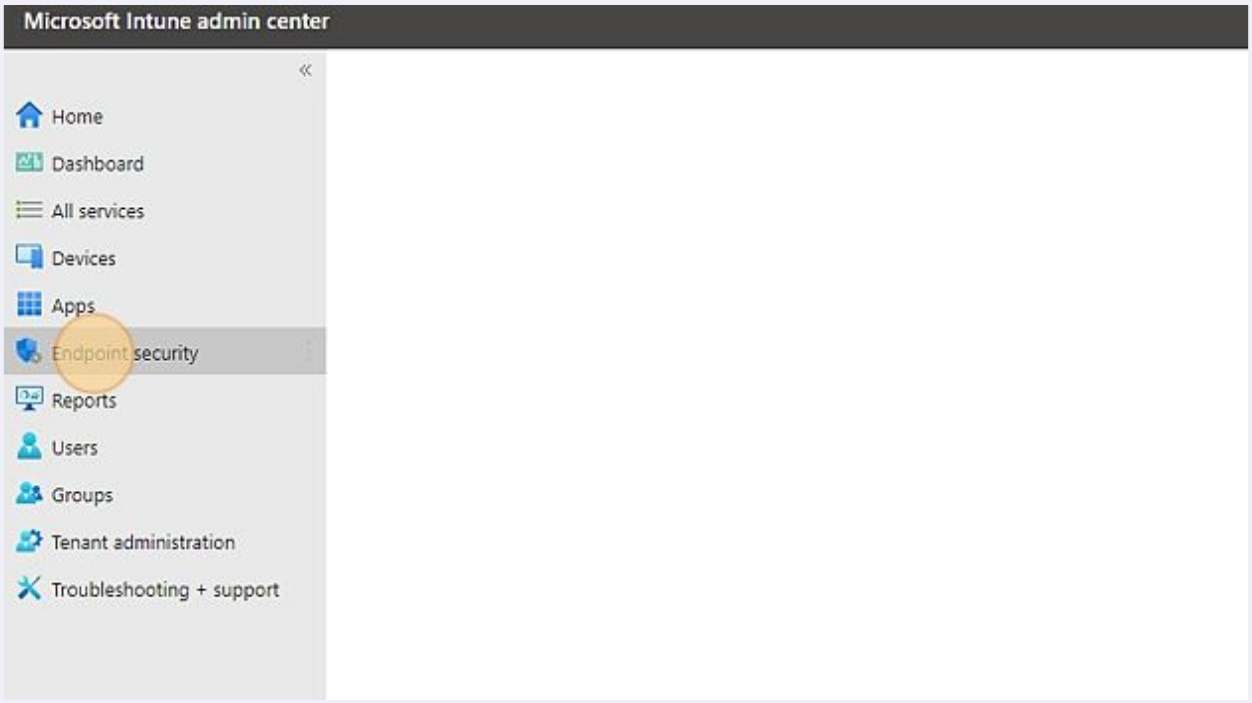
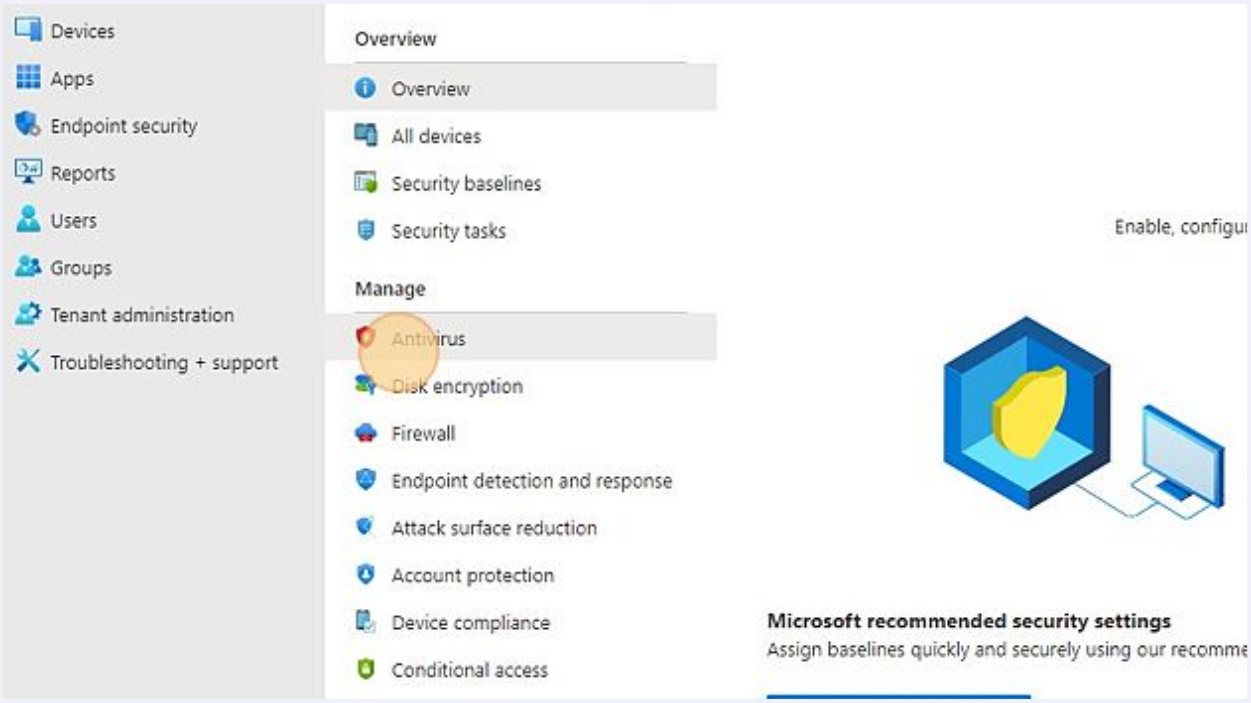
How to Create a Defender for Endpoint Antivirus Profile for Windows in Microsoft 365

1 Navigate to endpoint.microsoft.com

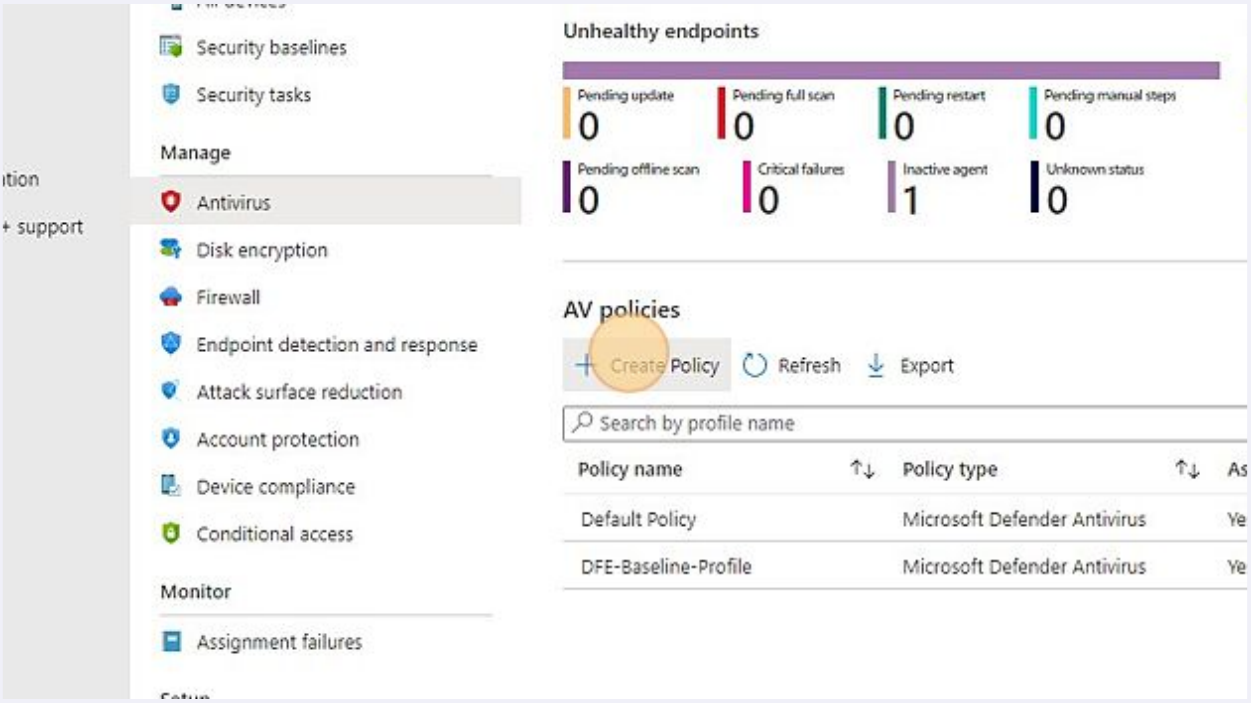
2 Click "Endpoint security"



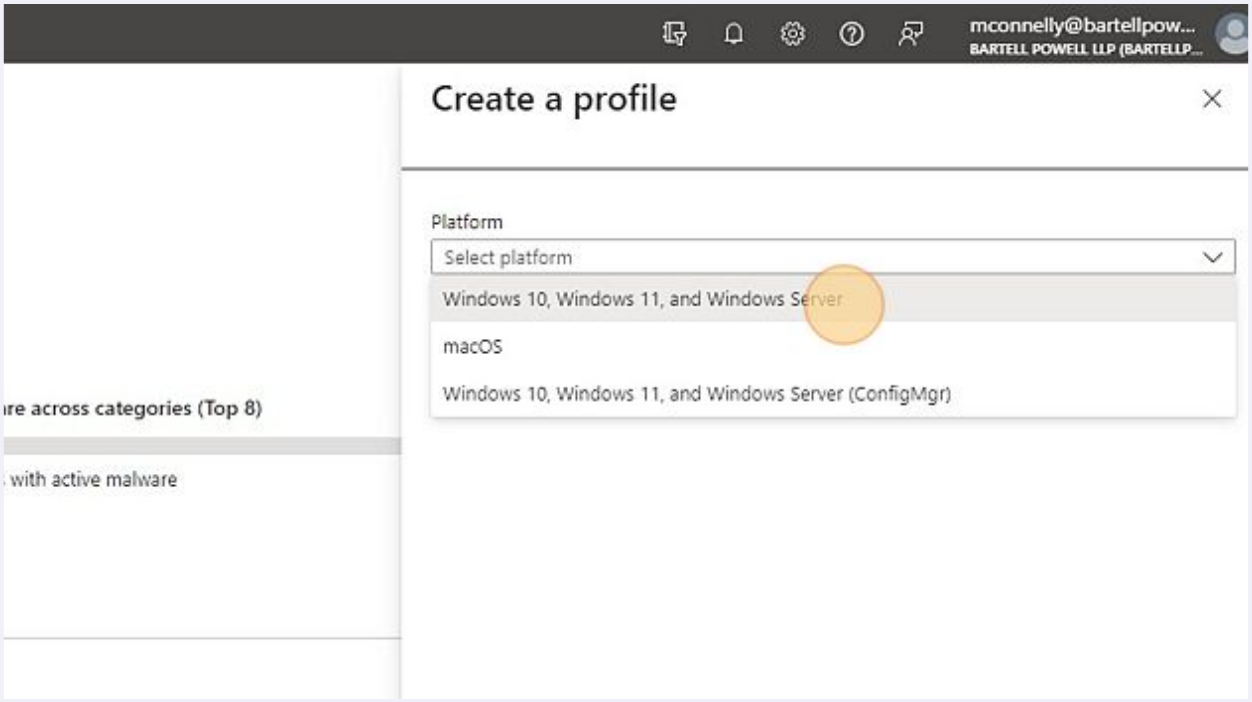
3 Click "Antivirus"



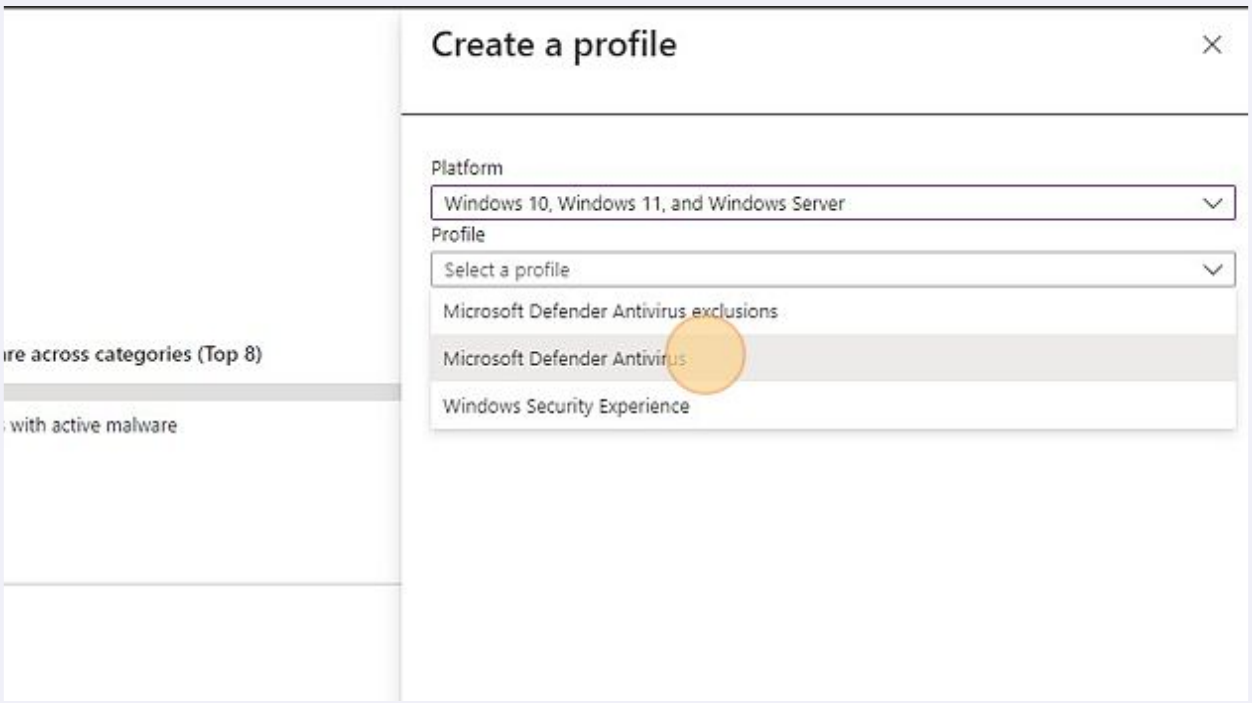
4 Click "Create Policy"



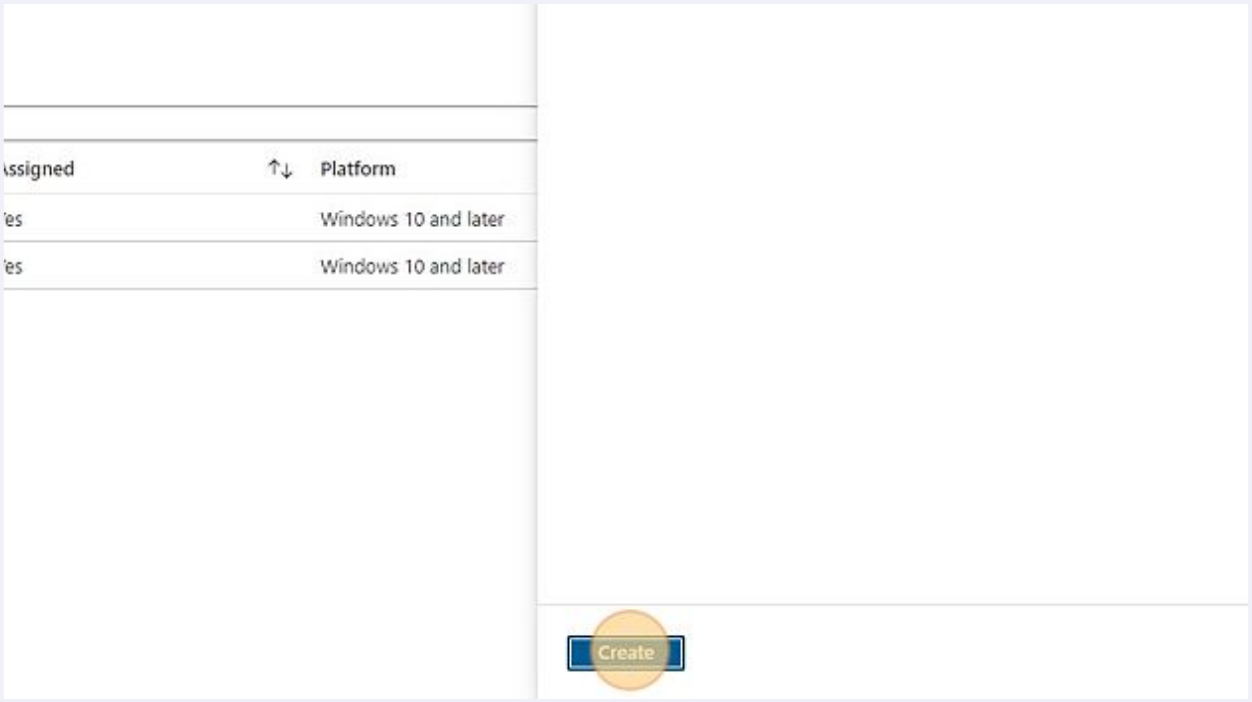
5 Select "Windows 10, Windows 11, Windows Server" for the "Platform"



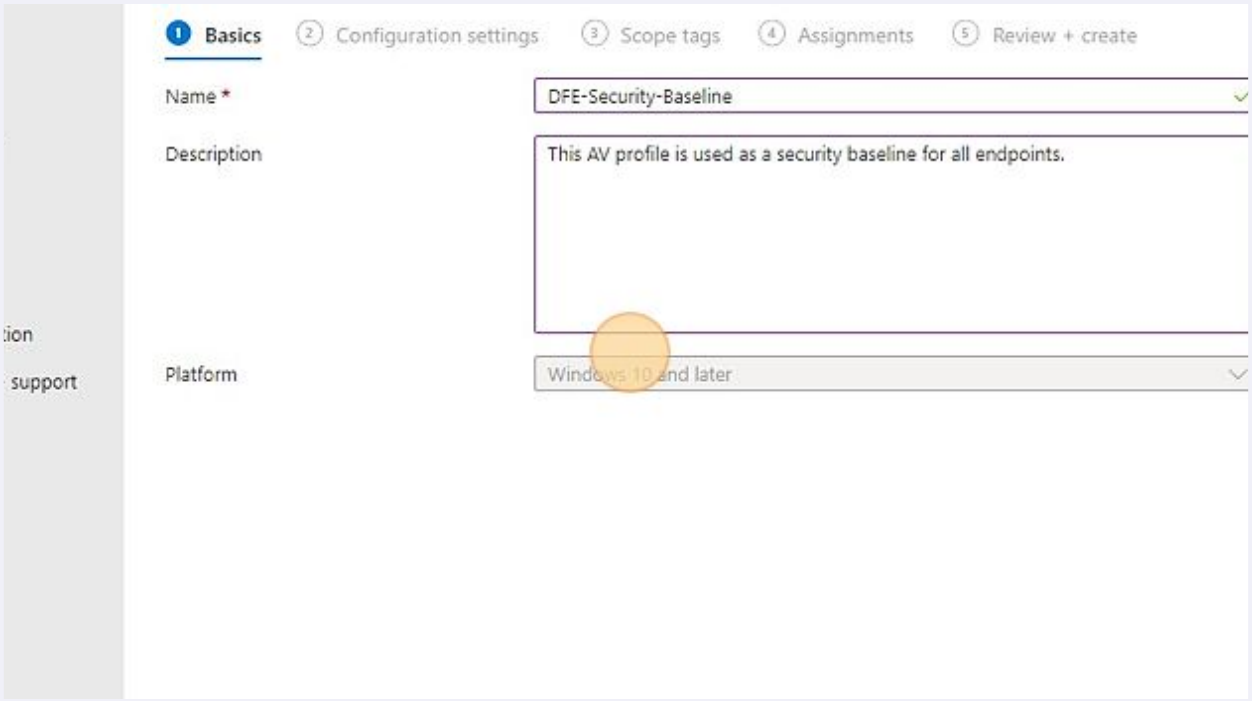
6 Select "Microsoft Defender Antivirus" for the "Profile"



7 Click "Create"

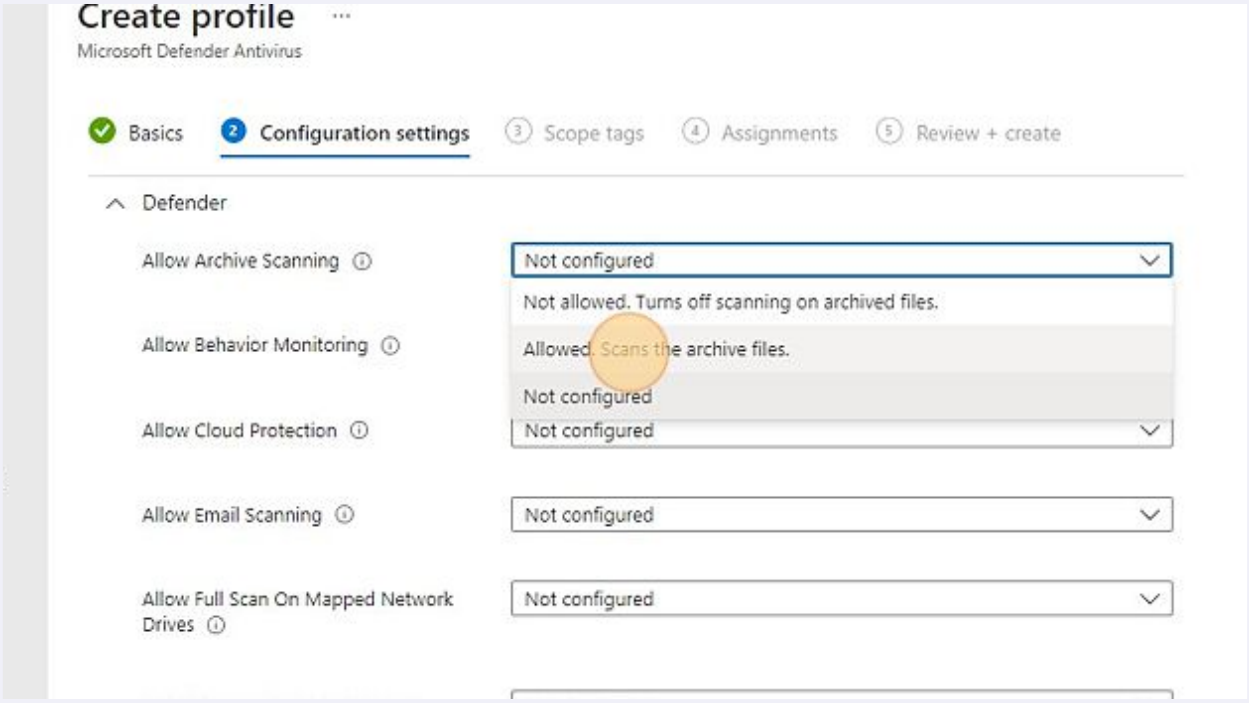


8 Name: DFE-Security-Baseline
Description: This AV profile is used as a security baseline for all endpoints.

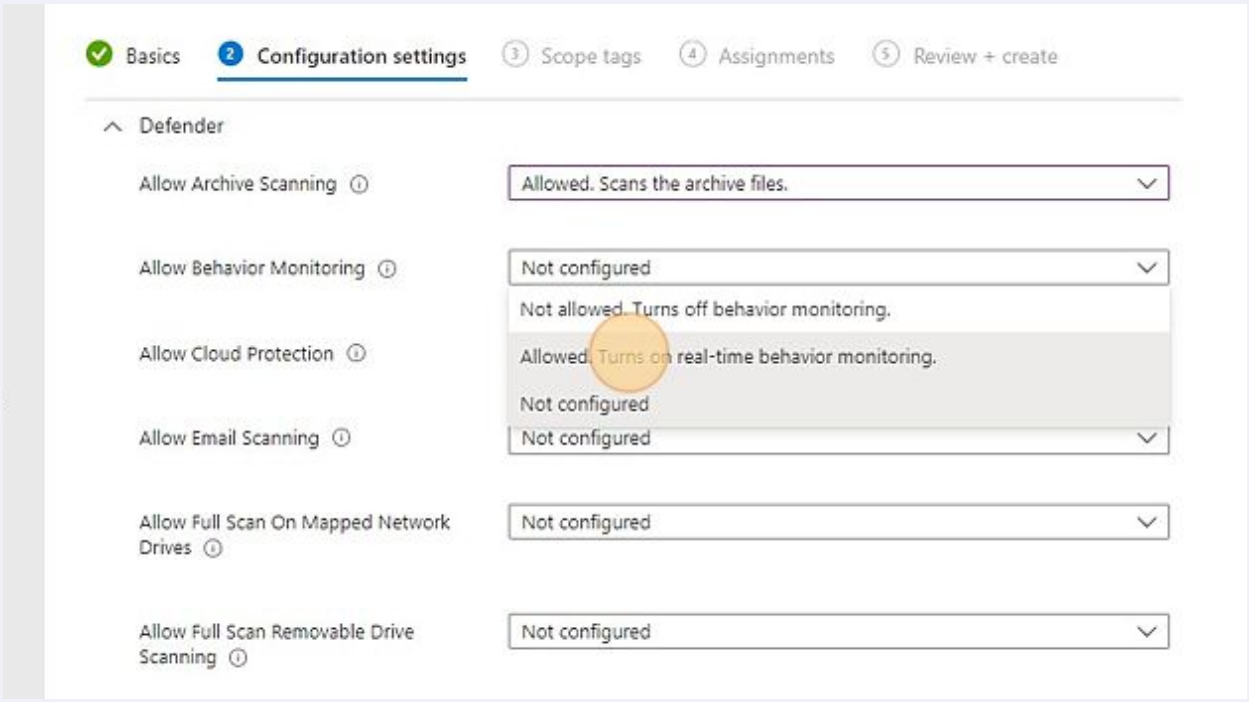


9 Click "Next"

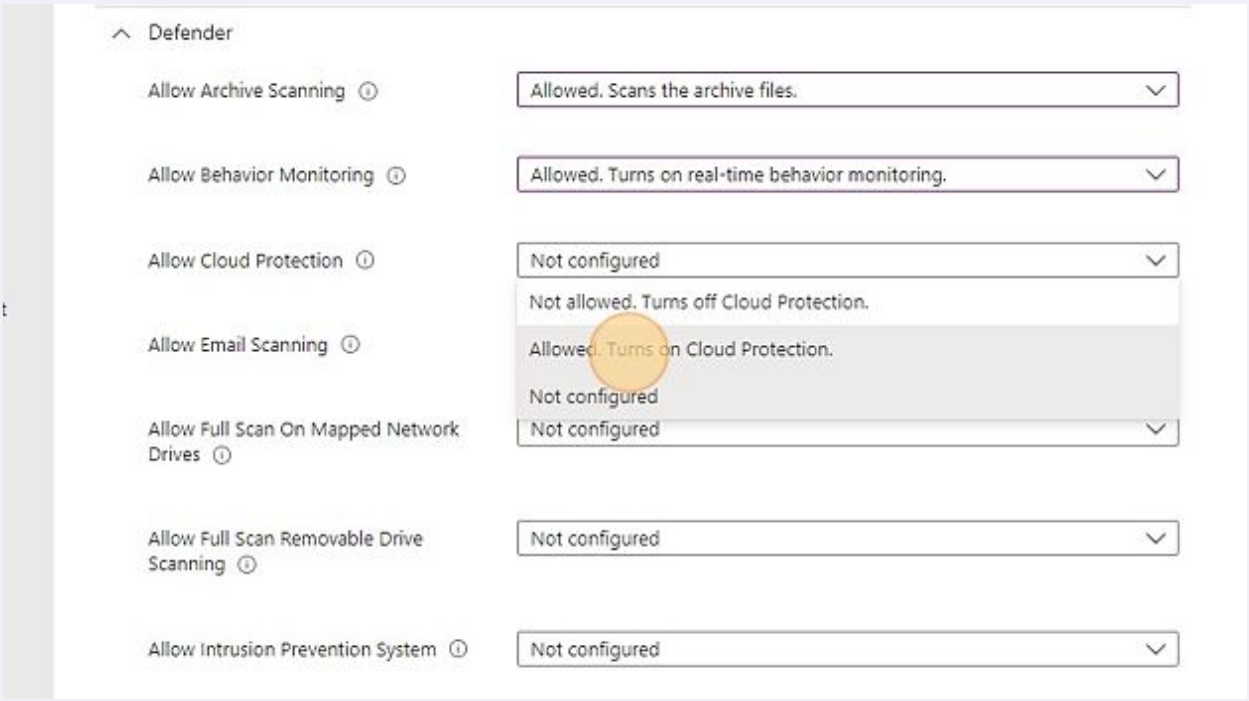
10 Click "Allowed. Scans the archive files."



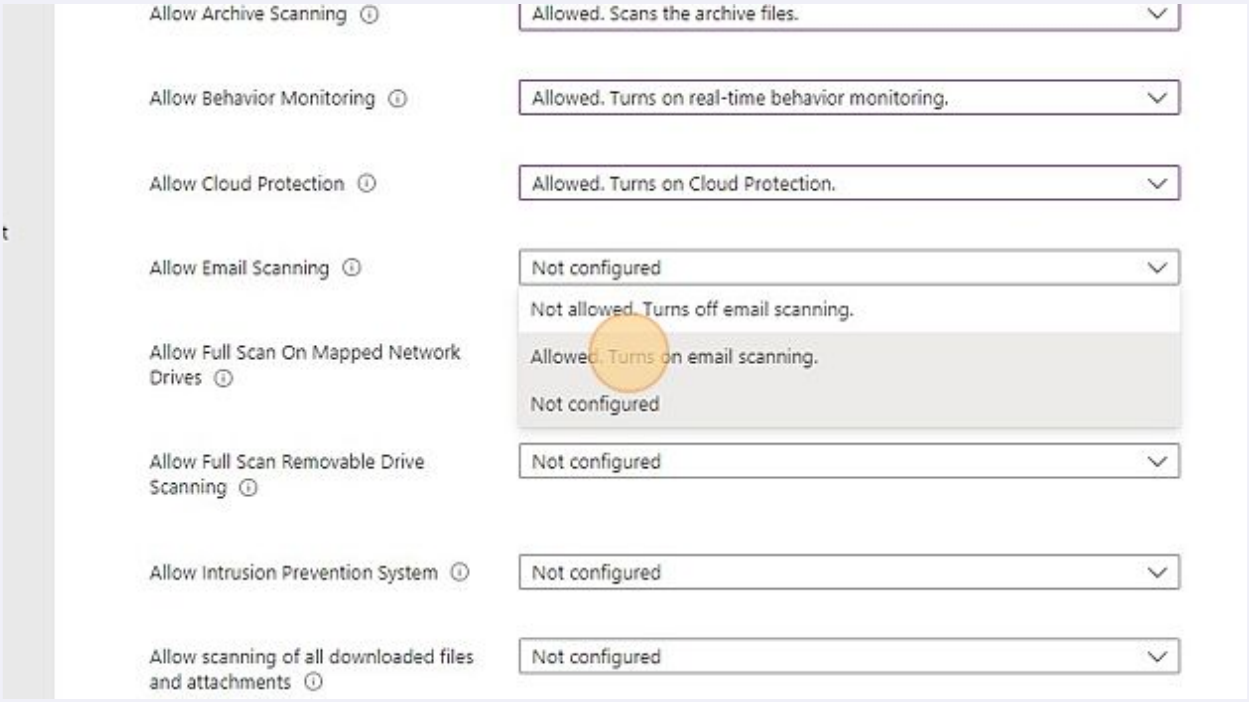
11 Click "Allowed. Turns on real-time behavior monitoring."



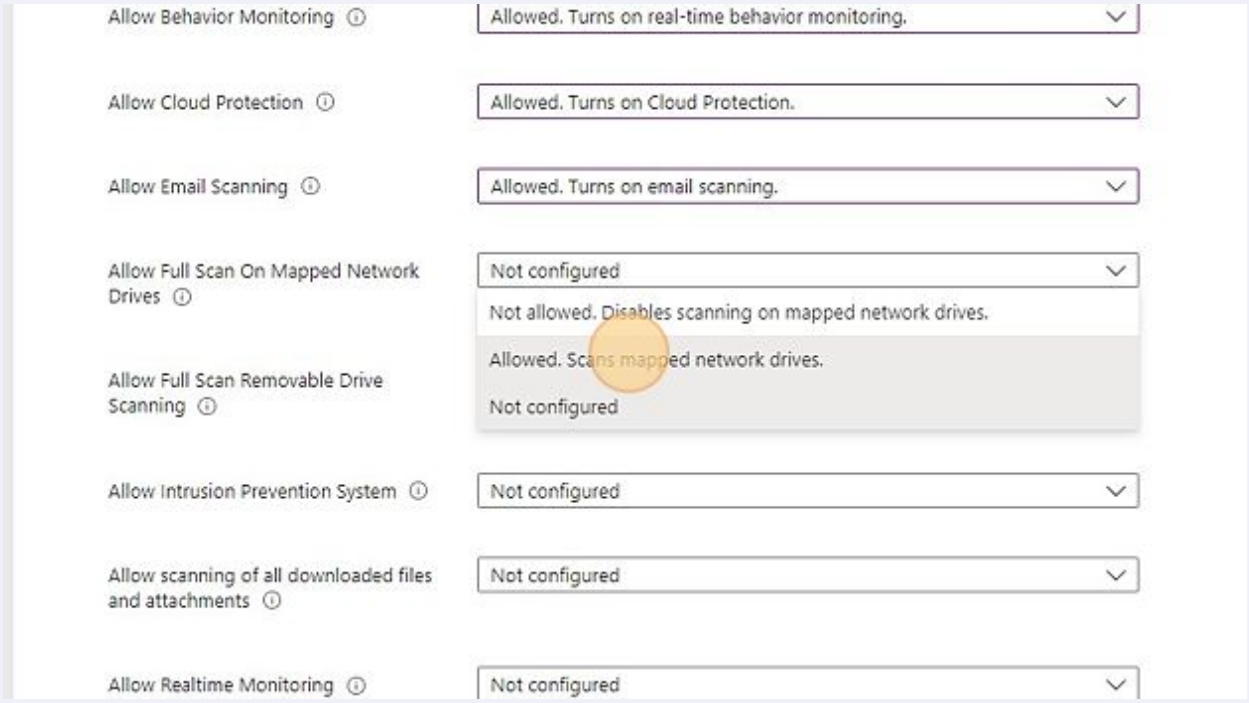
12 Click "Allowed. Turns on Cloud Protection."



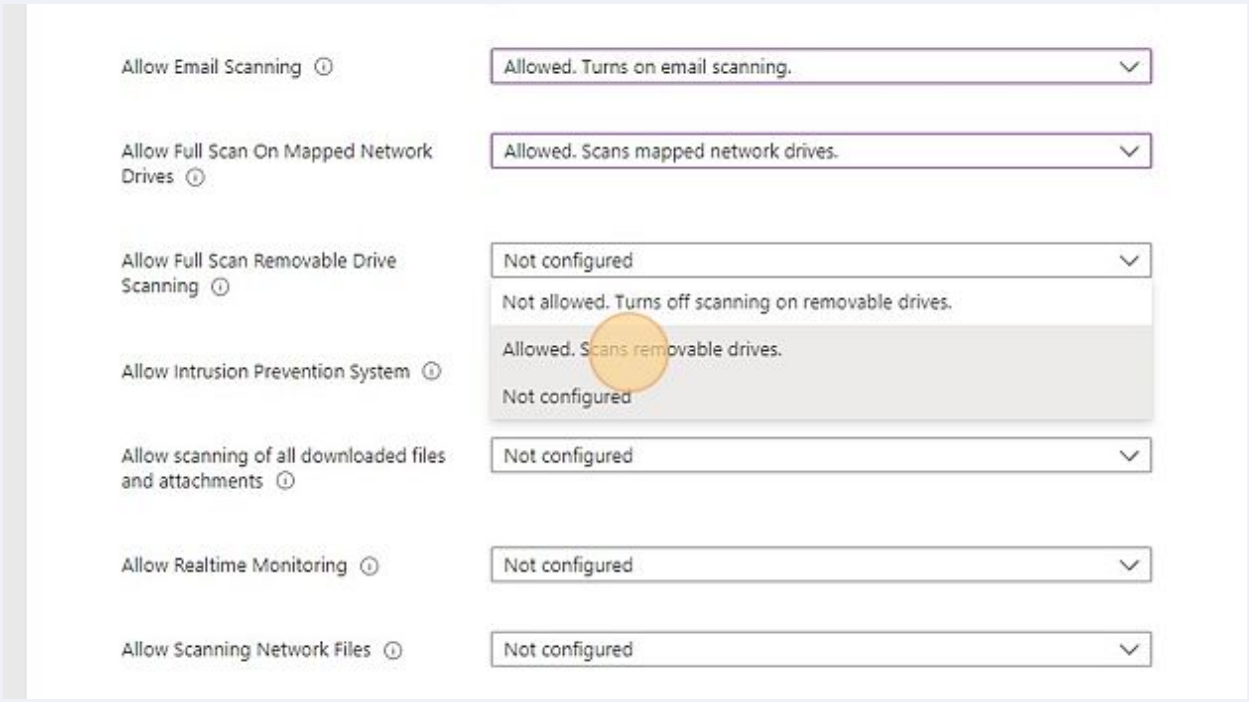
13 Click "Allowed. Turns on email scanning."



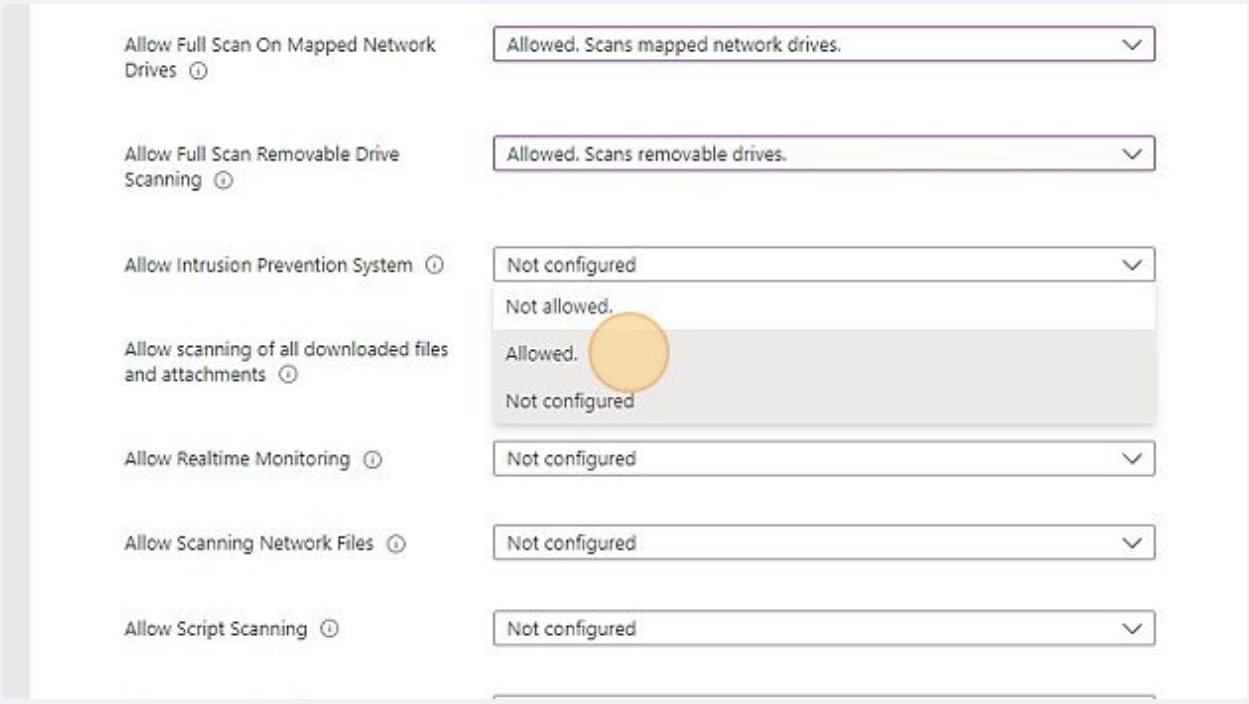
14 Click "Allowed. Scans mapped network drives."



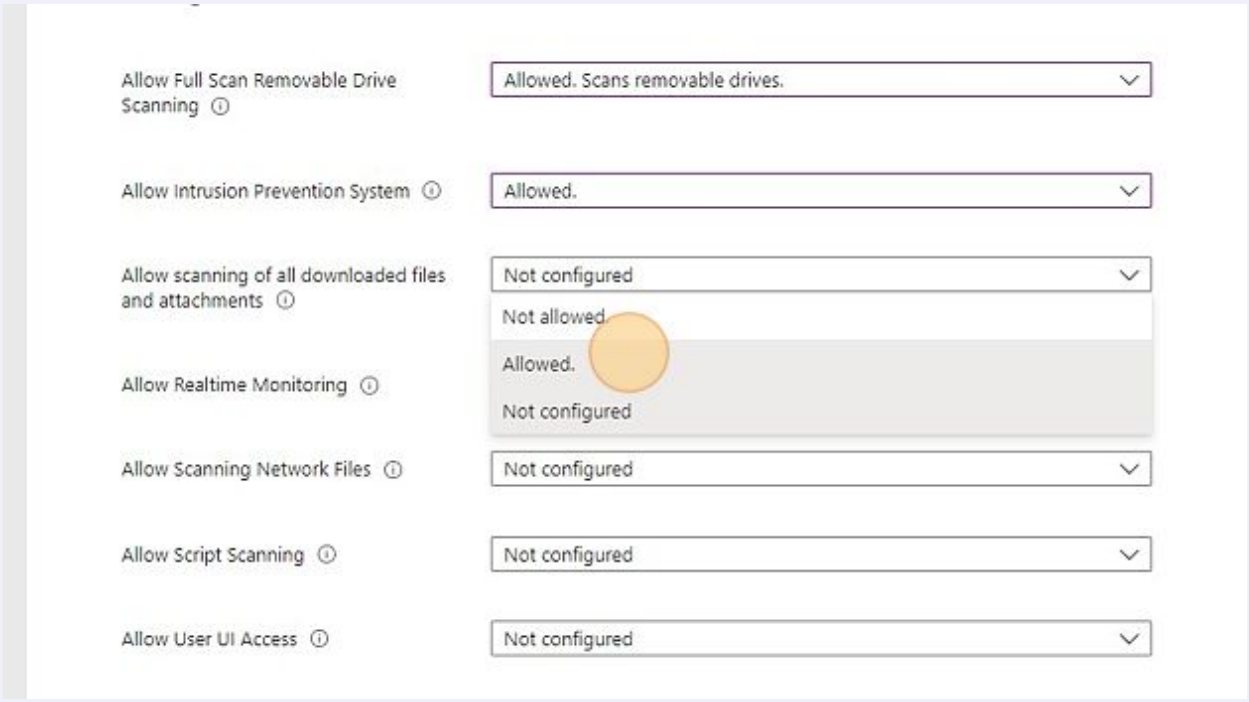
15 Click "Allowed. Scans removable drives."



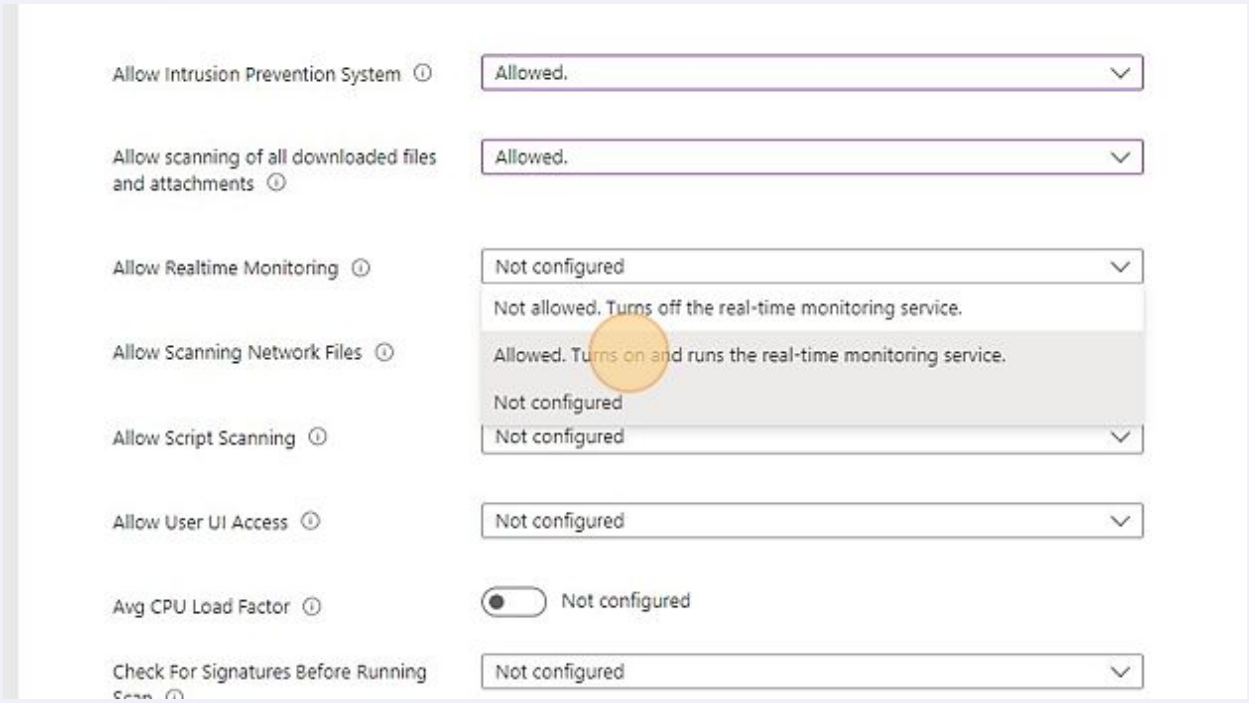
16 Click Allow Intrusion Prevention



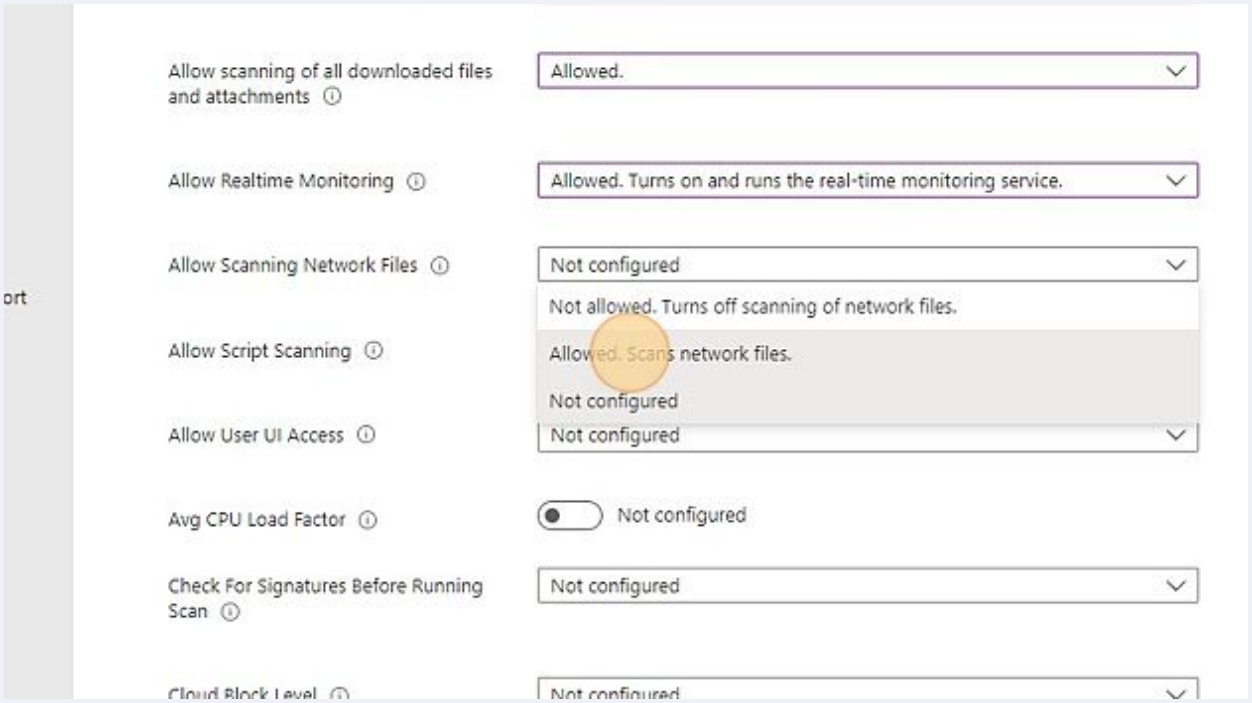
17 Click Allow scanning of all downloaded files and attachments



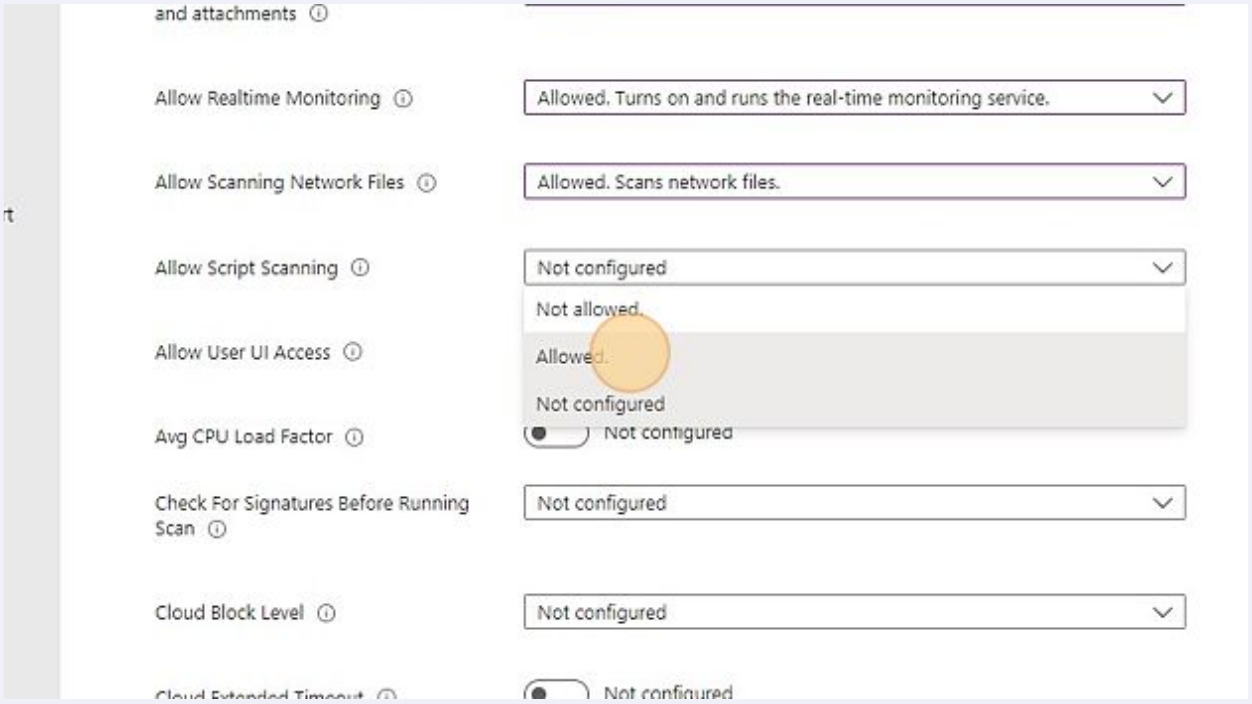
18 Click "Allowed. Turns on and runs the real-time monitoring service."



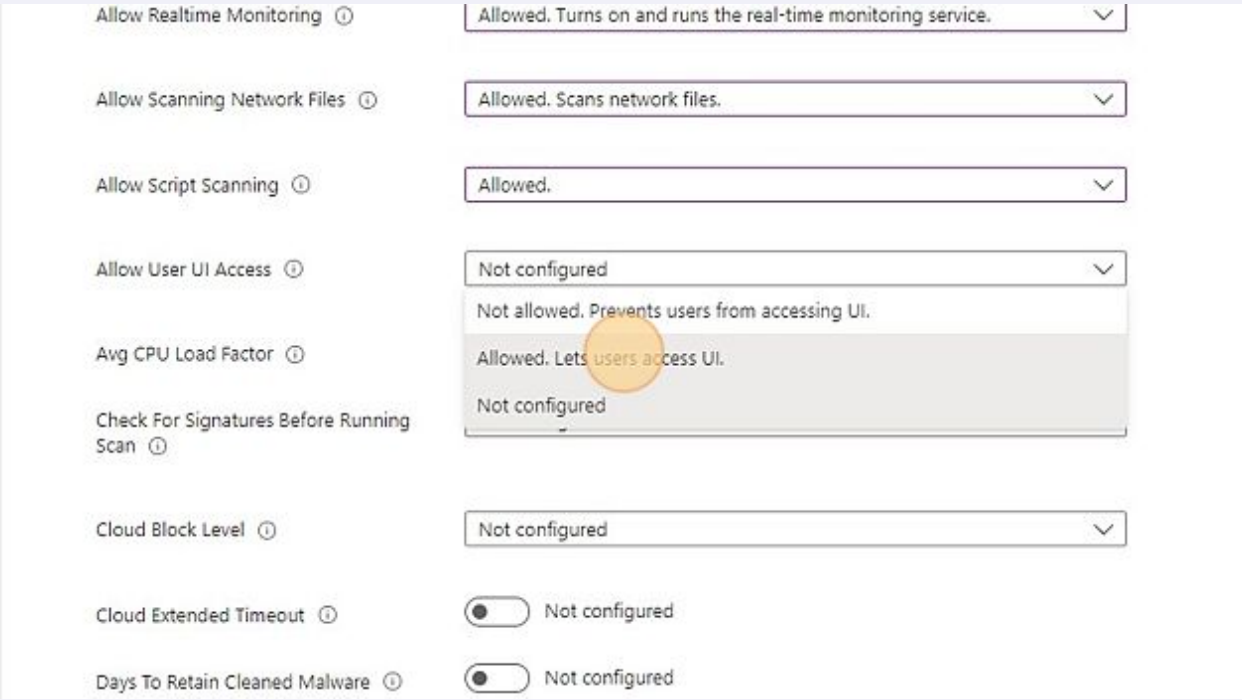
19 Click "Allowed. Scans network files."



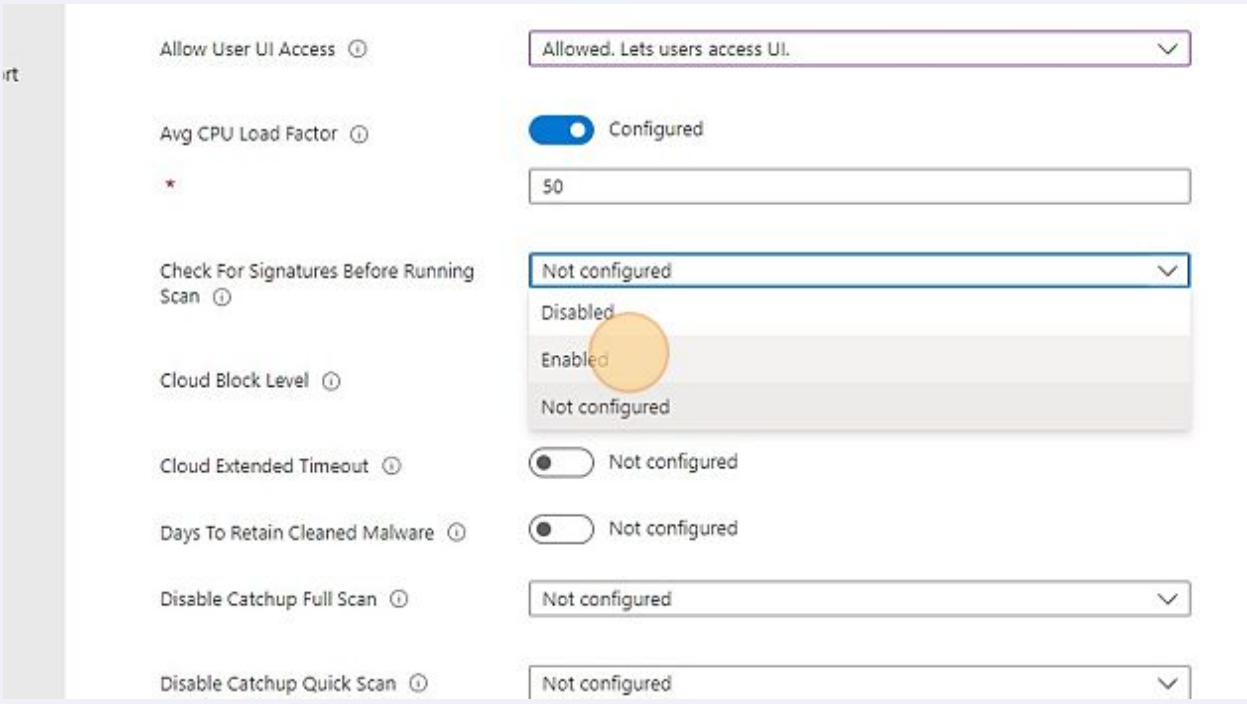
20 Click Allow script scanning



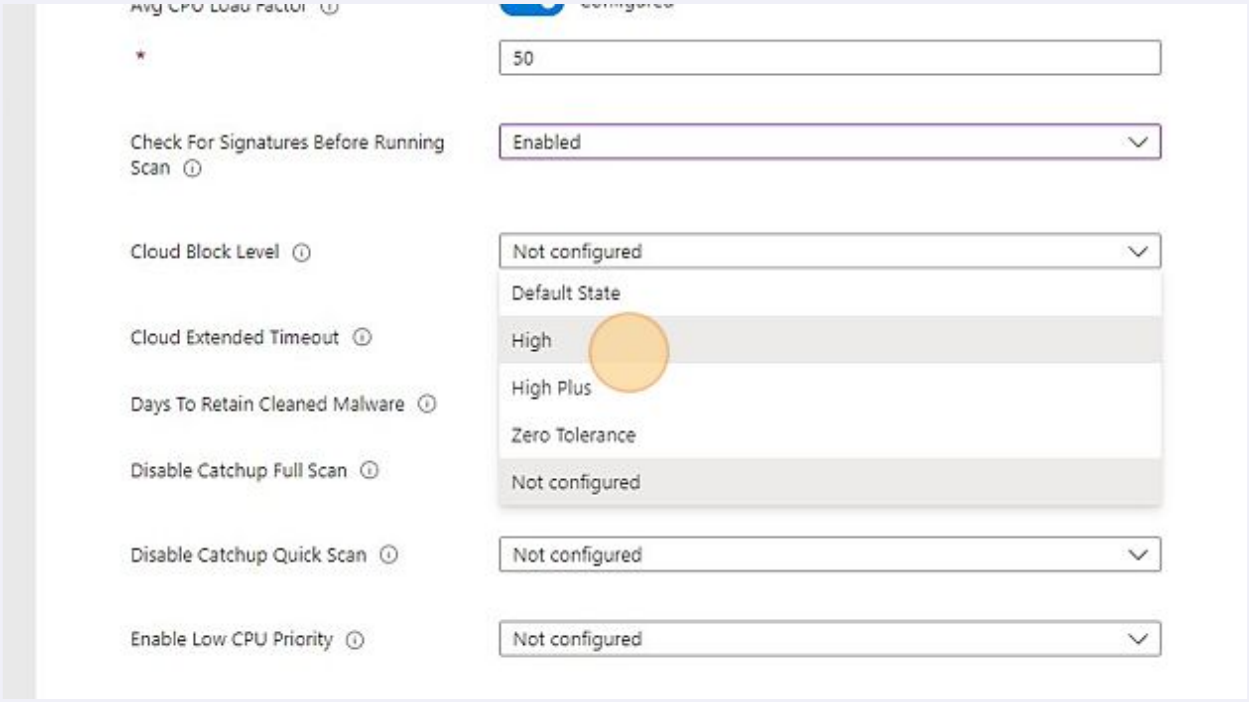
21 Click "Allowed. Lets users access UI."



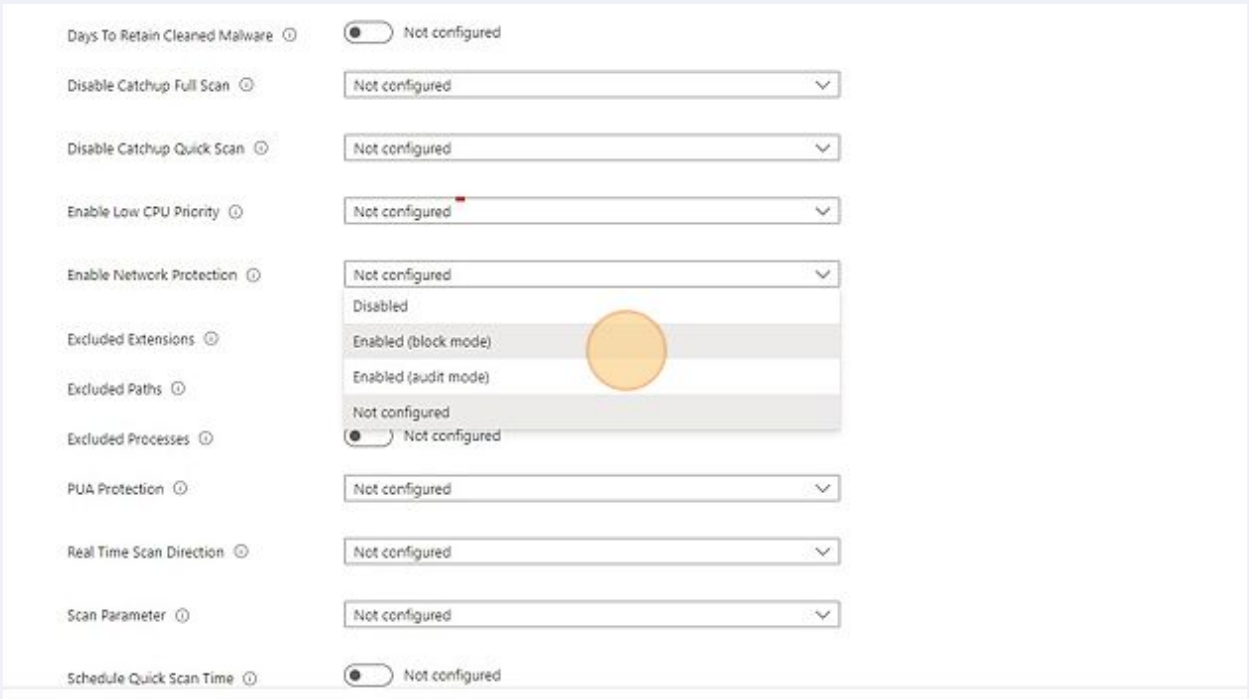
22 Enable Check for signatures before running scan



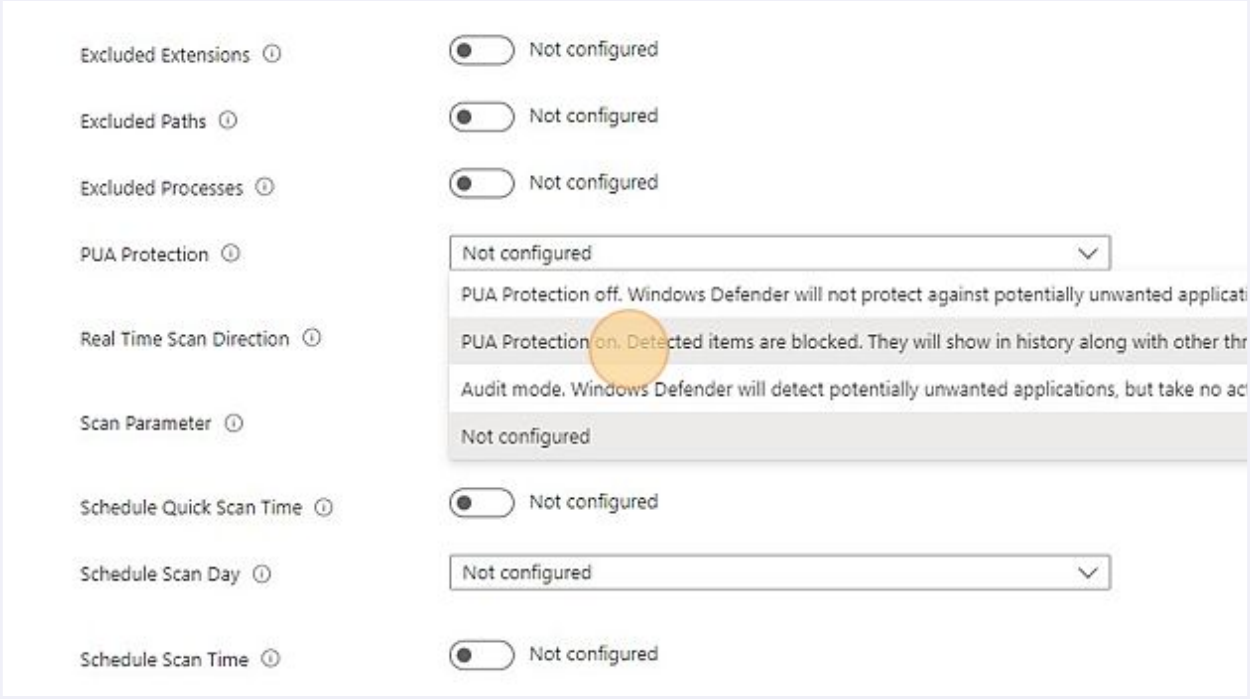
23 Set Cloud Block Level to High



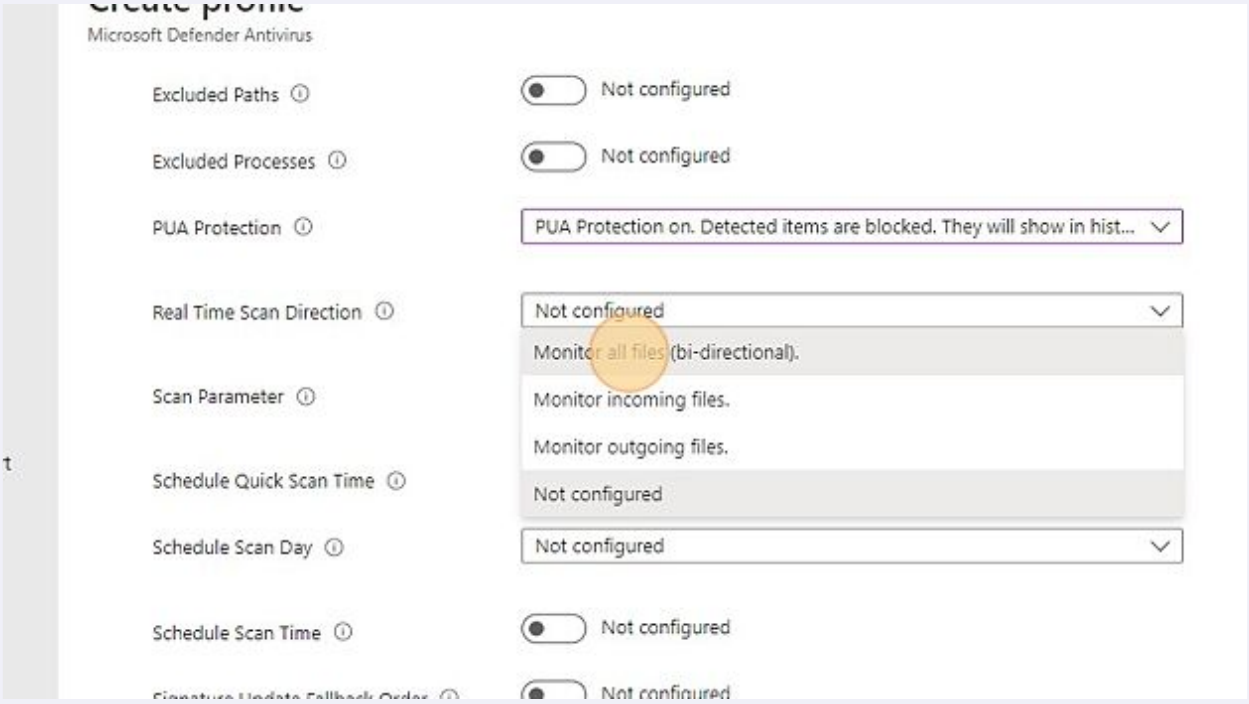
24 Enable Network Protection: Enabled (block mode)



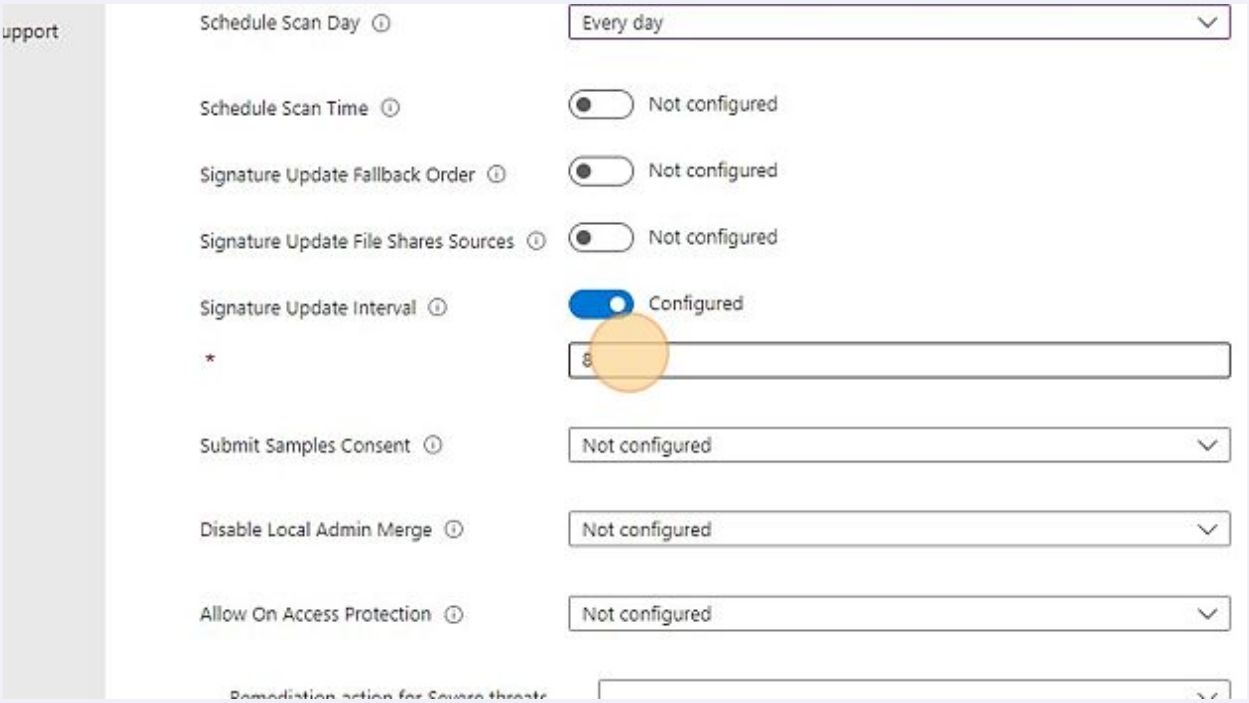
25 Click "PUA Protection on. Detected items are blocked. They will show in history along with other threats."



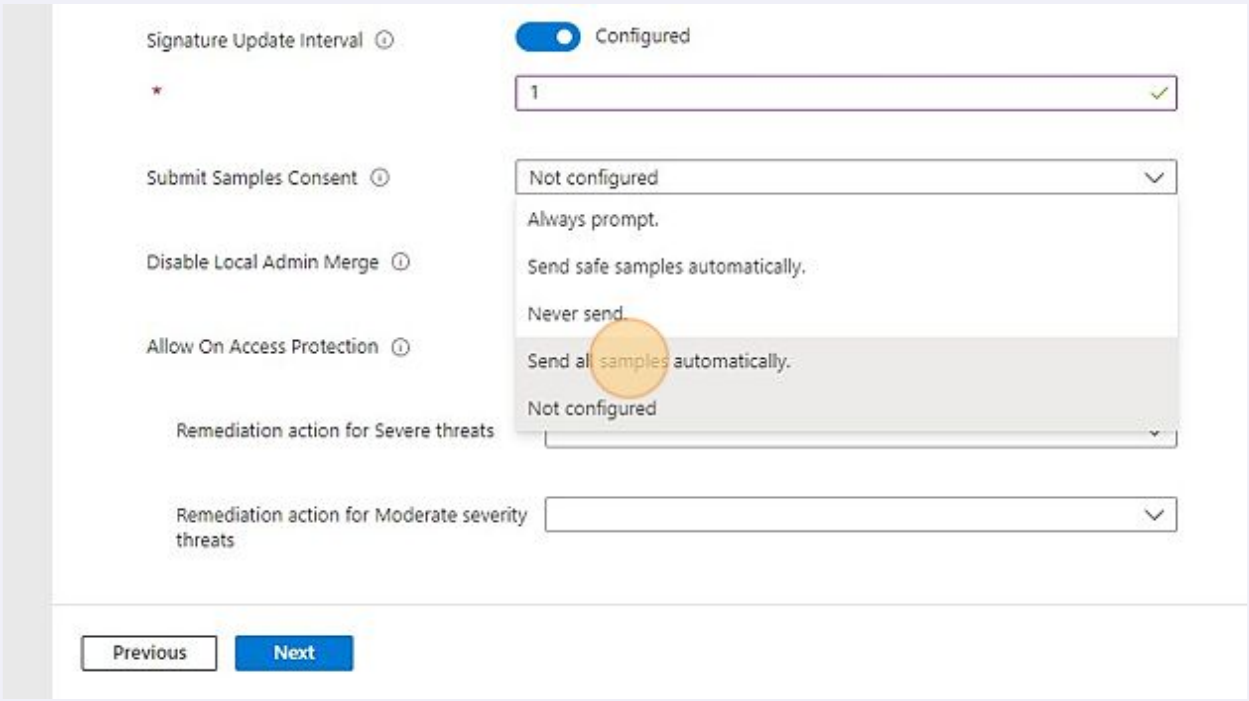
26 Click "Monitor all files (bi-directional)."



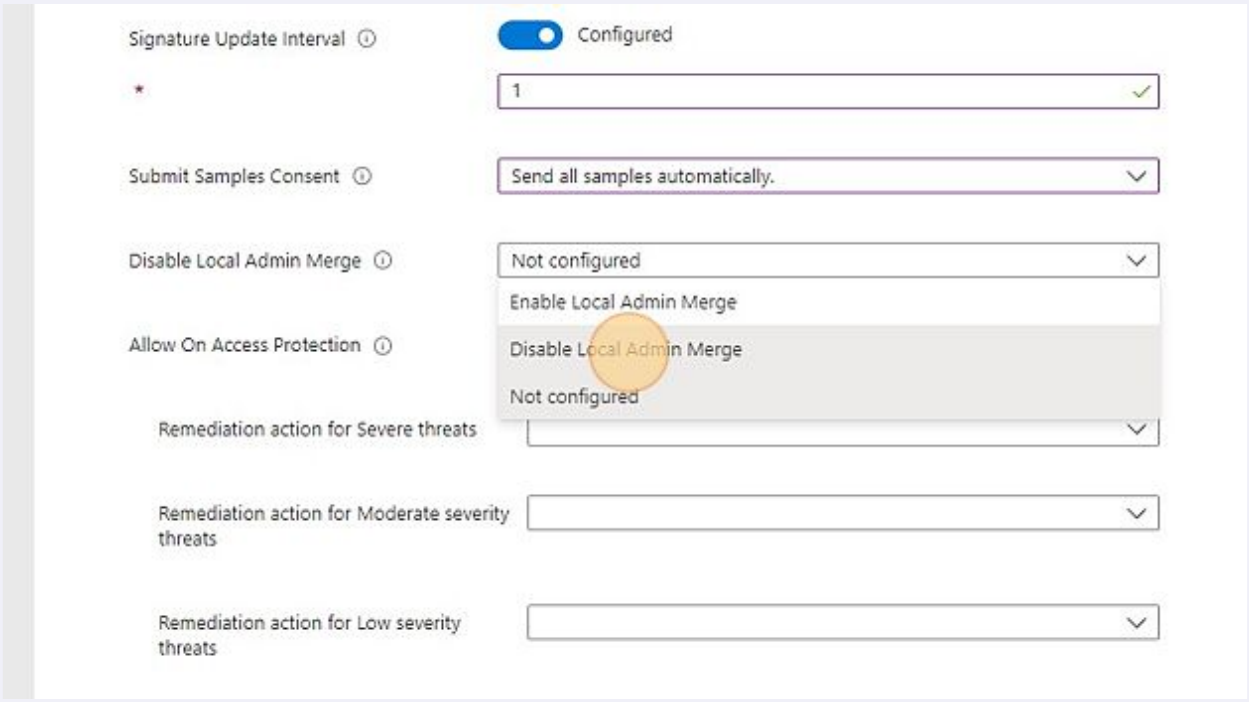
27 Set Signature update interval to 1 hour



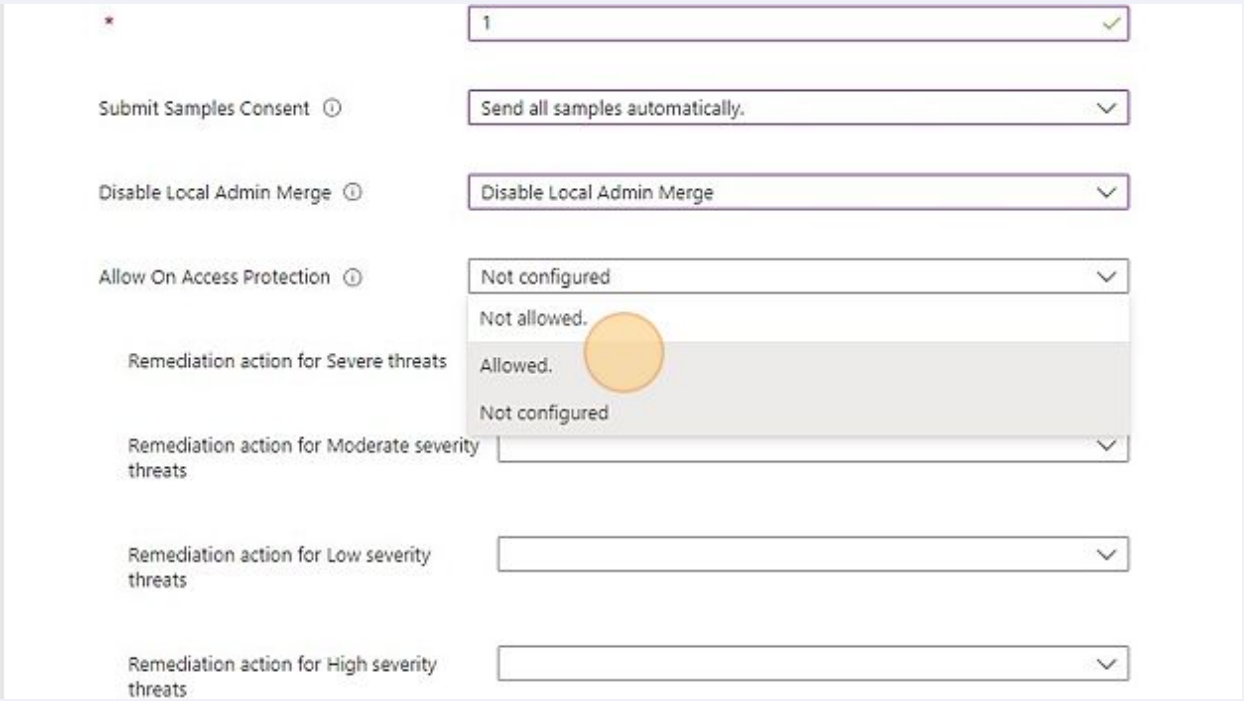
28 Click "Send all samples automatically."



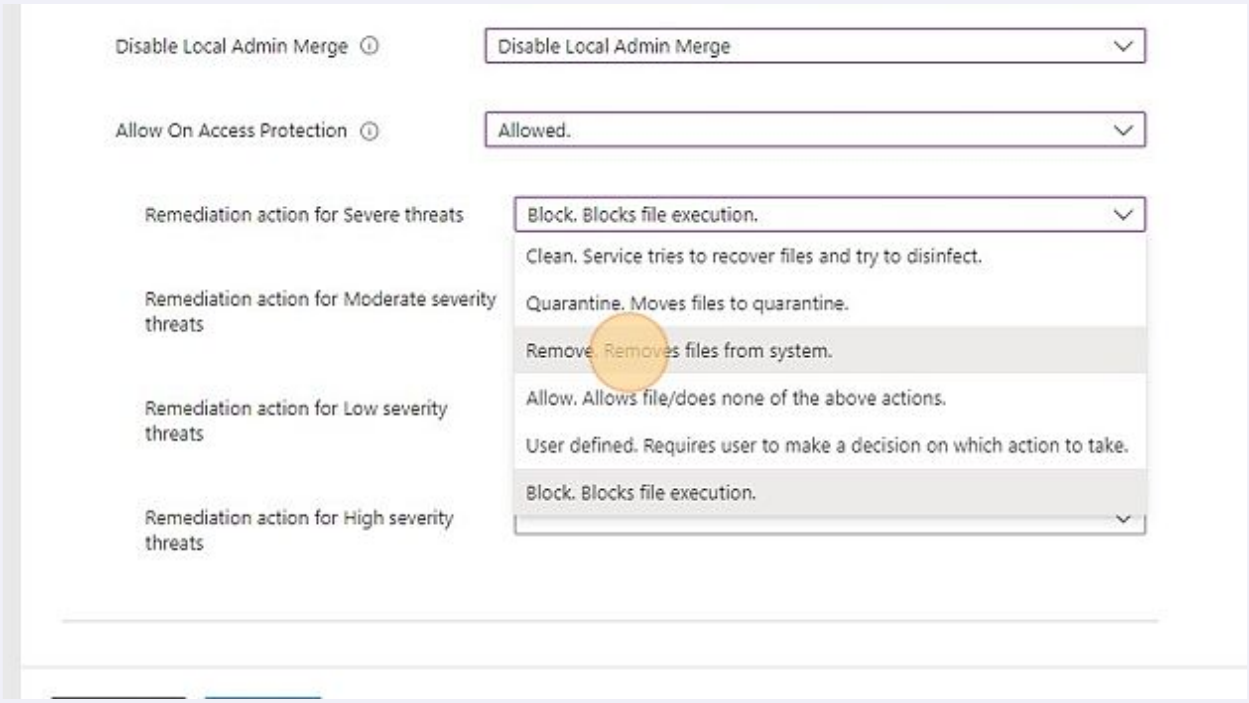
29 Click "Disable Local Admin Merge"



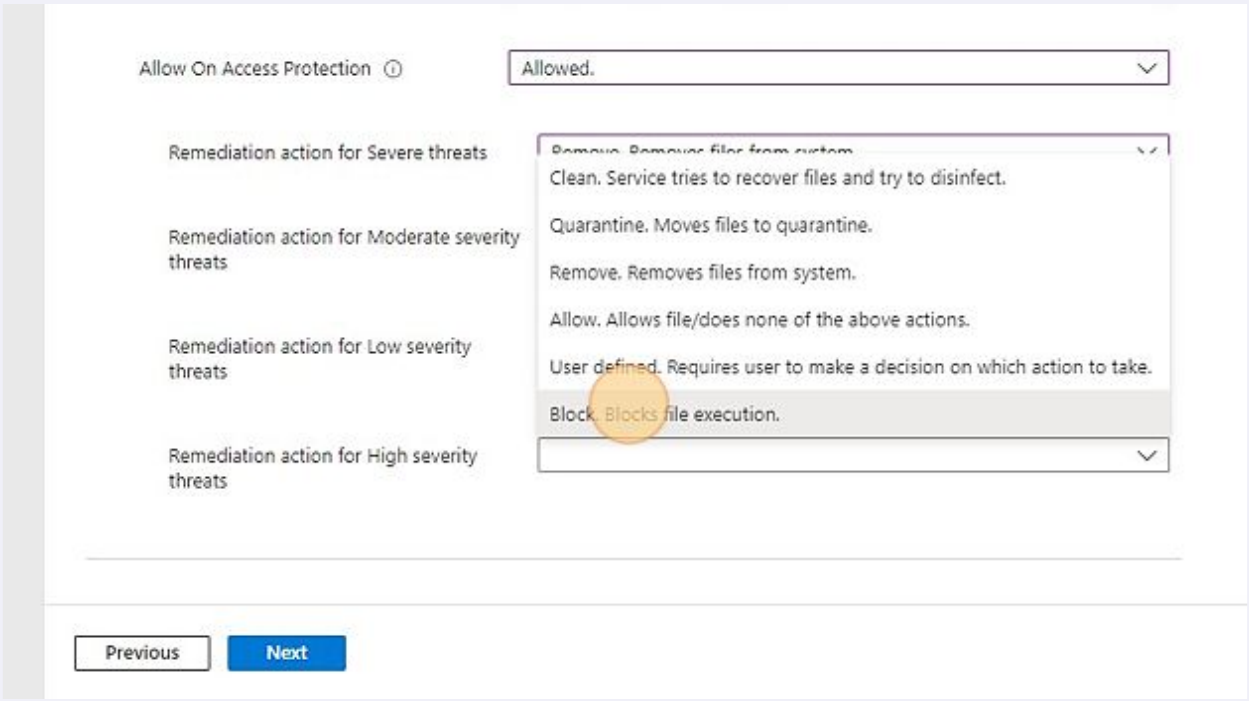
30 Allow on access protection



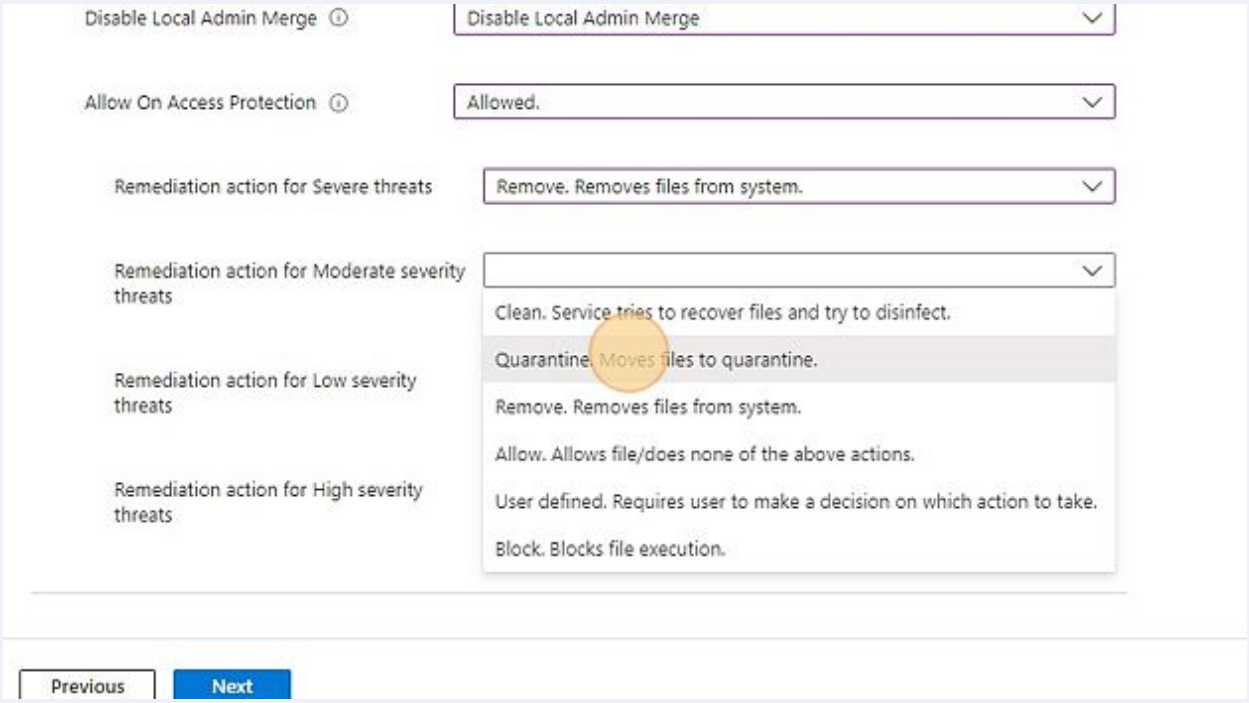
31 Set "Remediation action for Severe threats" to "Remove. Removes files from system."



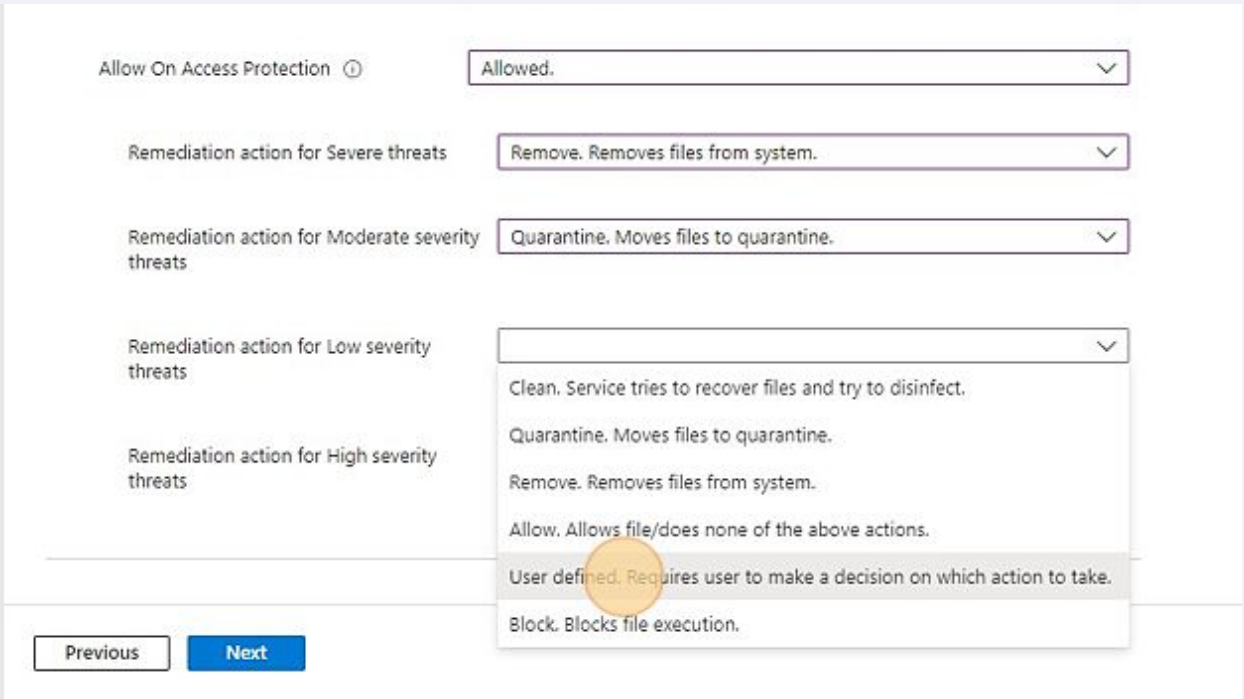
32 Set "Remediation action for High severity threats" to "Block. Blocks file execution."



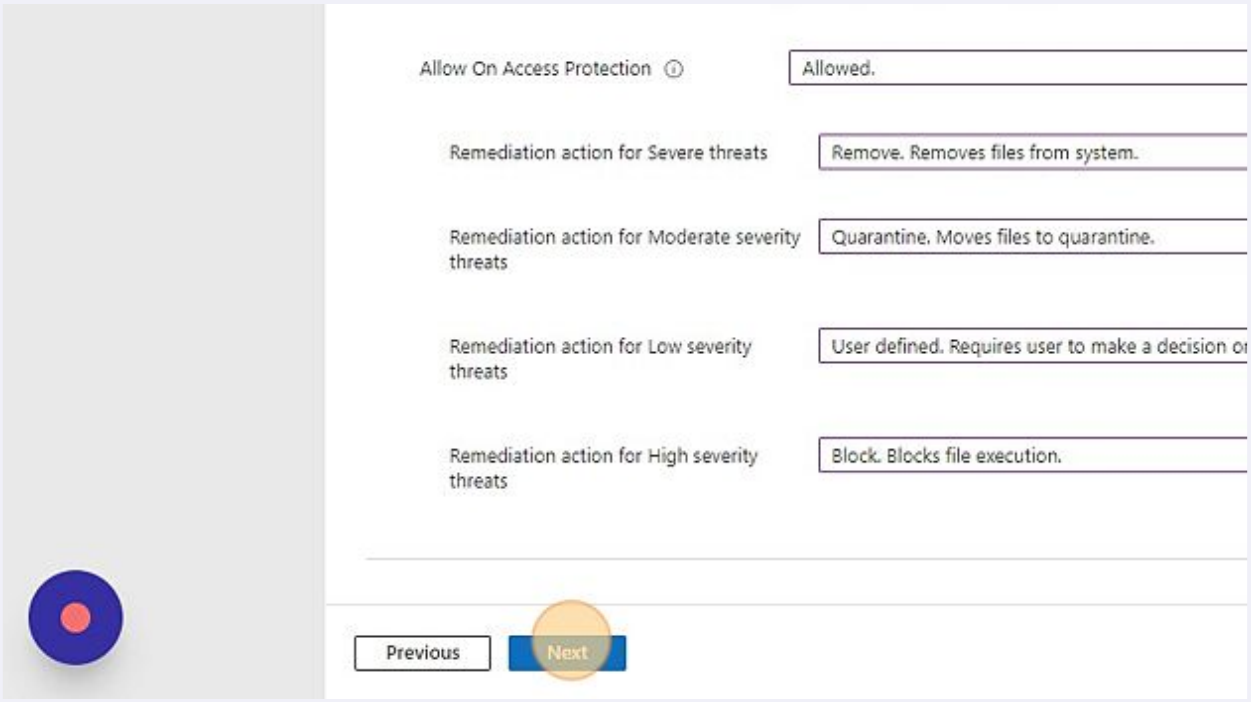
33 Set "Remediation action for Moderate severity threats" to "Quarantine. Moves files to quarantine."



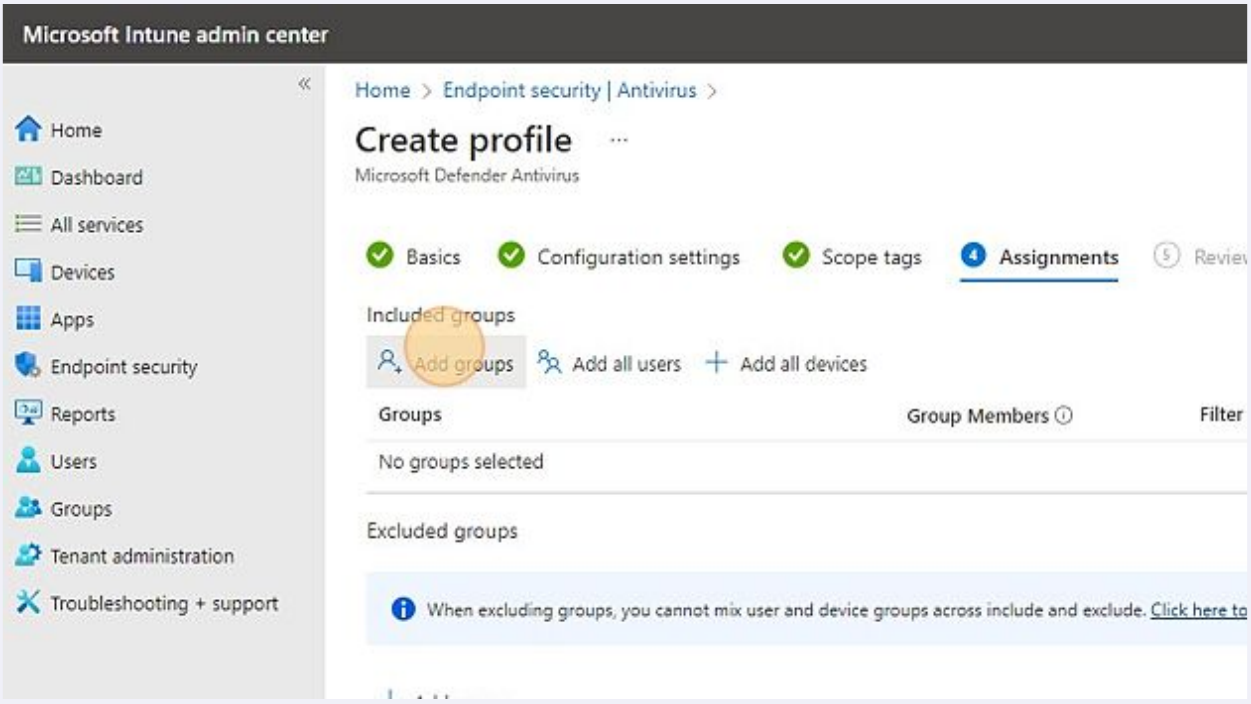
34 Set "Remediation action for Low severity threats" to "User defined. Requires user to make a decision on which action to take."



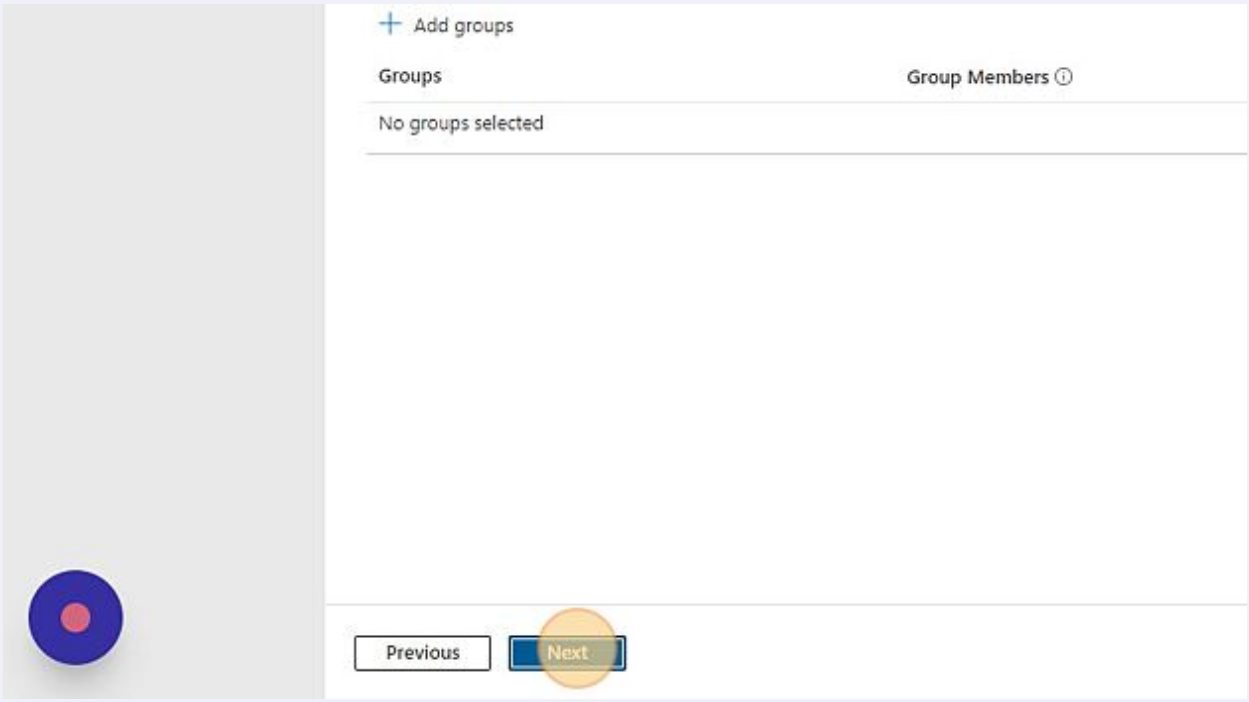
35 Click "Next"



36 Assign the profile to your security group



37 Click "Next"



38 Review your settings and click "Create"