Administrator Permission Model

1 Introduction

The On-Prem Thinscale Management Server 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.

2 Admin Permission Model

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

Term	Description
Admin Users	An Admin User represents an administrator on the system. Admin User accounts should not be shared by different administrators. "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. Admin User accounts are automatically generated for administrators who login via Auth Provider accounts. **Note:** Local Admin User accounts are only recommended for initial commissioning, proof or 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.
Admin User Groups	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. 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).
Admin Roles	Admin Roles are used to configure the permissions for administrators on the Device Portal. In its simplest form the Admin Role applies a set of permissions on a set of resources to a set of 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. **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.
Admin Permission Sets	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'. 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. 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.
Admin Resource Folders	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. 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. **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.
Admin Resource Groups	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.

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.

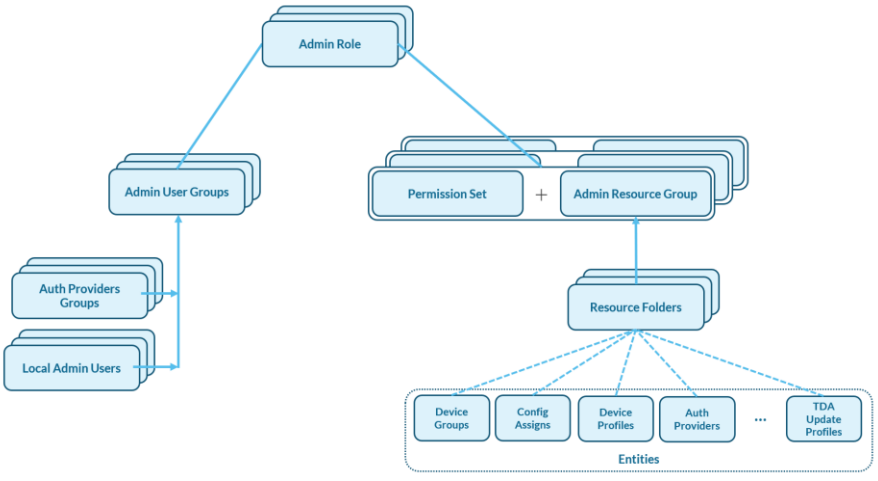

Figure 1: *The relationships between the entity types of the permission model*

3 Accumulated Permissions

3.1 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.

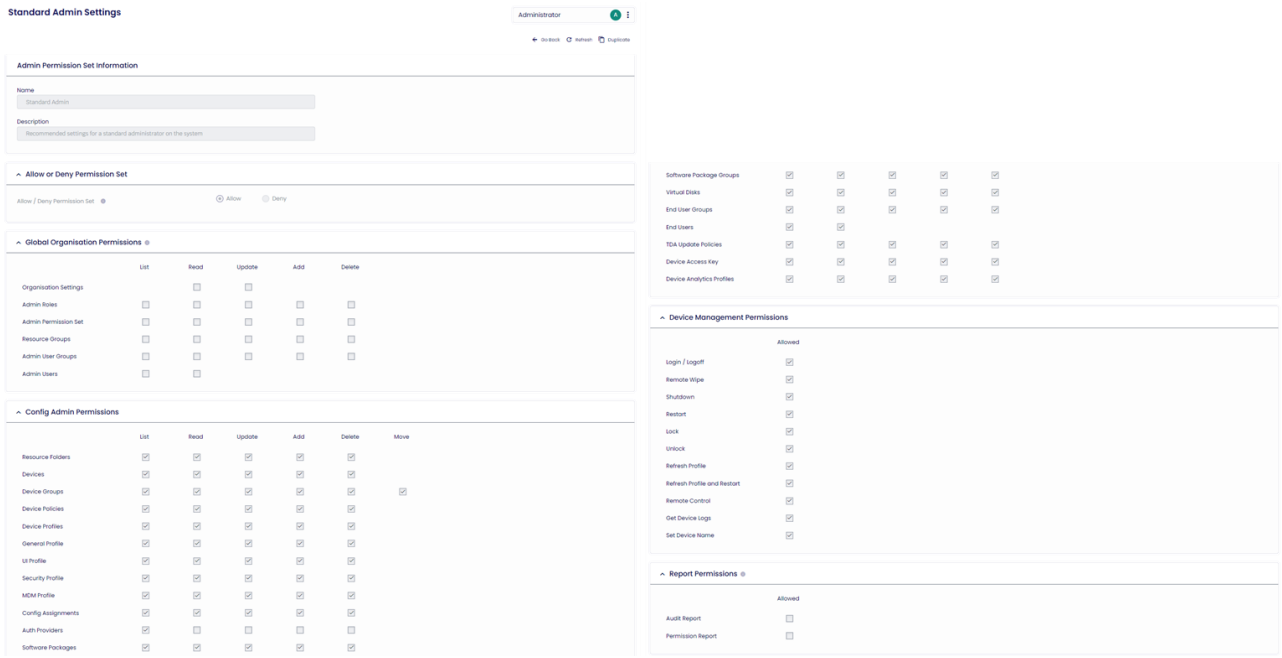

Figure 2: *Configuration of a “Standard Admin” Permission Set*

3.2 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, Addling, 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.

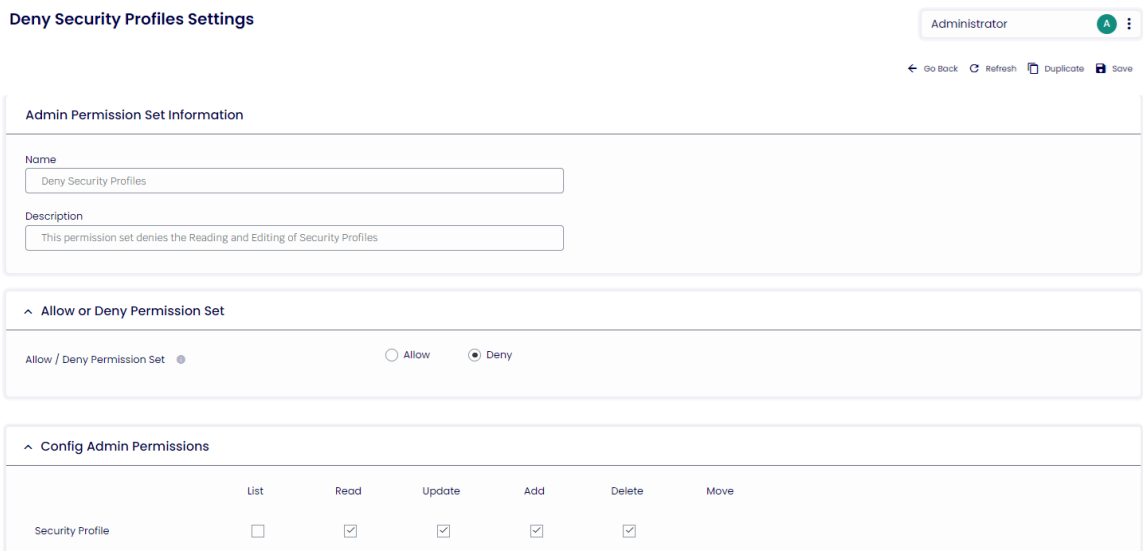

Figure 3: *An example of a Deny Permission Set being used to protect access to Security Profiles*

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.

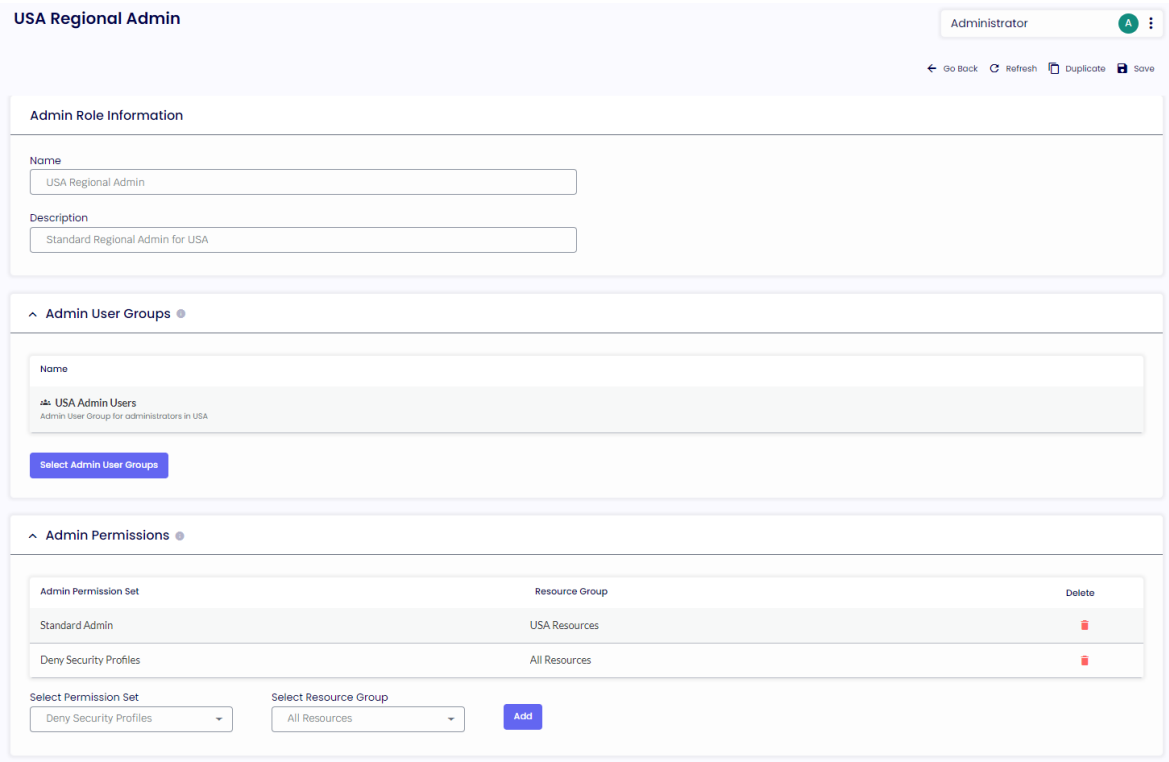

Figure 4: *Example configuration of an Admin Role "USA Regional Admin" protecting the Security Profiles by using a Deny permission set against all resources in the system.*

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.

3.3 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.

3.4 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.

4 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 formed 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 businesses 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 on 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.

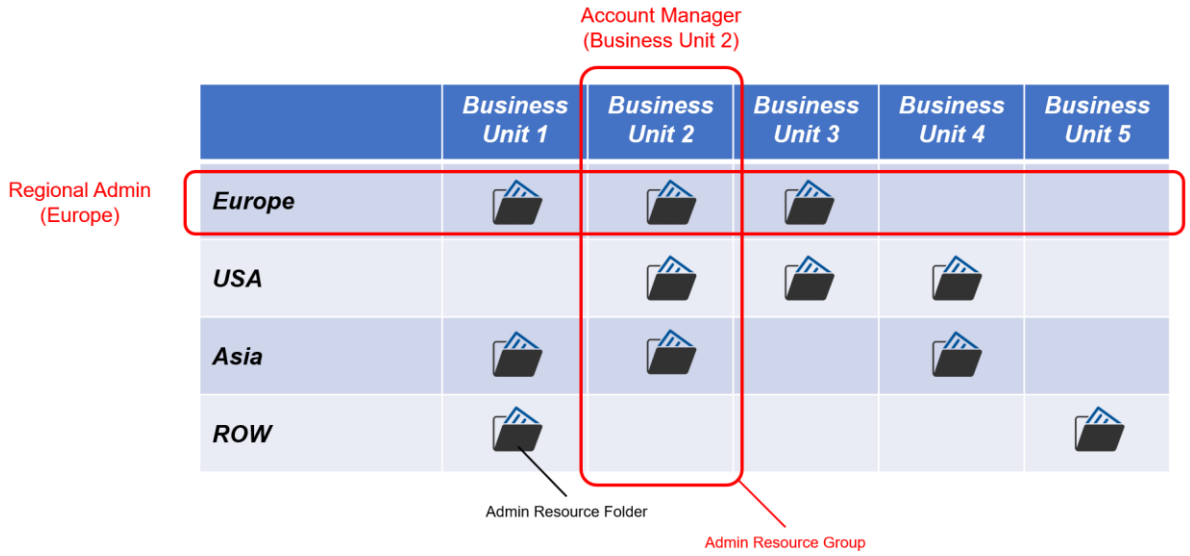

Figure 5: *Example use of Admin Resource Folders and Admin Resource Groups to allow permissions to be easily configured for a Regional Administrator and Account Manager roles.*

5 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.

5.1 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

5.2 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

5.3 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.