CenturyLink Technology Solutions

CenturyLink Technology Solutions Service Guide

Web Security Services 2.0

This CenturyLink Service Guide ("SG") sets forth a description of Threat Management Service ("Service") offerings by CenturyLink, including technical details and additional requirements, if any. This SG is subject to and incorporated into the Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG.

Version	Previous	Section Modified	Date
SEC-20140909-SG-WebSecurityServices	SEC-20091208-External-SSG-GL-Web Security Services	All	September 9, 2014

Table of Contents

Service Description

1. **Standard Solution Description**: The Web Security Service provides protection against Virus and Spyware, as well as providing URL and content filtering of network traffic**.** The Services are provided on a per User basis. The Service is cloud-based and can be delivered with minimal changes to the Customer's system configuration and require no additional Customer-side hardware or software. Web Security Services is a fully managed, cloud-based offering. The standard features of the Service consist of installation, configuration, administration, monitoring, maintenance and support consisting of the components listed in 1.1. The Service Level Agreement (SLA) associated with this service guide can be found in Appendix A.

   1.1. **Service Components**

      1.1.1. **Web Protection: Anti-Virus; Anti-Spyware:** Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Service. The Service will scan the first 50Mb of each file transfer for viruses and Spyware. Outbound communications passing through the proxy will be examined to determine if it represents Spyware communication. Where this is identified it will be blocked. When files are downloaded that exceed 50MB in size, the initial 50MB will be scanned and the remainder passed through if no infections are found in the initial 50Mb.

      1.1.2. **Network-Based URL Filtering:** Customer's external HTTP and FTP-over-HTTP requests are directed through the Service. Customer can implement policies based on URL categories, content types and file types. The Service allows Recreational Access at different times during the day and creation of multiple policies. Customer has access to activity reporting and can customize alert pages.

   1.2. **Installation**: CenturyLink will provide installation tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

      1.2.1. Installation of the Services will be completed within five (5) normal working days of receipt by CenturyLink of completed installation forms. Installation will include a scan of Customer's E-mail systems to detect for open relay configuration.

   1.3. **Configuration**: CenturyLink will provide configuration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

      1.3.1. **Configuration for Web Security Services**: include one IP or IP range as part of the original Agreement (IP or IP ranges can be added or changed during the life of the contract).

      1.3.2. **URL Filtering Policies:** Customers have the ability to configure their URL filtering policies via the Service Management Console user portal. Within the policy manager in the Service Management Console, different policies can be created to match web-browsing requirements.

      1.3.3. **Access**: Access to the Service is restricted via Scanning IP, i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the customer and dynamically select customer-specific settings.

   1.4. **Administration:** CenturyLink will provide administration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

      1.4.1. **System Administration:** CenturyLink will manage all system administration and passwords. Customer will not have access to passwords or be able to make direct changes to the configuration. Instead, Customer must request changes by contacting the CenturyLink Service Center. Customer must provide complete authentication credentials to the CenturyLink Service Center when requesting changes.

      1.4.2. **Passwords**: CenturyLink may manage all system administration passwords, including root level access, and may do so exclusively. In such case, Customer will not have access to system passwords nor able to make changes to the system configurations and must instead submit change requests to CenturyLink.

1.4.3. **Reconfiguration**: If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

1.5. **Monitoring:** CenturyLink will provide monitoring tasks marked with an ”X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.5.1. **Web Protection**: If a Customer’s web page or attachments are found to contain a virus (or are deemed unscannable, barring SSL traffic), access to that Web page or attachment is denied and the Internet user will see an automatic alert web page. Where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page, but access to the infected page or attachment will still be denied. The Web Protection Service will scan as much of the Web page and its attachments as reasonably possible. It may not be possible to scan certain Web pages, content or attachments (e.g., password- protected). Attachments specifically identified as unscannable will be blocked. Streamed and encrypted traffic (e.g., Streaming Media and/or HTTPS/SSL) cannot be scanned and will be passed through Web Protection unscanned.

1.5.2. **Network-Based URL Filtering**: If a User requests a Web page or attachment where an access restriction policy applies, then access to that web page or attachment is denied and the user will see an automatic alert web page in accordance with the specification below. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert web page, but access to the relevant page will still be denied.

1.6. **Maintenance and Support:** CenturyLink will provide maintenance and support tasks marked with an ”X” in the CenturyLink column in Table 1.0 Roles and Responsibilities.

2. **Customer Responsibilities:** Customer is responsible for all tasks marked with an ”X” in the Customer column in Table 3.0 Standard Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 3.0 may result in CenturyLink’s inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer’s failure.

2.1. **Web Protection:** Customer is responsible for the following:

2.1.1. Maintain the configuration settings required to direct external traffic to Service.

2.1.2. Ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via the Service.

2.1.3. Maintain the configuration settings required to not direct external traffic via Service for Internet services that mandate based on Customer needs direct connection (i.e. not via Service) to the Internet.

2.1.4. Configure the web URL to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Users or groups

2.2. **Network-Based URL Filtering:** Customer is responsible for the following.

2.2.1. Maintain the configuration settings required to direct external traffic to Service.

2.2.2. Ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via the Service.

2.2.3. Maintain the configuration settings required to not direct external traffic via Service for Internet services that mandate based on Customer needs direct connection (i.e. not via Service) to the Internet.

2.2.4. Configure URL filtering policies via the user portal.

2.3. **Use of Third Party Software:** If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third

party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

2.4. **Passwords and Access:** Customer shall (a) provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service; (b) not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink; (c) notify CenturyLink at least five (5) business days in advance of any changes that may affect the applicable Service (e.g., infrastructure, network topology changes); and (d) designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means an English-speaking technical point of contact available 24 x 7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems. Provision of the Service is subject to Customer's compliance with this Section.

3. Additional Terms:

3.1. **Web Protection**: NO WEB SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE CENTURYLINK DISCLAIMS ANY LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE WEB PROTECTION SERVICE TO DETECT VIRUSES AND/OR SPYWARE. CenturyLink emphasizes that the configuration of Web Protection is entirely in the control of the Customer. The services described in this SG are intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel, and so CenturyLink advises the Customer to always check their local legislation prior to deploying Web Protection Services. The Web Protection Service will scan as much of the Web page and its attachments as reasonably possible. It may not be possible to scan certain Web pages, content or attachments (e.g., password- protected). Attachments that cannot be scanned will be blocked. Streamed and encrypted traffic (e.g., Streaming Media and/or HTTPS/SSL) cannot be scanned and will be passed through Web Protection.

3.2. **Network Based URL Filtering:** NO WEB SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE CENTURYLINK DISCLAIMS ANY LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF NETWORK-BASED URL FILTERING TO DETECT BLOCKED URLs OR CONTENT. CenturyLink emphasizes that the configuration of Network-Based URL Filtering is entirely in the control of the Customer. The services described in this SG are intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel, and so CenturyLink advises the Customer to always check their local legislation prior to deploying Network- Based URL Filtering.

3.3. **Incompatibility:** The Services do not include the development of a comprehensive change control process. There may be incompatibilities between a Service and particular Customer environments, which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party's obligations with regard to unaffected environments.

3.4. **Pricing**: The Services are priced on a per User basis. Setup fees for Web Security Services include one IP or IP range as part of the original order. IP charges are assessed for IP or IP ranges added or changed during the life of the contract. Multiple users accessing the same machine are not treated as an exception. Any combination of Web Security Services must be purchased for Users in proportionate amounts; i.e., an order of Web Anti-Spyware and Anti-Virus Protection for 50 users combined with Web URL Filtering requires 50 Web URL Filtering users.

Tables and Appendices

Table 1.0 Roles and Responsibilities

Activity	Task	CenturyLink	Customer
Installation	Perform an initial set-up consultation with the Customer	X	
	Develop the Customer's alert policy, determine the appropriate response procedure, and answer Customer's questions regarding service	X	
	Verification that device configuration adhere to the Customers organizations security policies.		X
	Provide all required information during initial consultation		X
	Install and configure the system, apply the initial policy of the device, and set the device to a 'burn in' status for a minimum period of one week	X	
	Evaluate the alert traffic for false alarms and make appropriate recommendations for policy tuning	X	X
	Make required adjustments to the policy as necessary following the burn-in period; set device to full monitored status	X	X
Configuration	Configure alert policy and response procedures for Customer	X	X
	Perform a security review of the Service configuration, rule-set, make recommendations for improvements	X	X
	Make configuration changes to direct external traffic via Service. Make configuration changes to exclude sending traffic via Service where a direct connection is mandated by Customer rather than a proxy to Service		X
	Authentication and configuration of username and password using CenturyLink's managed Microsoft Active Directory services for Customers using Managed Hosting services within a CenturyLink data center.	X	
	Configure URL filtering policies via Service Management Console user portal		X

Activity	Task	CenturyLink	Customer
Administration	Request access restriction to a Web page or attachment		X
	Change policy rules after appropriately approved via the Customer's change management process.	X	
	Configure WebURL to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Users or groups.		X
	Create different policies within the policy manager in the Service Management Console to match web browsing requirements.		X
	Provide an explanation of the alert reports and statistics provided on web portal	X	
	Provide support for 24x7x365 end user administration requests by CenturyLink system administrators for Customers using Managed Hosting services within a CenturyLink data center.	X	
Monitoring	Receive and review alerts on Service Management Console		X
	Set-up automatic alert Web page in accordance with Customer specifications	X	
Maintenance and Support	Patch devices as required or when the Customer requests for a specific patch that has been approved by CenturyLink product team.	X	
	24/7 support for problem resolution and Customer inquiries.	X	
	Provide vendor based maintenance / support contracts to enable code updates and patches	X	
	Notify Customer via phone and/or email and initiate corrective action in the event that System fails to respond	X	

Appendix A Service Level Agreement

SLA Process

Customer must request any credit due hereunder within 30 days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this 30 day period. Credits will be issued once validated by CenturyLink and applied toward the invoice which Customer receives no later than two months following Customer's credit request. All performance calculations and applicable service credits are based on the records and data of CenturyLink or its partners/vendors.

The applicable SLA provides Customer's sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind. The SLA and any remedies hereunder will not apply and Customer will not be entitled to receive a credit in the case of an Excluded Event. "Excluded Event" means any event that adversely impacts the Service that is caused by (a) the acts or omissions of Customer, its employees, customers, contractors or agents; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink; (c) Force Majeure events; (d) scheduled maintenance; (e) any suspension of Service pursuant to the Agreement; or (f) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information.

Web Security Service Availability SLA

"Service Availability" means the availability of the Customer's designated Web Services primary or secondary infrastructure to accept the Customer's outbound web requests from a correctly configured Customer host on behalf of the Customer on a 24x7 basis, subject to correct configuration by the Customer of their hosts or gateway devices or proxy(s) as per CenturyLink's guidelines (available upon request). Measurement of Service Availability will be via the third party tracker system.

In the event that Web Service Availability is below one hundred percent (100%) in any given calendar month, the Customer's sole and exclusive remedy shall be a service credit calculated in accordance with the Table 2.0. In no event will the credits accrued in any single month exceed, in the aggregate across all incidents, one hundred percent (100%) of the invoice amount for the affected Service. Please refer to Table 2.0 for Percentage Availability figures regarding this Service.

Table 2.0 Service Calculations

Percentage availability per calendar month	Percentage credit of monthly charge for affected service
< 100% but >= 99.0%	20
< 99.0% but >= 98.0%	40
< 98.0% but >= 97.0%	60
< 97.0% but >= 96.0%	90
< 96.0% but >= 95.0%	100
< 95%	Termination of Web Services without liability for early termination charges at Customer's discretion

Definitions

CenturyLink Service Center: The primary organization for resolving infrastructure issues that is staffed 24/7/365 to respond in a timely manner to incidents and requests pertaining to Customer IT infrastructure.

File Transfer Protocol (**FTP**) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network (ie: the Internet).

Hypertext Transfer Protocol (**HTTP**) is structured text that uses hyperlinks between nodes containing text. HTTP is the application protocol for distributed, collaborative, hypermedia information systems that is also the fundamental basis of data communication on the Internet and is the protocol to exchange or transfer hypertext.

Maintenance Windows: A period of time designated in advance by CenturyLink, during which preventive maintenance that could cause disruption of service may be performed. Current Scheduled Maintenance windows are:

- Americas: Saturday 00:00AM to 5:00AM; Sunday 00:00AM to 5:00AM
- EMEA: Saturday 02:00AM to 6:00AM
- APAC (Except Japan): Saturday 21:00 (GMT) AM to Sunday 01(GMT)
- Japan: Sunday 04:00 (JST) to 8:00 (JST)

Service Management Console (SMC) - Each Service Management Console, as applicable, is an Internet-based resource and tool available to Customer as part of a Service. Customer can access the SMC by using a secure password protected login. The SMC provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service(s). A Customer may have access to multiple SMCs to manage different Services (e.g., ClientNet).