Microsoft Defender for Endpoint

IP Address Exclusion Procedure

Version 1.0

April, 2026

Panasonic Corporation

Table of contents

1 Introduction

1.1 Background

If you use the Media Production Suite software (hereinafter “MPS”) in a PC environment where Microsoft Defender for Endpoint (Microsoft Defender for Enterprise; hereinafter “MDE”) is deployed, MDE may block communication with the camera, causing MPS to behave abnormally.

Specifically, the following symptoms may occur in MPS:

1. The MPS screen stops updating.
2. Camera controls in MPS stop responding.
3. Auto Tracking and Auto Framing stop operating.

Depending on the timing, the camera may continue panning/tilting/zooming in one direction. The system becomes usable again after about 1–2 minutes, but the abnormal behavior may recur a few minutes later, repeating this cycle.

If the issue above occurs, the organization’s IT/system administrator must add the camera’s IP address to the exclusion list in the MDE management console.

You can determine whether MDE is enabled by confirming that the Windows service “Sense” is running.

Example check using a PowerShell command

```
PS> Get-Service Sense

Status      Name                    DisplayName
------      ----                    -----------
Running     Sense                   Sense
```

1.2 Purpose

This document provides procedures for organizational IT/system administrators to register a camera’s IP address as an exclusion in the MDE management console.

2 IP Address Exclusion Registration Procedure

2.1 Important Notes (Confirm Device Management Type)

The method for configuring IP address exclusions differs depending on how the device is managed (Microsoft Defender for Endpoint-managed device or Intune-managed device).

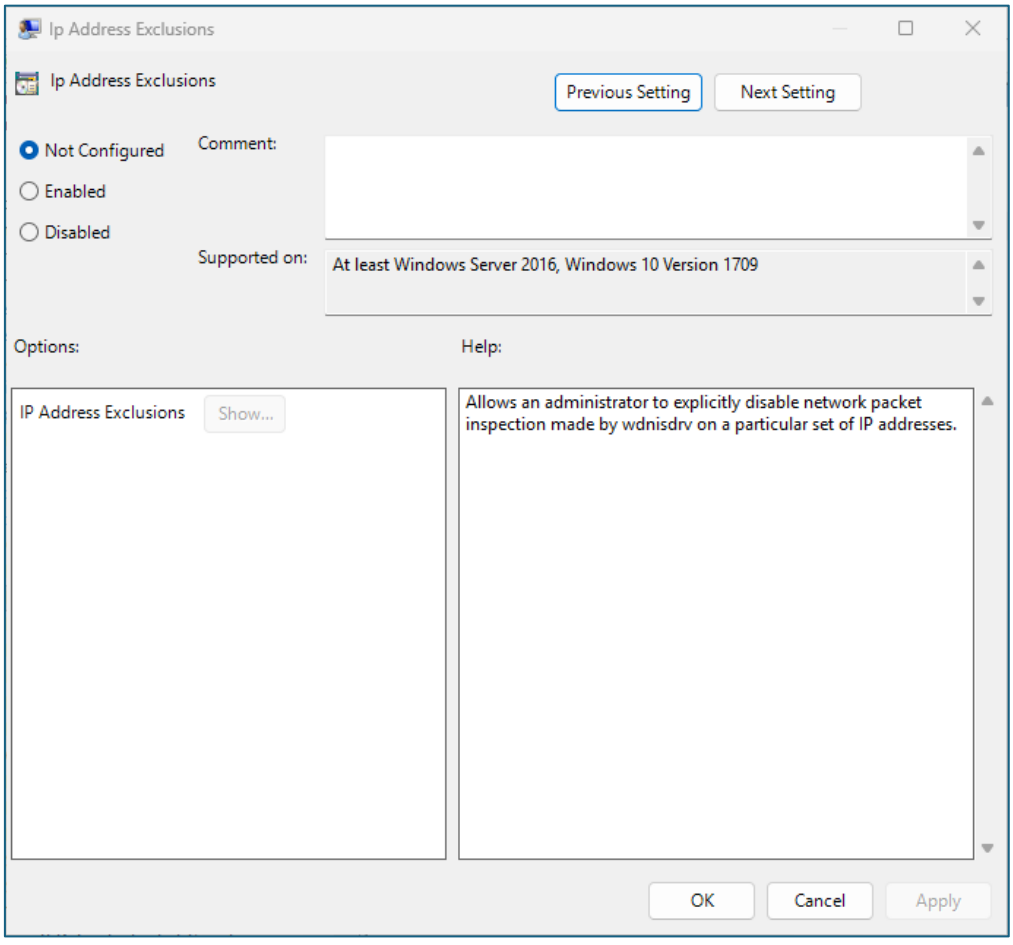
Refer to the section linked below and configure the exclusions.
2.2 How to Exclude a Camera IP Address Using Group Policy

Refer to the section linked below and configure the exclusions.
2.3 How to Exclude an IP Address Using Intune

2.2 How to Exclude a Camera IP Address Using Group Policy

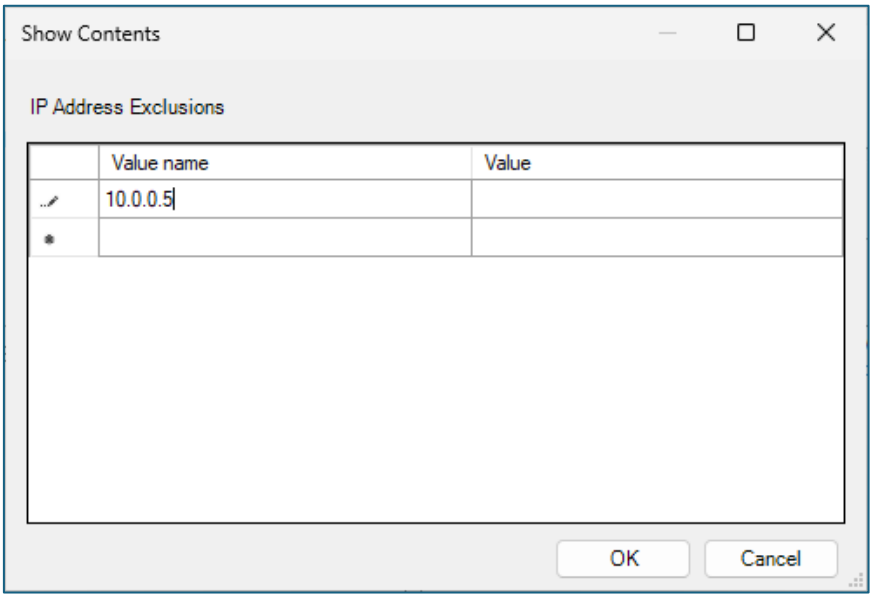
By specifying the camera's IP address as an exclusion in the following Active Directory Group Policy management settings, you can prevent that camera from being subject to MDE communication blocking.

From Windows [Run], type gpedit.msc to launch the Group Policy Editor, and then open the following item.
Path: [Administrative Templates] > [Windows Components] > [Microsoft Defender Antivirus] > [Exclusions]
Setting: IP Address Exclusions



In the "IP Address Exclusions" policy, set the camera IP address you want to exclude as the "Value name" to register it as an exclusion.

Example: Excluding IP address 10.0.0.5



Only individual IP addresses are supported. You cannot specify CIDR notation (e.g., 192.168.10.0/24) or wildcards. Enter each camera IP address you want to exclude one by one.

To verify the settings, run the following command in an administrator-elevated PowerShell session on the PC that runs Media Production Suite.

Verification command:
Get-MpPreference | select -expand ExclusionIPAddress

This completes the procedure for excluding an IP address using Group Policy.

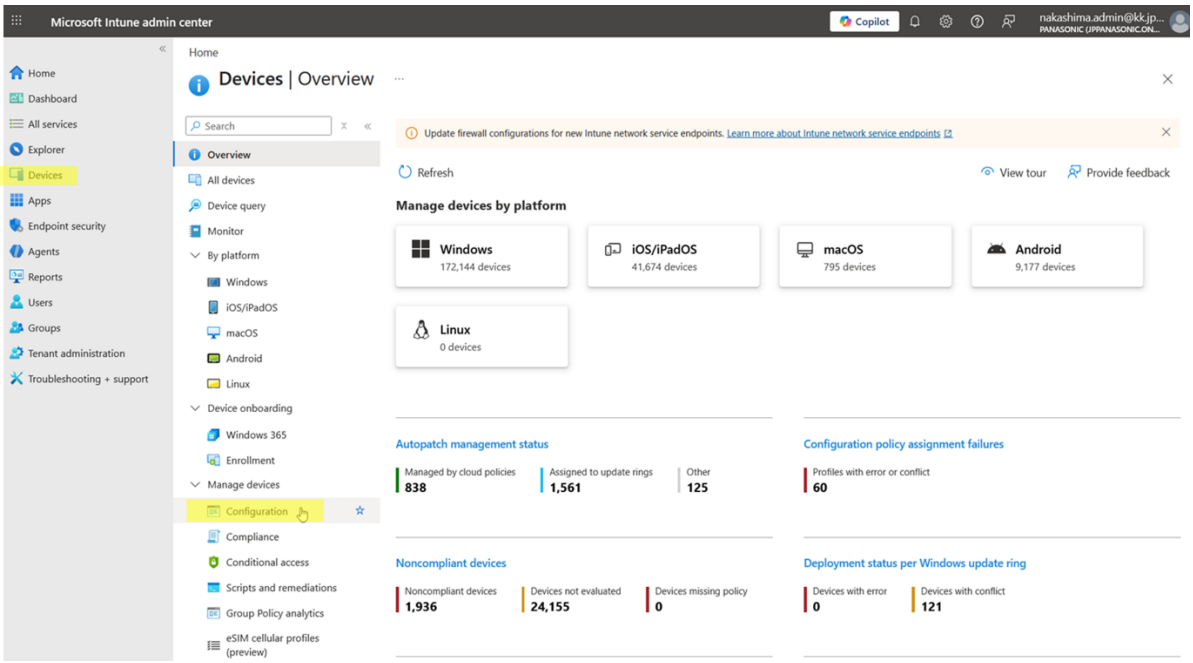
2.3 How to Exclude an IP Address Using Intune

Note (for Intune-managed devices): On devices managed by Intune, Microsoft Defender Antivirus settings configured by Intune take precedence. In that case, IP address exclusions configured via Group Policy or local PowerShell commands will not be applied. To exclude IP addresses on Intune-managed devices, use the Intune-based method described in this section.

Typically, to change Microsoft Defender Antivirus (MDAV) settings from Intune, you can use an AV policy under [Endpoint security] - [Antivirus].
However, AV policies do not support IP address exclusions. When using Intune, you can configure this by using the Settings catalog in a device configuration policy.

The following steps describe an example of creating a new policy.

After signing in to the Microsoft Intune admin center (intune.microsoft.com), navigate to [Devices] – [Manage devices] – [Configuration], and then start creating a new policy by selecting “Create”.

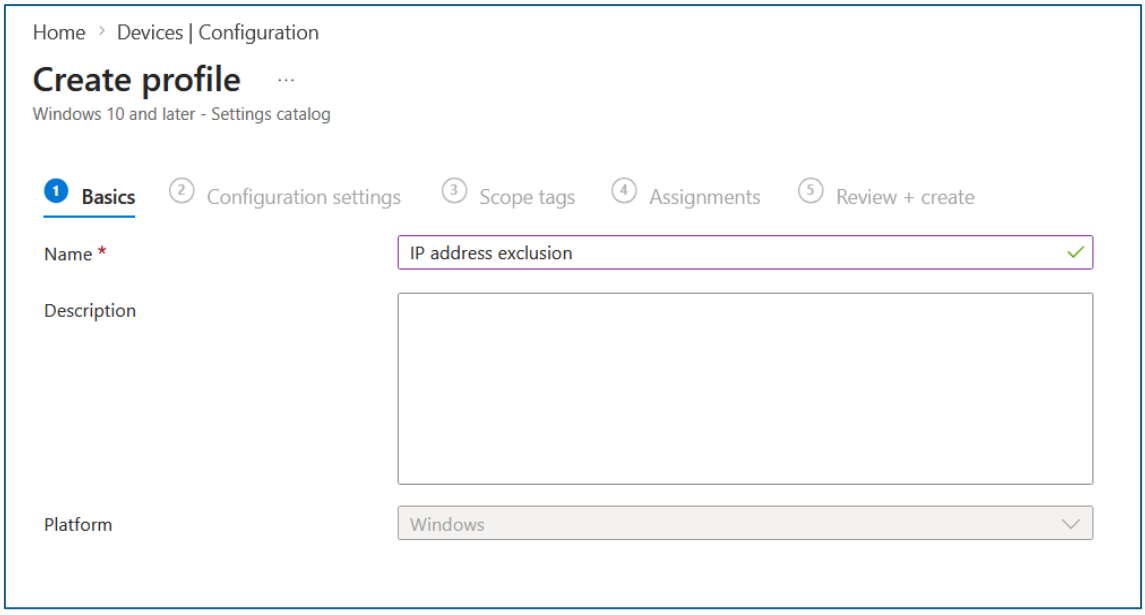


In “Create a profile”, specify the following:

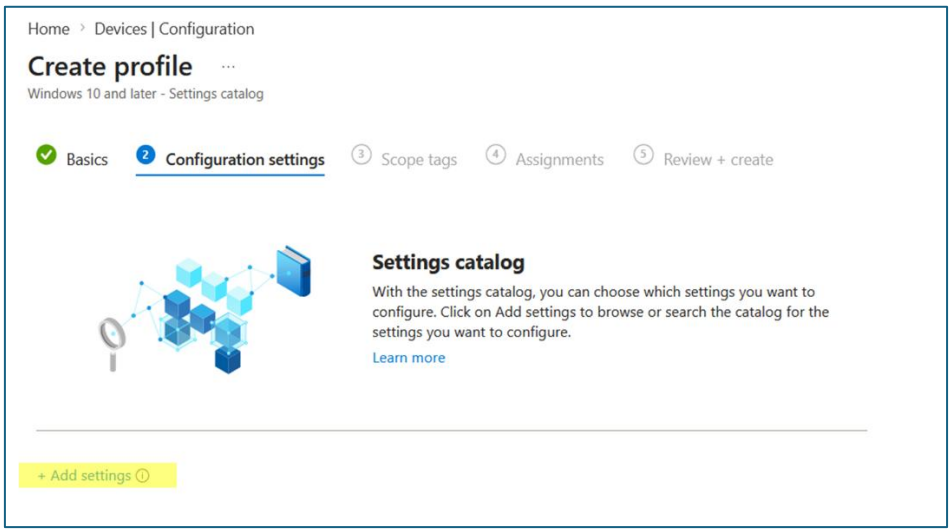
Platform: Windows 10 and later

Profile type: Settings catalog

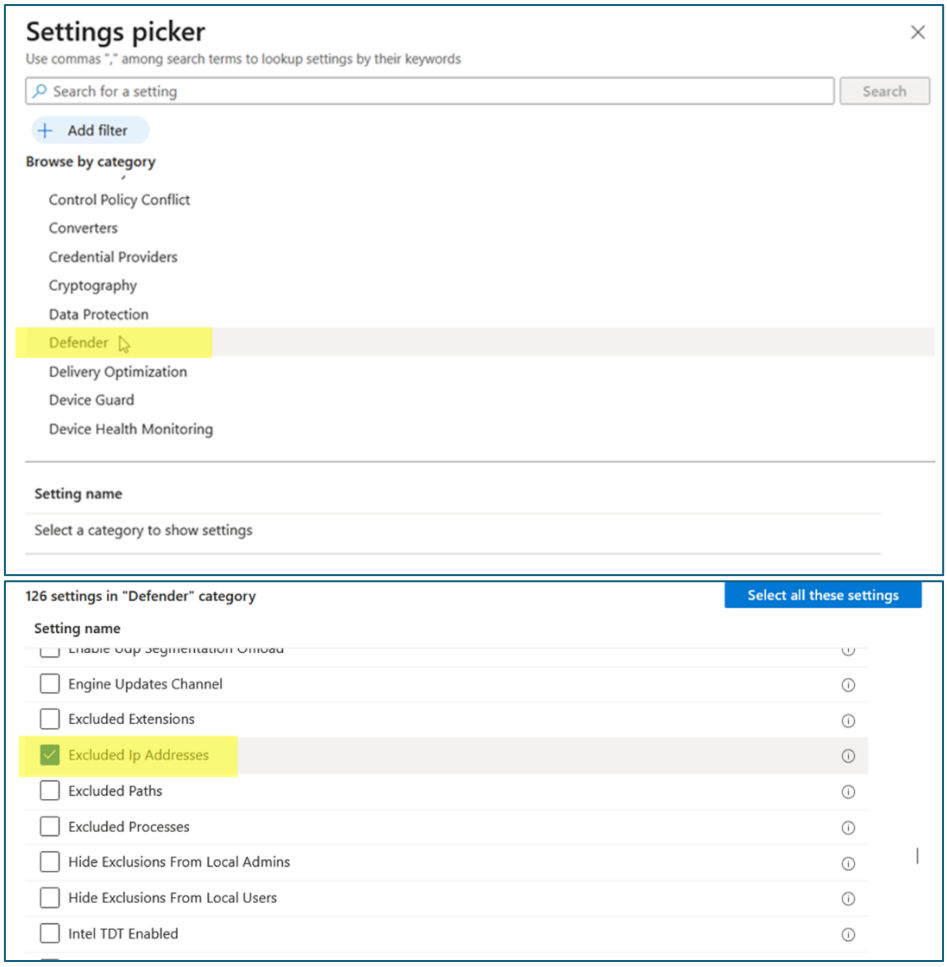
On the “Basics” tab, enter any policy name. In the example below, the policy name is set to “IP address exclusion”, but you can choose any name that fits your environment.



On the “Configuration settings” tab, select “Add settings” to open the Settings picker.

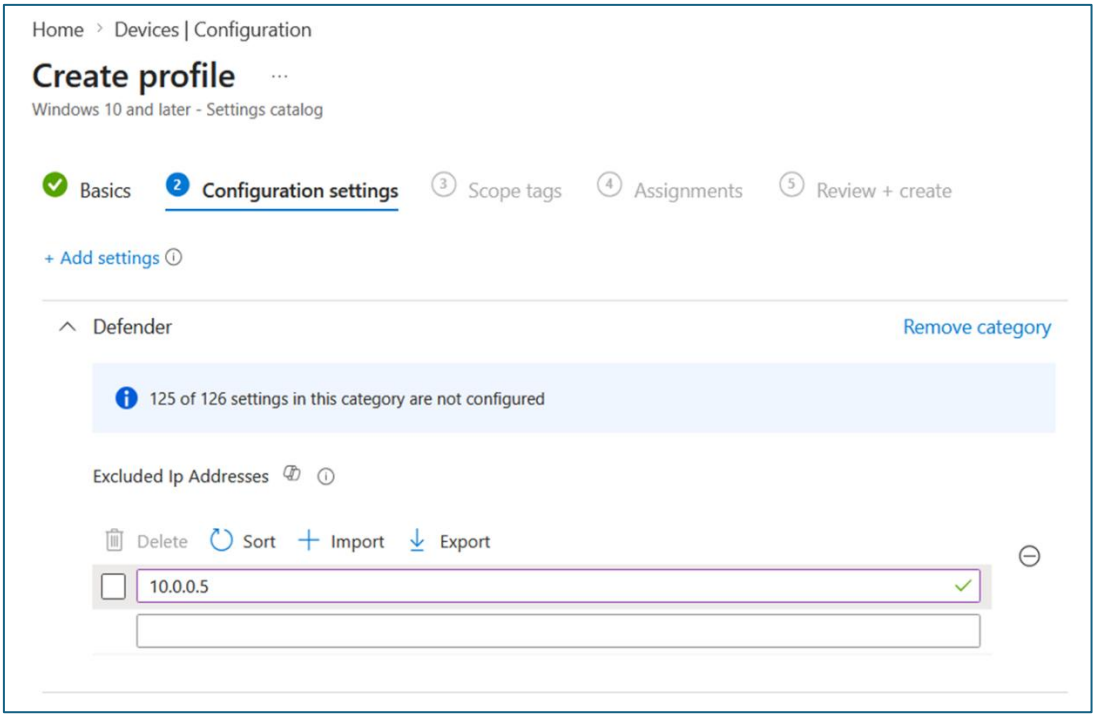


In the Settings picker, select Defender under “Browse by category”, check the setting named “Excluded Ip Addresses”, and then close the picker using the × shown in the picker window.



Back on the “Configuration settings” tab, enter the camera IP address you want to exclude into the input box.

Only individual IP addresses are supported. You cannot specify CIDR notation (e.g., 192.168.10.0/24) or wildcards. Enter each camera IP address you want to exclude one by one.



Intune also supports importing exclusions. You can import settings by using a text file that lists multiple IP addresses separated by line breaks, as shown below.

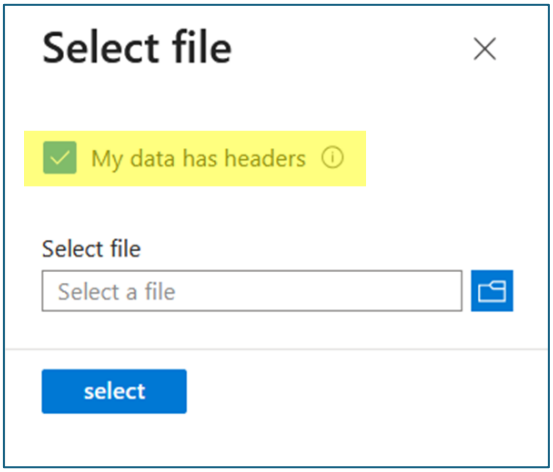
Example contents of the text file:

192.168.10.1

192.168.10.2

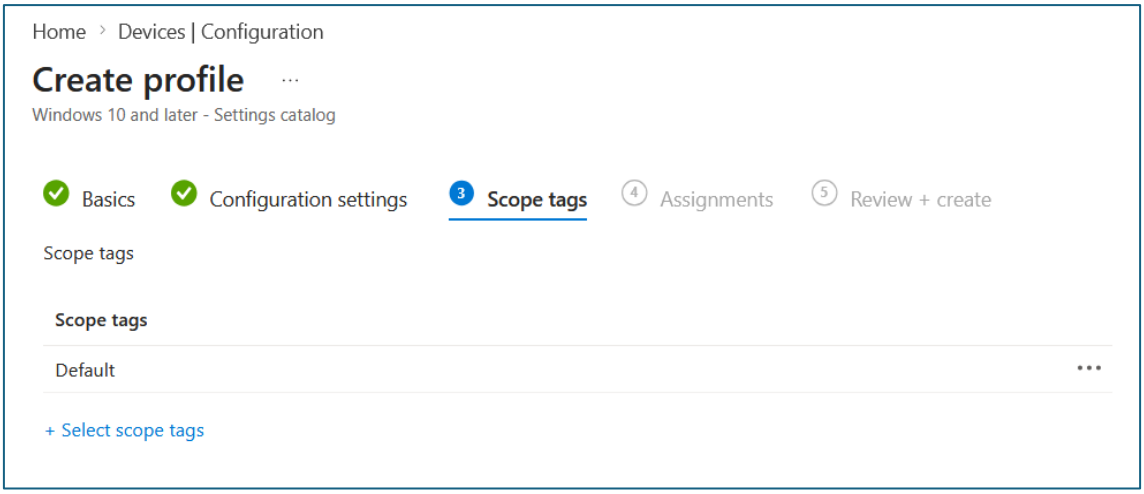
192.168.10.3

When importing a file in Intune, if the checkbox “My data has headers” is selected, Intune treats the first row that contains data as a header row and skips it.

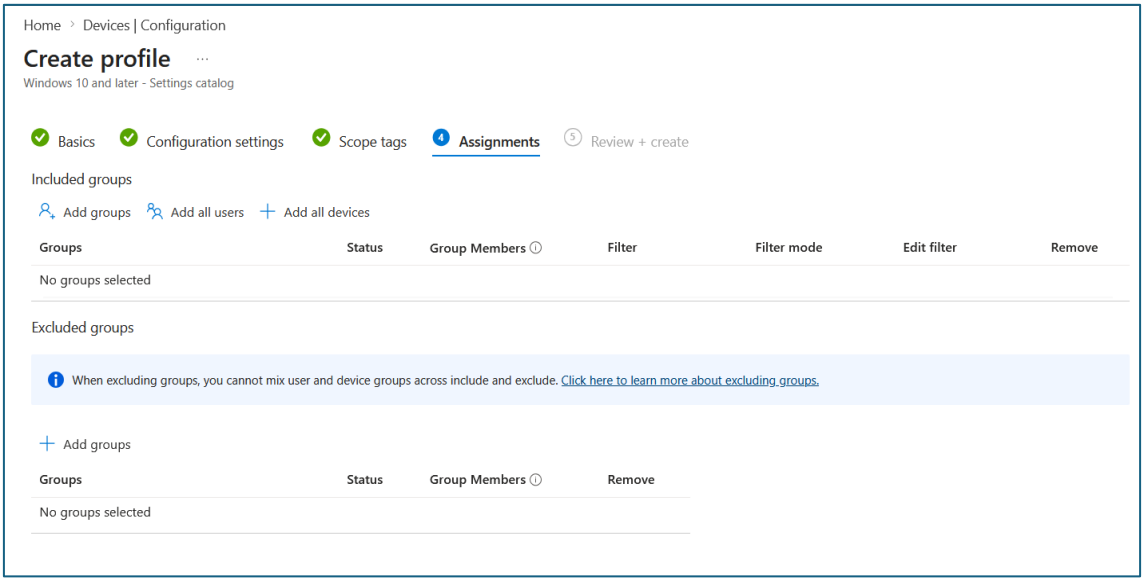


If your import file does not include a header row, clear this checkbox so that Intune imports starting from the first row containing data.

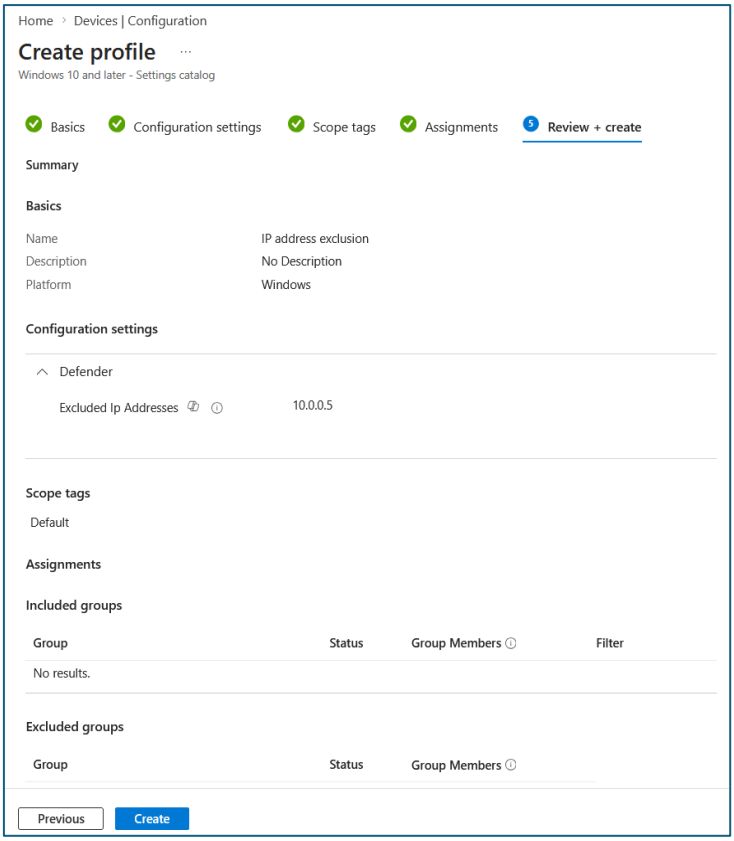
On the “Scope tags” tab, you can leave the default settings and proceed; this is optional.



On the “Assignments” tab, specify the groups to which the policy will apply and, if needed, the groups to exclude from the assignment.



On the “Review + create” tab, confirm that the settings are correct, and then complete policy creation.



After the policy has been applied to the device, to verify the settings on the device, run the following command in an administrator-elevated PowerShell session on the PC that runs Media Production Suite.

Verification command:
Get-MpPreference | select -expand ExclusionIPAddress

This completes the procedure for excluding an IP address using Intune.

Revision History

This section describes the revision history of this document.

Document Version	Changes
1.0	First edition