Event rules

Event rules let you automate reactions to supported device events. Open **Dashboard → Event rules** to create rules that watch enrollment, disenrollment, non-compliance, and geofence events (Android and Apple devices; geofence events come from Android devices, iPhones and iPads), then trigger one or more actions automatically.

What an event rule can do

Each rule combines a **subject**, an **event**, and one or two **actions**. Supported subjects are **All devices**, **Specific device**, and **Policy**.

- **Events**: device enrolled, device disenrolled, device becomes non-compliant, geofence enter, geofence exit.
- **Device actions**: disable device, enable device, lock device.
- **Email action**: send a notification email to administrators and, when enabled, delegated managers.

> A rule can contain an email action only, a device action only, or one device action plus one email action. If both actions are configured, Cerberus Enterprise executes the device action first and the email action second.

Platform and compatibility rules

The available events and actions depend on the selected subject and on the platform that applies to that subject.

- **Android** supports enrollment, disenrollment, non-compliance, and geofence events.
- **Apple** supports enrollment, disenrollment, non-compliance, and geofence events. Geofence events come from iPhones and iPads with the Cerberus Enterprise app.
- **Disable device** is available on both Android and Apple. On supervised iPhones and iPads it turns on lost mode; other Apple devices are locked instead (a Mac with a six-digit PIN, shown in the command history of the device). Lost mode is turned off from the device page.
- **Enable device** is only offered for geofence events, on Android and Apple. On iPhones and iPads it turns off lost mode.

- **Disable device** and **Enable device** leave out an Android device in lost mode: only the **Disable lost mode** command takes it out of lost mode. The other actions of the rule still run, and the system log says why the device action was left out.
- **Lock device** and **Send email** are available on both Android and Apple, when the selected event supports them. A Mac is locked with a six-digit PIN, shown in the command history of the device.
- **Device disenrolled** supports email only.

Rules list

The Event rules list is the main management page for this feature. It includes a searchable table with rule name, subject, event, actions, platform, enabled state, and update time.

- Use the filter chips to switch between all rules, enabled rules, disabled rules, and text search.
- Use the **Refresh** button to reload the current table view.
- Use the enable switch in each row to temporarily enable or disable a rule.
- Use the multi-row selection mode to delete several rules together.
- Use **Create event rule** to open the editor for a new rule.

Rule editor

The editor is divided into **General**, **Scope**, **Trigger**, and **Actions** sections. At the bottom of the page, a sticky action bar keeps the main buttons visible while you scroll.

General

- **Name**: required, up to 150 characters.
- **Description**: optional, up to 2000 characters.
- **Rule enabled**: saves the rule in enabled or disabled state.

Scope

The scope defines which devices the rule can match. The editor also shows the resolved platform and, when available, the effective policy context.

- **All devices**: the rule can match all supported devices in the enterprise.
- **Specific device**: select one managed device from the picker dialog.
- **Policy**: select one policy template from the picker dialog.

Trigger

The trigger section filters available events automatically based on the selected scope and platform.

Geofence triggers

Geofence enter and exit rules work for Android devices, iPhones and iPads, and a rule for a device or a policy requires a valid policy context. For the geofence definitions, see **Location and geofences** (Android) and **Location and geofences** (Apple).

- If the subject is **All devices**, the rule always applies to **Any geofence**.
- If the subject is a device or policy, you can choose **Any geofence** or one **Specific geofence**.
- The specific geofence list is loaded from the effective policy context of the selected device or policy.
- All-devices geofence rules saved before geofences were available on iPhone and iPad still apply only to Android devices. Open and save them again to apply them to Apple devices too.

Actions

The actions section lets you choose an optional device action and an optional email notification. The UI hides unsupported combinations automatically. The email notification is on by default, also when you choose a device action: turn it off if you only want the device action.

- If no device action is available for the selected event and scope, you can still save an email-only rule.
- If email is disabled for the selected event and platform, the email toggle is unavailable.
- A rule without any action is invalid and cannot be saved.

Email recipients

Email actions always include enterprise users with the **ADMIN** role. If the enterprise is managed through multi-tenancy, you can expand recipients to include MT managers.

- **Main managers only**: includes enterprise admins and the main MT manager contacts.
- **Main managers and sub-account managers**: adds assigned sub-account managers too.
- The preview list shows the actual email addresses that will be used when the rule runs.

- Only delegated managers with granted access to the enterprise are included in the final recipient list.

Execution behavior

Event rules run immediately when Cerberus Enterprise receives a supported event from the backend integrations. Disabled rules are skipped automatically.

Successful, skipped and failed executions are recorded in the system log with human-readable messages, including the reason when a rule or a device action was skipped.

> The system log keeps device status and location events, and successful or skipped rule executions, for **90 days**. The other events, such as administrator actions, sign-ins, warnings and errors (including failed rule executions), are kept for **12 months**. Older entries are deleted automatically every night.

Revision #23
Created 2026-06-11 16:16:36 UTC by Admin
Updated 2026-11-12 09:51:51 UTC by Admin