

After Giving Administrator Security role to MySelf

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

The screenshot shows the Microsoft Defender interface under the 'Endpoints' section. On the left is a navigation sidebar with various security categories like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, and Endpoints (which is currently selected). The main content area is titled 'Endpoints' and contains three numbered steps: 1. Turn on client device monitoring (status: On), 2. Install Microsoft Monitoring Agent (status: Refer to instructions), and 3. Configure connection (status: Configure the agents to connect using the following workspace information: Workspace ID).

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.

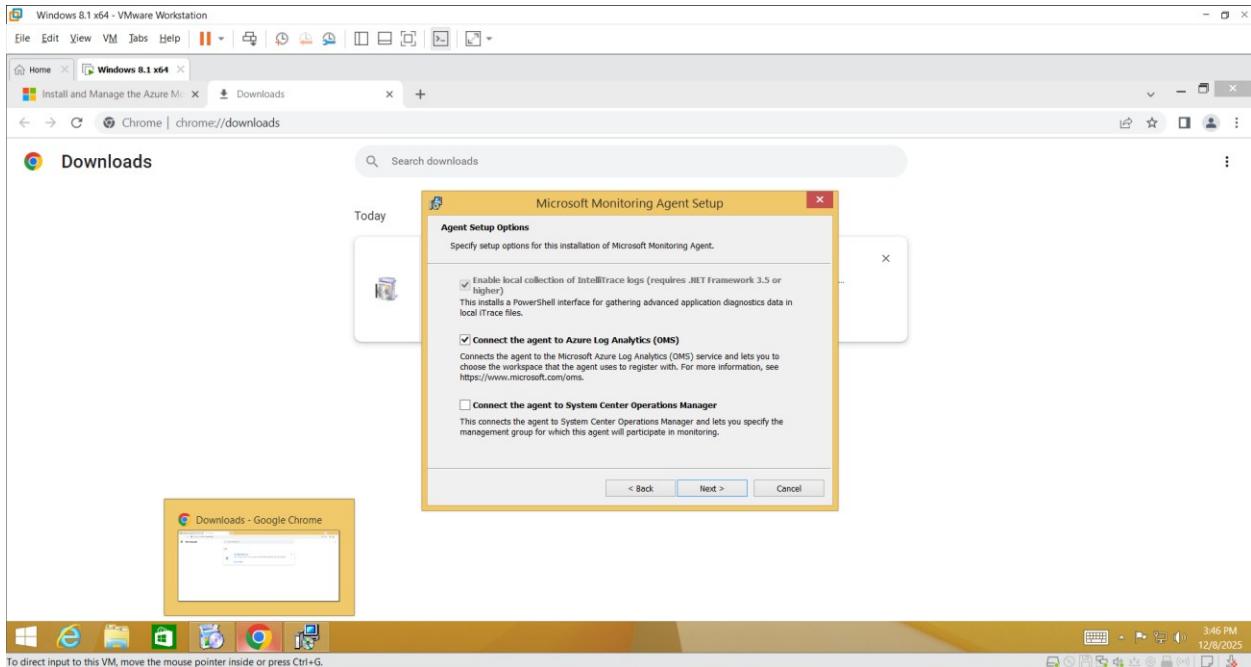
Local Script / Manual Onboarding → Run onboarding script manually on each device. Best for labs, proof-of-concept, or small environments. Simple, but not scalable.

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.

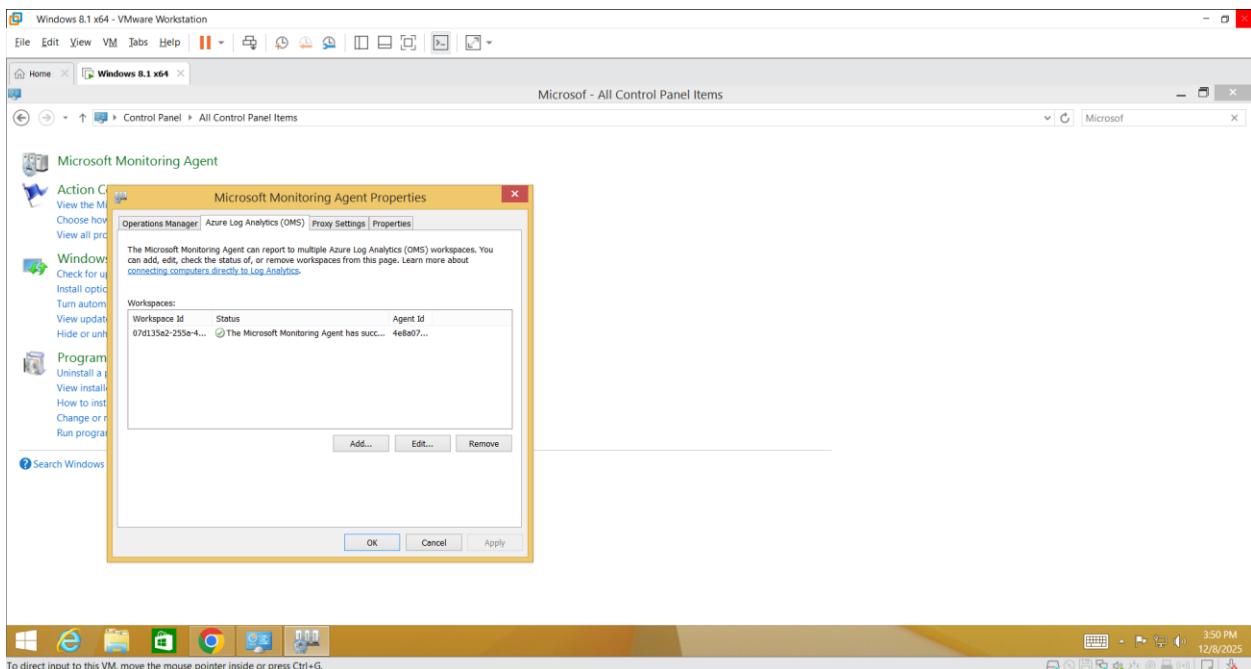
Linux/macOS Scripts → Platform-specific onboarding scripts deployed via Intune, MDM, or manual execution. Extends MDE protection beyond Windows. Reduced feature set compared to Windows.

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 Device Inventory interface. On the left, a navigation sidebar includes sections like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Cloud, AI agents, Microsoft Sentinel, Endpoints, Partners and APIs, Configuration management, Dashboard, Endpoint security policies, and Email & collaboration. The main area is titled "Device Inventory" and displays a summary: Total 1, Critical assets 0, High risk 0, High exposure 0, Not onboarded 0, Newly discovered 1. Below this, a table lists a single device: Name win-ceg7tag32mj, IP 192.168.73.130, Category Computers & Mobile, Type Workstation, Domain Workgroup. A search bar and filter options are at the top.

The screenshot shows the Microsoft Defender Permissions and roles settings page. The left sidebar includes sections like Microsoft Sentinel, Endpoints, Email & collaboration, Cloud security, SOC optimization, Reports, Learning hub, Trials, More resources, System, Data management, Permissions, Health, Settings, and Customize navigation. The main area is titled "Permissions and roles" and shows a table of roles: Tier support 1, assigned to All data sources, last updated 12/27/2025, 1:31:07 PM, and 1 user, 0 groups. A search bar and filter options are at the top.

The screenshot shows the Microsoft Defender Add device group wizard. The left sidebar includes sections like Microsoft Sentinel, Endpoints, Email & collaboration, Cloud security, SOC optimization, Reports, Learning hub, Trials, More resources, System, Data management, Permissions, Health, Settings, and Customize navigation. The main area is titled "Add device group" and shows the "Endpoint" tab selected. It lists categories: General, Devices, Preview devices (selected), and User access. To the right, under "Preview devices", it says "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." A "Show preview" button is present. The preview section shows one item: Device name \win-ceg7tag32mj. Navigation buttons Back, Next, and Cancel are at the bottom.

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

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

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

Add device group

1 item | Customize columns

| Rank ↑ | Device group | Devices | Remediation level | Description |
|--------|--------------|---------|-------------------|-------------|
| 1 | Regular User | 0 | Full remediation | |

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups

Rules

Alert suppression

Indicators

Isolation exclusion rules

Process Memory Indicators

Apply changes

Discard changes

The screenshot shows the Microsoft Defender interface for managing endpoints. On the left, a sidebar lists various security categories like Microsoft Sentinel, Cloud security, and System. Under the 'Endpoints' section, there's a 'Device groups' option which is currently selected, indicated by a blue underline. The main pane is titled 'Endpoints' and displays a message about device group configuration changes. Below this, it says 'Organize devices into groups; set automated remediation levels, and assign administrators.' A button to 'Add device group' is present. The central part of the screen shows a table with one item: a device group named 'Regular User' with a rank of 1, 0 devices, and a remediation level of 'Full remediation'. There are also buttons for 'Apply changes' and 'Discard changes' at the top of the table area. The overall theme is dark with light-colored text and icons.