

THINSCALE

DEVICE PORTAL

Administrator **GUIDE**



Table of Contents

Table of Contents	1
1. ThinScale Device Portal	5
Introduction	5
2. Minimum browser requirements	7
3. Login Screen	8
Native / OAuth Login.....	9
Adding the OAuth Login	10
Step 1:	10
Step 2:	11
Step 3:	12
Step 4:	13
Step 5:	13
4. User Interface Overview	16
Administrator Permission Model	17
Introduction	17
Admin Permission Model	18
Accumulated Permissions	22
Allow Permission Sets	22
Deny Permission Sets	23
Order of Admin Permission Sets or Admin Roles.....	25
Permissions and Types of data.....	28
Sidebar Navigation Buttons	30
Organisation	30
Organisation Settings	30
Auth Providers.....	31
Admin Roles	32
Admin Permissions Set.....	33
Allow or Deny Permission Set	34
Global Organisation Permissions	34
Config Admin Permissions	34



Device Management Permissions	34
Report Permissions	34
Admin Resource Group	35
Admin Resource Folder	35
Admin User Groups	35
Admin Users	35
5. Devices	36
6. Device Groups	37
7. Configuration.....	38
Config Assignments	38
Device Profiles.....	43
General Profiles.....	44
Windows Shell.....	45
Magic Filter	48
Local Device Restrictions.....	49
Logon Script.....	52
Logoff Script	53
Additional Registry Values	54
Session Timers.....	56
Lock Screen	57
Thinscale Virtual Desktop Agent	58
Windows Proxy	59
Privacy Settings	60
UI Profiles	61
User Interface.....	61
Profile Data Repository	62
Watermarking	65
Appearance	68
Applications.....	72
Secure Browser	76
Security Profiles	83
MDM Profiles	112
Device Policies.....	115



Operating Mode	116
Device Login Options.....	117
Use Local Managed Account.....	117
Use Custom Account	117
Don't Auto Login	117
Do Nothing	118
Ignore Shift Override.....	118
Set Local Managed Account display name to an authenticated user	118
General.....	119
Cache Configuration.....	119
Local Managed Account Per Profile	119
Local Managed Account Per Authentication User	120
Disable Folder Integrity Check	120
Hide Splash Screen	120
Branding and Shortcut	121
Startup Script	121
Enable Startup Script.....	121
Startup Script Timeout	121
Device Policy Configuration	122
Device Events	122
Enable Device Event Collection.....	122
Only collect the following events.....	122
Logging	123
Enable Agent Logging.....	123
Admin Actions	124
Only allow device action when in secure session	124
Perform device actions silently	124
Perform device actions if no user response is received.....	124
Device Settings	125
Troubleshooting.....	126
Logging	128
Enable Agent Logging.....	128
Administration	129



Authentication	130
Software Packages	131
Package Creator	131
Software Package.....	132
Name	135
Publisher	135
Description	135
Version	135
Reboot Required	135
Reboot Now	135
Per User Install	135
Install Files.....	135
Adding a new software package	137
Please check our library of already made package from the ThinScale Portal.....	138
Software Packages Groups.....	139
Authentication Providers	141
Azure, and Okta.....	142
Virtual Disks.....	143
End Users	145
End Users Groups.....	145
Device Access Keys.....	147
TDA Update Policies.....	149
Device Analytics Profile.....	150
8. Reports	157
9. Tools.....	159



















1. ThinScale Device Portal




Introduction


The ThinScale Device Portal represents the latest enhancement in the ThinScale product suite, capitalizing on the familiar features that administrators have previously appreciated and utilized in the "On prem" Management Console. This is achieved through a streamlined, responsive, and highly efficient web interface.


The new Device Portal makes it easy for you to:

- View your entire device estate 
- Set granular permissions within the organization 
- manage your **Devices**  and your Device Groups 
- manage all your device Configurations 
 - Configuration Assignments 
 - Device Profiles 
 - General 
 - UI 
 - Security 
 - MDM 
 - Device Policies 
 - Software Packages and Software Packages Groups 
 - Auth Providers 
 - Virtual Disks 
 - End Users and End User Groups 



- Device Access Keys 
- ThinScale Desktop Agent (TDA) Update Policies 
- Device Analytics Profile 

- manage and view Reports 
 - Audit and Permissions

- Tools 

The Device Portal 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 Portal.



2. Minimum browser requirements

The Device Portal is compatible with any standard's compliant web browser. We regularly test Device Portal with the following browsers:

Desktop:

- Edge
- Chrome,
- Firefox,
- Opera

Mobile:

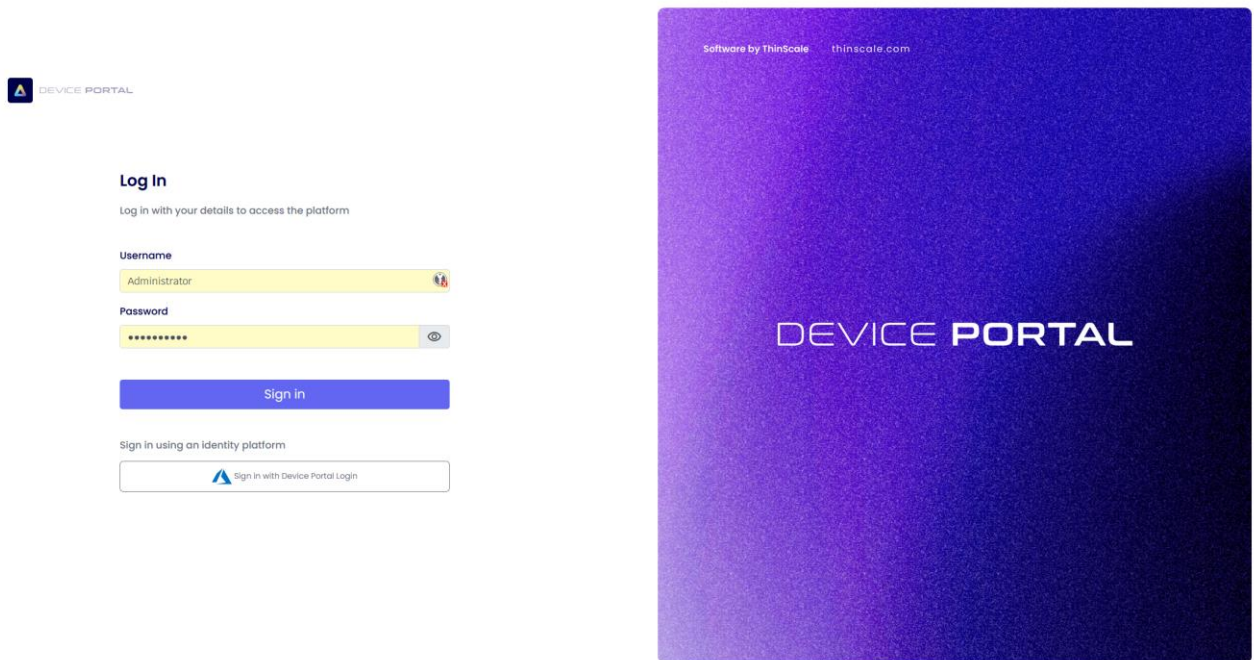
- Regarding mobile browsers, ThinScale Dev Team advises against their usage due to potential inaccuracies in presenting certain functionalities.

To ensure an optimal experience and bolster security, it is highly recommended that you maintain your browser up to date.



3. Login Screen

Whenever you start the Device Portal web page the first screen displayed is the Login screen.



Please note: The web page link will be automatically sent to you upon registration to the ThinScale Cloud. Alongside a Default Username and Password. It is recommended that you change your password upon logging.

Once you launch the site there are two ways you can connect:



Native / OAuth Login

The Device Portal supports both Native login and via an Auth Provider. To login with the OAuth Login using the Native account first, and then add the Auth Provider inside your Configuration Tab.

Upon first login this message will appear.

WARNING: Local administrator accounts are enabled!

Local administrator accounts are enabled on the system. The use of local administrator accounts is necessary for initial commissioning of the system however it is best practise to correctly configure the system to use Auth Providers for authorizing administrators on the system.

If the intention is to use local administrator accounts on a permanent basis this warning message can be turned off in company settings.

[OK](#)

To disable or enable this message please open Organization setting and switch on or off the toggle option.

- Organisation
 - Organisation Settings**
 - Admin Roles
 - Admin Permissions Sets
 - Admin Resource Groups
 - Admin Resource Folders
 - Admin User Groups

Local Administrator Accounts

- Enable Local Administrator Accounts ⓘ
- Warn if local Administrator accounts are left enabled ⓘ

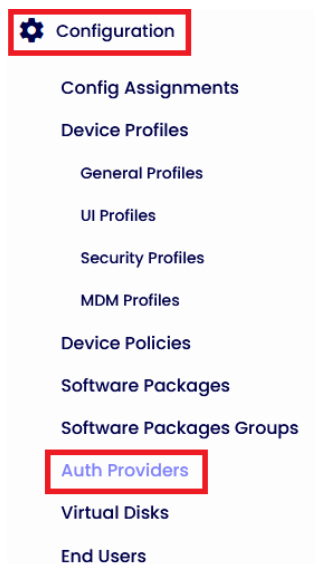


Adding the OAuth Login

For detailed instructions on configuring an Azure Authentication Provider on the Azure Control Plane, refer to the following [resource](#).

Step 1:

Click on Configuration and Auth Providers





Step 2:

Give it a name and assign it to the Resource Folder

Auth Provider Information

Name

Device Portal Login

Description

Device Portal Login

Resource Folder

General



Click Save on the top right of the screen



Step 3:

Select the Auth Provider Type and the flow

^ Auth Provider Type

Select the type of the authentication provider

Azure

Select which authentication flow is allowed

TDA and Admin Authentication



TDA and Admin Authentication

TDA Authentication

Admin Authentication

In this example we will be using Azure and only Admin Authentication.

Flow options:

TDA and Admin Authentication: the same Auth App is used to authenticate both the Device Portal and the new TDA client

TDA Authentication: the Auth App is used to authenticate only the TDA client

Admin Authentication the Auth App is used to authenticate only the Device Portal

Click Save



Step 4:

The retrieval of General Settings, Token Validation, and Server-Side Validation data necessitates the successful setup of the environment within the Azure Control Plane.

Copy the information from the Azure Portal as explained in the KB article.


Once done click Save and you are done.

Step 5:

Browser the Organization Tab. Click on Organisation Settings and Select the Auth Provider you have just created.

The screenshot shows the ThinScale web interface. On the left is a navigation sidebar with the following items: Organisation Settings (highlighted with a red box), Admin Roles, Admin Permissions Sets, Admin Resource Groups, Admin Resource Folders, Admin User Groups, Admin Users, Devices, Device Groups, Configuration, and Reports. The main content area is titled 'Local Administrator Accounts' and contains two toggle switches: 'Enable Local Administrator Accounts' (which is turned on) and 'Warn if local Administrator accounts are left enabled' (which is turned off). Below this is a section titled 'Auth Providers' with a dropdown arrow. Underneath, there is a form with a 'Name' label and a large text input field. At the bottom of the main content area, there is a blue button labeled 'Select Auth Providers' (highlighted with a red box).



Selected ▾	Name
<input checked="" type="checkbox"/>	 Device Portal Login Device Portal Login

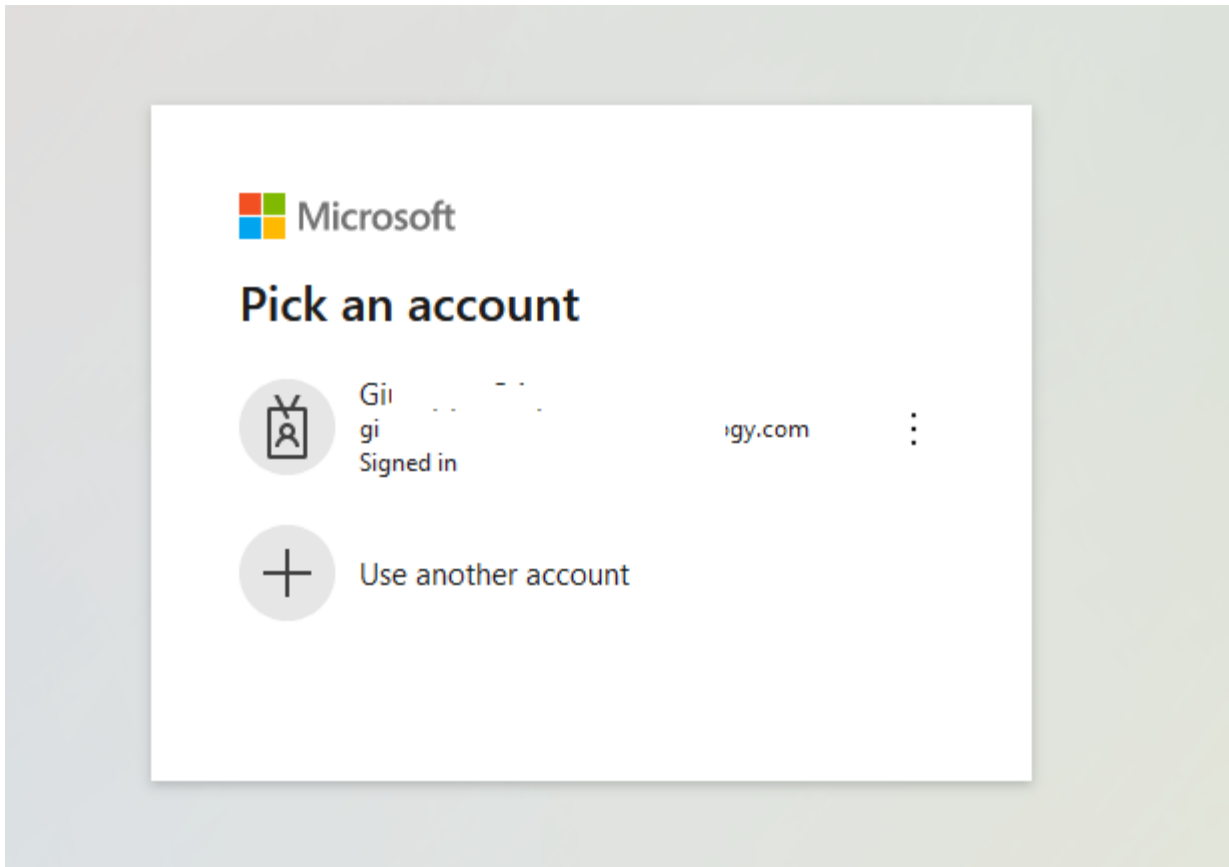
Click Save.

Go back to the main web page and click Sign in with Azure Auth Provider. Perform the Auth flow and you will be ready to use the Device Portal.

[Sign in](#)

Sign in using an identity platform

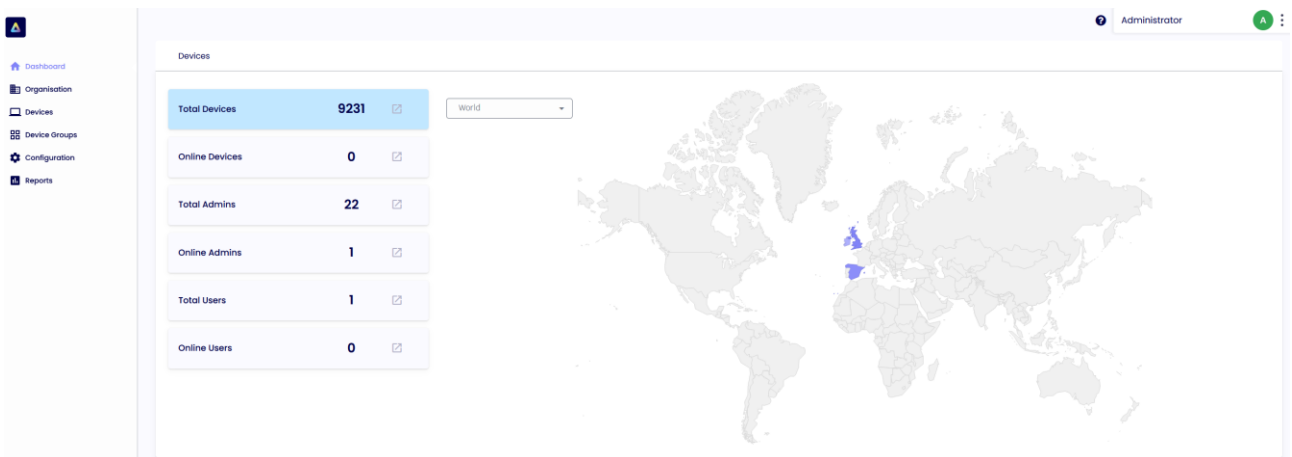
 [Sign in with Device Portal Login](#)





4. User Interface Overview

The Device Portal undergoes real-time updates in response to user selections within the left-hand side tree menu. The primary interface, referred to as the Dashboard, provides administrators with a comprehensive overview, including information on the number of online devices, active admin sessions, and the total count of online users.



Note: Please feel free to provide feedback regarding the design and positioning of features within the Portal. If you encounter any issues or areas of frustration, kindly share your feedback, and we will consider incorporating your suggestions in upcoming releases.



Administrator Permission Model

Introduction

The On-Prem ThinScale Device Portal uses a hierarchical data structure typically consisting of navigating many tree views to find the appropriate data. The permission model employed to manage the data was also a hierarchical permission model. However, this inheritance-based approach has lost favour due to its inflexibility, rigidity, and potential for unintended consequences.

One of the first decision that ThinScale performed when developing the Device Portal within ThinScale Cloud was to examine the data model that should be used. It was decided to use a flat data structure allowing data to be navigated via search queries that can be saved as views.

In general, flat data structures are simple, flexible, efficient, and easy to maintain. They are ideal for web applications that require fast access to data and frequent updates.

Based on the decision to employ a flat data structure the Device Portal embraces a flat permission model, allowing for direct configuration of permissions across all entities within an Admin Resource Group. This approach offers exceptional flexibility and granularity, with the ability to assign multiple roles and permission sets. Permission reports are also available to assess the permissions of every administrator for each entity in the system.

While understanding this model may require a learning curve, it ultimately provides a highly flexible and manageable permission system, affording greater control and adaptability. This document aims to help to explain the administrator permission model and the terminology used and to help understand the reasoning behind the design.



Admin Permission Model

The Administrator permission model is made up of the following entities:

Term	Description
<p>Admin Users</p>	<p>An Admin User represents an administrator on the system. Admin User accounts should not be shared by different administrators.</p> <p>“Local” Admin Users are generated by existing administrators with the appropriate permissions; however, it is recommended to configure and use Auth Providers for Administrator logins to authenticate and authorize administrators on the system.</p> <p>Admin User accounts are automatically generated for administrators who login via Auth Provider accounts.</p> <p>Note: Local Admin User accounts are only recommended for initial commissioning, proof of concept and evaluation purposes. It is not recommended to leave Local User accounts enabled on the system. For security reasons it is highly recommended to authenticate and authorize administrators via an Auth Provider.</p>
<p>Admin User Groups</p>	<p>Admin User Groups are used to group sets of Administrators on the system. Local Admin Users can be manually added to the Admin User Group or using Auth Provider Groups Identifiers groups of administrators from groups within your Auth Provider can be identified and added easily to the Admin User Group.</p> <p>The permissions model on the Device Portal will ultimately use Admin User Groups to identify the administrators that receive the appropriate permissions (via Admin Roles).</p>
<p>Admin Roles</p>	<p>Admin Roles are used to configure the permissions for administrators on the Device Portal.</p> <p>In its simplest form the Admin Role applies a set of permissions on a set of resources to a set of</p>



	<p>administrators. In fact, the admin role can take multiple “sets of permissions on a set of resources” and apply it to a set of administrators via multiple Admin User Groups. In the situation of an Admin User being assigned multiple Admin Roles the permissions will accumulate unless a “Deny” permission is configured. If any Permission Set in any Admin Role assigned to the Admin User gives the Admin User to perform an action on the entity, then the Admin User will have the permission to perform the action.</p> <p>Note: An Admin User can exist in several Admin User Groups and each Admin User Group could actually have several roles assigned to it. This allows great flexibility when configuring permissions as an Admin User or Admin User Group could be assigned multiple roles. During proof of concept or evaluation or until you have a thorough understanding of the permission model it is recommended to use a single Admin Role per Admin User Group.</p>
<p>Admin Permission Sets</p>	<p>An Admin Permission Set is a set of permissions associated with types of data in the system. Typical permissions include List, Read, Update, Add and Delete although for Actions and Reports the permission is simple ‘Allowed’.</p> <p>For some data types (e.g. Organisation) the permissions operate globally for all entities of that type however for most entities on the system a permission is applied to a set of entities e.g. Read Devices might be limited to a set of Devices in a certain region.</p> <p>The full settings associated with Admin Permission Sets are shown in the screenshot below. As part of the configuration of an Admin Role the Admin Permission Set is associated with a set of resources in an Admin Resource Group that limits the scope of the permissions to the set of resources.</p>



<p>Admin Resource Folders</p>	<p>Most entities in the Device Portal are associated with a single Admin Resource Folder which is used to help configure the permissions of administrators on the entity. Some entities (e.g. Organisation and Permission Entities) are not associated with an Admin Resource Folder as the permissions for that entity are NOT limited to set of resources.</p> <p>An Admin Resource Folders is a collection of entities that all have something in common (typically a business unit and region) and is only used to determine the permissions that will be associated with that entity.</p> <p>Note: An Admin Resource Folder can be included in many Admin Resource Groups to allow for highly flexible permissions to be assigned via Admin Roles. To allow for the greatest flexibility entities should be added into Admin Resource Folders with the smallest amount of commonality (e.g. the smallest business unit with the smallest region). Admin Resource Groups are then used to group the Admin Resource Folders unto more manageable groups for administrating permissions.</p>
<p>Admin Resource Groups</p>	<p>Admin Resource Groups are groups of Admin Resource Folders which essentially makes them groups of entities. They are used to limit the permissions on an entity type to a set of specific entities in the Admin Role configuration. While Admin Resource Folders are typically a collection of entities with the smallest amount of commonality Admin Resource Groups should be groupings of Admin Resource Folders that make more sense from the perspective of configuring permissions. Because the same Admin Resource Folders can be configured in multiple Admin Resource Groups it is possible to have Admin Resource Groups that may include all the entities in a region and other Admin Resource Groups that may include all the entities globally for a business unit.</p>



Table 1: Description of the terminology and entity types of the permission model

The relationships between the entity types discussed above is visualised in the diagram below. Admin Roles are used to assign permissions (Admin Permission Sets) to a set of resources/entities (Admin Resource Groups/Folders) for a set of Admin Users as defined in the Admin User Group.

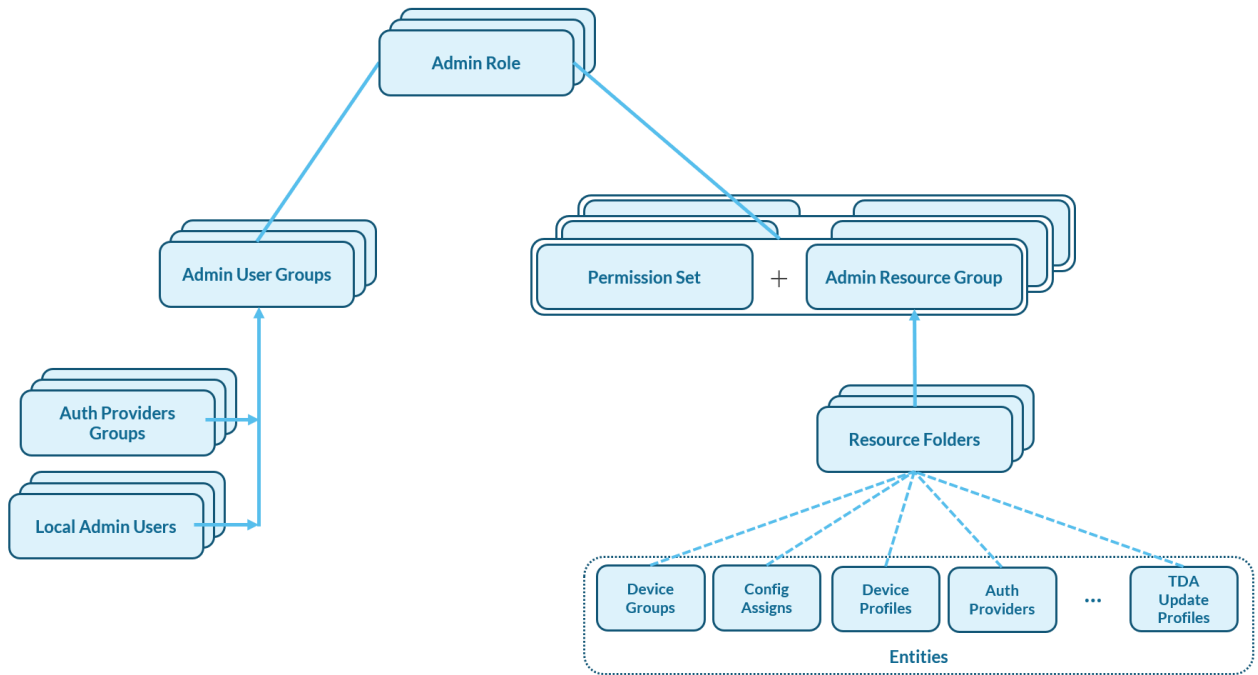


Figure 1: The relationships between the entity types of the permission model



Accumulated Permissions

Allow Permission Sets

For allow permission sets the setting of permissions on a resource is accumulative. This means that all administrators start with no permissions on any entity. The permissions are calculated for the administrator by checking every "Allow" Permission Sets in every Admin Role that the administrator is affiliated with and setting all appropriate permissions on all resources in the resource group. If a permission is unchecked the permission is simply not set for that permission set. The next permission set may grant the permission. In the example below the permissions are set for a "Standard Admin". You can see that they get full configuration, device management and reporting permissions for the associated resources in the Admin Role (e.g. USA Resources). They would not get any organisation permissions.

The screenshot displays the 'Standard Admin Settings' configuration page. It includes sections for 'Admin Permission Set Information', 'Global Organisation Permissions', 'Config Admin Permissions', 'Device Management Permissions', and 'Report Permissions'. The 'Global Organisation Permissions' table shows that 'Organisation Settings' is denied, while all other permissions are allowed. The 'Device Management Permissions' table shows that all listed permissions are allowed. The 'Report Permissions' table shows that both 'Audit Report' and 'Permission Report' are allowed.

	List	Read	Update	Add	Delete
Organisation Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admin Roles	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Admin Permission Set	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Resource Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Admin User Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Admin Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

	Allowed
Login / Logout	<input checked="" type="checkbox"/>
Remote Wipe	<input checked="" type="checkbox"/>
Shutdown	<input checked="" type="checkbox"/>
Restart	<input checked="" type="checkbox"/>
Lock	<input checked="" type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>
Refresh Profile	<input checked="" type="checkbox"/>
Refresh Profile and Restart	<input checked="" type="checkbox"/>
Remote Control	<input checked="" type="checkbox"/>
Get Device Logs	<input checked="" type="checkbox"/>
Set Device Name	<input checked="" type="checkbox"/>

	Allowed
Audit Report	<input checked="" type="checkbox"/>
Permission Report	<input checked="" type="checkbox"/>

Figure 2: Configuration of a "Standard Admin" Permission Set



Deny Permission Sets

Deny Permission sets are used to Deny a permission on a set of entities for an administrator. Once a permission is denied it can never be allowed again via an allow (or any) permission set. The only way to grant the permission again is to disassociate the Deny Permission Set with the administrator.

A typical example of using a Deny Permission Set would be to deny Reading, Adding, Updating or Deleting of Security Profiles on All Resources. This configuration could be added to a normal "Regional Admin Role" to prevent normal regional administrators having access to the Security Profiles.

Alternatively, this could have been accomplished by ensuring that the Security Profile permissions for Read, Add, Update and Delete were not set on any Permission Set associated with the administrator.

Deny Security Profiles Settings

Administrator A ⋮

[← Go Back](#)
[↻ Refresh](#)
[📄 Duplicate](#)
[💾 Save](#)

Admin Permission Set Information

Name

Description

^ **Allow or Deny Permission Set**

Allow / Deny Permission Set Allow Deny

^ **Config Admin Permissions**

	List	Read	Update	Add	Delete	Move
Security Profile	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Figure 3: An example of a Deny Permission Set being used to protect access to Security Profiles



The Deny Security Profiles permission set configured above could be used to protect Security Profiles in the configuration of an Admin Role. Consider the example below where an Admin Role is configured protecting the Security Profiles by using a Deny permission set against all resources in the system.

USA Regional Admin
Administrator A

← Go Back ↻ Refresh 📄 Duplicate 💾 Save

Admin Role Information

Name

Description

Admin User Groups

Name

👤 USA Admin Users
Admin User Group for administrators in USA

Select Admin User Groups

Admin Permissions

Admin Permission Set	Resource Group	Delete
Standard Admin	USA Resources	✖
Deny Security Profiles	All Resources	✖

Select Permission Set
Select Resource Group
Add

Figure 4: Example configuration of an Admin Role “USA Regional Admin” protecting the Security Profiles by using a Deny permission set against all resources in the system.

As said above the deny permission set would be unnecessary if the Read, Add, Update and Delete permissions for the Security Profile were removed from the Standard Admin permission Set. In this case the permissions would have never been set so would be in the Not Allowed state. The Deny permission set is a comfort factor to know that it cannot be accidentally granted via another permission set.



Order of Admin Permission Sets or Admin Roles

With the calculation of permissions as described above the order of Admin Permission Sets in an Admin Role (or the order of Admin Roles associated with an Admin User Group) does NOT matter.

Why does an Admin Role allow multiple sets of Admin Permission Sets and Admin Resource Groups?

Multiple pairs of Admin Permission Sets and Admin Resource Groups allow different sets of permissions to be applied to different sets of resources. For example, an administrator may need a lot of permissions on a certain set of resources but much less permissions (List or Read perhaps) on other resources. Three common uses for this are:

- (1) The Deny Permission set example that we saw above where the Deny Permission Set example is used to restrict access to sensitive entities.
- (2) Adding the "Allow List/Select Entities" permission set on all the resources in a "Shared" Admin Resource Group. This would allow administrators to share the entities that they are responsible for but knowing that the entities cannot be edited or deleted.
- (3) Setting up the main permissions for a role via a single pair of Admin Permission Sets and Admin Resource Groups and then configuring additional pairs of very specific Admin Permission Sets and Admin Resource Groups to add slightly different exceptions to the basic configuration. i.e. Grant Update right for a Device Policy to a small set of administrators as an extra right.



Why Admin Resource Groups and Admin Resource Folders?

Ultimately the management of administrator permissions will be based on the resources in Admin Resource Groups however the Admin Resource Folders are used to add flexibility to the management of these permissions.

It is recommended to use Admin Resource Folders as the smallest collection of resources that will have the same permissions. Typically, this would be a business unit and region. These Admin Resource Folders can then be combined to form Admin Resource Groups. Admin Resource Folders can be in many Admin Resource Groups offering excellent flexibility.

It is best to illustrate the above by example. Consider the use case where several business units are being managed across different regions (in this case global continents). It is possible that the day-to-day administration of the entities will be managed by “Regional Administrators” who will need various different permissions for reading, adding, updating and deleting for all the different resources in the region. Typically, a regional administrator may be responsible for all the different business units but only for that geographical region. Alternatively, each of the different business units may have an “Account Manager” responsible for reporting on the status of each of the business units. They may need their own permission set but for all the parts of the business unit across the different regions.

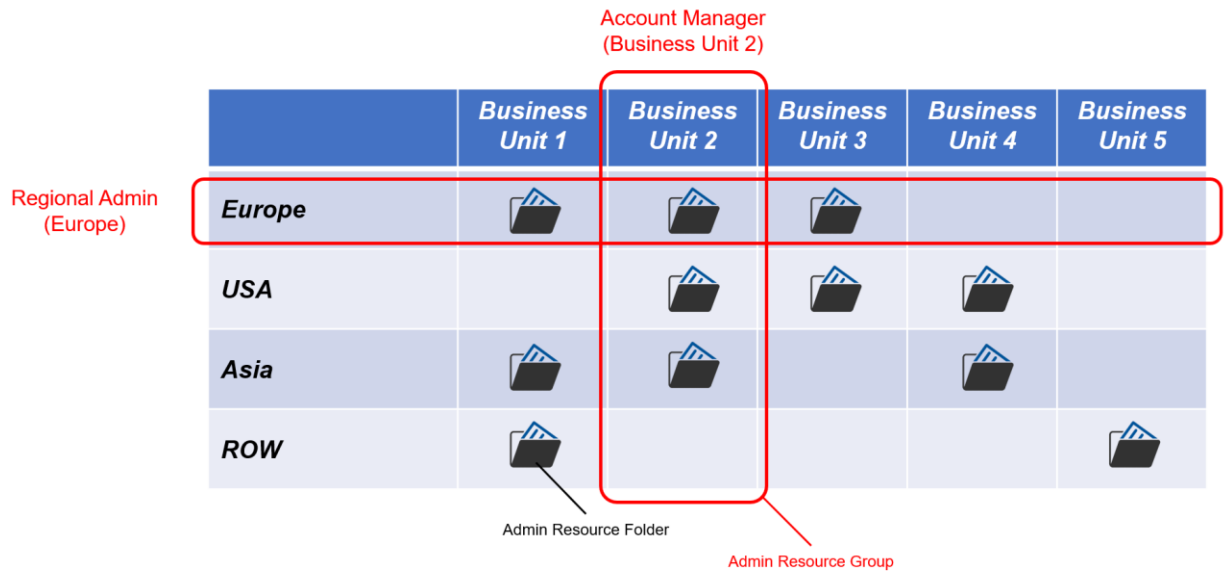


Figure 5: Example use of Admin Resource Folders and Admin Resource Groups to allow permissions to be easily configured for a Regional Administrator and Account Manager roles.



Permissions and Types of data

The management of data will vary depending on the needs of the organisation. The following example considers three different types of data that need to be managed differently by the organisation.

Regional Data

Regional Administrators manage the data. The data is not typically shared with other regions. Data may be specific to a customer or shared with many customers within the region.

Typical examples of this type of data include:

- Device Groups
- Config Assignments
- Device Profiles (including UI Profile, General Profile, MDM Profile)
- Device Policy
- Software Package Groups

Shared / Global Data

A global configuration of the entity is sufficient for most Regions / Customers. Regional Admins manage and share the entities (Shared Folder).

Typical examples of this type of data include:

- TDA Update Policy
- Software Packages
- Device Analytics Profile

In this case a single Admin Resource Folder called “Shared Folder” could be set up and added to each of the regional Admin Resource Groups so that the administrator gets the same permissions for the shared resources as the normal regional resources.

Alternatively, the “Shared Folder” could be added to an Admin Resource Group called “Shared Group”. Permissions could then be added by applying permissions specifically to this group.



In more complex situations the shared access may need to be limited and many shared folders and groups may need to be setup to customise the permissions

Protected Data

The data needs to be protected from most Admins. Specialist Admins manage and share the entities (Protected Folder). Regional Admins will get “List” or “Read” access.

Typical examples of this type of data include:

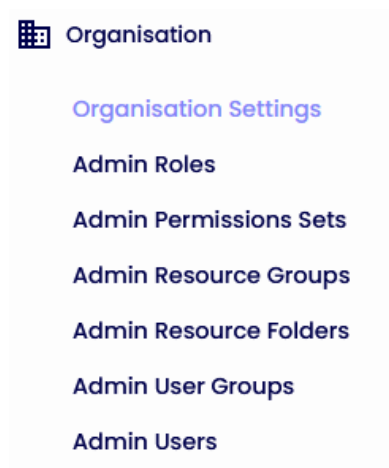
- Auth Providers
- Security Profiles

In this case a single Admin Resource Folder called “Protected Folder” could be configured and added to an Admin Resource Group called “Protected Group”. Permissions could then be granted to the group to give full read/write permission to a select few and “list only” permissions to the majority of administrators.



Sidebar Navigation Buttons

Organisation



Organisation Settings

In this section of the Device Portal, you will find 3 distinctive sections:

Local Administrator Accounts

Authentication Providers

Device Analytics

Local administrator accounts are required for initial configuration of Auth Providers on the System. It is recommended to disable local accounts once the Auth Providers have been successfully configured.

Warn if local Administrator accounts are left enabled, if enabled then every time an administrator, with permissions to add Auth Provider on the system, logs in they will be met with a warning to disable local administrator accounts.



WARNING: Local administrator accounts are enabled!


Local administrator accounts are enabled on the system. The use of local administrator accounts is necessary for initial commissioning of the system however it is best practise to correctly configure the system to use Auth Providers for authorizing administrators on the system.

If the intention is to use local administrator accounts on a permanent basis this warning message can be turned off in company settings.

Ok

Auth Providers

This feature enables the user to choose the Authentication Provider to access the Device Portal.

Auth Providers		
Name	Auth Provider Type	End User Groups
 Device Portal Auth Device Portal Auth	AZURE	-

Select Auth Providers



Admin Roles

Admin Roles are used to configure the permissions for administrators on the Device Portal. The "Super Admin Roles" feature encompasses all permissions associated with resources within the Device Portal.

This option is a default setting and is not removable.

Admin Role Information

Name

Description

^ Admin User Groups

Name

👤 Super Admins
 Group for administrator with full permissions on all resources

^ Admin Permissions

Admin Permission Set	Resource Group
Super Admin Permission Set	All Resources

Select Permission Set

Select Resource Group

Admin user groups represent ALL the groups of users that, once added, will receive the permission set in the Super Admin role.



Admin Permissions Set

By default, the Device Portal will be presented with 4 Default Permissions Set.

Those sets cannot be modified, just removed.

However, the easiest way of modifying an existing set is to duplicate the one you want to enhance or modify.

[← Go Back](#)
[↻ Refresh](#)
[📄 Duplicate](#)

Admin Permission Set



Row	Name
1	🔑 Super Admin Permission Set Default Admin Permission Set for administrators with full privileges to the system
2	🔑 Standard Admin Recommended settings for a standard administrator on the system
3	🔑 Auth Provider Only Recommended settings to restrict administration of Auth Provider to dedicated administrators
4	🔑 Allow List/Select Entities Allows administrators to list and select entities on the system.



Each of these roles is associated with a distinct set of permissions that are applied to various resource groups and folders.

It is important to note that you have the flexibility to create multiple permission sets with varying levels of granularity and visibility. These permissions are managed through checkboxes and are categorized into five groups:

Allow or Deny Permission Set

Allow permission sets allow permissions from different Permission Sets to accumulate on additional resources. A 'Deny' permission set is used to prevent specific permissions on resources. A deny permission can never be overwritten by an allow permission.

Global Organisation Permissions

These permissions operate globally across the full system and are not limited to the resources of the appropriate resource group.

Config Admin Permissions

These permissions operate on the configuration level and can be used to granularly allow or deny access just to a specific resource folder, device, or configurations

Device Management Permissions

These permissions control if any device actions like Shutdown, Restart or Refresh profile are allowed

Report Permissions

These permissions operate globally across the full system and are not limited to the resources of the appropriate resource group. You can either allow visibility of the Audit Report and Permission Report, or not.



Admin Resource Group

The Admin Resource group shows all the Resource Folder that have been created in the Device Portal

Admin Resource Folder

The admin resource folders denote the designated location for assigning various configurations option such as Devices and Device Groups, Profile Configuration settings, Authentication providers, Device Policies, and other related entities.

You can also add tags to a resource folder.

A “Search Tags” are value pairs parameters that enable you to categorize resources. Search Tags and Values are case-insensitive, and they are limited to 256 characters.

Admin User Groups

The Admin User group tab represent the list of the User having different permissions on different resources.

i.e.: Super Admin = Group for administrator with full permissions on all resources

Admin Users

The Admin Users Tab shows the list of all Users, local or connected via an Authentication Provider that logged in to the Device Portal.



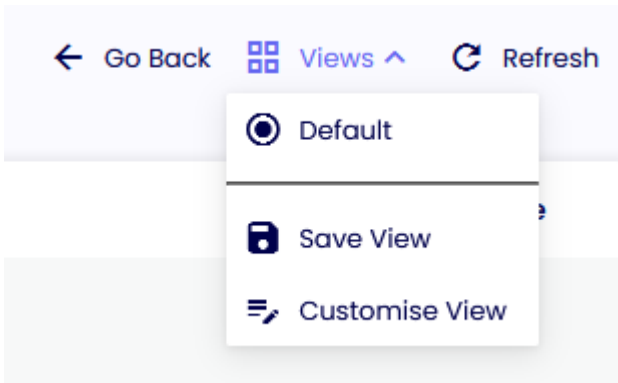
5. Devices

The Devices Tab is the collection of all the Devices registered within the Device Portal.

Row	Name	Online Status Overview	Last Heard From	IP Address Overview	Last IP Address (Country)
1	DESKTOP-9A22GM6	Offline 7/28/2023 9:08:26 PM	7/28/2023 9:08:26 PM	United Kingdom 82.9.170.78	78 (United Kingdom)
2	THINSCALE	Offline 7/31/2023 12:29:13 PM	7/31/2023 12:29:13 PM	Ireland 91.197.234.164	4.164 (Ireland)
3	THINSCALE	Offline 7/31/2023 4:21:18 PM	7/31/2023 4:21:18 PM	Ireland 91.197.234.164	164 (Ireland)
4	TSTWIN10PC	Offline 8/24/2023 3:08:22 PM	8/24/2023 3:08:22 PM	Ireland 91.197.234.164	1.164 (Ireland)

You can sort the Device using different views and filter.

To create a new View, click the “Views” button on the top right corner and then “Customise View”.



Select the filtering you want to apply, give it a name, and click Save.



6. Device Groups

The Device Groups is the main repository where all the Devices and Device Configuration are stored.

Inside the Device Group Information, you will find settings like Device Policy, TDA Update Policy, Auth Providers and more (See Point 7 for more info).

You will also be able to view all the Devices deployed within that Device Group.

Device Group Information

Name

Description

Resource Folder

General
▼

[🔗](#)

^ Device Policies

Device Policy

General Device Policy
▼

[🔗](#)



7. Configuration

The Configuration tab serves as the central repository for storing and managing all device settings, encompassing everything from Profiles and Software Packages to Virtual Disks. This is the primary location for configuring these settings.

Config Assignments

The Config Assignments tab is used to connect all the settings applied to the Devices and the Resource Folder where the Devices reside.

Row	Name	Resource Folder	Device Groups or User Groups	Device Profiles	Software Package Groups	Delete
1	General Configuration Assignment <small>Configuration Assignment for general use on the system</small>	General	General Device Group	General Device Profile	Support Software Package Group	

There are 2 modes:

^ Config Assignment Mode ⓘ

Config Assignment Mode

Device Group Assignment

User Assignment



Device Group Assignment: the settings are deployed to the Device without considering the User logged in to the machine.

i.e., User 1 and User 2 uses Machine 1, at different times, and they will both retrieve the same Device Profile

Device Groups

Name	Device Count	Device Policy	Auth Providers	Virtual Disks
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> </div> <div> General Device Group <small>Device group for general use on the system</small> </div> </div>	0	General Device Policy	-	-

[Select Device Groups](#)

Device Profiles

Name	Revision	General Profile	UI Profile	Security Profile	MDM Profile
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> </div> <div> General Device Profile <small>Device profile for general use on the system</small> </div> </div>	1	General Profile	UI Profile	Security Profile	MDM Profile

[Select Device Profiles](#)

Software Package Groups

Name	Software Packages
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 5px;"> </div> <div> Support Software Package Group <small>Support Software Package Group</small> </div> </div>	-

[Select Software Package Groups](#)

User Assignment: the settings are deployed to the Device based on the User logged in to the machine.

i.e., User 1 and User 2 uses Machine 1, at different times, and they will retrieve different profile based on their Auth Provider group. (the same profile will be delivered if they are part of the same group)

In order to use User Assignment an End User Groups needs to be created



Click on the “End User Groups” Tab and the “Add”

- Configuration
 - Config Assignments
 - Device Profiles
 - General Profiles
 - UI Profiles
 - Security Profiles
 - MDM Profiles
 - Device Policies
 - Software Packages
 - Software Packages Groups
 - Auth Providers
 - Virtual Disks
 - End Users
 - End Users Groups**

Give it a Name, a Description, pick a Resource Folder and Click Save

End User Group Information

Name

Description

Resource Folder



In the Auth Provider Groups, add the ID from the Azure Group which the user is part of.

^ Auth Provider Groups ⓘ

Auth Group ID	Description
291e5a42-d26b-425a-bc2a-23624f605bc4	Support Group

Id
Desc
Add

Every time a user that is part of that group logs in, the “End User Count” will automatically increase.

^ End Users

End User count (using End User Group)

1

Show End Users

If you click “Show End Users” you will see all the user authenticated against that Group ID

Row	Photo	Name	Last Login Date	Last Login Device	IP Address Overview
1		D	9/8/2023 3:42:47 PM	DESKTOP-QB7L1Q3	Ireland 10



Once done, go back to the Config Assignment, Select the End User Groups you just created and Click Save.

Select End User Groups

Administrator profile

Search... [Search] [Filter]

Go Back Views Refresh Save

Selected	Name	Resource Folder	Auth Group ID
<input checked="" type="checkbox"/>	Support End User Group Support End User Group	General	-

Config Assignment Mode

Assignment

User Assignment

^ End User Groups

Name	Auth Group ID
Support End User Group Support End User Group	-

Select End User Groups



Device Profiles

The Device Profiles Tab is used to assign all the settings from the 4 (General, UI, Security, MDM) different configurations with the Resource Folder.

Those settings will then be deployed to all Devices within that Resource Folder.

Device Profiles

Administrator profile

Search... [Go Back] [Views] [Refresh] [Add]

Row	Name	Resource Folder	General Profile	UI Profile	Security Profile	MDM Profile	Revision	Delete
1	General Device Profile Device profile for general use on the system	General	General Profile	UI Profile	Security Profile	MDM Profile	1	[Delete]

Device Profile Information

Name
General Device Profile

Description
Device profile for general use on the system

Resource Folder
General [Link]

Revision
1

Select Profiles

General Profile
General Profile [Link]

UI Profile
UI Profile [Link]

Security Profile
Security Profile [Link]

MDM Profile
MDM Profile [Link]



General Profiles

Below you will find the explanation of all the options within the General Profiles.

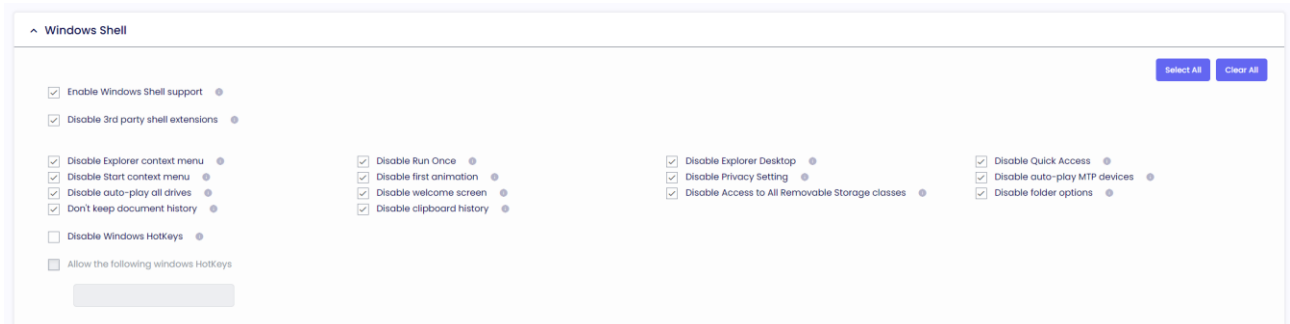
The screenshot displays the ThinScale web interface. On the left is a navigation sidebar with the following items: Dashboard, Organisation, Devices, Device Groups, Configuration, Config Assignments, Device Profiles, and General Profiles (highlighted in blue). The main content area is titled "General Profile" and features a search bar with a magnifying glass icon and a filter icon. Below the search bar is a table with the following content:

Row	Name
1	General Profile General profile for use on the system



Windows Shell

Below you will find the explanation of all the options within the Windows Shell Tab.



Enable Windows Shell support

If enabled, Windows Explorer process will be allowed to run.

Disable 3rd party shell extensions

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

Disable Explorer context menu

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

Disable Run Once

If enabled, machine and user run once will be disabled.

Disable Explorer Desktop

If enabled, the main desktop will be disabled.

Disable Quick Access

If enabled, Quick Access will be disabled inside the Explorer Tab.

Disable Start context menu

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



Disable first animation

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

Disable Privacy Setting

If enabled, the privacy settings will be disabled.

Disable auto-play MTP devices

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

Disable auto-play all drives

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

Disable welcome screen

If enabled, the Windows welcome experience will be disabled.

Disable Access to All Removable Storage classes

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

Disable folder options

If enabled, explore "Folder Options" will be disabled.

Don't keep document history

If enabled, all documents history will be deleted.

Disable clipboard history

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

Disable Windows Hotkeys

If enabled, all the windows hotkeys will be disabled.



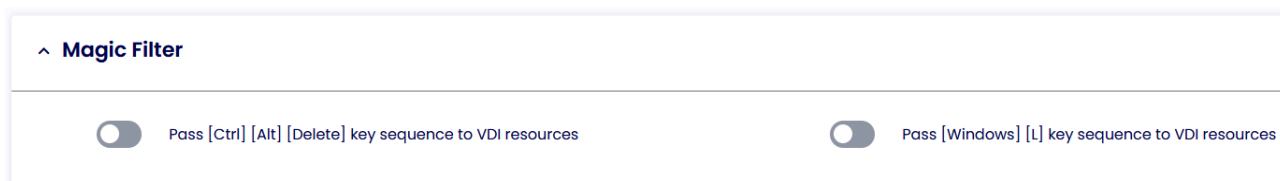
Allow the following windows Hotkeys

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



Magic Filter

Below you will find the explanation of all the options within the Magic Filter Tab.



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

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

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

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



Local Device Restrictions

Below you will find the explanation of all the options within the Local Device Restriction Tab.

Enable Command Prompt

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

Enable Task Manager

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

Enable Run Box Functionality

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

Enable Print Screen key

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



Enable Registry Tools

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

Enable access to all Computer's Settings

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

Select the Settings Items you want to show

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

Select the drives you want to show

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



Ctrl+Alt+Del Screen

Enable Ctrl+Alt+Del Screen

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

Enable Lock Workstation

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

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

Enable Restart

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

Enable Change Password

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

Enable Shutdown

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

Enable Fast User Switching

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

Enable Log Off

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



Logon Script

Below you will find the explanation of all the options within the Logon Script Tab.

^ Logon Script

Enable Logon Script Type

Run Logon Script visible to users Logon Script timeout (Secs)

Enable Login Script

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

Run Login Script Visible to users

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

Login Script Timeout

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



Logoff Script

Below you will find the explanation of all the options within the Logoff Script Tab.

^ Logoff Script

Enable Logoff Script

Run Logoff Script visible to users

Type BAT

Logoff Script timeout (Secs) 0

↻

Enable Logoff Script

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

Run Logoff Script Visible to users

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

Logoff Script Timeout

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



Additional Registry Values

Below you will find the explanation of all the options within the Additional Registry Values Tab.

^ Additional Registry Values
Apply

+ Add Item

No records to display.

Edit Registry Value
Apply

Enabled

Description

Registry Location

Registry Key

Value Name

Value Type

Value Data

With the TDA, you can add custom registry keys that are applied by the TDA engine and that are not persistent.

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

^ Additional Registry Values
Apply

+ Add Item

HKEY_LOCAL_MACHINE\SOFTWARE\ThinScale

Profile Test\Test

Edit Registry Value
Apply

Enabled

Description

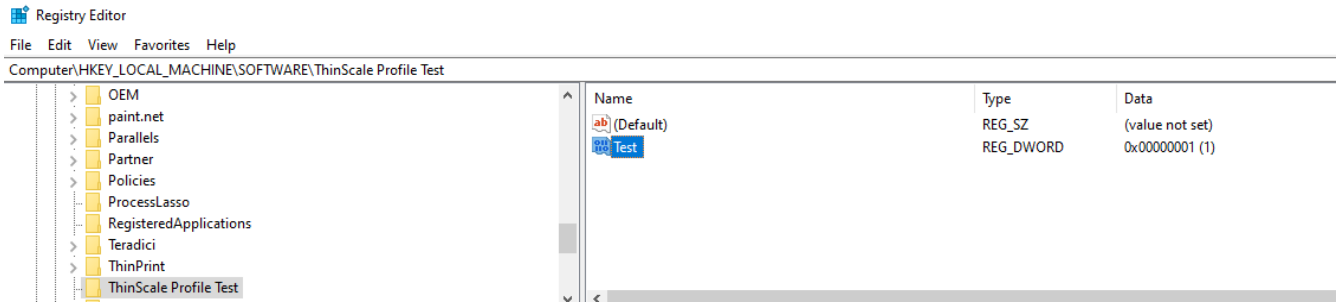
Registry Location

Registry Key

Value Name

Value Type

Value Data



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



Session Timers

^ **Session Timers**

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

Log Off Restart Shutdown Lock

Perform the following action when the device is idle for

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



Lock Screen

^ Lock Screen

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

- Use LDAP Auth Provider password if available
- Require complex password
- Minimum password length

Session Password

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



Create a session password

A session password is unique to you and this secure session and will be required to unlock this device

Password

Confirm Password

OK

Cancel



Thinscale Virtual Desktop Agent

^ Thinscale Virtual Desktop Agent

Enable Virtual Desktop support

- Don't send battery information
- Don't send Wi-Fi information
- Don't send device inventory data
- Update the device name in the Management Console to the VDI session username * ThinScale VDA 1.2 and above
- Include the domain name

Enable Virtual Desktop Agent support

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



Windows Proxy

^ **Windows Proxy**

Proxy Settings **Advanced Internet Settings**

Apply Proxy Settings

Auto Configuration

Automatically detect settings

Use automatic configuration script

Address

Proxy Server

Use a proxy server

Address Port

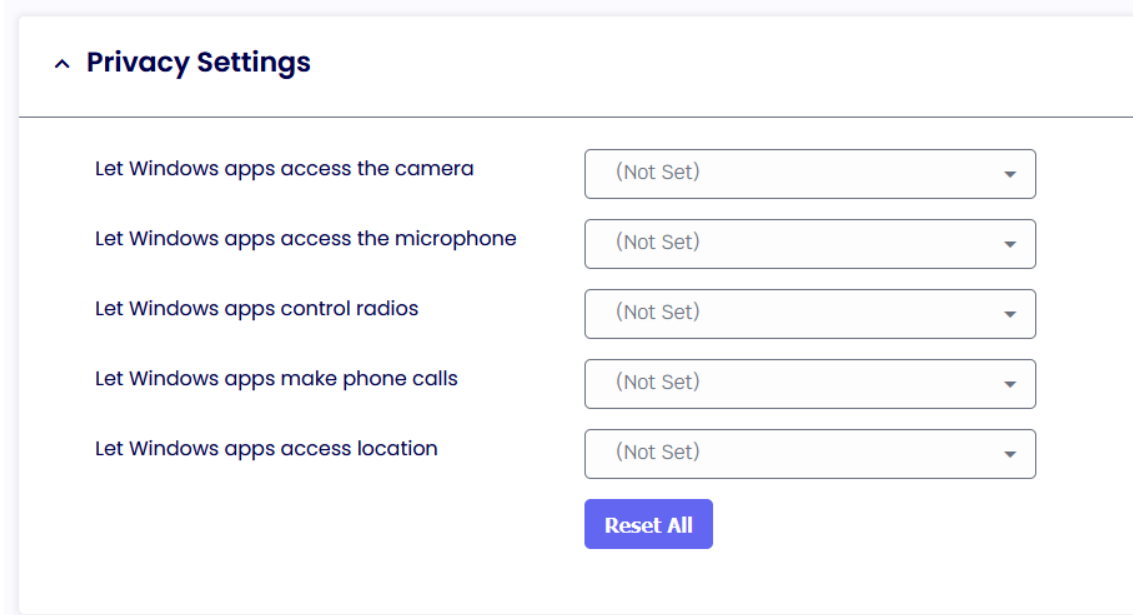
Use the proxy server except for addresses starts with the following entries. Use semicolon (;) to separate entries.

This Tab follows the standard Windows Proxy settings.

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

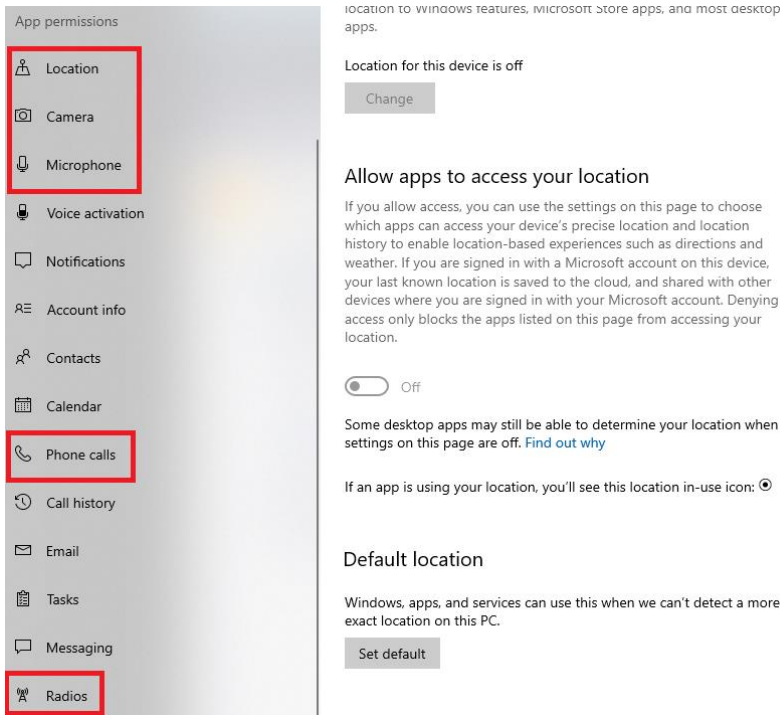


Privacy Settings



Privacy Settings in Windows 10/11 can be accessed by going into Settings / Privacy / App Permissions.

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





UI Profiles

Below you will find the explanation of all the options within the UI Profiles options

Row	Name
1	UI Profile UI profile for general use on the system

User Interface

Select the user interface that will be used:

ThinScale Launch Pad
 Windows Shell

ThinScale Launch Pad

If selected, this will launch the TDA UI automatically and the entire user windows desktop will be inaccessible

Windows Shell

If selected, the user will see the user desktop, but policy/ restrictions may still be applied.



Profile Data Repository

The profile data repository contains all data shared across the user interface, like Custom application, Website, Network Drives and Remote Desktop & Apps.

^ Profile Data Repository

General Custom Applications Remote Application Mapped Network Drives WebSites Auto Launch

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

Name	Value
Custom Applications	0
Remote Applications	0
Mapped Network Drives	0
Websites	0
Auto Launch Items	0

Custom Applications

To create a custom application, click the + symbol on the right panel.

Give it a name, command line and the Start in path if you wish.

Click Apply

^ Profile Data Repository

General Custom Applications Remote Application Mapped Network Drives WebSites Auto Launch

Name	Type	Visibility	Auto Launch	+
				+



Repeat the same for the Remote Application, Network Drives and Website if you need them.

[Apply](#)

Display Name

Visibility Option

Command Line

Start In

Arguments

Windows Style

Custom Icon

Windows Store App

Auto Launch when UI launches

Automatically re-launch the application when it closes



Remote Application

Apply

Display Name:

Vmware

Visibility Option:

Always Show

Connection Type:

VMware Horizon Connection

--serverURL="https://t: al/broker/xml"

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

Import



Auto Launch when UI launches

Mapped Network Drives

Apply

Display Name:

Dev

UNC Path:

\\server\Path

Custom Icon:

Visibility Option:

Always Show

Preferred volume driver letter:

R:



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



Auto Launch when UI launches



Use LDAP Auth Provider credentials if available



Watermarking

^ Watermarking			
Name	Type	Visibility	
			Add Text Watermark Add Image Watermark

The new TDA supports multiple watermarking and multiple types: Text and Image

To add a Text watermarking click “Add Text Watermarking”.
Give it a name, text and apply all the style that you wish.

Watermark Name:

Watermark Text:

Text Size: **Text Color:**

Display Mode:

Transparency: 8 %

Use Background Color:

Alignment **Offset X:** **Offset Y:**

<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="X"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>



To add an Image watermarking click “Add Image Watermarking”.

Give it a name, specify the image path location, and apply all the style that you wish.

Watermark Name:

Image Filename:

Display Mode:

Transparency: 63 %

Use Background Color:

Alignment

<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="text" value="0"/>	<input type="text" value="X"/>	<input type="text" value="0"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Offset X:

Offset Y:

Please note: When specify the image path, make sure that the image exists on the TDA device.

Watermark text

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



Image Filename

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

Display Mode

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

Transparency

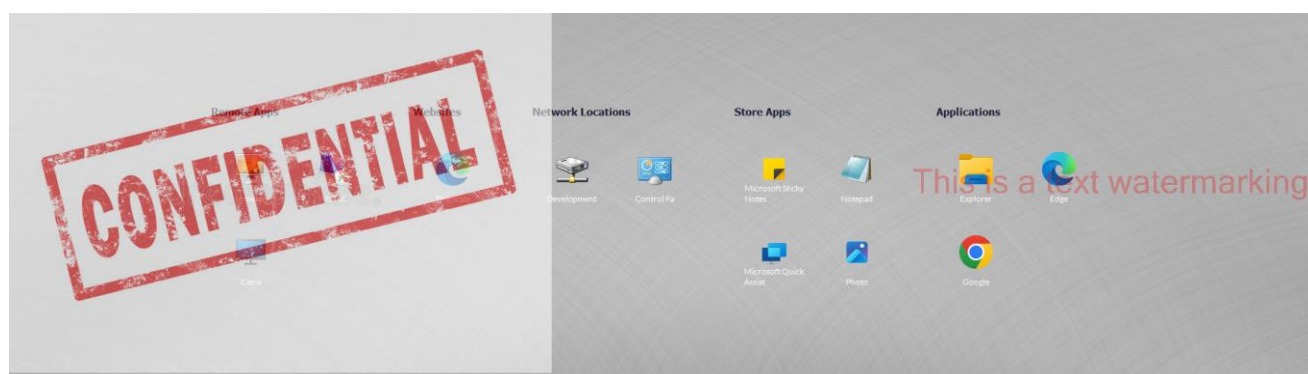
It is the transparency's value of the text/image displayed within the TDA desktop.

Use Background Color

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

Alignment

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





Appearance

General

^ Appearance

General Ribbon Toolbar Layout Pinned Applications Pinned Website Links Status Bar Layout

Custom Title

Theme
Grey Show UI maximised on launch

Window percent
85 Do not allow window resizing

Language

Use USA flag for English Use Swiss flag for German

Retain user's last language preference Enforce language

Custom Title

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

Theme

Sets the theme TDA UI will use.

Show UI Maximised on launch

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



Window Percent

Set's the size of the TDA UI.

Do not allow window resizing

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

Use USA flag for English

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

Use Swiss flag for German

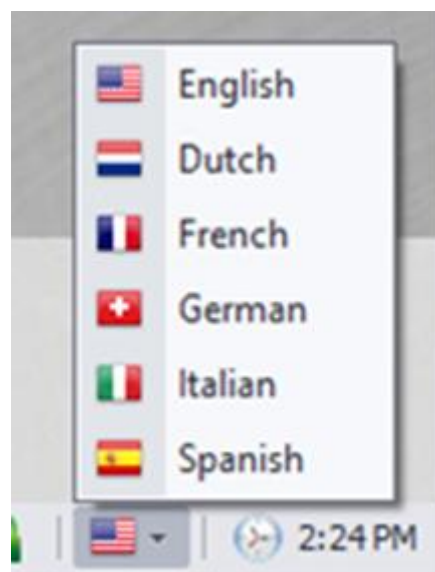
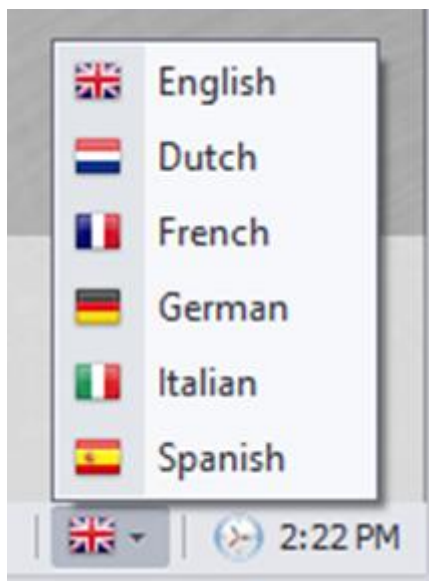
Switches the Swiss flag icon in language selection for the German language.

Retain Users Last Language Preference

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

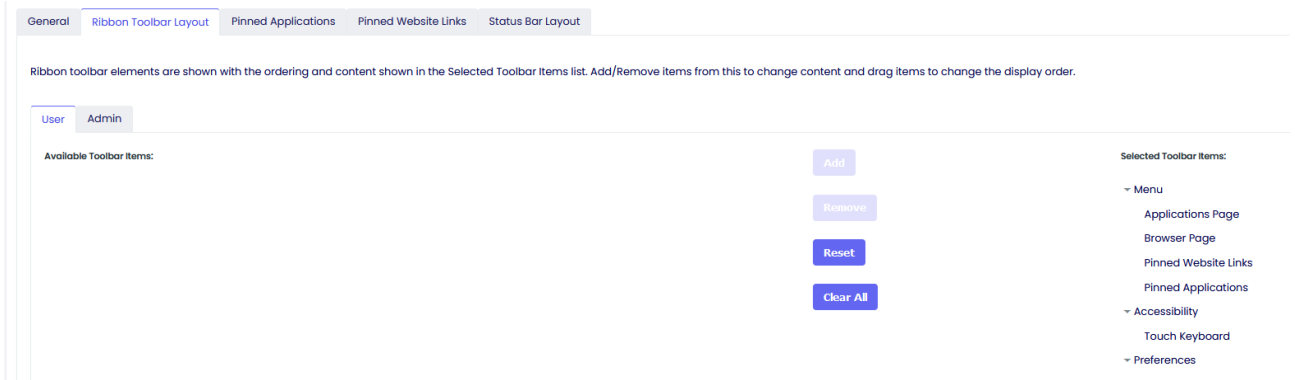
Enforce Language

Forces TDA to use the selected language.



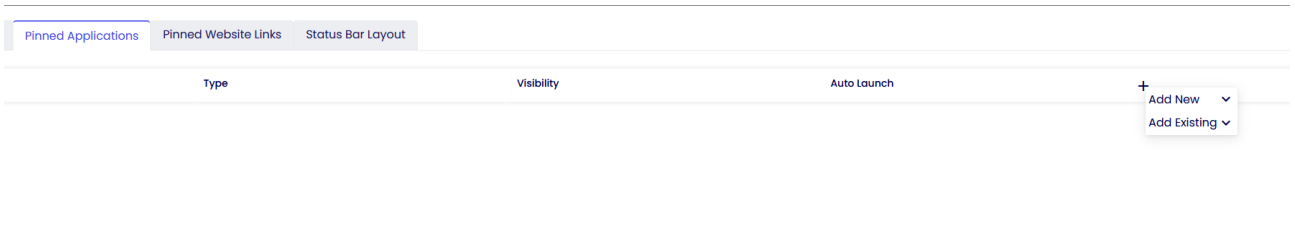


Ribbon Bar Layout

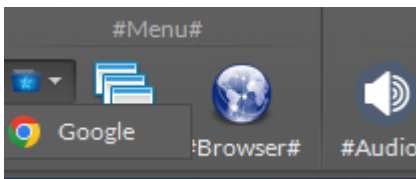


Ribbon toolbar elements are shown with the ordering and content shown in the Selected Toolbar Items list. Add/Remove items from this to change content and drag items to change the display order.

Pinned Applications and Website links



Pinned Application and Website Links are displayed on the TDA Ribbon Bar when enabled. You can either create a new one or use an existing from the Profile Data Repository. When the TDA will be launched, you will be able to see them here.





Status Bar Layout

General Ribbon Toolbar Layout Pinned Applications Pinned Website Links **Status Bar Layout**

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

<p>Available Toolbar Items:</p> <ul style="list-style-type: none"> Applications Page Browser Page Bluetooth Audio Device 	<p>Add Left</p> <p>Add Right</p> <p>Remove</p> <p>Reset</p> <p>Clear All</p>	<p>Selected Toolbar Items:</p> <ul style="list-style-type: none"> ~ Left Aligned Content ~ Right Aligned Content Date/Time Settings Battery Status Network Status Admin Unlock Language Selection Clock
--	---	--

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





Applications

General

^ Applications

General Application Desktop

Enable Applications

Use Apps Icon Caption

Background Appearance

Action Default Wallpaper Solid Colour Custom Wallpaper

Solid Colour

Custom Wallpaper

Tile Appearance

Text Colour Revert to Default

Hide Tile Group Title Text

Enable Application

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

Use Apps icon caption

Provides a caption to use for the applications tab icon.

Background Appearance

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



Tile Appearance

Text Colour

The colour of the application's text name.

Hide Tile Group Title Text

Hides the group headings in the applications tab.



Application Desktop

Applications

General Application Desktop

Name	Type	Visibility	Auto Launch		+		
Apps		Always Show			+		
Notepad	Custom Application	Always Show					
Google	Custom Application	Always Show					
Explorer	Custom Application	Always Show					
Thunderbird	Custom Application	Always Show					
VMWare	Custom Application	Always Show					
Mapp		Always Show			+		
Share	Mapped Network Drive	Always Show					
Website		Always Show			+		
TST	Website	Always Show					
Remote APPS		Always Show			+		
Citrix	Remote Application	Always Show					

In the Application Desktop Tab, you will be able to create an Application Desktop Group, Web sites Group, Remote Applications Group and more



Apply

Display Name

Visibility Option

Command Line

Start In

Arguments

Windows Style

Custom Icon

Windows Store App

Auto Launch when UI launches

Automatically re-launch the application when it closes

Windows Store App

Please follow [this article](#) to add a windows store App

Auto launch when UI launches

If enabled, the application will automatically launch when the TDA is initialised

Automatically re-launch the application when it closes

If enabled, the application will automatically relaunch if the user closes the application.



Secure Browser

Secure Browser

General | Browser Toolbar Layout | Websites Links | URI Filtering Rule General | URI Filtering Rule Groups | URI Filtering Rules

Enable the Enterprise Secure Browser

Use browser caption: Nearsol Links

Override user agent string

Proxy server control: None

Home Page:

<input checked="" type="checkbox"/> Disable non HTTP(s) URIs	<input type="checkbox"/> Disable Context Menus	<input checked="" type="checkbox"/> Disable Internal Edge// URIs	<input checked="" type="checkbox"/> Disable Web Capture
<input checked="" type="checkbox"/> Disable General Autofill	<input checked="" type="checkbox"/> Disable Downloads	<input checked="" type="checkbox"/> Disable Share	<input checked="" type="checkbox"/> Disable Password Autosave
<input checked="" type="checkbox"/> Disable History	<input checked="" type="checkbox"/> Disable Save	<input checked="" type="checkbox"/> Disable Scripts	<input type="checkbox"/> Disable Host Objects
<input checked="" type="checkbox"/> Disable Copy	<input type="checkbox"/> Disable Status Bar	<input checked="" type="checkbox"/> Disable Printing	<input type="checkbox"/> Disable Script Dialogs
<input type="checkbox"/> Disable Permission Requests	<input checked="" type="checkbox"/> Disable Dev Tools	<input type="checkbox"/> Disable Web Messages	

Select All | Clear All

Enable the Enterprise Secure Browser

If enabled, the browser will be opened inside the TDA UI

Use browser icon caption

Provides a caption to use for the browser tab icon

Override user agent string

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

i.e.

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

Proxy server control

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



VDI Control

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

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

Clear browsing data after Citrix Web Interface/ Storefront logoff

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

Browser Toolbar Layout

^ Secure Browser

General | **Browser Toolbar Layout** | Websites Links | Url Filtering Rule General | Url Filtering Rule Groups | Url Filtering Rules

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

Available Toolbar Items:

Add

Remove

Reset

Clear All

Selected Toolbar Items:

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

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



Website Links

Apply

Website Label:

Google

Website URL:

https://google.com

Include http:// or https://

Custom Icon:

Visibility Option:

Always Show

Start Option:

Use Secure Brower



Auto Launch when UI launches



Url Filtering Rule General

^ **Secure Browser**

General Browser Toolbar Layout Websites Links **Url Filtering Rule General** Url Filtering Rule Groups Url Filtering Rules

Enable Url Filtering

Passive mode

Enabled rule logging

Default Action

Allow ▼

Active Rule Group

▼

Default Action

The Default action is used to either whitelist (Allow) or Blacklist (Block) if any website browsed from the user are not found in the Url Filtering Rules.

In the case where you would like to **Block ALL** website and only allow some of them, your default action should be set to Block, and the Url Filtering Rules will be set to Allow

If on the other hand, you want to **Allow ALL** and only block certain website considered “dangerous”, your default action should be set to Allow, and the Url Filtering Rules will be set to Block



Active Rule Groups

The active rule group is used to group together URLs of the same category for example.

i.e., Google group may have all G-Suite URLs

Finance group may have access to Workday URLs and so on

To Create a Rule Group, give it a name and a description and click Apply

Uri Filtering Rule Groups | Uri Filtering Rules

Cancel **Apply**

Group Name
ThinScale Group

Description
ThinScale allowed websites

Browse the Uri Filtering Rules now. Switch the Enabled button, add a website with the preferred rule and click Apply.

Secure Browser

General | Browser Toolbar Layout | Websites Links | Uri Filtering Rule General | Uri Filtering Rule Groups | **Uri Filtering Rules**

ThinScale

Enabled

Name
ThinScale

Action
Allow

Uri Contains thinscale.com

Cancel **Apply**



Enabled Cancel Apply

Name
Citrix

Action
Allow

Host

Uri **Is** **Value** **Description** +

Once done, go back to your Rule Group, select the newly created Rule, and click Apply

Uri Filtering Rule Groups **Uri Filtering Rules** Cancel Apply

Group Name

Description

	Name	Enabled
<input checked="" type="checkbox"/>	ThinScale	True



Original string (e.g., the original string of the URL

<http://www.contoso.com:80//thick%20and%20thin.htm> is

<http://www.contoso.com//thick and thin.htm>

Scheme (e.g., https)

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

thinscale.com

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

Query (e.g., the query of the URL

<http://www.contoso.com/catalog/shownew.htm?date=today> is ?date=today

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



Security Profiles

Below you will find the explanation of all the options within the Security Profiles options

Security Profile

Search... 🔍 ⌵

Row	Name
1	Security Profile Security profile for general use on the system



Dual Persona

^ Dual Persona

Enabled Dual Persona

Volume Size

2 GB

Volume Label

ThinScale Dual Persona

Preferred volume drive letter

B:

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

Enable Dual Persona

Dual Persona lets you move the TDA local windows user profile away from the local hard drive of the personal device (C:\Users) to an encrypted virtual volume.

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

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

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

**Volume Size**

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

Volume Label

Specify the formatted volume label of the Dual Persona volume

Preferred Volume Drive Letter

Select the drive letter that will be assigned to the Dual Persona Volume

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

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



Temporary Storage

^ Temporary Storage

Enabled Temporary Storage

Volume Size

Volume Label

Preferred volume drive letter

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

Enable Temporary Storage

Temporary Storage lets you create a temporary encrypted virtual volume on the personal device that users can use to save data from within the TDA session. The encrypted virtual volume is managed by TDA and is only made available when the TDA is active.

Volume Size

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



Volume Label

Specify the formatted volume label of the Temporary Storage volume

Preferred Volume Drive Letter

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

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

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

Please Note: in order to have the DP and TS drives available within the TDA session a local path need to be created within the UI Profiles > Application tab

like so:

[Apply](#)

Display Name
Dual Persona

Visibility Option
Always Show

Command Line
C:\Windows\explorer.exe

Start In

Arguments
S:

Windows Style
Normal

Custom Icon

Local device restrictions need also applying General Profiles > Local Device Restrictions like so:

Select the drives you want to show

<input type="checkbox"/> A	<input type="checkbox"/> B	<input type="checkbox"/> C	<input type="checkbox"/> D	<input type="checkbox"/> E	<input type="checkbox"/> F	<input checked="" type="checkbox"/> G	<input type="checkbox"/> H	<input type="checkbox"/> I	<input type="checkbox"/> J	<input type="checkbox"/> K	<input type="checkbox"/> L
<input type="checkbox"/> M	<input type="checkbox"/> N	<input type="checkbox"/> O	<input type="checkbox"/> P	<input type="checkbox"/> Q	<input type="checkbox"/> R	<input checked="" type="checkbox"/> S	<input checked="" type="checkbox"/> T	<input type="checkbox"/> U	<input type="checkbox"/> V	<input type="checkbox"/> W	<input type="checkbox"/> X
<input type="checkbox"/> Y	<input type="checkbox"/> Z										

[Select All](#) [Clear All](#)



Access Policies

^ Access Policies

General
Access Policy Rule Groups
Access Policy Rules
Windows Update Settings
Network

Enabled Access Policies

Passive mode

Enabled rule logging

Start Rule Group

Disabled
▼
+

Repeat Rule Group

Disabled
▼
+

Repeat checks every

1
▲
▼

Minutes

Enable Access Policies

If enabled, the Administrator can create a list of requirements that a candidate must Pass in order to fully launch the TDA client.

Note: a "Continue" rule can also be created to let the user in the session even if they don't meet the requirements.

Passive mode

If enabled, any Access Policies that failed execution will be ignored.



Enable rule logging

If enabled, the administrator will be able to retrieve more information about the Access Policies from the TDA log file.

Start Rule Group

If enabled, the Access Policies in this group will only be executed during TDA startup.

Repeat Rule Group

If enabled, the Access Policies in this group will be executed also while in the TDA session.

Repeat check every

If enabled, the Access Policies in the repeat group will be reevaluated every x minutes.

Please Note: All these groups can be enabled at the same time.

⚙️

Checking your device compliance

is64bit	✔️ Pass	
download	⚠️ Warning	Learn more
upload	⚠️ Warning	Learn more
32bit	❌ Failed	Learn more

Continue



Windows Update Settings

^ Access Policies

General Access Policy Rule Groups Access Policy Rules **Windows Update Settings** Network

Only updates older than days

Only definition updates older than days

Ignore the following updates [View ignore list](#)

Only include the following updates [View include list](#)

Ignore 3rd party driver updates

Only updates older than

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

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

Only definition updates older than

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

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



Ignore the following updates

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

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

Only include the following updates

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

Ignore 3rd party driver updates

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



Network

^ **Access Policies**

General
Access Policy Rule Groups
Access Policy Rules
Windows Update Settings
Network

Perform download test for seconds

Perform upload test for seconds

latency / Jitter Test

Hostname

Perform TCP ping

Port

Hostname

Specify the hostname you would like to use to perform ma ping request.



Process Security

General

Process Security

General | Process Security | Process Sets | Process Identity Rules | Module Protection Rules | Module Identity Rules | Object Protection Rules | Volume Protection Rules | Registry Protection Rules | Registry Overlay Rules

Disable Process Security and All System Protections

Enable Process Security

Passive Process Creation

Passive Volume Restrictions

Block the process if it does not match any of the rules configured in the Process Security tab

Passive Module Loading

Passive Process Object Restrictions

Enabled rule logging

Passive Registry Restrictions

Disable Process Security and All System Protections

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

A restart is needed when applied.

Disabling this option is only recommended for troubleshooting.

Enable Process Security

if enabled,

Passive Rules (All)

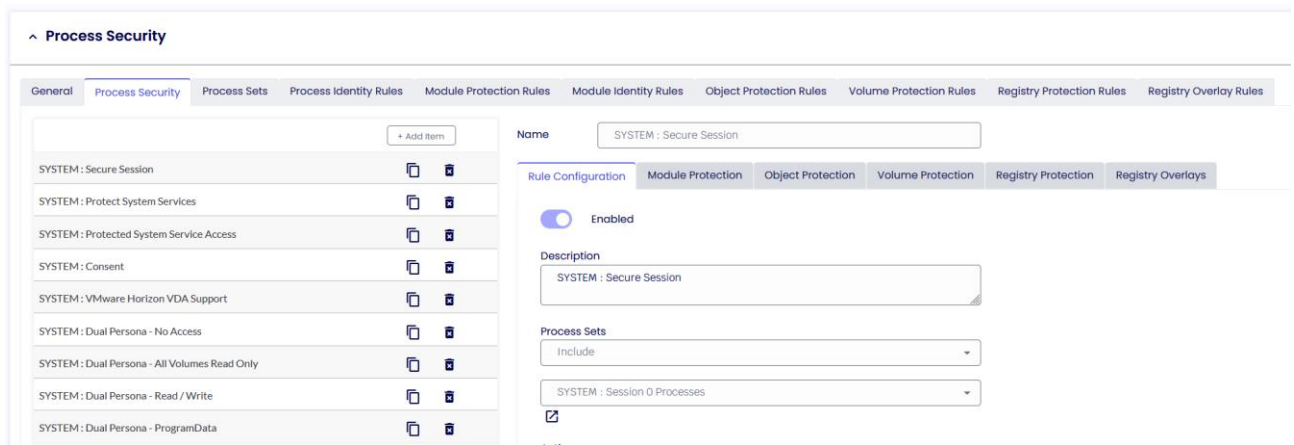
If enabled, any of the Process Security function (Volume, Module, Registry, etc) will be ignored.

Enable rule logging

If enabled, the administrator will be able to retrieve more information about the Process Security engine from the TDA log file.



Process Security



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

From the beginning, the Cloud Device Portal will be populated with “Default System Rules”. It is recommended that user unfamiliar with the Process Security Engine don’t delete these rules.

Deletion of these rules will impact the TDA operation

Process Security contains the list of all the Rule, either System or Custom.

Process Security Sets is the container where all the Process Security Identity are created.

Process Security Identity Rules is the container where you set all the processes identity for the specified process you want to Allow/ Block

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

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



Enabled

Name

Certificate Trusted
 And Certificate Issued To

Parent Process Rule:

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

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

Enabled

Name

Image Name

Secondly, we want to allow 2 possible file sizes as either of the 2. To do this we add another condition to test the file size as shown below.

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



Enabled

Name

TOOLS IDENTITY : Calculatorx

<input checked="" type="checkbox"/>		Image Name	Is	calc.exe
<input checked="" type="checkbox"/>	And	File Size	Is	27648
<input checked="" type="checkbox"/>	Or	File Size	Is	25432

Parent Rule

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

Enabled

Name

SYSTEM IDENTITY : Windows Updates

<input checked="" type="checkbox"/>		Microsoft Signed Binary	Is	True
<input checked="" type="checkbox"/>	And	File Description	Is	UsoClient
<input checked="" type="checkbox"/>	Or	File Description	Is	Windows Update
<input checked="" type="checkbox"/>	Or	File Description	Is	MoUSO Core Worker Process
<input checked="" type="checkbox"/>	Or	File Description	Is	App Uri Handlers Registration Verifier
<input checked="" type="checkbox"/>	Or	File Description	Is	Device Census
<input checked="" type="checkbox"/>	Or	File Description	Is	Host Process for Windows Tasks

Parent Process Rule:

<input checked="" type="checkbox"/>		Microsoft Signed Binary	Is	True
<input checked="" type="checkbox"/>	And	Is Session 0	Is	True
<input checked="" type="checkbox"/>	And	Is Service	Is	True
<input checked="" type="checkbox"/>	Or	Service Name	Is	wuauserv
<input checked="" type="checkbox"/>	Or	Service Name	Is	UsoSvc
<input checked="" type="checkbox"/>	Or	Service Name	Is	Schedule
<input checked="" type="checkbox"/>	Or	Service Name	Is	DcomLaunch



Enable Process Security

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

Passive modes

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

Enable rule logging

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

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

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



Process Sets

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

Name	Enabled
<input type="checkbox"/> SYSTEM IDENTITY: User Session Processes	True
<input checked="" type="checkbox"/> SYSTEM IDENTITY: Session 0 Processes	True
<input type="checkbox"/> SYSTEM IDENTITY: TDA Processes	True
<input type="checkbox"/> SYSTEM IDENTITY: Trusted Process	True

Action

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

System Priority

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

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

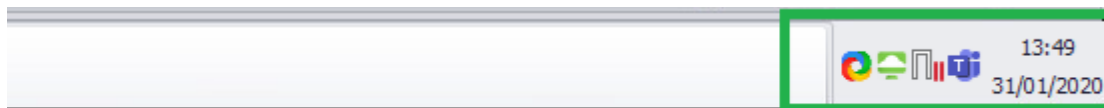
Priority

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



Systray Injection

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



Process Identity

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



Module Protection Rules

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

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

Enabled

Name

TOOLS MODULE IDENTITY : Google



Image Name

Ends With

chrome.dll





Object Protection Rules

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

More information can be found [here](#) or [here](#).

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

Enabled

Rule Name
SYSTEM OBJ : Consent Access

Description
SYSTEM : Consent Access

Include Target Process Set
Include

SYSTEM SET: AppInfo Service

Allow Process Access Rights

<input checked="" type="checkbox"/> Terminate	<input type="checkbox"/> Create Thread	<input type="checkbox"/> Set Session ID	<input type="checkbox"/> VM Operation	<input checked="" type="checkbox"/> VM Read	<input checked="" type="checkbox"/> VM Write
<input checked="" type="checkbox"/> Duplicate Handle	<input type="checkbox"/> Create Process	<input type="checkbox"/> Set Quota	<input type="checkbox"/> Set Information	<input type="checkbox"/> Query Information	<input type="checkbox"/> Suspend / Resume
<input checked="" type="checkbox"/> Query Limited Information	<input checked="" type="checkbox"/> Set Limited Information	<input checked="" type="checkbox"/> Synchronize			

Allow Thread Access Rights

<input checked="" type="checkbox"/> Terminate	<input type="checkbox"/> Suspend / Resume	<input type="checkbox"/> Alert	<input type="checkbox"/> Get Context	<input type="checkbox"/> Set Context	<input type="checkbox"/> Set Information
<input type="checkbox"/> Query Information	<input type="checkbox"/> Set Thread Token	<input type="checkbox"/> Impersonate	<input type="checkbox"/> Direct Impersonation	<input checked="" type="checkbox"/> Set Limited Information	<input checked="" type="checkbox"/> Query Limited Information
<input type="checkbox"/> Resume	<input checked="" type="checkbox"/> Synchronize				

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



Enabled

Name

SYSTEM : Consent Process

		Microsoft Signed Binary	Is	True
	And	Is Session 0	Is	False
	And	File Description	Is	Consent UI for administrative applications

Parent Process Rule:

		Microsoft Signed Binary	Is	True
	And	Is Session 0	Is	True
	And	Is Service	Is	True
	And	Service Name	Is	AppInfo

If the process running on the machine doesn't match these rules, then the Object protection rules will be denied.



Volume Protection Rules

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

Volume Type

All Volumes ▼

Local System Drive

Local Volume

Network Location

USB Mass Storage Device

All Volumes

Enabled

Rule Name

Description

Volume Type

All Volumes ▼

Volume Path

Allow Volume Access Rights

Read
 Execute
 Write



In the above example, you can see the rule applying a “Read Only” access right rule to all the Volumes. Meaning that no process in the system will be able to write on disk.

In the next example, however, you can see that the Dual Persona Volume has full access to write and read within the Dual Volume itself.

Enabled

Rule Name

SYSTEM : Dual Persona - Read / Write

Description

SYSTEM : Dual Persona - Read / Write

Volume Type

Dual Persona ▼

Volume Path

\

Allow Volume Access Rights

Read

Execute

Write



Registry Protection Rules

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

More information can be found [here](#).

ps
Module Identity Rules
Object Protection Rules
Volume Protection Rules
Registry Protection Rules
Registry Overlay Rules

Cancel Apply

Enabled

Rule Name

Description

Base Key

Subkey

Allow Registry Access Rights

<input type="checkbox"/> Query Value	<input type="checkbox"/> Set Value	<input type="checkbox"/> Create Subkey	<input type="checkbox"/> Enumerate	<input type="checkbox"/> Notify	<input type="checkbox"/> Create Link
<input type="checkbox"/> Write	<input type="checkbox"/> Read	<input type="checkbox"/> Full Access			



Registry Overlay Rules

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

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

Enabled

Rule Name

SYSTEM : Dual Persona - Program Data

Description

SYSTEM : Dual Persona - Program Data

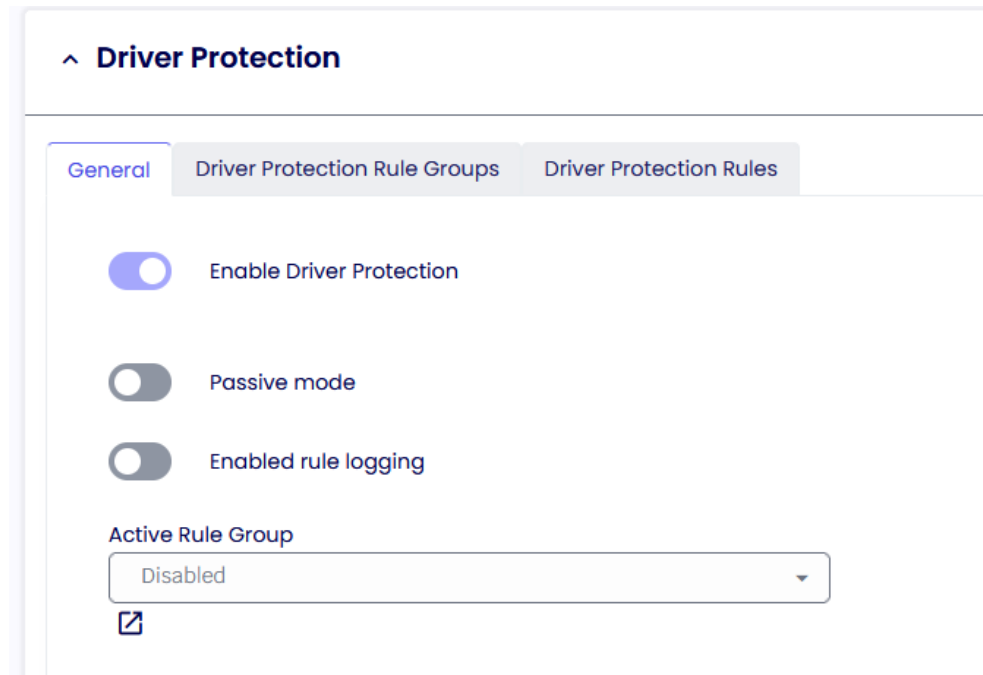
Registry Value	Value Type	Value Data	Enabled	+
ProgramData	REG_SZ	%OV_DPDRIVE%ProgramData	True	
ProfilesDirectory	REG_SZ	%OV_DPDRIVE%Users	True	



Driver Protection

Driver Protection provides functionality to blacklist Windows drivers.

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



Passive Rules

If enabled, any of the Driver Protection Rule will be ignored.

Enable rule logging

If enabled, the administrator will be able to retrieve more information about the Driver Protection Rule from the TDA log file.



Enabled

Name

Ctxusbmon

Action

Terminate SWA Service



Image Name

Ends With

\\ctxusbmon.sys



i.e., if during TDA operation, the Citrix drives will be found loaded on the system the TDA will not run.

When a driver is loaded on the system, there is very little the TDA can do to unload it, so to prevent any “potential” bad drivers from performing any malicious activity, the TDA will simply stop its operation completely.



Service Protection

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

Service Protection has 4 areas of operation:

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

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

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

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



^ Service Protection

General | Service Protection Rule Groups | Service Protection Rules

Enabled Service Protection

Passive mode

Enabled rule logging

Start Rule Group

Disabled

Close the session if any actions cannot be applied

Session Start Group

Session Start Actions

Close the session if any actions cannot be applied

Repeat Rule Group

Disabled

Close the session if any actions cannot be applied

Repeat checks every Minutes

Logout Rule Group

Disabled

Passive Rules

If enabled, any of the Service Protection Rule will be ignored.

Enable rule logging

If enabled, the administrator will be able to retrieve more information about the Service Protection Rule from the TDA log file.

Close the session if any actions cannot be applied

If enabled, the TDA will close the session if actions created in the Service Protection Rules list cannot be applied.



Service Protection builds on existing Process Security technology to provide Windows services execution control at the system level. Using familiar concepts from Process Security Identity, an administrator can define rules for a profile to control what services can run or should be stopped. As with Process Security Identity, control is asserted overall service applications including all Windows services.

Enabled

Name

Restart VMware Horizon Client Service

Action

Restart



Service Name

Is

client_service






MDM Profiles

Below you will find the explanation of all the options within the MDM Profiles options

The screenshot shows the 'MDM Profile' management page. On the left is a navigation sidebar with the following items: Dashboard, Organisation, Devices, Device Groups, Configuration, Config Assignments, Device Profiles (with sub-items: General Profiles, UI Profiles, Security Profiles), and MDM Profiles (highlighted in blue). The main content area is titled 'MDM Profile' and features a search bar with a magnifying glass icon and a filter icon. Below the search bar is a table with the following data:

Row	Name
1	 MDM Profile MDM profile for general use on the system



Windows Firewall Control

Windows Firewall Control

General Firewall Rules

Enable Windows Firewall Control

Firewall State
On

Inbound connections
Block

Outbound connections
Allow

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

Disable all existing firewall rules

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

Reapply firewall settings while running (recommended) Every(Mins): 15

Apply custom firewall rules

Enable Windows Firewall Control

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

Firewall state

Turns the Windows Firewall on or off.

Inbound connections

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

Outbound connections

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



Disable all existing rules

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

Hide notifications when a program is blocked from receiving inbound connections

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

Reapply firewall setting while running

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

Apply Custom firewall rules

Create custom rules for inbound and outbound traffic.

Enabled

Network Profile Public Private Domain All

Direction Inbound Outbound

Name:

Action All programs This program path:

Protocol type

Local Port

Remote Port


Local IP addresses






Remote IP addresses

Action Allow Block




Device Policies



-  **Dashboard**
-  **Organisation**
-  **Devices**
-  **Device Groups**
-  **Configuration**
- Config Assignments**
- Device Profiles**
 - General Profiles
 - UI Profiles
 - Security Profiles
 - MDM Profiles
 - Device Policies

Device Policy

🔍
⌵

Row	Name
1	 General Device Policy Device Policy for general use on the system

Device Policies contains the comprehensive configuration settings required for our latest TDA client.

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



Operating Mode

Device Policy Configuration

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

Operating Mode

Select the mode the Secure Worker Agent will operate in:

Operating Mode 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.

User Initiated (SRW)

This mode is useful for BYOD that are not company owned. The user will have to manually click the TDA icon before commencing its operation.

Always on (TK)

This mode is useful for corporate devices connected to the corporate network or joined to the company domain.

The TDA UI will automatically launch after machine boot up and access to the underlying OS will be restricted.

If operating using Windows Shell, the UI will not launch automatically but all the security restriction will be still applied in the background.



Device Login Options

Device Login Options

Use Local Managed Account
 Use Custom Account
 Dont Auto Login
 Do Nothing

Login Options

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 'TDA' created by the TDA. 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

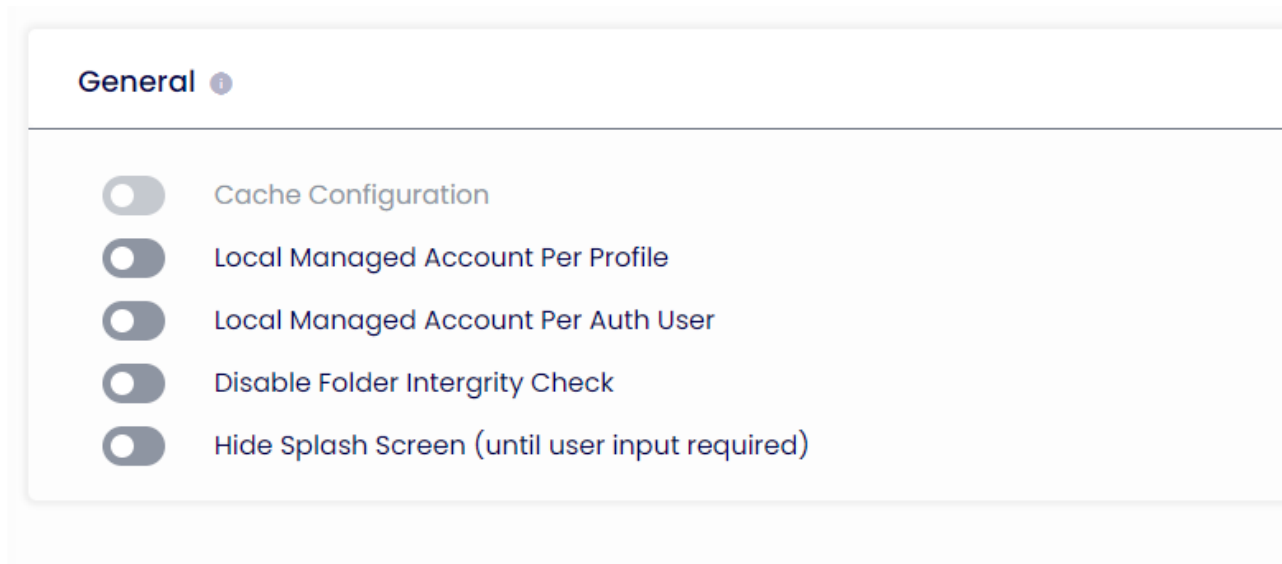
Prevents the left shift key from overriding the auto-login configuration.

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



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 the TDA, you can effortlessly configure custom splash screen images and personalized desktop icons directly through the Device Portal. Simply upload your desired image within the device policy, use a .ico file for the desktop shortcut, and your customization is complete.

Startup Script

Device Policy Configuration

- Device Policy
- Branding
- Shortcuts
- Startup Script**
- Device Settings
- Administration
- Authentication

Enable Startup Script

Type: PS

Startup Script timeout: 0 (seconds)

```
$keyPath = "HKLM:\SOFTWARE\Google\Chrome"  
$valueName = "Google Test"  
$valueData = "Web1"  
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 Policy Configuration

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."

Device Events

The screenshot shows the 'Device Policy Configuration' interface. At the top, there are tabs for 'Device Policy', 'Branding', 'Shortcuts', 'Startup Script', 'Device Settings' (which is active), 'Troubleshooting', 'Administration', and 'Authentication'. Below the tabs, there is a section titled 'Device Event' with two radio button options: 'Enable Device Event Collection' (which is selected) and 'Only collect the following events'. Underneath, there is a 'Filters' section with a grid of checkboxes for various events. The 'Process Security Process Denied' checkbox is checked. At the bottom, there is a dropdown menu for 'Max Device Events logged per minute' set to '300'.

Enable Device Event Collection

If enabled, events will be stored to the DB and displayed in the Device Portal.

Only collect the following events

If enabled, only specific events will be stored to the DB and displayed in the Device Portal.



Logging

^ Logging

Enable Agent Logging

Log Level

Maximum log files size (MB)

Maximum history files

Enable Agent Logging

If enabled, the TDA will store the events in a TDA.txt file inside the ProgramData folder.

Maximum log files size (MB)

If enabled, the TDA.txt will store only data worth X MB. It will then start overriding its content.

Maximum history files

If enabled, the TDA will store only X amount of the TD.txt upon service restart.



Admin Actions

^ Admin Action

Only allow device actions when secure session is active

Perform device actions silently

Perform device actions if no 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

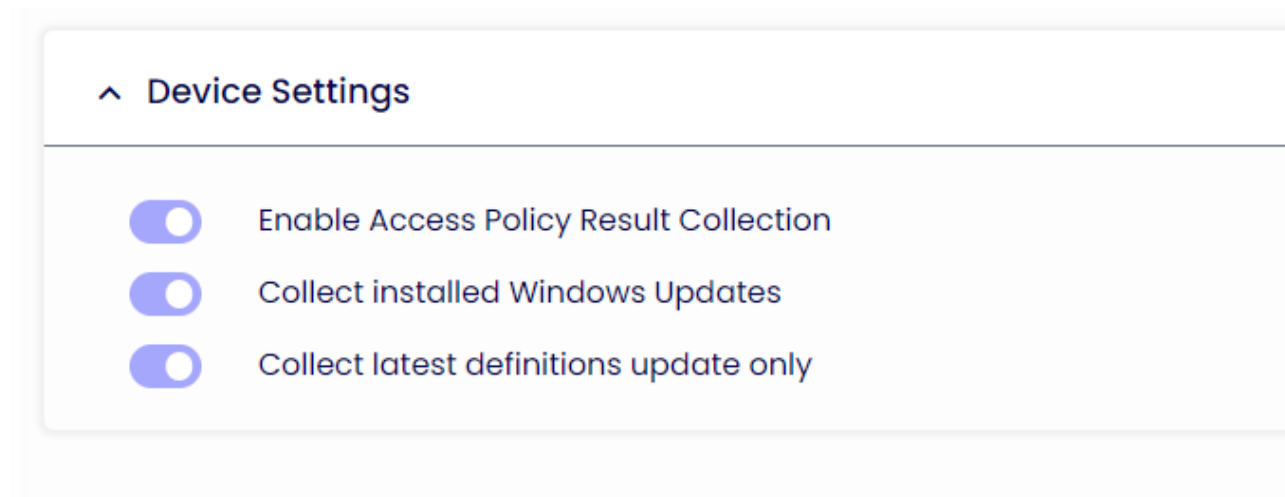
If enabled, actions like Restart, Profile Refresh will be performed silently without user consent.

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.



Device Settings



Enable Access Policy Result Collection

If enabled, events about Access Policy will be stored to the DB and displayed in the Device Portal.

Collect installed Windows Updates

If enabled, events about Windows Updates will be stored to the DB and displayed in the Device Portal.

Collect latest definitions update only

If enabled, only the latest windows updates will be stored to the DB and displayed in the Device Portal.



Troubleshooting

^ Troubleshooting Mode

Enable Device Event Collection
 Only collect the following events

Filters

<input type="checkbox"/> Device Inventory Change	<input type="checkbox"/> Device Connected	<input type="checkbox"/> Device Disconnect	<input type="checkbox"/> Device Unlock Attempt Failed
<input type="checkbox"/> Device Unlocked	<input type="checkbox"/> User Logoff	<input type="checkbox"/> User Logon	<input type="checkbox"/> Process Security Object Denied
<input type="checkbox"/> Process Security Process Allowed	<input type="checkbox"/> Process Security Process Denied	<input type="checkbox"/> Process Security Module Denied	<input type="checkbox"/> Process Security Volume Denied
<input type="checkbox"/> Process Security Registry Denied	<input type="checkbox"/> Driver Protection Denied	<input type="checkbox"/> User Authentication Success	<input type="checkbox"/> User Authentication Failed
<input type="checkbox"/> Session Start	<input type="checkbox"/> Session End	<input type="checkbox"/> Profile Activated	<input type="checkbox"/> SEP Actions
<input type="checkbox"/> SEP Notifications			

Max Device Events logged per minute:

Troubleshooting Mode will collect a lot more events than normal Device Events collection.

It is recommended only to use this mode when trying to resolve an agent issue.

Troubleshooting Mode is an “on demand” operation and it can be switched on and off via the Device Actions in the Devices Tab

Troubleshooting Mode

Enable for (mins)

Troubleshooting Mode



Object / Volume / Registry event filtering

Object / Volume / Registry event filtering

- Ignore Unknown Processes events
- Ignore Pending Services events
- Ignore Duplicate Events that happens within (mins)
- Ignore events from the services
- Ignore events from these processes

(to ignore mutple events & processes seperate with a ',')

Ignore Unknown Processes events

If enabled, unknown processes events will not be displayed in the Device Portal.

Ignore Pending Services events

If enabled, pending services events will not be displayed in the Device Portal.

Ignore Duplicate Events that happens within (mins)

If enabled, duplicate processes events that happen in X minutes will not be displayed in the Device Portal.

Ignore events from these services

If enabled, events that are logged from a specific service will not be displayed in the Device Portal.

Ignore events from these processes

If enabled, events that are logged from a specific process will not be displayed in the Device Portal.



Logging

^ Logging

Enable Agent Logging

Log Level

Maximum log files size (MB)

Maximum history files

Enable Agent Logging

If enabled, the TDA will store the events in a TDA.txt file inside the ProgramData folder.

Maximum log files size (MB)

If enabled, the TDA.txt will store only data worth X MB. It will then start overriding its content.

Maximum history files

If enabled, the TDA will store only X amount of the TD.txt upon service restart.



Administration

Device Policy Configuration

Device Policy Branding Shortcuts Startup Script Device Settings Administration Authentication

Device Unlock

Allow device 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

Device Policy Configuration

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

Authentication Providers

Perorm Authentication

EveryLaunch FirstLaunch

Every : Launches

Every : 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.

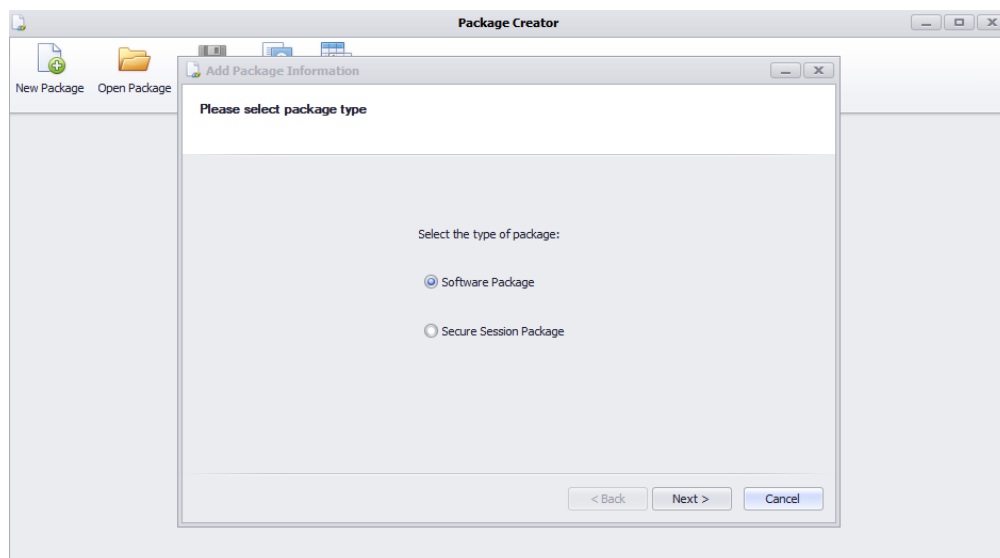


Software Packages

Software Packages can be deployed and installed on your TDA devices. To create a software package, you will need to use the Package Creator tool. Download is available [here](#)

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.





Add Package Information

Please provide package information

Name

Publisher

Description

Version

Reboot Required

Reboot Now

Per User Install

< Back Finish Cancel

Software Package

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

Package Creator

New Package Open Package Save As... Create Virtual Disk

Package Information Install Files Install Type Uninstall Type Pre-Install Tests and Conditions Install Script Uninstall Script Installation Info

Package Type: MachineSoftwarePackage

Name

Publisher

Description

Version

Reboot Required Install Uninstall

Reboot Now Install Uninstall



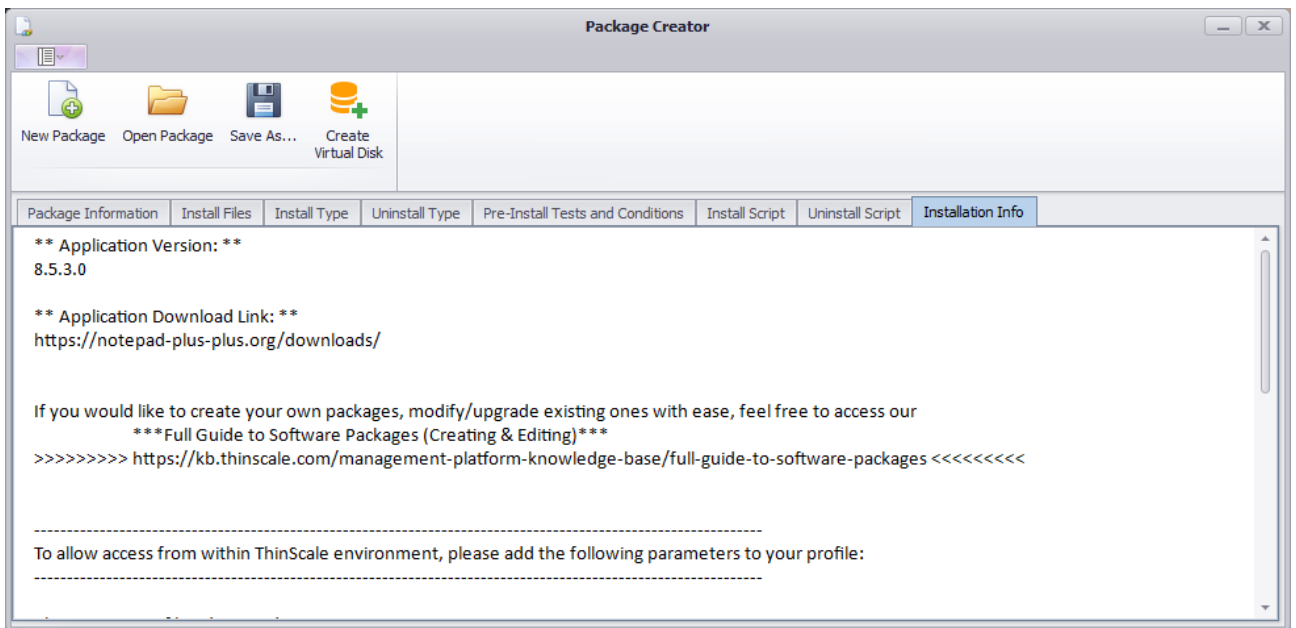
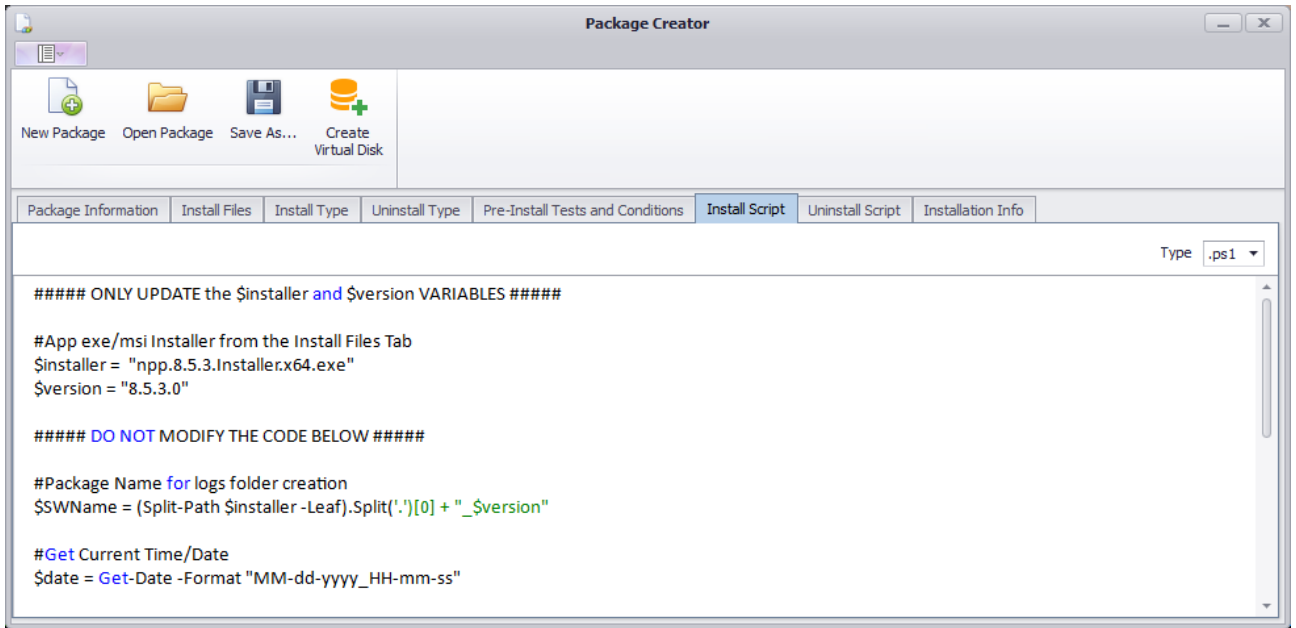
The screenshot shows the 'Package Creator' application window with the 'Install Files' tab selected. The interface includes a toolbar with 'New Package', 'Open Package', 'Save As...', and 'Create Virtual Disk' buttons. Below the toolbar is a navigation bar with tabs for 'Package Information', 'Install Files', 'Install Type', 'Uninstall Type', 'Pre-Install Tests and Conditions', 'Install Script', 'Uninstall Script', and 'Installation Info'. The main area displays a table of files:

Name	Size	Type	Version	Physical Path
npp.8.5.3.Installer.x64.exe	4544 KB	Applica...	8.5.3.0	C:\Users\adm_stirpeg\Ap...
package.ico	5 KB	ICO File		C:\Users\adm_stirpeg\Ap...
ReadMe.txt	4 KB	Text D...		C:\Users\adm_stirpeg\Ap...

The screenshot shows the 'Package Creator' application window with the 'Pre-Install Tests and Conditions' tab selected. The interface includes the same toolbar as the previous screenshot. Below the toolbar is a navigation bar with tabs for 'Package Information', 'Install Files', 'Install Type', 'Uninstall Type', 'Pre-Install Tests and Conditions', 'Install Script', 'Uninstall Script', and 'Installation Info'. The main area displays a table for test configuration:

Name	Check Type	Value
APP_Version	FileVersion	%ProgramW6432%\Notepad++\notepad++.exe

Below the table, there are two input fields: 'Tests' and 'Expression'. The 'Tests' field contains '[APP_Version]' and the 'Expression' field contains '[APP_Version] < [version#8.4.8.0]'. There are 'Insert' and 'Test' buttons at the bottom of the interface.





Name

Name of the package that will be displayed in the Device Portal.

Publisher

Name of the package publisher that will be displayed in the Device Portal.

Description

Description of the package that will be displayed in the Device Portal.

Version

A version of the package that will be displayed in the Device Portal.

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 TDA session.

Install Files

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



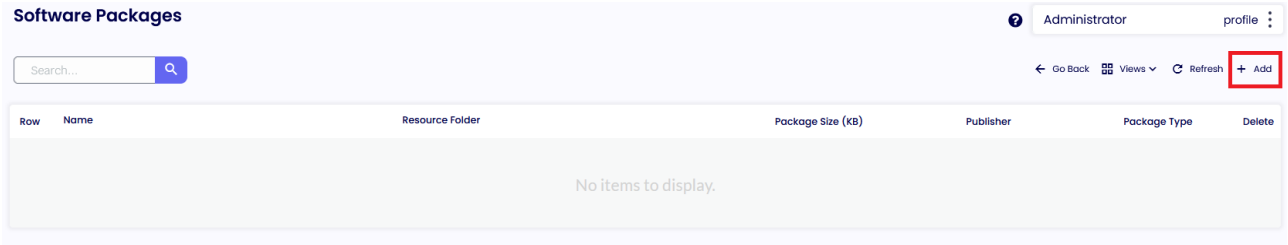
The list must contain every file required by the package installation VB script.

- 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/PS 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 Device Portal. Whenever you are ready to add it, please follow the next steps.

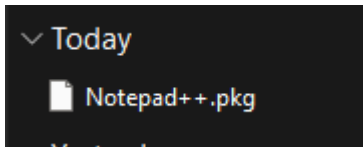


Adding a new software package

To add a new Software Package, browse to Software Package Tab and click Add



Browse the .pkg file that have been created from the Software Package Tool and Add it in the Device Portal.



Once the upload is finished you will see all the information related to the package.

Package Info

Package Name

Package Version

Publisher

Package Description

Package Type

Verify Package

Click Save

Once the package has been added to the portal you will see it in the list.



Software Packages Administrator profile

Search...

[← Go Back](#)






Row	Name	Resource Folder	Package Size (KB)	Publisher	Package Type	Delete
1	Notepad++	General	4,479 KB	DonHo	Software Package App (Machine)	

Please check our library of already made package from the [ThinScale Portal](#)






Software Packages Groups

Software Packages Groups are container where an administrator can store all the packages.

-  Dashboard
-  Organisation
-  Devices
-  Device Groups
-  Configuration
 - Config Assignments
 - Device Profiles
 - General Profiles
 - UI Profiles
 - Security Profiles
 - MDM Profiles
 - Device Policies
 - Software Packages
 - Software Packages Groups

Software Package Groups

Row	Name
1	 Support Software Package Group Support Software Package Group

To Add the newly created Package to the Software Packages Group please click the "Select Software Package" button, add Notepad++ and Click Save.



- Security Profiles
- MDM Profiles
- Device Policies
- Software Packages
- Software Packages Groups
- Auth Providers
- Virtual Disks
- End Users
- End Users Groups
- Device Access Keys
- TDA Update Policies

Software Packages

Name

Select Software Packages

Select Software Packages Administrator profile

Search...

Go Back Views Refresh Save

Selected	Name	Resource Folder	Package Size (KB)	Publisher	Package Type
<input checked="" type="checkbox"/>	Notepad++	General	4,479 KB	DonHo	Software Package App (Machine)

Software Packages Administrator

Search...

Go Back Views Refresh

Row	Icon	Name	Package Version	Package Size (KB)	Publisher	Package Type	Resource Folder
1		Notepad++	8.0	4,479 KB	DonHo	Software Package App (Machine)	Jason Resource Folder
2		Cisco AnyConnect Secure Mobility Client <small>Installation file for Cisco AnyConnect Secure Mobility Client</small>	4.10.5111	15,459 KB	Cisco Systems, Inc.	Software Package App (Machine)	Diego Resource Folder
3		Google Chrome <small>Google Chrome</small>	116.0.5845.97	190,535 KB	Google	Software Package App (Machine)	Jason Resource Folder
4		Microsoft Teams <small>Microsoft Teams</small>	1.6.0.18681	1,117 KB	Microsoft	Software Package App (User)	Jason Resource Folder
5		7 Zip <small>7 Zip 321</small>	23.1.0.0	1,539 KB	Igor Pavlov	Software Package App (Machine)	General
6		Azure VPN Client <small>Azure VPN Client</small>	2.1919.40.0	5,207 KB	Microsoft	Software Package App (User)	Pep Resource Folder
7		Firefox <small>Mozilla Firefox</small>	114.0.1	56,964 KB	Mozilla	Software Package App (Machine)	Pep Resource Folder
8		FortiClient VPN <small>FortiClient VPN</small>	7.0.7.345	100,278 KB	Fortinet	Software Package App (Machine)	Pep Resource Folder
9		Global Protect <small>VPN endpoint software</small>	5.2.4	31,559 KB	Palo Alto	Software Package App (Machine)	Pep Resource Folder
10		Microsoft Quick Assist <small>Microsoft Quick Assist</small>	2.0.21.0	4,418 KB	Microsoft Corporation	Software Package App (User)	Pep Resource Folder
11		Opera Browser <small>Opera Browser</small>	99.0.4788.65	2,579 KB	Opera	Software Package App (User)	Pep Resource Folder



Authentication Providers

The new Authentication Providers will give the administrator the option to authenticate the Device Portal or the TDA agents machines an Azure or Okta identity 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, OKTA to fully launch the TDA client.

Row	Name	Resource Folder	Auth Provider Type
1	Device Portal Login <small>Device Portal Login</small>	General	AZURE

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



Authentication Providers

Perorm Authentication

EveryLaunch FirstLaunch

Every: Launches

Every: Days

Set Device Name to Auth Provider Login Username

Use Display Name if available

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

Azure, and Okta

For the Azure, or Okta Auth Provider please look at the [KB articles](#) with detailed step by step on how to configure them.



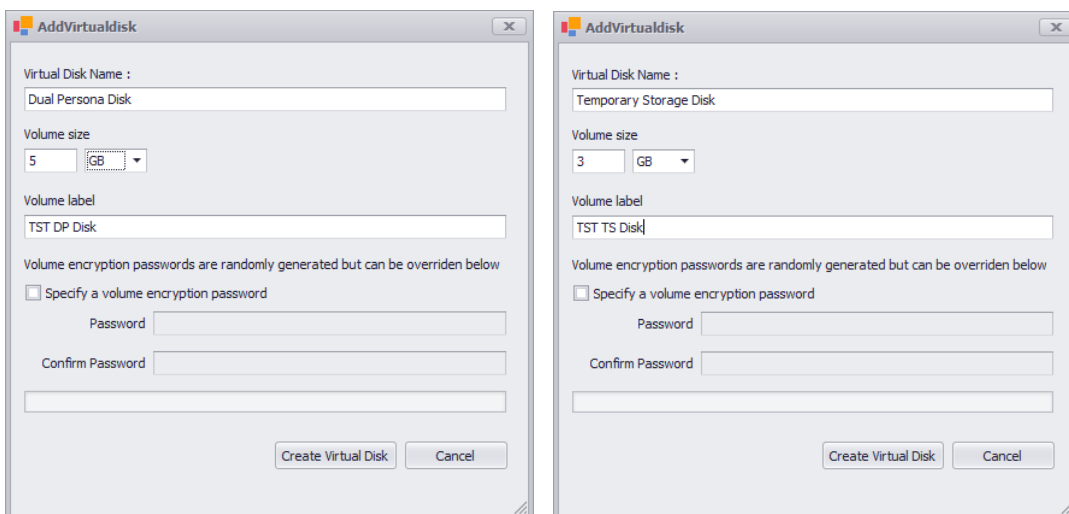
Virtual Disks

Virtual Disks are required by Home Edition Operating Systems when the Dual Persona or Temporary Storage features are enabled in your TDA Security profiles.

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

Launch the ThinScale Package Creator and click Create Virtual Disks. Give it a name, size, volume label and optionally an encryption password. Click "Create Virtual Disk".

Repeat for a Temporary Storage one.



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

Save the ".vd" file locally and then Add it to the Device Portal.



Virtual Disks Administrator profile

Search... Go Back Views Refresh **+ Add**

Row	Name	Resource Folder	Guid	Virtual Disk Type	Delete
No items to display.					

Give it a name and browse the file you just created with the Package Creator Tool.

Upload the Virtual Disk

Virtual Disk Filename: Browse... No file selected.

Resource Folder:

Select the Disk type and click Save when the upload is finished.

Virtual Disk Information

Name:

Description:

Virtual Disk Type:

Resource Folder:

Repeat for the Temporary Storage Disk

Virtual Disks Administrator profile

Search... Go Back Views Refresh + Add

Row	Name	Resource Folder	Guid	Virtual Disk Type	Delete
1	<input type="checkbox"/> Dual Persona Disk	General	9ef9dab1-216a-4a59-b177-2661b5d82549	Dual Persona	<input type="checkbox"/>
2	<input type="checkbox"/> Temporary Storage Disk	General	a25418ad-8506-41ea-8142-ff84f876e9de	Temp Storage	<input type="checkbox"/>



End Users

End Users
Administrator

🔍
⌵

← Go Back
☰

Row	Photo	Name	Last Login Date	Last Login Device	IP Address Overview
1		D: ... T	9/8/2023 3:42:47 PM	DESKTOP-QB7L1Q3	Ireland 10'

The End Users Tab will display all the users that logged in into the Device Portal via the Authentication Provider.

End Users Groups

End User Groups
⌵

🔍
⌵

Row	Name	Resource Folder	Auth Group ID
1	Support End User Group Support End User Group	General	-

The End User Groups Tab is where the administrator will set the Auth Group ID from the Azure Microsoft Entra ID.

All the users that are part of those Group will be added to the End Users section.



End User Group Information

Name:

Description:

Resource Folder: [+](#)

Auth Provider Groups

Auth Group ID	Description	Delete
291e	Support	-
5214	WVD	-

Id: Desc: [Add](#)

End Users

End User count (using End User Group):

[Show End Users](#)



Device Access Keys

Device Access Keys are the entry point for all devices into the Device Portal.

You can create any number of Access Keys that different devices can connect to. For example, you can create two Device Access Keys that have different registration keys and resource folders.

This will allow different devices connecting via the different Access Keys to require different credentials and can be registered into different resource folders in the device portal assigning different profiles and/or packages if desired.

- 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
 - Connection Key1 and Connection 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
- Require Authentication – if enabled during installation the machine will be forced to authenticate against an Authentication Provider (i.e., Azure, Okta)
- Devices can use either Key1 or Key2 to authenticate to the Device Portal. 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.
- Verify Machine SID is Unique – During the device registration process, this option verifies that the device's Machine SID is unique before registering the device as a new device.
- Verify MAC Address is Unique – During the device registration process, this option verifies that the device's MAC Address is unique before registering the device as a new device.

Device Registration Key

↻ Regenerate
📄 Copy

Default Device Group ⓘ

General Device Group

[🔗](#)

Require Authentication ⓘ

Verify Machine SID Unique ⓘ

Verify MAC Address Unique ⓘ

^ Device Connection Keys

Device Connection Key 1

↻ Regenerate

Device Connection Key 2

↻ Regenerate



TDA Update Policies

Tda Update Policies

🔍
⌵

Row	Name	Resource Folder
1	🔗 8.0 Latest 8.0 Latest	General

The TDA Update Policies serve as the primary hub for managing the automatic update functionality of the TDA client. Our advanced CDN technology hosted on Azure enables the global distribution of all TDA client versions.

Upon launching the TDA client, the software initiates a comparison between the locally installed version and the TDA Update Policies. If a newer version is available on the CDN, and the "Use latest build" option is selected or a specific version greater than the locally installed one is specified, the TDA client will automatically update itself.

8.0 Latest

TDA Update Policy Information

Name

Description

Resource Folder
 ▼

TDA Update Policy

TDA Version
 ▼

Use Recommended Settings (Use the latest build available for the appropriate version)



Device Analytics Profile

The Device Analytics is an essential toolkit that empowers IT to be first responders in addressing critical device performance issues.

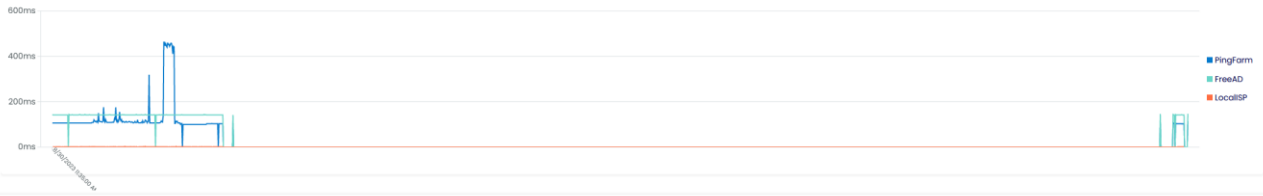
This comprehensive solution provides real-time insights into the health and performance of devices, both on an individual and estate-wide level.

Please have a look at the [KB articles](#) for more info about the Log Analytics workspace and the Application Insights





Network Latency (ms)



Bandwidth

Date	Download (Mbps)	Upload (Mbps)	Jitter (ms)	Latency (ms)	Test Host	Location
8/30/2023 11:35:09 AM	479.53	411.04	111	113	http://tsspeedtest-b-0westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
8/31/2023 11:06:12 AM	481.2	422.23	115	111	http://tsspeedtest-b-0westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
9/5/2023 11:42:41 AM	806.57	434.81	611	694	http://tsspeedtest-b-0westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
9/5/2023 1:24:10 PM	883.26	517.47	605	672	http://tsspeedtest-b-0westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
9/5/2023 1:41:19 PM	925.79	430.62	603	878	http://tsspeedtest-b-0westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)
9/5/2023 3:14:26 PM	750.92	432.01	607	643	http://tsspeedtest-b-0westeurope.azurecontainer.io	West Europe (ThinScale Technology Ltd.)

Device Details

Analytics Last Check-in	CO/Region	ST/Province	City
9/5/2023 3:15:28 PM	Ireland	Dublin	Dublin

Enable Latency Test

Latency Tests

Enable Latency Tests

Collection Interval (minutes):

Ping Count:

Name	Host	Threshold (ms)	Notifications
Google.com	www.google.com	30	True ✎ 🗑
LocalISP	www.internet.com	30	True ✎ 🗑

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



Internet Host Checks

^ Internet Host Checks

+ Add

Hostname

https://www.google.com

✎ ✖

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

^ Windows Log Data

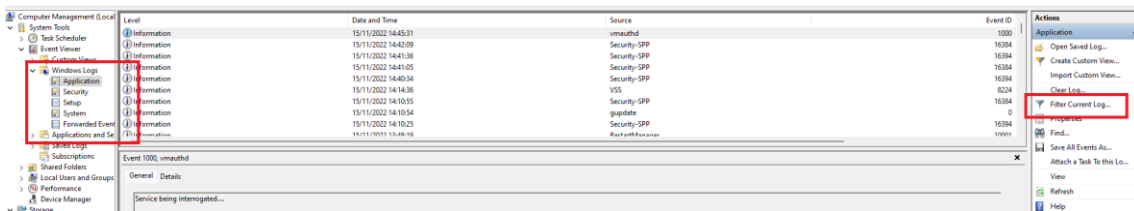
Collect Windows Event Log Data

+ Add

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	✎ ✖

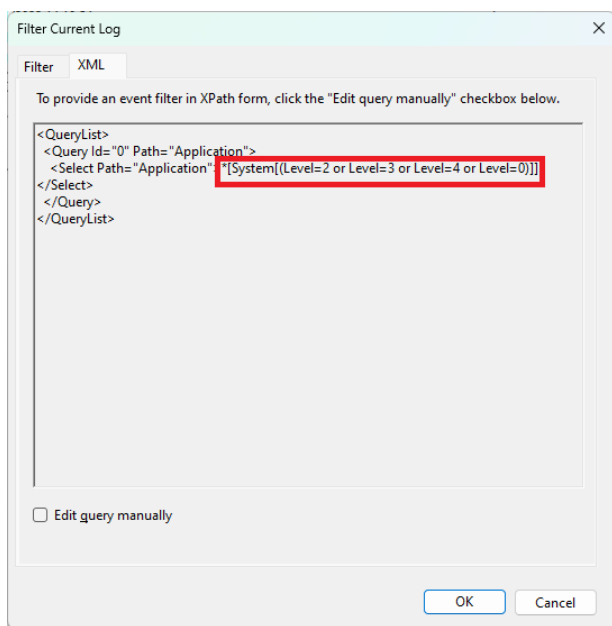
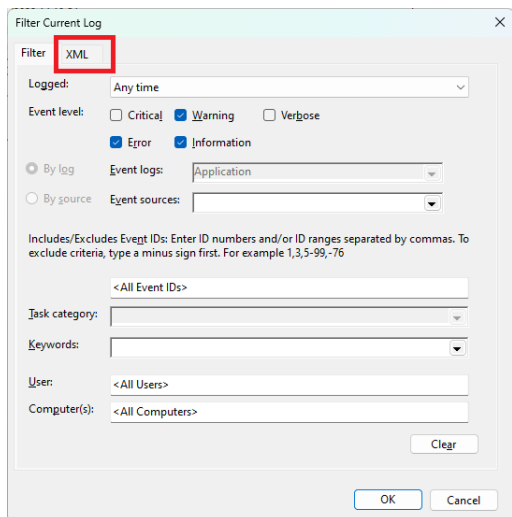
This option will set the Log Level of the Windows Event Viewer you want the clients to collect. By default, only Critical and Error Logs are saved in the Log Analytics Workspace.

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





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





Enable User Notification

^ **User Notification**

Enable User Notifications

Notification Interval (minutes)

Notification Window (minutes)

Enable CPU/Memory Notification

CPU Threshold (%)

Memory Threshold (%)

Notification Title

Notification Footer

Enable Detailed Messages

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.



Speed Test

^ Speed Tests

Enable Speed Tests

Delay (seconds)

Timeout (seconds)

Speed Test Servers

Please do not modify modified this value unless instructed by ThinScale Support.

<https://speedtest-api.thinscale.com/api/thinscale-speedtest-servers>

Standard Data Collection

^ Standard Data Collection

Collect CPU / Memory / Disk / Network Stats

Collection Interval (minutes)

Collect Software Inventory

Log Collection Level

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 of the DA.



8. Reports

Within the Report Tab you will be able to see activity like console login and logout, folder updates, resource folder update and more.

Audit Report

Show for the last:
 Start Date:
 End Date:
 Event:
 User:

User	Date	Action Type	Description
Administrator	10/11/2023 8:59:25 PM	Console Login	User Administrator logged in from Ireland
Administrator	10/11/2023 8:56:21 PM	Console Login	User Administrator logged in from Ireland
System	10/11/2023 8:56:14 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
System	10/11/2023 8:15:08 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
System	10/11/2023 7:00:27 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
System	10/11/2023 3:30:41 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
System	10/11/2023 3:30:02 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
Administrator	10/11/2023 3:15:34 PM	Console Login	User Administrator logged in
Administrator	10/11/2023 3:15:29 PM	Console Logout	User Administrator logged out.
System	10/11/2023 2:57:56 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
System	10/11/2023 2:56:30 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
System	10/11/2023 2:38:40 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
System	10/11/2023 2:36:36 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'
Administrator	10/11/2023 2:34:10 PM	Console Login	User Administrator logged in from United Kingdom
System	10/11/2023 2:29:06 PM	Organisation Settings Updated	User updated entity 'OrganisationSettings' with the id '1'

1 2 3 4

In the Permission Tab on the other hand, you will be able to quickly glance over all the permissions applied to a specific user and groups.

Permissions Report Administrator

Name	Add
Add a New Global Settings	✓

Name	Delete	Read	Select	Update
Organisation Settings	✓	✓	✓	✓
Admin Roles	✓	✓	✓	✓
Admin Permission Sets	✓	✓	✓	✓
Admin User Groups	✓	✓	✓	✓
Admin Users	✓	✓	✓	✓
End User Groups	✓	✓	✓	✓
End Users	✓	✓	✓	✓
Admin Resource Groups	✓	✓	✓	✓



USAdmin Global Settings Export Current Export All

Name	Add
Add a New Global Settings	✓

Name	Delete	Read	Select	Update
Organisation Settings	✗	✗	✗	✗
Admin Roles	✗	✗	✗	✗
Admin Permission Sets	✗	✗	✗	✗
Admin User Groups	✗	✗	✗	✗
Admin Users	✗	✗	✗	✗
End User Groups	✓	✓	✓	✓
End Users	✓	✓	✓	✓
Admin Resource Groups	✗	✗	✗	✗



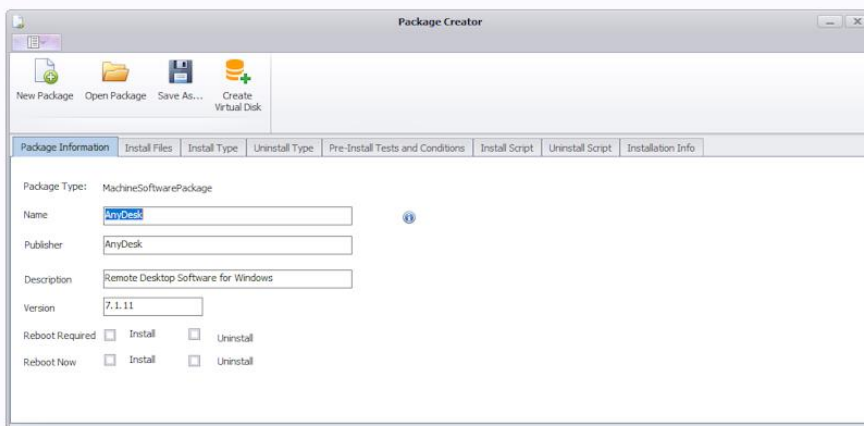
9. Tools

The Tools Tab is just a repository location where you can download our latest Device Portal Package Creator and the latest TDA.msi.

Tools

Package Creator

The Package Creator is a windows application that allows administrators to generate Software Packages and Virtual Disks that can be uploaded to the Device Portal. For more information on the Package Creator and to download the application refer to this [ThinScale Knowledge base article](#).



ThinScale Desktop Agent (TDA) Installer

The ThinScale Desktop Agent Installer is the installer for Secure Remote Worker or Thinkiosk applications.

For more information on the TDA Installer and to download the installer refer to this [ThinScale Knowledge base article](#).

