Service Level Agreements

Contents

1. Overview

This Service Level Agreement ("SLA") defines McAfee's service level commitments in the delivery of specified Cloud Services to our Customers. It describes the methods for measuring service level attainment and the exclusive remedies available to Customers if commitments are not met.

2. Definitions

A. Customer. McAfee customers with current and valid contracts for one or more Service.
B. Service. McAfee Cloud Service offerings that have been assigned specific service levels within this SLA.
C. User. A unique individual person within a company, organization, or other entity that is a Customer.
D. Management Access. Access to the cloud console.
E. Inline Traffic Data Path. Duration of filtering in the Service after the last byte received from the server.
F. Inline (block) - Web proxy doing inline block of traffic per policy.

3. Service Availability

A. Availability. The Availability of a Service is the percentage of time a Service's specified functionality is generally operating as described in the applicable and

current documentation. Services achieving Availability, as calculated and described in section 3 have met the prescribed service level.

The Services Availability is defined as follows:

Service	Covered Functionality	Availability SLA
Web Gateway Cloud Service	Inline Traffic Data Path-Availability	99.999%
	Management Access	99.900%

B. Availability Calculation. Availability will be calculated per calendar month and shall be measured using industry standard monitoring tools/software. Availability will be calculated as follows:

$$\frac{Total\ Min. - NonExcused - Excused\ Outages}{Total\ Min. - Excused\ Outages} * 100) \geq (99.999\%\ general\ availibility)$$

- "Total Min." means the number of minutes for the calendar month.
- "Non-Excused" means unplanned downtime, in minutes.
- "Excused Outages", in minutes, means the service will be unavailable for any downtime or outages relating to: (i) a Customer Outage Event, (ii) equipment, applications, interfaces, integrations, or systems not owned by McAfee, or service not offered by McAfee or (iii) a Force Majeure Event.
- "Customer Outage Event" means a period of time in which Service is not available due to acts, omissions or requests of Customer, including without limitation (a) configuration changes in, or failures of, the Customer end of the network connection, (b) work performed by McAfee at Customer's request, or (c) Customer's unavailability or untimely response to incidents that require its participation for source identification and/or resolution
- Availability Calculation Example:
  August has 31 days, or 44,640 minutes, of potential availability (Total Min.)

  One hour of scheduled maintenance was performed (Excused Outage).

  44,640 min. – 60 min. = 44,580 min.
  (This is the denominator and represents total potential availability for August).

  One minute of service interruption was experienced (unexcused outage).
  44,580 – 1 = 44,579 min.
  (This is the numerator and represents the total availability for August.)

  Availability= (44,640 – 1 – 60) / (44,640 – 60) * 100 = 99.997%

C. Partial Subscription Months. For any partial calendar month during which Customer subscribes to the Service, general availability will be calculated based on the entire calendar month, not just the portion for which customer subscribed.

D. Availability Restrictions. This Availability SLA does not apply if: (a) Customer fails to correctly configure the Service in accordance with McAfee policies or instructions; (b) failures in Customer equipment or third party computer hardware, Software, or network infrastructure not within the sole control of McAfee; (c) failure of Customer's network to forward traffic to the Service; (d) the unavailability of a specific third party web page or data center outage outside of McAfee's networks or data centers; (e) failure of an intermediate ISP (other than McAfee direct ISP(s)) to deliver traffic to McAfee; (f) unavailability of one or more specific features, functions, or equipment hosting locations within the Service, while other key features remain available; (g) actions or inactions of Customer (unless undertaken at the express direction of McAfee) or third parties beyond the control of McAfee; or (h) Customer requests for additional configuration or system changes that require downtime to complete.

E. Force Majeure. McAfee is not responsible for, and this SLA does not apply to, any Availability issues caused by circumstances beyond McAfee´s control, including, without limitations, acts of God; acts of government; flood; fires; earthquakes; civil unrest; acts of terror; strikes or other labor problems (excluding those involving McAfee employees); overall internet congestion, slowdown or unavailability; computer or telecommunications failure or delays involving hardware or software not within McAfee possession or reasonable control, and network intrusions or denial of service attacks.

4. Web Gateway Cloud Service Latency

A. Latency. Latency means the web page load time attributable to the Web Protection Service ("Latency").
B. Average Latency. Average Latency means the average time it takes for the Web Protection Service to scan, process and apply the Customer policy to the web content data, assuming a 100KB web page, as measured by the monthly average among samples taken by McAfee in a given month using industry standard monitoring tools/software ("Average Latency"). ("Average Latency"). Average Latency does not include: (a) traffic that is SSL-intercepted; (b) traffic not related to streaming applications; (c) traffic not subject to bandwidth management rules (QoS enforcement); or (d) the time required to download the web page from the origin content server (OCS) to the Web Protection Service. The processing of content is measured from when the Web Protection Service proxy receives the content to the point when the Web Protection Service proxy attempts to transmit the content.
C. Latency Commitment. McAfee will deliver the Web Protection Service with an Average Latency of 100 milliseconds or less ("Latency Commitment"). The Latency Commitment is only applicable to reasonable number of Transactions/Data Packets per User (based on McAfee cloud-wide average).

5. SLA Restrictions

A. The service levels are based upon Customer use of a configuration that is at least as protective as Service default settings. For clarity, McAfee is not responsible, and this SLA does not apply, if Customer configuration does not meet or exceed the protections provided by the default settings.
B. McAfee is not responsible, and this SLA does not apply, if Customer configuration is unsupported.
C. This SLA does not apply to Web Gateway Cloud Service Customers who use a proxy IP address rather than the supported Global Routing Manager (GRM) hostname (i.e. c<customer-ID>.saasprotection.com).
D. Site to Cloud VPN is restricted to static IP Addresses or valid DNS names, and it is the Customer's responsibility to configure their own Firewall or Router and establish at least two separate VPN tunnels to the Cloud to achieve High Availability.
E. This SLA does not apply to Beta Services or if Customer is receiving Service under an Evaluation Agreement or if the Customer is otherwise receiving the Service for free (such as Free Services, as defined in the Cloud Terms of Service).
F. This SLA does not apply if Customer is using Services in violation of the McAfee Cloud Services Agreement, Standard Support Terms and Conditions, Acceptable Usage Policy or other McAfee Cloud Service subscription agreements.
G. This SLA does not apply if Customer was contracted for, but not actively using, the affected Service at the time of an incident covered by the SLA.
H. The Service does not include the customer's internet access connections or hardware on the customer's side to access the internet or the Service. This SLA does not cover any issues arising from the compatibility of the customer's hardware or the software used to connect to the Service.
I. For hybrid SKUs that include entitlement to both Cloud Services and appliance (including virtual) form factors, this SLA only applies to the Cloud Service component within the hybrid SKU, and does not apply to any other product or service.
J. SLA, and the services it covers, is subject to the McAfee End of Life process.
K. Pervasive Data Protection Connector SLA does not apply if the third party service to which we connect is not available or makes changes to is service or API

Unless specifically stated herein, this document does not replace, modify, or in any way restrict other McAfee terms and conditions that may apply, including:

- Standard Support Terms and Conditions: http://www.mcafee.com/us/resources/misc/mfe-techsupport-terms.pdf
- McAfee Cloud Services Agreement: https://www.mcafee.com/us/resources/legal/cloud-terms-of-service-agreement-en-us.pdf

6. Customer's Responsibilities

A. The customer is required to use, configure, deploy and manage the Service in accordance with the McAfee Cloud Services Agreement, and according to the documentation, including Knowledge Based articles and other online content on public Community, such as but not limited to the expert center on

www.mcafee.com/expertcenter, that is made available to the customer upon purchasing the usage rights for the service.

B. Customer is responsible for failures of the equipment or software used to access the Service.
C. The customer commits to using the Service based on the published individual proxy name per the documented terms and conditions. The customer will use IP addresses in their configuration to access the proxy unless explicitly documented.

7. Service Credits

A. Sole Remedy. Customer's **sole remedy** for breach of this SLA is the receipt of Service Credits, as defined below.
B. Service Credit Defined. A Service Credit is the number of days of the relevant Service that will be added to the end of the Customer's current contract term as a result of a breach of this SLA. The number of days awarded as a Service Credit is as follows:

Web Gateway Cloud Service Level Credits				
Inline Traffic Data Path-Availability	Inline Traffic Data Path-Performance	Management Access	Rating	Service Credit Number of Days
>= 99.999%	<100ms	>= 99.9%	Meets Goals	None
<99.999% but >= 99.99%	>100ms but <= 200ms	<99.9% but >= 99%	Tolerable	8 days
<99.99% but >= 99%	>200ms but <= 300ms	<99% but >= 98%	Less Tolerable	16 days
<99%	>300ms	<98%	Unacceptable	31 days

8. Claims Process

A. To initiate a Service Credit claim, the customer must contact McAfee and provide the following information: McAfee Grant Number, date and time of the service interruption, and a brief description of the event. Claims must be received by McAfee within **ten (10) business days** of an event. If confirmed by McAfee, service will be applied within 60 days of McAfee's receipt of the Customer credit request. Credits are not refundable and can be used only towards future billing charges.

9. Revision History

Version Number	Revision Date	Revision Description	Revised by
1	15-Mar-2017	Initial version	R. Manning
2	18-May-2017	Terminology changes, Revision history added	R. Manning
3	23-May-2017	Formatting changes	R. Manning
4	28-Jul-2017	Product updates	R. Manning
5	21-Feb-2018	Data Path Performance update	R. Manning
6	4-Sep-2018	Included SLA example, removed CTD (end of life)	R. Manning