Understand Update Events in Secure Endpoint for Group Deletions

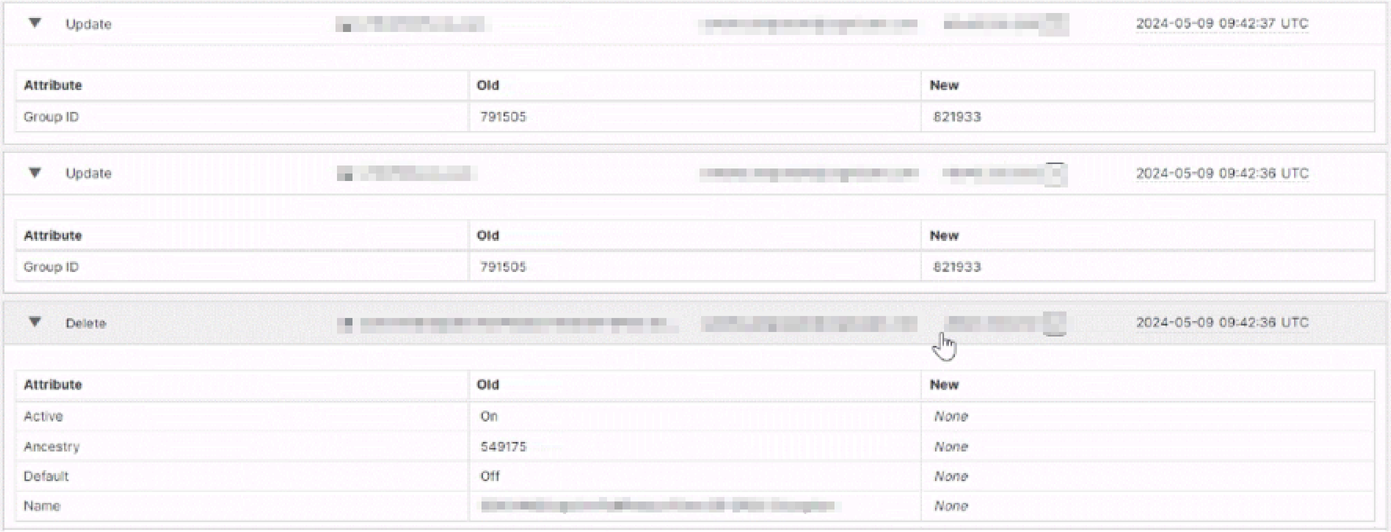
Contents

Introduction

This document describes how Secure Endpoint audit logs recorded both update and delete events when empty groups were deleted.

Problem

The update events in this image display a new group ID for machines or workstations, even though these workstations are not visible on the AMP console computer page. These update events are associated with the user email of the person who logged in to perform the deletion, which could lead to client confusion about what occurred. In some cases, 30-40 update events can be generated after deleting an empty group.



▼ Update [redacted] [redacted] [redacted] 2024-05-09 09:42:37 UTC

Attribute	Old	New
Group ID	791505	821933

▼ Update [redacted] [redacted] [redacted] 2024-05-09 09:42:36 UTC

Attribute	Old	New
Group ID	791505	821933

▼ Delete [redacted] [redacted] [redacted] 2024-05-09 09:42:36 UTC

Attribute	Old	New
Active	On	*None*
Ancestry	549175	*None*
Default	Off	*None*
Name	[redacted]	*None*

Solution

This is an expected behavior. The machine or computer hostnames seen in the audit log update events during the deletion of empty groups belong to devices that were once part of those groups but are now inactive. These machines were automatically removed from the console after 90 days of inactivity, but they remained part of the group in the backend.

When the group is deleted, these inactive machines are moved to the default group, which triggers the update events. Unfortunately, since these computers are inactive, they do not appear in the console, which is why they cannot be found when searching under computers.

To obtain a complete list of inactive machines that are still assigned to a group, you need to reach out to the TAC, as this information cannot be retrieved via the Secure Endpoint portal.