



## Device Actions Cheat Sheet

### DEVICE TAGGING

Tags can be added to devices to **create logical groups**. Tagging is a good way to filter devices and adds context to what the device is. Device tagging can be used to create device groups.

You can assign tags in multiple ways, please refer to this [blog](#) for the methods on Windows Machines.

### INVESTIGATION PACKAGE

Investigation Packages will allow you to **collect key information** about a device for offline investigations. Investigation Packages collect the following:

- Autoruns
- Installed Programs
- Network Connections
- Processes
- Scheduled Tasks
- Security Event Logs
- Services
- System Information
- Temp Directories
- Users & Group Info
- WdSupportLogs

### RESTRICT APP EXECUTION

Restricting App Execution applies a code integrity policy that only allows files to execute if they are signed by a **Microsoft issued certificate**.

This is reversible and the end user will be notified.

### RUN ANTIVIRUS SCAN

Run an on-demand scan on individual devices as required. 2 types of scans can be executed:

- Quick Scan
- Full Scan

In most cases, a **quick scan is sufficient** as it will check key locations of the device.

**Note:** The default CPU limit is 50%. This is adjustable via Endpoint policies.

### INITIATE LIVE RESPONSE

Initiating a Live Response session will provide **instant remote shell access** to the device, giving administrators the ability to conduct deeper investigations. There are specific commands for Live Response that allows analysis and actions to be taken on the device.

### AUTOMATED INVESTIGATION

Initiating an Automated Investigation will create an investigation. During this period, any alert generated from the device is added to the ongoing investigation.

If the same threat is seen on other devices, the scope is expanded, and those devices are added to the investigation.

This feature allows organised management when responding to a Security Incident.

**Note:** Windows devices are currently supported.

### DEVICE ISOLATION

Isolating a device will restrict network connectivity, **only allowing connectivity to Defender for Endpoint**. This can help contain attackers from remotely controlling the infected device whilst remediation actions are applied.

Options are available for supported devices to allow Teams, Outlook and Skype for Business communications.

To list all devices in isolation, the following [KQL query](#) can be used in the advanced hunting section.

You can release the isolation from the Defender for Endpoint device page. There is also an option to force the release via script.