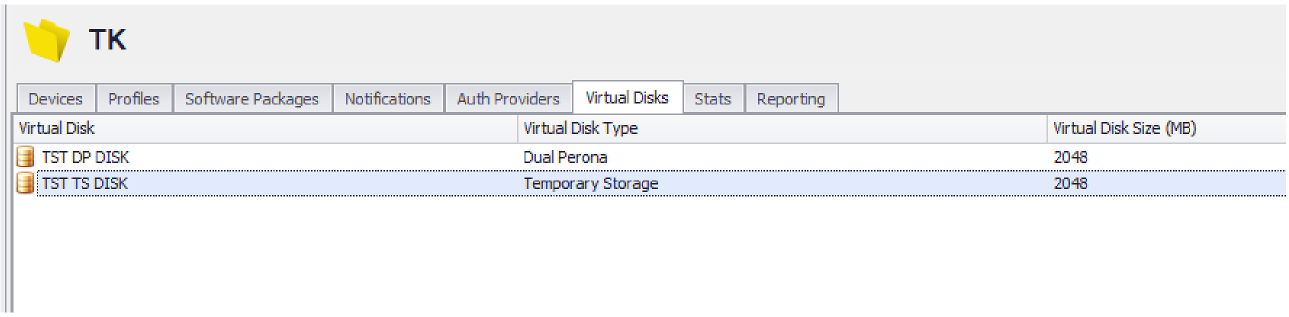


Virtual Disk:
<Select Virtual Disk>
Virtual Disk Type:





Virtual Disk:
TST DP DISK
Virtual Disk Type:

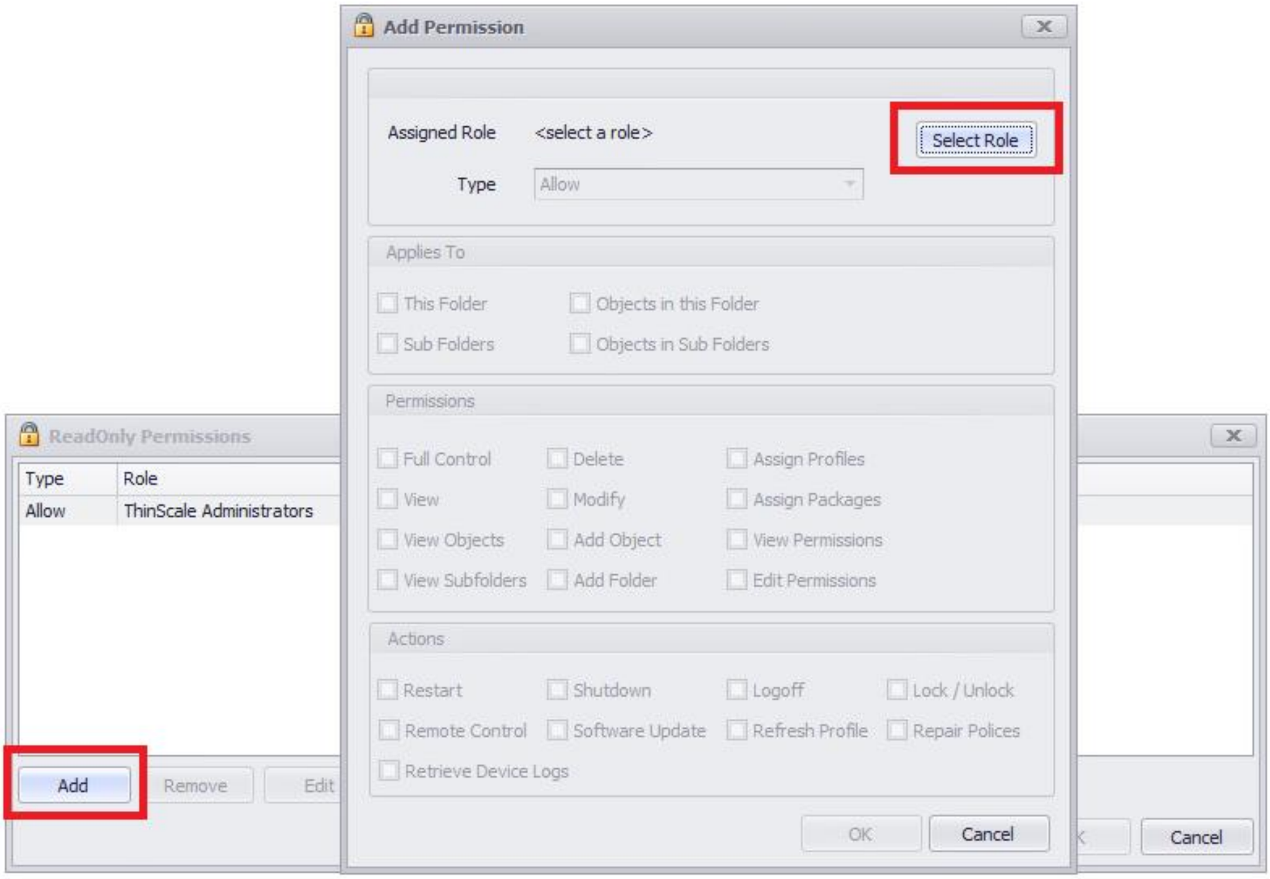


Virtual Disk	Virtual Disk Type	Virtual Disk Size (MB)
TST DP DISK	Dual Perona	2048
TST TS DISK	Temporary Storage	2048

16. Roles

Role's membership determines what access a user has within the Console.
A Role can be used to assign Permissions to any object in the Console (Devices, Profiles, Sites etc.). Once a Role is created it becomes available to use in the Permissions dialog.

Note: A Role relates to Management Console access only.



Add Permission

Assigned Role <select a role>

Type: Allow

Applies To

□ This Folder □ Objects in this Folder
□ Sub Folders □ Objects in Sub Folders

Permissions

□ Full Control □ Delete □ Assign Profiles
□ View □ Modify □ Assign Packages
□ View Objects □ Add Object □ View Permissions
□ View Subfolders □ Add Folder □ Edit Permissions

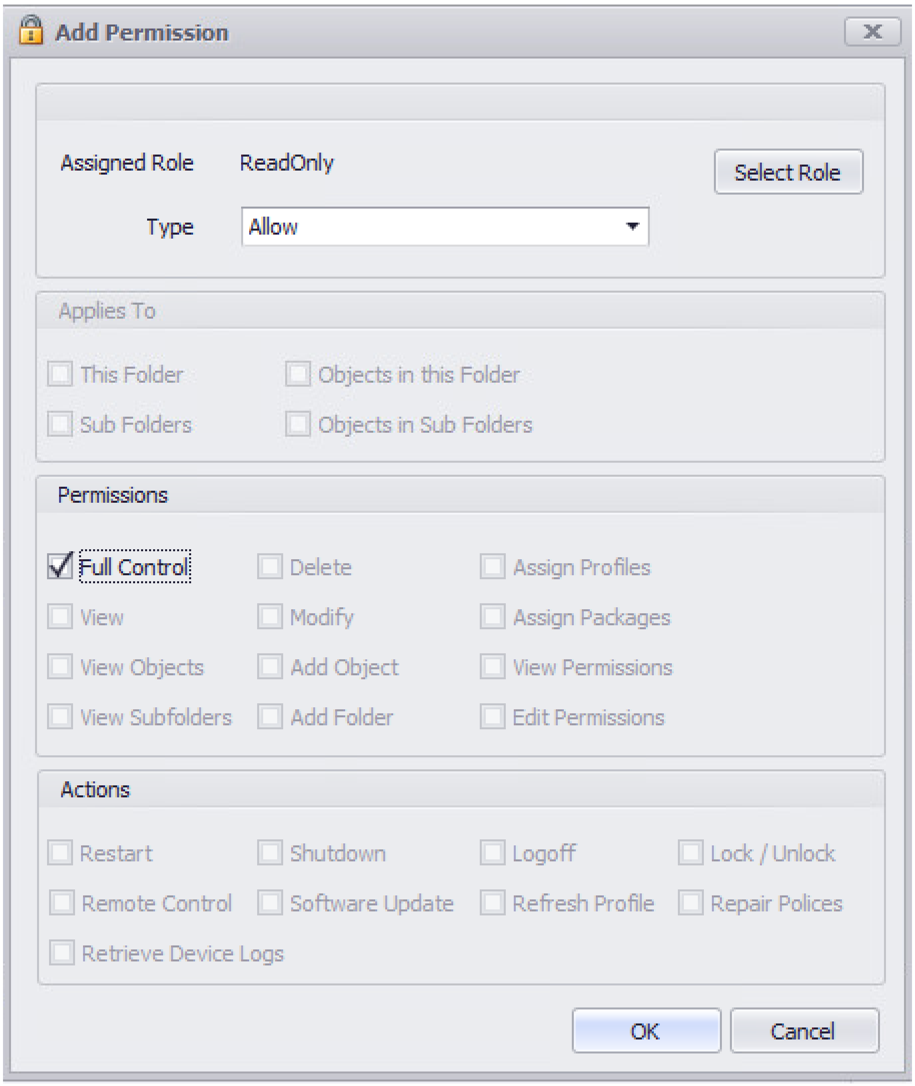
Actions

□ Restart □ Shutdown □ Logoff □ Lock / Unlock
□ Remote Control □ Software Update □ Refresh Profile □ Repair Polices
□ Retrieve Device Logs

ReadOnly Permissions

Type	Role
Allow	ThinScale Administrators

Selecting a Role then allows Permissions to be set. In the example below the Role only has View Permissions:



Assigned Role ReadOnly

Type Allow

Applies To

□ This Folder □ Objects in this Folder

□ Sub Folders □ Objects in Sub Folders

Permissions

☑ Full Control □ Delete □ Assign Profiles

□ View □ Modify □ Assign Packages

□ View Objects □ Add Object □ View Permissions

□ View Subfolders □ Add Folder □ Edit Permissions

Actions

□ Restart □ Shutdown □ Logoff □ Lock / Unlock

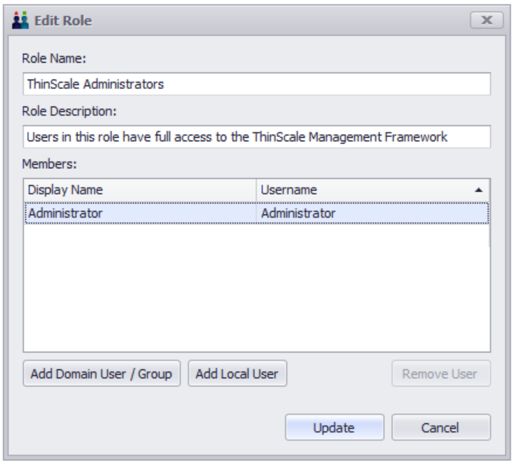
□ Remote Control □ Software Update □ Refresh Profile □ Repair Polices

□ Retrieve Device Logs

Domain Account Roles

To create a Domain account, firstly log in with the auto-created “Administrator” account, then within the Roles section, you can either edit the Administrator role by right-clicking “Edit Roles” or add a new one.

- If you Edit the Administrator role a dialog box will open. Select Add Domain User/ Group and add the domain account you want to use to authenticate.



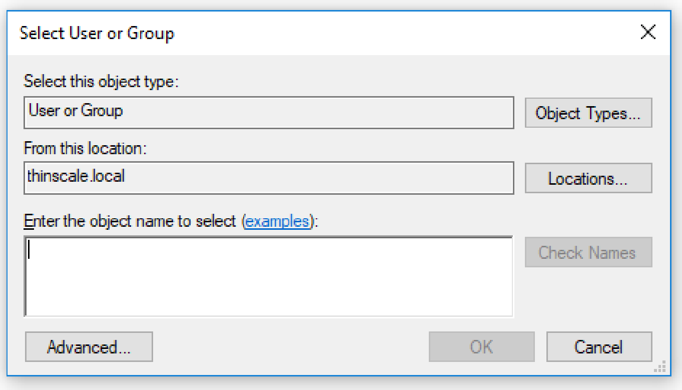
Edit Role

Role Name:
ThinScale Administrators

Role Description:
Users in this role have full access to the ThinScale Management Framework

Members:

Display Name	Username
Administrator	Administrator



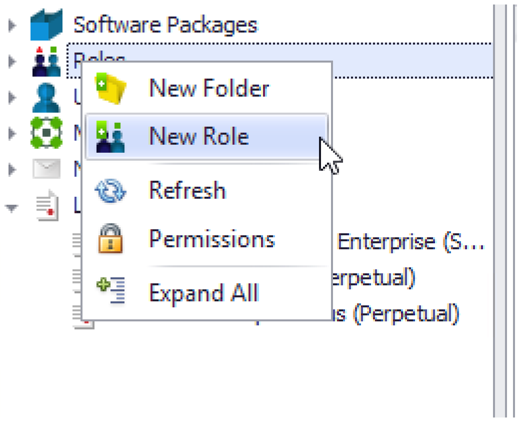
Select User or Group

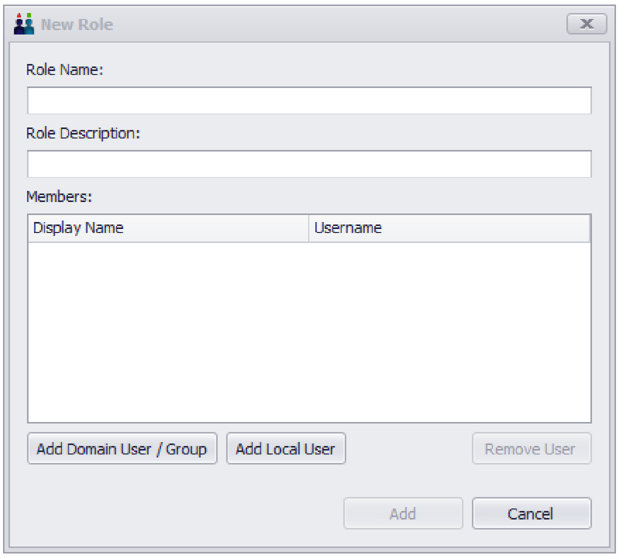
Select this object type:
User or Group

From this location:
thinscale.local

Enter the object name to select (examples):

- If you create a new role, right click on the Roles icon and select “New Role”, specify a role name, and a description and then add the domain account as in the previous step.





New Role

Role Name:

Role Description:

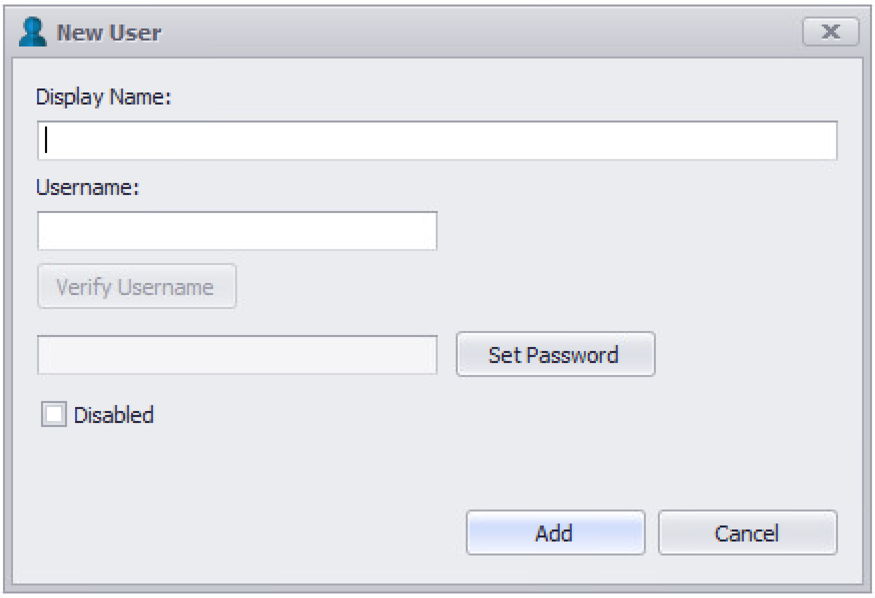
Members:

Display Name	Username

17. Users

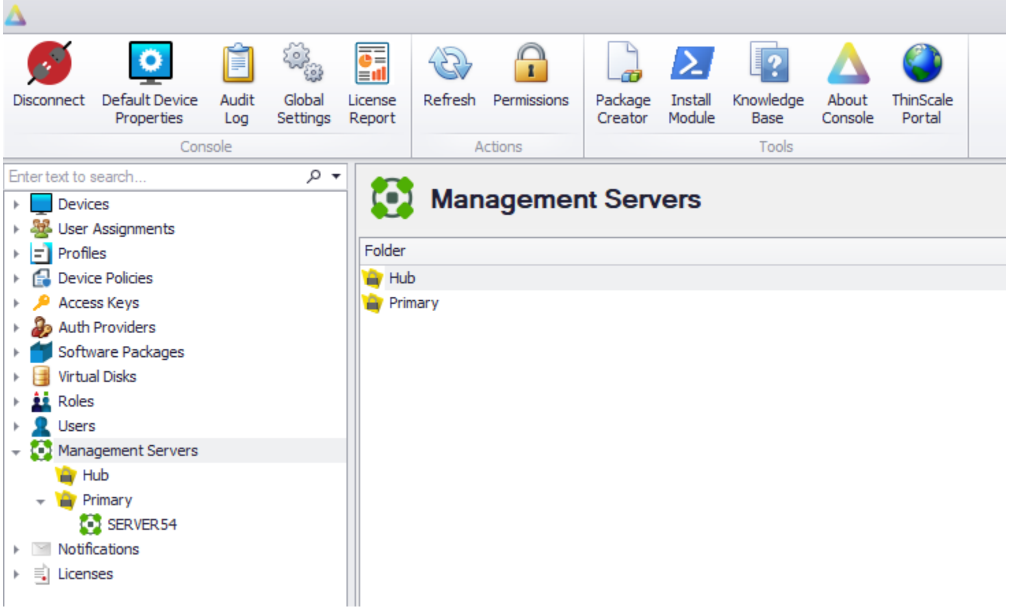
A User can be assigned to any number of Role(s). It is the Role that gives the User permissions to certain objects (Devices, Profiles etc.).

Note: A User relates to Management Console access only.



18. Management Servers

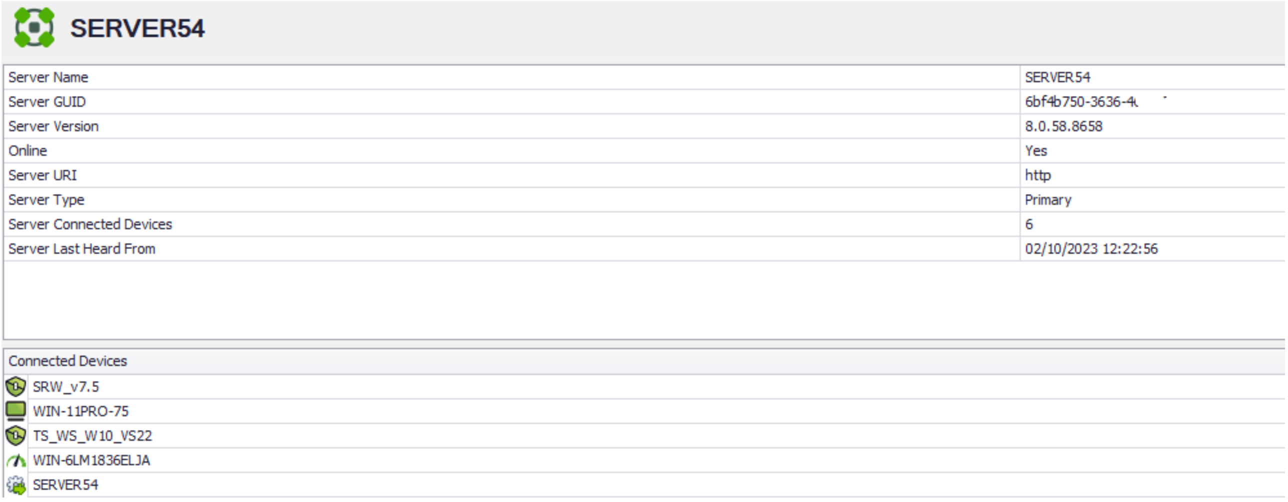
Management Servers that have been deployed will appear here. They are split into two folders by server type: primary and hub. To understand the differences between primary and hub servers please refer to **Management Server Deployment Types** in the **ThinScale Management Server 8.0.x Admin Guide** document.



Management Servers

Folder
Hub
Primary

Selecting a Management Server will show some information about the server, such as the version it is running, and a list of connected devices:



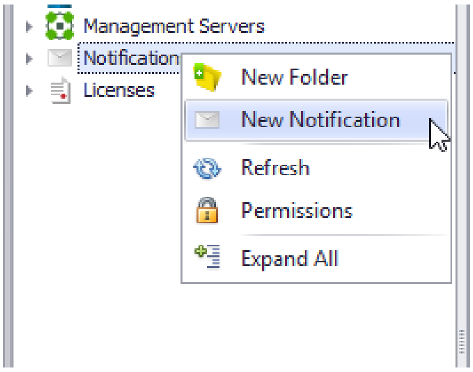
SERVER54

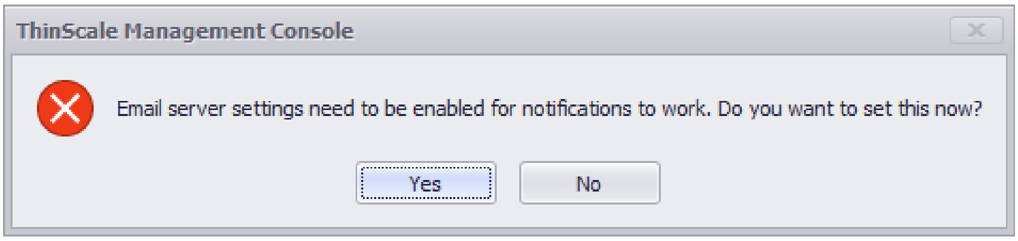
Server Name	SERVER54
Server GUID	6bf4b750-3636-4
Server Version	8.0.58.8658
Online	Yes
Server URI	http
Server Type	Primary
Server Connected Devices	6
Server Last Heard From	02/10/2023 12:22:56

Connected Devices
SRW_v7.5
WIN-11PRO-75
TS_WS_W10_VS22
WIN-6LM1836ELJA
SERVER54

19. Notifications

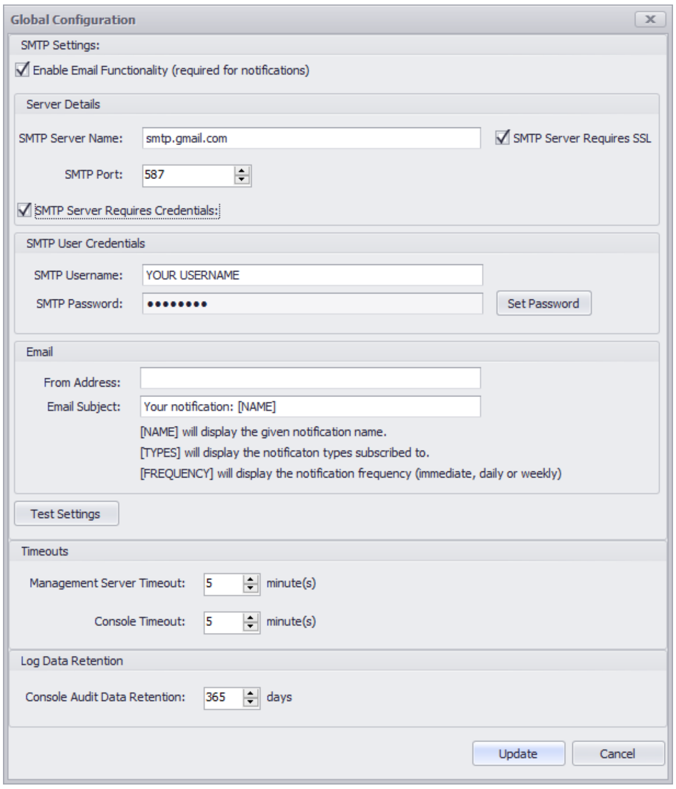
Click “**New Notification**” to open the notification dialog box. If the SMTP server settings were not enabled a message box will be shown.




ThinScale Management Console

Email server settings need to be enabled for notifications to work. Do you want to set this now?

If yes is selected the Global Configuration dialog box will appear.


Global Configuration

SMTP Settings:

☑ Enable Email Functionality (required for notifications)

Server Details

SMTP Server Name: smtp.gmail.com ☑ SMTP Server Requires SSL

SMTP Port: 587

☑ SMTP Server Requires Credentials:

SMTP User Credentials

SMTP Username: YOUR USERNAME

SMTP Password: •••••••• Set Password

Email

From Address:

Email Subject: Your notification: [NAME]

[NAME] will display the given notification name.
[TYPES] will display the notificaton types subscribed to.
[FREQUENCY] will display the notification frequency (immediate, daily or weekly)

Test Settings

Timeouts

Management Server Timeout: 5 minute(s)

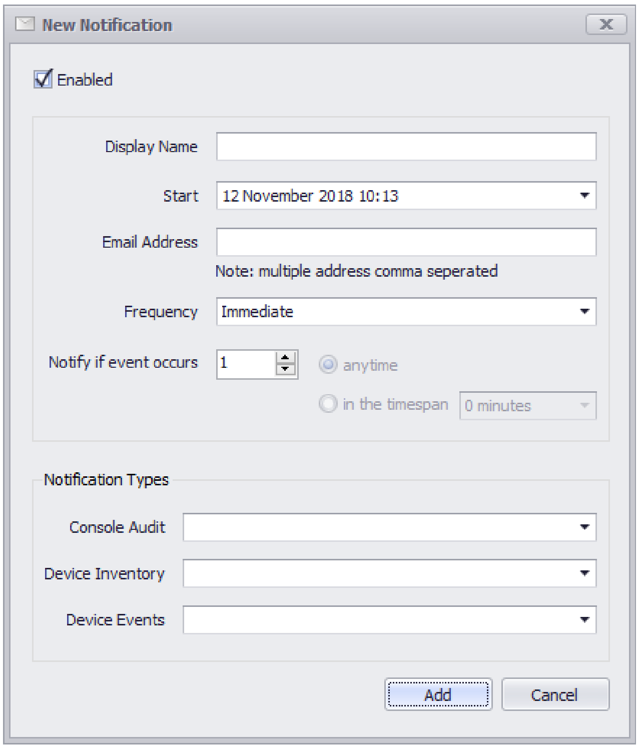
Console Timeout: 5 minute(s)

Log Data Retention

Console Audit Data Retention: 365 days

Update Cancel

If the settings have been tested and the notification email has been received, you can start adding new Notifications inside the Management Console.



☑ Enabled

Display Name:

Start: 12 November 2018 10:13

Email Address:

Note: multiple address comma seperated

Frequency: Immediate

Notify if event occurs: 1 ● anytime ○ in the timespan 0 minutes

Notification Types

Console Audit:

Device Inventory:

Device Events:

Display Name

The Notification's name will show in the email Title

Start

The starting date when the notification will commence is to be sent.

Email Address

The email address where the Notifications will be sent out. Multiple emails can be used.

Frequency

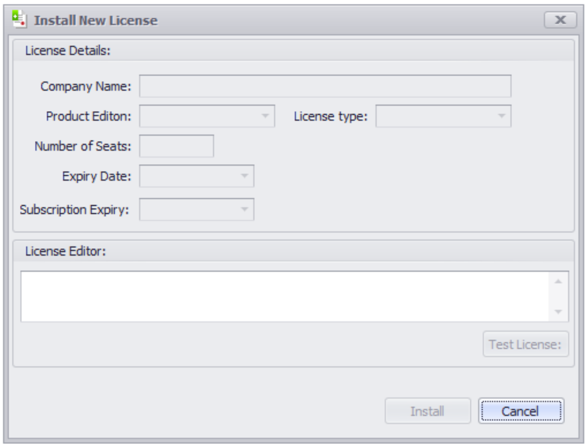
It represents how often the Notifications will be sent out. Choose between Immediate, Daily and Weekly
Additionally, you can choose to be notified at any time or in a specific period if the event occurs once or multiple times.

Notification Types

Choose between Console Audit, Device Inventory, Device Events or all of them together.

20. Licensing

Click the **Install License** button to open the licensing dialog. By default, the ThinKiosk Management Server service will register a 30-day trial.



Install New License

License Details:

Company Name:

Product Editon: License type:

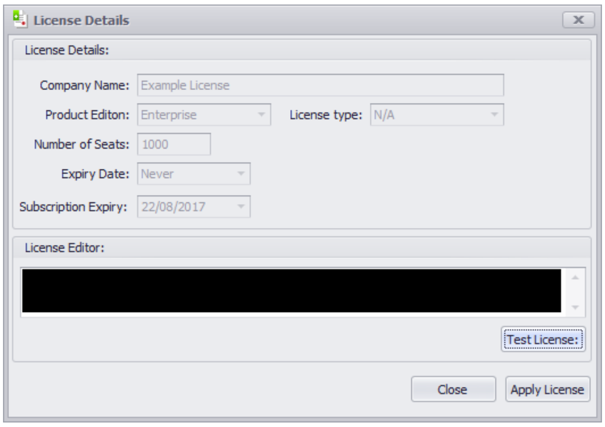
Number of Seats:

Expiry Date:

Subscription Expiry:

License Editor:

To update this trial, simply paste the license key received from sales@thinscaletechnology.com into the license editor then click test license.



License Details

License Details:

Company Name: Example License

Product Editon: Enterprise License type: N/A

Number of Seats: 1000

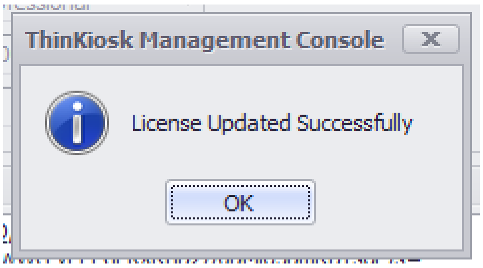
Expiry Date: Never

Subscription Expiry: 22/08/2017

License Editor:

[redacted]

Assuming the license is ok, click Apply License to send the license to the server.



ThinKiosk Management Console

License Updated Successfully

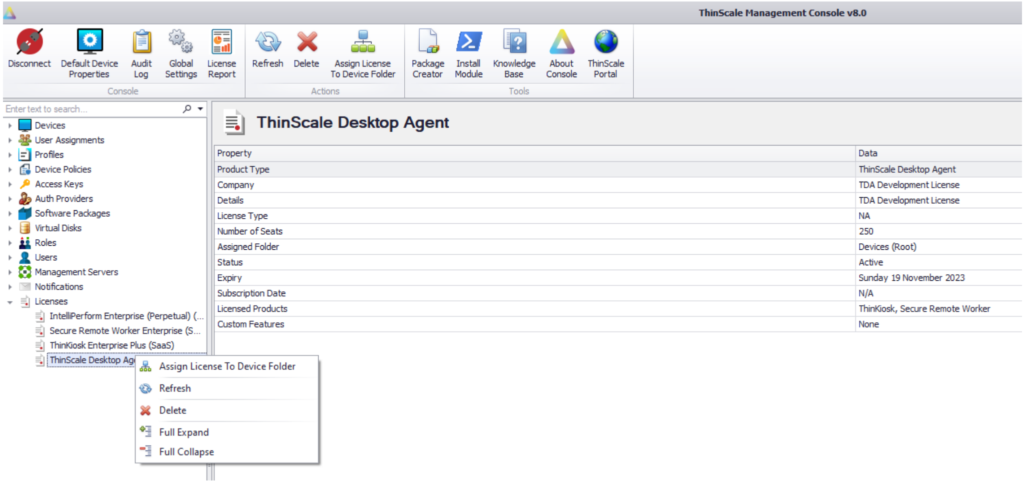
Note: When a ThinKiosk device checks into the Broker service, a copy of this license key is stored in the registry on the device.

Assign the License to a device folder

From version 1.2 of the Management Console, you can install multiple ThinKiosk or IntelliPerform licenses. Different licenses can be applied to all or a subset of devices by assigning a license to either the root Device Folder or a specific device folder.

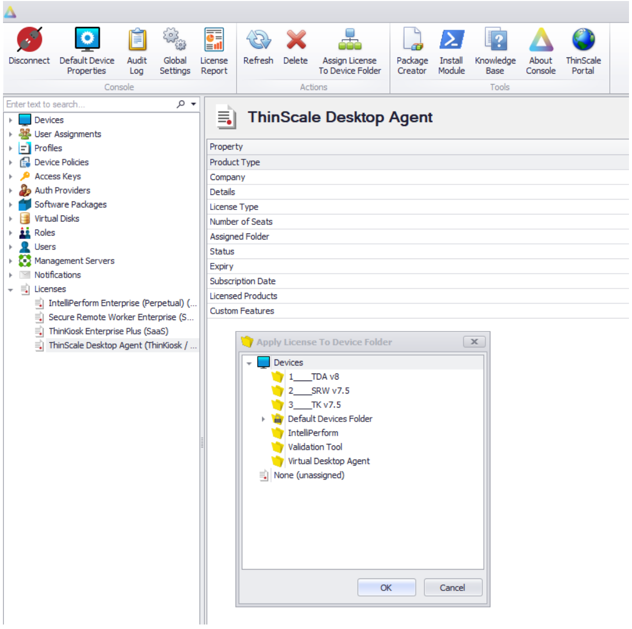
Once a license has been installed, by right-clicking on it or by using the “Assign License to Device folder” option from the Ribbon Bar, you will be able to assign the license to a specific device folder.

By assigning a license to a folder it will license the entire folder branch. Assigning the device to the top-level Devices folder will assign the license to all your devices.



ThinScale Desktop Agent

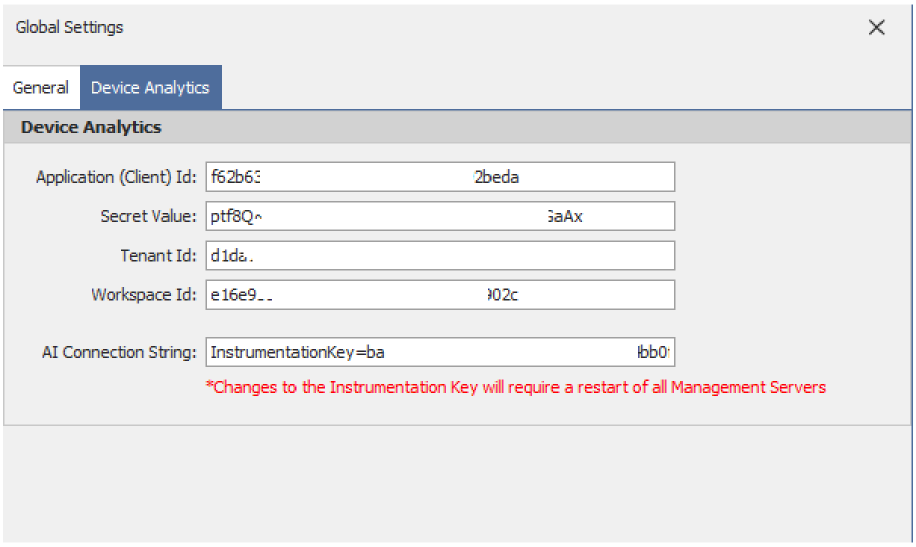
Property	Data
Product Type	ThinScale Desktop Agent
Company	TDA Development License
Details	TDA Development License
License Type	NA
Number of Seats	250
Assigned Folder	Devices (Root)
Status	Active
Expiry	Sunday 19 November 2023
Subscription Date	N/A
Licensed Products	ThinKiosk, Secure Remote Worker
Custom Features	None



ThinScale Desktop Agent

Property
Product Type
Company
Details
License Type
Number of Seats
Assigned Folder
Status
Expiry
Subscription Date
Licensed Products
Custom Features

21. Device Analytics



Global Settings

Device Analytics

Application (Client) Id: f62b63 2beda

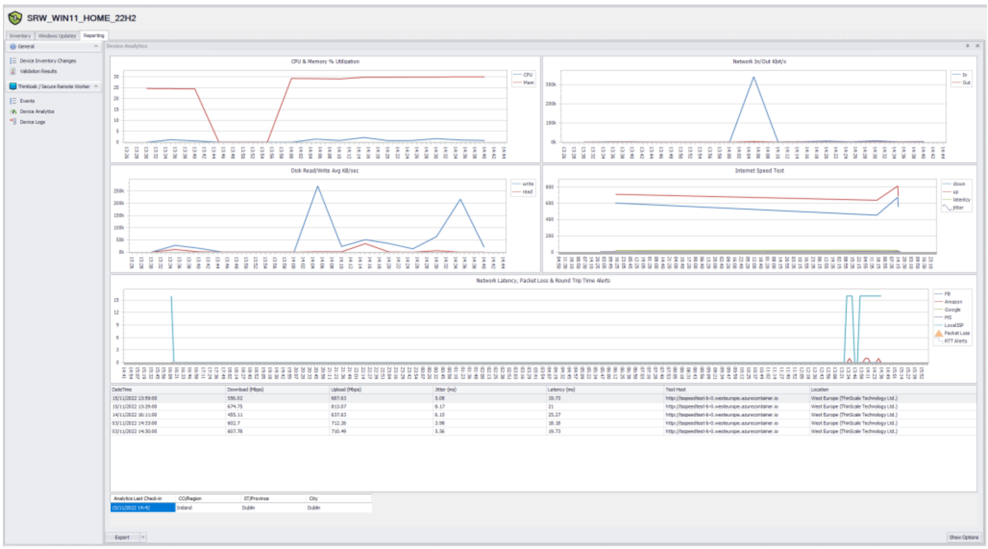
Secret Value: ptf8Q GaAx

Tenant Id: d1da.

Workspace Id: e16e9 02c

AI Connection String: InstrumentationKey=ba bb0

*Changes to the Instrumentation Key will require a restart of all Management Servers



SRW_WIN11_HOME_22H2

DateTime	Download (Mbps)	Upload (Mbps)	Jitter (ms)	Latency (ms)	Test Host	Location
15/11/2022 13:59:00	556.02	687.63	5.08	19.73	http://tsspeedtest-b-0.westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
15/11/2022 13:29:00	674.75	813.07	8.17	21	http://tsspeedtest-b-0.westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
14/11/2022 16:11:00	455.11	637.63	6.15	25.27	http://tsspeedtest-b-0.westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
03/11/2022 14:33:00	602.7	712.26	3.98	18.18	http://tsspeedtest-b-0.westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
03/11/2022 14:30:00	607.78	710.49	5.56	19.73	http://tsspeedtest-b-0.westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)

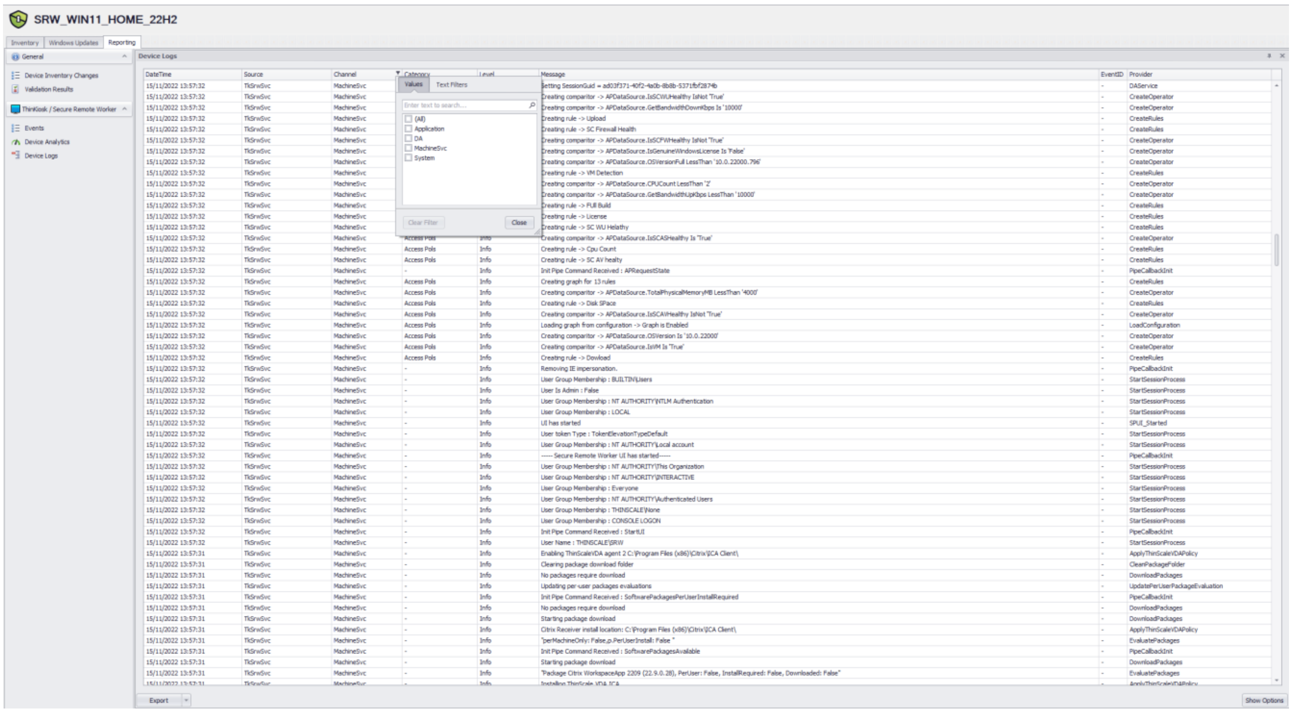
Analytics Last Check-in	CO/Region	ST/Province	City
15/11/2022 14:42	Ireland	Dublin	Dublin

Please have a look at the KB articles for more info about the Log Analytics workspace and the Application Insights.

22. Device Logs

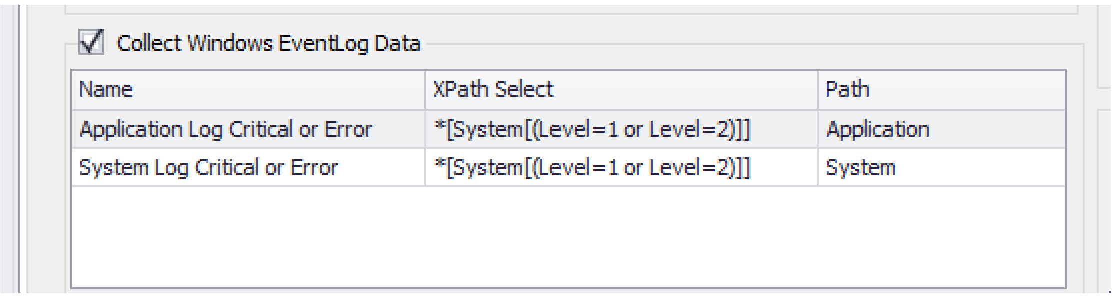
The new Device Logs Tabs together with the Device Analytics is a powerful tool to analyze the state of a machine directly from the console.
You will be able to see in almost real-time a consolidated view of multiple logs & event sources. This includes:

- “Startup Events” (including installed applications if enabled),
- “Windows Event Logs”,
- “TK/SRW “Machine Service” log events, and
- the “Device Analytics” events.



DateTime	Source	Channel	Category	Level	Message	EventID	Provider
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Setting SessionGuid = ad03f371-40f2-4a0b-8b8b-5371fbf2874b	-	DAService
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating comparitor -> APDataSource.IsSCWUHealthy IsNot 'True'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating comparitor -> APDataSource.GetBandwidthDownKbps Is '10000'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating rule -> Upload	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating rule -> SC Firewall Health	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating comparitor -> APDataSource.IsSCFWHealthy IsNot 'True'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating comparitor -> APDataSource.IsGenuineWindowsLicense Is 'False'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating comparitor -> APDataSource.OSVersionFull LessThan '10.0.22000.796'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating rule -> VM Detection	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating comparitor -> APDataSource.CPUCount LessThan '2'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating comparitor -> APDataSource.GetBandwidthUpKbps LessThan '10000'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating rule -> FUll Build	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating rule -> License	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc			Creating rule -> SC WU Helathy	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating comparitor -> APDataSource.IsSCASHealthy Is 'True'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating rule -> Cpu Count	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating rule -> SC AV healty	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	Init Pipe Command Received : APRequestState	-	PipeCallbackInit
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating graph for 13 rules	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating comparitor -> APDataSource.TotalPhysicalMemoryMB LessThan '4000'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating rule -> Disk SPace	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating comparitor -> APDataSource.IsSCAVHealthy IsNot 'True'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Loading graph from configuration -> Graph is Enabled	-	LoadConfiguration
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating comparitor -> APDataSource.OSVersion Is '10.0.22000'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating comparitor -> APDataSource.IsVM Is 'True'	-	CreateOperator
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	Access Pols	Info	Creating rule -> Dowload	-	CreateRules
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	Removing IE impersonation.	-	PipeCallbackInit
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : BUILTIN\Users	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Is Admin : False	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : NT AUTHORITY\NTLM Authentication	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : LOCAL	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	UI has started	-	SPUI_Started
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User token Type : TokenElevationTypeDefault	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : NT AUTHORITY\Local account	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	------ Secure Remote Worker UI has started------	-	PipeCallbackInit
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : NT AUTHORITY\This Organization	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : NT AUTHORITY\INTERACTIVE	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : Everyone	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : NT AUTHORITY\Authenticated Users	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : THINSCALE\None	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Group Membership : CONSOLE LOGON	-	StartSessionProcess
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	Init Pipe Command Received : StartUI	-	PipeCallbackInit
15/11/2022 13:57:32	TkSrwSvc	MachineSvc	-	Info	User Name : THINSCALE\SRW	-	StartSessionProcess
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Enabling ThinScaleVDA agent 2 C:\Program Files (x86)\Citrix\ICA Client\	-	ApplyThinScaleVDAPolicy
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Clearing package download folder	-	CleanPackageFolder
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	No packages require download	-	DownloadPackages
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Updating per-user packages evaluations	-	UpdatePerUserPackageEvaluation
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Init Pipe Command Received : SoftwarePackagesPerUserInstallRequired	-	PipeCallbackInit
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	No packages require download	-	DownloadPackages
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Starting package download	-	DownloadPackages
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Citrix Receiver install location: C:\Program Files (x86)\Citrix\ICA Client\	-	ApplyThinScaleVDAPolicy
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	"perMachineOnly: False,p.PerUserInstall: False "	-	EvaluatePackages
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Init Pipe Command Received : SoftwarePackagesAvailable	-	PipeCallbackInit
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Starting package download	-	DownloadPackages
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	"Package Citrix WorkspaceApp 2209 (22.9.0.28), PerUser: False, InstallRequired: False, Downloaded: False"	-	EvaluatePackages
15/11/2022 13:57:31	TkSrwSvc	MachineSvc	-	Info	Installing ThinScale VDA ICA	-	ApplyThinScaleVDAPolicy

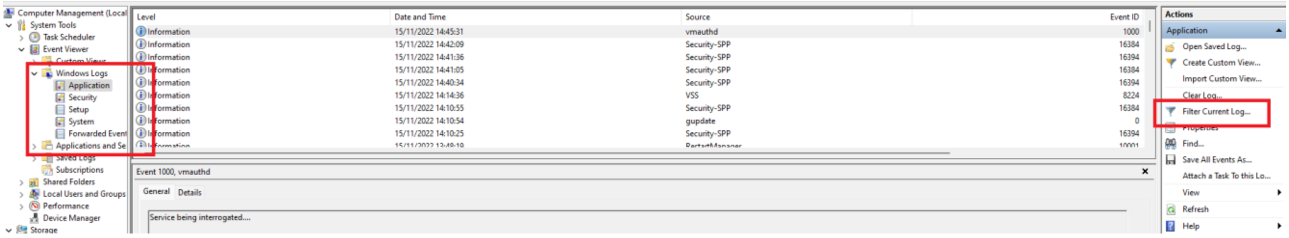
By default, only Critical and Error Logs are saved in the Log Analytics Workspace.



☑ Collect Windows EventLog Data

Name	XPath Select	Path
Application Log Critical or Error	*[System[(Level=1 or Level=2)]]	Application
System Log Critical or Error	*[System[(Level=1 or Level=2)]]	System

These can be modified using Windows standard XPath Select statements. The easiest way of doing so is via the “Computer Management” option.



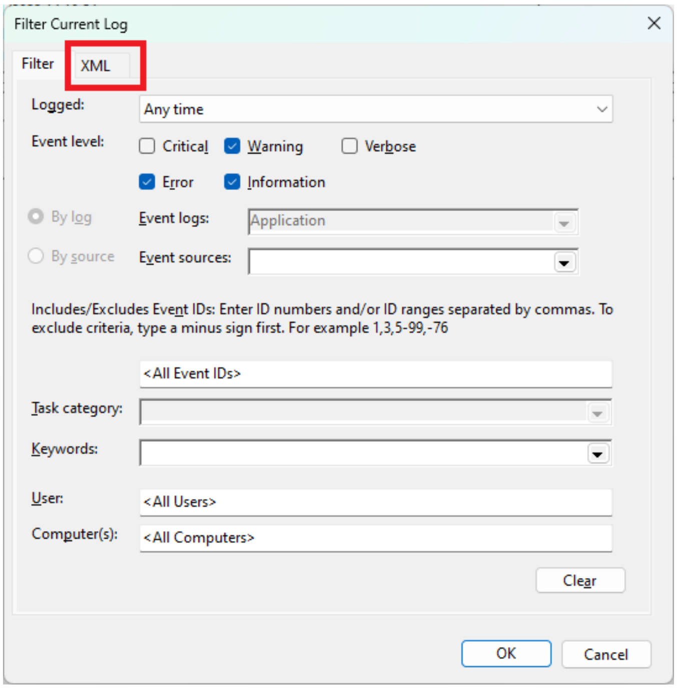
Level	Date and Time	Source	Event ID
Information	15/11/2022 14:45:31	vmauthd	1000
Information	15/11/2022 14:42:09	Security-SPP	16384
Information	15/11/2022 14:41:36	Security-SPP	16394
Information	15/11/2022 14:41:05	Security-SPP	16384
Information	15/11/2022 14:40:34	Security-SPP	16394
Information	15/11/2022 14:14:36	VSS	8224
Information	15/11/2022 14:10:55	Security-SPP	16384
Information	15/11/2022 14:10:54	gupdate	0
Information	15/11/2022 14:10:25	Security-SPP	16394
Information	15/11/2022 13:49:19	RestartManager	10001

Event 1000, vmauthd

General Details

Service being interrogated....

Click Filter Current Logs. Select the level desired and then simply copy the XML Value within the Management Console, like so.



Logged: Any time

Event level: ☐ Critical ☑ Warning ☐ Verbose

☑ Error ☑ Information

● By log Event logs: Application

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

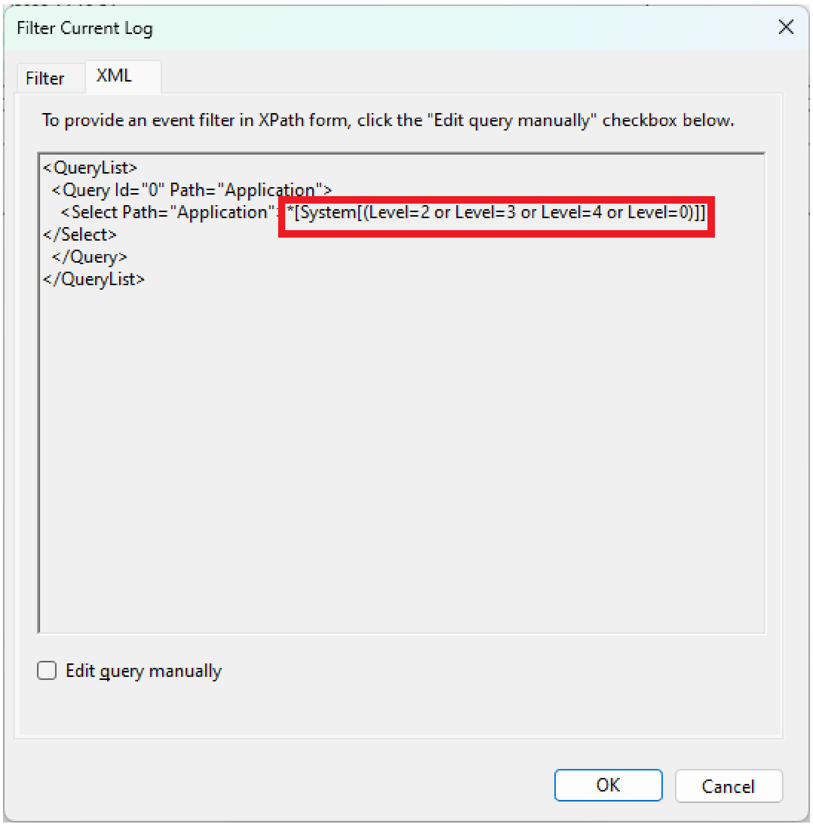
<All Event IDs>

Task category:

Keywords:

User: <All Users>

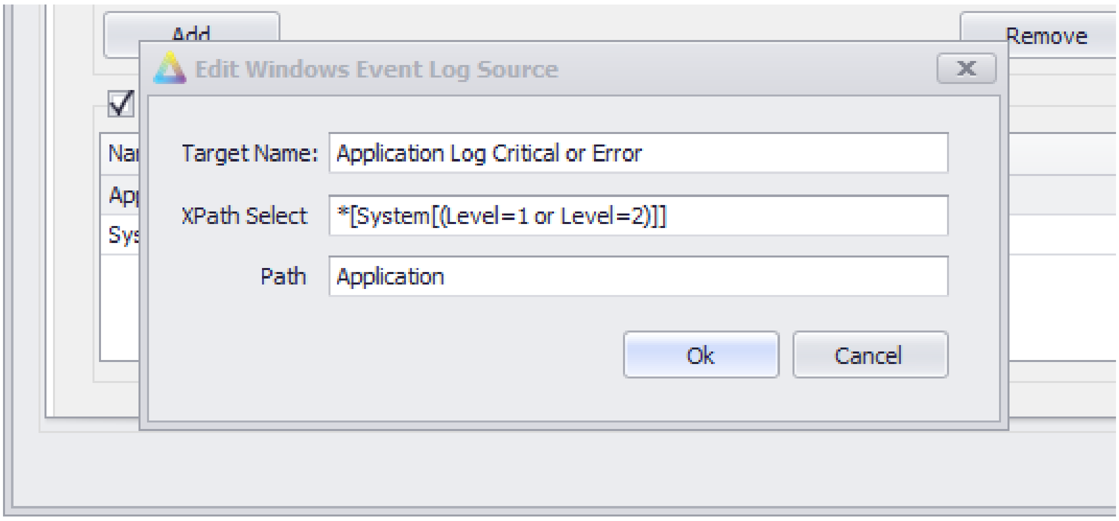
Computer(s): <All Computers>



To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
  <Query Id="0" Path="Application">
    <Select Path="Application">*[System[(Level=2 or Level=3 or Level=4 or Level=0)]]
</Select>
  </Query>
</QueryList>
```

□ Edit query manually

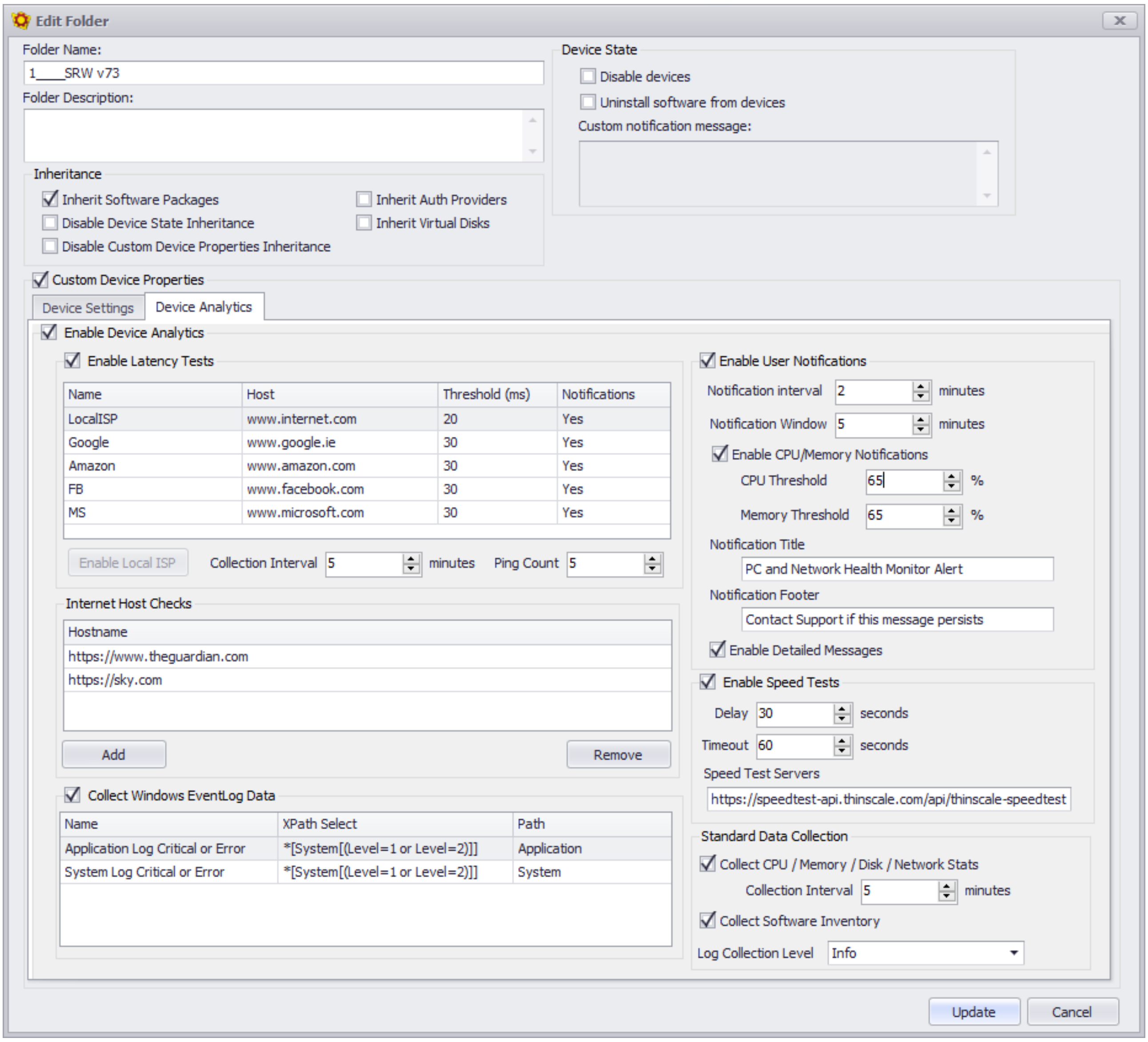


Target Name: Application Log Critical or Error

XPath Select: *[System[(Level=1 or Level=2)]]

Path: Application

Example of Device Analytics



Edit Folder

Folder Name: 1____SRW v73

Folder Description:

Inheritance

☑ Inherit Software Packages
□ Inherit Auth Providers
□ Disable Device State Inheritance
□ Inherit Virtual Disks
□ Disable Custom Device Properties Inheritance

Device State

□ Disable devices
□ Uninstall software from devices

Custom notification message:

☑ Custom Device Properties

☑ Enable Device Analytics

☑ Enable Latency Tests

Name	Host	Threshold (ms)	Notifications
LocalISP	www.internet.com	20	Yes
Google	www.google.ie	30	Yes
Amazon	www.amazon.com	30	Yes
FB	www.facebook.com	30	Yes
MS	www.microsoft.com	30	Yes

Collection Interval 5 minutes

Ping Count 5

Internet Host Checks

Hostname
https://www.theguardian.com
https://sky.com

☑ Collect Windows EventLog Data

Name	XPath Select	Path
Application Log Critical or Error	*[System[(Level=1 or Level=2)]]	Application
System Log Critical or Error	*[System[(Level=1 or Level=2)]]	System

☑ Enable User Notifications

Notification interval 2 minutes

Notification Window 5 minutes

☑ Enable CPU/Memory Notifications

CPU Threshold 65 %

Memory Threshold 65 %

Notification Title: PC and Network Health Monitor Alert

Notification Footer: Contact Support if this message persists

☑ Enable Detailed Messages

☑ Enable Speed Tests

Delay 30 seconds

Timeout 60 seconds

Speed Test Servers: https://speedtest-api.thinscale.com/api/thinscale-speedtest

Standard Data Collection

☑ Collect CPU / Memory / Disk / Network Stats

Collection Interval 5 minutes

☑ Collect Software Inventory

Log Collection Level: Info

Enable Latency Test

This is the place where you want your users to perform a speed test against specific URLs or IP Addresses.

Internet Host Checks

This option is to evaluate if the machine has or does not have an internet connection for local diagnostic purposes. A TCP port test of the URI will be logged in the local Machine Service, log file

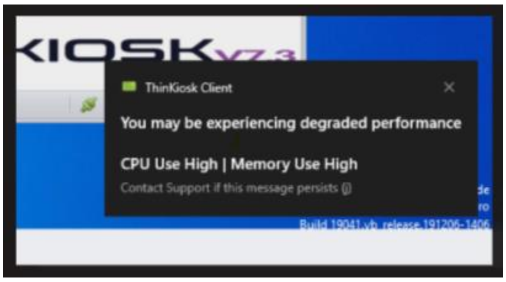
Collect Windows Event Log Data

This option will set the Log Level of the Windows Event Viewer you want the clients to collect.

Enable User Notification

This option is used to set a specific collection interval and a threshold to show users a systray notification.
When that threshold has been reached an example notification will be displayed.

i.e.

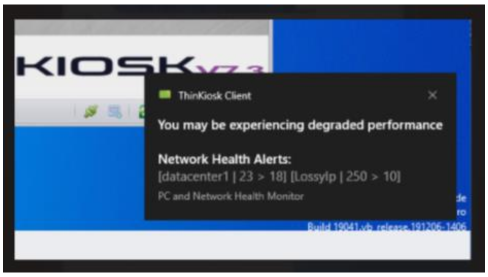


ThinKiosk Client

You may be experiencing degraded performance

CPU Use High | Memory Use High

Contact Support if this message persists



ThinKiosk Client

You may be experiencing degraded performance

Network Health Alerts:
[datacenter1 | 23 > 18] [Lossylp | 250 > 10]
PC and Network Health Monitor

Speed Test Server

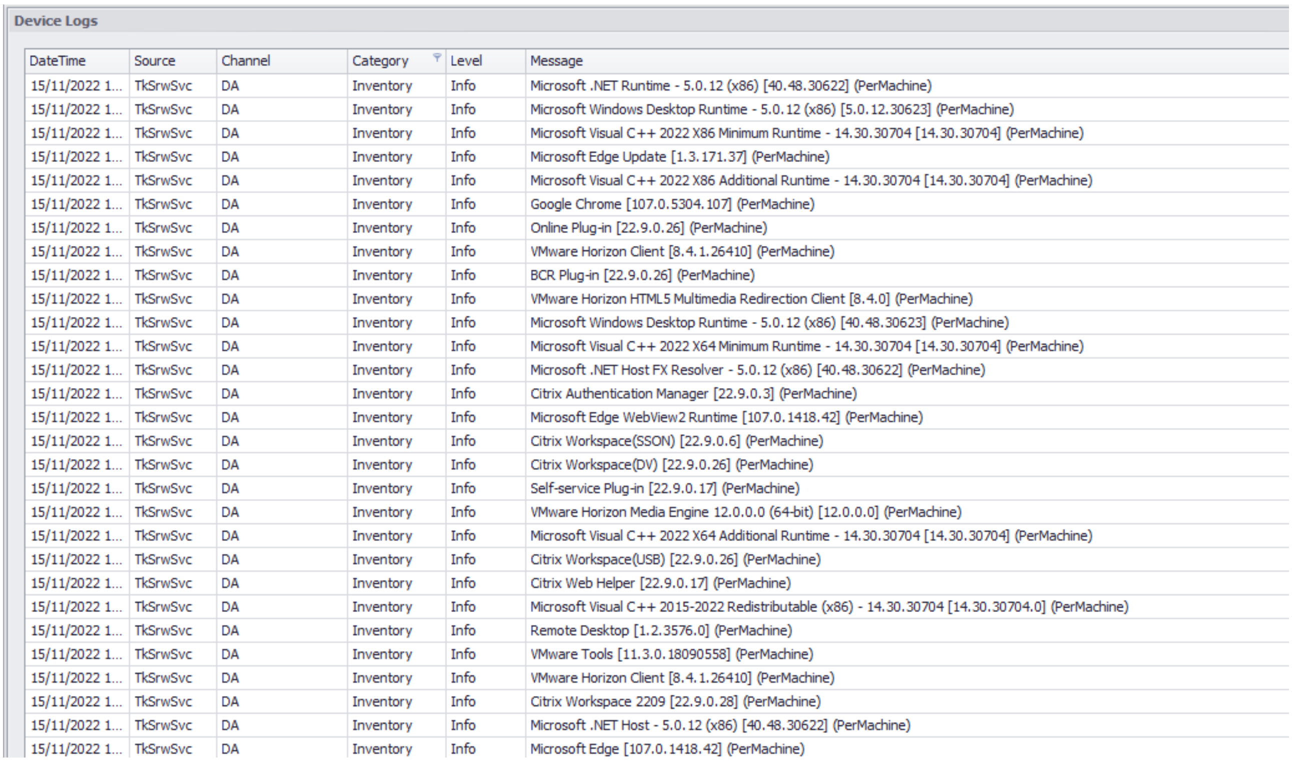
Please do not modify modified this value unless instructed by ThinScale Support.
https://speedtest-api.thinscale.com/api/thinscale-speedtest-servers

Standard Data Collection

This is the interval in which the data will be collected.

Collection Software Inventory

When enabled Device Analytics will collect all the Installed Applications on the machine. *Please note: AppData (user-based) applications are not collected with this version.*



Device Logs

DateTime	Source	Channel	Category	Level	Message
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft .NET Runtime - 5.0.12 (x86) [40.48.30622] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Windows Desktop Runtime - 5.0.12 (x86) [5.0.12.30623] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.30.30704 [14.30.30704] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Edge Update [1.3.171.37] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Visual C++ 2022 X86 Additional Runtime - 14.30.30704 [14.30.30704] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Google Chrome [107.0.5304.107] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Online Plug-in [22.9.0.26] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	VMware Horizon Client [8.4.1.26410] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	BCR Plug-in [22.9.0.26] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	VMware Horizon HTML5 Multimedia Redirection Client [8.4.0] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Windows Desktop Runtime - 5.0.12 (x86) [40.48.30623] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.30.30704 [14.30.30704] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft .NET Host FX Resolver - 5.0.12 (x86) [40.48.30622] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Citrix Authentication Manager [22.9.0.3] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Edge WebView2 Runtime [107.0.1418.42] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Citrix Workspace(SSON) [22.9.0.6] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Citrix Workspace(DV) [22.9.0.26] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Self-service Plug-in [22.9.0.17] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	VMware Horizon Media Engine 12.0.0.0 (64-bit) [12.0.0.0] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Visual C++ 2022 X64 Additional Runtime - 14.30.30704 [14.30.30704] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Citrix Workspace(USB) [22.9.0.26] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Citrix Web Helper [22.9.0.17] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.30.30704 [14.30.30704.0] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Remote Desktop [1.2.3576.0] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	VMware Tools [11.3.0.18090558] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	VMware Horizon Client [8.4.1.26410] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Citrix Workspace 2209 [22.9.0.28] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft .NET Host - 5.0.12 (x86) [40.48.30622] (PerMachine)
15/11/2022 1...	TkSrwSvc	DA	Inventory	Info	Microsoft Edge [107.0.1418.42] (PerMachine)

23. Icons

For reference, you can find a table list of the icons and their text below.

NEW

	Online ThinKiosk Device
	Online ThinKiosk Device Disabled
	Online ThinKiosk Device Uninstalled
	Offline ThinKiosk Device
	Offline ThinKiosk Device Disabled
	Offline ThinKiosk Device Uninstalled
	Online Secure Remote Worker Device
	Online Secure Remote Worker Device Disabled
	Online Secure Remote Worker Device Uninstalled
	Offline Secure Remote Worker Device
	Offline Secure Remote Worker Device Disabled
	Offline Secure Remote Worker Device Uninstalled
	Online IntelliPerform Device
	Offline IntelliPerform Device
	Online VDA Device
	Online ThinScale Desktop Agent Device
	Online ThinScale Desktop Agent Device Disabled
	Online ThinScale Desktop Agent Device Uninstalled
	Offline ThinScale Desktop Agent Device
	Offline ThinScale Desktop Agent Device Disabled
	Offline ThinScale Desktop Agent Device Uninstalled
	Protected folder (this cannot be deleted)
	Folder
	New Folder
	Edit Folder
	Disabled Folder
	Uninstall Folder
	New Profile
	Edit Profile
	Copy Profile
	Profile Revision
	View Profile
	Assign Profile
	Unassign Profile
	Jump To…
	Management Server

	Software Package
	Add Software Package
	Assign Software Package
	Unassign Software Package
	Roles
	New Role
	Edit Role
	License
	Install License
	Users
	New User
	Edit User
	User Disabled
	Permissions
	New Device
	Refresh
	Move To
	Delete
AB	Rename
	Default Device Properties
	Audit Log
	About
	Knowledge Base
	Assign a license to Device Folder
	Install PowerShell Module
	New Notifications
	Assign Notification to folder
	Unassign Notification from folder
	Expand All
	Collapse All
	Retrieve Server Logs
	ThinScale Portal
	Access Key
	Add Access Key
	Edit Access Key
	Auth Provider

	New Auth Provider
	Edit Auth Provider
	Assign Auth Provider
	Unassign Auth Provider
	Import Auth Provider
	Export Auth Provider
	Virtual Disks
	New Virtual Disks
	Assign Virtual Disks
	Unassign Virtual Disks
	License Report
	User Assignments
	New User Assignments
	Edit User Assignments
	Global Settings
	Device Policies

24. Troubleshooting

If you experience any crashes when communicating with the Management Server or Device, please refer to the Management Server Log (documented in the **Logging** section of the **ThinScale Management Server 8.x Admin Guide**).

Also, if related to a Device please check the debug log on the ThinKiosk device covered in the **ThinKiosk documentation.**

For any other queries about the ThinScale Management Console or ThinKiosk client, Profile, general settings or maybe a new feature you would like to have, feel free to contact us at:

https://kb.thinscale.com/contact-support