

CLOUD SERVICE DESCRIPTION – CONTRAIL SERVICE ORCHESTRATION

Contents

Introduction.....	2
Cloud Service Description	2
Data Protection and Security.....	2
Data Ownership.....	3
Data Location	3
Data Retention.....	3
Encryption of Data.....	4
Access Controls	4
Security Incident Response Team (SIRT)	4
Cloud Environment and Security	4
Security Testing	5
SLA/Performance Measures and Reporting	5
Cloud Service Resiliency	5
Availability	5
Support Services Eligibility	6
Support Services Features and Deliverables	6
JTAC Access	6
On-Line Support.....	6
Support APIs	7
Case APIs	7
End User Responsibilities	8
Compliance with Laws; Export Requirements.....	8
Availability	9
Scope	9
Exclusions	9
About Juniper Networks.....	10

Introduction

This Cloud Service Description (the “CSD”) describes Juniper’s Contrail Services Orchestration hosted in the cloud, (the “Cloud Service”), as well as the Juniper Care Services offering (“Support Services”) that Juniper Networks makes available as a part of the Cloud Service Subscription for end users of Juniper Networks products (“End User”) directly or through its authorized resellers. Your Subscription to the Cloud Service is governed by this Cloud Service Description and the Juniper Master Purchase and License Agreement posted at <https://support.juniper.net/support/eula/> (or another written master services agreement signed by Juniper Networks and the End User and covering within its scope, the terms and conditions under which Juniper Networks will render support and maintenance services) (the “Master Agreement”). Capitalized terms used in this CSD not otherwise defined herein have the meaning given to them in the Master Agreement.

The Support Services are subject to the terms of this CSD and the Master Agreement.

If applicable to the Cloud Service, all license terms for Software provided by Juniper Networks as part of the Cloud Services are subject to the Master Agreement.

The Terms of Service for Support API provided by Juniper Networks as part of the Services are subject to the Juniper Networks Support API Terms of Service, a copy of which is posted at <https://support.juniper.net/support/legal/supportapitos/> (the “TOS”).

In the event of any conflict between the terms of this CSD and those of the Master Agreement or TOS, the terms of the Master Agreement and TOS shall take precedence.

Cloud Service Description

This Cloud Service designs, secures, automates, and runs the entire service life cycle across SRX Series next-generation firewalls and NFX Series Network Services Platforms. It integrates and federates with Mist Cloud for seamless Wi-Fi management. It is also a service orchestrator for the vSRX Virtual Firewall, available in public cloud marketplaces. The Cloud Service overview, including links to its specifications and technical documentation can be found at <https://www.juniper.net/uk/en/products-services/sdn/contrail/contrail-service-orchestration/>. For purposes of clarity, all referenced Juniper Hardware or Software must be purchased and/or licensed separately.

Data Protection and Security

In this CSD, “End User Data” shall mean all information submitted by End User to Juniper and may include third party data that End User submits to Juniper. “Processed Data” shall mean information about End User’s devices or systems in connection with End User’s usage of Juniper’s products and services, as well as any network management information or configuration data from the use of End User’s Processed Data.

Juniper shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of End User Data.

In accordance with the End User's use of the Cloud Service, the categories of data that may be processed are as set forth in the Juniper Privacy Notice available at <https://www.juniper.net/us/en/privacy-policy/> together with any Supplemental Privacy Information referenced therein which includes Juniper Networks' collection and use of network device logs configured by the End User such as the metadata from managed devices including IP address of source and destination and application or websites accessed. To the extent End User Data includes Personal Data, as defined in the DPA located at <https://www.juniper.net/us/en/privacy-policy/customer-dpa/>, the terms of the DPA are hereby incorporated by reference and shall apply. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by Juniper, the Standard Contractual Clauses shall apply, as further set forth in the DPA. For the purposes of the Standard Contractual Clauses, Company and Company's applicable Affiliates are each the data exporter, and Company's acceptance of this Agreement, and an applicable Company Affiliate's execution of an order form for Juniper Products or Services, shall be treated as its execution of the Standard Contractual Clauses and Appendices.

Data Ownership

End User retains ownership of End User Data. In connection with End User's use of the Cloud Service, Juniper collects and uses Processed Data in accordance with the Juniper Privacy Policy. Juniper uses Processed Data to enable, optimize and provide the Cloud Services and support to End User and to improve Juniper's Cloud Services in general, including but not limited to, integrating such Processed Data on an anonymized basis into our Cloud Services. By using the Cloud Service, End User agrees to allow Juniper to use suggestions and collect End User Data to generate Processed Data as defined in this CSD.

Data Location

The Cloud Service's public cloud instance is hosted in top-tier AWS data centers in the United States. Juniper personnel who are granted access to network management data or a Cloud Service instance may be located in regions outside of the EU where data privacy and data protections laws may differ. Nonetheless, Juniper has established standard information security policies and practices that apply globally to all Juniper locations.

Data Retention

Logs, including access, network management data, incidents, and devices, are captured at a centralized location in AWS and retained for one to 30 days or, in select cases, based on the duration of the customer's tenancy, and are available to customers via API or the CSO platform. End Users may purge some of the network management earlier.

Encryption of Data

Industry standard encryption is utilized for the Cloud Service web interface, data communications across network devices, data at rest and passwords.

- Communication between customers and the Cloud Service web interface use HTTPS connections.
- Access to the SD-WAN network device console is protected using SSH cryptographic network protocol.
- Data traveling from SD-WAN network devices to the Cloud Service is encrypted with AES-256 through secured IPsec tunnels.
- Data at rest, including passwords, is protected by whole-disk encryption with AES-256.

Access Controls

The Cloud Service access authentication can be configured for single sign-on (SSO) and authenticated using customer authentication controls (such as through Active Directory, LDAP, and Okta).

Juniper provides the following access controls and restrictions to End Users and follows its own access procedures:

- (i) End User access restrictions and controls:
 - End User access to the Cloud Service is based on the role assigned by the End User.
 - End Users can leverage predefined roles or define customized roles.
- (ii) The Cloud Service access restrictions and controls:
 - The Cloud Service access to End User network management data is restricted based on role or customer-granted permission and is based on the principle of least privilege.
 - Access is logged.
 - There is no Cloud Service access to network traffic data.

Security Incident Response Team (SIRT)

Juniper's SIRT is accountable for security vulnerabilities related to Cloud Services. SIRT manages vulnerability reports from and acts as support for security incidents. SIRT works with the Operational Security Community, other CSIRT Teams, customers, and other media to maintain situational awareness of threats. This information is processed and communicated to the larger SIRT Team, our peers in the company, and our customers. To Report a Potential Security Vulnerability, refer to: www.juniper.net/us/en/security/report-vulnerability/.

Cloud Environment and Security

Servers are hosted in an ISO 27001-certified data center, which also provides SOC 2 attestation reports over its security controls and across multiple availability zones.

All servers run Linux OS and are hardened per best practices. Servers are hosted at AWS with security groups. Only the required ports are opened on front-end servers.

The Cloud Service is developed and maintained following Juniper's Secure Development Life-Cycle practices.

Security Testing

Juniper performs Web security testing from development through production. Juniper periodically scans for SQL injections, cross-site-scripting (XSS), and more than 700 other vulnerabilities, including the OWASP Top 10.

SLA/Performance Measures and Reporting

Cloud Service Resiliency

By leveraging the public cloud, the infrastructure components and services of the Cloud Service are deployed redundantly (across AWS clusters and zones) in an effort to provide 24 x 7 availability. In addition, the Cloud Service is divided into microservices so issues with one microservice do not directly affect other microservices. The Cloud Service buffers data in the event of a component disaster, such as the loss of backend microservice. Once the disaster has been addressed, the data is replayed to fill in the lost analytics. System upgrades and feature introductions also benefit from microservices to avoid impact to the Cloud Service when performing either. This reduces the need for planned downtime, however, the Cloud Service has a scheduled downtime during release upgrade, and End Users are notified 48 hrs. in advance of any such downtime. Minor updates/patches can be performed without a downtime.

Availability

Juniper Networks will use commercially reasonable efforts to make the Cloud Services fully available and operable over the internet in full conformity with the Cloud Service specifications for access and use by End Users, as measured over the course of each calendar month, an average of 99.9% of the time, calculated as follows:

$$\left[\left(\frac{\text{total} - \text{nonexcluded} - \text{excluded}}{\text{total} - \text{excluded}} \right) * 100 \right] \geq \text{Available \%}$$

Where:

“total” means the total number of minutes in the calendar month;

“nonexcluded” means downtime that is not excluded; and

“excluded” means any planned downtime of which Juniper gives three business days or more written notice via email or banner on the Cloud Service dashboard. All scheduled maintenance work and planned downtime will be during the hours from 7:00 p.m. PST to

7:00 a.m. PST on any day. Planned downtime is not expected to occur more than once or twice per year and is not expected to exceed 120 minutes in any given month.

Support Services Eligibility

A Subscription to a Cloud Service (as defined in the Master Agreement) purchased by the End User shall be treated as a Juniper Care Software Advantage Support Services contract (the “Support Service”) for purposes of this CSD. The Support Service is available only to qualified End Users who have purchased the Subscription for their own end use. The Cloud Service will be supported only for the duration of the Subscription Term. In addition, if a Juniper Networks device is managed by the Cloud Service, then the Juniper Networks device must be under an active support contract.

Support Services Features and Deliverables

Juniper Networks will use commercially reasonable efforts to provide the End User with the Support Services. The Support Services may include access to Juniper Networks technical support engineers, software releases, and online tools.

JTAC Access

With Juniper Networks Technical Assistance Center (JTAC) support, the End User will have unlimited access to JTAC engineers by phone and online 24/7/365. JTAC engineers will help diagnose system problems, configure, troubleshoot, and provide work-around solutions where necessary. Automatic escalation alerts to senior management are triggered on all priority issues.

For details on the JTAC support center structure, how to access JTAC support, JTAC response time guidelines, problem reporting and escalation procedures, case workflow, and customer communication guidelines, please refer to the JTAC User Guide at www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.

On-Line Support

During the term of the Juniper Networks Service Contract, Juniper Networks provides the End User with self-service access to the Juniper Networks Customer Service Center (CSC) online portal, which provides information, answers, tools, and service options for the End User’s use in supporting the Cloud Service. Offerings include, but are not limited to:

Online case management: create new cases, check the status of existing cases, update cases with new information, and search by case numbers, RMA numbers, and the End User’s own internal case reference numbers.

Juniper Knowledge Center: ability to search thousands of articles, including configuration assistance, known issues, interoperability, and compatibility information.

Problem Report (PR) Search: ability to access the most complete and up-to-date information about known Juniper Networks operating system defects. This tool allows you to search for defects by PR number, Junos OS release version and keyword, providing upgrade analysis and impact information.

The End User can also subscribe to PRs of interest in order to receive automated updates as specific PRs change.

Online Tools: various tools to help analyze hardware and software information such as configuration tool, translator, migration tool, etc.

Technical Bulletins: timely notification on new features release, end of life, known product issues, etc.

Security Advisories: provide known security vulnerability issues to help avoid network impact. Use of online tools is subject to the following:

The End Users shall have personal, non-transferrable, non-sublicensable, nonexclusive access during the term of the Support Services to Juniper Networks' online Customer Support Center (CSC), subject to limited use terms posted at such site, all solely for the End User's internal use in support of Juniper Networks product covered under Juniper Networks Service Contract.

The End User shall maintain an active subscription contract to access resources on CSC related to the Cloud Service. The End Users are not entitled to access CSC resources for any products that are not covered by an active Juniper Networks support contract.

Juniper Networks reserves the right in its discretion to limit or prohibit access by any End User if Juniper Networks believes that such access may give rise to violation of export control laws or regulations or any other violation of Juniper Networks' rules or the limited use terms identified above.

Support APIs

As part of the Support Services, Juniper Networks grants to the End User access to, and usage of, Support APIs. The Support APIs provide a mechanism for Business-to-Business integration of the End Users Customer Relationship Management (CRM) systems and Juniper Networks through a well-defined secure set of APIs.

The license granted herein as part of the Support Services is subject to all terms of the TOS.

Case APIs

The Juniper Support Case APIs enable an End User to integrate their Support CRM system with Junipers Support CRM system in a programmatic way.

An equivalent record (Case) is first created on the client system and via this API channel a Case is requested to be created on Juniper's Support System. The lifecycle of the Service Request is then managed via this API channel.

The Case APIs are subject to an onboarding process as specified in the Case API Onboarding Guide: https://eng.juniper.net/site/global/build/support_automation/support_api/case_api/v10/onboarding/index.gsp

End User Responsibilities

For any Problem identified as a Priority 1 Problem, the End User will provide Juniper Networks or its authorized service representative access to the affected network environment and will assign a technical contact for Juniper Networks. Furthermore, if Juniper Networks determines that its technical personnel need access to the End User's network in order to remotely diagnose a problem, the End User will ensure that Juniper Networks' personnel have the necessary level of authorized access to such network. The End User shall have the right to observe such access.

The End User shall maintain a reasonable number of support engineers who are trained on Juniper Networks Products.

The End User's support engineers must be proficient in the operation of the Products and be able to perform basic Hardware and Software configuration and troubleshooting. All communication to Juniper Networks' engineers of customer issues and responses will be conducted in English.

The End User shall inform Juniper Networks about the role changes or resignation of its support engineers so that their individual CSC accounts can be modified/deactivated as needed.

The End User shall provide access to servers, equipment, information, logs, infrastructure, and resources that are necessary for the delivery of the Service.

The End User shall advise Juniper Networks of any Information Juniper Networks may reasonably request about the execution of the Services throughout the delivery of Services. If third-party participation and cooperation is required in order for the End User to perform the End User responsibilities, the End User shall be responsible for getting such participation and cooperation.

The End User shall provide written notice to Juniper Networks as soon as it becomes clear or there is reason to believe that the End User will not meet any of the End User responsibilities.

In order to leverage the Support Case API, the End User will need to fully understand and develop against the Support Case API as defined by the Support Case API definition and documentation: https://eng.juniper.net/site/global/build/support_automation/support_api/case_api/index.gsp.

Compliance with Laws; Export Requirements

The End User shall comply with all applicable laws and regulations and with all terms of the Export Note incorporated in the Shipment Terms posted at []. The End User warrants that it has no knowledge or reason to believe that it has received any Juniper product through any export or re-export in violation of US or other applicable laws or regulations, that it is not a Sanctioned Party (as that term is defined in the Export Note), that no Juniper product or Cloud Service is located in or controlled from a site in a Group E country (Cuba, Iran, North Korea, Syria, or in the region of Crimea), and that it is not using any product or Cloud Service to support activities in support of development, manufacture or use of nuclear fuel or weapons, missiles, or chemical or biological weapons or other Prohibited Uses as that term is defined in the Export Note. The End User further covenants that it will immediately notify Juniper Networks if at any time such warranties and representation become no

longer accurate at such time. Regardless of any disclosure made by the End User to Juniper Networks of an ultimate destination of the Products. The End User will not export, either directly or indirectly, any Juniper products or Cloud Service without first obtaining any and all necessary approvals from the competent government authorities administering U.S. and other applicable country export controls. The End User understands and agrees that certain restrictions on services described herein may be imposed by Juniper Networks in order to avoid violations of export control laws.

Availability

These Support Services are available where they can lawfully be sold and subject to applicable limitations posted by Juniper Global Support Operations on the Juniper website or the Juniper price list; Support Services are available with a Subscription for a minimum fixed duration of 12 months.

Scope

Support Services shall be delivered remotely from an authorized Juniper Networks location unless specified otherwise.

All service deliverables in this offering are available in English only unless otherwise specified by Juniper Networks.

Juniper Networks' obligation to perform any particular Support Services hereunder is contingent upon Juniper Networks receiving from the End User such cooperation, network access, consents, information, and materials that Juniper Networks may reasonably request to enable Juniper Networks' proper and efficient performance of such Support Services and to enable Juniper Networks to do so in compliance with all applicable laws and regulations.

Exclusions

Juniper Networks is not obligated to provide Support Services for any of the following:

Third-party devices (hardware, software cabling, etc.) not provided by Juniper Networks or Problems associated with or arising directly or indirectly from such components;

Problems with a Cloud Service that have been modified without Juniper Networks' written consent by any person (including unauthorized modifications by Support Services Specialist);

Problems relating to incompatibility of the Cloud Service with third-party devices;

Problems caused by the use of the Cloud Service other than in accordance with applicable Documentation;

Problems with the Cloud Service where Customer did not provide the required information; Problems caused by the misuse of the Cloud Service generally;

Problems with Software used in connection with a Cloud Service that is not a Supported Release;

Problems with a cloud managed hardware device that is not compatible, nor under a supported release of the Cloud Service.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

Copyright 2021 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.