Juniper Contrail Service Orchestration Privacy Policy Supplement

This notice is provided as a supplement to the Juniper Privacy Policy. In order to understand the personal information processing practices relevant for a particular Juniper Product, you should read both the Juniper Privacy Policy and any applicable Juniper Product supplement. Any terms not defined in this Supplement are defined in the Juniper Privacy Policy. In the event of a conflict between the terms of this Supplement and the Juniper Privacy Policy, this Supplement shall control to the extent of the conflict.

This Juniper Contrail Service Orchestration Privacy Policy Supplement describes our practices with respect to how personal information is processed by Juniper in connection with the provision of the Juniper Contrail Service Orchestration (CSO) service. For information on CSO, please visit our CSO Website.

Personal Information Processed

As part of the onboarding of new customers to CSO, CSO requires customer username (first name, last name, and email address). Additional information that may be collected includes site name and metadata from managed devices such as IP address of source and destination and application or websites accessed.

Purposes of Processing Personal Information

CSO includes a web-based management interface to visualize and automate the provisioning and management of devices running within the SD-WAN environment. CSO analyzes logs generated by SD-WAN network devices to provide powerful analytics regarding websites and applications used on an SD-WAN. CSO does not analyze traffic data transmitted through an SD-WAN. It only analyzes network device logs configured by the customer and sent to CSO.

Retention of Personal Information

CSO retains logs, such as access, incident, and device logs, for one to 30 days, or in select cases, based on the duration of a customer's tenancy. These logs are available to customers via API or the CSO platform. Customers may earlier purge some of these logs.

Security of Personal Information

All device communication between CSO and the customer's device is via secure protocols (SSH, SSL, TLS) and authenticated. The information we collect, including device configurations, is hosted on services which have certified security technologies and procedures in place to ensure integrity and security of customer data (e.g., data separation, physical security, encryption of data in transit and rest and role-based access control).

Limited Juniper Access to Data

CSO is designed to give customers options for whether Juniper may access the customer's CSO data for support or trouble-shooting purposes.

Changes to this Supplement

We may update this Supplement from time to time to reflect any changes in our CSO personal information processing practices.

Other

Your use of CSO is subject to the Juniper End User License Agreement (and, if relevant, the related Software Specific License Addendum) and Terms of Use, or to the extent applicable, as otherwise agreed by the parties in writing.

9010076-002-EN