

Adlumin MDR

Microsoft Entra ID application setup script for Adlumin

Version 2

Table of Contents

PREFACE	3
OVERVIEW.....	3
PREREQUISITES.....	3
INSTRUCTIONS	4
MAKING SURE THAT SCRIPTS CAN RUN ON YOUR SYSTEM	4
RUNNING THE SCRIPT	5
CHECKING FOR POWERSHELL MODULES	5
CONNECTING TO ENTRA ID.....	5
CONNECTING TO EXCHANGEONLINE	6
CHECKING IF UNIFIED AUDIT LOG INGESTION IS ENABLED	7
PROVIDING AN EXISTING ENTRA ID APP TO THE SCRIPT	7
RECEIVING THE OUTPUT FROM THE SCRIPT	8
ENTERING THE OUTPUT INTO ADLUMIN	8

Preface

This document is provided for informational purposes only. Information and views expressed in this document may change and/or may not be applicable to you. This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of N-able. N-ABLE DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL N-ABLE, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF N-ABLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Overview

To configure Adlumin MDR to connect to your Entra ID tenant, an Entra ID Application needs to be registered, providing the required permissions for specific SKUs, authorizing them, and ensuring that full auditing in Microsoft Purview is enabled.

As this is a time intensive process, N-able has created a script which automates the creation of an Entra ID app, along with applying and authorizing the required permissions based on the SKUs which the Entra ID tenant has. Additionally, the script connects to Exchange Online and enables full auditing for the tenant in question.

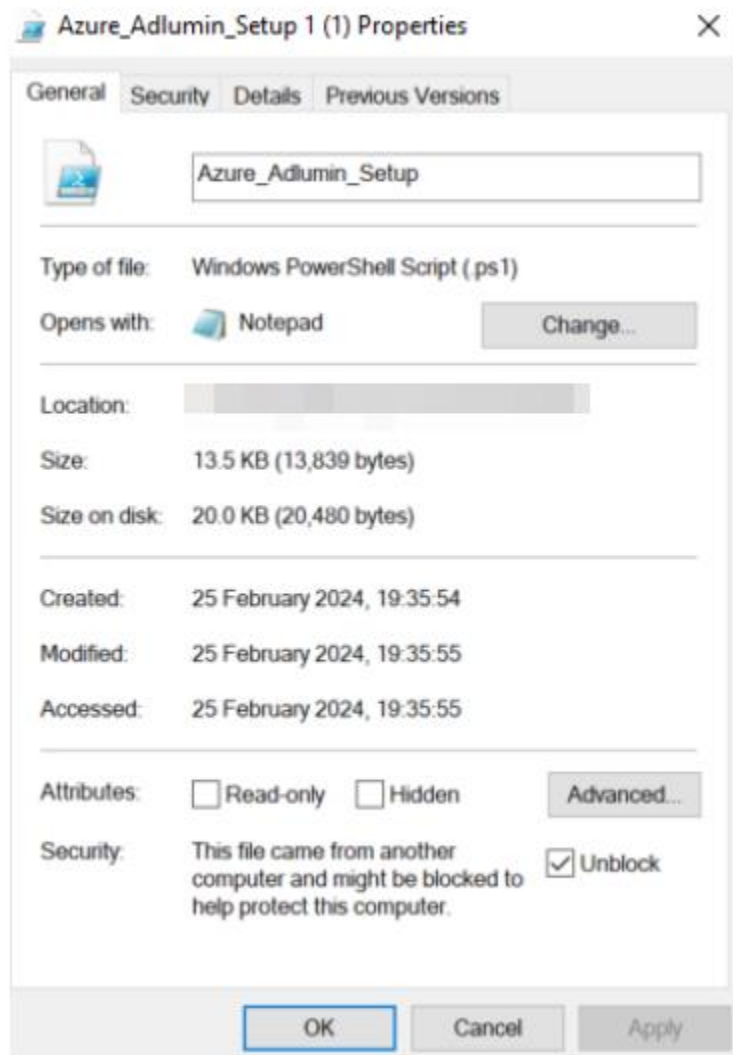
Prerequisites

There are a few prerequisites required for the script to run successfully:

- Windows PowerShell 5.0 or higher, or PowerShell Core 7 or higher, running on a Windows OS device.
- An Entra ID account which has permissions to use the following Entra ID scopes (Admin access to the tenant contains these by default):
 - Application.Read.All
 - Application.ReadWrite.All
 - User.Read.All
 - RoleManagement.ReadWrite.Directory
 - Directory.ReadWrite.All
 - Organization.Read.All
 - AuditLog.Read.All
 - AppRoleAssignment.ReadWrite.All
- The following PowerShell modules installed (the script will request approval to install these on your behalf if they are not found on the device running the script):
 - Microsoft.Graph.Authentication (version 2.26.1)
 - Microsoft.Graph.Applications (version 2.26.1)
 - Microsoft.Graph.Identity.Governance (version 2.26.1)
 - Microsoft.Graph.Identity.DirectoryManagement (version 2.26.1)
 - ExchangeOnlineManagement

Instructions

This document will have been provided to you inside a zip file. You will find a script file called *Azure_Adlumin_Setup.v3.0.ps1*. Extract the zip file if you haven't already. Find the file through Explorer, right click > Properties and tick **Unblock** if visible. Click **OK**.



Making sure that scripts can run on your system

Open up your Windows PowerShell instance as administrator, and type *powershell.exe -executionpolicy bypass -nopprofile*. This will start a PowerShell session ready to run the script.

```
PS C:\Users\ [redacted] > powershell.exe -executionpolicy bypass -nopprofile
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ [redacted] > get-executionpolicy
Bypass
```

Running the script

To run the script, **change directory** using the `cd` cmdlet, to the location of the script. For this document, the script is contained in `C:\users\<username>\downloads\Entra ID Adlumin Setup`. To `cd` to this folder, you would run `cd "C:\users\<username>\downloads\Entra ID Adlumin Setup"` like so:

```
PS C:\Users\<username>\downloads\Entra ID Adlumin Setup> cd "C:\users\<username>\downloads\Entra ID Adlumin Setup"
PS C:\users\<username>\downloads\Entra ID Adlumin Setup> |
```

And finally, run the script using dot backslash, typing `.\Azure_Adlumin_Setup.v3.0ps1` like so:

```
PS C:\users\<username>\downloads\Entra ID Adlumin Setup> .\Azure_Adlumin_Setup.ps1
Working directory C:\ProgramData\N-Able Technologies\N-hanced Services\Azure Adlumin Setup has been created.
[24/04/25 14:39:56] - [VERBOSE]: Log file C:\ProgramData\N-Able Technologies\N-hanced Services\Azure Adlumin Setup\Azure_Adlumin_Setup.log has been created. Switched to logfile logging format.
[24/04/25 14:39:56] - [VERBOSE]: Checking if modules Microsoft.Graph.Authentication, Microsoft.Graph.Applications, Microsoft.Graph.Identity.Governance, Microsoft.Graph.Identity.DirectoryManagement, ExchangeOnlineManagement are installed, and if Microsoft Graph modules are installed with version 2.26.1.
```

Checking for PowerShell modules

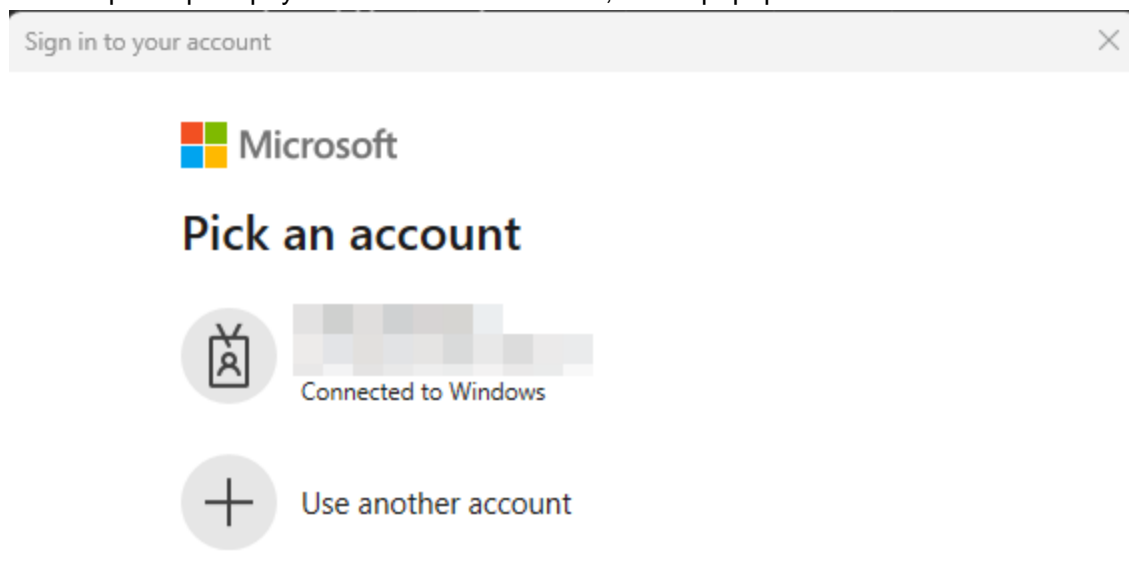
Once the script runs, the first thing it does is check for the required PowerShell modules, as seen below. If the modules are not found, or the versions of the modules required are not found, the script will prompt you to approve installation of the modules.

Note: The script locks the Microsoft Graph modules to version 2.26.1, as 2.25.0 and 2.27.0 cause breaking issues with Entra ID applications. At the time of writing, 2.27.0 has not received a patch.

```
[24/04/25 14:50:01] - [VERBOSE]: Checking if modules Microsoft.Graph.Authentication, Microsoft.Graph.Applications, Microsoft.Graph.Identity.Governance, Microsoft.Graph.Identity.DirectoryManagement, ExchangeOnlineManagement are installed, and if Microsoft Graph modules are installed with version 2.26.1.
[24/04/25 14:50:02] - [ERROR]: The following modules are missing: Microsoft.Graph.Authentication, Microsoft.Graph.Applications, Microsoft.Graph.Identity.Governance, Microsoft.Graph.Identity.DirectoryManagement, ExchangeOnlineManagement
[24/04/25 14:50:02] - [INFO]: Do you wish to install these modules? [Y/N]
y
[24/04/25 14:50:04] - [INFO]: Installing module Microsoft.Graph.Authentication with version 2.26.1.
[24/04/25 14:50:13] - [INFO]: Installing module Microsoft.Graph.Applications with version 2.26.1.
```

Connecting to Entra ID

The script will prompt you to connect to Entra ID, with a popup:

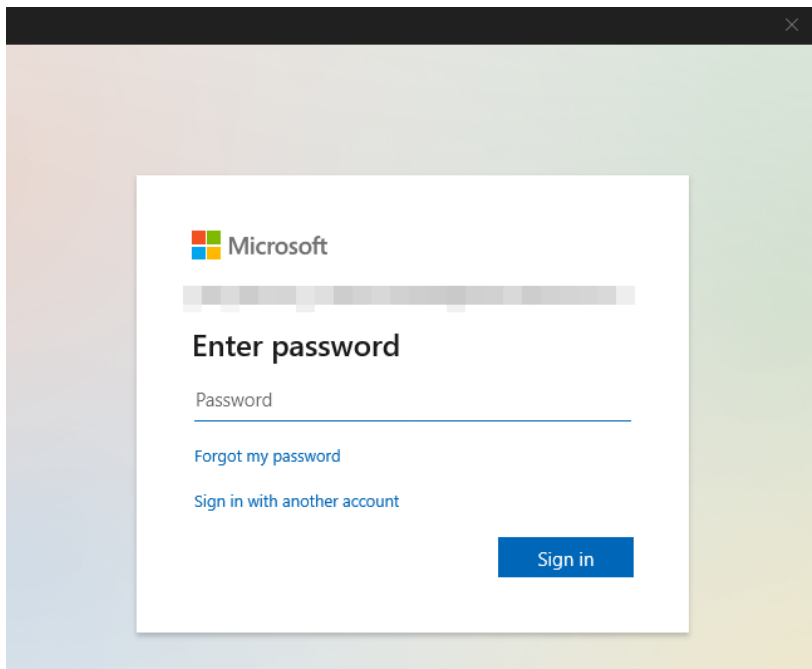


Please provide the required credentials to connect to your Entra ID tenant. If you are unsure which to provide, please use an Entra ID administrator account.

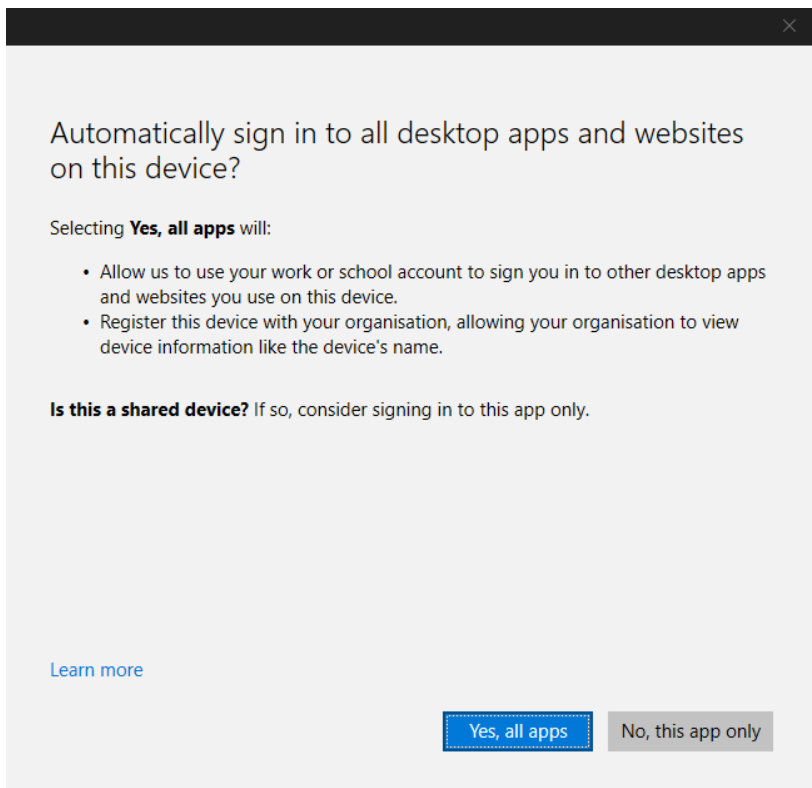
Connecting to ExchangeOnline

The script will then prompt you to connect to Exchange Online. This is for the purposes of determining whether full auditing is enabled in Microsoft Purview. The same username entered when connecting to Entra ID, is automatically populated for connecting to ExchangeOnline.

Note: While Microsoft Graph and Exchange Online use similar authentication methods, the authentication from Microsoft Graph cannot be used to automatically authenticate Exchange Online.



If prompted, choose **No, this app only**.



Checking if Unified Audit Log Ingestion is enabled

After connecting to Entra ID and ExchangeOnline, the script will check whether Unified Audit Log Ingestion is enabled, and if it is disabled, will enable this for you.

```
[24/04/25 14:58:37] - [INFO]: Connecting to Exchange Online to determine if Purview auditing is enabled.
[24/04/25 15:01:22] - [INFO]: Unified Audit Log Ingestion is enabled. Purview logging is fully enabled.
```

Providing an existing Entra ID app to the script

The script will check to see if an existing app called *N-able Technologies – Adlumin MDR Integration* exists. If so, the script will continue on.

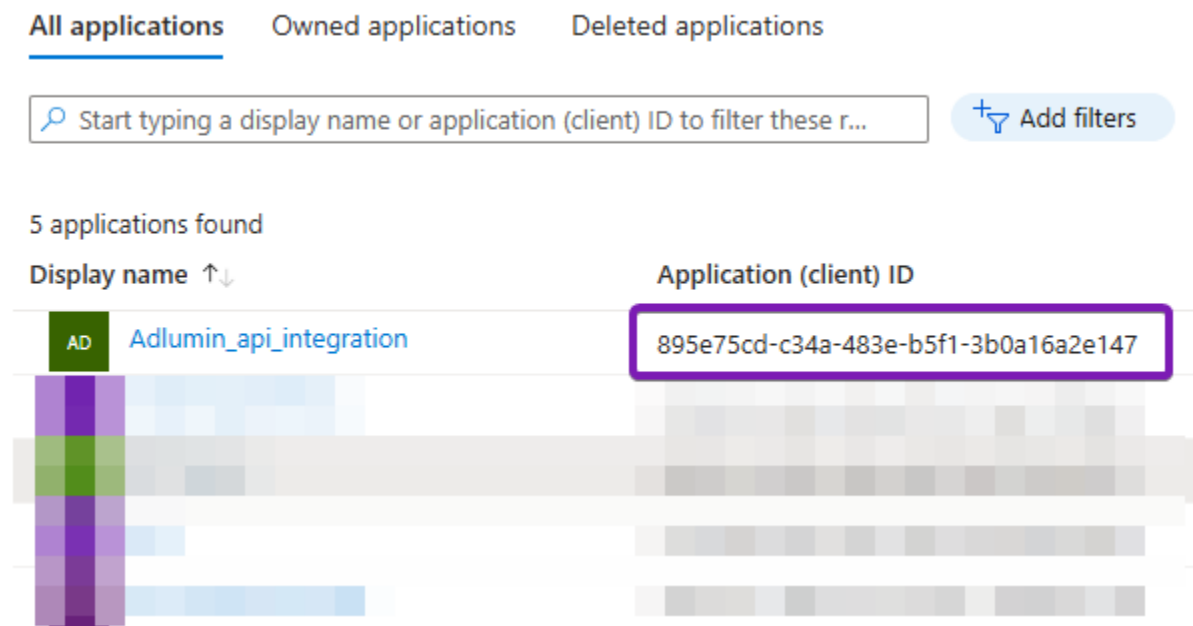
If this is your first time running the script, or if you have a previously created Entra ID app integrated with Adlumin which was created using a different script or by the Entra ID console, you will see this:

```
[24/04/25 15:01:22] - [INFO]: Looking for an existing app with name N-able Technologies - Adlumin MDR Integration.
[24/04/25 15:01:22] - [INFO]: App N-able Technologies - Adlumin MDR Integration not found.
[24/04/25 15:01:22] - [INFO]: Do you have an existing Entra ID App registered for Adlumin? [Y/N]
```

The script will wait for you to enter **Y** or **N**.

If you have not integrated Entra ID with Adlumin, type in **N** into PowerShell and press **Enter**.

If you have an existing Entra ID app integrated with Adlumin, login to your Entra ID Portal, navigate to **Applications > App Registrations**, click on the **All applications** tab and copy the *Application (client) ID* as seen in the below example.



Back in PowerShell, type in **Y** and press **Enter**. Paste (right click to paste in PowerShell) in the *Application (client) ID* you copied, and press **Enter** as seen below.

```
[24/04/25 15:01:22] - [INFO]: Looking for an existing app with name N-able Technologies - Adlumin MDR Integration.
[24/04/25 15:01:22] - [INFO]: App N-able Technologies - Adlumin MDR Integration not found.
[24/04/25 15:01:22] - [INFO]: Do you have an existing Entra ID App registered for Adlumin? [Y/N]
y
[24/04/25 15:09:54] - [INFO]: Please enter the App ID of the existing app. This will be called Application (client) ID i
n the Entra ID portal.
895e75cd-c34a-483e-b5f1-3b0a16a2e147
[24/04/25 15:11:14] - [INFO]: *****
[24/04/25 15:11:14] - [INFO]:
[24/04/25 15:11:14] - [INFO]: Enterprise App Adlumin_api_integration has been found in your tenant.
[24/04/25 15:11:14] - [INFO]: Would you like the script to update the existing app permissions? [Y/N]
```

Type **Y** and press Enter.

Receiving the output from the script

No matter whether an existing application is found/used above, the script will either create a new app, then add and authorize permissions, or the script will update and authorize permissions on the existing app.

Once this is completed, an output will be sent to the console.

For a new app, this looks like the following:

```
[24/04/25 15:16:25] - [INFO]: *****
[24/04/25 15:16:25] - [INFO]: The Following Items Should Be Entered Into the Adlumin Azure Integration Section For Tenant
[24/04/25 15:16:25] - [INFO]:
[24/04/25 15:16:25] - [INFO]: Domain Name:
[24/04/25 15:16:25] - [INFO]: ClientID:
[24/04/25 15:16:25] - [INFO]: TenantID:
[24/04/25 15:16:25] - [INFO]: Client Secret:
[24/04/25 15:16:25] - [INFO]:
[24/04/25 15:16:25] - [INFO]: Audit Logging is fully enabled.
[24/04/25 15:16:25] - [INFO]: *****
```

For an existing app, this looks like the following:

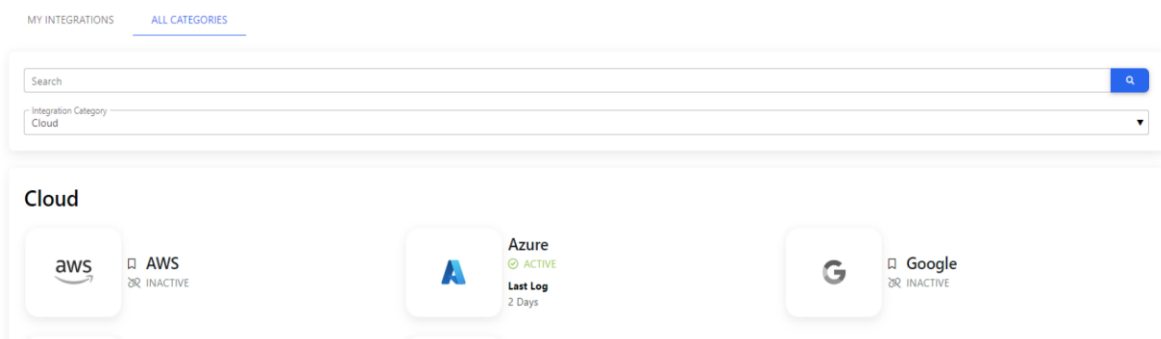
```
[24/04/25 15:12:25] - [INFO]: *****
[24/04/25 15:12:25] - [INFO]: The Following Items Should Be Entered Into the Adlumin Azure Integration Section For Tenant
[24/04/25 15:12:25] - [INFO]:
[24/04/25 15:12:25] - [INFO]: Domain Name:
[24/04/25 15:12:25] - [INFO]: ClientID:
[24/04/25 15:12:25] - [INFO]: TenantID:
[24/04/25 15:12:25] - [INFO]: Client Secret: The Client Secret has not been regenerated. If you do not remember your existing secret, please regenerate it manually.
[24/04/25 15:12:25] - [INFO]:
[24/04/25 15:12:25] - [INFO]: Audit Logging is fully enabled.
[24/04/25 15:12:25] - [INFO]: *****
```

Entering the output into Adlumin

If you have never integrated Entra ID with Adlumin, take the output from PowerShell (highlight with left click and hold, and right click to copy), and open up your Adlumin MDR console.

1. Navigate to Integrations in the left navigation bar.
2. Under the *cloud* integration, choose **Azure**.

Integrations



3. Input the details you copied into the configurations menu. Once complete, click **Enable**, and Adlumin will link to your Entra ID tenant.

If you have previously integrated Entra ID with Adlumin, any additional permissions the script added to your Entra ID app, will allow Adlumin more visibility into your Entra ID tenant.

If required, open up your Entra ID app in your Entra ID console (**Applications > App registrations**)

and click on **API Permissions** under Manage to review the permissions added, and authorized.

[N-able Technologies - Adlumin MDR Integration | API permissions](#)

[Refresh](#)
[Got feedback?](#)

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (31)				
AuditLog.Read.All	Application	Read all audit log data	Yes	Granted for N-Able Tec...
DeviceManagementApps.Rea	Application	Read Microsoft Intune apps	Yes	Granted for N-Able Tec...
DeviceManagementApps.Rea	Application	Read and write Microsoft Intune apps	Yes	Granted for N-Able Tec...
DeviceManagementConfigur	Application	Read Microsoft Intune device configuration and policies	Yes	Granted for N-Able Tec...
DeviceManagementConfigur	Application	Read and write Microsoft Intune device configuration and ...	Yes	Granted for N-Able Tec...
DeviceManagementManagec	Application	Perform user-impacting remote actions on Microsoft Intu...	Yes	Granted for N-Able Tec...
DeviceManagementManagec	Application	Read Microsoft Intune devices	Yes	Granted for N-Able Tec...
DeviceManagementManagec	Application	Read and write Microsoft Intune devices	Yes	Granted for N-Able Tec...
DeviceManagementRBAC.Re	Application	Read Microsoft Intune RBAC settings	Yes	Granted for N-Able Tec...
DeviceManagementRBAC.Re	Application	Read and write Microsoft Intune RBAC settings	Yes	Granted for N-Able Tec...
DeviceManagementServiceC	Application	Read Microsoft Intune configuration	Yes	Granted for N-Able Tec...
DeviceManagementServiceC	Application	Read and write Microsoft Intune configuration	Yes	Granted for N-Able Tec...
Directory.Read.All	Application	Read directory data	Yes	Granted for N-Able Tec...
IdentityRiskEvent.Read.All	Application	Read all identity risk event information	Yes	Granted for N-Able Tec...
IdentityRiskyUser.ReadWrite	Application	Read and write all risky user information	Yes	Granted for N-Able Tec...
Policy.Read.All	Application	Read your organization's policies	Yes	Granted for N-Able Tec...
Policy.ReadWrite.Conditional	Application	Read and write your organization's conditional access poli...	Yes	Granted for N-Able Tec...
SecurityActions.Read.All	Application	Read your organization's security actions	Yes	Granted for N-Able Tec...
SecurityActions.ReadWrite.All	Application	Read and update your organization's security actions	Yes	Granted for N-Able Tec...
SecurityAlert.Read.All	Application	Read all security alerts	Yes	Granted for N-Able Tec...
SecurityAlert.ReadWrite.All	Application	Read and write to all security alerts	Yes	Granted for N-Able Tec...



N-able, Inc.(NYSE: NABL), the solutions partner helping IT services providers deliver security, data protection, and remote monitoring and management services. N-able fuels IT services providers with powerful software solutions to monitor, manage, and secure their customers' systems, data, and networks. Built on a scalable platform, we offer secure infrastructure and tools to simplify complex ecosystems, as well as resources to navigate evolving IT needs. We help partners excel at every stage of growth, protect their customers, and expand their offerings with an ever-increasing, flexible portfolio of integrations from leading technology providers. n-able.com

The N-ABLE, RMM, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

© 2025 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.