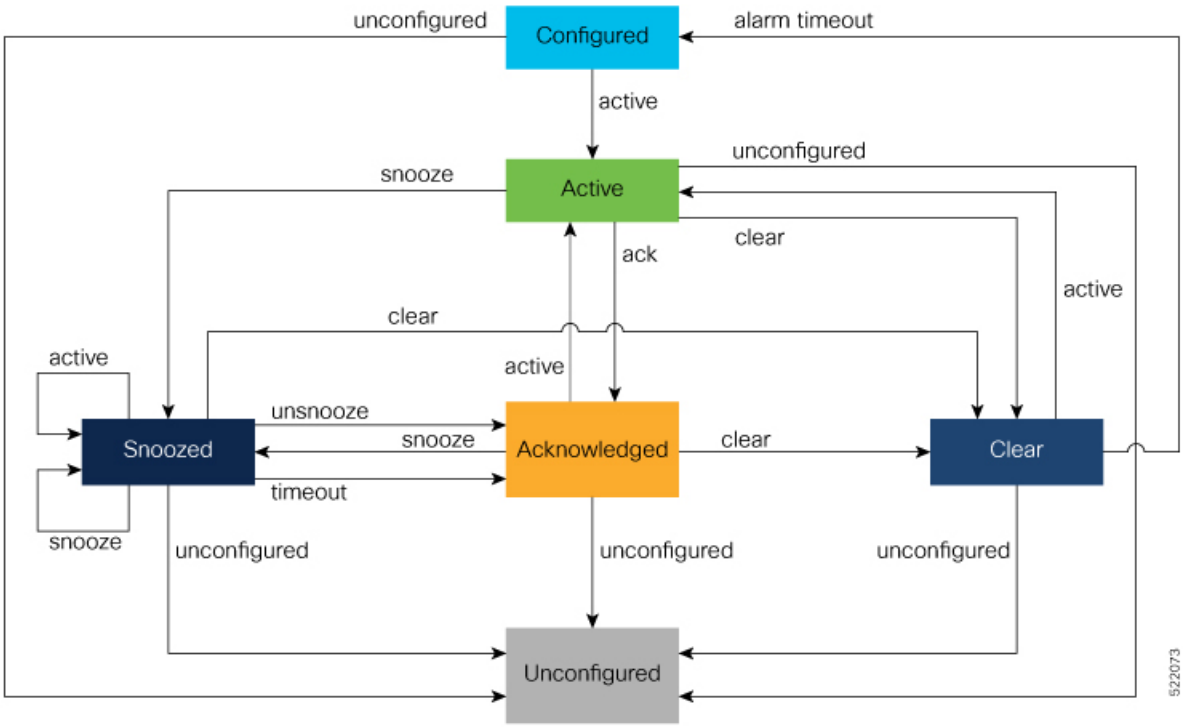
Alarm Lifecycle

Crosswork Cloud creates an alarm instance for each rule in a fully configured alarm policy. A fully configured alarm policy has one or more rules and depending on the alarm policy type, has one or more prefixes, ASNs, or peers associated with it.

Each alarm instance has a lifecycle, transitioning between various states after it is created. The following diagram shows what transitions can occur from each state. For more information, see Alarm States, on page 2.

Note Each alarm instance starts its lifecycle in a **Configured** state.

Figure 1: Alarm Lifecycle



- Alarm States, on page 2

Alarm States

An alarm instance transitions between the states in response to events or in response to a user action.

The following table describes the possible alarm states.

Table 1: Alarm State Descriptions

Alarm Status	Description
Configured	Initial state of an alarm.
Active	The state when an alarm is triggered with an active event.
Acknowledged	In this state, a user has indicated the alarm is recognized and acknowledged. An alarm that is in **Active** or **Snoozed** state can be marked as acknowledged. **Note** • An alarm in the **Acknowledged** state will not show up in the list of active alarms. • An alarm in the **Acknowledged** state will transition back to **Active** state, if there is another active alert.
Clear	The alarm is no longer active. The **Clear** state is an ephemeral state. The alarm instance transitions to a configured state after a 30 second hold time.
Snoozed	An alarm that is in **Active** or **Acknowledged** state can be marked as **Snoozed** by the user for a specified time period. During this period, the alarm shows up in the active alarms list. However, if the alarm condition clears, then a notification will be sent to the notification endpoint (if one was configured).
Active (Snoozed)	The alarm has been **Snoozed**, but the conditions that would trigger the alarm to be **Active** are present.
Cleared (Snoozed)	The alarm has been **Snoozed** and the conditions that would trigger the alarm are no longer present.
Unconfigured	An alarm transitions to an **Unconfigured** state and is eventually deleted when the user deletes the alarm policy, or the rule corresponding to the alarm instance. The **Unconfigured** state is an ephemeral state, and the alarm instance is deleted after a 30 second hold time.

Note

- An alarm instance can transition to an **Active** or **Clear** state, only in response to an event received from the alarm detection layer.

Alarm Notifications

When a policy rule is violated, you can configure an alarm notification to be sent to one or more endpoints (see Configure Notification Endpoints). The notification contains information about the alarm state and alarm event data.

Notifications are sent if one of the following alarm state changes occur:

- From Active to Clear
- From Configured to Active
- From Acknowledged to Clear
- From Snoozed to Clear

A notification will not be generated if an alarm becomes active again *and* is already in one of the following states:

- Active
- Snoozed
- Acknowledged

Related Links

- About Notification Endpoints

Crosswork Network Insights Alarm Types

Alarms are categorized into three types:

Type	Description
ASN	Autonomous System Number (ASN) type alarms monitor the state of a configured BGP Autonomous System (AS). These alarms are generally used to detect unexpected prefixes coming from your ASN and alert you if an expected condition is violated. For example, an alarm becomes active if Crosswork Cloud Network Insights detects a new prefix that was not previously observed and should not be originating from a configured ASN.
PEER	Peer type alarms monitor the state of a configured Peer and its Routing Information Base (RIB). These alarms are used when you have configured peer monitoring. For example, an alarm becomes active if Crosswork Cloud Network Insights detects a number of prefixes in RIB that is outside the configured parameters.
PREFIX	Prefix type alarms monitor the state of a configured prefix and a number of its BGP attributes, such as the Origin ASN of the prefix or the length of the AS path attribute. It is the most common alarm type and is designed to detect unknown events on prefixes that are being monitored. A set of prefix type alarms also monitor the ROA status (VALID, INVALID or ABOUT-TO-EXPIRE) of the configured prefix.

Alarm Thresholds

Alarm thresholds are used to control the sensitivity of alarms. Consider configuring alarm thresholds if some alarms are often being triggered by small numbers of observed changes and are considered "false alarms".

An alarm is triggered (Active) when Crosswork Cloud Network Insights detects a violation against a set of conditions related to a monitored AS, peer, or prefix. The alarm clears when all conditions are no longer violated. Since data is collected from many BGP Peers, Crosswork Cloud Network Insights has access to multiple views of the state of a prefix or AS. These views are not always identical, and the frequent state changes in a small number of peers (such as those caused by router flap) can produce a lot of alarm noise. Thresholds can act as a noise dampening mechanism.

The following Peer Count thresholds can be configured for certain alarm rules to dampen alarm noise:

Peers to Trigger—The minimum number of violation peers required to report a condition violation that would cause the alarm to become Active. For example: A **Peers to Trigger** threshold has been set to 1 for the Prefix Withdrawal alarm. The number of peers reporting that a prefix has been withdrawn has to exceed 1 before External Routing Analysis issues an Active prefix withdrawal alarm.

Peers to Resolve—After an alarm has been activated, it remains Active. The alarm is triggered again with every new condition violation until the violation peer count is less than or equal to the **Peers to Resolve** threshold (for example, this can occur due to the withdrawal of violating advertisements or an increase to the Peers to Resolve threshold). The alarm then goes into Clear state.

Note The **Peers to Resolve** threshold must be less than the **Peers to Trigger** threshold.

Figure 2: Example: Expected AS Path Alarm Rule Threshold Options