Telemetry Data

https://campus.barracuda.com/doc/73719632/

To be able to continuously update and improve frequently used features based on real-world data, the Barracuda CloudGen Firewall sends performance and usage data to the Barracuda telemetry servers. Sending statistics is opt-out for new or freshly installed CloudGen Firewalls and opt-in for updated firewalls. After collecting data, the CloudGen Firewall starts one attempt to update the telemetry data via an HTTPS connection. If the connection to the update servers fails, no further attempts are made until the next day. A copy of all parameters sent to the telemetry servers is logged every time an update is initiated. The Barracuda Firewall Control Center sends data collected only on box level. No data from the Control Center layer is collected. For firewalls in the public cloud (AWS, Google, or Azure) telemetry can not be completely disabled, the minimal set of parameters is always transmitted.

Minimal telemetry parameters:

Name	Key	Value Type	Description
General Information			
Serial Number	sn	number	Serial number of the box
Model	appliance	type	The appliance type e.g. VM - vmware or F100 for a CloudGen F100
Virtual Subtype	virt_subtype	type	Information about the hypervisor
Firmware version	firmware	Version String	Version of the CloudGen Firewall firmware software
EU Expiration Date	euexpiration	Date	Expiration Date of the Energize Update
Services			
Virus Scanner	virscan	Enabed / Disabled	AV Scanner service installed
ATP	fwatp	Enabled / Disabled	ATP used in access rule(s)
IPS	ips	Enabled / Disabled	IPS detection enabled

Full telemetry parameter list:

Name	Key	Value Type	Description
General Information			
Serial Number	sn	number	Serial number of the box
MAC Address	mac	MAC address (hex format)	MAC address which was used for the license
Model	appliance	type	The appliance type e.g. VM - vmware or F100 for a CloudGen F100

Virtual Type	virt_type	type	Information about the hypervisor (VMware, Azure...)
Virtual Subtype	virt_subtype	type	Information about the hypervisor
DevMap	devmap	Text	Device mapping
Number of CPU's	numcpu	Number	Number of CPU's
Memory usage	memory	Percent	Percent of used memory
Swap usage	swap	Percent	Percent of used swap memory
Average CPU load	cpu	Float	15 Minutes CPU average load at the moment of collecting the data
Used Firmware partition	diskfirmware	Percent	Allocation of partition "/" in Percent
Used Data partition	diskdata	Percent	Allocation of partition "/phion0" in Percent
Firmware version	firmware	Version String	Version of the CloudGen Firewall firmware software
Uptime	uptime	Seconds	Box up time in seconds
Box location	country	Location	Location of the box if configured
Stand Alone / Centrally Managed	mcmanaged	Yes / No	Is box managed by a control center
EU Expiration Date	euexpiration	Date	Expiration Date of the Energize Update
EU Status	eustate	Status	Status of the Energize Update
License Staus	licstatus	Status	Status of the license
Services			
App Control	appcontrol	Status	Shows the status of Application Control (license and activation)
SSL Inspection	sslice	Enabled / Disabled	SSL Inspection for firewall service enabled
Port Protocol Protection	protocolprotection	Enabled / Disabled	Is protocol protection in the firewall service enabled

Google Safe Search	safesearch	Enabled / Disabled	Google Safe Search enabled
YouTube for Schools	ytforschools	Enabled / Disabled	Youtube for schools enabled
URL Filter	cofs	Enabled / Disabled	Webfilter serivce enabled
Virus Scanner	virscan	Enabed / Disabled	AV Scanner service installed
Virus Scan in Firewall	fwavscan	Enabled / Disabled	AV Scan used in access rule(s)
ATP	fwatp	Enabled / Disabled	ATP used in access rule(s)
HTTP Proxy	proxy	Enabled / Disabled	HTTP proxy service installed
HTTP Proxy mode	proxymode	Reverse / Forward / Transparent	HTTP Proxy mode
Proxy SSL Inspection	squidbump	Enabled / Disabled	SSL Intercept mode from proxy service enabled
DHCP Enterprise	dhcpe	Enabled / Disabled	DHCP Enterprise service installed
DHCP Relay	dhcprelay	Enabled / Disabled	DHCP relay service installed
SSH Proxy	sshprx	Enabled / Disabled	SSH proxy service installed
FTP Gateway	ftpgw	Enabled / Disabled	FTP Gateway service installed
OSPF Routing	ospf	Enabled / Disabled	OSPF service installed
Mail Gateway	mailgw	Enabled / Disabled	Mail Gateway service installed
SPAM Filter	spamfilter	Enabled / Disabled	Spamfilter service installed
DNS Service	dns	Enabled / Disabled	DNS service installed
IPS	ips	Enabled / Disabled	IPS detection enabled
IPS report only mode	ipsreportonly	Enabled / Disabled	IPS reporting only mode enabled
IPS Scan mode	ipsscanmode	Full / Fast / Auto	IPS scan mode
Stream Reassembly	streamreassmbly	Yes / No / Auto	Mode of the stream reassembly for the firewall service

RPC Tracking	rpc	Enabled / Disabled	RPC tracking enabled
Guest Access	guestaccess	Enabled / Disabled	guest access enabled
Audit Log	audit	Enabled / Disabled	Firewall Audit logging enabled
RCS	rcs	Enabled / Disabled	Version Control System for the Configuartion enabled
IPFIX Streaming	ipfixstream	Enabled / Disabled	IPFIX streaming enabled
Syslog Streaming	syslogstream	Enabled / Disabled	Syslog streaming enabled
SNMP Service	snmp	Enabled / Disabled	SNMP service installed
QoS	qos	Enabled / Disabled	Qualtity of Service (Shaping) enabled
App based provider selection	appbasedprovider	Enabled / Disabled	Enables/Disables the provider (ISP) selection based on the application detection (e.g. facebook uses ISP1 and google uses ISP2)
SIP Proxy	sipproxy	Enabled / Disabled	SIP proxy service installed
TCP Proxy	tcpproxy	Enabled / Disabled	TCP proxy for firewall service enabled
VPN Service	vpnserver	Enabled / Disabled	VPN Service installed
Firewall			
Number of Access rules	fwrulesenable	Number	Number of forwarding access rules
Number of Application rules	apprulesenable	Number	Number of application rules
Number of Network Objects	netobjs	Number	Number of Network objects inthe forwarding firewall
Number of App Objects	appobjs	Number	Number of application objects in the forwarding firewall

Number of URL Filter Objects	urlcatpolicys	Number	Number of URLCAT policies configurated in the forwarding firewall
Number of Connection Objects	connectionobjs	Number	Number of connection objects in the forwarding firewall
Number of Schedule Objects	schedules	Number	Number of time schedule objects in the forwarding firewall
Number of Proxy ARP Objects	proxyarpobjs	Number	Number of Proxy ARP objects in the forwarding firewall
Number of Generic IPS patterns	genipspattern	Number	Number of generic IPS pattern in the forwarding firewall
Number of bridge groups	bridginggroups	Number	Number of bridge groups in the forwarding firewall
VPN			
Mobile Portal	vpn_mobile_portal	Enabled / Disabled	VPN Mobile Portal enabled
Mobile App Access	vpn_mobile_app_access	Enabled / Disabled	VPN Mobile App Access enabled
Number of Web Forwards	vpn_web_forwards	Number	Number of the VPN Web forwards
Number of Apps	vpn_applications	Number	Number of VPN applications
Number of VPN Profiles	vpn_profiles	Number	Number of VPN profiles
VPN Clients			
Number of Client to Site Tunnels	vpn_client2site_tunnels	Number	Number of all Client to Site tunnels
Number of Client To Site Tunnels with Windows clients	vpn_client2site_windows	Number	Number of Client to Site tunnels with Windows clients
Number of Client To Site Tunnels with Mac clients	vpn_client2site_mac	Number	Number of Client to Site tunnels with Mac clients

Number of Client To Site Tunnels with Linux clients	vpn_client2site_linux	Number	Number of Client to Site tunnels with Linux clients
Number of Client To Site Tunnels with BSD clients	vpn_client2site_bsd	Number	Number of Client to Site tunnels with BSD clients
Number of Client To Site Tunnels with Android clients	vpn_client2site_android	Number	Number of Client to Site tunnels with Android clients
Number of Client To Site Tunnels with IP Sec clients	vpn_client2site_ipsec	Number	Number of Client to Site tunnels with IP Sec clients
Number of Client To Site Tunnels with L2TP clients	vpn_client2site_l2tp	Number	Number of Client to Site tunnels with L2TP clients
Number of Client To Site Tunnels with PPTP clients	vpn_client2site_pptp	Number	Number of Client to Site tunnels with PPTP clients
VPN Tunnels			
Dynamic Path Selection (TI)	vpn_dynamic_path_selection	Enabled / Disabled	Indicates if at least one VPN tunnel uses Traffic Intelligence
Dynamic VPN Routing	vpn_dynamic_vpn_routing	Enabled / Disabled	Shows if dynamic routing via VPN tunnels is enabled
WAN Opt	vpn_wanopt	Enabled / Disabled	Shows if WAN optimization is enabled for the VPN service
SSL VPN	vpn_sslvpn	Enabled / Disabled	Shows if SSL VPN is enabled for the VPN service
Single Routing Table	vpn_single_routing_table	Enabled / Disabled	Show if the VPN routes are added to the main routing table, or if separate routing tables are used
Dyn Mesh	vpn_dynamic_mesh	Enabled / Disabled	Shows if Dyn Mesh is enabled for the VPN service

Number of IP Sec site to site tunnels	vpn_site2site_tunnels_ipsec	Number	Number of site to site tunnels with IP Sec
Number of TINA site to site tunnels	vpn_site2site_tunnels_tina	Number	Number of site to site tunnels with TINA
Number of TINA site to site transports	vpn_site2site_tunnels_tina_transports	Number	Number of Site-to-Site TINA VPN transports
Number of down site to site tunnels	vpn_site2site_tunnels_down	Number	Number of Site-to-Site TINA VPN transports or IPSec tunnels that are currently down (for whatever reason)
Authentication			
DC Client	auth_dcclient	Enabled / Disabled	Authentication via DC Agent / DC Client enabled/disabled
TS Agent	auth_tsclient	Enabled / Disabled	Authentication via TS Agent / TS Client enabled disabled
WIFI AP	auth_wifiap	Enabled / Disabled	Authentication via WIFI access point enabled/disable
Networking			
3G (UMTS)	net_umts	Enabled / Disabled	Is UMTS setup enabled or disabled
xDSL	net_dsl	Enabled / Disabled	Is DSL connection enabled or disabled
Barracuda DSL Modem	net_barracuda_dsl_mode	bridgemode / advancedmode	How is the Barracuda DSL Modem configured
	net_barracuda_dsl_wan1	Enabled / Disabled	Is DSL/WAN1 enabled or disabled
	net_barracuda_dsl_wan2	Enabled / Disabled	Is WAN2 enabled or disabled
DHCP	net_dhcp	Enabled / Disabled	Is DHCP connection enabled or disabled
WIFI	wifi	Enabled / Disabled	Is WIFI connection enabled or disabled
HA	net_ha	Enabled / Disabled	Is HA setup enabled or disabled
IPv6	net_ipv6	Enabled / Disabled	Is IPv6 setup enabled or disabled

Percentage of network ports used	net_portusedperc	Percent	Percent of used network ports
Number of VLAN's	net_vlans	Number	Number of VLANs used on the box
Number of Ethernet Bonds	net_bonds	Number	Number of bonded network ports
Number of Uplinks	net_portused	Number	Number of network ports in use
SSD			
Media wearout level of 1st disk	ssd1_wearout	Number	Normalized value indicating the sanity of the first SSD (Intel SSDs): 100=brand new; 1=worn out
Media wearout level of 2nd disk	ssd2_wearout	Number	Normalized value indicating the sanity of the second SSD (Intel SSDs): 100=brand new; 1=worn out
Endurance level of 1st disk	ssd1_endurance	Number	Normalized value indicating the prospective lifetime of the first SSD (Innodisk SSDs): 0=brand new; 100=at the end of the lifetime as defined by the manufacturer
Endurance level of 2nd disk	ssd2_endurance	Number	Normalized value indicating the prospective lifetime of the second SSD (Innodisk SSDs): 0=brand new; 100=at the end of the lifetime as defined by the manufacturer

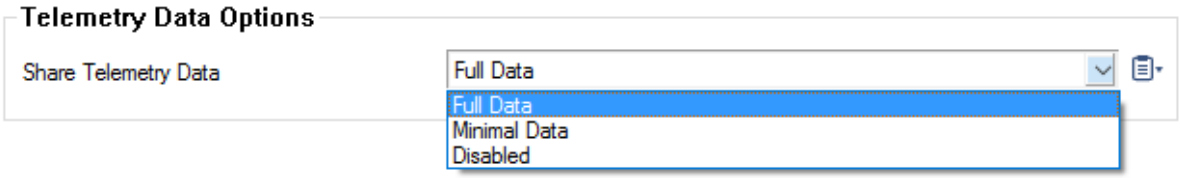
Barracuda Telemetry Server

- updates.cudasvc.com

Enable / Disable Telemetry Data

You can enable or disable the sending of usage statistics.

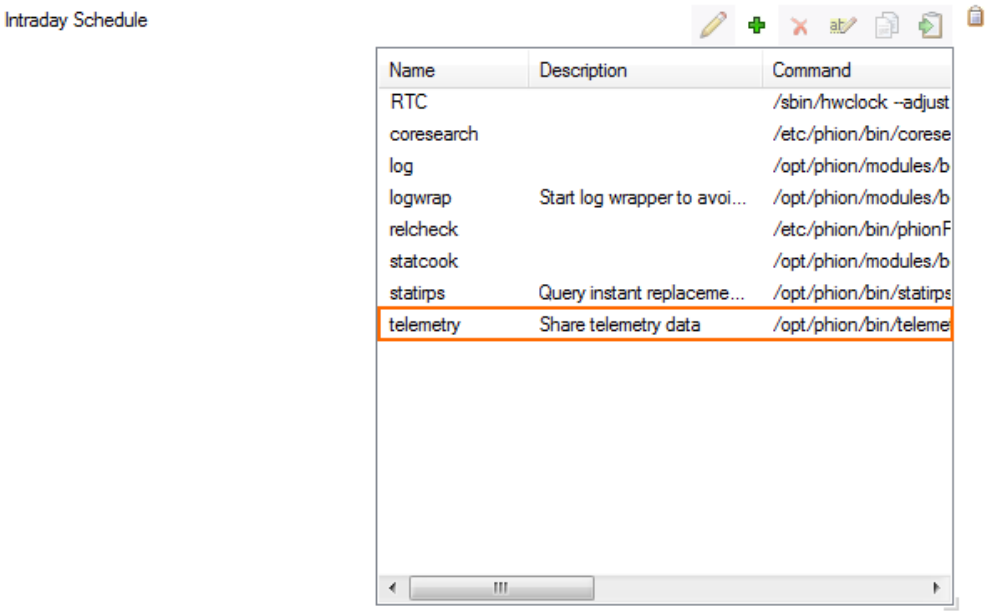
1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **Telemetry Data**.
3. Click **Lock**.
4. In the **Telemetry Data Options** section, select one of the following options:
   - **Full Data**
   - **Minimal Data**
   - **Disabled** (This option is not available for firewalls in the public cloud.)



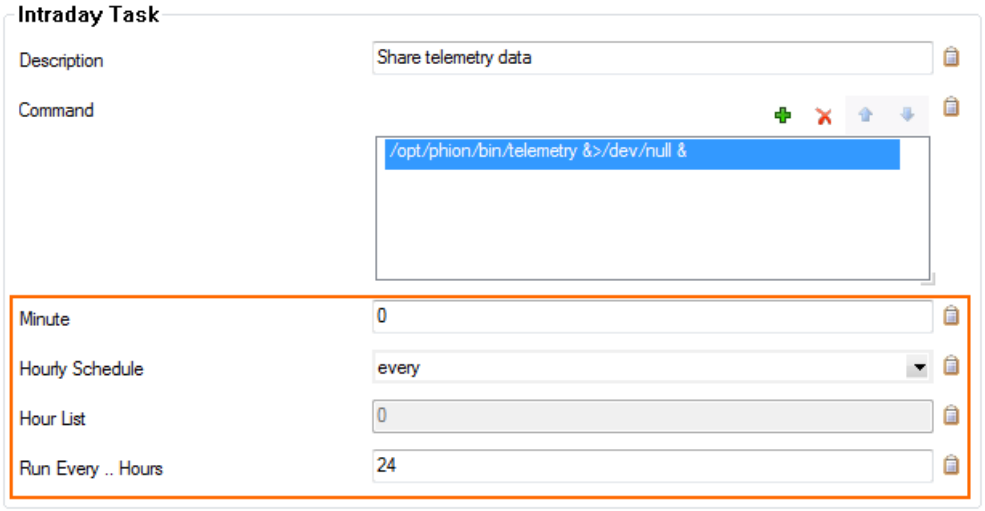
5. Click **Send Changes** and **Activate**.

Change the Schedule for Sending Telemetry Data

1. Go to **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > System Scheduler**.
2. In the left menu, click **Daily Schedule**.
3. Click **Lock**.
4. In the **Intraday Schedule**, double-click **telemetry**. The **Intraday Schedule** window opens.



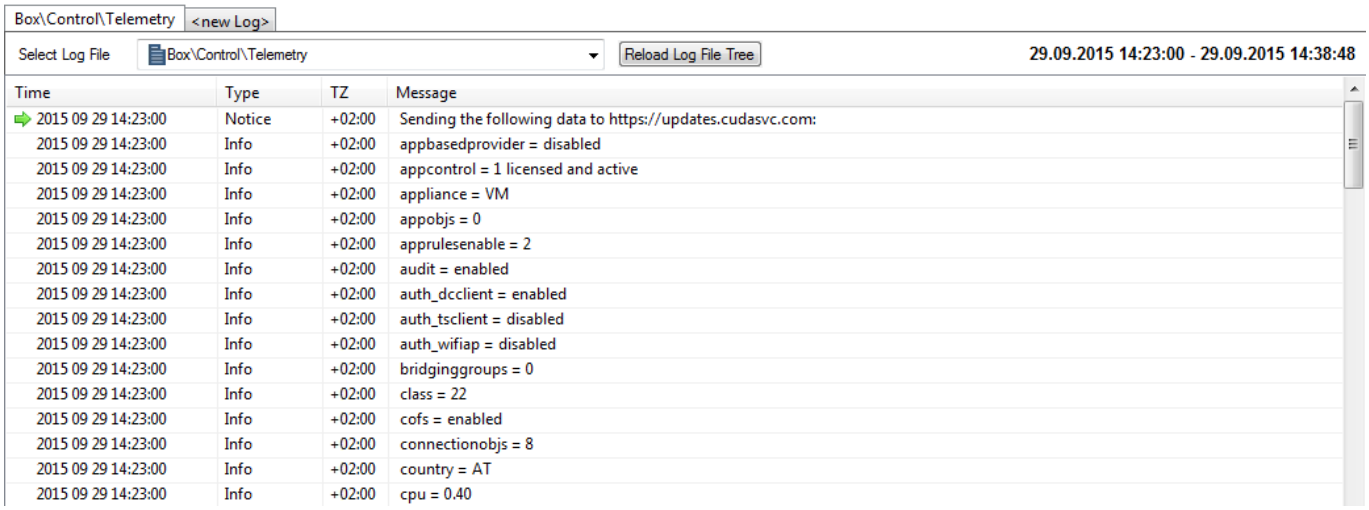
5. Change the scheduling of the telemetry task as needed.
6. Click **OK**.



7. Click **Send Changes** and **Activate**.

Viewing Data Sent to Barracuda Telemetry Servers

To see what data your CloudGen Firewall sends to the Barracuda telemetry servers, see the **\Box\Control\Telemetry** log file.



Time	Type	TZ	Message
2015 09 29 14:23:00	Notice	+02:00	Sending the following data to https://updates.cudasvc.com:
2015 09 29 14:23:00	Info	+02:00	appbasedprovider = disabled
2015 09 29 14:23:00	Info	+02:00	appcontrol = 1 licensed and active
2015 09 29 14:23:00	Info	+02:00	appliance = VM
2015 09 29 14:23:00	Info	+02:00	appobjs = 0
2015 09 29 14:23:00	Info	+02:00	apprulesenable = 2
2015 09 29 14:23:00	Info	+02:00	audit = enabled
2015 09 29 14:23:00	Info	+02:00	auth_dcclient = enabled
2015 09 29 14:23:00	Info	+02:00	auth_tsclient = disabled
2015 09 29 14:23:00	Info	+02:00	auth_wifiap = disabled
2015 09 29 14:23:00	Info	+02:00	bridginggroups = 0
2015 09 29 14:23:00	Info	+02:00	class = 22
2015 09 29 14:23:00	Info	+02:00	cofs = enabled
2015 09 29 14:23:00	Info	+02:00	connectionobjs = 8
2015 09 29 14:23:00	Info	+02:00	country = AT
2015 09 29 14:23:00	Info	+02:00	cpu = 0.40

Figures

1. t_data.png
2. telemetry_data_schedule.png
3. telemetry_data_schedule02.png
4. telemetry_data_log.png