

RESPONSE ACTIONS

Managed Cyber Services

DOCUMENT CONTROL

Version	Completed by	Date
1.4	George Dunning	1 October 2025
1.5	George Dunning	02 February 2026
1.6	George Dunning	24 September 2026

PREPARED BY

Name	Job title
George Dunning	Service Development Product Manager

Introduction

This document provides additional information on the available and supported response actions available as part of the Managed XDR for Microsoft Sentinel Service.

The customer will need to be licensed as per the vendor requirements for the response action capabilities to be leveraged within the Service.

Vendors

Platform	URL	Microsoft Sentinel	Level Blue USM Anywhere
Microsoft Defender for Endpoint	https://www.microsoft.com/en-gb/security/business/endpoint-security/microsoft-defender-endpoint	✓	
Microsoft Entra ID	https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-remediate-unblock	✓	
SentinelOne	https://www.sentinelone.com/	✓	✓
Carbon Black EDR	https://www.broadcom.com/products/carbon-black	✓	
Sophos XDR	https://www.sophos.com/	✓	
CrowdStrike Falcon	https://www.crowdstrike.com/	✓	
FortiEDR	https://www.fortinet.com/	✓	

Response Actions

The available actions for each supported vendor can be found below. Available actions or behavior may differ between OS, please refer to the vendor documentation for any specific queries surrounding Linux or Mac devices.

Microsoft Defender for Endpoint

Action	Description
Collect investigation package	Provides a .zip file of information from the specified device to help investigate the current state of the device. Information such as, Autoruns, Installed programs, Network connections, Prefetch files, Processes and more. Full list can be found here: https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alerts#collect-investigation-package-from-devices
Isolate machine	Depending on the severity of the attack and the sensitivity of the device, you might want to isolate the device from the network. This action can help prevent the attacker from controlling the compromised device and performing further activities such as data exfiltration and lateral movement.
Release machine from isolation	Releases a machine that has previously been isolated.
Restrict app execution	In addition to containing an attack by stopping malicious processes, you can also lock down a device and prevent subsequent attempts of potentially malicious programs from running.
Remove app restriction	Removes the restrict app execution policy for endpoints that have had this applied.

Action	Description
Run antivirus scan	As part of the investigation or response process, you can remotely initiate an antivirus scan to help identify and remediate malware that might be present on a compromised device.
Stop and quarantine file	The Stop and Quarantine File action includes stopping running processes, quarantining the files, and deleting persistent data such as registry keys.

Microsoft Entra ID

Action	Description
Disable User	This response action temporarily prevents a user from logging in. This action helps prevent compromised users from moving across the network, accessing sensitive data, or causing further harm.
Enable user	This response action re-enables the disabled user.
Force Change Password	This response action prompts the user to change their password the next time they sign in. This helps ensure the account cannot be used for further impersonation attempts.
Confirm User Compromised	This response action confirms the user is compromised and sets the targeted user's risk level to high. This action confirms the user as a true positive and identifies them as currently at risk until appropriate remediation steps are completed.
Dismiss User Risk	This response action dismisses the risk of the risky user and sets the targeted user's risk level to none. This action is used for benign true positives—situations where the detected risk is real but not malicious, like activity from a known penetration test.
Revoke all Users' Sessions	This response action revokes a user's active sessions.

SentinelOne

Action	Description
Get Applications	Get the installed applications for a specific Agent.
Fetch Logs	Get the Agent and Endpoint logs from the Agent. The Agent logs are encrypted and only Support can read them. The Endpoint logs, for operations on the computers, laptops, or servers that have the Agent installed, are readable. The Endpoint logs are available for Windows endpoints only and require Agent version 3.6 or later. After you run this command, download the fetched logs. You can download the logs from the Console GUI or collect them.
Isolate Machine	Use this command to isolate (quarantine) endpoints from the network.
Release Machine	Use this command to release an endpoint that has been previously isolated.
Run Full Disk Scan	Full Disk Scan finds dormant suspicious activity, threats, and compliance violations, that are then mitigated according to the policy. It scans the local file system. Full Disk Scan does not inspect drives that require user credentials (such as network drives) or external drives. Full Disk Scan does not work on hashes. It does not check each file against the blacklist. If the Static AI determines a file is suspicious, the Agent calculates its hash and sees if the hash is in the blacklist. If a file is executed, all aspects of the process are inspected, including hash-based analysis and

Action	Description
	blacklist checks. Full Disk Scan can run when the endpoint is offline, but when it is connected to the Management, it can use the most updated Cloud data to improve detection.
Abort Full Disk Scan	Stop a Full Disk Scan on the Agent.
Restart Machine	Use this command to restart endpoints.
Shutdown Machine	You can shut down endpoints remotely for performance, maintenance, or security.

Carbon Black EDR

Action	Description
General Information	Performs a POST request to the Specific Device Information API, returning a JSON object of information pertinent to the current state of the endpoint. Please see the below API link for an example response of what this data may contain. https://developer.carbonblack.com/reference/carbon-black-cloud/platform/latest/devices-api/
Isolate Machine	Use this command to isolate (quarantine) endpoints from the network.
Release Machine	Use this command to release an endpoint that has been previously isolated.
Run Scan	Initiate an initial, one-time inventory scan in the background to identify malware files that are pre-existing on the endpoints.

Sophos XDR

Action	Description
Scan Endpoint	Sends a request to the specified endpoint to perform a scan. Any detections will generate events within the Sophos console, and if configured within the SIEM, may generate further security events.
Get Isolation	Gets the current isolation status of the endpoint.
Isolate Machine	Use this command to isolate (quarantine) endpoints from the network.
Release Machine	After you run isolate machine on endpoints, analyse the issue, and mitigate threats. Use this command to reconnect to the network.
Get Tamper Protection	Get Tamper Protection settings for a specified endpoint.
Enable Tamper Protection	Enable Adaptive Attack Protection settings for an endpoint.
Disable Tamper Protection	Disable Adaptive Attack Protection settings for an endpoint.
Get Adaptive Attack Protection	Get Adaptive Attack Protection settings for an endpoint.
Enable Adaptive Attack Protection	Enable Adaptive Attack Protection settings for an endpoint.
Disable Adaptive Attack Protection	Disable Adaptive Attack Protection settings for an endpoint.

CrowdStrike Falcon

Action	Description
Restart the Host	This command will restart the host.
Shutdown the Host	This command will shutdown the host.
Collect Diagnostics Logs	This command will run the CrowdStrike Windows diagnostic tool. The tool will gather log files and information about the state of a Windows host and packages them into a zip file.
Get File from Host	This command will download the provided file from the remote host and upload it to the CrowdStrike cloud for analyst download. - Files retrieved with the get command are stored in the CrowdStrike cloud for 7 days. - Files can be downloaded multiple times by any users with the appropriate roles until they expire or are deleted. - Files are downloaded as 7-zip archives. Open them with the password infected. - The maximum file size for get is 4 GB on macOS or Windows, and 2 GB on Linux. - You can't get a directory. Run zip first to package the directory into a zipped file.
Kill a Process	This command will kill the provided process via its PID. You may need to run the ps (List Running Processes) command first to find the PID of the process you wish to kill. You can't kill processes that are used to run the Falcon sensor.
List Directory Contents	This command will list all files and directories in the provided path.
List Running Processes	This command will display host process information.
Query the Registry	This command will query a registry subkey or values. Run reg query with no parameters to see the list of available hives.
Sets Registry Keys and Values	This command will create a new registry key or update an existing key or value.
Dump the Compute or Kernel Memory	This command will generate and save a memory dump file of the compute or kernel memory on a host. When xmemdump is executed, it might take a long time to finish running (depending on RAM size).

FortiEDR

Action	Description
Isolate Machine	This command will isolate (quarantine) endpoints from the network.
Release Machine	This command will release an endpoint that has been previously isolated.
Get File	This command will securely collect a copy of a potentially harmful file from the endpoint for deeper forensic analysis or sandbox detonation.
Delete File	This command will remove a confirmed malicious or unwanted file from the endpoint to eliminate the threat and prevent re-execution.
Kill Process	This command will terminate a running process identified as malicious or suspicious to immediately stop harmful activity on the endpoint.