

# Valid AS Path Violation


- Valid AS Path Violation, on page 1


# Valid AS Path Violation

This alarm detects when a prefix advertisement AS path does not match a specified ASN pattern.

Crosswork Network Insights compares the configured **Valid AS Path Pattern** with the advertised AS path of a prefix. The ASN pattern is the expected sequence of AS numbers in order, separated by spaces, and ends with the origin AS such as 107 3462 109. You can use operators to express complex patterns. If the patterns do not match, Crosswork Network Insights triggers the alarm to be active.

**Note** It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights policies.

**Example pattern: [0-]* 806 * 200**

- Valid AS path: 1900 1731 806 100 200
- Violating AS path: 1900 1731 807 100 200
- Violating AS path: 1900 1731 806 150 100 200

### Possible Problem Detected

This alarm detects unexpected BGP AS-path changes indicating potential MITM attacks or latency degradation.

### Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > Valid AS Path Violation**):

- Valid AS path pattern (Click **Edit**)

- Thresholds