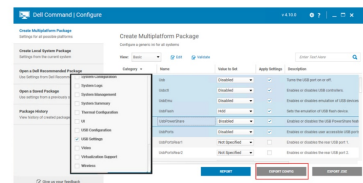


## DELL Command Endpoint Configure for Microsoft Intune



# DELL Command Endpoint Configure for Microsoft Intune User Guide

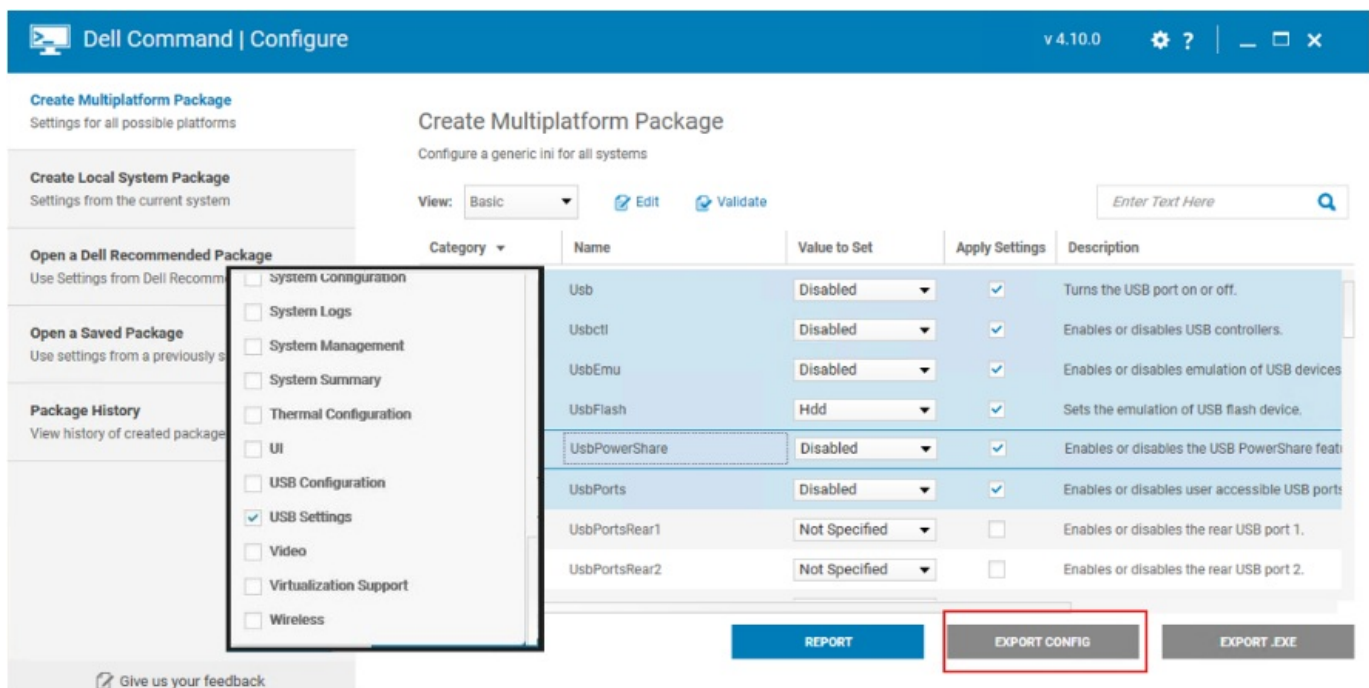
[Home](#) » [Dell](#) » DELL Command Endpoint Configure for Microsoft Intune User Guide 

## Contents

- [1 DELL Command Endpoint Configure for Microsoft Intune](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Introduction](#)
- [5 BIOS configuration profile](#)
- [6 Dell BIOS management](#)
- [7 Log Location for Troubleshooting](#)
- [8 Frequently asked questions](#)
- [9 Documents / Resources](#)
  - [9.1 References](#)



**DELL Command Endpoint Configure for Microsoft Intune**



## Product Information

### Specifications:

- **Product Name:** Dell Command | Endpoint Configure for Microsoft Intune
- **Version:** March 2024 Rev. A00
- **Functionality:** Manage and configure BIOS settings with Microsoft Intune

## Product Usage Instructions

### Chapter 1: Introduction

Dell Command | Endpoint Configure for Microsoft Intune (DCECMI) allows easy and secure management and configuration of BIOS settings through Microsoft Intune. It utilizes Binary Large Objects (BLOBs) to store data, configure BIOS settings with zero touch, and maintain unique passwords. For more detailed information on Microsoft Intune, refer to the Endpoint management documentation in Microsoft Learn.

### Chapter 2: BIOS Configuration Profile

Creating and Assigning a BIOS Configuration Profile:

1. Craft the BIOS configuration package as a Binary Large Object (BLOB) using Dell Command | Configure.
2. Sign in to Microsoft Intune admin center with the appropriate account having the Policy and Profile Manager role assigned.
3. Go to Devices > Configuration in the admin center.
4. Click on Policies and then Create Profile.
5. Select Windows 10 and later as the Platform.
6. Choose Templates in Profile type.
7. Select BIOS Configurations under Template name.
8. Click Create to create the BIOS configuration profile.

## FAQ




- **Q: Where can I find more information about installing Dell Command | Endpoint Configure for Microsoft Intune?**

A: The Installation Guide for Dell Command | Endpoint Configure for Microsoft Intune is available on the documentation page of Dell Command | Endpoint Configure for Microsoft Intune.

- **Q: How can I troubleshoot issues with Dell Command | Endpoint Configure for Microsoft Intune?**

A: The Log Location section in Chapter 4 of the user manual provides information on troubleshooting methods for the software.

## Notes, cautions, and warnings

-  **NOTE:** A NOTE indicates important information that helps you make better use of your product.
-  **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.
-  **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

© 2024 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

## Introduction

### Introduction to Dell Command | Endpoint Configure for Microsoft Intune (DCECM):

Dell Command | Endpoint Configure for Microsoft Intune (DCECM) enables you to manage and configure BIOS easily and securely with Microsoft Intune. The software uses Binary Large Objects (BLOBs) to store data, configure, and manage Dell system BIOS settings with zero-touch, and set and maintain unique passwords. For more information on Microsoft Intune, see Endpoint management documentation in [Microsoft Learn](#).

### Other documents you may need

The Dell Command | Endpoint Configure for Microsoft Intune Installation Guide provides information about installing Dell Command | Endpoint Configure for Microsoft Intune on supported client systems. The guide is available at Dell Command | Endpoint Configure for Microsoft Intune documentation page.

## BIOS configuration profile

### Creating and assigning a BIOS configuration profile

Once the BIOS configuration package is crafted as a Binary Large Object (BLOB), the Microsoft Intune administrator can use it to create a BIOS configuration profile. The profile can be created through Microsoft Intune Admin Center to manage the Dell commercial client systems in an IT environment.

### About this task

You can create a BIOS configuration package (.cctk) file using Dell Command | Configure. See Creating a BIOS package in Dell Command | Configure User's Guide at [Support | Dell](#) for more information.

## Steps

1. Sign in to [Microsoft Intune admin center](#) using the Intune account having the Policy and Profile Manager role assigned option.

2. Go to Devices > Configuration.
3. Click Policies.
4. Click Create Profile.
5. Select Windows 10 and later from the Platform drop-down list.
6. Select Templates in Profile type from the Platform drop-down list.
7. Under Template name, select BIOS Configurations.
8. Click Create. The BIOS configuration profile creation begins.
9. In the Basics tab, on Create BIOS configurations profile page, enter the Name of the profile and Description. The description is optional.
10. In the Configurations tab on Create BIOS configurations profile page, select Dell in the Hardware dropdown.
11. Select any of the following options for Disable per-device password protection:
  - If you select NO, then Microsoft Intune sends a unique-per-device, random BIOS administrator password that is applied on the device.
  - If you select YES, then the previously applied BIOS administrator password set through Microsoft Intune workflow is cleared.

**NOTE:** If the BIOS administrator password is not set through Microsoft Intune workflow, then the YES setting keeps the devices in a password-less state.
12. Upload the BIOS configuration package in Configuration file.
13. In the Assignments tab on Create BIOS configurations profile page, click Add groups under Included groups.
14. . Select the device groups where you want to deploy the package.
15. In the Review tab on Create BIOS configurations profile page, review the details of your BIOS package.
16. Click Create to deploy the package.

**NOTE:** Once the BIOS Configuration Profile is created, the profile is deployed to the targeted Endpoint Groups. The DCECM agent intercepts and applies it securely.

### Checking the deployment status of the BIOS Configuration Profile

To check the deployment status of the BIOS Configuration Profile, do the following:

#### Steps

1. Go to the Microsoft Intune admin center.
2. Sign in with a user who has the Policy and Profile Manager role assigned.
3. Click Devices in the navigation menu on the left.
4. Select Configuration in the Manage devices section.
5. Locate the BIOS Configuration Policy that you created, and click the policy name to open the details page. On the details page, you can view the device status—Succeeded, Failure, Pending, Unknown, Not applicable.

### Important considerations when deploying a BIOS configuration profile

- Use one BIOS configuration profile for a device group and update it when required, instead of creating a profile for a given device group.
- Do not target multiple BIOS Configuration Profiles to the same device group.
- Using one BIOS configuration profile avoids conflict between multiple profiles that are assigned to the same endpoint group.

- Deploying multiple profiles to the same endpoint group causes a race condition and results in a conflicting BIOS configuration state.
  - A Possible replay attack detected error message is also displayed in the EndpointConfigure.log. See Log Location for Troubleshooting for more details.
  - In the Intune portal, the error message is displayed as Verification of Metadata failed. See Verification of Metadata failed section in Frequently asked questions for more details.
- For updating an existing profile, do the following in the Properties tab of the BIOS configuration profile:
  1. Click Edit.
  2. Edit Disable per-device password protection or Configuration file by uploading a new .cctk configuration file. Modifying either or both of the above-mentioned options updates the profile version and triggers a profile redeployment to the assigned endpoint group.
  3. Click Review + save button.  
In the next tab, review the details and click Save.
- Do not modify BIOS Configuration Profiles in the Pending state.
  - If there is already an existing BIOS Configuration Profile that is deployed to the endpoint groups and the status is displayed as Pending, do not update that BIOS Configuration Profile.
  - You must not update until the status transitions from Pending to Succeeded or Failure.
  - Modifying may cause conflicts and subsequent BIOS Configuration Profile version failures. Sometimes, BIOS Password sync failures may occur, and you may not be able to see the newly applied BIOS Password.
- When managing passwords using Microsoft Intune Admin Center user interface, remember the following:
  - If you select NO for Disable per-device password protection, then Intune sends a random BIOS administrator password that is applied on the device.
  - If you select YES for Disable per-device password protection, then the previously applied BIOS administrator password through Intune workflow is cleared.
  - If no BIOS administrator password was applied earlier through Intune workflow, then the setting helps keep the devices in a password-less state.
- Dell Technologies recommends using Intune Password Manager for BIOS Password Management, as the application provides superior security and manageability.

## **Dell BIOS management**

### **Microsoft Graph API for Dell BIOS management**

In order to use graph APIs for Dell BIOS Management, an application must have the following scopes assigned:

- DeviceManagementConfiguration.Read.All
- DeviceManagementConfiguration.ReadWrite.All
- DeviceManagementManagedDevices.PrivilegedOperations.All

The following graph APIs can be used for Dell BIOS management:

- Create hardware configuration
- assign Hardware Configuration action

- List hardware configurations
- Get hardware configuration
- Delete hardware configuration
- Update hardware configuration

The following graph APIs can be used for Dell BIOS Password management:

- List hardware Password Infos
- Get hardware Password Info
- Create hardware Password Info
- Delete hardware Password Info
- Update hardware Password Info

### Using Graph APIs to retrieve the Dell BIOS Password manually

- **Prerequisites**

Ensure that you use Microsoft Graph Explorer.

- **Steps**

1. Sign in to Microsoft Graph Explorer using Intune Global Administrator credentials.
2. Change the API to beta version.
3. List the hardware password information of all the devices using the URL  
<https://graph.microsoft.com/beta/deviceManagement/hardwarePasswordInfo>.
4. Click Modify permissions.
5. Enable DeviceManagementConfiguration.Read.All, DeviceManagementConfiguration.ReadWrite.All, and DeviceManagementManagedDevices.PrivilegedOperations.All.
6. Click Run Query.

The hardware password information of all the devices, the current password, and the list of the previous 15 passwords are listed in a readable format in Response preview.

### Important Information

- System administrators can use Microsoft Graph Explorer or create PowerShell scripts using PowerShell SDK for Microsoft Intune Graph API from [PowerShell Gallery](#) to fetch Dell BIOS Password Information.
- Dell BIOS Password management Graph APIs also supports filters. For example, to get the hardware password information of a particular device using Serial number, go to  
[https://graph.microsoft.com/beta/deviceManagement/hardwarePasswordInfo?\\$filter=serialNumber](https://graph.microsoft.com/beta/deviceManagement/hardwarePasswordInfo?$filter=serialNumber).

**NOTE:** Only List hardwarePasswordInfos and Get hardwarePasswordInfo APIs are supported. Create hardwarePasswordInfo, Delete hardwarePasswordInfo, and Update hardwarePasswordInfo APIs are not supported now.

### Log Location for Troubleshooting

Dell Command | Endpoint Configure for Microsoft Intune (DCECM) implements file logging functionality. You can use verbose logs for DCECM.

The log file is available at C:\ProgramData\Dell\EndpointConfigure. The file name is EndpointConfigure.log.

To enable detailed logs, do the following:

1. Go to the registry location HKLM\Software\Dell\EndpointConfigure\.
2. Create a DWORD 32 registry key with the name LogVerbosity.
3. Assign it a value of 12.
4. Restart DCECMI, and observe the verbose logs.

**Table 1.** DCECMI logs

Verbosity Value	Message	Description
1	Fatal	Critical error has occurred, and the system is considered unstable.
3	Error	A serious error has occurred that is not deemed fatal.
5	Warning	Warning message for user.
10	Informational	This message is for informational purposes.
12	Verbose	Other informational messages that can be logged and viewed depending on the verbosity level.

## Frequently asked questions

- **How do I switch over to the Intune or AAD-managed password when I already have a BIOS password?**
  - Intune does not provide a way to seed the initial password into AAD.
  - To switch over to the Intune or AAD-managed password, clear the existing BIOS password using the same method that is used to set the BIOS password.

**NOTE:** Dell Technologies does not have a master password and cannot bypass the customer password.
- **How do I get the password for a device that I have to manually service?**

Microsoft Intune does not display the password in the device properties. Go to Using Graph APIs to retrieve the Dell BIOS Password manually for more information.

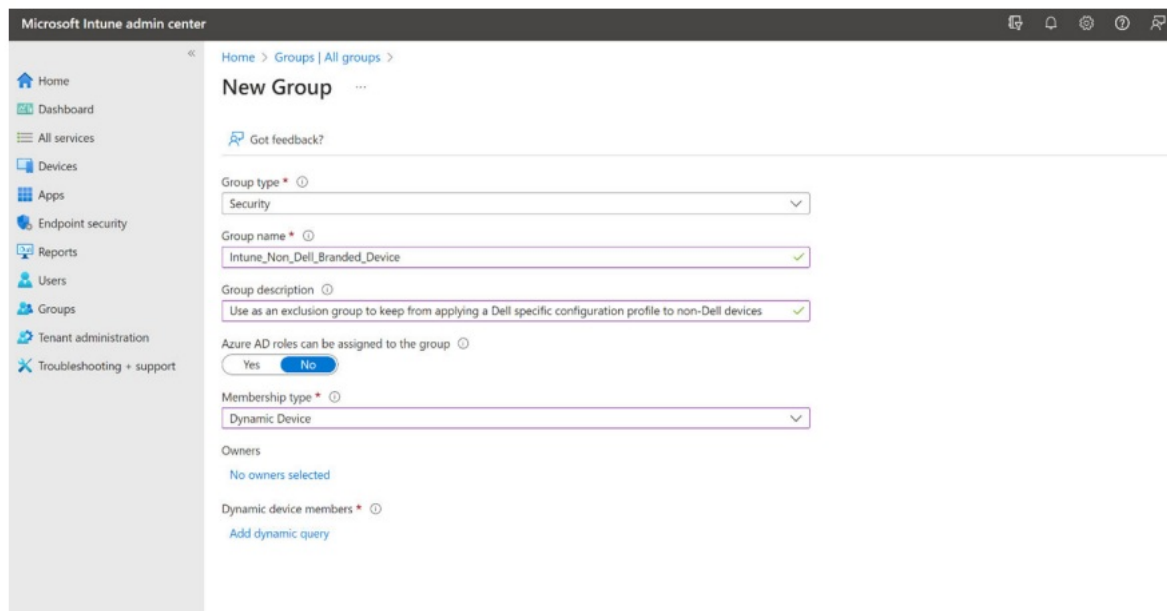
**NOTE:** Only List hardwarePasswordInfos and Get hardwarePasswordInfo are supported.
- **How do I pass a unique-per-device password to Dell Command | Update so that it can update the firmware?**

Dell Command | Update does not use a capsule BIOS update method that can securely bypass the BIOS password. Windows Update, Autopatch, and Windows Update for Business uses the Dell capsule BIOS update method. If you have deployed a unique-per-device password, you can use them. Ensure that Capsule BIOS update is enabled in BIOS settings.
- **How do I keep from applying the BIOS configuration profile to non-Dell devices?**

Currently, filters are not supported in the BIOS configuration profile assignment. Instead, you can assign an exclusion group for non-Dell devices.

To create a dynamic exclusion group, follow these steps:

1. In Microsoft Intune admin center, go to Home > Groups | All groups > New Group.



**Figure 1. Dynamic exclusion group**

2. In the Membership type drop-down list, select Dynamic Device.
3. Create the dynamic query according to the Dynamic membership rules for groups in Azure Active Directory guidelines in [Microsoft](#).

- **Where do I find the logs to debug any issues?**

Dell log files can be found here: C:\ProgramData\dell\EndpointConfigure\EndpointConfigure<\*>.log. Microsoft log files can be found here: C:\ProgramData\Microsoft\IntuneManagementExtension\Logs\<\*>.log

- **How do I resolve agent-reported errors?**

Here are some agent-reported errors that you may see:

- Agent reported error: 65
  - Description—The setup Password is required to change the setting. Use –ValSetupPwd to provide a password.
  - This issue is observed when the device already has a BIOS password. To resolve the issue, use the Intune BIOS password manager and clear the current BIOS password using Dell Command | Configure tool or by logging into BIOS Setup. Then, deploy a new BIOS Configuration profile using Intune with the option Disable per-device password protection set to NO.
- **Agent reported error: 58**
  - Description—The setup password that is provided is incorrect. Try again.
  - The issue is observed when multiple BIOS configuration profiles are used for the same device group. Delete the additional BIOS configuration profiles that are failing to fix the issue.
  - The issue can also be observed when the BIOS configuration profiles are modified when the status is Pending.

**NOTE:** See Important Information for more details.

- **Verification of Metadata failed**

- The issue is observed when there are any failures while verifying the correctness of BIOS Configuration Profile metadata.
- The agent reports the status as Failed with the error Verification of Metadata failed.
- No BIOS configurations are performed.
- To resolve this issue, try redeploying the BIOS Configuration Profile, or delete and create a BIOS



- **How do I decode the error code return from DCECMI in the Microsoft Intune report?**

See Dell Command | Configure Error Codes at Support | Dell for a list of all the error codes and their meaning.

- **How do I enable DCECMI verbose logs for troubleshooting?**

1. Go to the registry location HKLM\Software\Dell\EndpointConfigure\.
2. Create a DWORD 32 registry key with the name LogVerbosity.
3. Assign it a value of 12.
4. Restart Dell Command|Endpoint Configure for Microsoft Intune-service from Services.msc and observe the C:\ProgramData\Dell\EndpointConfigure\EndpointConfigure.log log for verbose messages.

See Dell Command | Configure Error Codes at Support | Dell for a list of all the error codes and their meaning.

You can also see Log Location for Troubleshooting for more information.

- **How do I deploy DCECMI or create and deploy Win32 applications from Microsoft Intune?**

See Dell Command | Endpoint Configuration for Microsoft Intune Installation Guide at Support | Dell on how to deploy a DCECMI Win32 application using Microsoft Intune. The package autopopulates the DCECMI install commands, uninstall commands, and the detection logic, once uploaded to Windows applications on Microsoft Intune.

- **If I do not want to use the secure random password from Intune password manager and instead use CCTK files for password operations with my custom password, is that allowed?**

- It is highly recommended to use Intune Password Manager for BIOS password management due to the advantages offered.
- If the password is set using .cctk file and not using Intune Password Manager, the password does not switch to Intune or AAD-managed password.
- The Intune password manager does not know anything that is related to the BIOS password set using a .cctk file or manually.
- The BIOS password is displayed as null/empty when Microsoft Graph APIs are used to fetch the BIOS password.

- **Where are my passwords stored or synced?**

Passwords generated by you, in the CCTK file, are not stored, synced, or managed by Intune or Graph. Only secure, random, unique per device passwords that are generated by Intune, using the Yes/No toggle for Disable per-device BIOS password protection, are synced or managed by Intune or Graph.

- **In which scenarios are profiles retrigged?**

- BIOS configuration profiles are not designed for proactive remediations in Intune.
- A profile is not deployed repeatedly once successfully applied on the device. A profile is redeployed only when you modify the profile in Intune.
- You can also edit Disable per-device password protection or Configuration file by uploading a new .cctk configuration file.
- Modifying either or both of the above-mentioned options updates the profile version and triggers a profile redeployment to the assigned endpoint group.

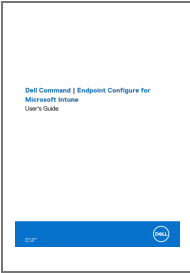
## **Contacting Dell**

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues, go to [dell.com](https://www.dell.com).






If you do not have an active Internet connection, you can find contact information on your purchase invoice,

packing slip, bill, or Dell product catalog

Documents / Resources

	<p><a href="#">DELL Command Endpoint Configure for Microsoft Intune</a> [pdf] User Guide</p> <p>Command Endpoint Configure for Microsoft Intune, Endpoint Configure for Microsoft Intune, Configure for Microsoft Intune, Microsoft Intune, Intune</p>
---	--

References

-  [graph.microsoft.com/beta/](https://graph.microsoft.com/beta/)
-  [Microsoft Intune admin center](#)
-  [Microsoft Learn: Build skills that open doors in your career](#)
-  [Your request has been blocked. This could be due to several reasons.](#)
-  [PowerShell Gallery | Home](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.