Service Description: Advanced Services: Cisco Managed Subscription Service for OpenStack

Service Description: This document describes Cisco's Managed Subscription Service for OpenStack Foundation's OpenStack® on-premises cloud.

Contents

1 General Terms

Incorporation by Reference: The **Glossary of Terms, Glossary of Terms for Cisco Managed Services, List of Services Not Covered** and **Severity and Escalation Guidelines** posted at www.cisco.com/go/servicedescriptions/ are incorporated by reference into this Service Description.

If you purchased the Services directly from Cisco, your **Master Agreement** (as defined in the Glossary of Terms identified above) is also incorporated by reference. If there is a conflict between this Service Description and any of the documents listed above, then this Service Description governs such conflict.

If you purchased the Services through a Cisco Authorized Reseller then your contract, if any, is between you and your Cisco Authorized Reseller. As such, this Service Description is for informational purposes only and is not a contract between you and Cisco. Your Cisco Authorized Reseller should provide you with a copy of this Service Description and related documents, or you can obtain a copy at www.cisco.com/go/servicedescriptions/.

This Service is for Customer-hosted, on-premises deployment only. This Service is intended to supplement a current support agreement for Cisco Products and is only available if all Products in Customer's Network are supported by a minimum of core services such as Smart Net Total Care or SP Base. If available, Cisco will provide the Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco will provide a Quote for Services ("Quote") setting out the extent and duration of the Services. Cisco requires a Purchase Order referencing a valid and agreed-upon Cisco Quote.

General Cisco Responsibilities

- Cisco will provide Standard Business Hours (Eastern Time Zone) monitoring of the systems within the multi-cloud security boundary.
- Provide a VPN end point to enable Cisco's remote connectivity to the Managed Components.
- Design, implement, and test network connectivity and communication between Cisco and Customer sites.
- Cisco will use commercially reasonable efforts to materially comply with Customer's reasonable security policies, as applicable, provided that such policies do not conflict with Cisco's policies, amend or conflict with any applicable Cisco agreement or this Service Description, or cause Cisco to incur materially increased risks or costs to comply with such policies.
- Services are delivered remotely unless otherwise expressly stated in this Service Description.
- Cisco will maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any (i) unauthorized access, use, distribution, or deletion of Customer's data and (ii) compromise of the Managed Components. More information on Cisco's security and privacy policy can be found here: http://www.cisco.com/c/en/us/about/trust-transparency-center/data-protection.html.
- Cisco will participate in any reasonable Customer training required relating to Cisco's performance of the Services for Customer (up to a maximum of eight (8) hours per year).

General Customer Responsibilities

The OpenStack on-premises cloud is hosted on Customer -owned and –managed network(s), and the authorization for Cisco or the Authorized Reseller to connect to any Cisco OpenStack cloud software and hardware on the network and any local networks where Cisco OpenStack on-premises cloud end-points may reside. As such, the Customer has specific responsibilities:

- Provide sufficient network bandwidth and latency.
- Provide a routable network.
- Provide network troubleshooting support to facilitate the identification and remediation of the root cause issues in the event of service interruption or disruption.
- Provide functional host names, IP addresses, SNMP strings, passwords (or means to modify passwords and SNMP strings), and similar information for all Managed Components and Customer applications.
- Provide the technical and environmental requirements (e.g. power, rack spaces, HVAC, etc.), as specified by Cisco, for the Data Collection Tools used as a part of the Services.
- Resolve any configuration issues and stabilize each site before handing over operations to Cisco.
- Install all pluggable optics prior to the start of Services.

- Unless, provided for in a separate SOW or Service Description, be responsible for receipt of all inventory and delivery of all equipment and Managed Components at all Customer locations.
- Be responsible for selecting Managed Components appropriate for its anticipated use.
- Provide Internet Link speed for the VPN connection with Cisco: The minimum speed is 5Mbps for both download and upload (symmetric circuit). Delay of the internet connection to be within acceptable limits.
- Provide Cisco input such that they are capable of completing an accurate dial-plan as a part of subscriber on-boarding.
- Resolve any configuration issues and stabilize each site before handing over operations to Cisco.
- Provide Cisco timely physical and remote access to the Managed Components and Customer's other infrastructure (including obtaining any internal approvals), as reasonably required for Cisco to perform the Services.
- Provide any specialized training of Cisco personnel required for onsite access as requested by Cisco.
- Ensure that only authorized users have access to, and are using the compute, network and storage services provided by Cisco on-premises OpenStack cloud.
- Provide reasonable physical, administrative and technical security to prevent the loss, theft, damage or destruction of any Data Collection Tools and other Cisco software or hardware provided by Cisco for Customer's use in conjunction with the Services.
- Provide access to, and technical support for, the Customer's Identify Management (IdM) service which will be used to authenticate authorized end-users.
- Maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any: (i) unauthorized access, use, distribution, or deletion of Customer's data and (ii) compromise of the Managed Components.
- Promptly supply Cisco with reasonably requested and necessary technical data (e.g. network diagrams) and other information to allow Cisco to provide the Services in a timely manner.
- Provide and maintain the locations and environmental conditions, including power, HVAC, connectivity, space (physical and rack space), security, raised floors, fire containment, connectivity, reliable out of band access, and other requirements necessary for the proper operation of the Managed Components and Customer's other infrastructure, managed infrastructure, and applications in Customer locations as they relate to the Services.
- Provide reasonable physical, administrative and technical security to prevent the loss, theft, damage or destruction of any Cisco software or hardware provided by Cisco used in conjunction with the Services.
- Be responsible for maintaining reasonable technical, administrative, and procedural data security and data privacy safeguards to protect its data that may be processed using the Services.
- Perform and cooperate with Cisco in the performance of, all tasks approved via Customer's Change Advisory Board (CAB) process.
- Be responsible for backing-up and protecting its own data against loss, damage, theft or destruction.
- Be responsible for managing all third-party products and/or services that are not in the scope of Services.
- Identify any dependencies for out of scope hardware, software and/or services.
- Provide an authorized Letter of Agreement (LOA) between Cisco and any Third-Party vendor that the Customer has chosen to have the hardware pod interact with and must maintain a valid maintenance service agreement.
- Notify Cisco in advance of any updates or changes planned in Customer's environment. Failure to notify Cisco of such updates or changes may result in Customer being charged for additional Service Request Units.
- Maintain Cisco SMARTnet support on all Managed Components.
- Provide a change window for Cisco to implement changes to the Managed Components.

- Represent Cisco in, or permit Cisco to be directly involved in, any CAB processes related to third party products and services, as necessary.
- Be responsible for reviewing, analysing, and (if needed) discussing with Cisco the information contained in the reports provided. Customer will notify Cisco within a reasonable timeframe if Customer believes there is an inaccuracy in any report.
- Understand and agree that third-party products covered as part of the Services and managed by Cisco are supported on an up/down basis only, unless otherwise specified in writing by Cisco.

For Classified Network Service (CNS) Only

Cisco will provide Services through the Cisco Classified Network Services (CNS) delivery team if a customer falls into one of the following categories.

- US Government Agencies operating on classified networks.
- Small to Medium Companies operating on classified networks.
- Non-Federal US Government Entities with strict security requirements.
- Small to Medium Companies with strict security requirements.

Cisco will deliver all Services by United States (US) citizens, in secure US locations, with strict data access controls in place. All customer data is stored on networks with strict access controls. For Customers on either unclassified or classified networks, these Services will be remotely offered from the CNS secure data center, located in Research Triangle Park, North Carolina.

Customer Responsibilities for Classified Network Service (CNS) Only

- Customer will obtain and maintain the Authorization to Operate for the cloud hosted components, which are within the OpenStack On-Premises Cloud security boundary.
- Contracts with DoD customers have the appropriate DD254 such that both the Authorized Reseller and Cisco will have sufficient security clearances to operate the system.
- Contracts with the DoD customers provide a means for the Authorized Reseller to access the network such that their Help Desk personnel can access MCS-RN via the network to perform their Help Desk functions.
- Provide the Authorized Reseller and Cisco employees the necessary security clearance billets to operate the service via a DD Form 254 (Contract Security Classification Specification).

Exclusions

Products and services that are not described in this Service Description are not part of the Services, including, but not limited to, the following examples:

- Cisco will not provide Services for any Managed Components that are EoX (e.g. End of Life, End of Support, etc.) unless expressly provided in the applicable Ordering Document(s).
- Internet connectivity or any equipment necessary to establish such connectivity.
- Services or software to resolve any Incidents or Problems resulting from a third party product or causes beyond Cisco's control unless specified otherwise in the applicable Ordering Document(s).
- Maintenance on any third-party hardware or software that is not provided by Cisco.
- Software or hardware upgrades unless expressly referenced in this Service Description.
- Migration services.

- Providing Services with respect to equipment not managed by Cisco and identified by the parties as part of the pod Components.
- Change Management or implementation of changes with respect to equipment not managed by Cisco.
- Unless otherwise expressly agreed, all Services will be provided in English.

2 Managed Subscription Service for OpenStack

General Description
Cisco provides the following managed subscription services for OpenStack on-premises cloud data centers as and if Ordered by Customer:

2.1 Ongoing Monitoring and Management

The Services are a set of multi-technology managed services, as further described below, that consist of the monitoring, management, and troubleshooting of Cisco hardware for OpenStack Components. Service components common to all Cisco Managed Services are based upon practices recommended by the Information Technology Infrastructure Library (ITIL). Unless otherwise expressly provided for in the applicable Ordering Document(s), all Services will be delivered remotely from global NOCs using the "follow-the-sun" delivery model and all Services will be provided 24x7x365, except where noted.

Monitored Components
All devices, hardware, or equipment ordered by Customer from Cisco that comprise an OpenStack pod may be Onboarded as Managed Components. As part of this service, Cisco will also identify certain devices, hardware, or equipment on Customer's network that may be monitored (but not managed) by Cisco ("Monitored Components"). With respect to these Monitored Components, Cisco's responsibilities will be limited to including any Events recorded by Cisco with respect to the Monitored Components in any applicable reports provided to Customer. Cisco and Customer acknowledge and agree that, during the course of Change Management, certain Cisco changes to Managed Components may have a resulting impact on the Monitored Components. Any such changes would be discussed and agreed with Customer via Customer's CAB process.

Service Elements included with Remote Management
The following Service elements are included:

Item	High-Level Description
Event Management	Perform logging and monitoring of events from the pod
Incident Management	Perform troubleshooting and restoration of events.
Reactive Problem Management	Identify the root cause of chronic incidents
Configuration Management	Manage configuration of the pod's hardware and software
Service Asset Inventory Management	Collect and manage the inventory data

Emergency Change Management	Handle urgent changes that need immediate intervention
Operations Service Review – Quarterly	Deliver quarterly briefings on operational outcomes

2.1.1 Event Management

Cisco will monitor for Events on Managed Components.

Cisco Responsibilities

- Create and implement Event Management policies.
- Detect that an Event has occurred by monitoring syslog, SNMP trap messages, KPIs, and/or Threshold Crossing Alerts from Managed Components.
- Help identify meaningful Events by creating filtering rules.
- Implement Event correlation and filtering though Event Management policies when an Event occurs.

Customer Responsibilities

- Provide access and configuration changes for Cisco to receive messages from the Managed Components.

2.1.2 Incident Management

Cisco will identify, troubleshoot, and attempt to restore normal operational functionality if an Incident is detected in a Managed Component.

Cisco Responsibilities

- Create tickets from detected or reported Events, where required.
- Manage Incidents by classifying, prioritizing, troubleshooting, and restoring normal operation.
- Assign and reassess Incident priorities in accordance with the process defined in Appendix A of this Service Description.
- Notify relevant parties about Incidents, keeping the parties updated through Incident closure.
- Provide Incident reports pertaining to the Managed Components.

Customer Responsibilities

- Provide means for Cisco to access, troubleshoot, and resolve Managed Components.
- Provide details about support contracts and other documentation/authorization required to facilitate Incident resolution.
- Contact Cisco if Customer believes an Incident is in-progress or has occurred, per Runbook.
- Perform Cisco or third-party recommended changes to Managed Components or third-party hardware, software, or services, if outside of the scope of the Managed Services.
- Provide Cisco with updates to Customer initiated and related to the Incident(s). Please note: Incident Tickets will be on “hold” for any period of time Cisco is delayed in receiving required information from Customer, the End User, or applicable third-party service providers.

2.1.3 Reactive Problem Management

Cisco will analyze Incidents after Incident Management has restored Services to identify a Root Cause for P1 Incidents (as defined in Appendix A).

Cisco Responsibilities

- Analyze Cisco Product Security Incident Response Team (PSIRT) notifications, Cisco security vulnerabilities, Known Error databases, and field notices to determine if action is necessary.
- Define remediation of PSIRT notifications, if necessary.
- Correlate and organize Incidents to create a Problem Record.
- Analyze the Problem Record, including any available history.
- Characterize and prioritize the Problem Record and determine appropriate actions.
- Provide actionable recommendations to Customer, consulting Cisco's Known Error database where needed.
- Work with Customer's Change Management team to deploy a permanent fix.
- Provide Root Cause analysis for P1 Incidents (as defined in Appendix A).
- Once resolved, close the Problem Record.

Customer Responsibilities

- Provide additional information regarding Managed Component or third party Device configurations and/or information that may relate to the Problem Record.
- Coordinate with third-party suppliers to address situations or incompatibilities where a Non-Standard Managed Component is the cause of a Problem Record, if applicable.
- Implement Cisco-recommended changes.
- Review the Problem Root Cause Analysis report and discuss, as needed.
- Approve PSIRT remediation recommendations.

2.1.4 Configuration Management

Cisco will backup and manage the configuration(s) of IOS-based Managed Components.

Cisco Responsibilities

- Implement and manage a Configuration Management system that will import and archive configurations of Managed Components.
- Backup Managed Components supported by Cisco CatOS®, Cisco-IOS® and Cisco NX-OS® and IOS-XR® device configurations.
- Provide change management processes for updating configurations.
- Provide change management reports with recommendations about Managed Components.
- Where needed, load configurations onto Managed Components in response to a Service Request.

Customer Responsibilities

- Provide Cisco with access to the Managed Components through the Configuration Management system.
- Perform and verify backups on devices not running Cisco CatOS®, Cisco-IOS® and Cisco NX-OS® IOS-XR® device configurations.

2.1.5 Service Asset Inventory Management

Cisco will collect and maintain inventory information about the Managed Components and the associated environment.

Cisco Responsibilities

- Provide a list of all Managed Components from Cisco's CMSP, upon Customer request.
- Complete addition or deletion of Managed Components listed within Data Collection Tool via the Service Request Process.

Customer Responsibilities

- See General Customer Responsibilities above.

2.1.6 Operations Service Review – Quarterly

Cisco will host a remote service review meeting on a quarterly basis and review operational data including incident tickets and historical trends.

Cisco Responsibilities

- With Customer input, provide an agenda and schedule for the Operations Service Review with Customer.
- Provide information about Incident tickets trends and response times, as applicable.
- Provide report of historical, trended, and operational data about Service delivery.
- Provide recommendations for improving the Service delivery.
- Where applicable, discuss with Customer the performance of the Services with respect to the Service Levels.

Customer Responsibilities

- Provide a representative to attend and agree to perform any Customer actions agreed during the meeting.
- Evaluate and approve Cisco-recommended actions and provide updates regarding past actions.

2.2 Lifecycle Management Services

With the Cisco Lifecycle Management (LCM) services, Cisco manages the Pod hardware and software lifecycle, which includes scaling up or down the compute and storage nodes as needed; applying software and firmware patch upgrades; and applying upgrades to OpenStack software on demand and reconfiguring OpenStack services and passwords. The LCM services as includes applying bug fixes and security patches and reconfiguration of optional services such as Heat and Keystone V3. In addition, this service includes applying Cisco Integrated Management Controller (CIMC) upgrades as they become available. There are several components to this service: software upgrades, pod management, management node backup and log management and log management as described below.

2.2.1 Software Upgrade

Cisco will review the current software implementation, develop plan to apply minor and major release updates to existing operations product toolset as well as support for the operations toolset.

Cisco responsibility

- Validate upgrade path for product(s).
- Document upgrade plan for Customer.
- Collaboration with Customer to evaluate the potential impact of the proposed changes.
- Review implementation procedures and provide remote assistance for Customer to resolve problems during release updates.
- Provide a test plan for the upgraded tools before they are rolled into the production environment (major upgrades only).

Deliverables

- Validated upgrade plan
- Test plan
- As-built document with software release notes

2.2.2 Pod management

Cisco will remotely manage Customer's Cisco OpenStack pod(s) to support the customer who is responsible for physically adding, removing, or replacing any of the storage, compute or control nodes.

Cisco responsibility

- Operationally maintain and install the software when adding or removing elements in the existing pod.
- Manage the lifecycle of pod service requests.
- Coordinate, provide governance and execute changes to pod software components, using commercially reasonable efforts to minimize any adverse impacts of those changes to Customer's environment.
- Validate and prioritize Change Requests based on urgency.
- Manage end-to-end lifecycle of Change Requests.
- Provide notifications of service request start and completion for Customer-impacting changes.
- Create backup of the management node. Includes up to five (5) backups per subscription year.
- Create backup when making changes to the pod.
- Forward ELK logs to external syslog server for continuous monitoring and reconfiguration to a different syslog cluster.

Customer responsibility

- Customer will add or remove any nodes to/from the pod. This includes replacement of any node for maintenance.
- Notify Cisco of and review with Cisco any planned or unplanned changes to the pod.
- Inform Cisco when scheduling, communicating, and executing any changes.
- Confirm and maintain scheduled windows for change activities.
- Customer is to provide or identify NFS store for backup and restore purposes.

- Identify and provide access to a syslog server.

Deliverables

- Update document showing baseline pod architecture along with any changes to architecture.
- Update log indicating completed backup and restores.
- Quarterly report that indicates delivery of logs that were forwarded to syslog server, Cisco requires access to syslog server in order to provide this deliverable.

2.3 Security Compliance Service

The OpenStack cloud has the appropriate high-level security policies and periodically audits and reports inconsistencies.

Cisco responsibility

- Provide security governance for the supported solution.
- Enable consistency between approved environment and production environment.
- Monitor and report on security relevant information such as users, roles, and any type changes to the environment.

Deliverables

- Security governance plan.
- System security plan.
- Audit reports.
- Monthly report of relevant security information.

2.4 Administration and Provisioning Services

This service provides customized configuration of management, compute, network, and storage nodes, plus provisioning for virtual instances. The service also optimizes the pod based on Cisco recommendations.

Cisco responsibility

- Provision and manage resources on OpenStack on-premises cloud that includes users, groups, access controls, projects, quotas, instances, volumes, networks and security groups, by using service requests and other documentation provided by the customer.

Customer responsibility

- Provide a document that describes the specifications for administration and provisioning the various aspects of the pod.
- Issue service requests for changes to users, groups, access controls, projects, quotas, instances, volumes, networks and security groups.

Deliverables

- Quarterly Report of Service Requests that indicating status of requests.

2.5 Data Retention Services

This Service provides data retention and business continuity via workload backup and restore. A user can audit or track the lifecycle of any data file by leveraging the snapshots of the workload.

Cisco responsibilities

- Provide specifications for hardware and Linux OS.
- Installation of data retention software and its agent on the controller node and compute nodes.
- With the customer identify workloads to be backed up.
- Verifying backups are valid and useable.
- Create a backup of workloads in response to a service request.
- Monitor the continuous operation of data retention services.
- Restore data to OpenStack cloud in response to a service request.

Customer responsibilities

- Identify and provide access to backup location.
- With Cisco identify workloads to be backed up.
- Create Service Request for backup or restore of workloads.

Deliverables

- Quarterly report of backup and restore activities.

2.6 Billing and Chargeback Enablement

Cisco Responsibilities

- Install billing software, and create rate card.
- Configure billing software based on client rate card requirements.
- Periodic update to rate cards.

Customer Responsibilities

- Provide input to direct and indirect costs to be reflected in rate card.

Deliverables

- Monthly billing report
- Periodic updates to rate card made by Service Request.

3 Priority Levels

This Section 3 describes the methodology and associated terminology used in determining the priority level of an Incident. Cisco classifies Incidents according to "Impact" and "Urgency" and subsequently defines the priority of the Incident by applying the Impact and Urgency terms to the chart below.

3.1 Impact Definitions

An Incident is classified according to the breadth of its impact on Customer's business (the size, scope, and complexity of the Incident). Impact is a measure of the business criticality of an Incident, often equal to the extent to which an Incident affects the availability of the Service. Cisco will work with Customer during the provision of Transition Planning and Support Services to specify the impact for specific Managed Components, if necessary.

There are four impact levels:

- Widespread: Entire Service is affected (more than three quarters of individuals, locations or Managed Components).
- Large: Multiple locations are affected (between one-half and three-quarters of individuals, locations or Managed Components).
- Localized: Single location and/or multiple users are affected (between one-quarter and one-half of individuals, locations or Managed Components)
- Individualized: A single user is affected (less than one-quarter of individuals, locations or Managed Components)

3.2 Urgency Definitions

The Urgency of an Incident is classified according to its impact on the Services or ability for Customer to receive the Services and the financial impact to Customer's business. Cisco Incident urgency levels are defined as follows:

- Critical – Primary function is stopped with no redundancy or backup. There may be a significant, immediate financial impact to Customer's business.
- Major – Primary function is severely degraded and supported by backup or redundant system. There is a probable significant financial impact to Customer's business.
- Minor – Non-critical function is stopped or severely degraded. There is a possible financial impact to Customer's business.
- Low/Notice - Non-critical business function is degraded. There is no impact. Customer perceives the issue as low.

3.3 Priority Definitions

Priority defines the level of effort that will be expended by Cisco and Customer to resolve the Incident. The Priority level is determined by applying the Impact and Urgency definitions to the chart below.

Cisco Incident Management priorities are defined as follows:

- P1: Cisco and Customer will commit any necessary resources 24x7 to resolve the situation.
- P2: Cisco and Customer will commit full-time resources during Standard Business Hours to resolve the situation.
- P3: Cisco and Customer are willing to commit resources during Standard Business Hours to restore service to satisfactory levels.
- P4: Cisco and Customer are willing to commit resources during Standard Business Hours to provide information or assistance.

	IMPACT			
Urgency	Widespread	Large	Localized	Individualized
Critical	P1	P1	P2	P2
Major	P1	P2	P2	P3
Minor	P2	P3	P3	P3
Low/Notice	P4	P4	P4	P4

Cisco will adjust the case priority in accordance with updated Priority of Impact or Incident resolution.

The case may be left open for a prescribed period while operational stability is being assessed.

4 Additional Terms

a. **No Termination for Convenience.** If your Master Agreement contains a right to terminate for convenience, including any such termination for convenience right found in an order or SOW, then such right to terminate for convenience shall be null and void with respect to the Services described in this Service Description.

b. **Cisco Recommendations.** To the extent that Customer fails to implement any Cisco recommendations or requirements with respect to the Managed Components or the Services or to the extent that Customer makes changes to the Managed Components in violation of this Service Description, Cisco shall have no liability for any failure(s) with respect to the performance of the Services.

c. **Data Collection Tools.** Customer receives a limited, non-transferable, internal use, license to use the Data Collection Tools only to the extent and duration reasonably required to receive the Services. Upon cessation or termination of the Services, the license to the Data Collection Tools will automatically terminate and Customer will return all Cisco-owned hardware and software licensed for the receipt of the Services (e.g. Data Collection Tools). Except to the extent caused by Cisco, Customer will be responsible for any loss, theft or damage to the Data Collection Tools until they are returned. The following document is incorporated into this Service Description: http://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/data-collection-tools-supplement.pdf.

d. **Data Retention.** Upon cessation or termination of the Services, and within 30 calendar days of receipt of all Cisco-owned hardware and software licensed for the receipt of the Services, Cisco will destroy any Customer Data, Telemetry Data or Cisco Operations Data from the Data Collection Tools, unless otherwise required by applicable law to retain such information.

e. **Third Party Contracts.** Customer will be responsible for enforcing any third party supplier contract terms (and Service Level Agreements, as applicable) and will release Cisco from any affected performance obligations to the extent Customer fails to do so.

f. **Usage Data.** Cisco may collect data on User's usage of the Services ("**Usage Data**") in order to maintain, improve, market or promote the Services. Partner acknowledges and agrees that Cisco owns all Intellectual Property Rights in, and may freely use, the Usage Data. In any event, Cisco will comply at all times with Applicable Law related to Cisco's collection and use of all Usage Data and will use reasonable physical, technical, and procedural means to protect the Usage Data in accordance with the Cisco Online Privacy Statement, which is made available at http://www.cisco.com/c/en/us/about/legal/privacy-full.html or such other site(s) as Cisco may publically communicate from time to time.