Cisco VMSaaS Offer Description

This document describes the Cisco VMSaaS Cloud offer and the associated support services.

Definitions

Capitalized terms used in this VMSaaS Offer Description are defined below.

"Cisco Operation Center" means Cisco's operation center where services are remotely managed.

"Cloud Hosting" means Cisco operation of a VMS Platform instance(s) hosted in a 3rd party public cloud provider data center, or other data center.

"Control Plane" means the cloud application programming interfaces ("API") and website interfaces (such as Cloud Portal) used to orchestrate and manage service provided by the VMS Platform.

"**Change**" means the addition, modification or removal of anything that could have an effect on the Service.

"Data Plane" means the network that physical or virtual network functions use to communicate with each other and to external IP addresses and network segments. The demarcation point of the data plane between internal and external communications is a networking device responsible for providing the network gateway for a specific VMS installation.

"**Incident**" means an unplanned interruption to the Service or reduction in the quality of the Service.

"**Problem**" means a cause of one or more Incidents.

"**Response Time"** means the period between the receipt of a request and the time of an initial response by a Cisco support engineer (via phone, email or through Cisco's support portal). "**Service(s)**" means any service provided as part of VMSaaS.

"**Service Desk**" means an ITIL compliant tool used to manage ITIL tickets including Incidents, Service Requests, Changes and Problems

"**Service Request**" means a user request for information, advice, for a standard change, or for access to a service.

"SP" means a service provider.

"Status Updates" means the updates provided by Cisco on the status of a support ticket. Status Updates will be provided via email and include current state, and most recent findings / updates (if any available).

"Unavailable" or **"Unavailability"** means:

- For Control Plane, when requests to facilitate consumption of cloud resources, via the API or website interface are inaccessible because the cloud resources are down or unresponsive to requests.
- For Data Plane, when an SP running a virtual instance has no connectivity to any other virtual instances or external connectivity.

"VMSaaS Installation " means a single deployment of VMSaaS service including the Control Plane, the Data Plane, and the servers and storage that provide cloud computing resources. Any required VMS service packs or previously agreed to third party components are considered to be part of this installation.

"VMS Platform" means the entire VMS software stack including the associated installed Service Packs and previously agreed to third party VNF components.

"VNF" or Virtual Network Function means a software component that performs a network function such as routing or firewall.

Overview of VMSaaS

VMSaaS delivers the Cisco VMS service creation and delivery platform in a cloud-based SaaS model, enabling rapid delivery of service offerings to market. With VMSaaS, SPs can quickly launch their VMS based offerings using established operational models while minimizing impact to internal operations team. Acting as an IT partner, Cisco deploys and manages a production environment hosted in a public cloud.

VMSaaS provides VMS software installation and hosting in a public cloud. The VMS Installation will support a single production instance and a single pre-production instance that is used by VMSaaS for staging. Both instances will be geographically located in a mutually agreed to data center. VMS software and required VNFs are installed and operated as part of the SaaS offering.

Each independent VMSaaS deployment includes a Control Plane and a Data Plane. The Control Plane provides key platform services such as the API endpoints, Device Orchestration, Management Interface etc. that allows for VNF and self service provisioning, management, and consumption. The Data Plane is comprised of virtual and physical network functions participating in an end-customer service configuration.

Each VMSaaS Installation is securely connected at all times to Cisco's Operation Center using an encrypted tunnel that only accepts connections sourced from Cisco. The Operation Center will utilize this secure connection to remotely provide the VMSaaS Services.

The key features of VMSaaS are listed below:

- Setup Service: installation and management of the VMS Platform in the cloud hosting environment.
- Monitoring and Assurance: 24/7 monitoring and diagnostics of the VMS Platform and hosting environment
- Service Reports: VMS enabled service(s) status and system health dashboard
- Operations Support: 24/7 Level 2 & 3 operations support. (Level 1 support is provided by the SP)
- Backup & Restore: backup of system installation and associated configurations
- Maintenance and Updates: system updates using Cisco's CI/CD pipeline
- Capacity Planning: VMS system capacity monitoring and reporting
- Security and vulnerability management of the VMSaaS Installation

VMSaaS provides additional optional Services that are tailored to meet specific requirements. They are mentioned below for reference only and will be detailed in a separate document:

- Application of customer-specific branding (UI "skinning")
- Identity federation
- Service template design
- Integration into existing OSS/BSS systems
- Service desk integration with SP incident management system
- Assigned program manager until launch
- Assigned Service Delivery Manager for duration of engagement
- Customized Reporting
- Physical CPE device or VNF management
- Service Provisioning

Services included in VMSaaS

The services and processes outlined in this section are included with the VMSaaS subscription and apply to each VMSaaS Installation.

VMSaaS Setup Service

The setup Service provides installation and validation of the VMS Platform in the selected hosting environment. The ability to orchestrate and monitor services is verified. Any requested optional Services such as OSS/BSS or identity management integration efforts are completed and validated during this setup Service. The SP is expected to execute its own testing to validate the operational readiness of the installation and follow the acceptance process described below.

Restrictions and Limitations of the Setup Services

- Installation and setup are provided during Cisco Normal Business Hours only.
- Setup Service is only provided in English (including all written and oral communication, documents, etc.), regardless of address/country of the SP.
- All services are performed remotely

Upon completion of the installation and setup for the particular VMSaaS Installation, Cisco will send an email to the SP designated contacts that the Setup Service is complete and the service is ready for SP use. If the SP reasonably believes the Setup Services have not been completed or there is a material error with them, the SP must notify Cisco (via Cisco's Support Portal) within 7 calendar days of receipt of the email notification above or the Setup Services will be deemed accepted. If there is a material error as reported by the SP and the error is attributable to Cisco, Cisco will work to reasonably correct the error and will repeat the acceptance process described in this paragraph.

The VMSaaS subscription term begins when the Setup Services are accepted as described in the previous paragraph.

Monitoring and Assurance

Cisco will monitor the VMS Platform for any issues and will be solely responsible for investigating and resolving any issues with the VMS Platform. Cisco will alert the SP of potential issues and provide assistance to the SP to resolve any OSS/BSS detected issues. Any incidents resulting from monitoring will also be reported to Service Desk.

Service Reports

The VMSaaS offering includes a reporting dashboard that provides the status of:

- Infrastructure components and the health status of the infrastructure compute and storage
- VMS software key components
- VMS enabled service(s) status across the deployment
- VMS enabled Service status on a per tenant basis
- Infrastructure and Platform availability (SLA available)

VMSaaS Service Desk will provide the following reports:

1. Time to Respond and Time to Resolve Metrics for VMS Platform incidents (SLA available)
2. Monthly Open, Resolved incident report for VMS Platform

Operations Support Center

Access to a Level 2/3 support services is available 24/7 to troubleshoot and resolve issues. Incidents are managed using Cisco Service Desk. Cisco Service Desk is an ITIL compliant tool. The SP is responsible for Level 1 support and initial triage.

Support Model

1. SP will utilize the Cisco Service Desk to create and view Incidents, create and view Service Requests, submit and view Changes and view Problems. All records within the Service Desk will accept comments. Automatic email notifications are sent to SP operators at various stages of each ticket's lifecycle.

2. SP may call VMS Operations Center to create an incident in the Service Desk.

Hours & Service

- VMSaaS Service support operates 24x7 for Production incidents and technical support.
- Non-production related technical support is provided during standard business hours, Monday thru Friday,8AM - 5PM PST.
- Support service is only provided in English (including all written and oral communication, documents, etc.) – regardless of address/country of the SP.

Event Monitoring Service Request

Incidents identified by VMS Platform monitoring are submitted and tracked in the Service Desk. The SP will be notified via email and will have access to view the status of open issues.

Support Classifications

When submitting a support ticket the severity of an issue related to the Service is classified by SP based on the condition of the Service when submitted. Cisco support personnel use the following definitions to classify issues and may revise severity levels according to actual impact of a reported issue after an initial investigation.

Severity level	Severity Level definitions
P1	A total loss of service at one End User Site or multiple End User Sites.
P2	Partial loss of service (at one End User Site or multiple End User Sites) which has a significant detrimental effect on End User's ability to perform normal communications but which does not represent a total loss of service. For example: (a) if End User has ordered a resilient service, loss of resilience at one or more End User Sites (meaning a loss of any of the primary, secondary, or backup access circuits); (b) packet loss over 25%; (c) loss of capacity or (d) Control Plane inoperable or unreachable.
P3	Degradation of service performance Service does not perform as expected, but there is no loss of service. For example: (a) slower than normal performance times (b) unexpected results (c) maintenance requests that could improve service quality.
P4	An Incident not related to the Service or Incidents not classifieded as Severity Level 1, 2 or 3 Incidents.

Service Level Objectives

The following table identifies the performance targets for support of the Service.

Severity level	Response Time by Support Type	Plan of Action Submitted	Frequency of Status Updates
P1	30 minutes	Within 4 hours	Every 30 minutes
P2	2 hours	Within 8 hours	Every 12 hours
P3	1 Business day	N/A	N/A
P4	3 Business days	N/A	N/A

Support Escalation Triggers

A support ticket may be escalated based on any of the following criteria:

- Recommendation by VMSaaS personnel.
  - Technical Support Engineer
  - System Engineer
  - VMSaaS Management.
- Response time: failure to provide a response time or resolution within the timeframes described in the service levels above may generate an escalation.
- Issue severity: system outage automatically generates an escalation. Other severe service issues may generate an escalation at the discretion of VMSaaS personnel list above.
- SP satisfaction: poor SP satisfaction scores may generate a support escalation.

Escalation Process

If a support ticket is escalated, the following persons will be notified and kept apprised of the issue until de-escalation or resolution:

- **Tier 1**
  - SP
  - Cisco's Account Representative for SP
  - Cisco Technical Support Engineer owning the case
- **Tier 2**
  - Cisco Director of Services
  - Cisco Engineer and/or Product Manager owning any associated bug or feature
- **Tier 3**
  - Cisco V.P. of Sales
  - Cisco V.P. of Engineering
  - Cisco V.P. of Product Management

Escalation Actions

- The team above is notified of the escalation in order of severity.
- If fully escalated, the Cisco Director of Services will be responsible for ownership of the issue until resolution/ priority reduction.
- Assemble appropriate team from persons listed above to assess the issue and develop a resolution plan, and communicate plan to SP:
  - Specific actions to be taken in order to resolve the issue
  - Issue owners
  - Due date/time for each action
  - Explicit agreement from engineering management for resources to perform engineering tasks
  - Decision on the next escalation meeting
  - Decision to de-escalate
- Plan is agreed upon and executed
- Case is resolved and SP are informed

Backup and Restore Service

Cisco will provide daily backups of VMS Platform configuration and relevant data and will perform restoration as required. Backup sets capture the complete Control Plane databases and are not intended for temporary data recovery. Backup sets are encrypted and will be stored off-site.

Maintenance and Updates

Cisco will apply upgrades, patches, bug fixes or other maintenance to the VMS Platform. These updates are scheduled and completed using SP established maintenance windows (except for Emergency Updates). SP agrees to use reasonable efforts to comply with any maintenance requirements.

Capacity Planning

Cisco will implement capacity planning as system scaling on an ongoing basis. This scaling is based upon several

factors such as:

- Customer forecasts (if available)
- VMS Platform KPIs
- Hosting infrastructure KPIs
- Number of attached devices

Security and Vulnerability Management

Cisco will use automated scanners to scan all VMSaaS Installations weekly. When a vulnerability is detected, Cisco will apply the necessary corrective action and re-scan the environment to verify resolution. Cisco will also apply necessary security patches to installed products, either through a maintenance release update, or direct patching depending on the complexity and severity of the patch.

VMSaaS Orders and Billing

VMSaaS is a subscription service that includes the following charges:

1. A one-time Platform activation fee
2. A one-time per VMS Service Pack activation fee
3. Monthly operating charge: covers cloud hosting, operations and management

VNF licensing and management fees are not included in VMSaaS charges.

VMS Management Transfer Option

VMSaaS offers the SP the option to manage the VMS stack on its own. The SP, at its option, may transfer the VMSaaS operation to its management and terminate the VMSaaS monthly operating subscription, subject to mutual agreement on VMS licensing fees and terms and conditions.

Service Termination

The SP, at its option, may terminate VMSaaS subscription, with or without cause, with at least thirty day written notice provided the SP has paid Cisco for delivered Services.

Cisco, at its option may terminate the Service, without cause with no less than a 90 day written notice. Cisco may terminate the Services due to non-payment with no less than 30 day written notice.

SP Responsibilities and Service Exclusions

VMSaaS, while structured to accelerate deployment, requires activities to be completed by the SP to have a successful deployment. The SP further agrees to reasonably assist Cisco's efforts to provide the Services; provide timely information reasonably requested by Cisco; and perform the responsibilities outlined below:

- Provide and maintain the required data plane infrastructure and physical network connectivity
- End customer onboarding, billing, and support
- Provide periodic maintenance windows for Cisco to perform maintenance; establish emergency maintenance windows where necessary
- Provide technical resources for the following: capture and provide details of reported issues; aid in replication and triaging issues as reasonably requested by Cisco; aid in testing fixes of issues; and, confirm that issues are not related to SP provided hardware, software, applications, or other sources

Support Exclusions

VMSaaS does not include support for or following:

- Onsite support

- Management of SP physical circuits, lines or network devices not under management.
- Proactive Problem Management: processes to identify and solve Problems before Incidents occur.
- Pre-emptive Event Management: processes to identify events that may result in an Incident.
- Supplier Management: management of third party suppliers or contracts made available through SP