

Secure Access Activity Search Displays UNKNOWN Rule Names

Contents

Issue

During an Umbrella to SSE migration, Secure Access Activity Search events display Rule Name as **UNKNOWN** instead of showing named policy rules. This behavior was observed for various traffic types, including allowed traffic such as requests to chatgpt.com. The concern was whether these **UNKNOWN** rule name entries indicated a policy configuration issue or migration problem that required remediation.

Environment

- Cisco Secure Access (SSE)
- Organization undergoing Umbrella to SSE migration
- Secure Access Activity Search reporting
- Traffic categorized as Newly Seen Domains

Resolution

The Rule Name **UNKNOWN** behavior is expected and normal for events handled by Secure Access system logic rather than customer-created/named rules. This commonly occurs for traffic categorized as Newly Seen Domains, where the domain was newly seen at query time and is reported as such in Activity Search or Security Activity reports.

Interpreting Activity Search Events with UNKNOWN Rule Names

When encountering events with Rule Name **UNKNOWN**, review these event fields to determine the enforcement reason and confirm proper policy application:

- **Action** - Shows whether traffic was allowed or blocked
- **Event Block Reason / Block Reason** - Provides specific enforcement details
- **Categories** - Shows content categorization (such as **Newly Seen Domains**)
- **Destination domain/IP** - Target of the request
- **User/source identity** - Source of the traffic
- **Timestamp** - When the event occurred

If the **Categories** field shows **Newly Seen Domains**, then **UNKNOWN** in the rule-name field is expected behavior and does not indicate a failed migration or policy corruption.

Validation Steps for Unexpected Behavior

If traffic was expected to match a specific named rule but shows **UNKNOWN**, collect this information for policy path validation:

- 2-3 sample event timestamps
- Destination domain/IP for each event
- User/source identity for each event

This information can be used to compare the expected policy path against the actual event behavior and determine if further investigation is required.

Cause

The **UNKNOWN** rule name appears when Secure Access system logic processes traffic rather than applying a customer-created/named policy rule. This is documented behavior for certain traffic categories, particularly Newly Seen Domains, where the built-in categorization and handling mechanisms take precedence over named rules during the initial domain assessment.

Related Content

- [Enable Newly Seen Domains Security](#)

- [Cisco Technical Support & Downloads](#)