

Gateway Connectivity

• Gateway Connectivity, on page 1

Gateway Connectivity

After a Crosswork Data Gateway is installed for Crosswork Cloud Traffic Analysis or Crosswork Cloud Trust Insights, a policy is automatically created to monitor the connection between Crosswork Data Gateway and Crosswork Cloud. If the Crosswork Data Gateway loses connection to Crosswork Cloud (fails to communicate with Crosswork Cloud within its reporting interval), an alarm is generated and displayed in the Alarms page (or > **Monitor** > **Alarms**).

To view gateway connectivity details or to update the alarm severity level, list of monitored gateways, or notification endpoints, do the following:

Procedure

Step 1 Navigate to or > **Configure** > **Policies.**

Under **Gateway Connectivity**, you can view the number of active alarms, the number of gateways monitored, and the gateway that has the most recent active alarm.

Step 2 Under **Gateway Connectivity**, click **Details**.

Step 3 By default, the **Overview** tab displays the current gateway connectivity policy configuration.

Step 4 To view Alarm details, click the **Alarms** tab. From this page, you can click the **Lost Gateway Connection** alarm for further details about a particular alarm or navigate between the Active, Acknowledge, or History tabs.

Step 5 To modify the alarm severity, list of monitored gateways, or configure endpoint notifications, click **Edit**.

a) Under **Triggers** > **Gateway Rules** > **Severity** drop-down menu, select the severity level.

b) Under **Data**, click **Modify** to update which gateways you want to monitor or ignore.

c) Under **Actions**, you can either modify existing endpoint notifications or add more. For more information on the types of endpoint notifications you can configure, see About Notification Endpoints.

d) Click **Save**.

Gateway Connectivity