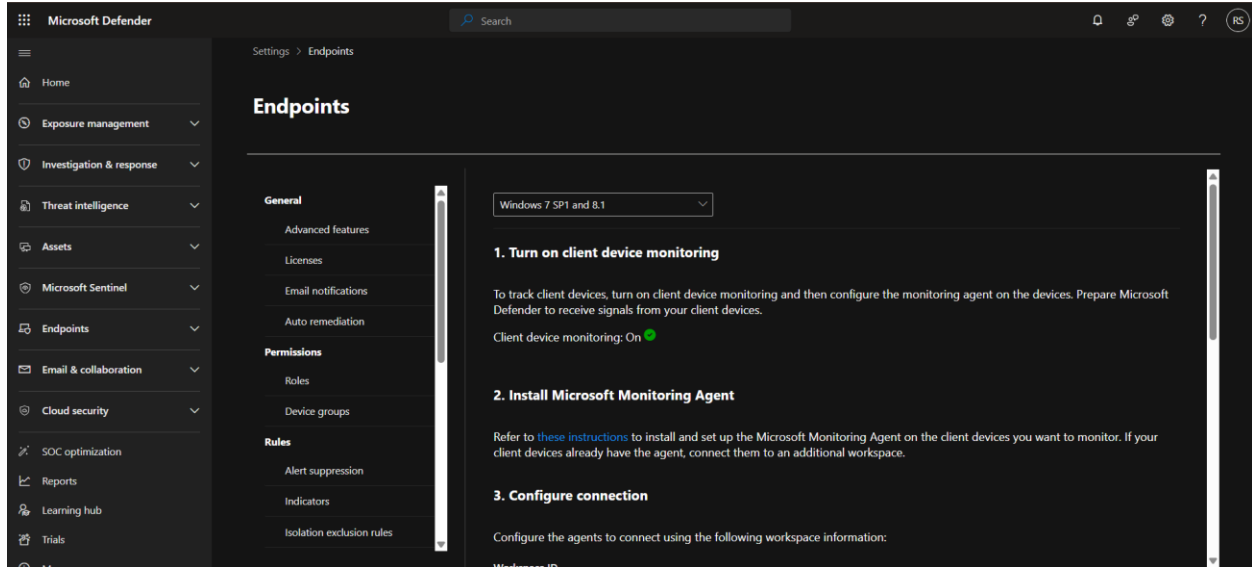


After Giving Administrator Security role to MySelf

Open the Security.microsoft.com and go to settings → on boarding →



Download Microsoft Monitoring Agent (MMA) on Endpoint → In my case it is Window 8.1

Summary of Deployment Methods

Intune (Microsoft Endpoint Manager) → Cloud-native method using Intune policies, Best for modern, managed devices (Windows, macOS, iOS, Android), Automated, scalable, integrates with compliance and Conditional Access.

Group Policy (GPO) → Uses Active Directory to push onboarding scripts/packages, Best for traditional on-premises, domain-joined Windows devices, Familiar to admins, but limited to Windows and less flexible for hybrid setups.

Microsoft Configuration Manager (SCCM/MECM) → Deploys onboarding package via SCCM software distribution, Best for enterprises already using SCCM, Powerful targeting and scheduling, but requires SCCM infrastructure.

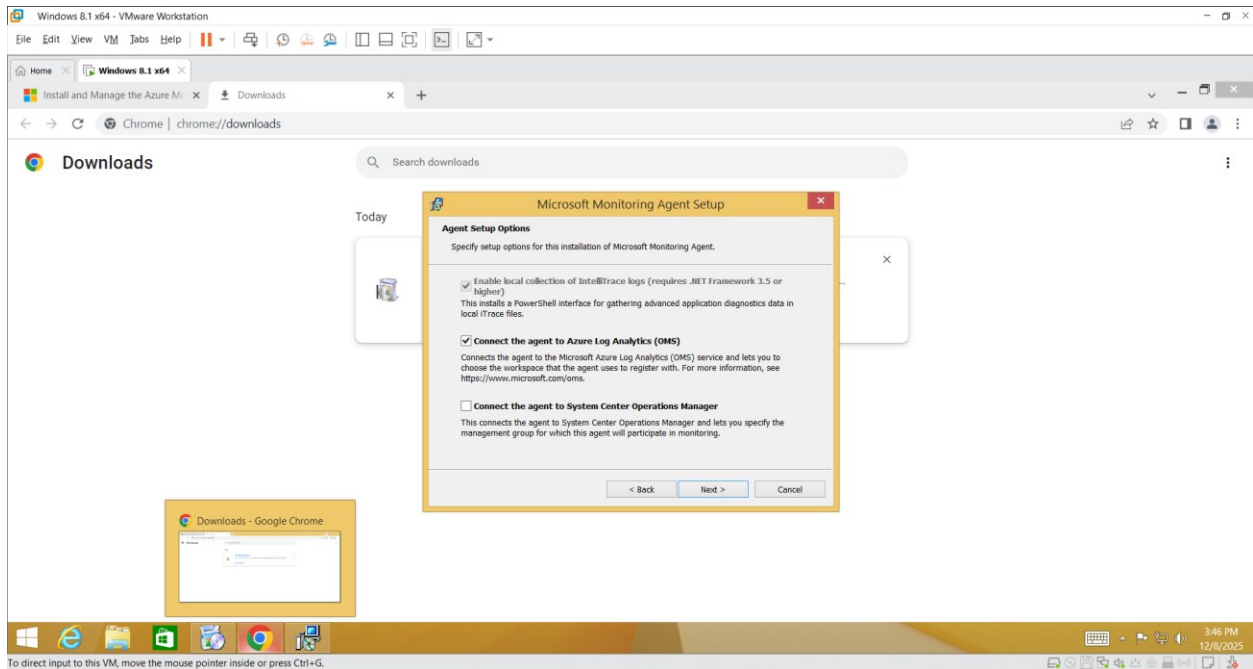
Local Script / Manual Onboarding → Run onboarding script manually on each device. Best for labs, proof-of-concept, or small environments. Simple, but not scalable.

Other MDM Solutions (Workspace ONE, MobileIron, Jamf, etc.) → Push onboarding package via third-party MDM, Best for organizations not using Intune but with other MDM platforms, Flexible, but less integrated than Intune.

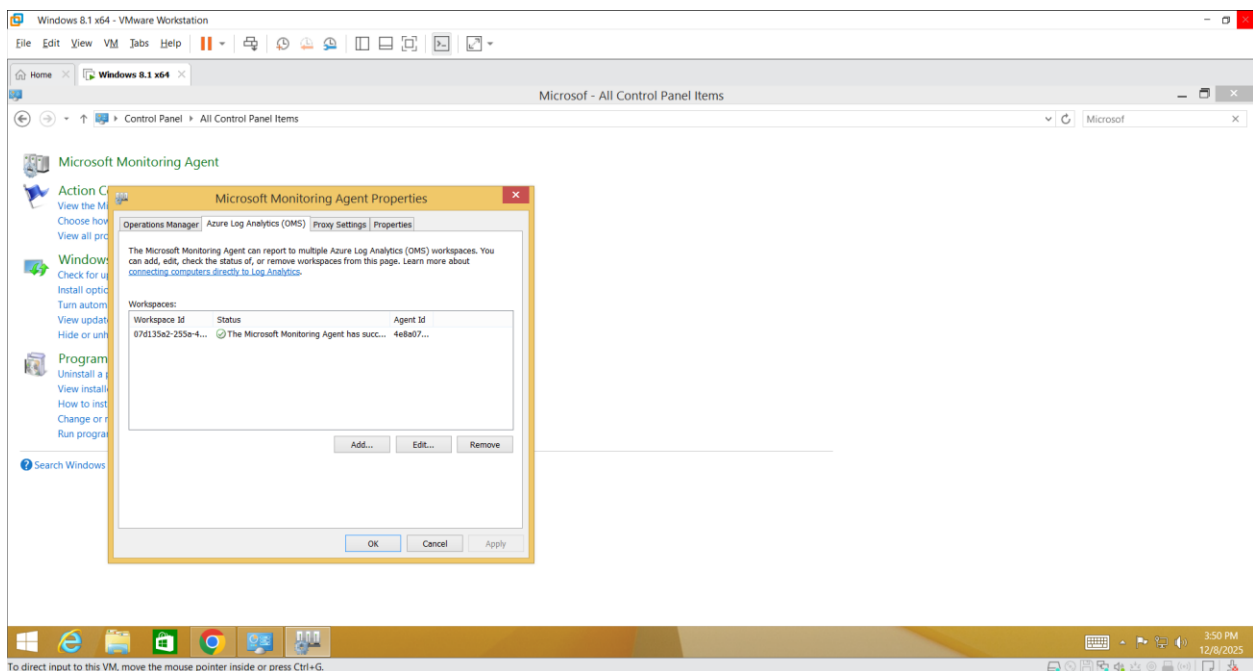
Linux/macOS Scripts → Platform-specific onboarding scripts deployed via Intune, MDM, or manual execution. Extends MDE protection beyond Windows. Reduced feature set compared to Windows.

VDI (Virtual Desktop Infrastructure) → Special onboarding packages for non-persistent VDI (Citrix, etc.), Best for enterprises with virtual desktop environments, Tailored for VDI, but requires careful configuration.

MMA (Microsoft Monitoring Agent) → Required for legacy OS (Windows 7, 8.1, Server 2008 R2) Connects devices to Log Analytics workspace, then MDE. Enables basic telemetry, but deprecated and limited compared to modern onboarding.



Enter Workspace ID and Key from Security.microsoft.com onboarding portal



Device Inventory Can find a Device

The screenshot shows the Microsoft Defender console with the 'Device Inventory' page selected. The left sidebar contains navigation options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Cloud, AI agents, Microsoft Sentinel, Endpoints, Partners and APIs, Configuration management, and Email & collaboration. The main content area displays the 'Device Inventory' title and a 'Create rules for devices' link. Below this are two cards: 'Classify critical assets' and 'Upgrade your vulnerability management capabilities'. A notification banner states: 'Transient devices have been automatically filtered out from some tabs to minimize noise. This filtering is determined by an internal algorithm, which mainly depends on the frequency of appearances of these discovered devices. To disable this automatic filtering, navigate to the filter menu.' The 'All devices' tab is active, showing a summary of device counts: Total (1), Critical assets (0), High risk (0), High exposure (0), Not onboarded (0), and Newly discovered (1). Below the summary is an 'Export' button and a search bar. A table lists the devices with columns: Name, IP, Criticality level, Device category, Device type, Domain, Device AAD id, Risk level, and Exposure level. One device is listed: 'win-ceg71ag32mj' with IP '192.168.79.130', categorized as 'Computers and Mo...' and 'Workstation'.

The screenshot shows the 'Permissions and roles' page in the Microsoft Defender console. The left sidebar is the same as the previous screenshot. The main content area shows the 'Permissions and roles' title and a 'Learn more' link. Below the title is a description: 'Roles define what users can see and do in Microsoft Defender. Assign only the permissions they need to stay secure.' There are buttons for 'Export', 'Create custom role', and 'Delete roles'. A search bar shows '1 item'. A table lists the roles with columns: Role name, Description, Data source, Last updated, and Assigned to. One role is listed: 'Tier support 1' with description '...', data source 'All data sources', last updated '12/27/2025, 1:31:07 PM', and assigned to '1 users, 0 groups'.

The screenshot shows the 'Add device group' page in the Microsoft Defender console. The left sidebar is the same as the previous screenshots. The main content area shows the 'Add device group' title and a 'Preview devices' section. The 'Preview devices' section has a notification: 'Shows up to 10 devices. If a device in this group matches groups with a higher rank, it will show in the preview but will only be added to the group with the highest rank.' There is a 'Show preview' button. Below this is a table with columns: Device name. One device is listed: 'win-ceg71ag32mj'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Microsoft Defender

Microsoft Sentinel

Endpoints

Email & collaboration

Cloud security

SOC optimization

Reports

Learning hub

Trials

More resources

System

Data management

Permissions

Health

Settings

Search

Settings > Endpoints

Endpoints

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups

Rules

Alert suppression

Indicators

Isolation exclusion rules

Process Memory Indicators

Device group configuration has changed. Apply changes to check matches and recalculate groupings.

Apply changesDiscard changes

Organize devices into groups, set automated remediation levels, and assign administrators.

+ Add device group1 itemCustomize columns

<input type="checkbox"/>	Rank ↑	Device group	Devices	Remediation level	Description
<input type="checkbox"/>	1	Regular User	0	Full remediation	