CenturyLink Technology Solutions

CenturyLink Technology Solutions Service Guide

Email Protection Services 2.0

This CenturyLink Service Guide ("SG") sets forth a description of Email Protection Services 2.0 ("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-20140922-SG-EmailProtectionServices2.0	SEC-20140430-SG-eMailProtectionServices	All	September 22, 2014

CenturyLink Technology Solutions
www.centurylink.com/technology

Town & Country, MO 63017
Office: 314.628.7000

Table of Contents

Service Description

Service Description: Email Protection Services 2.0 is a CenturyLink service provided in the cloud (the "Service"). The standard features of the Service consist of the installation, configuration, administration, monitoring, and maintenance and support for the elements listed in section 1.1. The Customer can choose one or more of the four distinct Email Protection Elements located in table 2.0 Email Protection Service Description at the time of purchase. The Services are not subject to any SLA. As a target for the level of service to be expected, the processing time for 99% of E-mails processed, including inbound queuing, routing and scanning, is typically 30 seconds or less, with the remaining 1% being processed within 10 minutes.

1.1. **Service Elements**

1.1.1. **E-mail Anti-Virus Protection (AV):** AV is a fully managed Service that can be switched on with minimal changes to the Customer configuration and no additional Customer-side hardware or software. Once AV is activated, all inbound and outbound email is re-routed and scanned by scanners before being passed on to its final destination.

1.1.1.1. **Virus Detection:** If a virus is detected, the infected email is automatically routed to a secure server, where it is held in quarantine for a number of days (based on user configuration via a Customer Portal), after which time the email is destroyed.

1.1.1.2. **Alert Notification:** The sender and email administrator receives immediate notification in the event of virus detection. Where a quarantined email is shown to be releasable on the Customer portal, a Customer may release it from the secure server to the originally intended recipient(s). The email will be released to the first address of the original recipient list (if this address is a group email name or alias, the email will be released to all addressees in the group or alias).

1.1.1.3. **Infected E-mail Redirection:** AV can redirect the infected email to an alternate address within 8 normal working hours of receipt of a "Release Authorization Form" from Customer. Emails containing a particularly infectious or damaging virus may not be releasable, in which case Customer will receive notification through the Customer portal. In the case of a major breakout of a new virus, an alert message is posted on the Customer portal.

1.1.2. **Anti-Spam (AS):** AS identifies and blocks unsolicited commercial email. Customer selects the level and type of spam scanning and customizes white and black lists.

1.1.2.1. **Reporting:** CenturyLink provides the following reports analysis of spam patterns and other spam data collected by day, week, month or year.

1.1.2.2. **Spam Detection:** The Customer's inbound email is scanned. If an inbound email is suspected of being Spam, one or more actions are taken based on the configuration options selected by the Customer. Suspected spam will not be stored. AS is only available in user blocks of 25, and additional increments of 25.

1.1.3. **Image Filtering (IF):** IF uses neural network technology to accurately pornographic images.

1.1.3.1. **Reporting:** IF provides reporting patterns to alert staff of breaches in internal acceptable use policies. Options are available for specifying the level of detection sensitivity, from low to medium to high.

1.1.3.2. **User Blocks:** IF is available in user blocks of 25, and additional increments of 25. IF is only available to Customers who have purchased AV.

1.1.3.3. **Applicable Policies:** Customer determines actions to be taken upon the detection of a pornographic image. These options can be determined independently for inbound and outbound email. Action options for email detected as pornographic are: log only (provides statistics viewable via the Customer portal), tagging of suspect email within its header (for inbound email only), copying suspect email to a pre-determined email address, redirection of suspect email to a pre-determined email address or deletion of suspect email. Suspected pornographic images will not be stored.

1.1.4. **Content Control (CC):** Customers configure Rule-based filtering to support Customer's Acceptable Use Policy.

1.1.4.1. **Rule Creation:** Customer builds a collection of rules upon which incoming and outgoing email is filtered. CenturyLink enables Content Control for each of the Customer's applicable domains. The Customer is responsible for implementing the configuration options for Content Control. For each domain Customer may configure rules on a 'per domain', 'per group' or 'individual' basis, changes made by the Customer to the rules will become effective within 24 hours of such change being made. Options are available for defining the action to be taken upon detecting a suspected email. These options may be set independently for inbound and outbound email. These options are block and delete suspected email, tag (if inbound) and redirect suspected email to administrator, tag (if inbound) and copy suspected email to administrator, tag (if inbound) header of suspected email, compress email attachments and log only to InSight statistics.

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. **Supported Environments:** The Service supports any modern email servers that can forward email using common email MX records.

1.2.2. **Implementation:** Except as otherwise noted in this Service Guide, 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 email systems to detect for open relay configuration (see Additional Terms of Service below regarding prohibition of open relay).

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

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. **Passwords:** CenturyLink will manage all system administration passwords, including root level access. Customer will not have access to system passwords must submit change requests to CenturyLink.

1.4.2. **Access:** CenturyLink may require access to Customer's staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. 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.

1.4.3. **Reporting:** Through the portal, a Customer will be able to review the results of their Content Control rules in the form of daily, weekly, monthly and annual summaries organized by both rule and by User. Reports containing service activity logs can be generated on a weekly or monthly basis and emailed to the Customer upon request.

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

Notification: Emails containing a particularly infectious or damaging virus may not be releasable, in which case Customer will receive notification through the Customer portal. In the case of a major breakout of a new virus, an alert message is posted on the Customer portal. Customer will be provided with a unique user name and password for accessing the Customer portal in connection with the Services. Customer is solely responsible for maintaining the confidentiality of this information.

1.5.1. **Monitors:** All email is re-routed and inspected according to AV, AS, IF and CC rules setup by the Customer.

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.

1.6.1. **Tuning:** 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.

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. **Permissions:** Provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service

2.2. **Testing:** Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing or external network scans on CenturyLink’s network without the prior written consent of CenturyLink.

2.3. **Network Topology Changes:** The Customer must notify CenturyLink in advance of any network topology or system changes that may affect the Service or the effectiveness of the Service policy.

2.4. **Customer Contact:** 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 24x7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems.

2.5. **Confidentiality:** Customer is wholly responsible for maintaining the confidentiality of all email content, reports, and notifications.

2.6. **Third Party:** 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.

2.7. **Unsolicited Email:** Customer will not send unsolicited commercial email and flagged as a source of spam.

2.8. **Bulk Email:** Customer will not send bulk email (more than 500 email messages with substantially similar content, sent or received in a single operation or series of operations).

2.9. **Open Relay:** Customer will not support open relay within its email systems. Customer must ensure its server does not send or forward unauthenticated emails.

2.10. **Right to Refusal:** CenturyLink maintains the right to refuse or discontinue the Services to any Customer in violation of the obligations in this agreement. In the event that, after the initiation of service, Customer is found to be in violation of this agreement, and CenturyLink continues to provide the Services, Customer shall be responsible for the cost of any remedial work necessary as a result of such violation, at CenturyLink’s then-current rates for Professional Services.

3. **Additional Services:** At Customer’s option and expense Customer can choose to add the services listed below. The items can be added to the standard Service (described in Section 1.0) for an additional fee described in a separate Statement of Work (“SOW”) or Service Order. Contact a sales representative for additional information.

3.1. **Additional Domains:** Customer may add domains and/or user accounts that are being scanned to the Service.

3.2. **Changes to Ports and VLANs:** For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges.

4. **Additional Terms and Conditions**

4.1. **Suggested Words**: Suggested word lists supplied by CenturyLink's underlying vendor for the service ("Vendor") contain words that may be considered offensive. Customer agrees that neither CenturyLink nor Vendor shall have any civil or criminal liability in respect of any claim or action arising out of supply to the Customer of such word lists. Customer accepts and agrees that Vendor may compile and publish default word lists using words obtained from the Customer's custom word lists.

4.2. **Quarantine Action**: The Customer recognizes that if Content Control is used in conjunction with the quarantine action of the Anti-Spam service, this may result in suspected Spam being quarantined before it has been filtered by the Content Control service.

4.3. **Configuration**: CenturyLink emphasizes that the configuration of Content Control is entirely under the control of the Customer and that the accuracy of such configuration will determine the accuracy of the Content Control service, therefore neither CenturyLink nor Vendor shall have any liability for any damage or loss resulting directly or indirectly from any inaccuracy or mistake in configuration.

4.4. **Acceptable Computer Use Policy**: CenturyLink recommends that the Customer have an Acceptable Computer Use Policy (or its equivalent) in place governing its Users' use of email. 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 Content Control. Neither CenturyLink nor Vendor shall have any civil or criminal liability that may be incurred by the Customer as a result of the operation of Content Control.

4.5. **Upgrades:** CenturyLink may upgrade or revise the Service at any time for legal, safety, business, or technical reasons. CenturyLink will provide Customer with reasonable prior notice of any planned maintenance. In order to minimize disruption to the Service, planned maintenance will be carried out during periods of anticipated low E-mail traffic whenever possible, and E-mail traffic will be diverted around sections of the network not undergoing maintenance. Where emergency maintenance is necessary and is likely to affect the Service, CenturyLink will attempt to inform Customer beforehand, and in any event, will post an alert message on the Customer portal within one hour of the start of such emergency maintenance.

If, as a result of hacking attempts, denial of Service attacks, mail bombs or other disruptive activities either directed at or originating from the Customer's domains, CenturyLink determines, in its sole discretion, that continued provision of the Service to Customer may compromise the CenturyLink network, or affect the ability of CenturyLink or its vendors to provide the Services to other customers, CenturyLink reserves the right to temporarily suspend Service to the Customer. In such an event, CenturyLink will (i) promptly inform the Customer upon suspension of the Service, (ii) use commercially reasonable efforts to resolve such issues, and (iii) resume Service to the Customer as soon as CenturyLink determines that the threat has passed.

4.6. **Disclaimer:** CenturyLink does not make, and specifically disclaims, any guarantee or warranty that the Services will enable Customer to operate a completely virus, spam, and/or pornography-free environment within its email systems, or that the Services will result in identification of all email viruses or other destructive code, spam, or pornography.

4.7. **Additional Charges:**

4.7.1. **Service Requirements:** The Services are priced according to the number of domains being scanned. In the event that the actual number of domains being scanned exceeds the Customer's registered usage, fees may be adjusted accordingly.

Tables and Appendices

Table 1.0 Roles and Responsibilities

Activity	Task	CenturyLink	Customer
Installation	Provide all required information during initial consultation		X
	Perform an initial set-up consultation with the Customer	X	
	Develop the Customer's alert policy, determine the appropriate response procedure		X
Configuration	Configure alert policy and response procedures for Customer	X	
	Implement proactive deny rules as part of Email security configurations and requirement(s)	X	
	Configure rules on a 'per domain', 'per group' or 'individual'		X
	Determine configuration settings for Email Anti-Virus Protection (AV)		X
	Determine configuration settings for Anti-Spam (AS)		X
	Determine configuration settings consistent with Customer's applicable policies for Image Filtering (IF)		X
	Determine configuration settings for Content Control (CC)		X
	implement the configuration options for Content Control for each domain according to the Customer needs		X
Administration	Setup redirection rules for infected Emails		X
	Oversee Anti-Virus re-routing and scanning	X	
	Provide CenturyLink with all passwords, credentials, and required clearance credentials to carryout administrative tasks related to the Service		X
	Acknowledge all additional service terms and applicable conditions and fees related to the Service including Service exclusions and add-ons		X
Monitoring	Refer to the InSight portal to review Content		X

Activity	Task	CenturyLink	Customer
	Control policy rules and reports		
	Maintain the confidentiality of all email content, reports, and notifications		X
Maintenance and Support	Inform Customer beforehand when possible and post an alert message on the Customer portal within one hour of the start of such emergency maintenance.	X	
	24/7 support in CenturyLink Service Center for problem resolution and Customer inquiries.	X	
	Provide Customer with reasonable prior notice of any planned maintenance	X	
	Cooperate with CenturyLink to perform maintenance activity		X

Definitions

Anti-Virus Protection (AV): Inbound and outbound email is re-routed and inspected by four scanners for viruses

Anti-Spam (AS): Anti-spam refers to services and solutions that focus on blocking and mitigating the effects of unsolicited emails - or spam.

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.

Content Control (CC): Content Control allows for a collection of rules upon which incoming and outgoing email is filtered. A rule is an instruction set up by the Customer which is used to identify a particular format of message/attachment or content which has prescribed to it a particular course of action to be taken in relation to the email.

Image Filtering (IF): Image Filtering is a capability that detects certain type of images (e.g. pornographic images) and filters those images based on the set policies.

Local Area Network (LAN): A local area network (LAN) is a computer network that interconnects computers within a limited area.

Open Relay: An open mail relay is an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users.

Rule: A rule is an instruction set up by the Customer which is used to identify a particular format of message/attachment or content which has prescribed to it a particular course of action to be taken in relation to the email.

Virtual Local Area Network (VLAN)