Technical Paper

Dell Management Portal Technical Paper

Overview of Dell Management Portal including features, capabilities and launch experience.

Abstract

Dell Management Portal amplifies and extend the management capabilities in Microsoft Intune of Dell PCs
August 2025

Revisions

Date	Description
August 2024	Initial release
August 2025	BIOS Policies section

Acknowledgments

Author: Prasanth, KSR, Prateek Vishwakarma
Support: Thompson, Jocelynn
Other:

Table of contents

Executive summary

The Dell Management Portal aims to streamline PC management by integrating Dell solutions with Microsoft Intune. Its vision is to deliver top-notch system and workspace management for highly manageable devices. The portal serves as a conduit for Dell Services and Software within the Microsoft Intune ecosystem.

Using the Dell Management Portal enables our customers with:

Convenience – Centralize access to Dell services and software in a tool that IT administrators use regularly.

Credibility – Including Dell services and software solutions in Intune reinforces the perception that Dell solutions are top-tier.

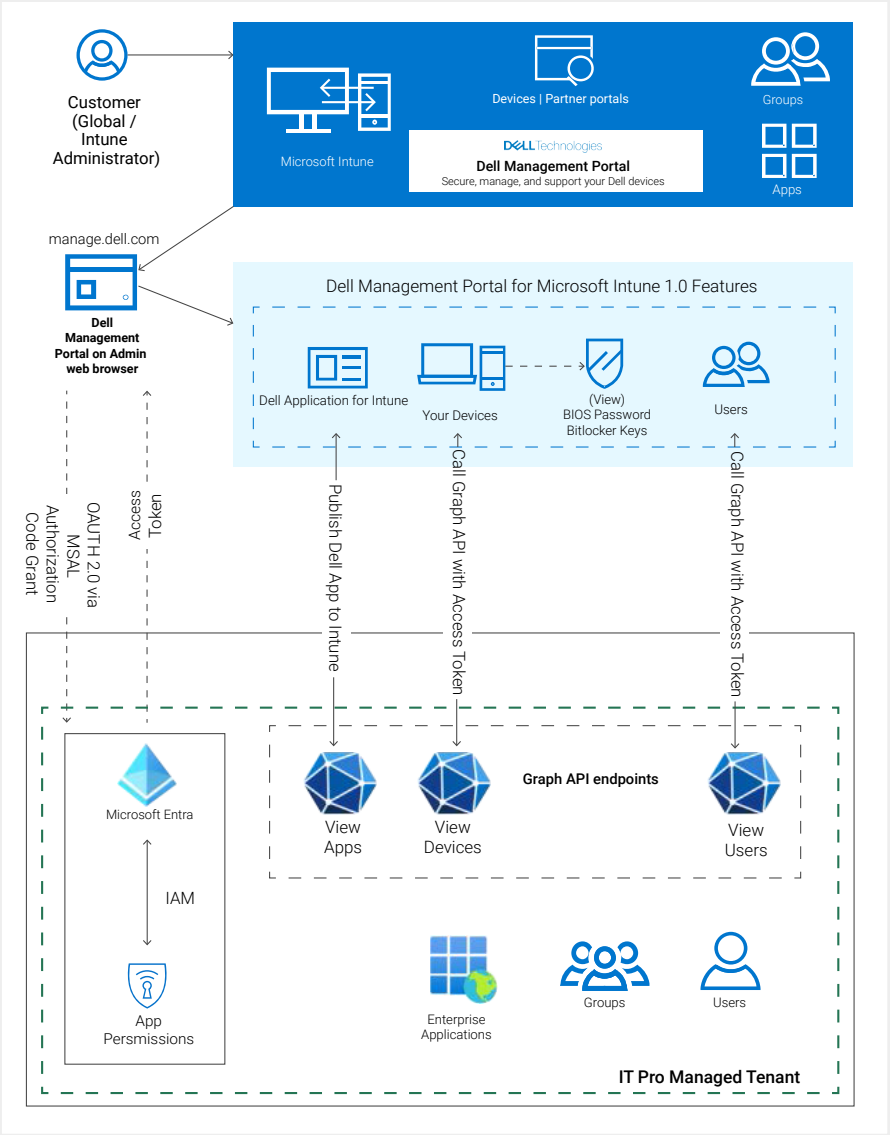
Awareness and Adoption – Promote the awareness and usage of Dell software and services

1. Getting Started with Dell Management Portal

The Dell Management Portal is a cloud-based application aimed at streamlining the management of Dell Client Devices via Microsoft Intune. It utilizes customer Microsoft Entra for Identity and Access Management. It offers an interface that supports the following features:

- Fleet Overview
  - Dell Device Count
  - Dell Application Count
  - BIOS Password Search
  - Dell Services
  - Fleet Overview
- Devices
  - Overview
  - User Information
  - Credentials
  - Installed Dell Enterprise Applications
- Application
  - Manageability
  - Security
  - Application Status
  - Publishing Application to Intune
  - Application Assignments
  - Dell Pro AI Studio
- BIOS Policies

1.1. Reference Architecture



2. Requirements

Before you use Dell Management Portal, make sure you have met the following prerequisites.

- Intune Global Administrative access to a Microsoft Azure tenant
- Internet browser (Microsoft Edge, Mozilla Firefox, Safari, Google Chrome)

Note: Dell Management Portal requires specific permissions to access the company tenant. These permissions are vital for retrieving information related to devices and users, as well as for publishing Dell Enterprise Applications. A Global Administrator of the tenant has the authority to grant these permissions on behalf of the organization. The Dell Management Portal communicates with Azure and Intune through the Microsoft Graph API.

The Dell Management Portal integrates with the Microsoft Entra tenant to access device information, user groups, credentials, and to distribute Dell Enterprise Applications.

3. Login Process – Connect Now

Customers can access the Dell Management Portal via the Intune Partner Portal at Devices | Partner Portals, or directly by visiting https://manage.dell.com/.

To enable integration, a tenant Global Administrator must log in with Entra Credentials and approve the necessary permissions through the Microsoft Authentication dialog box.

The following permissions are required for Dell Management Portal:

- Read all users' full profiles
- Read directory data
- Read all BitLocker keys
- Read Microsoft Intune devices
- Perform user-impacting remote actions on Microsoft Intune devices
- Read all Microsoft Device Management Configuration
- Read and write Microsoft Intune apps
- Read and write Microsoft Intune Device Configuration and Policies

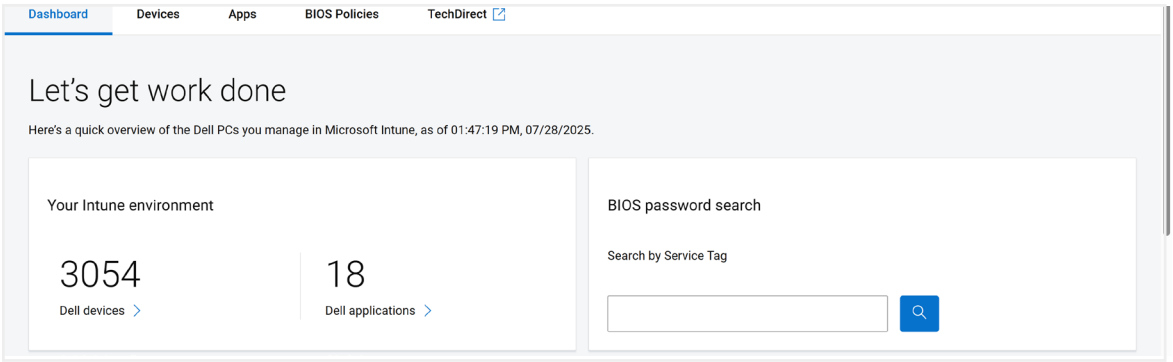
- Dell Management Portal requires write access to Intune Applications and Intune Device Configuration and Policies
- The remaining permissions are Read-Only
- The data remains in the Microsoft tenant but is supplemented with Dell specific capabilities which are transacted with Microsoft infrastructure through the Graph API calls

4. Dell Management Portal Capabilities

The Dell Management Portal's functions become available once the IT Administrator logs in with their Entra ID credentials, has Intune administrative rights, and grants Dell permission to access specific sections of their Intune data.

4.1. Dashboard

This part of the Dashboard and home page will provide swift insights and immediate actions for the IT Administrator.
Dashboard view



Dashboard view

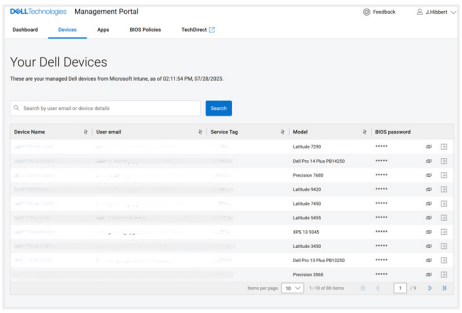
Quick Nav -	This section provides an overview of your Intune environment with the following details: **1. Dell Devices:** This indicates the number of Dell devices enrolled in Intune and includes a link to the devices page. **2. Dell Applications:** This indicates the number of Dell applications supported by Dell Management Portal presently published in Intune.
Quick Actions -	In this section, IT Administrators can search for a device using the Service Tag to retrieve the BIOS password. **1. BIOS Password Retrieval:** Upon clicking "search," the hidden password appears in the search field. Clicking the "eye" icon reveals the characters, allowing the IT Administrator to copy it if required.

4.2. Devices

This page provides a list of devices registered in Intune and accessible through graph API calls. Additionally, it includes access to the BIOS Password and BitLocker recovery key.

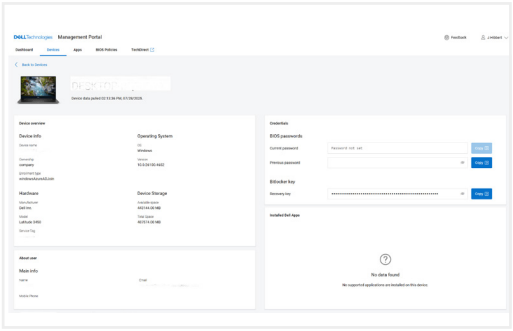
4.2.1. Your Dell Devices

This section provides information about Dell PCs managed within the Intune environment, The device page displays a table featuring the Device name (with hyperlinks to detailed info on each device), the associated User ID, Service Tag, Model, BIOS password (hidden initially), and icons for viewing (eye icon) or copying the BIOS password (clipboard icon).



4.2.2. Device Details

When the Administrator clicks on the Device name in the table, they will be taken to a page that shows the device details.



Device Overview Details: This section includes detailed information about the device.

- Device Information – includes the device name, the owning company, and the type of device enrolment
- Operating System – provides details about the OS running on the device and its version
- Hardware – lists the device manufacturer, model number, and serial number
- Device Storage – indicates the available and total storage space on the device

User Information: This section contains specifics about the user, including their name, mobile number, and email address.

Credentials: This section includes the current and previous BIOS Passwords and BitLocker Recovery Key. These fields are initially hidden and can be revealed when the IT Administrator clicks the "eye" icon beside each field. There are also options to copy the Current BIOS password, Previous BIOS password, and BitLocker Recovery Key.

Installed Apps: This part includes a list of the suggested Dell applications that are present on the device along with their respective versions. An "update available" notification will appear if the application version published in Intune is not the latest.

4.3 Applications

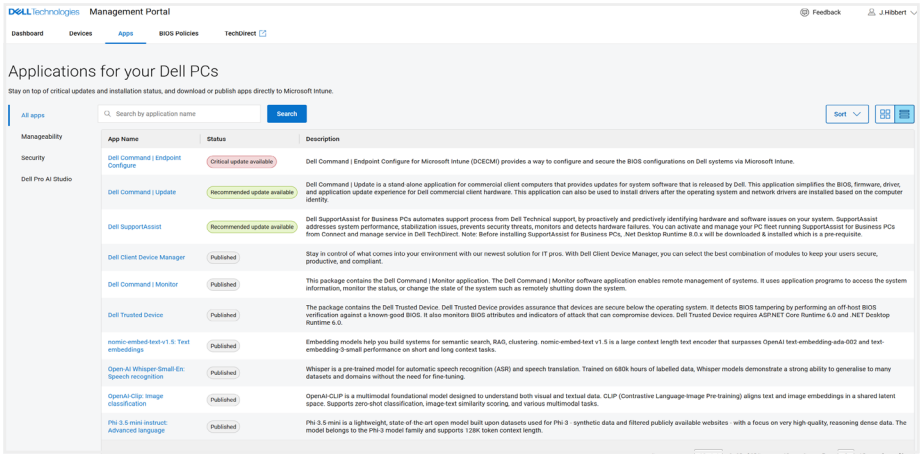
The Intune Administrator can reach the “Apps” page via:

1. Apps in the header menu
2. “Dell Applications” link in Quick Nav

Central List of Applications will display the following information about the available Apps in the Dell Portal:

1. Application name – Title of the application
2. Status – Application status indicating its criticality or publish state. This section will show one of four states:

Critical update available (red)	Recommended update available (green)	Optional update available (blue)	Published (Gray)

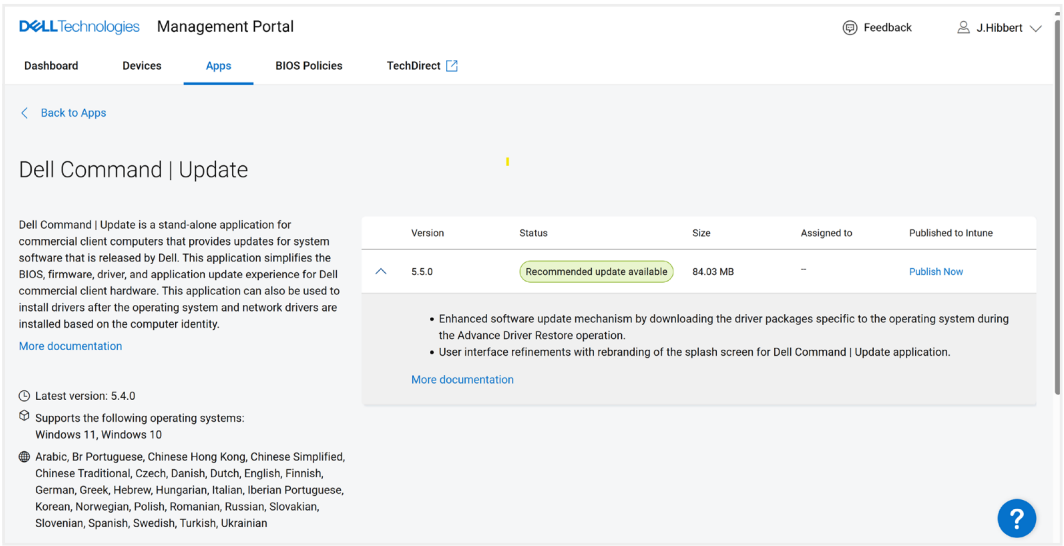


4.3.1. Dell Application Detail Page

By clicking on the Application tile or name, the IT Administrator is directed to the Application Detail page with essential application information which includes:

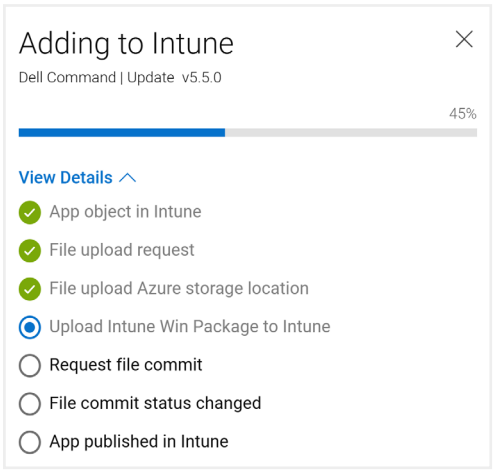
1. Name of the application
2. Application Description
3. Application Version
4. Supported Operating Systems
5. Languages supported

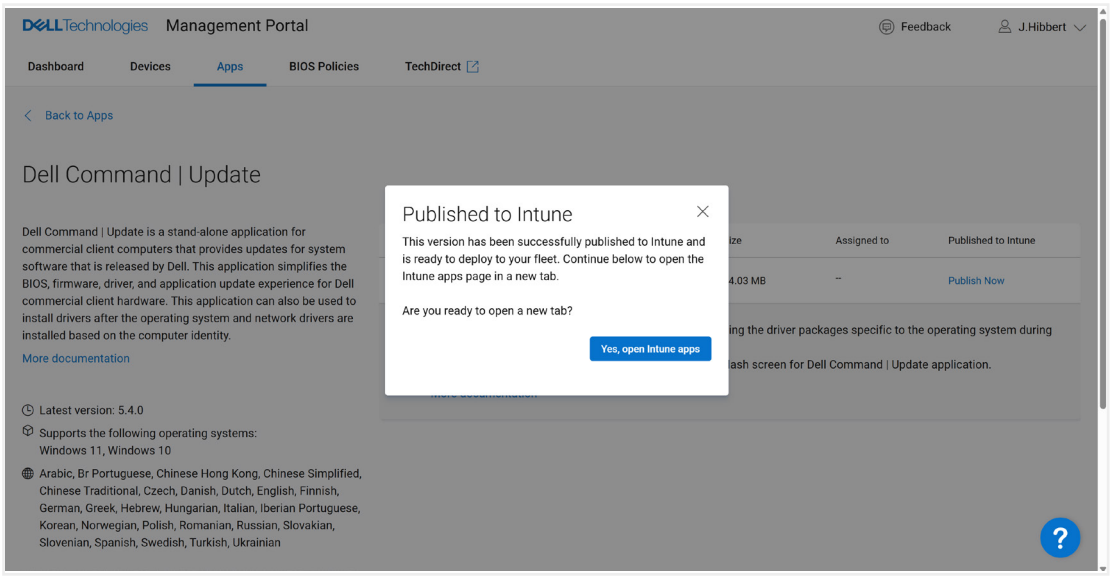
Versions table with drill-down for details such as update status, Size, Assignments, and publish to Intune status. Refer Appendix for Applications supported for the launch and Status categories for an application update in the Dell Management Portal



4.3.2. Publishing an Application to Intune

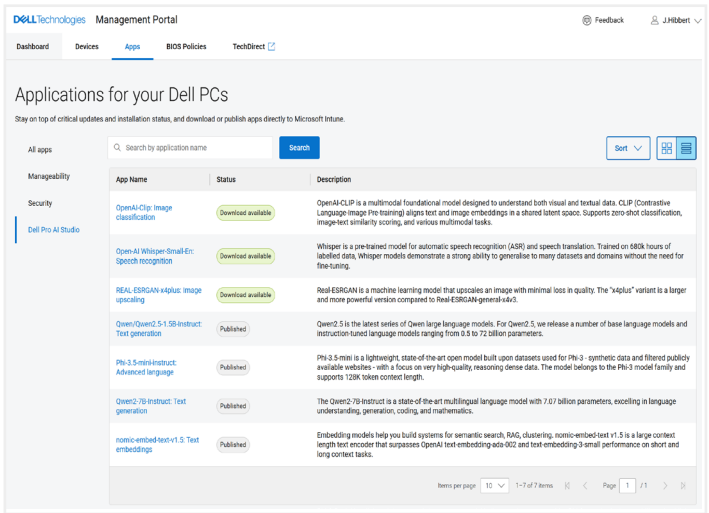
Upon the IT Administrator selecting “publish now,” the chosen version of the application will be automatically published to Intune. The IT Administrator will then observe a series of steps being executed to confirm that the application has been successfully uploaded as shown below:





4.3.3. Dell Pro AI Studio

An IT admin can discover and download these AI model packages in the Dell Management Portal.

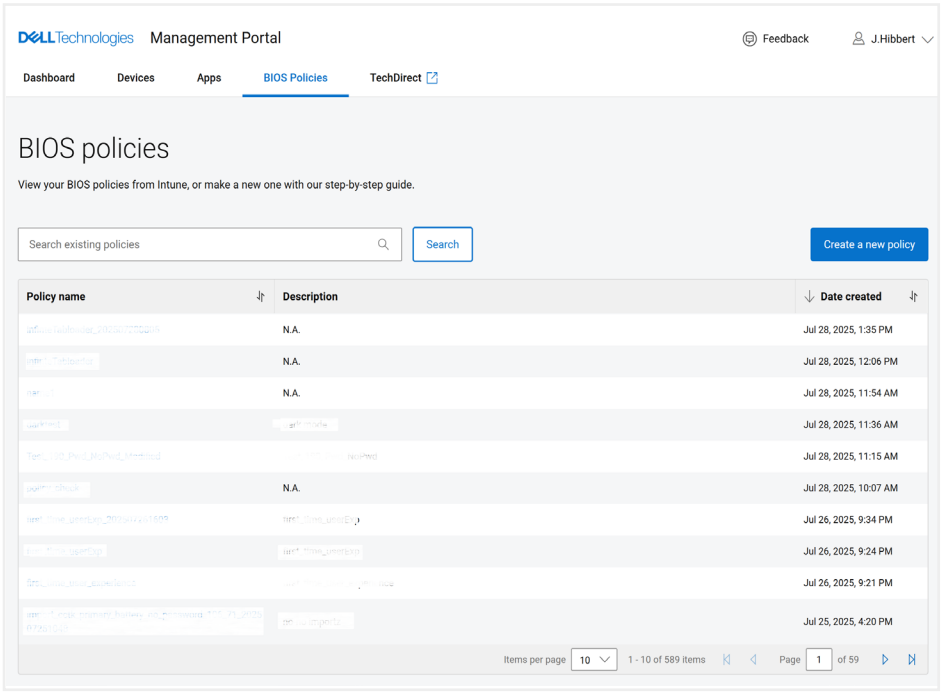


Model Detail Page

4.4 BIOS Policies

This page provides a list of hardware configuration policies in Intune and accessible through graph API calls. Policies are sorted chronologically.

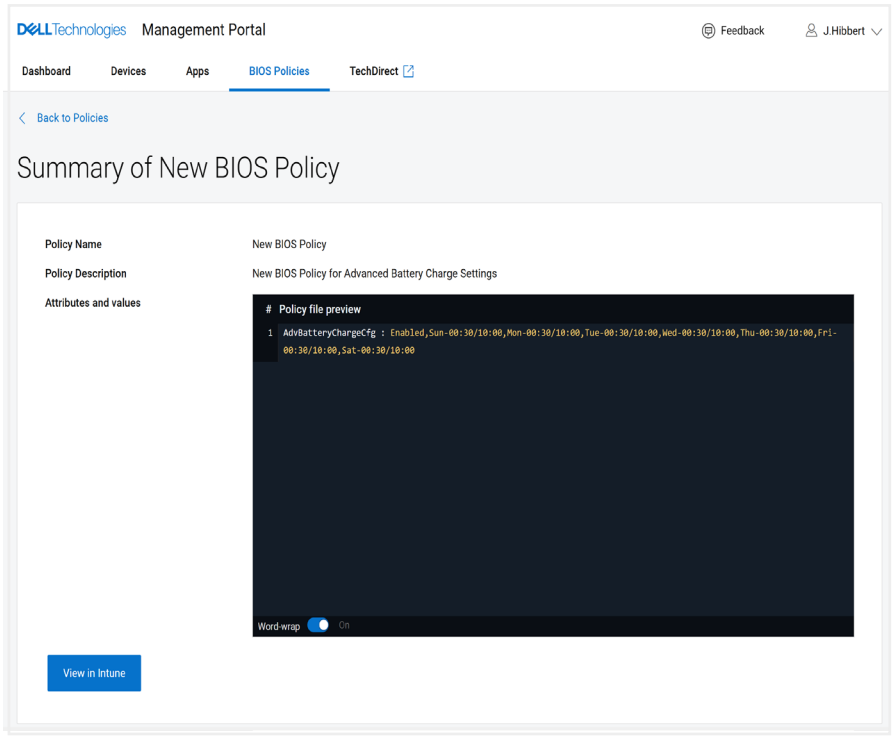
From here, you can either view details of an existing policy or create a new policy.



4.4.1 BIOS Policies Details

The policy details page displays the policy name and policy description.

It also provides detailed policy file preview including the BIOS attributes and corresponding values configured by an IT administrator.



4.4.2 Create a new policy

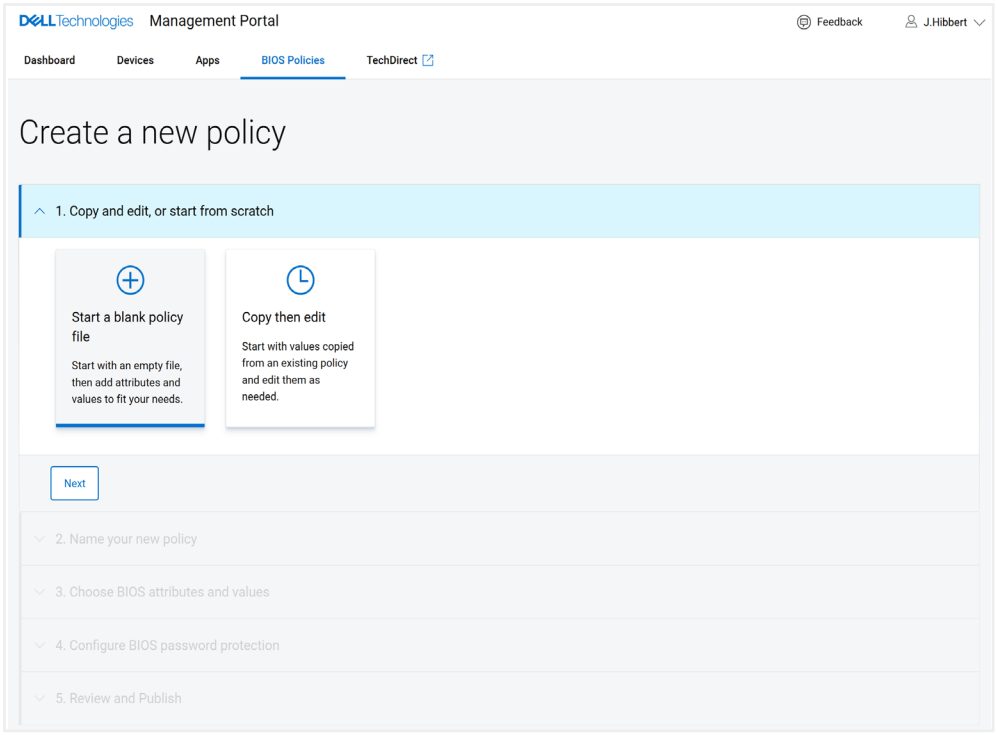
An IT administrator can click on “create a new policy” button to start the policy creation workflow.

4.4.2.1 Start a blank policy file

Start with an empty file, then add attributes and values to fit your needs.

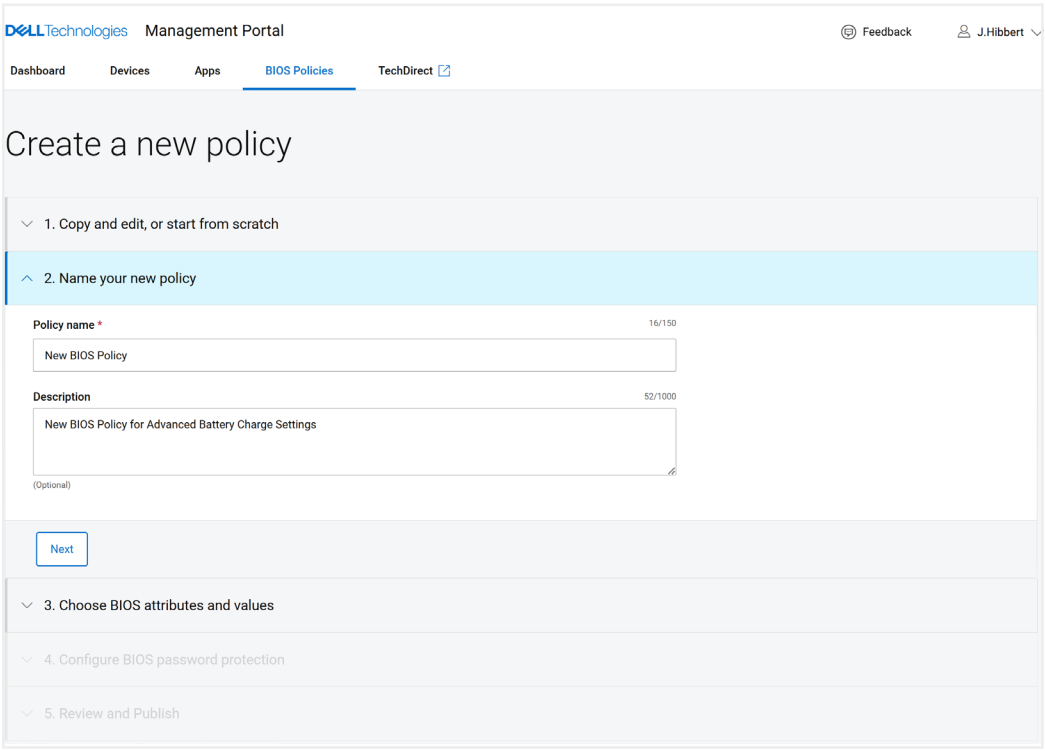
4.4.2.1.1

Start a blank policy card” to start crafting a BIOS policy from scratch and click next.



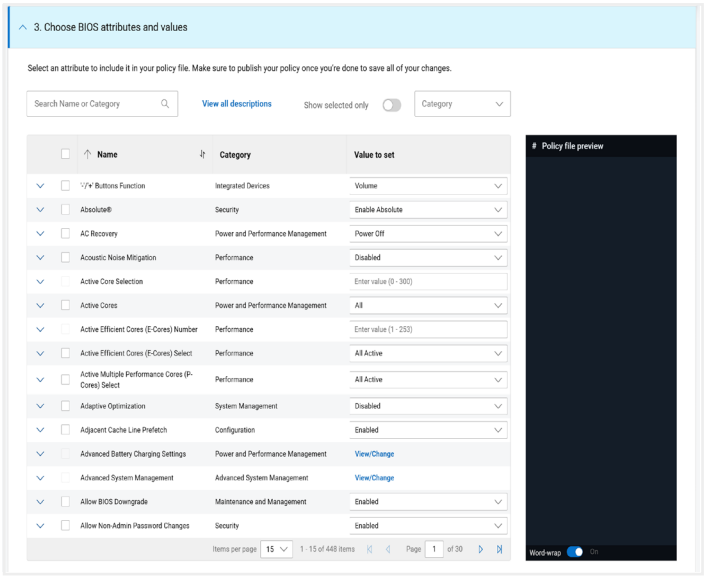
4.4.2.1.2

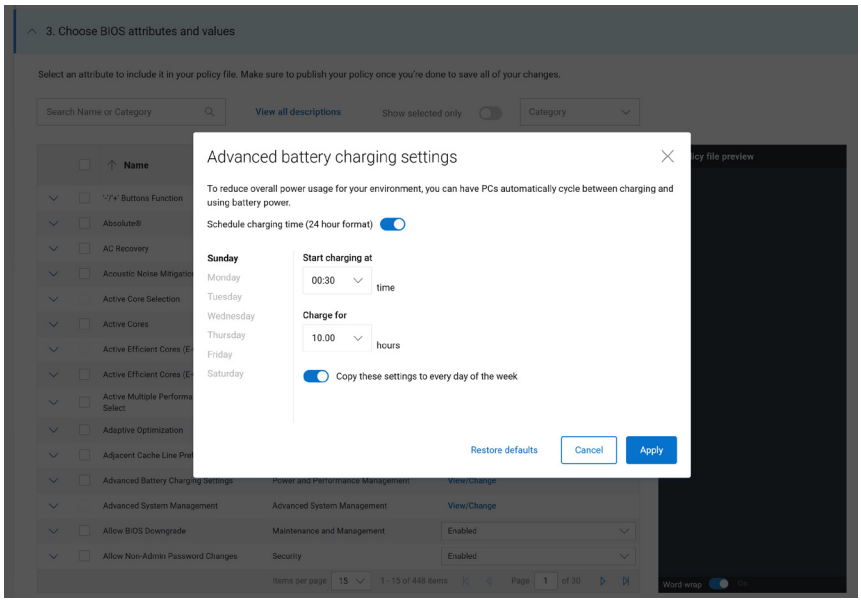
Name your new policy and add description and click next.

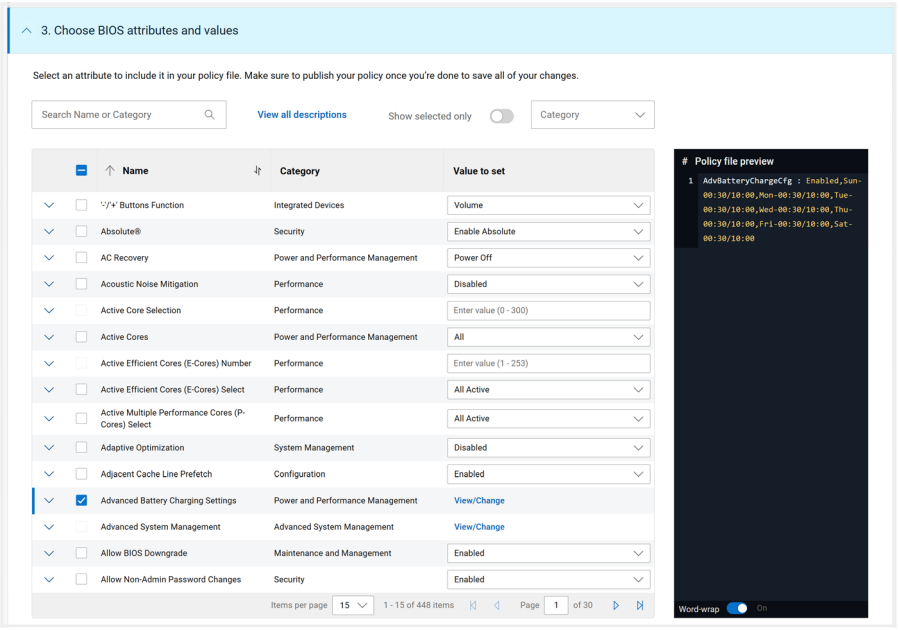


4.4.2.1.3

Configure BIOS attributes according to the requirements and add it to the policy and click next.

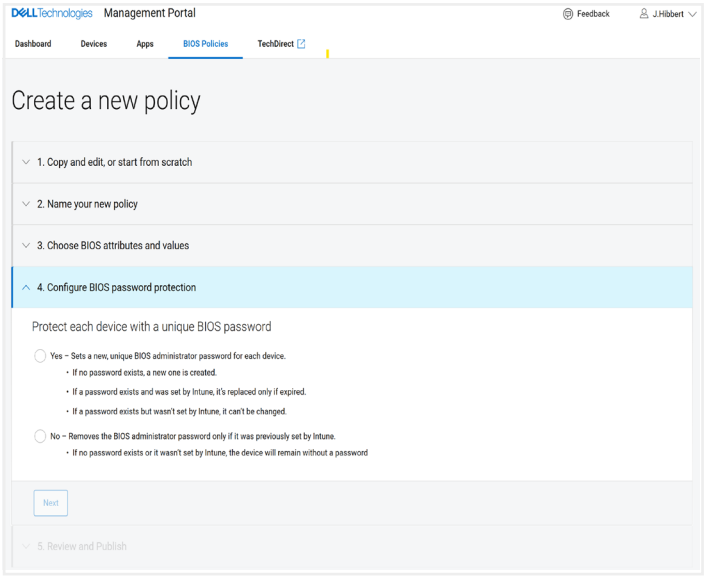


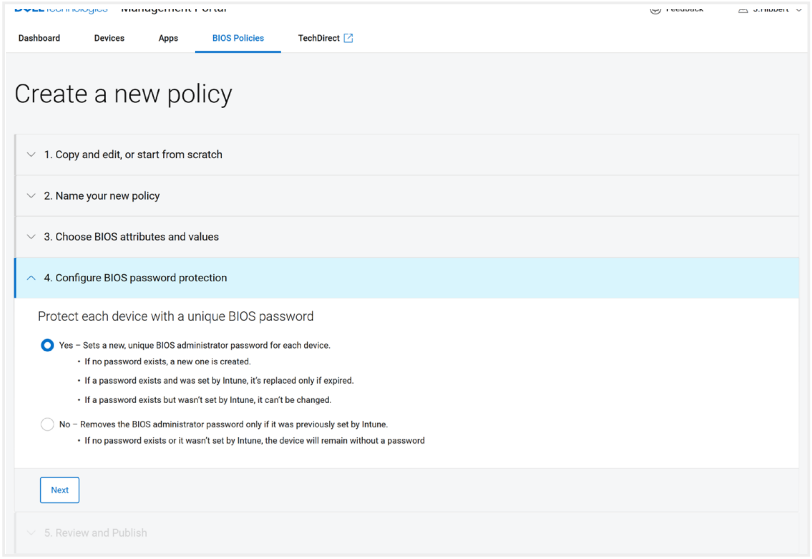




4.4.2.1.4

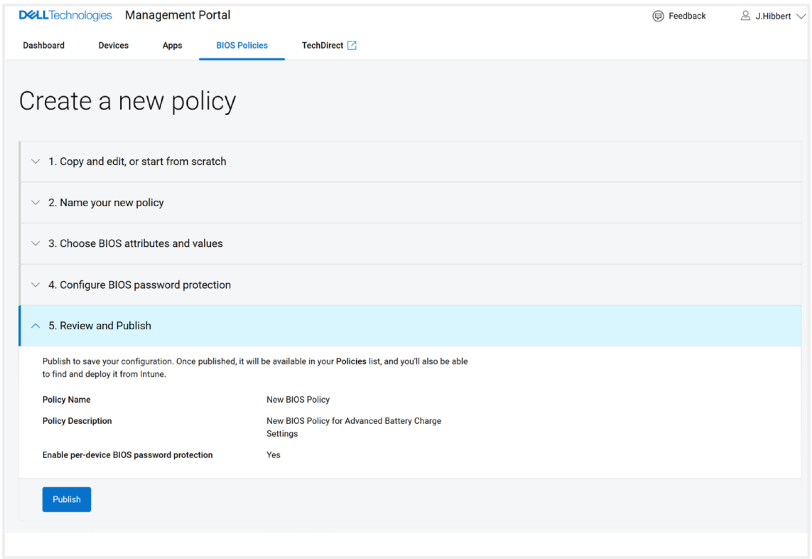
Select password protection preferences and click next.

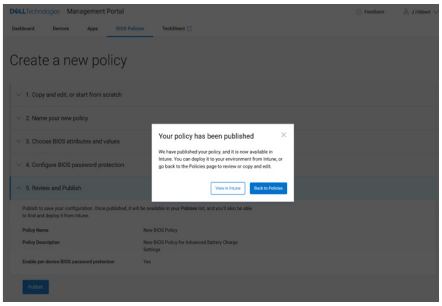




4.4.2.1.5

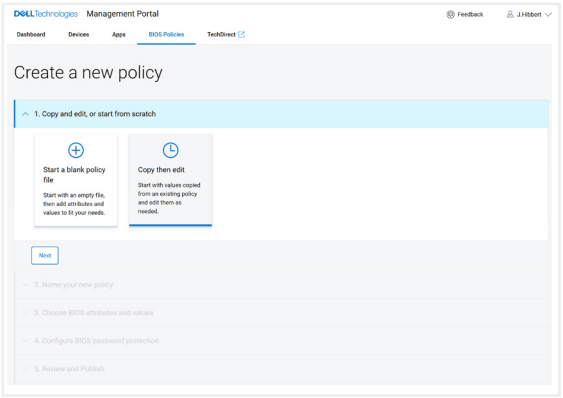
Review the policy details and click publish





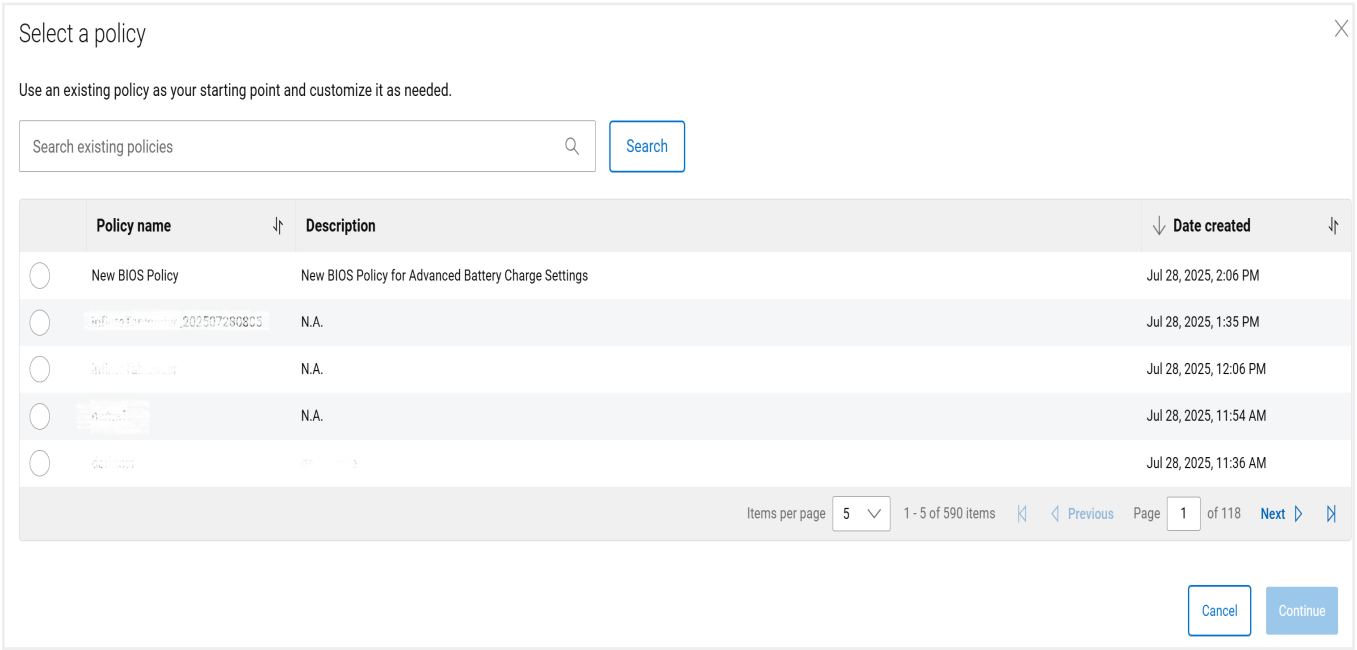
4.4.2.2 Copy then edit

Start crafting a BIOS policy from values copied from an existing policy, then click next.



You would be presented with a list of BIOS policies available to select from.

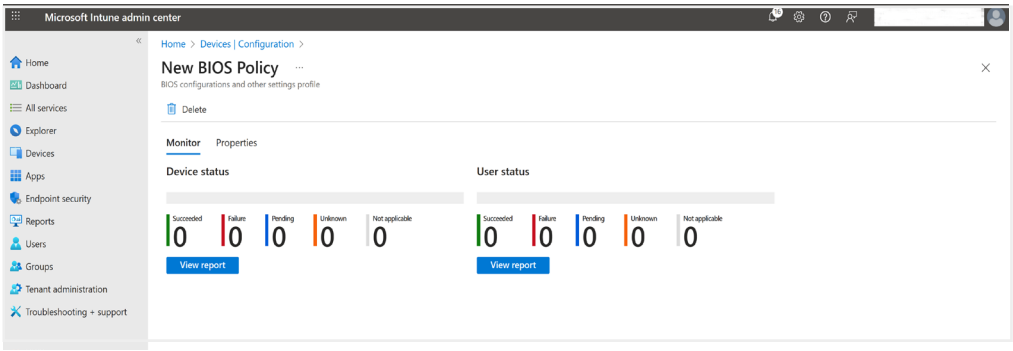
Select a policy from the list and click continue



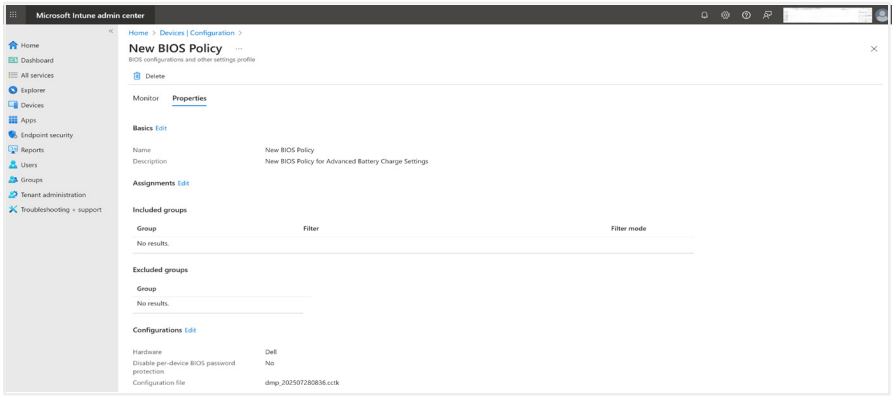
You would notice that the policy name, policy description, BIOS Password preference and the BIOS attributes and corresponding values are pre-populated for you to edit and republish.

4.4.3 Policy assignments in Microsoft Intune.

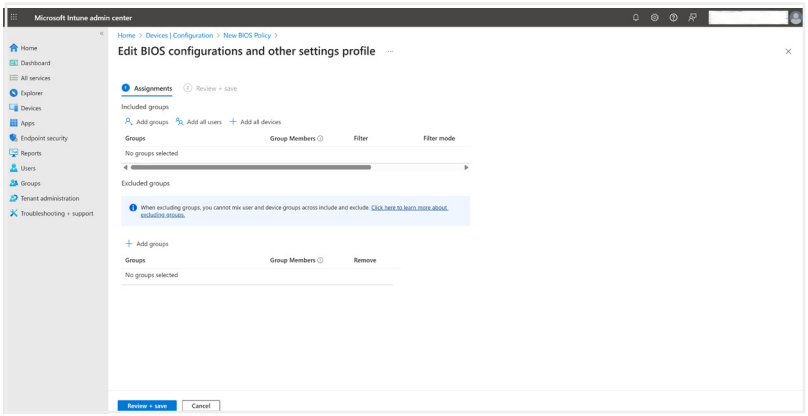
Once the policy is published successfully, click on “view in intune” button to navigate to policy details page on Microsoft Intune.



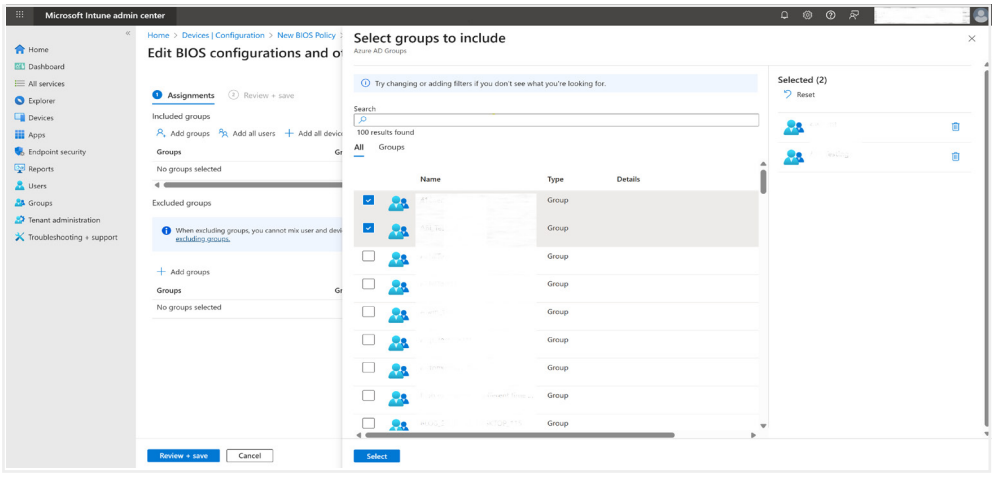
Click on “Properties”



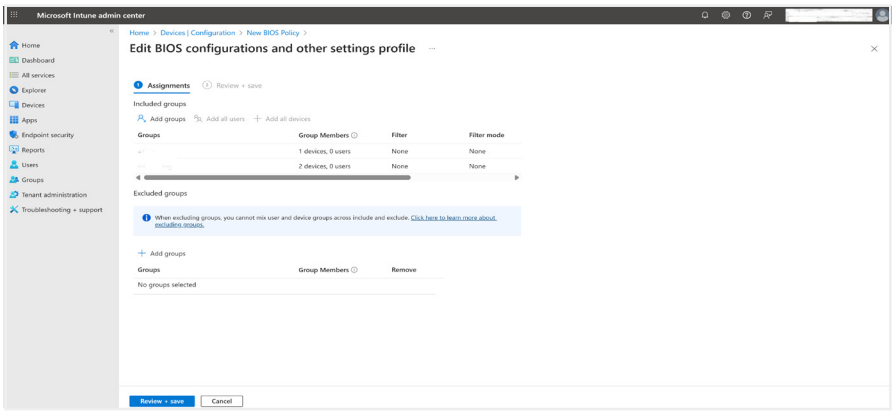
Click on “edit” option next to “Assignments”



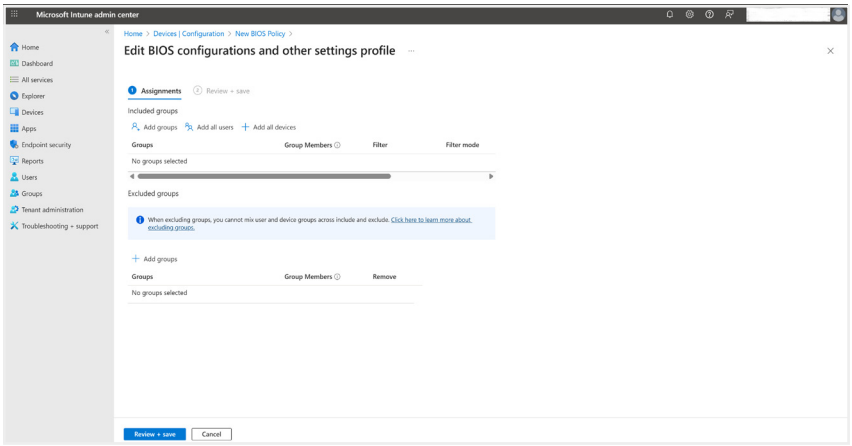
Under “Included Groups” section, click on “Add groups” button and add the required deployment groups for the BIOS policy



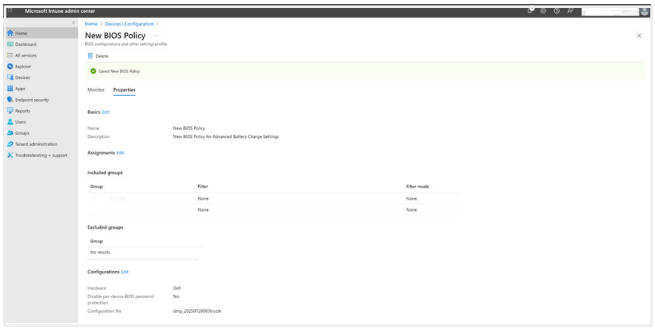
Click on ‘review + save’ button



Review the details and click on save button to deploy the policy to selected groups.



The policy is deployed to selected groups successfully



A. Appendix

Note: As a best practice, present the purpose of the paper up front (summary). The main supporting details belong in the numbered sections. An appendix is used to hold information for the more inquisitive readers. In other words, get the reader's attention first, and the further they read in the paper, the deeper they dive into the details.

Dell Management Portal

The Dell Management Portal will support updates and Intune publishing for 6 Dell Applications:

1. **Dell Command | Monitor**
2. **Dell Command | End Point Configure for Microsoft Intune**
3. **Dell Command | Update**
4. **Dell Support Assist for Business PCs**
5. **Dell Trusted Device**
6. **Dell Client Device Manager**

Dell Management Portal – Application Status

There are 4 status categories for an application update in the Dell Management Portal

1. **Published –** Application versions already live in Intune, which may be deployed across IT Administrators' fleets. Status field will display "Installed" with a Gray icon.
2. **Optional Update Available –** Updates marked as optional by the development team. Status field will show "optional" with a blue icon.
3. **Recommended Update Available –** Updates tagged as recommended by the development team. Status field will display "recommended" with a green icon.
4. **Critical Update Available –** Updates deemed critical by the Dell team. Status field will show "critical" with a red icon.

Dell Management Portal – Model Status

'Dell Pro AI Studio' section displays the following information for available models
App Name –Title of the model
Status–Model status will show: Download available (green)