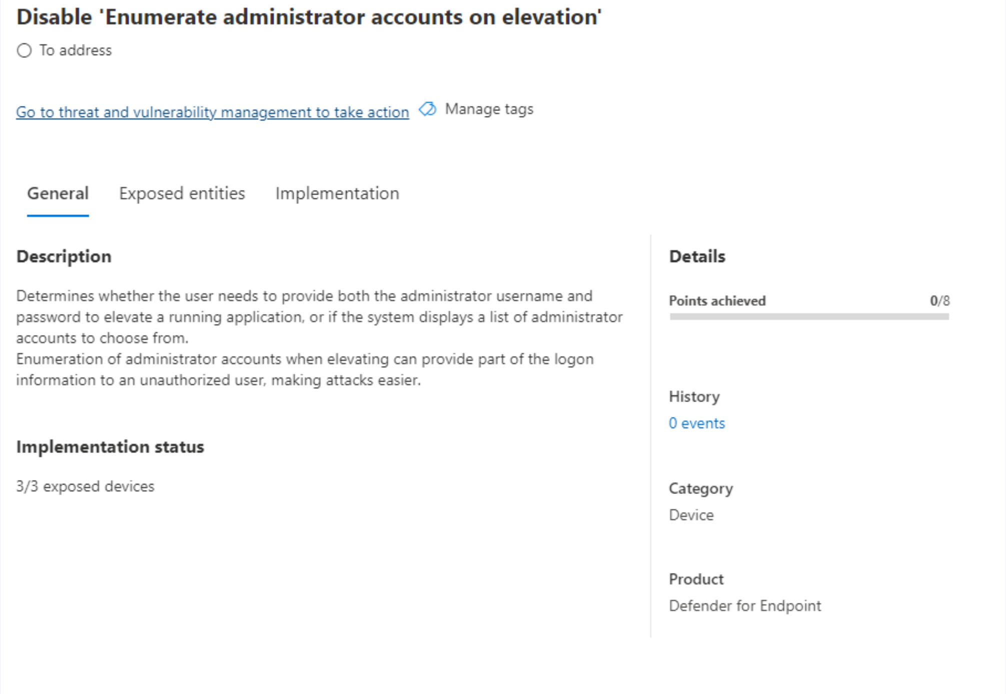
Disable 'Enumerate administrator accounts on elevation'

In this guide, we address the recommended setting in Microsoft Secure Score to disable enumeration of admin accounts.

1 This guide is used to address a Microsoft Secure Score recommendation.



Disable 'Enumerate administrator accounts on elevation'

○ To address

Go to threat and vulnerability management to take action

Description

Determines whether the user needs to provide both the administrator username and password to elevate a running application, or if the system displays a list of administrator accounts to choose from.
Enumeration of administrator accounts when elevating can provide part of the logon information to an unauthorized user, making attacks easier.

Implementation status

3/3 exposed devices

Details

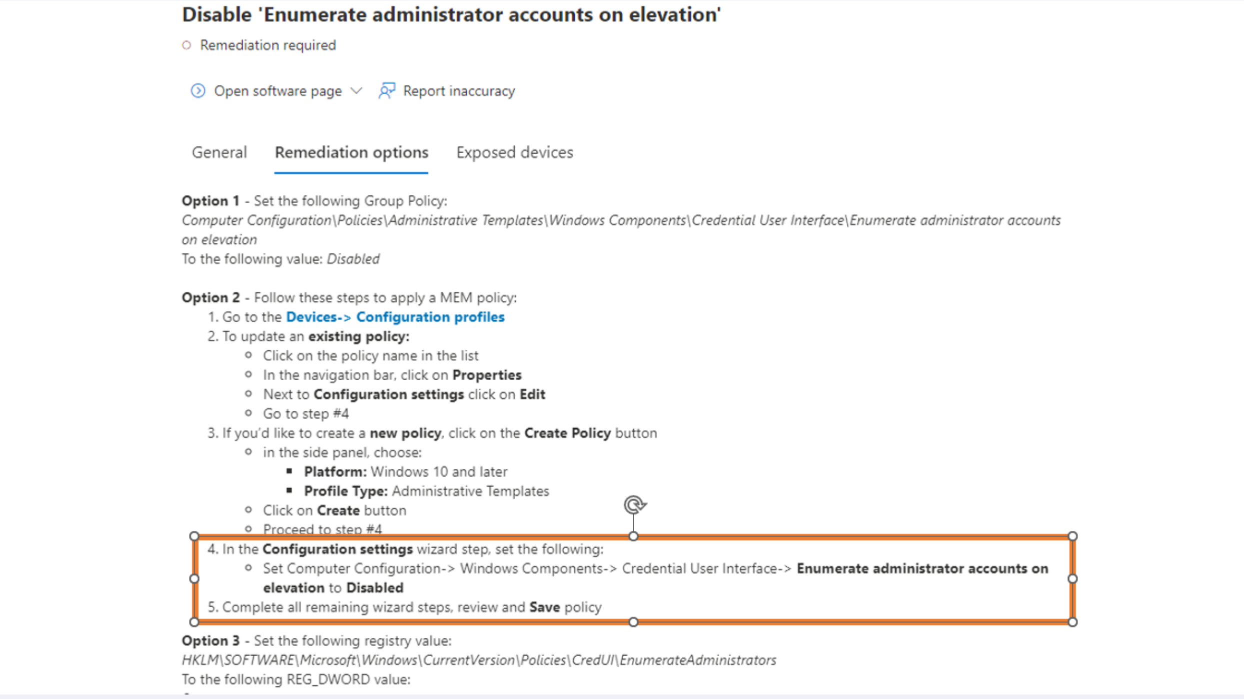
Points achieved 0/8

History
0 events

Category
Device

Product
Defender for Endpoint

2 We are managing devices via Intune, so we will select step 4 of the pictured recommendation.



Disable 'Enumerate administrator accounts on elevation'

○ Remediation required

Option 1 - Set the following Group Policy:
Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation
To the following value: *Disabled*

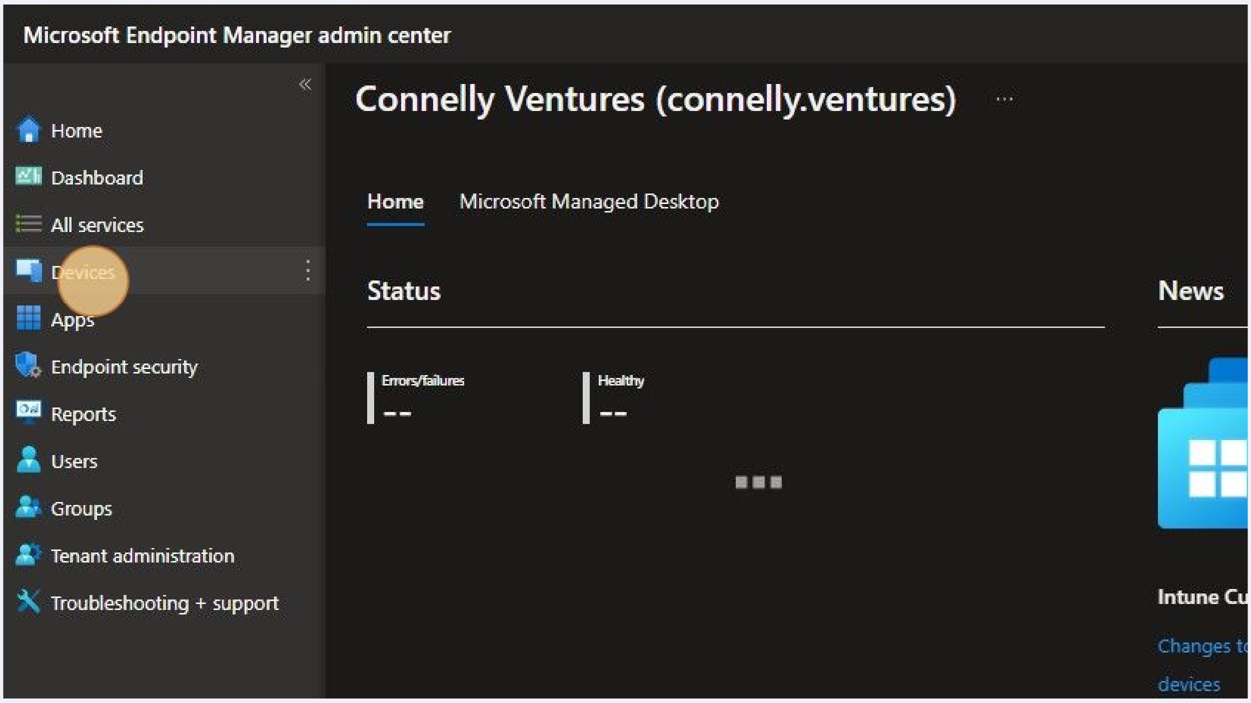
Option 2 - Follow these steps to apply a MEM policy:

1. Go to the **Devices-> Configuration profiles**
2. To update an **existing policy:**
   - Click on the policy name in the list
   - In the navigation bar, click on **Properties**
   - Next to **Configuration settings** click on **Edit**
   - Go to step #4
3. If you'd like to create a **new policy**, click on the **Create Policy** button
   - in the side panel, choose:
     - **Platform:** Windows 10 and later
     - **Profile Type:** Administrative Templates
   - Click on **Create** button
   - Proceed to step #4
4. In the **Configuration settings** wizard step, set the following:
   - Set Computer Configuration-> Windows Components-> Credential User Interface-> **Enumerate administrator accounts on elevation** to **Disabled**
5. Complete all remaining wizard steps, review and **Save** policy

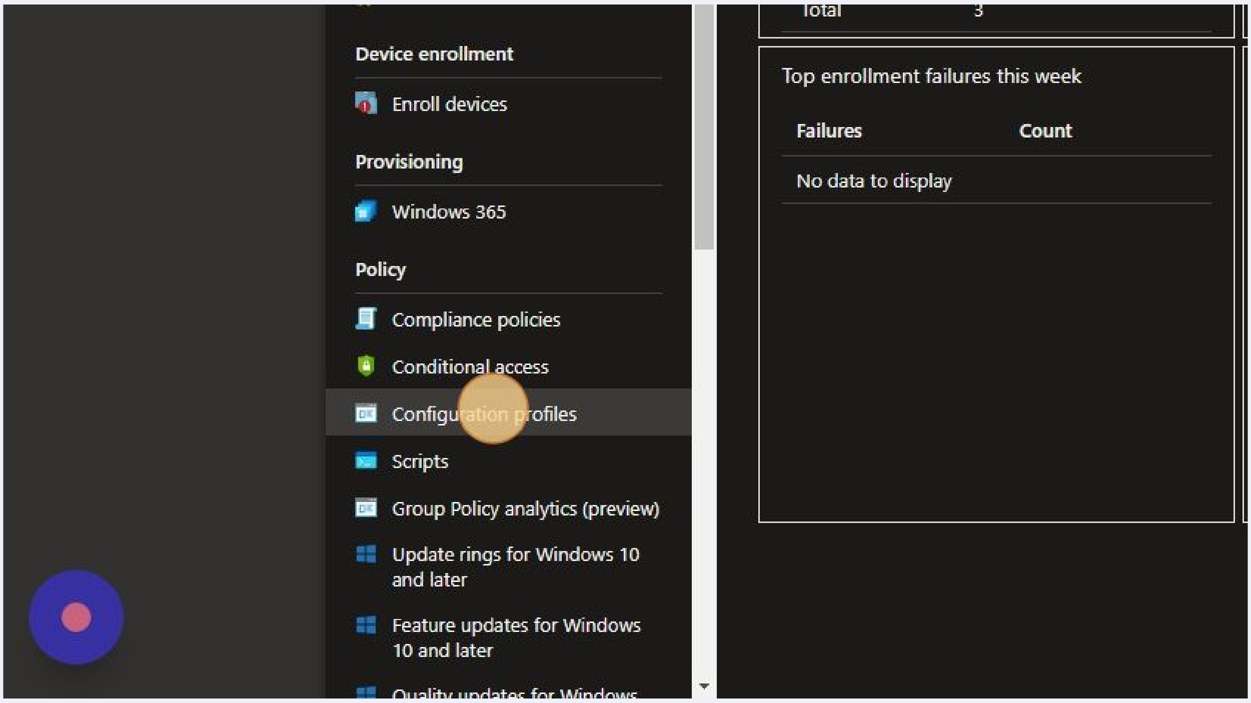
Option 3 - Set the following registry value:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators
To the following REG_DWORD value:

3 Navigate to endpoint.microsoft.com

4 Click "Devices"

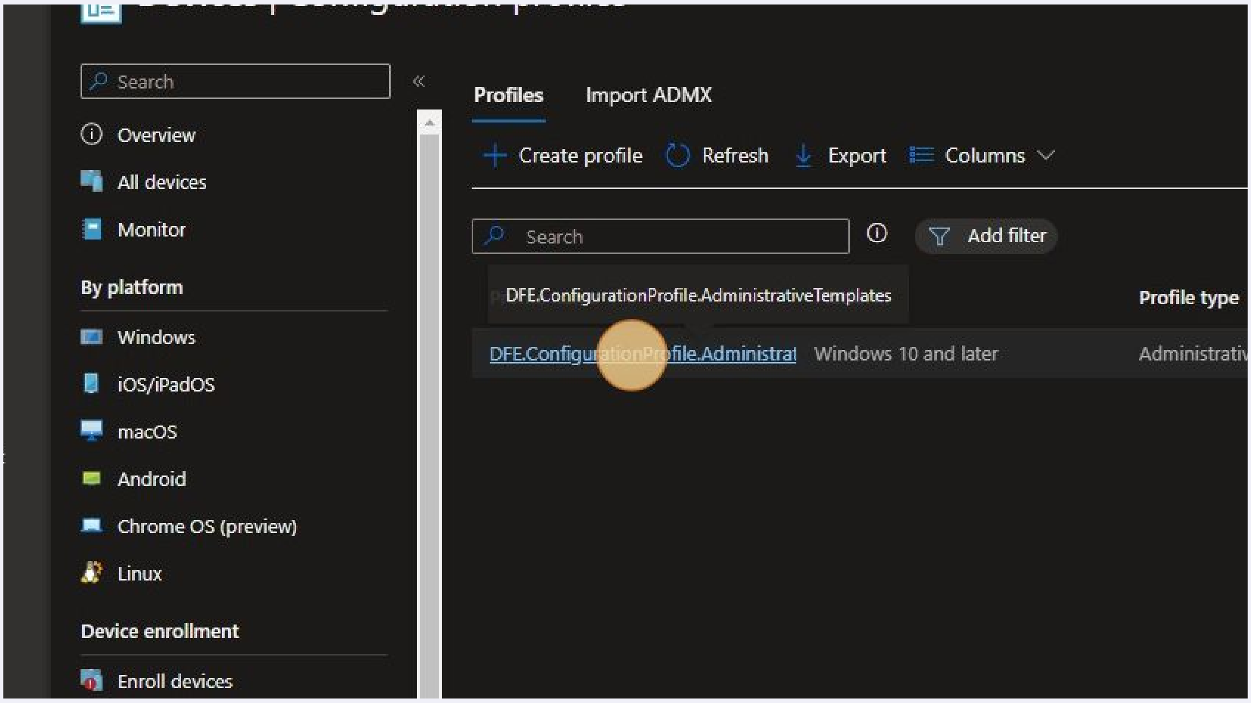


5 Click "Configuration profiles"

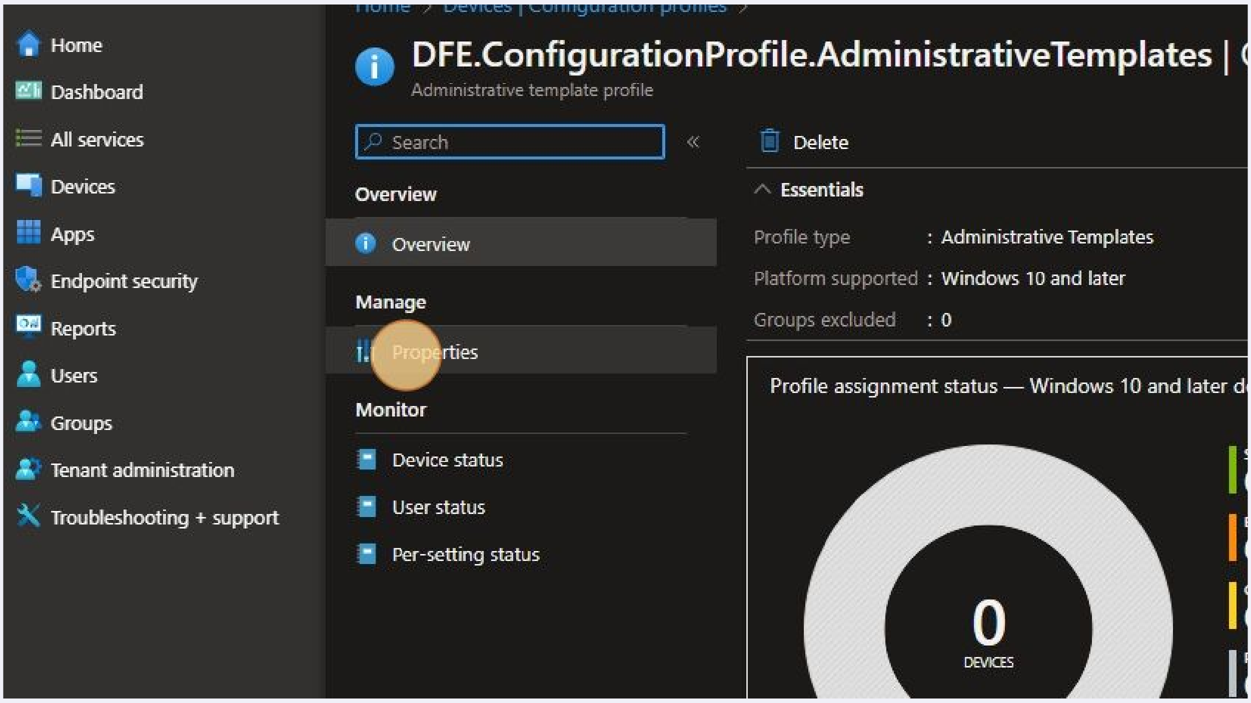


Total
3
Device enrollment
Enroll devices
Provisioning
Windows 365
Policy
Compliance policies
Conditional access
Configuration profiles
Scripts
Group Policy analytics (preview)
Update rings for Windows 10 and later
Feature updates for Windows 10 and later
Quality updates for Windows
Top enrollment failures this week
Failures
Count
No data to display

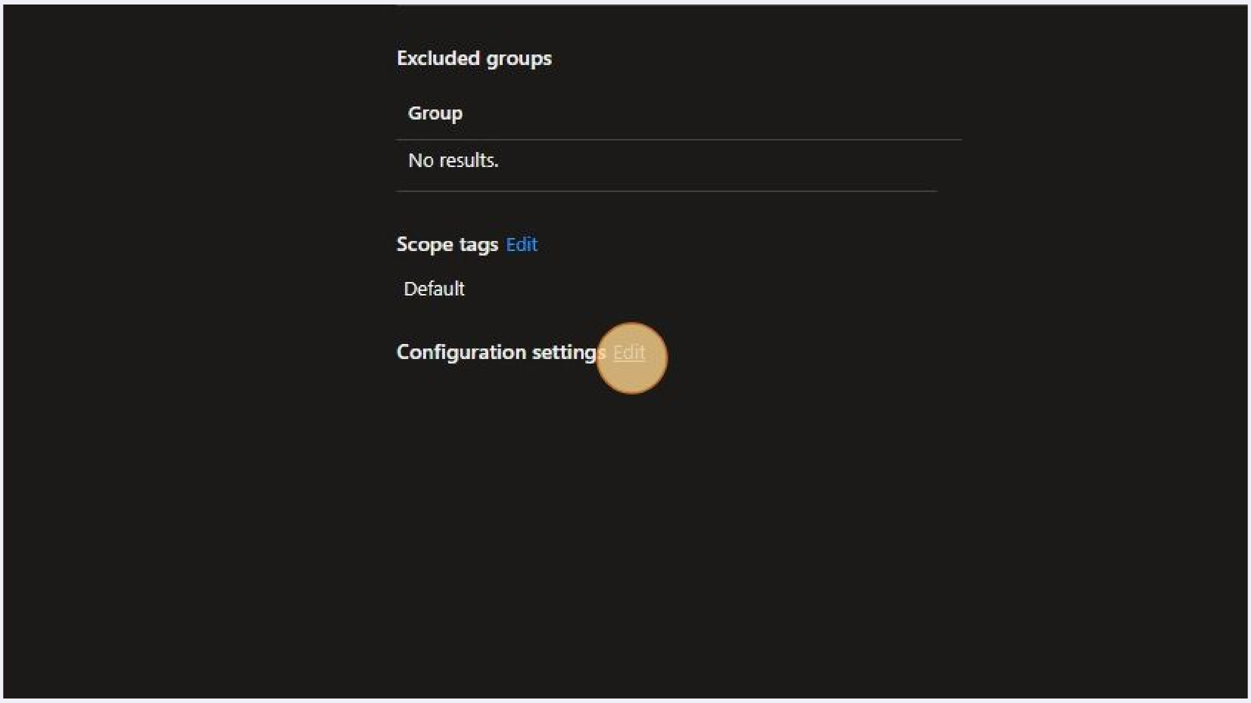
6 Click "DFE.ConfigurationProfile.AdministrativeTemplates"



7 Click "Properties"


Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
DFE.ConfigurationProfile.AdministrativeTemplates |
Administrative template profile
Search
Overview
Overview
Manage
Properties
Monitor
Device status
User status
Per-setting status
Delete
Essentials
Profile type : Administrative Templates
Platform supported : Windows 10 and later
Groups excluded : 0
Profile assignment status — Windows 10 and later d
0
DEVICES

8 Click "Edit"



Excluded groups

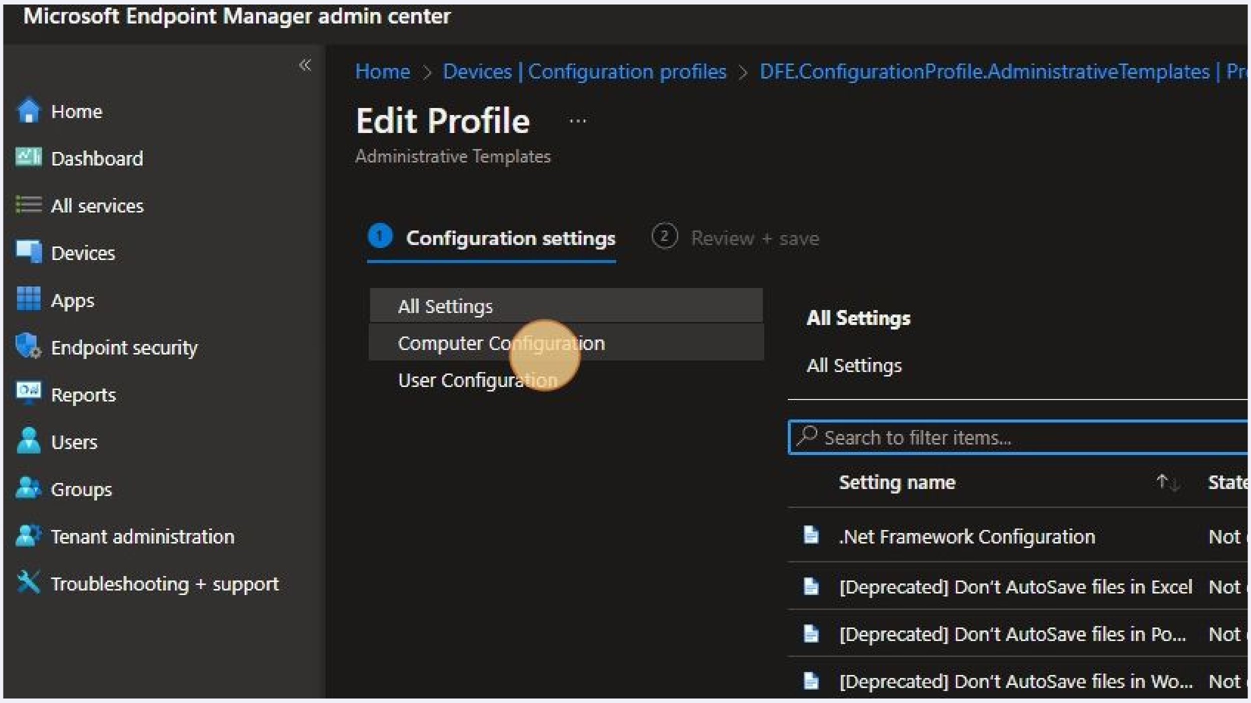
Group
No results.

Scope tags Edit

Default

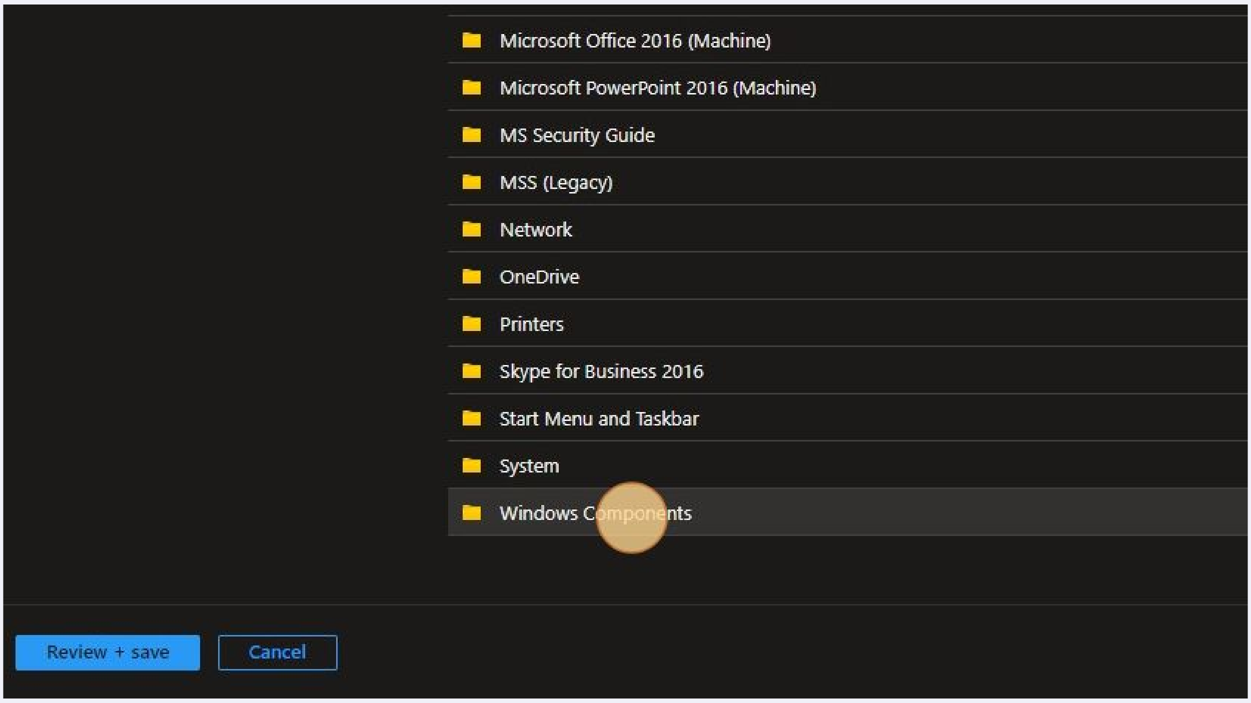
Configuration settings Edit

9 Click "Computer Configuration"



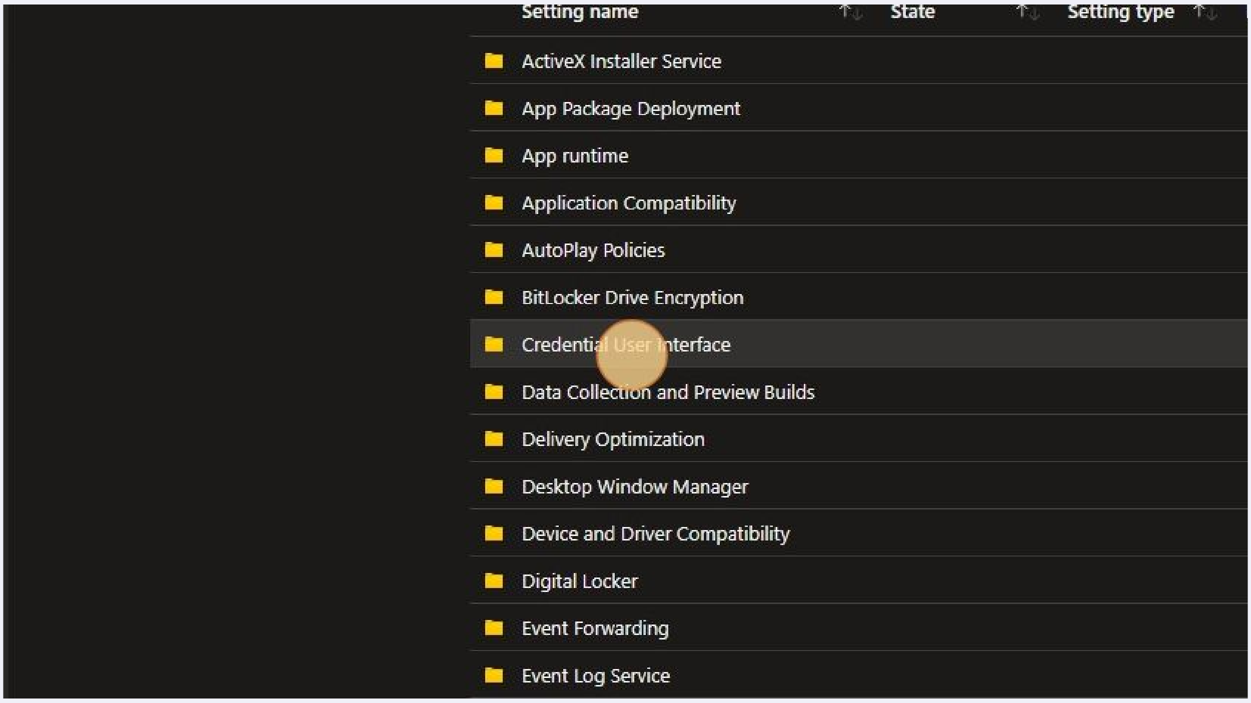
Setting name	State
.Net Framework Configuration	Not
[Deprecated] Don't AutoSave files in Excel	Not
[Deprecated] Don't AutoSave files in Po...	Not
[Deprecated] Don't AutoSave files in Wo...	Not

10 Click "Windows Components"



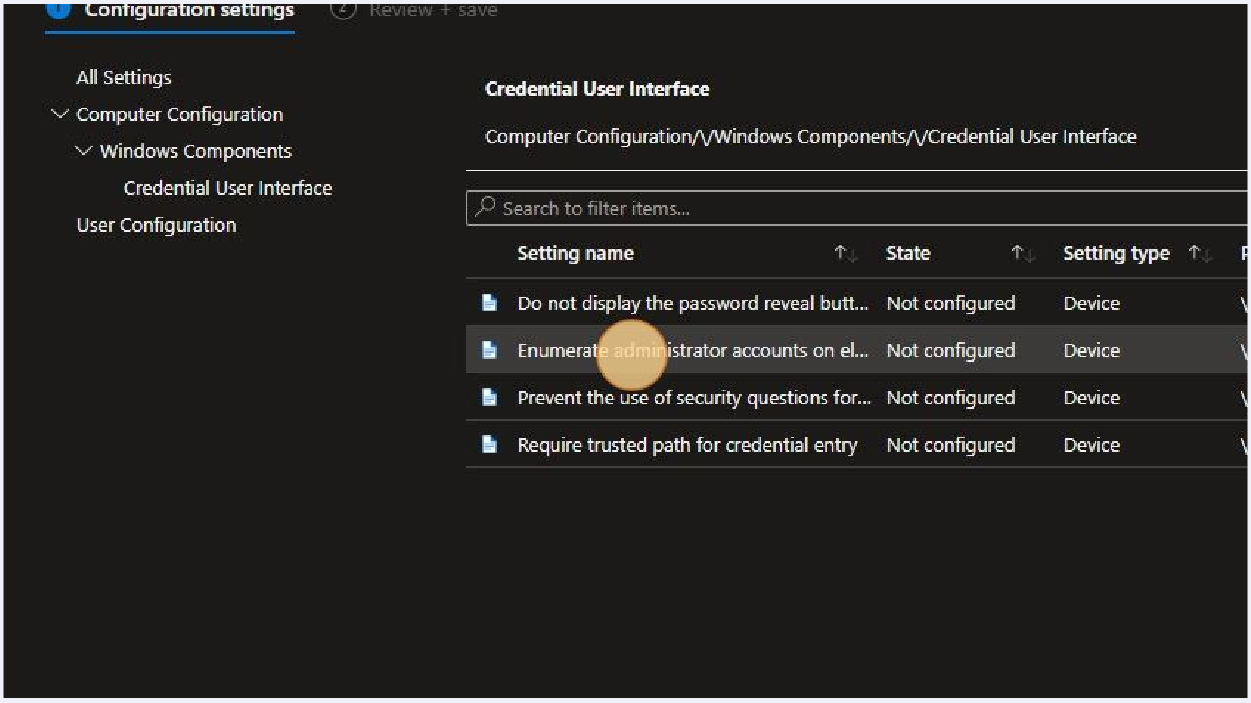
- Microsoft Office 2016 (Machine)
- Microsoft PowerPoint 2016 (Machine)
- MS Security Guide
- MSS (Legacy)
- Network
- OneDrive
- Printers
- Skype for Business 2016
- Start Menu and Taskbar
- System
- Windows Components

11 Click "Credential User Interface"



Setting name	State	Setting type
ActiveX Installer Service		
App Package Deployment		
App runtime		
Application Compatibility		
AutoPlay Policies		
BitLocker Drive Encryption		
Credential User Interface		
Data Collection and Preview Builds		
Delivery Optimization		
Desktop Window Manager		
Device and Driver Compatibility		
Digital Locker		
Event Forwarding		
Event Log Service		

12 Click "Enumerate administrator accounts on elevation"



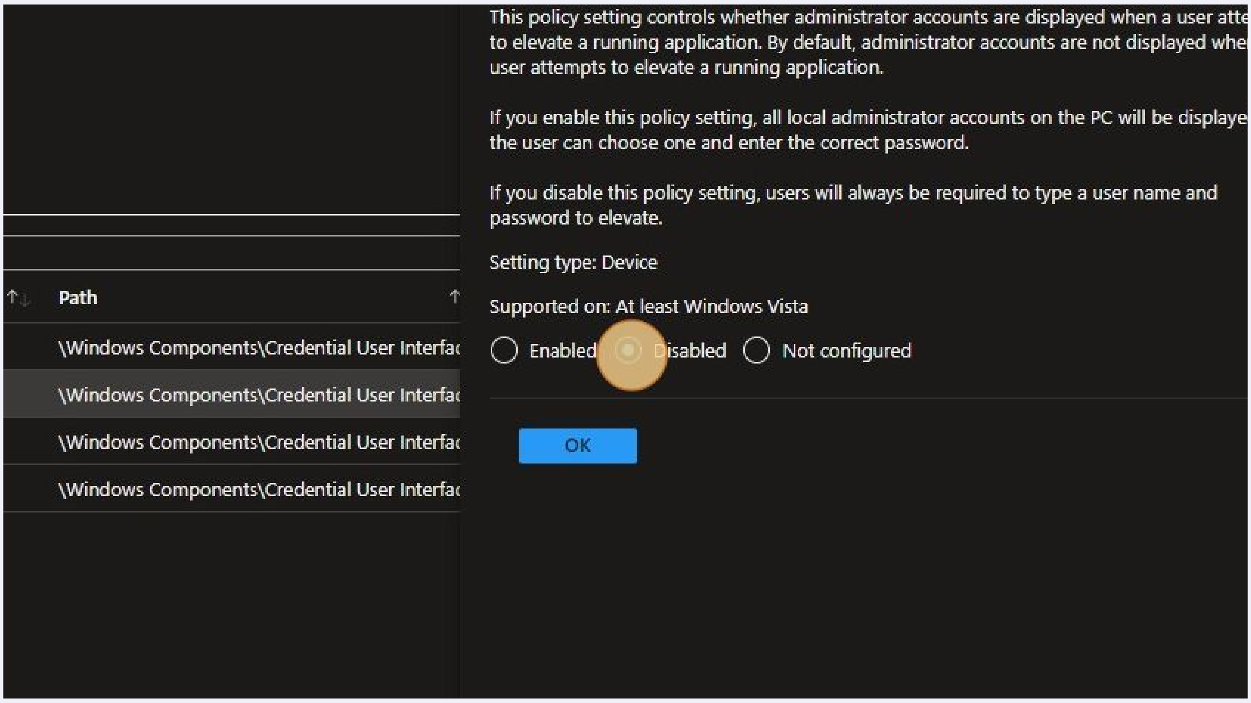
Credential User Interface

Computer Configuration/\/Windows Components/\/Credential User Interface

Search to filter items...

Setting name	State	Setting type
Do not display the password reveal butt...	Not configured	Device
Enumerate administrator accounts on el...	Not configured	Device
Prevent the use of security questions for...	Not configured	Device
Require trusted path for credential entry	Not configured	Device

13 Click "Disabled"



This policy setting controls whether administrator accounts are displayed when a user atte to elevate a running application. By default, administrator accounts are not displayed whe user attempts to elevate a running application.

If you enable this policy setting, all local administrator accounts on the PC will be displaye the user can choose one and enter the correct password.

If you disable this policy setting, users will always be required to type a user name and password to elevate.

Setting type: Device

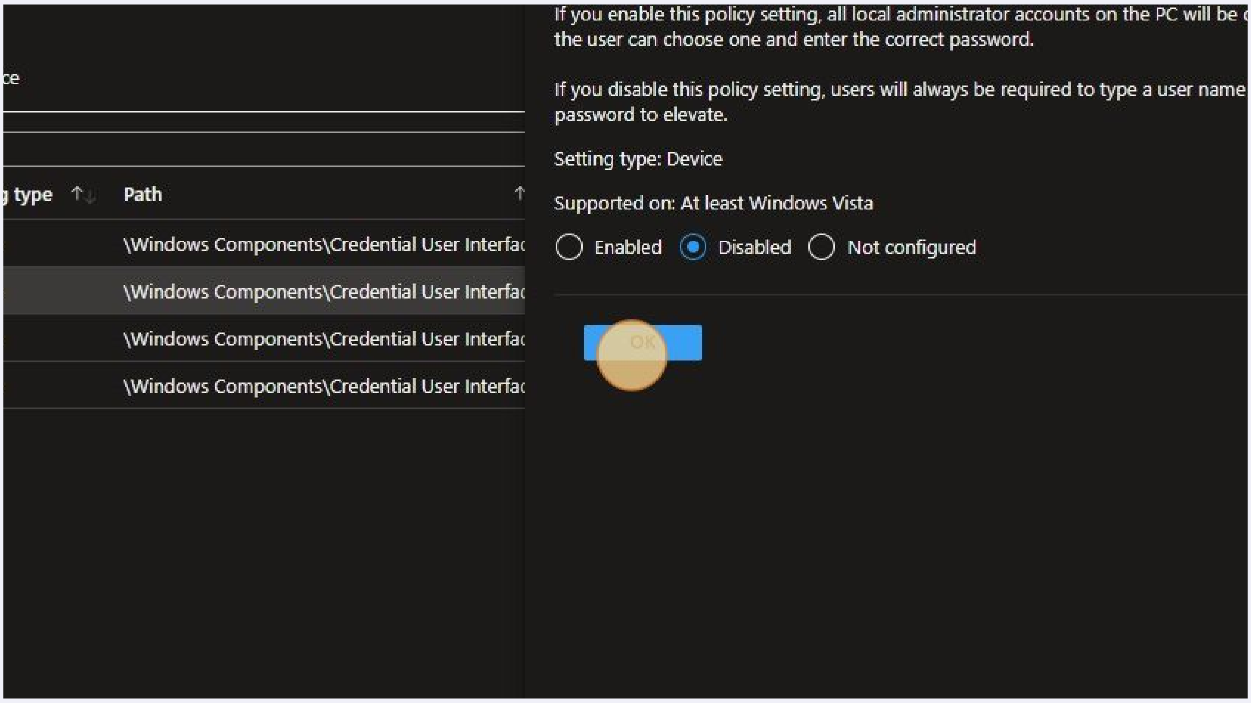
Supported on: At least Windows Vista

○ Enabled ○ Disabled ○ Not configured

OK

Path
\Windows Components\Credential User Interfac
\Windows Components\Credential User Interfac
\Windows Components\Credential User Interfac
\Windows Components\Credential User Interfac

14 Click "OK"



If you enable this policy setting, all local administrator accounts on the PC will be d
the user can choose one and enter the correct password.

If you disable this policy setting, users will always be required to type a user name
password to elevate.

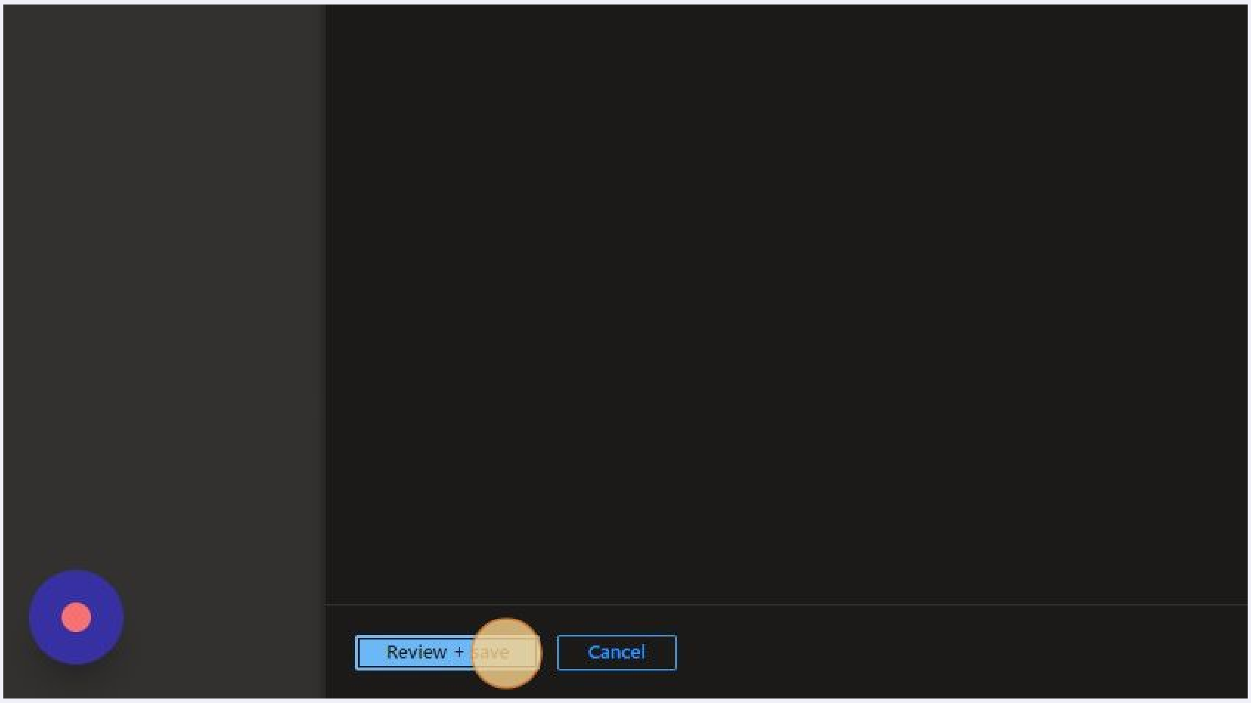
Setting type: Device

Supported on: At least Windows Vista

○ Enabled ● Disabled ○ Not configured

ce
g type
Path
\Windows Components\Credential User Interfa
\Windows Components\Credential User Interfa
\Windows Components\Credential User Interfa
\Windows Components\Credential User Interfa
OK

15 Click "Review + save"



16 Users on targeted devices will now be required to enter their username and password each time they elevate.