BARRACUDA XDR

DO AGENTS DISAPPEAR FROM THE CONSOLE IF THEY HAVE BEEN OFFLINE FOR A WHILE?

By default, agents that are inactive for 21 days are automatically decommissioned. If you'd like your agents to remain in the console longer, submit a request to the SOC.

WHAT DOES DECOMMISSION MEAN?

Decommissioning removes the agent from the Management Console. Decommissioning the agent does not uninstall the agent from endpoints and does not affect protection. If the agent communicates with the Management again, the Management recommissions it and returns it to the Management Console. When an agent is recommissioned, it gets the latest assets and policy from management and starts to report new threats and new Deep Visibility™ events.

For example, let's say you decommission the agent of an end-user who is on vacation. When the end user returns and turns on the computer, the agent communicates with Barracuda XDR Dashboard. Barracuda XDR Dashboard registers the agent and you see it on the Endpoint Devices page.

WHY DOES THE AGENT HAVE HIGH CPU USAGE RIGHT AFTER INSTALLATION?

Upon installation, when the agent connects to Barracuda XDR Dashboard successfully, it does a comprehensive full disk scan of the device. Decreased performance is common while the scan takes place. We recommend letting the agent run to detect dormant malicious items such as malware files and registry keys. You can stop the scan upon request, but we strongly recommend letting it finish. System performance returns to normal after the scan is completed.

WHY CAN'T I DELETE VSS SNAPSHOTS?

One of the telltale signs of ransomware is deleting shadow copies. Deleting VSS copies makes it much harder for an organization to restore from backup should an incident occur. A feature called VSS Protection actively prevents attempts to delete VSS snapshots or resize the VSS partition. This also helps prevent the deletion of shadow copies taken by the agent. To resize the VSS partition, you must disable VSS protection. If necessary, contact the SOC for more information on how to delete VSS snapshots.

HELP! SHADOW COPIES ARE TAKING UP A LOT OF DISK SPACE.

Contact the SOC for urgent inquiries. By default, the agent uses the existing VSS configuration on the device. In some cases, if the VSS is configured incorrectly, shadow copies can take up a large portion of disk space. With help from the SOC, you can resize shadow copies to take up less space on the disk.

WHY ARE SOME OF MY MACHINES NOT CONNECTING TO THE CONSOLE OR SHOWING UP IN THE BARRACUDA XDR DASHBOARD?

This issue can happen with Windows Server 2008 or Windows Server 2012/2012 R2 devices. Though rare, it can also occur on Windows 10/11 agents. To maintain the highest level of security, the SentinelOne Management Console requires updated TLS ciphers for agents to connect. If certain ciphers (such as TLS 1.2 or 1.3) are not enabled, the agent may not be able to communicate to the console and the agent appear offlines. Contact the SOC for best practices and the resolution.

WHY DO SOME AGENTS BECOME DISABLED?

Agents can be disabled if the device doesn't have the resources to support the agent's capabilities. In upcoming versions of the agent, there will be additional failovers and implementations to prevent the agent being disabled.

WHY AREN'T MY USB DEVICES OR HUBS WORKING ANYMORE?

By default, we block USB mass storage (Class 08) devices as they can be a vector of attack to organizations. This feature is called Device Control. While uncommon, Device Control can cause a rare issue with docking stations, so it is worth disabling in the troubleshooting process. You can disable USB Blocking via the Barracuda XDR Dashboard, but the SOC can also facilitate your request.

Barracuda Managed XDR™

Why is there a New Threat Mitigated alert for "xyz" file?

The agent looks at many factors when analyzing files, including vulnerabilities the file may have or the actions the file is taking. The agent uses a combination of static machine learning analysis and dynamic behavioral analysis to protect systems. Files are evaluated in real-time before they execute and as they execute. These detections can be mapped against MITRE threat indicators, which you may see in the ticket. If you need an in-depth explanation of detection, contact the SOC.

Is the agent compatible with other anti-virus solutions?

We strongly recommend against using multiple antivirus products, though we do understand that layered security is a very important practice. Running two Endpoint Protection applications on a single endpoint can cause issues with mitigating threats. Other AV solutions may perform intrusive tasks that may be flagged as malicious. We can place some solutions on the Allow List, but others, such as Crowdstrike, may require disabling some features of the agent, reducing protection. For more information, contact the SOC.

Can we migrate existing agents/policies into the Barracuda SentinelOne console?

Yes, you can migrate existing SentinelOne agents into the Barracuda XDR Dashboard. You will need access to the originating SentinelOne console. We can provide a Site Token for you to migrate your tenants into the new console. We also recommend exporting the existing exclusions and blocklist from the original console to ensure the transition is seamless. Contact the SOC if you need assistance with any steps.

Will the agent detect "xyz" threat?

We are confident in the agent's ability to detect malicious activity. However, for your peace of mind, we can test sample malware files, and ensure that specific pieces of malware are detected if needed. If there is a major security incident or concern in the cybersecurity world, we will actively make sure your devices are protected from the related threat.

HELP! I'VE INSTALLED THE SENTINELONE AGENT ON MY DOMAIN CONTROLLER AND NOW MY VEEAM BACKUPS ARE FAILING.

This is a known interaction caused by the SentinelOne agent's built-in Safe Boot Protection. On Domain Controllers only, part of the Veeam backup process is to modify the boot record (BCD) and the SentinelOne agent prevents this by default. Contact the SOC for further assistance.