Public IaaS Services Description

This Public IaaS Service Description (this "**Service Description**") describes generally the features of Cisco's public IaaS offering ("**Public IaaS**"). Information on Cisco's Public IaaS pricing, including pricing for the features described in this Service Description, can be found at Public IaaS pricing. Capitalised terms used but not defined herein have the meanings set forth in the Terms of Use for Cisco IaaS (the "**Terms**"), available at http://www.cisco.com/web/about/doing_business/legal/isb1_xaas_customer_tc/index.html. Cisco may amend this Service Description from time to time by posting the updated version of this Service Description at this URL or otherwise providing notice to Client.

> **Note:** This Service Description may provide links to documents and web pages that contain additional detail on matters described herein, such as technical specifications and documentation for specific Public IaaS features (each, a "**Supplemental Document**"). All Supplemental Documents are provided on an "AS IS" basis and for reference purposes only, and are subject to change from time to time by Cisco (for example, when Cisco modifies Public IaaS features). Nothing in any Supplemental Document creates or comprises, or is intended to create or comprise, a representation, warranty, covenant or obligation of Cisco, and except as otherwise expressly provided herein, no Supplemental Document is deemed to be part of or incorporated by reference into this Service Description or the Terms.

1. Public IaaS Summary

1.1 Public IaaS is comprised generally of servers, storage and network elements coupled with virtualisation technology and operating system (OS) software. Public IaaS seeks to provide Client with a segmented hosting environment with virtual server, virtual storage and virtual network elements that are logically isolated from those of other Cisco clients and customers, even though such elements may be running on the same physical infrastructure. Public IaaS is intended to allow Client to create separate "accounts" for Client's internal departments (each, a "**Department**"), allowing such Departments to be logically separate and enabling Client to take advantage of separate metering and usage tracking for charge-back purposes.

2. Public IaaS Details--Elements of Public IaaS

2.1 Public IaaS is comprised of the following:

(a) Cloud Networks

Public IaaS provides Client with the ability to provision Client-specific layer 2 virtual Local Area Networks (VLANs) (each, a "**Cloud Network**"). Client can then use Cisco's Cloud Control software to automatically deploy virtual cloud servers ("**Cloud Servers**," described in more detail below) on Client's Cloud Network(s). Client may deploy multiple Cloud Networks using Public IaaS. Each Cloud Network is initially isolated from other Cloud Networks from a network perspective, but can be configured to communicate with other Cloud Networks and the public

Internet by an Authorised User. Each Cloud Network includes firewall and load balancing capabilities, and can be independently customised based on Client's specific needs. Public IaaS can be used to build multi-tier Cloud Network architectures to separate data tiers from front-end web tiers, thereby providing an additional layer of firewall rules to help protect sensitive data.

Cloud Networks are deployed and managed either through the Management Portal or through corresponding functions of the Representational State Transfer (REST)-based application programming interface (API) provided by Cisco (the "**Cloud REST API**").

Each Cloud Network is provided with its own range of private IP addresses with the goal of isolating the Cloud Servers deployed within such Cloud Network from the public Internet. Cloud Servers are assigned private IP addresses from within such range by Authorised Users when they are deployed within a Cloud Network, and can be made accessible to the public Internet when the Authorised User specifically enables such access. All private and public IP addresses for Cloud Networks and Cloud Servers are provided by Cisco, and, as between Cisco and Client, are solely the property of Cisco.

Additional features available from Cisco include:

(i) One primary administrative account (the Administrator, as described in clause 6.1 of the Terms).
(ii) The ability to create multiple sub-administrator accounts (Sub-Administrators, as described in clause 6.1 of the Terms). Client can create unlimited Sub-Administrators, however, only one hundred (100) Sub-Administrators can log in concurrently.
(iii) Private IP addresses for each Cloud Server, with the ability to enable communication across Cloud Servers located on the same Cloud Network.
(iv) Two (2) public IP addresses per Cloud Network, with the ability to add additional public IP addresses.
(v) Virtual private network (VPN) access to manage Cloud Servers on Client's Cloud Networks.
(vi) Customizable ACL-based firewall rules to help control access into each Cloud Network.
(vii) NAT and VIP functions to expose private IP addresses to the public Internet.
(viii) VIP functions to help support load balancing and port translation across multiple Cloud Servers, with the ability to take Cloud Servers in and out of service based on Client-defined monitoring probes.
(ix) Layer 2 multicast support.

(b) Cloud Servers

Each Cloud Server is required to be provisioned with one (1) OS. Client can elect to have Cisco provide OS images for its Cloud Server deployments, and to provide corresponding OS licenses, within the Public IaaS infrastructure. The complete list of operating systems currently supported by Cloud Servers on Public IaaS is available at http://www.dimensiondata.com/Services/CloudServices/Community/SupportedOS. Client is

responsible and liable for all Client-provided software, including Client Applications, that are loaded, installed and/or operated by or on behalf of Client on Cloud Servers.

In addition, Cisco makes available certain optional third-party application software for installation onto Cloud Servers. A complete list of such third-party software is available at http://www.dimensiondata.com/Global/Services/Cloud-Services/Pages/Technical-Specifications.aspx.

Public IaaS seeks to provide Client with granular control over the configuration of Client's Cloud Servers. Client can control the number of virtual central processing units (CPUs), the amount of random access memory (RAM), and the amount of local storage allocated to each Cloud Server. As with Cloud Networks, Cloud Servers are deployed and managed either through the Management Portal or through corresponding functions of the Cloud REST API.

Additional features available from Cisco include:

(i) Cloud Server management capabilities, including start, shutdown, reboot, power off, restart, delete, add local storage and change CPU/RAM.
(ii) Static private IP addresses assigned to each Cloud Server, accessible via VPN. These private IP addresses can be mapped to static public IP addresses if an Authorised User makes the applicable Cloud Server(s) accessible to the public Internet.
(iii) Role-based administration control, through which Sub-Administrators can manage specific Cloud Servers, Cloud Networks, images and reports.
(iv) The ability to duplicate (clone) Cloud Servers to create images that can be used to deploy copies of Cloud Server configurations.
(v) Capability to import/export Cloud Server images.

(c) Cloud REST API

Public IaaS provides Client with Cloud REST APIs, which are intended to allow Client to control most aspects of Client's Cloud Servers and Cloud Networks. The Cloud REST API is described in further detail in Cisco's Cloud REST API specification, available at http://www.dimensiondata.com/Global/Services/Cloud-Services/Pages/API.aspx.

(d) Cloud Files

"**Cloud Files**" is an API-based file storage solution, intended to allow Client to store and retrieve its data from supported Internet-connected devices. Cloud Files storage is designed primarily for archiving and similar purposes and is not connected to Cloud Servers. Note: Cloud Files storage is provided solely in the United States, even if the Geography in which Client has allocated the majority of Client's IaaS resources is not within the United States. All data stored in a Cloud Files storage account is transferred to the United States.

Client may create multiple Cloud Files storage accounts, each with its own administrative password, allowing the creation of isolated virtual storage units. Each Cloud Files storage account can be configured to store up to ten (10) terabytes (TB) of data.

Cloud Files features include:

(i) Access to and management of Cloud Files accounts through the Management Portal and Cloud REST API.
(ii) Ability to set storage quotas and control Sub-Administrator access on a per-Cloud Files account basis.
(iii) Use of 256-bit AES encryption for each stored file, with SSL encryption for files in transit.
(iv) Ability to programmatically access the contents of Cloud Files accounts from anywhere on the Internet via the Cloud REST API.
(v) Compatibility with third-party WebDAV clients.
(vi) Interoperability mode for compatibility with Amazon S3-style API calls.

Once created, Cloud Files accounts are managed through the Cloud REST API, which provides control over the content of such Cloud Files accounts, including:

(i) Read, write, delete and restoration of files and containers.
(ii) MetaContainers support for cross-container views of specific file types such as documents, videos and images.
(iii) Permission controls to allow files and containers to be shared across multiple Cloud Files counts.
(iv) Tagging of one or more files or containers.
(v) Creation, deletion and management of Cloud Files accounts.

Additional Public IaaS Features

2.2 In addition to the features discussed above, Public IaaS provides the following features:

(a) Reporting

Public IaaS provides metering, usage tracking and reporting for Client on a per-Department basis.

(b) Security

Public IaaS is designed to provide flexibility to configure Client's environment to its needs, and several elements described elsewhere in this Service Description (e.g., the initial isolation of Client's Cloud Network) are intended to support security. However, Client remains responsible for overall security, including Client's network configurations for the underlying Cloud Network and Cloud Servers. Cisco strongly recommends that Customer employ appropriate encryption technologies to help ensure security of Customer data.

(c) Tech Ops

Client may elect to separately purchase Tech Ops as part of Public IaaS. Tech Ops, and certain additional terms and conditions governing Tech Ops, are described in further detail in the Tech Ops Service Description, available at http://cloud.dimensiondata.com/saas-

solutions/services/operational-services/technical-operations (hereby incorporated herein by this reference), as updated by Cisco from time to time.

Geographies

2.3 Public IaaS is available in the Geographies and Locations listed in the table below; the locations in the "Location" column of the table are the Locations available for the applicable Geography. Client's initial Geography is indicated in the applicable Order and Client may use any Location that is available in such Geography when Client logs into the Management Portal. Thereafter, Client may elect to enable additional Geographies and use additional Locations as described in and subject to Section 17 of the Terms.

Geography	Location(s)
Public IaaS North America	Santa Clara, CA
	Ashburn, VA
Public IaaS Europe	Amsterdam
Public IaaS Australia	Sydney
Public IaaS MEA	Johannesburg
Public IaaS Asia Pacific	Japan, Hong Kong

Service Levels for Public IaaS

2.4 The Service Levels and Service Level Credits applicable to Public IaaS are described in the Public IaaS Service Level Terms document, available at http://www.cisco.com/web/about/doing_business/legal/isb1_xaas_customer_tc/index.html (hereby incorporated herein by this reference), as updated by Cisco from time to time. Note: Service Levels and Service Level Credits do not apply to Tech Ops.