

Endpoint device USB Lockdown

USB device drives can be locked. A device policy governs the blocking of USB devices. You can use the **USB Lockdown** device policy to:

- **Block portable devices:** USB connected mobile device.
- **Block mass storage devices:** USB flash drive or USB external hard drive.

Note

The **USB Lockdown** device policy is supported on both *Windows* and *macOS* devices. **Block portable devices** and **Block mass storage devices** are supported on *Windows* devices. **Block mass storage devices** is supported for *macOS* devices.

Locking USB drives on a device offers several benefits, primarily focused on enhancing security and data protection:

- **Reduced attack surface:** Limiting USB usage reduces the attack surface, simplifying the security landscape and allowing organizations to focus on other critical areas of defense against malware.
- **Malware prevention:** Safeguard against malware spread via infected USB drives, lowering the risk of infecting your device or network. Malware can infect a device via:
 - **Malware distribution:** Malicious software can easily spread via infected USB drives when plugged into a device. Blocking USB devices reduces the chances of malware being introduced through these means, protecting the network from potential infections.
 - **Automated malware execution:** Some malware is designed to execute automatically when a USB drive is inserted into a device. By blocking USBs, this automatic execution is prevented, giving security teams more time to analyze and respond to potential threats.
 - **Zero-day exploits:** USB-related vulnerabilities, known as zero-day exploits, can be targeted by malware. Blocking USB devices can mitigate the risk associated with such vulnerabilities, reducing the potential for malware attacks.
 - **Insider threat mitigation:** Blocking USB devices helps mitigate insider threats where employees with malicious intent attempt to introduce malware via portable storage devices. This proactive measure reduces the risk of internal attacks.