Offer Description

IMPORTANT: READ CAREFULLY

Infinite Video for OTT

This Infinite Video (IV) for OTT Offer Description ("**Offer Description**") describes the services comprising IV for OTT (the "**Services" or "Offering**") that Cisco Systems, Inc. and its affiliates ("**Cisco**") or Cisco Approved Sources will provide to the applicable customer ("**Customer**"). The specific quantity and type of Services will be documented in a written Offering Order between the parties or as ordered by Customer via Cisco's website (**"Offering Order"**).

Related Documents. This Offer Description should be read in conjunction with the Cisco Universal Cloud Terms at http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-terms.pdf (the "**Agreement**").

Defined Terms. Capitalized terms used in this Offer Description, as well as the Offering Order, are defined in the Glossary of Terms in Annex A at the end of this document. Capitalized terms used in this Offer Description and/or the Offering Order and not otherwise defined herein have the meanings given them in the Agreement.

Direct or Indirect Purchases

- **Direct Sale from Cisco.** If a Customer has purchased this Offering directly from Cisco, this document is incorporated into the applicable purchase agreement between Customer and Cisco. If there is a conflict between this Offer Description and the Agreement, this Offer Description shall govern. The terms of this Offer Description are limited to the scope of this Offer Description and Offering Order or Statement of Work (SOW) under which the Offering is ordered, and shall not be applicable to any other service descriptions or statements of work.
- **Sale through Cisco-Authorized Reseller**. If an Authorized Reseller has purchased this Offering either directly from Cisco for resale to a Customer or from a Cisco authorized distributor for resale to a Customer, this document is incorporated into the Authorized Reseller's Resale Agreement with Cisco (Indirect Channel Partner Agreement, Systems Integrator Agreement, or the equivalent agreement governing the resale of Cisco Services) (the "**Resale Agreement**"). This document is for informational purposes only except for Data Privacy section which the Cisco-Authorized Reseller must flow to Customer and Customer must agree to comply with, as a condition of sale. This document is not a contract between Customer and Cisco. The contract, if any, governing the provision of this Offering is the one between Customer and its Cisco-Authorized Reseller. Such Cisco-Authorized Reseller should provide this document to Customer, or Customer can obtain a copy of this and other Cisco service descriptions and offer descriptions at www.cisco.com/go/servicedescriptions/.

Cisco reserves the right to change this Offer Description at any time.

1. OVERVIEW

1.1 Summary of Offering

The Offering is a multi-tenant, cloud-based software solution that enables customers to create and distribute streaming video apps across multiple device platforms. The Offering is comprised of the following components:

- Control Plane and Web Console (Uplink)
- Platform Types (also known as Device Bundles)
- Launch Management Assistance
- Support & Maintenance
- Knowledgebase Documentation
- Content Distribution Network (CDN)
- Digital Rights Management (DRM)
- API-based Integrations

The Offering is licensed to customers on a subscription basis for a monthly fee for the Control Plane, Platform Type(s), Launch Management and Support & Maintenance ("Platform Fees") where the Platform Fees are based on the Platform Type(s) chosen by the Customer, with additional monthly fees based on the number of active users and/or monthly video sessions ("Usage Fees"), depending on the Customer's monetization model. The additional Offering components are licensed or supplied at an additional fee. License fees are quoted on a per branded app basis.

1.2 Features & Functionality

Control Plane

The Control Plane is comprised of the following cloud-hosted components:

- Web Console (Uplink): Portal used for:
  - Service configuration
  - Content workflow, management and curation
  - Customer App configuration and branding
- Analytics Portal:
  - Web console using Google Analytics
- Content Processing:
  - Ingest and transcoding of VOD assets on a best-efforts basis
  - Playback enablement
- Storage:
  - Up to 2.5GB of storage for VOD assets is included in the Offering.
  - Additional storage is available at an additional monthly fee on a per-GB stored basis.

Platform Types
The Offering enables Customers to create video apps and distribute Content on hardware devices supported in each Platform Type as follows:

Platform Types (see Note 1 below)	Included Devices (see Note 1 below)
Streaming Players	Apple TV, Roku, Amazon Fire TV, Amazon Fire Stick, Android TV, Samsung Smart TVs
Personal Devices	IOS and Android for tablet and phones Web for Mac/PC
Games Consoles	Xbox One, Xbox 360, Sony Playstation 3/4
Software Development Kit (SDK)	For iOS, Android and JavaScript. The SDK enables Customers to build or integrate their own custom client video UIs that can use the Control Plane.

Note 1:
- *Cisco reserves the right to modify this list from time to time.*
- *Xbox One and Sony Playstation are Closed Platforms*
- *Microsoft is no longer accepting new titles for the Xbox 360 platform.*
- *Cisco does not support every version of firmware and OS versions on the Devices; however, Cisco generally supports the then-current version and the immediately preceding version.*

Cisco also offers the Personal Devices Premium UX as a fee-based, add-on option to the Personal Devices bundle, available on the same Devices as listed in the Personal Devices above.

Content Distribution Network (CDN)

Customers may elect to use Cisco's CDN offer (currently Verizon Edgecast and Amazon CloudFront) or they may elect to use their own CDN provider. Cisco will configure Customer's Content for distribution with their chosen CDN provided that such CDN supports industry standards. For Customers using Cisco's multi-CDN, fees are charged on a per-GB streamed per month basis.

Support & Maintenance

- Technical support as outlined in Section 3.1 of this Offer Description is included in the Device Platform license fees.
- Updates to the Control Plane are included in the Platform Type license fees.
- Updates to any Device in a Platform Type as well as new Devices (if any) added into any Platform Type are included in the applicable Platform Type(s)'s license fee.

Digital Rights Management ("DRM")

The following DRM protocols are available via the Offering:
- Cisco Videoguard
- Apple Fairplay Streaming
- MS PlayReady
- Widevine

While DRM is supported on all Devices, not all DRM protocols are supported or available on each Device. Please contact your

Cisco sales representative to determine the applicable DRM protocols that are supported on your Device. The Personal Device Premium UX profile only supports Cisco Videoguard.

API-based Integrations

For Customers using their own backend systems for services (including but not limited to login/authentication, favorites, user entitlements and search), Cisco provides API specifications whereby if the Customer's end points conform to such specifications, Customers can designate these end points in the Uplink portal and no custom integration is needed.

If a Customer's end points do not or cannot meet the Cisco specification, Customers can request custom integrations. Pricing for Cisco integration services (if requested) is subject to a mutually agreed Statement of Work, implementation timeline and contract terms.

Launch Management Assistance

Cisco provides all Customers with a Cisco Customer Operations Project Manager and Technical Lead, included with the License Fees, to assist with Customer's use of the Services and to assist Customer in launching Customer Apps. Customer still retains primary responsibility for the overall management and launch of Customer Apps and Customer products.

1.3 Additional Terms and Conditions

Offer Terms.

- Customer may cancel their subscription within the first two (2) months of the Contract Term if they have elected the Monthly Billing option; if the Customer has elected Prepaid Term, the subscription is non-cancellable.
- Customer may add Device Platforms or optional services at any time, but cancellation or removal of optional services are not allowed during the Contract Term (outside of the Termination Window).
- Usage Fees are based on reports from Cisco's backend systems and are available to Customers upon request.
- License Fees exclude any third-party software licenses or other third-party elements unless specifically included in this Offer Description.
- Prices quoted are net of any taxes, e.g. import duties and withholding taxes for third parties, unless expressly stated.

License Grant.

Subject to the terms of this Offer Description and the Agreement, Cisco grants Customer a limited, nonexclusive, nontransferable, non-sublicensable object code license to use the Services during the Contract Term for the sole purpose of creating and distributing Customer Apps. Cisco is the owner of all right, title and interest in and to the Services (and all intellectual property rights therein), and Cisco reserves all rights not expressly granted herein.

Term and Termination:

- Customer has an option to Auto-Renew based on a yearly Contract Term or Customers can select Do Not Renew. If the Customer selects Do Not Renew, they will have to then manually renew via the Cisco or Cisco Partner's ordering system prior to the termination of the then-current Contract Term.
- The Services are provided on a best-efforts basis. In addition to Cisco's rights to terminate or suspend Services to the Customer as described in Section 9 of the Agreement , Customer acknowledges that: (i) its access to and use of the Services may be suspended for the duration of any unanticipated or unscheduled downtime or unavailability of any portion or all of the Services for any reason, including as a result of power outages, broadband connection failure, system failures or other interruptions; and (ii) Cisco shall also be entitled, without any liability to Customer, to suspend access to any portion or all of the Services at any time, on a Service-wide basis: (a) for scheduled downtime to permit us to conduct maintenance or make modifications to any Service; (b) in the event of a denial of service attack or other attack on the Services or other event that Cisco determines, in its sole discretion, may create a risk to the applicable Service, to Customer or to any of Cisco's other customers if the Service were not suspended; or (c) in the event that Cisco determine that any Service is prohibited by any applicable law, regulatory requirement or any other statutory or non-statutory provision or Cisco otherwise determine that it is necessary or prudent to do so for legal or regulatory reasons (collectively, "Service Suspensions"). Without limitation, Cisco shall have no liability whatsoever for any damage, liabilities, losses (including any loss of data or profits) or any other consequences that Customer may incur as a result of any Service Suspension. To the extent Cisco is able, it will endeavor to provide Customer notice of any Service Suspension in accordance with the notice provisions set forth in Section 12 (g) of the Agreement and to post updates regarding resumption of Services following any such suspension, but shall have no liability for the manner in which Cisco may do so or if Cisco fails to do so. To the extent Cisco is able, is will endeavor to restore the Services to Customer as soon as is reasonably practicable following any Service Suspensions. Cisco shall have no liability for the

manner in which it may restore or fail to restore the Services to Customer as soon as is reasonably practicable following any Services Suspensions.

1.4 Excluded Services

The following services are not included in the Offering:

- Changes to or customization of the APIs or Control Plane.
- Custom client applications on any Device beyond standard configuration options available via Uplink.
- Any support or operational services not specifically outlined in this Offer Description

2. OFFERING ACTIVATION

2.1. Activation for SAAS Offering

After Customer has accepted the Agreement and booked an Offering Order, Customer will be contacted by Cisco's IV Customer Operations team with Uplink Account information within 48 hours. The Customer may then access Uplink and begin using the Services.

2.2. Customer Requirements

2.2.1 General Requirements

Customer shall:

- Provide a project manager, technical lead and design lead for self-service integration and day to day operational responsibilities.
- Supply Cisco with all reasonably requested and reasonably necessary, accurate, complete, and up to date information and assets to allow Cisco to supply the Offer to the Customer.
- Provide updated and accurate information on Customer's hardware and software environment, networking information, and similar information reasonably required or requested to provide the Offer.
- Reasonably work with Cisco in a timely manner to aid in Cisco's provision of Offer to Customer by any third party cooperation, documents or approvals required for provision of Cisco's Service.
- Notify Cisco of any change to its system requirements in a timely manner before the commencement of the Services and Customer is responsible for any delay and additional costs which arise due to any change in its system requirements.
- 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, confirming issues are not related to Customer provided hardware, software, applications, or other sources.
- Maintain appropriate protection and backup of Customer data and Content at all times. Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.
- Maintain appropriate security against unauthorized access, use or deletion of Customer data. Establish and maintain appropriate security policies within the infrastructure, as well as any operating systems or applications.
- Be responsible for implementing and using strong passwords for accessing Cisco infrastructure and the associated support portal. The following are common guidelines for choosing strong passwords. These are designed to make passwords less easily discovered by intelligent guessing: (i) Include numbers, symbols, upper and lowercase letters in passwords; (ii) Password length should be around 12 to 14 characters; (iii) Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information (e.g., dates, ID numbers, ancestors' names or dates...).
- Not use the Services to send spam, viruses or malware.
- Be responsible for any catastrophic security events that result from any unauthorized configuration of the Offering components by Customer's personnel. These include, but are not limited to, configuring the Offering components in a manner not prescribed in the Documentation, creating an open relay, changing the network configuration set by Cisco, shutting down Cisco's infrastructure, etc.
- Be assigned a user ID and a password for the use of the Offering and Customer shall protect the access authorization against third-party access and shall immediately modify the same if a third party may have become aware thereof. Customer shall ensure the access authorization may be used only by that to whom it was assigned. Cisco shall not be liable if a third party uses or abuses Cisco Offering with a user ID assigned to the Customer. The Customer shall indemnify and hold Cisco harmless in respect of any damage Cisco may incur as a result from such use or abuse.

2.2.2 Compliance with Law. Customer recognises that information sent to and from Customer will pass through Cisco's systems and accordingly Customer undertakes to comply with all relevant legislation applicable to its use of the Services. Customer shall comply with such laws and regulations governing use, export, re-export, and transfer of products and technology and will obtain all required authorizations, permits, or licenses, if any. Cisco shall not be in default of its obligations to the extent that it cannot provide the Services either because such approvals have not been obtained or because any third party prevents Cisco from providing the Offer. Customer will also be responsible for approving any recommendations provided by Cisco related to the Services and implementation of any Policies. The failure of Customer to comply with this Section may be deemed a material breach.

2.2.3 Customer is solely responsible for its Content that it makes available for distribution through the Customer Apps, and Customer will ensure that it complies with any requirements imposed by third parties on the use of the Content, including payment of any money owed to those third parties (such as royalties). Customer represents and warrants (and Customer will demonstrate to Cisco's full satisfaction upon its request) that:

- Customer owns, controls or has sufficient licenses, rights, consents and permissions to use and distribute and authorize Cisco to use and distribute all Content, and each and every image and sound contained or embodied therein, to enable use, display and distribution of the Content through the Customer Apps;
- Customer has the written consent, release, and/or permission to use the name or likeness of each and every identifiable individual person and to include and use such individual's name or likeness in the Content to enable use, display and distribution through the Customer Apps;
- the use, sale or other promotion or distribution of the Content on or through the Customer Apps or otherwise does not violate the privacy rights, publicity rights, intellectual property rights, contract rights, or any other rights of any person or entity; and
- Customer has full authority to act on behalf of any and all owners or licensees of any right, title or interest in and to any Content.

2.2.4 Customer shall indemnify, defend and hold harmless Cisco and all of, its agents, customers, affiliates and suppliers and employees, from all liabilities and expenses resulting from third party claims, including reasonable outside attorneys' fees that arise from or relate to Customer's breach of the foregoing representations and warranties in this Section Cisco reserves the right (but not the obligation) at any time to assume the exclusive defense and control of any matter otherwise subject to indemnification by Customer, in which event Customer will assist and cooperate with Cisco in asserting any available defenses.

2.2.5 Customer acknowledges and agrees that for Closed Platforms, the device manufacturer (and not Cisco) must approve Customer's development of Apps on device manufacturer's Closed Platform.

2.2.6 Customer acknowledges and agrees that Cisco is only providing a software platform, and that Customer has the sole discretion to select and distribute the Content.

2.2.7 Customer is responsible for ensuring Cisco is granted rights to share content metadata from the Content within Customer Apps with the metadata management systems of device vendors for the purpose of enabling unified content search on those devices.

2.2.8 Rights Granted to Cisco:

a) Customer hereby grants to Cisco for as long as Customer is using the Services and/or Customer Apps, and solely as needed for Cisco to perform its obligations under this Agreement, a worldwide, non-exclusive, royalty-free right to:

i) use, display and otherwise perform the Customer Apps on behalf of the Customer (including, without limitation, use, display, performance, publishing, and reproduction of the Content for that purpose)

ii) stream, transmit, feature, promote, market, or otherwise sell and distribute the Content to users on or through the Customer Apps;

iii) use, display and perform, and to permit others to use, display and perform, the name(s), trademarks, likeness, biographical materials and similar proprietary rights of Customer and all other members of its organization (e.g., band or group), in connection with the Customer Apps, and

iv) use, display and perform all other information provided by Customer in connection with the Customer Apps, Customer's Account and/or the Cisco Services.

3. OFFERING SUPPORT & MAINTENANCE

3.1 Support

The Offering includes technical support via phone and a web support portal. Additional details regarding Offering support, processes and escalation are provided in the Annex B.

The Customer will be able to contact Cisco support by web or telephone (as applicable) to report an Incident related to the supported IV for OTT subscription or to obtain status of a logged Incident. The Customer's main method of requesting support will be via a login to Cisco's web portal ticketing system. Customers will be provided with details of how to obtain credentials to the web portal ticketing system and Documentation after completion of their Order.

3.2 Maintenance & Updates

- From time to time, Cisco performs scheduled maintenance, to update the servers and software that are used to provide the

  Service. Cisco will make reasonable efforts to notify Customers in advance of any such scheduled maintenance. Notwithstanding the foregoing, Customer acknowledges that Cisco may need to perform emergency maintenance without providing advance notice.

- Cisco reserves the right to modify and provide Updates to the Services.

- Cisco will make good faith efforts to give Customer notice of any material modification or update in release notes provided in the Documentation. Cisco will use reasonable efforts to ensure that any modifications or updates do not materially degrade the performance of the Services or Customer's use of the Services. Cisco will make good faith efforts that any modifications or updates do not require Customer to incur any material additional cost to continue its use of the Services.

- Cisco will use reasonable efforts to implement Updates in a manner that minimizes the impact on Customer's use of the Services but makes no guarantees that advance notice will be provided.

ANNEX A
Glossary of Terms

Term	Definition
Account	Customer's account for access to Uplink.
Active User	A unique End User on a registered Device that consumes video services during the monthly billing cycle.
Auto Renewal Term	Period for which Customer wishes to automatically renew its Contract Term. Customer may also select "Do Not Renew" and then will have to manually renew prior to the end of the then-current Contract Term.
Billing Model	Either Monthly Billing or Prepaid Term applicable to License Fees.
CDN	Content Delivery Network
Closed Platform	A device platform where the device manufacturer (and not Cisco) must approve development for that platform prior to commencement of such development.
Content	All artwork, videos, digital media, metadata, logos, branding elements and other media assets used in Customer Apps
Contract Term	Duration for which Customer is ordering the Services. The first Contract Term is also called the Initial Term. The Contract Term shall commence upon Customer submitting the Offering Order for the Services.
Control Plane	Operational platform for content management, curation and device configuration for the provision of video services. Does not include media processing or delivery.
CPM	Cost per thousand (Mille), generally applicable in the Offering Order to video views.
Customer Apps	Any application, tool or service created by or on behalf of Customer using the Service
Device	Hardware platform upon which Content/Customer Apps are distributed (e.g, Roku, Apple TV, Xbox).
Documentation	Cisco OTT for IV online knowledgebase (available for Customers via secure login site)
DRM	Digital Rights Management

• End User	• Any customer of the Customer who utilizes Customer's App.
• Household	• An account (and any sub-accounts) for an End User of the Customer App. A single Household may include up to 10 video consumption Devices.
• Incident	• An unplanned interruption to the Service or a reduction in the quality of the Service
• Infinite Video for OTT	• Cisco's E2E software solution for enabling the delivery of live and on demand video over unmanaged networks to IP devices in and out of the home.
• License fees	• The fees paid by the customer for the right to use Cisco software for the applicable Solution(s).
• Minimum Contract Term	• 12- months from the commencement of the Contract Term.
• Monthly Billing	• Customer is billed monthly for Services during the Contract Term
• Prepaid Term	• Customer is billed at the beginning of the Contract Term (in advance) for Services.
• Session	• Each time a video is viewed.
• Storage	• Space used on Cisco's platform for storing Content
• Termination Window	• The two (2) months of the Contract Term, during which the Customer may terminate the Services for convenience owing only the prorated portion of the fees incurred in such period. The Termination Window is not applicable with the Prepaid Term option.
• Updates	• Changes to the software used in the Offering, including but not limited to error corrections, bug fixes and other enhancements Unless specifically outlined in this Offer Description, Updates shall not include any release, option or future product which Cisco licenses separately or which is not included under the applicable level of support.
• UX	• User experience, especially the user interface

ANNEX B

Support Services

Overview of the VCS Support Service
VCS Support Services are a set of support Software as a Service (SaaS) offerings for Cisco's Video Portfolio. The deployment typically comprises a Control Plane and a Data Plane as described in Section 0 below. These main services, which are described in further detail in this document are Customer Operations, Service Delivery and Service Assurance. Cisco may provide supplemental services as described in an addendum to this document (each an "Addendum") as purchased by Customer pursuant to any relevant Ordering Documents.

Deployment Options
The solution is broken into two primary components – a Control Plane and a Data Plane. The primary deployment option for the System is for Cisco to provide Control Plane hosted in an off-premise Cisco provided Cloud. Cisco completely owns, operates and manages the Control Plane. Cisco also hosts VOD Video Environment Data Plane video processing in the cloud.
In the primary deployment option, the Customer provides the Live Video Environment Data Plane. The Customer owns, manages and controls the Live Data Plane hardware and platform layer.
Other deployment options are available for discussion and subject to approval by Cisco.

Support Services
The Support Services offered through VCS are meant to guide the Customer experience from deployment through ongoing support. They are described below in further detail.

Customer Operations
The Infinite Video for OTT platform is cost effective and easy to deploy. In most deployments, the Customer provides a Tech Lead, Design Lead, and Program Manager to configure the system; they are responsible for the standard setup and configurations with guidance from Cisco. Cisco provides a Customer Operations Manager to assist with system setup at no additional charge.
Additionally, Cisco can provide Custom Buildout or integration services that could include integration with a Customer's billing and/or subscriber management system or integration/deployment of media and data plane elements. The fees for these services are based upon the integration work required, subject to an agreed Statement of Work with the Customer and will need to be ordered separately.
Note that the solution has published APIs; Cisco encourages Customers to use these APIs to handle the integration themselves, with our Partners or 3rd parties.
Customer Operations will also support the on boarding of the Customer into the self-service portal and service desk described below in Section 0.

Service Delivery
Cisco will handle platform definition, set up of appropriate architecture and tools, stand up in the cloud and application deployment and provide maintenance, bug fixes and new features following a continuous delivery methodology. Ongoing improvements are not limited to the core portions of the System but also includes tools for monitoring and alarming.
Service Assurance
Service Assurance activities are supported by people, process and technology. The priority of Service Assurance is to maximize System up time. During an incident, focus is initially on Video Service restoration. Once the Video Service is restored root-cause analysis will take place and any longer term corrective actions up to and including bug fixes to software will follow. There are several main functions of the Service Assurance arm of VCS.

Monitoring
Cisco's service assurance involves a 24 x 7 x 365 monitoring capability directly integrated into the System. There is a continuous stream of monitoring information with a goal if reacting to events and resolving incidents before subscribers are impacted. Cisco looks at system performance and will adjust the system as necessary or provide insight as to system expansion requirements. This includes availability and capacity management.

Reporting
Cisco will provide regular reports indicating numbers of Incidents/Requests dealt with, planned releases/changes and other KPIs provided by the product. The KPIs are used to determine the quality of the Video Service delivered by the System.
Service Desk
Should the Customer wish to contact Cisco regarding the technical operations of the System they can do so via the Service Desk, which can be contacted by web (for non-critical questions) or telephone (for System impacting Priority 1 concerns) for the following purposes:
To report an incident related to the supported software
To ascertain the status of a logged Incident
To discuss an action plan or escalate an Incident with the Cisco Support Manager

The Service Desk is the first point of contact for all the Control Plane and VOD Video Environment software supported by this Support Service. The Customer will be provided with information how to contact Cisco during on-boarding.

Your main method of requesting support will be via a login to Cisco's Service Now ticketing system. Details of how to obtain your credentials will be provided in the order acceptance notification from Cisco.

Incident Management
Service Assurance will be responsible for overseeing all activities related to incidents opened either by Cisco or the Customer. This includes incident detection and recording, triaging incidents to the appropriate system components and engaging the appropriate engineering teams, communication of incident status and closing the incident when resolved.

Problem Management
If a high priority Incident is resolved either without the root cause being known or with the root cause known but still existing (such that it could cause future Incidents) then a Problem record will be created. Cisco shall update Customer on the progress of any Problems at intervals agreed when the Problem is created.

Change Management
The Support Service includes a continuous delivery process that will give the Customer access to the most recent releases of software developed using agile software development practices. These regular software updates include product roadmap items as well as bug fixes from the field. Cisco will be responsible for the installation of all software related to the System in the cloud.

Environment Software Releases
Cisco will provide software updates and patches and will install the software patches for the Control Plane and VOD Video Environments.
In emergency Incident resolution situations, a patch may have only undergone minimal testing and should therefore be considered for emergency use only until full testing may be concluded.
Client application updates, including patches, shall be implemented only after approval from Customer and should be subject to Customer's change management process.

Remote Support and VPN provision
The ability to connect into Customer's Live Video Environment using a continuous VPN communications link provided and approved by Customer will enable Cisco to run diagnostics remotely. Cisco must have the capability to monitor the status of various components of the System. This provides valuable information that Cisco engineers can analyse to facilitate the rapid diagnosis and resolution of Incidents should they occur.
Cisco recognizes that System data and customer information is confidential information, and shall be treated accordingly.
The customer is responsible for setup and maintenance of the remote connection.

Service Level Objectives

Response Times
The following section details the agreed to response times for incidents. Initial Response is applicable to incidents opened by the Customer.

Table 1 Response Times

Priority	Hours	Initial Response	Update Response
Priority 1	24 x 7	30 mins	4 hours, then every 8 hours
Priority 2	8 x 5	4 hours	8 hours, then every 48 hours
Priority 3	8 x 5	Next Business Day	5 days, then every month
Priority 4	8 x 5	5 Business Days	Not applicable

Incident Priorities
Cisco classifies Control Plane and VOD Video Environment software Incidents into four general priorities, dependent on the impact on the Customer's ability to deliver the Video Service:

Priority 1 means a Video Service is down or there is a critical impact to the Customer's business operation. The Customer and Cisco both will commit fulltime resources to resolve the situation.

Priority 2 means operation of an existing network or environment is severely degraded or significant aspects of the Customer's business operation are negatively impacted by unacceptable Video Service performance. The Customer and Cisco both will commit full-time resources during standard business hours to resolve the situation.

Priority 3 means operational performance of the Video Service is impaired, although most business operations remain functional. Customer and Cisco both are willing to commit resources during standard business hours to restore Video Service to satisfactory levels.

Priority 4 Requests for information.

> ***Note:*** *Incidents cannot be raised for known issues that are subject to a Waiver.*

Incident Response Times

- Initial response – The time elapsed between receiving a log number for a reported Incident and being contacted by a Cisco engineer from the local VCS Service Assurance team. The engineer will then commence to make an initial assessment of the Incident. If the incident is proactively opened by Cisco, this metric does not apply.
- Update response – Cisco will continue to work on the Incident and update Customer with an action plan within the timescale specified in Section 0 of this document. The update may be via telephone, face to face or email for an Incident that is Priority 1 or via e-mail for all others.
- Additional onsite response – In situations where Cisco and Customer agree that an engineer onsite is the best course of action, a Cisco service engineer may be dispatched onsite, subject to a separate service contract purchased by Customer for such effort.
- Escalation response – Where resolution of the Incident becomes protracted, Cisco and Customer will follow the escalation procedure and timescales specified in Section 0 of this document.

Incident Resolution Process

Cisco will work on Incidents that are Priority 1 on a 24 x 7 basis until the Incident is resolved or a workaround is applied such as to downgrade the Incident to a lower Priority value.
Incidents that are Priority 2 will be worked on continuously during business hours. Incidents that are Priority 3 or Priority 4 will be worked on during business hours as required.
An Incident is considered resolved if the Video Service impact can no longer be classified in accordance with the priority definitions in Section 0.
The escalation management process assists with providing available resources to resolving any Incident.

Escalation Key Contacts

The following escalation process applies for Priority 1.

Table 2 Escalation Process – Priority 1 Incidents

Escalation Stage	Timing (T = Logging of Incident)	Cisco Contact	Customer Contact
First escalation	T + 8hrs	Support Manager	Technical Manager
Second escalation	T + 24hrs	Service Operations Manager	Technical Director
Third escalation	T + 48hrs	VP VCS	CEO/Board

Service Level Management

Service Reviews

Cisco and Customer shall conduct service review meetings at agreed upon intervals, as well as on demand (by conference call) in case of the need for escalation following a particular Incident, in order to find ways of improving collaboration and quality of the Support Service. The Service Review participants should include both technical and managerial representatives from Cisco and Customer.

Exceptions

The Support Services shall not include the correction of any Incident due to:

- Customer's neglect or misuse of the System or its failure to operate the System for the purposes for which it was designed;
- Any accident or disaster affecting the System including without limitation fire, flood, water, wind, lightning, transportation, vandalism or burglary;
- Customer's failure, inability or refusal to afford Cisco's personnel access to the System;
- Any fault in any attached or associated third party equipment (whether or not supplied by Cisco or forming part of the System);
- The provision, renewal or repair of supplies for use in association with the System;
- Sending non-compliant data to any interface of the System

Additional Obligations of Customer
In addition to any obligations noted previously, Customer shall also:

- Maintain the Data Plane location/s in a manner consistent with the specific site requirements identified during system delivery and generally provide a suitable environment for the operation and maintenance of the System, cables and fittings associated therewith and the electricity supply at the Data Plane location(s). To this end, Customer shall observe such reasonable directions with respect to the operating environment of the System as Cisco may specify from time to time.
- Provide Cisco with all reasonable co-operation to facilitate Cisco's efficient discharge of its obligations under these Support Services and, in particular, but without limitation, provide accurate information concerning the System, make available Customer owned spares, and any other matters arising that Cisco reasonably considers pertinent to its provision of the Support Services from time to time.
- Take all reasonable precautions to safeguard the health and safety of Cisco staff and sub-contractors whilst working with the System or any other equipment, which belongs to Customer or is located at any of the Live Video Environment location(s).
- Keep and operate the System in a proper and prudent manner in accordance with Cisco's operating instructions and ensure that only competent trained employees are allowed to operate the System. System operation includes the day to day exercising of the system APIs, either via automated interfaces or supplied user interfaces, in order to modify the system data to effect changes based on business requirements. Examples of this would include adding new linear content, defining new offers, updating channel logos etc.
- Implement data-security for the network and its interface with the Cisco components.
- Ensure any necessary support agreements are in place for third party equipment.
- Be responsible for renewal of third party support contracts on-going.
- Provide remote access (VPN) to the System for Cisco personnel.
- Certify that only Cisco-trained personnel, or persons working under their direct supervision, shall be responsible for diagnosing Incidents.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA CXX-XXXXXX-XX 05/16